

BIOMETRÍAS 2



BIOMETRÍAS 2

Compilado por Eduardo Thill. - 1a ed. - Buenos Aires : Jefatura de Gabinete de Ministros - Presidencia de la Nación, 2011.

590 p. ; 22x15 cm.

ISBN 978-987-27495-0-7

IMPRESO EN ARGENTINA - PRINTED IN ARGENTINA

1. Políticas Públicas. 2. Biometría. 3. Tecnologías de Información. I. Thill, Eduardo, comp.

CDD 320.6

BIOMETRÍAS 2

Eduardo Thill

Pedro Janices

Bradford Wing

Mark Branchflower

Jess Maltby

Virginia Kannemann

Julio Fuoco

Ali M. Al – Khouri

Marcos Elías Claudio de Araujo

Jorge Arturo Reina García

Mónica Litza

Néstor Mastosian

Gustavo Donato

Gabriel Casal

Mercedes Rivolta

Autoridades

Presidenta de la Nación

Dra. Cristina Fernández de Kirchner

Jefe de Gabinete de Ministros

Dr. Aníbal Domingo Fernández

Secretaría de Gabinete

Dra. Silvina Zabala

Subsecretario de Tecnologías de Gestión

Eduardo Alberto Thill

Subsecretario de Gestión y Empleo Público

Lic. Daniel Fihman

Oficina Nacional de Tecnologías de Información – ONTI

Director Nacional: Pedro Janices

Oficina Nacional de Contrataciones – ONC

Director Nacional: Guillermo Alfredo Bellingi

Instituto Nacional de Administración Pública

Director Nacional: Lic. Carlos Caramello

Este libro reúne las experiencias de algunos de los asistentes al VI Congreso Internacional de Biometría de la República Argentina (CIBRA) desarrollado en la Ciudad Autónoma de Buenos Aires los días 14, 15 y 16 de Noviembre de 2011. Su distribución es gratuita quedando expresamente vedada la utilización del presente ejemplar con fines de lucro así como la reproducción de su contenido sin la autorización de la Jefatura de Gabinete de Ministros y sus autores.

Agradecimientos

Esta publicación es el resultado del esfuerzo de todos aquellos interesados en el desarrollo y promoción de la Biometría, convocados en el marco del **VI Congreso Internacional de Biometría de la República Argentina** celebrado en la Ciudad Autónoma de Buenos Aires, durante los días 14, 15 y 16 de Noviembre de 2011.

Como en años anteriores, hemos querido sintetizar en este volumen el resultado, no solo de siete años de continuo trabajo en pos de la defensa de la identidad, sino el de poder compartir las experiencias con nuestros referentes internacionales.

Gracias al Jefe de Gabinete de Ministros, Dr. Aníbal Domingo Fernández por apoyar este proyecto desde sus comienzos depositándonos su confianza.

Gracias a Bradford Wing por su apoyo y guía en el camino transitado, a Virginia Kannemann y Natalia Aguerre por la laboriosa colaboración en el armado del libro, a Julio Fuoco por sus valiosos aportes, al Dr. Juan Antonio Travieso por su incondicional respaldo y al Lic. Carlos Caramello por su inestimable ayuda.

El mayor agradecimiento va dedicado a los investigadores y funcionarios quienes incentivarón, directa o indirectamente, a la generación de este libro.



Pedro Janices
Director Nacional
Oficina Nacional de Tecnologías de Información

Prólogo

Este libro no tiene pretensiones científicas. Su mayor interés radica en la difusión de diversos conocimientos de aplicación biométrica, pertenecientes a cada situación alcanzada en el ámbito de la Administración Pública Nacional e Internacional y del sector privado.

Su objetivo, entonces, es brindar al público interesado algunas orientaciones, o, mejor dicho, información específica. Por eso es que el orden de los artículos va de los problemas generales hacia los más especializados, aquellos que, para el universo de individuos vinculados activamente a la cuestión de la biometría, revisten de una importancia capital.

Esta suma de artículos responde, además, a una cuestión de época dado que invariablemente, todos estos temas suelen ser más hijos de la época que de sus propios autores e investigadores. Vivimos en una sociedad fragmentada e individualizada que exige respuestas particulares. Y este libro las ofrece, porque cada aporte ha sido producido por expertos que están en condiciones de formular valiosas contribuciones a la temática.

Cierto es que la mayoría de los artículos reunidos en este volumen son trabajos puntuales y que, la decisión de realizar un abordaje ecléctico de los temas hace que no ofrezcan una verdadera sistematización en su relato, pero sí hay unidad temática y un eje central: **la biometría**.

El tema es abordado desde los más diferentes ángulos, lo cual ha hecho inevitable que se produjeran algunas reiteraciones conceptuales. El hecho de que no las hayamos eliminado responde a una estrategia que invita a seguir el hilo de esas nociones repetidas una y otra vez ya que en ellas residen los más significativos núcleos de la biometría. Esa letanía casi minimalista de un mismo tema es, precisamente un signo que, al modo de una plataforma giratoria, conduce simultáneamente a muchos problemas diferentes, sin abandonar por ello su ubicación y centralidad.

En nuestro país se han llevado a cabo sucesivas ediciones de Congresos Internacionales de Biometría, acompañado de proyectos e implementaciones concretas en la Administración Pública Nacional. Esa realidad nos permite afirmar hoy que este compendio de artículos establece un foro de debate público a la vez que refuerza el desafío de las políticas públicas de inclusión social, democratización de la información e integración regional que, desde el Gobierno nacional, se vienen llevando a cabo para seguir trabajando en el marco de la protección de la identidad de las personas para brindar un aporte efectivo a las políticas de seguridad de la Nación.

Esperamos que esta iniciativa contribuya y desarrolle un campo de conocimiento que nos permita continuar realizando aportes efectivos a las demandas que nuestra realidad nos depara.



Dr. Aníbal D. Fernández
Jefe de Gabinete de Ministros

Índice

El rol de la identificación de personas en las políticas de desarrollo e inclusión digital: el Marco para la Identificación Electrónica Social Iberoamericana	
Eduardo Thill	11
Herramientas biométricas para la inclusión social y digital	
Pedro Janices	33
Normas y Biometría	
Bradford J. Wing	51
La cooperación internacional y las iniciativas de seguridad en la identificación de individuos usando el ADN o las huellas dactilares propuesta por INTERPOL	
Mark Branchflower / Jess Maltby	71
Los registros dentales: su importancia en la identificación	
Virginia Kannemann	83
Tendencias Biométricas, desafíos y oportunidades	
Julio Fuoco	99
Tecnología en Biometría y la Nueva Economía: Una Revisión del Campo y el Caso de los Emiratos Árabes Unidos	
Ali M. Al – Khouri	113
El “Proyecto RIC” como paradigma de la identificación civil brasileña	
Marcos Elías Claudio de Araujo	151
Proyecto integral de renovación tecnológica del Registro Nacional de las Personas de Honduras	
Jorge Arturo Reina García	163
Identificación para la inclusión social y digital	
Mónica Litza	179
Avance de los proyectos biométricos en el Servicio Penitenciario Federal	
Néstor Mastosian	191
Herramientas biométricas en la Provincia de Buenos Aires: Casos de Éxito	
Gustavo Donato	201
Identidad, biometría y firma digital en la región.	
El marco iberoamericano de Identificación Electrónica Social	
Gabriel Casal / Mercedes Rivolta	213
Anexo: Marco para la Identificación Electrónica Social Iberoamericana	243

El rol de la identificación de personas en las políticas de desarrollo e inclusión digital: el Marco para la Identificación Electrónica Social Iberoamericana

Eduardo Thill



Eduardo Thill

Subsecretario de Tecnologías de Gestión. Secretaría de Gabinete.



Actualmente se desempeña como Subsecretario de Tecnologías de Gestión de la Secretaría de Gabinete, Jefatura de Gabinete de Ministros de la República Argentina. Ocupó sucesivamente el cargo de Director General de Gestión Informática del Ministerio del Interior y del Ministerio de Justicia y Derechos Humanos, en el periodo comprendido entre 2003 y 2009.

Durante su gestión en el Ministerio del Interior fue responsable Técnico de elaborar el proyecto global que permite contar con una base de datos poblacional, contemplando la identificación plena de los individuos. En el año 2002 fue Director de Gestión Informática de la Secretaría General de la Presidencia de la Nación, donde además de las funciones del cargo, actuó como responsable de enlace entre dicha Secretaría, el gobierno de Tucumán y el Consejo Nacional de Coordinación de Políticas Sociales, estando a cargo de las acciones concernientes al Operativo Rescate implementado en esa Provincia.

Ha participado como co-expositor por el Gobierno Argentino en el Biometric Consortium Conference 2008 y como asistente en BCC2007 y BCC2009 y al Biometrics 2005 en Londres. Es co-fundador y organizador de los Congresos Internacionales de Biometría de la República Argentina (CIBRA), que se realizan anualmente desde 2006 a la fecha.

Información de contacto: ethill@jefatura.gob.ar

Resumen

Los gobiernos de nuestra región se encuentran transitando un camino de crecimiento económico con justicia social. Para ello, despliegan políticas públicas para el desarrollo, con los objetivos de mejorar la calidad de vida de sus habitantes y lograr la plena inclusión social de aquellos que quedaron rezagados en el pasado. Nuestras administraciones han ido incorporando en su gestión el uso de las tecnologías de la información y las comunicaciones tanto para ejecutar políticas públicas sustantivas, como para vincularse con el ciudadano. Han diseñado agendas para lograr la plena inclusión digital de los habitantes de la región, apuntando a lograr una efectiva inserción de nuestros países en la sociedad del conocimiento. Por otra parte, nuestros gobiernos han resaltado la importancia de llevar adelante políticas públicas tendientes a superar las brechas existentes en nuestras sociedades. Así, la región está ejecutando políticas de educación, de salud, de desarrollo social, que se proponen objetivos de desarrollo económico social en un marco de inclusión, justicia y equidad.

En este contexto, la identificación de personas cobra un rol relevante. Sin identificación no existen derechos. El ejercicio de los derechos requiere necesariamente la identificación plena de las personas, función que corresponde al Estado. El Estado es el responsable de la identificación de las personas, y de garantizar la identidad a cada uno. En un mundo cada vez más informatizado, los gobiernos utilizan las TIC para la implementación de las políticas públicas sustantivas. Cómo lograr la plena identificación de las personas, cómo reconocer entre países dichas identificaciones, cómo facilitar el acceso remoto a los servicios que brinda la administración, son cuestiones que tienen que ver con una adecuada identificación electrónica de las personas. Esta identificación electrónica es necesaria para el acceso a sistemas informáticos, a las aplicaciones de gobierno electrónico, de comercio electrónico, pero también para la ejecución de políticas sociales. Además de este uso, los modernos documentos de identidad, básicamente los pasaportes y los documentos nacionales, están utilizando elementos de identificación electrónica, lo cual lleva a considerar que aún en los supuestos de identificación presencial, las tecnologías de la información y las comunicaciones cumplen un rol relevante.

El artículo presenta el Marco para la Identificación Electrónica Social Iberoamericana, las cuestiones problemáticas que surgen en la materia y los principales aspectos involucrados.

Palabras clave: inclusión digital, ciber-identidad, biometría, seguridad.

El rol de la identificación de personas en las políticas de desarrollo e inclusión digital: el Marco para la Identificación Electrónica Social Iberoamericana

Introducción

“Los objetivos del gobierno electrónico deben trascender la mera eficacia y eficiencia de los procesos de administración, hacia formas que permitan cambios sociales, políticos, económicos en pro del desarrollo humano, la igualdad de oportunidades y la justicia social.”
(DECLARACIÓN DE LISBOA; 2010)

Los gobiernos de nuestra región se encuentran transitando un camino de crecimiento económico con justicia social. Para ello, despliegan políticas públicas para el desarrollo, con los objetivos de mejorar la calidad de vida de sus habitantes y lograr la plena inclusión social de aquellos que quedaron rezagados en el pasado.

Este nuevo enfoque latinoamericano, que pone en el centro de la escena a la persona, pudo corroborarse en las distintas reuniones realizadas durante el año 2010 en el marco de la Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Los países participaron de distintos encuentros sectoriales (Agricultura, Salud, Trabajo, Administración Pública y Reforma del Estado, Turismo, Educación, Infancia y Adolescencia, Justicia, Presidencia, Vivienda y Urbanismo), confluendo en la XX Cumbre Iberoamericana, que emitió la Declaración de Mar del Plata “Educación para la Inclusión Social”.

En cada una de las reuniones ministeriales sectoriales se abordó el tema de la inclusión social como eje de las políticas públicas de la región. Especialmente, en la XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), celebrada en Lisboa, Portugal, en la cual se trató el tema de la Participación de los Ciudadanos en la era del Gobierno electrónico. En ese marco, por primera vez se introdujo en forma consensuada el concepto de “**justicia social**” como principio inspirador de las políticas públicas de Iberoamérica.

En dicho encuentro, se acordó trabajar en la construcción de “*un modelo de Administración más abierto, transparente y colaborativo, que permita responder eficazmente a los desafíos económicos, sociales, culturales y ambientales que se plantean a nivel mundial*”. A tal fin, la Declaración contempla el uso de las TIC para transformar la Administración, recomendando a los países que impulsen “*las políticas de administración electrónica y simplificación administrativa deben contribuir, de manera articulada, al desarrollo de servicios públicos con mayor calidad*”.
(MARCO; 2011)

La Declaración de Lisboa reconoce que “*el desarrollo de mecanismos de identificación y autenticación electrónica seguros, es otra de las condiciones para el cambio pretendido, destacándose su papel en la promoción de simplificación de procedimientos y en el fomento de*

la utilización de los servicios electrónicos.”

Nuestras administraciones están protagonizando un momento muy especial. Cada país lleva adelante su agenda digital, con una clara visión: lograr la más amplia inclusión digital de su gente. En Argentina, por ejemplo, a partir del año 2003, tanto durante la presidencia del Dr. Kirchner como con la actual Presidenta de la Nación, Cristina Fernández de Kirchner, el gobierno construyó una política de Estado de inclusión social, para lograr garantizar la igualdad de oportunidades a todos los habitantes. Estas políticas, inspiradas en el principio de Justicia social, se tradujeron en los distintos programas e iniciativas que lleva adelante el gobierno nacional: Asignación Universal por Hijo, Argentina Conectada, Televisión Digital Abierta, Conectar Igualdad, etc. Estos programas, a su vez, se interconectan, se realimentan, se reconfiguran permanentemente; son la expresión del modelo social de la agenda digital argentina: inclusión digital, igualdad de oportunidades, justicia social.

Estos programas han requerido para su ejecución efectiva en tan poco tiempo, de un despliegue muy importante de organizaciones públicas. Esto no hubiera sido posible si los organismos responsables no hubieran estado preparados para ello, y esta preparación incluye sin lugar a dudas, de los elementos tecnológicos de gobierno electrónico que les ha facilitado tanto para su gestión interna como para vincularse con los beneficiarios y con el ciudadano.

Los países iberoamericanos, por su parte, están desarrollando sus propias agendas para lograr la plena inclusión digital de los habitantes de la región, apuntando a lograr una efectiva inserción de nuestros países en la sociedad del conocimiento. En general, nuestros gobiernos han resaltado la importancia de llevar adelante políticas públicas tendientes a superar las brechas existentes en nuestras sociedades. Así, la región está ejecutando políticas de educación, de salud, de desarrollo social, que se proponen objetivos de desarrollo económico social en un marco de inclusión, justicia y equidad.

En este contexto, la identificación de personas cobra un rol relevante. Por un lado, porque sin identificación no existen derechos. El ejercicio de los derechos requiere necesariamente la identificación plena de las personas. Este rol en nuestro país lo cumple el Estado. El Estado es el responsable de la identificación de las personas, y de garantizar la identidad a cada uno. Por otra parte, la ejecución de las políticas públicas sustantivas que implican una interrelación masiva con los habitantes, sobre todo las de carácter social y las de inclusión digital, requiere la identificación de las personas en entornos electrónicos.

La identificación electrónica es necesaria para el acceso a sistemas informáticos, a las aplicaciones de gobierno electrónico, de comercio electrónico, pero también para la ejecución de políticas sociales. Además de este uso, los modernos documentos de identidad, básicamente los pasaportes y los documentos nacionales, están utilizando elementos de identificación electrónica, lo cual lleva a considerar que aún en los supuestos de identificación presencial, las tecnologías de la información y las comunicaciones cumplen un rol relevante.

A nivel regional se plantea también el tema: cómo lograr la plena identificación de las personas, cómo reconocer entre países dichas identificaciones, cómo facilitar el acceso remoto a los servicios que brinda la administración, son cuestiones que tienen que ver con una adecuada

identificación electrónica de las personas.

El presente artículo presenta el Marco para la Identificación Electrónica Social Iberoamericana, complementario de la Carta Iberoamericana de Gobierno Electrónico.

Las Políticas de Inclusión Social

En esta segunda década del S XXI, con una crisis económica que afecta a los países desarrollados, nuestro país y los países hermanos de la región nos encontramos transitando un camino distinto al recorrido en los años 90. Nuestros gobiernos se han propuesto hacer jugar al Estado un rol activo, tanto en la economía como en otros aspectos de la vida social. En ese marco, asistimos a un proceso de reconstrucción de la relación entre el Estado y la sociedad.

Protagonizamos un momento en el cual en conjunto estamos repensando lo que entendemos por Estado-nación. Después de la crisis de fin de siglo, nos encontramos frente al desafío de reconstituir una comunidad ética, política y socioeconómica. *"Ello implica, una vez más, poner en el centro la cuestión de la igualdad."* (CEPAL; 2010)

Estamos en un verdadero punto de inflexión entre el modelo neoliberal donde el Estado cumplía un rol subsidiario, y el modelo social en el cual el Estado cumple un rol activo. Un cambio de esta magnitud requiere e implica un cambio en los valores subyacentes, en los valores compartidos por todo el cuerpo social.

En efecto, el nuevo modelo social implica poner en lugar central el interés general y la provisión de bienes públicos. Según la CEPAL (2010), el interés general *"remite a la creación y provisión por parte del Estado de bienes públicos que beneficien a toda la sociedad. Estos bienes requieren de inversiones considerables cuyos resultados muchas veces se materializan solo a largo plazo. Se pueden encontrar bienes públicos en esferas tan diversas como la educación, la salud, la infraestructura productiva, el transporte, las comunicaciones, la energía, el medio ambiente, la inversión en ciencia y tecnología, la paz social tanto interna como externa, la administración de justicia, las elecciones democráticas y la seguridad pública."*

En este sentido, nuestros países están avanzando notablemente. A modo de ejemplo, cabe mencionar los acuerdos alcanzados por los gobiernos de la región en las sucesivas reuniones de sus ministros. La Declaración de Mar del Plata de 2010 refleja esta decisión. En ella, los países signatarios expresaron su consenso acerca de la necesidad de enfrentar *"el desafío de consolidar modelos de crecimiento económico que profundicen la equidad e inclusión social"*, señalando que *"la educación es un vehículo fundamental para el logro de tales objetivos"*. (DECLARACION MAR DEL PLATA; 2010)

En consonancia, los gobiernos reforzaron la idea a través del Consenso de Asunción de este año, en el cual los Ministros de Administración Pública y Reforma del Estado acordaron que *"el Estado es un instrumento fundamental e insustituible para promover y garantizar el desarrollo sostenible de Iberoamérica. Desarrollo que comprende el incremento de la calidad de vida y la felicidad de la ciudadanía, en todos los ámbitos: privado, público, individual y colectivo; abarcando diferentes dimensiones tales como lo político, lo social, lo cultural, lo económico, lo*

ambiental, entre otros. Desarrollo para el bienestar de toda la sociedad, con inclusión, equidad y justicia social". (CONSENSO ASUNCION; 2011)

Otro de los valores que a nuestro entender deben estar presentes es el valor de la visión estratégica concertada acerca del nuevo rol para el Estado, que implica estar presente, tomar la iniciativa, articular los medios, anticiparse a las crisis y prevenirlas, todo ello en un marco de amplia participación social. Pensar el futuro, actuar el presente, aprender del pasado: para construir hacia adelante. *"Tal como en la vida de las personas, el futuro de las sociedades se construye a lo largo del tiempo: una sociedad que no se educa, que no invierte en cohesión social, que no innova, que no construye acuerdos ni instituciones sólidas y estables, tiene pocas posibilidades de prosperar. Ante estos desafíos, el Estado debe ser capaz de proveer una gestión estratégica con una mirada de largo plazo, tener un papel anticipador e intervenir en el diseño de estrategias orientadas al desarrollo nacional. Esto exige tomar en cuenta que la acción estatal se desenvuelve en un escenario de poder compartido, de manera que la negociación y la construcción de consensos nacionales estratégicos son medio y fin a la vez."* (CEPAL; 2010)

Como síntesis, la época rescata el valor de la política. La experiencia nos ha demostrado que el modelo basado en el mercado es insuficiente, y a la larga lleva a crisis profundas. Un modelo basado en la persona, implica que el Estado se juegue para garantizar la igualdad de acceso a los bienes públicos para todos los habitantes. La persona como sujeto de derecho, el Estado como garante de la igualdad de oportunidades. Acceso igualitario a la educación, a la salud, a la seguridad social, a la sociedad del conocimiento.

En esta línea de pensamiento, nuestros gobiernos han impulsado políticas que han retomado lo público como el espacio de lo colectivo, del hacer de todos los ciudadanos y no solo del gobierno o el Estado.

En Argentina, a partir de 2003 con la presidencia del Dr. Néstor Kirchner, se abrió un período de reconstrucción social. En su discurso de asunción ante la Asamblea Legislativa, el entonces presidente señaló los ejes de la política que iba a guiar su gobierno. Después de señalar que en los 80 se puso el énfasis en la recuperación democrática, que en los 90 se centró la gestión en el mercado con las consecuencias sabidas, señaló su propósito de *"promover políticas activas que permitan el desarrollo y el crecimiento económico del país, la generación de nuevos puestos de trabajo y la mejor y más justa distribución del ingreso. Como se comprenderá el Estado cobra en eso un papel principal, en que la presencia o la ausencia del Estado constituye toda una actitud política."* (KIRCHNER; 2003).

Más adelante, el Presidente Kirchner señala que *"Se trata de tener lo necesario para nuestro desarrollo, en una reingeniería que nos permita constar con un Estado inteligente. Queremos recuperar los valores de la solidaridad y la justicia social que nos permitan cambiar nuestra realidad actual para avanzar hacia la construcción de una sociedad más equilibrada, más madura y más justa. Sabemos que el mercado organiza económicamente, pero no articula socialmente, debemos hacer que el Estado ponga igualdad allí donde el mercado excluye y abandona."* (KIRCHNER; 2003). Con esta reflexión, daba vuelta la página de la historia previa de crisis continuas.

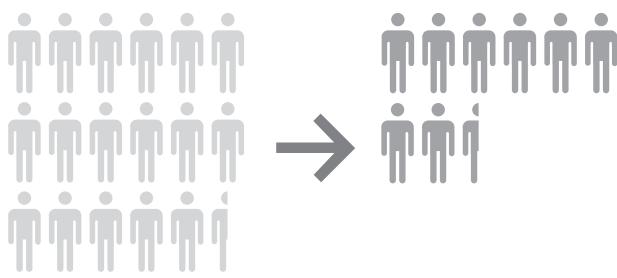
Desde esta concepción cuyo pilar es la justicia social, el gobierno de entonces inició un camino destinado a brindar acceso igualitario a los bienes públicos, incluyendo para integrar socialmente. Se trabajó fuertemente en los temas sociales, educativos, de salud, y especial énfasis se puso en elaborar políticas públicas orientadas a superar la brecha digital. En ese sentido, se anticipó 7 años a lo que advirtió la CEPAL en 2010, cuando al referirse a los valores, reclama un nuevo rol del Estado en el marco de la plena vigencia de la democracia. (CEPAL; 2010) Expresaba el Presidente Kirchner en el mensaje de asunción: “*Es el Estado el que debe actuar como el gran reparador de las desigualdades sociales en un trabajo permanente de inclusión y creando oportunidades a partir del fortalecimiento de la posibilidad de acceso a la educación, la salud y la vivienda, promoviendo el progreso social basado en el esfuerzo y el trabajo de cada uno.*” (KIRCHNER; 2003)

Desde esta visión, se construyeron consensos para definir políticas de Estado inclusivas, básicamente en educación, empleo e infraestructura. Estas políticas a la hora de ser ejecutadas, presentaron un importante desafío para su instrumentación. Uno de las primeras cuestiones a resolver fue la de poder identificar a las personas beneficiarias. Otro de los aspectos distintivos, fue que se contempló la inclusión digital desde un primer momento. Se consideró que el Estado tiene un rol preponderante en garantizar el acceso igualitario a los bienes públicos, uno de los cuales tiene que ver con superar la brecha digital y facilitar la participación de todos en la sociedad del conocimiento.

En consecuencia, podemos afirmar que tal como señala CEPAL, las políticas desarrolladas por el gobierno en Argentina, lograron transformar la estructura productiva a partir de la coordinación de políticas. Se logró mejorar el perfil industrial, estimulando los sectores más intensivos en innovación; el tecnológico, fortaleciendo la oferta y su articulación con la demanda; el educativo, mediante la distribución de instrumentos informáticos en los establecimientos públicos y la inversión del 6,7% del PBI. (CEPAL; 2010). Como consecuencia de estas políticas disminuyó el nivel de desempleo en un 50% (ver Cuadro Nro.1) y aumentó notablemente la participación de los trabajadores en el PBI, alcanzando a 2010 el 44,9% (ver Cuadro Nro. 2).

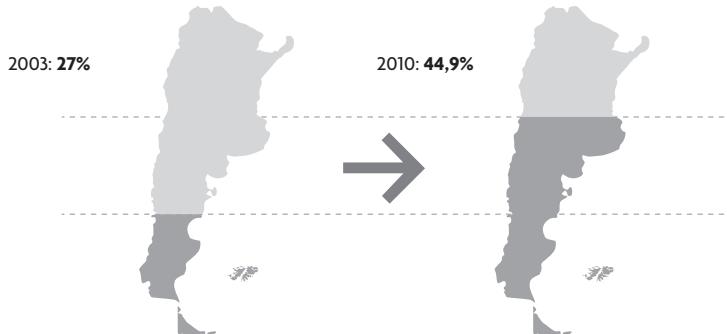
Cuadro Nro. 1: Evolución del nivel de empleo

Desocupación



Fuente: Indec. <http://www.presidencia.gov.ar/component/content/article/138-indicadores/6177-desempleo>

Cuadro Nro. 2 – Participación de los trabajadores en el PBI



Fuente: Indec. <http://www.presidencia.gov.ar/component/content/article/138-indicadores/6191-mayor-participacion-de-los-trabajadores-en-el-pbi>

Con respecto a lo que sucedió en América Latina, en las reuniones que se fueron desarrollando a lo largo del año 2010 para preparar la Cumbre Iberoamericana de Jefes de Estado y de Gobierno, los ministros de las distintas carteras convocados, responsables de las áreas de Agricultura, Salud, Trabajo, Administración Pública y Reforma del Estado, Turismo, Educación, Infancia y Adolescencia, Justicia, Presidencia, Vivienda y Urbanismo, fueron acordando los objetivos a lograr en cada uno de los países, que se tradujo en la Declaración de Mar del Plata “Educación para la Inclusión Social”.

En esa oportunidad, los Jefes y Jefas de Estado y de Gobierno reiteraron el objetivo común de avanzar en la construcción de sociedades justas, democráticas, participativas y solidarias en el marco de la cooperación e integración cultural, histórica y educativa iberoamericanas, lograr una educación con inclusión social intra e intercultural en la región iberoamericana de calidad para todos y todas, para promover una Iberoamérica más justa, con desarrollo económico, social y cultural en el marco de sociedades democráticas, solidarias y participativas que promuevan el bienestar de todos los habitantes de nuestra región.

En las reuniones ministeriales sectoriales preparatorias se planteó la problemática de la inclusión social como eje de las políticas públicas de la región. En la XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), celebrada en Lisboa, Portugal, se abordó el tema de la Participación de los Ciudadanos en la era del Gobierno electrónico, acordando que “los objetivos del gobierno electrónico deben trascender la mera eficacia y eficiencia de los procesos de administración, hacia formas que permitan cambios sociales, políticos, económicos en pro del desarrollo humano, la igualdad de oportunidades y la justicia social.” (DECLARACION DE LISBOA; 2010)

En el encuentro de Lisboa, los países acordaron la conveniencia de avanzar en acciones de gobierno electrónico. En concreto, declararon su propósito de abordar los siguientes puntos:

- Impulsar programas que relacionen la administración electrónica con la simplificación administrativa, con el objetivo de hacer más simples, rápidas y eficaces las interacciones de los ciudadanos y de las empresas con la Administración,

- Intercambiar experiencias entre la comunidad iberoamericana, en lo que concierne a la creación de servicios integrados únicos, físicos o virtuales, que se organicen en función de la demanda ciudadana y de las empresas,
- Intercambiar experiencias relativas a la implementación de formas de identificación electrónica y biométrica seguras y de mecanismos de articulación para el desarrollo de los servicios electrónicos transfronterizos, en el espacio iberoamericano,
- Articular el Intercambio de experiencias de utilización de las TIC, para asegurar la transparencia de los procesos de decisión pública y para ofrecer nuevas formas de participación democrática,
- Promover políticas y prácticas de inclusión digital y otros mecanismos que faciliten el acceso a los servicios electrónicos, para que los ciudadanos puedan beneficiarse de las potencialidades de las TIC, en condiciones de igualdad y universalidad, de forma de asegurar la cohesión social y territorial.

En síntesis, asistimos a un proceso de revalorización del Estado en un rol activo orientado a mejorar las condiciones de vida de nuestra gente. Un Estado presente, que promueva la inclusión social mediante políticas públicas efectivas. Estas iniciativas van de la mano con la convicción de que la sociedad del conocimiento es el escenario futuro, así como con la convicción de la necesidad de acercar el Estado al ciudadano, para lo cual el gobierno electrónico es una herramienta eficaz.

Relevancia de la cuestión de la identificación de las personas

En el contexto señalado, con los países de la región llevando adelante políticas públicas de inclusión social activas, el tema de la correcta identificación de las personas constituye un elemento clave de éxito, tanto para la ejecución de políticas masivas de inclusión social, como para la autenticación de los ciudadanos en entornos electrónicos. Como nuestros países han avanzado en la implementación de medidas de gobierno electrónico, uno de los aspectos que han surgido es el de la correcta identificación de personas en plataformas informáticas.

En 2007 la Carta Iberoamericana de Gobierno Electrónico señalaba la necesidad de que el empleo de las TIC en la gestión pública debe estar centrado en el ciudadano y sus derechos, considerando como “ciudadano” a “*cualquier persona natural o jurídica que tenga que relacionarse con una Administración Pública y se encuentre en territorio del país o posea el derecho a hacerlo aunque esté fuera de dicho país.*”

La Carta Iberoamericana de Gobierno Electrónico enfatiza el rol central de la persona, no de la tecnología; en consecuencia, impulsa el reconocimiento del derecho del ciudadano a relacionarse electrónicamente con la Administración Pública. Este reconocimiento del derecho de toda persona a relacionarse con la administración por medios electrónicos implica establecer una puerta de acceso a la información, sentar las bases para el gobierno abierto; acercar el Estado al ciudadano superando las barreras físicas y geográficas.

En ese sentido, la Carta Iberoamericana de Gobierno Electrónico destaca “el rol insustituible que le corresponde a los Estados en estas materias, para garantizar la universalización a toda la

población y la continuidad de los servicios electrónicos y el fortalecimiento de la democracia.” Vemos entonces cómo se enlaza el tema de la inclusión digital con el despliegue de las políticas públicas en general en democracia.

La Carta define el concepto de “gobierno electrónico” como sinónimo de “administración electrónica”, entendiendo por tal al *“uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos.”*

La Carta aborda la cuestión de la identificación de las personas como un instrumento del gobierno electrónico. Señala la obligación que tiene el Estado de facilitar a los ciudadanos (en sentido amplio) el acceso electrónico a la administración. La Carta identifica como un factor fundamental *“la identificación de los ciudadanos, Administraciones Públicas, funcionarios y agentes de éstas que empleen medios electrónicos, así como la autenticidad de los documentos electrónicos en que se contiene la voluntad o manifestaciones de todos ellos.”* (CARTA; 2007).

La Carta recomienda a los Estados emitir las normas jurídicas y técnicas que aseguren a los ciudadanos y a las Administraciones Públicas las condiciones necesarias para que *“en sus relaciones electrónicas puedan tener seguridad y confianza, tanto en lo que se refiere a la identidad de la persona, órgano o institución que se comunica, como en lo que se refiere a la autenticidad e integridad del contenido de la comunicación, así como, consecuentemente, en la imposibilidad de ser repudiada por el emisor.”*

Con respecto a la autenticidad e integridad de la comunicación, la Carta considera que una comunicación es tal si se corresponde con la originalmente emitida sin que sus contenidos hayan sido alterados. Recomienda en tal sentido a los Estados, que contemplen en la regulación sobre seguridad del Gobierno Electrónico los *“sistemas físicos, sistemas de firma electrónica, incluso avanzada, así como otros sistemas alternativos a la firma electrónica, cuanto la naturaleza del trámite lo aconseje, que permitan identificar al comunicante y asegurar la autenticidad del contenido de la comunicación.”*

Vemos entonces que la Carta Iberoamericana de Gobierno Electrónico destaca a la identificación de las personas como un elemento central para la implementación de políticas de gobierno electrónico. El rol del Estado es central para lograr una correcta identificación de las personas que permite la ejecución de políticas públicas, como en su rol vinculado con la identificación en entornos electrónicos.

En el ambiente electrónico, la Carta menciona como elementos de autenticación a la firma electrónica simple y a la firma digital o firma electrónica avanzada, como instrumentos que permiten identificar la autoría de un documento electrónico, confirmar su integridad y también, confirmar la identidad de una persona en el entorno digital.

En ese contexto, y siguiendo las recomendaciones de la Declaración de Lisboa, los gobiernos iberoamericanos consideraron la necesidad de complementar la Carta Iberoamericana de Gobierno Electrónico con un Marco específico de identificación electrónica social, que brinde

un marco conceptual en la región que sirva de guía para la identificación de las personas y la autenticación electrónica, elemento básico para el pleno ejercicio de los derechos y la efectiva implementación de políticas públicas de inclusión social. (MARCO; 2011)

Marco para la identificación electrónica social Iberoamericana

En base a los antecedentes mencionados, se presentó a consideración el Marco Iberoamericano de Identificación Electrónica Social en la XIII Conferencia Iberoamericana de Ministros y Ministras de Administración Pública y Reforma del Estado realizada en Asunción, Paraguay, el 1º de julio de 2011, cuyo texto fue aprobado.

El Marco presenta la problemática de la identificación de las personas desde la perspectiva tecnológica, considerando que es una necesidad comenzar a plantear estándares comunes para lograr articular la correcta identificación de personas en la región. El documento presenta entonces una sección explicativa, en la cual describe los elementos que están presentes en la identificación de personas, el marco legal involucrado y las consecuencias que se derivan.

Además, describe en términos sencillos las tecnologías involucradas: biometrías y firma digital. Porqué dichas tecnologías y no otras? Pues porque el mundo ha avanzado en el uso de tecnologías biométricas para los documentos nacionales que acreditan las identidades de las personas, por ejemplo, pasaportes. Y firma digital porque en nuestros países se ha avanzado en el dictado de leyes que reconocen su valor legal y su uso para el comercio electrónico y el gobierno digital. Pero dado que dichas normas son de carácter nacional, se torna necesario comenzar a plantear estándares comunes que permitan el reconocimiento de dichas firmas digitales más allá de las fronteras.

Elementos de la identificación electrónica

Identificación y Pleno Ejercicio de los Derechos

La identidad de la persona es la base sobre la que se apoya el conjunto de derechos y obligaciones. La posibilidad de reclamar y ejercer un derecho está asociada a una persona en particular, con sus atributos y su identidad. El procedimiento que mediante elementos externos, permite asignar una identidad con determinados atributos a una persona concreta es lo que denominamos “identificación”. (MARCO; 2011)

Esta relación entre la persona concreta y determinados atributos que definen su identidad, por ejemplo, el nombre, el lugar de nacimiento, las huellas dactilares, los datos de filiación, permite por un lado, identificar únicamente a cada persona; y por otra parte, verificar dicha identidad cada vez que resulte necesario, ya sea para ejercer un derecho, acceder a un plan social, trasladarse de un país a otro, etc.

Este proceso de identificación en nuestro país es una función indelegable del Estado. Es el Estado quien identifica a las personas, quien verifica los datos que permiten esta identificación, quién emite el documento que acredita la identidad y quien debe resguardar el ejercicio del derecho a la identidad.

Por otra parte, el Estado necesita esta identificación para una correcta y efectiva implementación de políticas públicas de alcance social. La identificación de las personas es un elemento esencial de los actos jurídicos, ya que el error sobre la identidad de la persona, acarrea la nulidad del acto, al constituir un vicio del consentimiento que invalida la relación jurídica.

En Argentina, la identificación de las personas está regulada por la Ley Nro. 17.671 (Ley de Identificación, Registro y Clasificación del Potencial Humano Nacional), y se realiza mediante un Documento Nacional de Identidad. Por esta razón, desde el año 2003 se ha ido trabajando en la digitalización del trámite de dicho documento, primero con las bases de datos biométricos existentes en formato papel, que implicó el tratamiento electrónico de 50.000.000 de fichas. Esto permitió luego informatizar el trámite de solicitud y otorgamiento del documento, lo cual hoy es una realidad.

Internacionalmente, los documentos de identificación transfronteriza que se utilizan son los pasaportes. Algunos países cuentan con normas que establecen documentos únicos de identificación. Pero todos comparten los estándares para los pasaportes, debido a la necesidad de ser reconocidos más allá de las fronteras del país emisor.

En síntesis, una persona que no ha sido identificada por el Estado, es una persona “inexistente”, desde el punto de vista legal. La implementación de políticas públicas sustantivas, sobre todo las de alcance social, requieren para su ejecución la correcta identificación de las personas. Y esto no es posible en esta segunda década del S XXI sin apoyo de la tecnología. Tecnologías biométricas que están disponibles y que responden a estándares internacionalmente aceptados.

Biometría e Identificación

El mecanismo de identificación de una persona se basa en la comparación de un rasgo con un dato. Hoy existen tecnologías que permiten automatizar este cotejo de datos, acelerando el tiempo de otorgamiento de documentos y de verificación de identidad.

Aun para los documentos en soporte papel, o sea, para la identificación de personas en entornos físicos, se han ido incorporando tecnologías biométricas automatizadas que, dado que siguen estándares internacionales, facilitan la trazabilidad de los datos.

Las tecnologías biométricas permiten la identificación en base a características físicas de un individuo: el ADN, las huellas digitales, los rasgos faciales o las características del iris, datos que son propios y únicos a una persona en particular.

Las tecnologías biométricas hoy están presentes en múltiples aplicaciones públicas y privadas. Por ejemplo, en las redes sociales, cuando al subir una fotografía el aplicativo automáticamente le asigna el nombre y apellido de la persona que, de acuerdo con los datos de reconocimiento facial que dispone, el sistema interpreta como correctos. Esta aplicación ha sido cuestionada, pues podría afectar el derecho a la intimidad y privacidad, identificando sin autorización una foto y con un alto grado de error.

En el ámbito público, la biometría se utiliza tanto para identificar a las personas, como para

autenticar su identidad en sistemas informáticos, reforzar la seguridad pública en aeropuertos y ciudades, y restringir el acceso a sitios seguros, tanto físicos (edificios) como virtuales (sistemas y aplicaciones informáticas). Este reconocimiento se realiza a partir de características físicas (huellas dactilares, rasgos de la mano o de la cara, patrones del iris) o de características conductuales aprendidas o adquiridas (patrones de voz, patrones de firma ológrafo, patrones de teclado).

Existen diversos dispositivos que se usan para albergar las tecnologías biométricas, para identificar personas. Estos dispositivos que se utilizan para autenticar personas se apoyan en distintos factores, de acuerdo al nivel de seguridad que la aplicación requiera. Comúnmente se considera como factores de autenticación algo que sé (por ejemplo, una clave), algo que tengo (por ejemplo, una tarjeta inteligente) y algo que soy (biometría). El uso de los tres factores de autenticación dota de seguridad al proceso.

El Marco de Identificación Electrónica Social contiene una descripción de estos factores de autenticación, incluyendo la definición de los conceptos de biometrías y tecnologías biométricas.

Infraestructuras de Firmas Digitales

Los países de la región han avanzado en la consolidación de sus marcos legales para otorgar valor jurídico a los documentos y firmas electrónicas y digitales. En ese proceso, muchos han adoptado esquemas de firma digital, es decir, de infraestructuras de clave pública en las cuales un órgano del Estado licencia a proveedores de certificados digitales.

Sin embargo, estas infraestructuras de clave pública tienen un alcance legal limitado: las fronteras de cada país. Esto es así no por un problema tecnológico, sino por la naturaleza de los sistemas jurídicos nacionales, en los cuales las leyes solo tienen alcance dentro de las fronteras, a menos que medien acuerdos internacionales hasta la fecha.

En el caso del reconocimiento de las firmas digitales, si bien en general las normas nacionales lo contemplan como una posibilidad, no se han formulado acuerdos de reconocimiento mutuo entre países.

Esta circunstancia dificulta el ponerse de acuerdo en aplicaciones transnacionales, tanto de orden público como privado. Es así que surgió la idea de comenzar a establecer un marco conceptual compartido que permita ir delineando mínimos comunes denominadores para avanzar en futuros acuerdos sobre firma digital y autenticación electrónica.

Finalidad y ámbito de la identificación electrónica social Iberoamericana

En su Capítulo I, el Marco Iberoamericano define los objetivos, principios y finalidades que lo inspiran.

Dentro de sus **objetivos** se propone conformar un marco genérico de principios rectores, políticas y procedimientos de gestión, para sentar las bases a que permitan diseñar un futuro esquema de reconocimiento mutuo de dispositivos de identificación electrónica social

entre nuestros países. También se propone promover el uso de documentos electrónicos de identificación en los países de la región, incluyendo pasaportes electrónicos y documentos nacionales de identidad, respetando las características y especificidades propias de cada país.

En el mismo sentido, el Marco se propone el objetivo de delinear recomendaciones técnicas a las administraciones públicas para los procesos de autenticación electrónica, especialmente para facilitar los procesos de autenticación remota de usuarios sobre redes abiertas.

En cuanto a los fines que inspiran el Marco Iberoamericano de Identificación Electrónica Social, se inspiran en la Carta Iberoamericana de Gobierno Electrónico, de la cual forma parte. En consecuencia, el Marco tiene como fin acercar las administraciones públicas al ciudadano, reconocer el derecho de éste a vincularse electrónicamente con su administración, facilitar el acceso y participación en la gestión pública.

En relación con la cuestión de la identificación, el Marco plantea como fines establecer un marco de reconocimiento transfronterizo de dispositivos de identificación y autenticación electrónica; promover el uso y reconocimiento mutuo de documentos de identidad electrónicos; garantizar la protección del derecho a la identidad de las personas y facilitar el intercambio de datos entre los países de la región.

Por otra parte, el Marco contempla fines vinculados con la superación de la brecha digital y el acceso igualitario a la sociedad del conocimiento. En ese sentido, se propone como fin el de contribuir a que los pueblos de nuestros países accedan en plenitud a la sociedad de la información y del conocimiento mediante la implementación de programas de inclusión digital y el de superar la brecha digital interna y externa.

Concepto de identificación electrónica

Sin perjuicio de las denominaciones adoptadas en las legislaciones nacionales, el Marco adopta una definición común para el concepto de “Identificación Electrónica Social”. Entiende por tal “al procedimiento que mediante elementos externos, permite asignar una identidad con determinados atributos a una persona concreta, esto es, a la comprobación de los datos que acreditan que un individuo es efectivamente la persona que dice ser, sujeto de derecho, con determinados atributos.”

En igual sentido, define el concepto de “Autenticación Electrónica”, entendiendo por tal “al proceso de verificación de la autenticidad de las identificaciones realizadas o solicitadas por una persona física o entidad, sobre los datos tales como un mensaje u otros medios de transmisión electrónica. El proceso de autenticación es la segunda de dos etapas que comprenden: 1) La presentación de un medio que acredita la identificación ante el sistema y, 2) La presentación o generación de información que corrobora la relación entre el medio presentado y la persona o entidad identificada.” La introducción del concepto de “autenticación electrónica” es un elemento innovador. Hasta el momento, los conceptos contemplados en normativas nacionales eran los de “identificación” y los de “firma electrónica” o “firma digital”. El concepto de “autenticación electrónica” es común en el glosario tecnológico pero no había sido aún

introducido en normas de gobierno o comercio electrónico. Esta es la primera iniciativa en tal sentido, y creemos que constituye un gran aporte del Marco Iberoamericano de Identificación Electrónica Social.

El Marco define una serie de fundamentos que lo inspiran, vinculados con el rol del Estado.

Reconoce como fundamentos en forma expresa que:

1. La identificación de las personas es una obligación indelegable de los Estados, así como la protección de su inviolabilidad.
2. El reconocimiento del derecho a la identidad que gozan todas las personas, así como a la protección de su integridad y la garantía de su pleno ejercicio.
3. El acceso igualitario a la sociedad de la información como bien público relevante, que debe ser impulsado por los gobiernos de la región.
4. El reconocimiento de los principios definidos en la Carta Iberoamericana de Gobierno Electrónico.

Finalmente, el Capítulo I del Marco Iberoamericano repasa los **principios** en los cuales se inscribe, aquellos reconocidos en la Carta Iberoamericana de Gobierno Electrónico, de la cual forma parte. Estos principios son:

1. **Principio de igualdad o no discriminación:** en ningún caso el uso de medios electrónicos puede implicar la existencia de restricciones o discriminaciones para los habitantes que se relacionen con las administraciones públicas.
2. **Principio de legalidad:** mantener las garantías previstas en los modos tradicionales de relación de las personas con el Gobierno y la Administración cuando se realice por medios electrónicos.
3. **Principio de conservación:** garantiza que las comunicaciones y documentos electrónicos se conserven accesibles para su posterior consulta, en las similares condiciones que por los medios tradicionales.
4. **Principio de transparencia y accesibilidad:** garantiza que la información de las administraciones públicas y el conocimiento de los servicios por medios electrónicos se haga en un lenguaje comprensible según el perfil del destinatario.
5. **Principio de proporcionalidad:** de modo que los requerimientos de seguridad sean adecuados a la naturaleza de la relación que se establezca con la Administración
7. **Principio de responsabilidad:** de forma que la Administración y el Gobierno respondan por sus actos realizados por medios electrónicos de la misma manera que de los realizados por medios tradicionales.
8. **Principio de adecuación tecnológica:** las administraciones elegirán las tecnologías más adecuadas para satisfacer sus necesidades.

Aspectos técnicos de la identificación electrónica social

El Marco Iberoamericano promueve en su Capítulo II el reconocimiento del derecho a relacionarse electrónicamente con la administración, en consonancia con la Carta Iberoamericana de Gobierno Electrónico.

En efecto, el artículo 6 expresa “*Los Estados iberoamericanos están en la obligación de atender el ejercicio efectivo del derecho de las personas a relacionarse electrónicamente con la Administración, lo que requiere que garanticen la identificación electrónica social de sus habitantes.*”

A continuación, el marco de identificación electrónica social contiene un glosario de términos que apunta a establecer un marco común de entendimiento sobre las definiciones de aspectos técnicos involucrados en el proceso de identificación electrónica.

El artículo 7 define un glosario común que permitirá elaborar a futuro acuerdos de entendimiento mutuo, al unificar la terminología utilizada y sentar criterios comunes en cuanto a estas importantes cuestiones.

El Marco define los siguientes términos en el Glosario:

1. Factores de autenticación: Son aquellos elementos que integran el proceso de identificación.

Los factores de autenticación que se utilizan actualmente son tres, que se basan en:

- *Algo que sé*: la persona se autentica mediante algo que sabe: una clave, un número que la identifica – PIN, una frase o una respuesta a una pregunta de seguridad.
- *Algo que tengo*: la persona se autentica utilizando algo que posee: un token, una tarjeta inteligente, un certificado digital.
- *Algo que soy*: el individuo se autentica con base en una característica que tiene su persona, esto es, un dato biométrico.

Los factores sustentados en conocimiento y en posesión requieren que la persona que se va a autenticar ante un sistema recuerde o lleve consigo el dispositivo. En cambio, cuando se aplican tecnologías biométricas, el dato lo lleva consigo, y resulta casi imposible que se lo falsee, esto es, que sea utilizado por otra persona para suplantar su identidad. Se dice que en los dos primeros factores, el vínculo entre el dato y su verificación es débil, lo cual facilita la usurpación de identidad, ya que el sistema no puede distinguir entre el legítimo poseedor del dispositivo y alguien que lo haya sustraído, lo mismo se aplica a la clave.

2. Tecnologías Biométricas: Se entiende por reconocimiento biométrico a los métodos automatizados que aseguran el reconocimiento de individuos con base en rasgos físicos o conductuales distinguibles. Las tecnologías que se usan en biometría incluyen el reconocimiento de huellas dactilares, de rostros, de patrones de las venas, del iris, de voz y del tecleo, entre otros.

3. Sistema Biométrico: Es un sistema informático de reconocimiento con base en uno o varios patrones, que opera requiriendo datos biométricos a un individuo, extractando un patrón de estos datos adquiridos y comparando el ejemplo contra una plantilla previamente registrada. Dependiendo de la aplicación, esta plantilla puede estar almacenada en una base de datos centralizada o en un dispositivo individual, como un token o una tarjeta inteligente.

4. Infraestructuras de Clave Pública: (también conocidas como Infraestructuras de Firma Digital o PKI por sus siglas en inglés - Public Key Infrastructure. Puede definirse como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de clave pública basados en criptografía asimétrica,

que facilitan la creación de una asociación verificable entre una clave pública y la identidad del tenedor de su correspondiente clave privada.

5. Firma Digital -también llamada firma electrónica segura, firma electrónica avanzada o firma electrónica reconocida-. El concepto de firma digital tiene al menos dos acepciones: una tecnológica, vinculada con las tecnologías de clave pública, y otra jurídica, que responde a la definición que las leyes nacionales han incluido como equivalente a la firma manuscrita.

Desde el punto de vista tecnológico, una firma digital es el mecanismo de autenticación que, sustentado en criptografía asimétrica, esto es, que usa dos claves, una pública y una privada, permite identificar al firmante y garantizar la integridad del contenido del documento electrónico firmado.

Desde el punto de vista jurídico, las leyes incluyen un requisito administrativo. Ello significa que para ser considerada legalmente firma digital, ese mecanismo debe haber sido aplicado mediante el uso de un certificado digital emitido por una entidad de certificación acreditada por el órgano rector del Estado en dicha materia.

6. Firma Electrónica: el concepto se aplica a cualquier sonido, símbolo o proceso, adjunto o lógicamente asociado a un documento electrónico que exprese el consentimiento de una persona emitido en formato digital, y ejecutado o adoptado por dicha persona con el propósito de firmar el documento electrónico. En general, las leyes denominan “firma electrónica” a cualquier mecanismo de autenticación que no cumpla alguno de los requisitos exigidos para una firma digital. “Firma electrónica” es el término genérico y neutral para referirse al universo de tecnologías que una persona puede utilizar para expresar su consentimiento con el contenido de un documento.

Bases para acuerdos de reconocimiento mutuo

Finalmente, el Marco en su Cap III establece una serie de consideraciones relativas al establecimiento de criterios comunes que permitan en el futuro alcanzar un efectivo medio común de Identificación Electrónica Social Iberoamericana.

En tal sentido, promueve el establecimiento de acuerdos de reconocimiento mutuo vinculados a los procesos de identificación electrónica de personas en entornos físicos o virtuales.

El documento propugna la discusión de los aspectos legales y técnicos necesarios para la celebración de acuerdos de intercambio de datos, la interoperabilidad de sistemas y el establecimiento de estándares tecnológicos comunes entre los países iberoamericanos, en base a sus contenidos.

Asimismo, promueve el intercambio de experiencias nacionales vinculadas con la implementación del documento de identidad electrónico y del pasaporte electrónico, y de todo otro mecanismo de autentificación digital.

Finalmente, y constituyendo un gran avance para la consolidación del comercio electrónico y del gobierno digital, el Marco define que sus disposiciones sean los contenidos de entendimiento para que los Estados iberoamericanos celebren acuerdos de reconocimiento mutuo de certificados digitales, sentando las bases para futuros acuerdos que permitan la articulación de las infraestructuras de firma digital en la región.

Conclusiones

Hemos visto que nuestros países se encuentran desplegando políticas públicas destinadas a lograr la plena inclusión digital de su gente. El Marco Iberoamericano de Identificación Electrónica Social es un paso más para lograr esta meta. Representa un punto de partida para nuestros países, para avanzar en forma coordinada y articulada en una materia de alta importancia para la efectiva implementación de políticas sociales: la identificación de las personas.

Pero también el Marco representa un gran avance para la puesta en marcha de las iniciativas de gobierno electrónico que nuestros países están llevando adelante, y para la implementación efectiva de la Carta Iberoamericana de Gobierno Electrónico.

En este sentido, este Marco nos permitirá avanzar en el reconocimiento de firmas electrónicas y firmas digitales, ayudando al desarrollo del gobierno abierto y del comercio electrónico.

Si avanzamos en la superación de la brecha digital y con el gobierno electrónico, en breve nuestros países estarán en condiciones de reconocer el derecho de sus habitantes a relacionarse electrónicamente con sus administraciones.

Sin embargo, debemos reiterar conceptos que hemos planteado en otras oportunidades en este mismo Congreso del Clad, que tienen que ver con los resguardos que se deben dar para la ejecución exitosa de estos proyectos.

Hemos mencionado que las dificultades para su implementación no están vinculadas con la tecnología, que ya existe con un suficiente grado de madurez. Tampoco con la existencia de estándares internacionales, que han sido desarrollados y aceptados. Como todo proyecto que implica implantar Tecnologías de la Información y las Comunicaciones en la gestión administrativa del Estado, los proyectos orientados a construir una base de datos biométricos o a reemplazar los documentos de identidad actuales por otros electrónicos, enfrentan los mismos factores de riesgo que cualquier otro proyecto tecnológico transversal. (THILL; 2010)

El desafío que nuestros países enfrentan a la hora de implementar proyectos tecnológicos en el sector público que permitan desarrollar el Gobierno Electrónico, no se relaciona tanto con la escasez de recursos, ni con una infraestructura insuficiente ni tampoco con la carencia de profesionales, sino más bien con la falta de coordinación entre las organizaciones públicas. En efecto, los esfuerzos que realizan los gobiernos muchas veces no obtienen los resultados esperados no por falta de recursos sino porque los distintos organismos realizan proyectos en forma descoordinada, lo cual genera comportamientos estancos.

Es claro que el logro de resultados en la implementación de proyectos tecnológicos en la gestión pública requiere una planificación adecuada y un monitoreo y evaluación que陪伴e su desarrollo. Pero esto no alcanza para garantizar el éxito del proyecto, sobre todo en aquellos que involucran a varios organismos, o sea, que son transversales en la Administración. Un elemento crucial es el rol de los decisores políticos, especialmente de aquellos que intervienen en los procesos de definición de las políticas públicas vinculadas al uso de las tecnologías en la Administración o a la modernización del Estado.

Destacamos el rol central del “liderazgo” en el diseño e implementación de estrategias electrónicas. Sin un decidido liderazgo no se podrán superar las resistencias al cambio que naturalmente implica la modificación de las formas de trabajo derivadas de la incorporación de TIC en la gestión pública. (THILL; 2010)

En síntesis, el consenso alcanzado sobre los mecanismos de autenticación electrónica e identificación mediante herramientas tecnológicas entre nuestros países, plasmado en el Marco Iberoamericano de Identificación Electrónica Social, constituye un avance para seguir avanzando en acciones de gobierno electrónico. También es un importante logro para comenzar a delinejar acuerdos de reconocimiento mutuo de certificados electrónicos de firma digital. Pero el logro mayor radica en que es la primera iniciativa conjunta orientada a lograr estándares comunes para documento de identidad, procesos identificatorios y tecnologías biométricas.

Esta iniciativa nos va a permitir comenzar a intercambiar experiencias y alcanzar pautas comunes para mejorar la calidad de las prestaciones públicas así como lograr la plena identificación de nuestros habitantes, requisito esencial para el despliegue de políticas públicas de inclusión social.

Bibliografía

CEPAL (2010), “La hora de la igualdad: Brechas por cerrar, caminos por abrir”, Naciones Unidas, Mayo 2010. Disponible en internet en http://www.eclac.org/publicaciones/xml/0/39710/100604_2010-114-SES.33-3_La_hora_de_la_igualdad_doc_completo.pdf

CLAD (2007), “Carta Iberoamericana de Gobierno Electrónico”, Disponible en internet en <http://www.clad.org/documentos/declaraciones/cartagobelec.pdf/view>

CLAD (2011), “Consenso de Asunción”, Disponible en internet en <http://www.clad.org/documentos/declaraciones/consenso-de-asucion/view>

CLAD (2011), “Marco Iberoamericano de Identificación Electrónica Social”, aprobado en la XIII Conferencia Iberoamericana por los Ministros de Administración Pública y Reforma del Estado, Asunción, julio 2011. Disponible en internet en http://www.agendadigital.ar/docs/identificacion_electronica_social_iberoamericana.pdf

KIRCHNER, Néstor (2003), Discurso en la asunción presidencial ante la Asamblea Legislativa, 25 de mayo 2003. Disponible en Internet en http://www.anibalfernandez.com.ar/Documentos/Asuncion_de_20Nestor_Kirchner.pdf

ORGANIZACIÓN DE ESTADOS IBEROAMERICANOS (2009), “Declaración de Lisboa”, XIX Conferencia Iberoamericana de Educación, Lisboa, Diciembre 2009. Disponible en internet en http://www.oei.es/Declaracion_Lisboa.pdf

ORGANIZACIÓN DE ESTADOS IBEROAMERICANOS (2010), “Declaración de Mar del Plata”, XX Conferencia Iberoamericana Argentina 2010, Diciembre 2010. Disponible en Internet en <http://www.oei.es/declaraciondemardelplata.php>

THILL, Eduardo (2010): “Identidad, Identificación Electrónica y Ciudadanía Digital”. Ponencia presentada en el XV Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Santo Domingo, Noviembre 2010.

Herramientas biométricas para la inclusión social y digital

Pedro Janices



Pedro Janices

Director Nacional de la Oficina Nacional de Tecnologías de Información (ONTI).



En 1995 comenzó su carrera en la Administración Pública Nacional desempeñándose en diversas funciones en el Gobierno Nacional en las cuales, por diferentes proyectos, ha ido acumulando experiencia y conocimiento en temáticas relacionadas a la gestión pública, a la tecnología y a la identidad. En todos estos años de gestión, ha podido recoger las experiencias y necesidades del Gobierno Nacional y de la demanda de la sociedad.

En el presente, sus funciones se orientan a la coordinación de proyectos sobre implementación de gobierno electrónico (e-government), la relación y fortalecimiento de las herramientas que propendan a la creación del ciudadano digital (e-citizen), el desarrollo y aprobación de planes de implementación de firma digital (pki), el desarrollo de las políticas que permitan la instrumentación de acciones tendientes a la protección de la información de las infraestructuras críticas (CIIP), y a la elaboración de estándares de hardware, software y datos de la Administración Pública Nacional, entre otras tareas.

Información de contacto: PJanices@jefatura.gob.ar

Resumen

Las políticas de inclusión digital deben sustentarse en brindar los conocimientos y capacidades necesarias para una mejor comunicación gobierno-ciudadano en la democratización de la información, por medio de las TIC's teniendo como objetivo la disminución de la desigualdad, la apertura de nuevas posibilidades de crecimiento social, capacitando y concientizando a los ciudadanos sobre el uso de las redes y de su contenido para obtener conocimiento y desenvolver competencias. Para esto es necesario conocer e identificar únicamente al usuario.

Para hablar de inclusión digital hay que mencionar las políticas de inclusión social y de seguridad. Las primeras deben sustentarse en favorecer a los excluidos, brindándole los mecanismos y herramientas necesarias para el mejoramiento de su calidad de vida. Los planes de asistencia deben ser garantizados a todos los ciudadanos, pero poniendo atención en aquellos que sufren esas carencias; para lo que el Gobierno debe conocer e identificar eficazmente a cada ciudadano que recibe dicho beneficio, asegurándose que el mismo llegue al necesitado.

Las políticas de seguridad ciudadana deben fundarse en la prevención y disuasión de posibles actos delictivos; y parte sustancial de esta política es la correcta y precisa identificación de las personas siendo ésta una función esencial del Estado para la correcta verificación de la identidad.

El denominador común para estos tres escenarios es el ciudadano, al que el Estado debe conocer, tener la capacidad de identificar y brindarle precisa identidad JURIDICA y preservar la privacidad de su información.

Palabras clave: inclusión digital, ciber-identidad, biometría, seguridad.

Herramientas biométricas para la inclusión social y digital

Introducción

El presente trabajo pretende mostrar la experiencia adquirida en los últimos 7 años en materia biométrica, a través de diversos proyectos encarados por el Gobierno Nacional y exponer los nuevos planes de acción para los próximos 5 años, entendiendo el uso de la herramienta biométrica como un proceso integral que exige a los distintos actores de la sociedad compromisos y responsabilidades en la aplicación del modelo.

Para ello, se describirán diferentes indicadores sociales del trabajo que está llevando a cabo el Gobierno Argentino, y su relación con el programa “2011 -2016. Biometría: herramienta clave para la inclusión social y digital”.

Estado de la cuestión

A partir del año 2005, desde el Gobierno Nacional se impulsó la adopción de estándares internacionales en materia de biometría que permitieran compartir la información entre los organismos de competencia en la materia, así como entre los gobiernos provinciales y la Nación. Asimismo, se propició la implementación de equipamiento con las certificaciones necesarias de calidad biométrica que permitan asegurar la materia prima con la que se habría de garantizar y custodiar la identidad de los ciudadanos.

La adopción de los estándares del tipo ANSI-NIST en materia de comunicaciones de datos biométricos para la identificación fue un paso estudiado y asimilado viendo los beneficios que este tipo de comunicación brindaba en la interoperabilidad de los sistemas. La Ley 17.671 de “Identificación, Registro y Clasificación del Potencial Humano Nacional” en su capítulo II, Sección I, Art. 7 contempla el registro de patrones biométricos pero no su forma de comunicarse ni resguardarse, dejando esto librado solo a su clasificación de la siguiente forma “se llevarán por lo menos ficheros patronímicos, numéricos y dactiloscópicos según el sistema argentino Vucetich u otro que en el futuro aconseje la evolución de la técnica”. Esto permite la constante y necesaria evolución de los sistemas de resguardo, clasificación, comparación y registro de los datos biométricos que permitan optimizar los procesos y procedimientos en el otorgamiento de identidad y la emisión de Documentos Nacionales de Identidad.¹

Además, la adopción de estos estándares posibilita la interconsulta con otros Estados (provinciales y extranjeros) para apoyar a las políticas de seguridad públicas, nacionales e internacionales.

Las mismas tienen como base la correcta identificación de personas; y vale recalcar que éstas son imprescindibles para la constitución de una Nación dado que posibilitan la defensa de la identidad de las personas, y son una herramienta esencial contra el robo de identidad ayudando a la prevención y lucha contra el delito, la optimización de los sistemas de registro de tránsito

¹ <http://www.infoleg.gov.ar/infolegInternet/anexos/25000-29999/28130/texact.htm>

fronterizo, la autenticación en transacciones comerciales, el ejercicio de derechos sociales y electorales, entre otros.

Al ser entonces, las políticas de identificación y de seguridad un eje central de la administración de gobierno donde se pudieron aplicar herramientas biométricas a los proyectos que requieran verificación de identidad en los organismos dependientes de la Administración Pública Nacional.

Entonces, teniendo como marco conceptual las políticas de inclusión social y digital en la relación Ciudadano – Gobierno (C2G), se establecieron los siguientes objetivos básicos:

- Garantizar la plena y unívoca identidad.
- Garantizar la privacidad de los datos personales.
- Optimizar los mecanismos de registro e identificación de los ciudadanos.
- Optimizar los procesos de seguridad pública en el marco científico del reconocimiento en actos delictivos.
- Fortalecer la capacidad del Estado usando las TIC's.
- Continuar en forma de mejoramiento continuo con las políticas de inserción de herramientas biométricas.

De esta manera, se emprendieron proyectos tales como: la mejora en los circuitos de emisión del Documento Nacional de Identidad y del Pasaporte Argentino, la actualización tecnológica del sistema automatizado de identificación de huellas dactilares (AFIS) en poder de la Policía Federal Argentina, la creación del sistema multi-biométrico de registro de acceso al Servicio Penitenciario Federal, la actualización del sistema del Registro Nacional de Reincidencias y la propuesta de creación del “Programa Nacional de Estandarización de datos biométricos y biométricos forenses”.

En los últimos 8 años, se ha producido un extraordinario desarrollo de las tecnologías biométricas en general y de sus diferentes ramas en lo particular: verificación e identificación a través de huellas dactilares, facial, iris, vascular, voz y ADN, entre otras, así como nuevas combinaciones: multi-biometría, fusión, etc. permitiendo mejorar aún más, la precisión de los resultados.

En el mismo camino, se ha colaborado con el NIST (National Institute of Standards and Technology – USA) participando activamente en la elaboración de estándares biométricos abiertos (ANSI NIST-ILT 1-2011) y propiciando con éxito la incorporación de registros del sistema estomatognático (comparación dental, impresiones labiales, rugas palatinas y huellas de mordeduras) liderando el grupo de registros dentales, con organismos tales como el Federal Bureau of Investigation (FBI), INTERPOL, Bundeskriminalamt, Miami Dade, entre otros.

Se llevaron y llevan a cabo también, ya en su sexta edición, el “**Congreso Internacional de Biometría de la República Argentina**” denominado **CIBRA**, en el cual se presentan proyectos concretos a nivel nacional e internacional. En el mismo, se intercambian saberes y experiencias con las provincias y con otras naciones del mundo. La quinta edición del Congreso, en el año 2010, estuvo acompañada de la publicación del libro “Biometrías” (2010), que compila alguna de las tantas contribuciones presentadas.

2011 -2016: La Biometría como inclusión social

Pero haciendo hincapié en los objetivos de la actual política de Estado, es que no se debe olvidar que la seguridad es una de las dimensiones del desarrollo humano que incluye el ambiente, la educación y las condiciones socioeconómicas de una población siendo éstos los componentes básicos para la construcción de la ciudadanía y el fortalecimiento del Estado y sus instituciones.

La exclusión social es una problemática que genera constantes conflictos en los países de nuestra región: sustracción de menores, deserción escolar, mercado laboral ilegal, desaparición de personas con privación de la vida, trata de personas, robo de identidad, entre otros. Ante esta situación se ha comenzado a pensar en futuros campos de abordaje, analizando sus contextos externos e internos donde se desarrolla la problemática para determinar cómo alcanzar los objetivos que se han propuesto.

Planes como la Agenda Digital Argentina, que tiende a la eliminación de la llamada “brecha digital” proveyendo de comunicaciones y herramientas tecnológicas para que los ciudadanos en edad escolar y grupos familiares se integren al mundo digital. El acceso a los contenidos áulicos, culturales e informativos forma parte del mejoramiento de la calidad de la ciudadanía en su relación con los gobiernos, provinciales y nacionales, dando igualdad de oportunidades y generando más y mejor empleo gracias a las iniciativas de producción nacional de equipos de tecnología que alientan a una mayor inversión. Todo esto, hace al conjunto de un gobierno estable y fuerte que impulsa la inclusión social y digital.

Es por ello que, al analizar el desarrollo sustentable de los proyectos, se nos presenta la certeza de que a la biometría no solo se la debe abordar desde una perspectiva tecnológica, de aplicación y de uso, sino que debe también, ser parte de los avances en materia de inclusión social.

La seguridad perseguida no debe basarse en construir más cárceles, ni en proveer de más armas para su represión, sino en insertar a los sector más desprotegidos a un ecosistema social donde los mismos puedan capacitarse, opinar y ser parte de un modelo de crecimiento, y para esto la inclusión digital es indudablemente el paso siguiente de la inclusión social, permitiéndoles a los ciudadanos desde su infancia ser parte de la sociedad.

Niñez

Teniendo como marco conceptual la “XII Conferencia Iberoamericana de Ministros y Altos responsables de Infancia y Adolescencia” celebrada los días 23 y 24 de Junio de 2011, en la Ciudad Autónoma de Buenos Aires, en la cual se fijó el compromiso de tomar medidas legislativas que faciliten la construcción de sistemas integrales de protección de la infancia y la adolescencia, es que se decidió acompañar este proceso desde el ámbito de nuestra competencia.²

Es sabido que es obligación del Estado proteger y, llegado el caso, restablecer los aspectos fundamentales de la identidad de un niño como ser el nombre, nacionalidad y las relaciones familiares.

² <http://www.xxcumbreiberamericana.mrecic.gov.ar/?q=node/17>

Pero, ¿por qué es importante tener un nombre? Porque es la forma social más común de presentarse ante otros, de manifestar una identidad. Toda persona, todo ser humano nace con rasgos biométricos, tales como las huellas dactilares, pero necesita ser identificado frente a sí mismo y frente a los demás con sus propios datos biográficos (nombres, apellidos, etc.) y frente a los procesos administrativos necesarios con sus documentos y números de identidad. Si no se tiene un nombre y una nacionalidad no se pueden adquirir otros derechos, es decir, el nombre y la nacionalidad son pilares que contribuyen al ejercicio de otros derechos, como por ejemplo el acceso a la salud, a la educación, a la información, el acceso a la recreación, esparcimiento, etc.

La *Convención sobre los Derechos del Niño (CDN)* incorporada a la Constitución Nacional por la reforma del año 1994 (art. 75 inc.22) indica en su Artículo 7 que “*el niño será inscrito inmediatamente después de su nacimiento y tendrá derecho desde que nace a un nombre, a adquirir una nacionalidad y, en la medida de lo posible, a conocer a sus padres y a ser cuidado por ellos*”. Por su parte, el artículo 8 manifiesta que “*los Estados Partes se comprometen a respetar el derecho del niño a preservar su identidad, incluidos la nacionalidad, el nombre y las relaciones familiares (...)*”.³

En nuestro derecho interno se ha consagrado la Ley N° 26.061 de **protección integral de los derechos de las niñas, niños y adolescentes** la cual establece en su Artículo 11 que “*Las niñas, niños y adolescentes tienen derecho a un nombre, a una nacionalidad, a su lengua de origen, al conocimiento de quiénes son sus padres, a la preservación de sus relaciones familiares de conformidad con la ley, a la cultura de su lugar de origen y a preservar su identidad e idiosincrasia, salvo la excepción prevista en los artículos 327 y 328 del Código Civil*”.⁴

Los niños y las niñas presentan una serie de dificultades al no tener un documento de identidad. Un niño sin documento de identificación carece de acceso pleno a la protección que los poderes públicos tienen la obligación de realizar a todas las personas. El mundo se le cierra al niño en cuanto a las posibilidades de acceder al sistema jurídico, legal y al sistema social de protección de un país, si el Estado no los protege y les brinda sus derechos.

Si bien es cierto que esto forma parte de una decisión de gestión de política interior, como ya se ha mencionado, también conforma la política exterior tratando de lograr los compromisos asumidos en la “Cumbre Mundial sobre el Desarrollo del Milenio”, como es el caso del “Estado Mundial de la Infancia”, donde las estadísticas plantean que millones de niños tienen negados sus derechos básicos a la identidad, educación de calidad, salud, protección de abusos, y explotación laboral.

Pero no sólo los niños están dentro de la agenda política sino también la esfera de salud.

Salud

En la “XII Conferencia Iberoamericana de Ministros de Salud”, celebrada entre los días 3 y 4 de diciembre de 2010 en la ciudad de Mar del Plata, se resolvió impulsar una agenda integrada de

³ La CDN y el derecho a la identidad: <http://www.unicef.es/infancia/derechos-del-nino/convencion-derechos-nino>

⁴ Ley 26061: <http://www.infoleg.gov.ar/infolegInternet/anexos/110000-114999/110778/norma.htm>

salud y educación para la inclusión social y se acordó la realización de acciones conjuntas para fomentar el impulso de la formación y la capacitación de recursos humanos.⁵

El sistema de información sanitaria es una de las bases esenciales de las actividades de salud pública, pocos países en desarrollo cuentan con sistemas eficaces y aunque el nivel de conocimientos aumenta por las nuevas herramientas de comunicación e información, se nota una brecha considerable entre lo que los planificadores de políticas sanitarias saben y lo que necesitan saber para mejorar los proyectos de salud. Esta demás decir que entre los temas necesarios a considerar esta la identificación del paciente, su historia clínica y la confidencialidad de su identidad y datos asociados.

Las dificultades no sólo se deben a limitaciones financieras. En esta esfera, la medición es una labor conceptual y técnicamente compleja que requiere datos sólidos sobre los resultados sanitarios (por ejemplo, las enfermedades, los tratamientos, los fármacos y la mortalidad), las aportaciones del sistema de salud (tales como recursos humanos, infraestructura y financiación) y los determinantes de la salud. Una porción de la información sanitaria no incumbe únicamente a una determinada entidad estatal; la producen y utilizan diversas instituciones, tales como los ministerios y secretarías de salud, las oficinas nacionales de estadística, los ministerios de trabajo, bienestar social, planificación y finanzas, el sector privado, entre otros.

La niñez y la salud son algunos de los primeros indicadores sociales, pero también se encuentra el sector de viviendas y desarrollo urbano, el de turismo y educación, integrando en la dinámica de trabajo no solo a las dependencias de la Administración Pública Nacional sino también a las Universidades y organismos del tercer sector como las ONGs, emprendiendo la tarea de armar proyectos y programas que puedan intentar resolver las demandas de la sociedad, siendo que muchos de estos pueden encararse con recursos humanos obtenidos de la inclusión social, su protección y capacitación.

Inclusión social y digital

Como se señaló con anterioridad, hay otros derechos como ser el acceso a la información, a la educación y a la libre expresión, que se encuentran estrechamente relacionados en la actualidad al acceso y uso de las TIC's.

El acceso a los diferentes factores que lo permiten, se puede ver reflejado en diversos proyectos en ejecución del actual Gobierno Argentino que propenden a la inclusión social, y fundan los eslabones de la Agenda Digital en busca de terminar con la Brecha Digital.

Concatenando cada eslabón de esta cadena de proyectos, se fue logrando desde la inclusión en la escuela a menores que carecían de recursos a la asistencia social con los proyectos del plan denominado “Asignación Universal por Embarazo” y “Asignación Universal por Hijo” con más de 4,5 millones de familias asistidas, al que se le suma el proyecto del “Nuevo DNI Argentino” con más de 8,2 millones de nuevos documentos de identidad otorgados a la fecha, así como el

⁵ <http://www.xcumbreiberoadamericana.mrecic.gov.ar/>

acceso público y gratuito a Internet a través del proyecto “**Argentina Conectada**”, continuando con la dotación de más de 1 millón de equipos de computadoras personales entregados a las nuevas generaciones en edad escolar para su educación y acercamiento a las TIC’s a través del proyecto “**Conectar Igualdad**” y el acceso a la información libre, igualitaria y gratuita de la “**Televisión Digital Abierta**” que cuenta en la actualidad más de 16 señales de información, capacitación, educación y contenidos culturales.

Cabe mencionar que acompañan estos proyectos programas como el de “**Monotributista Social**” mediante el cual personas con vulnerabilidad social y económica pueden ser contratados directamente por organismos de la Administración Pública Nacional siendo estos seleccionados de una base de datos de público acceso, brindando la transparencia a dicha acción y permitiendo su inclusión de forma ágil y certera al mercado laboral.

Como se ha señalado, estos eslabones le dan solidez a la cadena de hechos que propendan a la inclusión de los sectores más necesitados y brindan, a su vez, las herramientas tecnológicas no solo de información, sino también de formación, opinión y participación.

Esta inclusión, viene aparejada de la necesidad de ofrecer una interface de acceso a la información más accesible, usable, ágil y certera, propendiendo a un Gobierno Electrónico que permita que el ciudadano pueda acceder a la información que el Gobierno posee de él.

A estos fines, es que el Gobierno debe asegurarse el “quien” está requiriendo y recibiendo “que” información privada de un ciudadano, en otras palabras, “quien” se encuentra del otro lado del ordenador.

Aquí es donde el factor de identificación es importante y a donde se apuntala la estrategia de que dicha identificación digital sea forjada a través del “triple factor”.

“*Algo que sé, algo que tengo y algo que soy*” es la frase acuñada por aquellos que esgrimen la utilización de una clave, un dispositivo tipo token/tarjeta y un registro biométrico verificable como elementos que refuerzan a la integridad de la verificación de la identidad por medios digitales. Es más, se puede encontrar que dependiendo de la información a la que se desea acceder se habla en el mundo TI y se encuentra en discusión de su utilidad, seguridad y privacidad un cuarto factor, el “donde estoy”.

Es indiscutible, que más allá de las políticas de inclusión digital y del camino iniciado hacia el “**Open Data**” y el “**Open Government**”, el eje de toda administración, su sustento y su servicio está centrado en el ciudadano, su cuidado, su protección, su educación y su opinión. Por ello, incluirlo socialmente, incluirlo digitalmente y reconocerlo únicamente protegiendo su ciberidentidad, no una alternativa sino una obligación.

Identificación, biometrías y la pirámide biométrica

Es de suma importancia, entender que los métodos de validación de usuarios conocidos y tratados en diferentes documentos, se basaron durante las distintas épocas de evolución humana, en la seguridad digital, en la protección por clave (algo que sé) y en un dispositivo (algo

que tengo) que “autorice” a quien lo posea a acceder a, por ejemplo, un sistema.

Al señalar el agregado de un tercer factor, el factor biométrico, aumenta la certidumbre pero “¿de quién?”.

Se comenzará, a modo de ejemplo y en su versión resumida, a andar el camino del ciudadano Argentino acorde a la legislación vigente.

El individuo nace con patrones biométricos (ej. huellas plantares y dactilares), se registra en el nosocomio la huella plantar (huella del pie del recién nacido) y sus padres, tutores o encargados lo informan al Registro Nacional de las Personas, a través de las correspondientes oficinas, declarando el nombre que ellos le asignan, para su registración y donde se le asigna un número de identidad brindándole, a cambio, una identidad jurídica materializada en un Documento Nacional de Identidad que permite cabalmente que pueda reclamar, en caso de necesitarlo, asistencia social, sanitaria y otras, en el marco jurídico que le compete.

A la edad escolar se renueva por primera vez este documento y ya, con fotografía facial, se entrega un nuevo Documento con el primer identificador biométrico (fotografía facial) asociado al biográfico (Apellidos, Nombres, etc.).

A partir de los 16 años se realiza la tercera generación del Documento, añadiendo en su trámite de renovación, el registro de las huellas dactilares del ciudadano que permite realizar una comprobación, a través de sistemas automatizados de identificación dactilar, que sus huellas sean unívocamente asociadas a su número de documento, imagen facial y a sus nombres y apellidos.

Nombres + Num_identidad + Biometrias = Identidad

Desde este último paso, en adelante, el ciudadano se asocia a una identidad única en el universo de registros de individuos que el Gobierno posee para su identificación.

Entonces, volviendo al interrogante planteado anteriormente, podemos decir que tenemos que VERIFICAR la identidad del ciudadano con la comparación de alguno de los factores biométricos que el Estado posea de él, contra los que se presenten al momento de requerir la información, logrando de esta forma la certidumbre deseada.

Se deberá, a esta altura, ahondar en algunas definiciones meramente informativas y sustancialmente necesarias para la buena interpretación de los enunciados, y en base a las enseñanzas de Don Arturo Jauretche, se tratará que el lenguaje utilizado sea libre de “zonceras”.

Al hablar de **biometría**, se habla de aquellos rasgos identificatorios únicos y medibles que una persona posee. Huellas dactilares, conformación de los iris, configuración del rostro, rasgos particulares con los son intrínsecos al individuo. Los demás como nombres y apellidos le son impuestos por sus padres, su número de identidad le es asignado por el estado, pero los rasgos biométricos son del individuo desde su desarrollo en el vientre uterino.

Al hablar de **registrar** a un individuo, conocido también como “enrolar”, es cuando al momento de su identificación no se encontraron en los registros uno que sea idéntico y entonces se agregan esos registros biométricos a los ya existentes.

Al hablar de **identidad**, en su marco biométrico, se está refiriendo a una asociación bi-unívoca o de correspondencia univoca (que el primero refiere a otro y el otro al primero sin ambigüedades e inequívocamente) entre un individuo y sus registros biométricos, los que previo al momento de otorgarse (registrarse) se ha verificado que no haya otro con los idénticos patrones biométricos. En otras palabras y a modo de ejemplo, “esta huella es solo de tal persona y solo tal persona tiene esta huella”.

Si se habla de **verificar** la identidad biométrica, se dice que ese individuo se encuentra en los registros y se comparan las particularidades biométricas registradas contra las que el individuo presenta, si coinciden se brinda una verificación positiva.

Dicho esto, queda mencionar que no hay un solo método biométrico que no pueda ser vulnerado por artifugios o por acciones de la naturaleza humana (ejemplo enfermedades o accidentes) o al menos engañado si las condiciones de usabilidad y seguridad no son tenidas en cuenta. No se pretende hacer de este texto un manual de usurpación de identidad biométrica pero si tratará de mostrar que la biometría no es una “bala de plata” que soluciona y actúa en desmedro de las demás medidas a tener en cuenta, sino solo como lo que es, **una herramienta que facilita, agiliza y asegura una identidad**.

Por lo expuesto, es que participamos activamente en la elaboración, debates, propuestas y votaciones en el **NIST** (National Institute of Standards and Technology - USA), para profundizar los conocimientos en materia de estándares biométricos y poder exponer nuestra posición al respecto.

No debemos dejar de pensar en cuanto mas ágil hubiera sido el trabajo de las “Madres y Abuelas de Plaza de Mayo” en encontrar a hijos y nietos de los desaparecidos durante la dictadura en nuestro país, si se hubieran tenido más registros y métodos biométricos en las bases de datos con sistemas automatizados de verificación de identidad que en forma inviolable recauden esta información.

El caso es que, para lograr asegurar una identidad biométrica ya no basta un método (ejemplo solo la huella dactilar) sino se debe pensar en lo que se ha llamado “la pirámide biométrica”.

La Pirámide Biométrica

Desde sus orígenes, remontados por algunos investigadores en antiguas dinastías chinas o al menos “antes de Cristo”, el ser humano ha utilizado la huella dactilar como elemento adicional para “firmar” sus obras y posesiones, permitiendo verificar esa huella contra las huellas del que reclamaba su autoría o pertenencia.⁶

La huella dactilar es sin duda el método biométrico más efectivo en la historia de la humanidad,

⁶ <http://www.applied-biometrics.com/spanish/tecnologia/huella-dactilar/posicion-del-desarrollo.html>

dado que hasta el día de hoy, y considerando las centenas de millones de registros dactilares automatizados alrededor del mundo, no se ha encontrado una huella dactilar idéntica a la de otra persona ni siquiera en una misma persona.⁷

Si se pusieran los métodos biométricos estáticos (porque también los hay dinámicos o también llamados de comportamiento) en representación de fichas de ajedrez podríamos decir que la “Reina” estaría siendo la huella dactilar. Como otros métodos, sus cualidades de **perennidad** (desde su formación se mantienen invariables en número, posición, forma y dirección), **inmutabilidad** (no mutan, desde su formación en la 6ta semana de vida intrauterina no son alteradas y se regeneran a su diseño original) **invariables** (no pueden variarse e incluso dependiendo del corte producido por una herida se regeneran o el diseño se invalida por un dibujo cicatrizal, pero no cambian de forma) y **diversiformes** (son diferentes una de otras) le dan la supremacía ante otros métodos de identificación, tanto más en base a que en hechos delictuales son los elementos biométricos (rastros) que más se encuentran. Esto sin dejar de lado que no hay religión ni “usos y costumbres” que obliguen a un individuo a usar guantes o cubrirlas, por lo que la huella dactilar es el elemento de identificación más expuesto en las tareas cotidianas.

Es una cuestión de usabilidad, practicidad y estadística el poder acercarnos al grado más alto de certidumbre. Para ello es necesario sumar otros métodos biométricos siendo esto al día de hoy imprescindible.

Continuando con el tablero de ajedrez, si bien el “Rey” podría ser el ADN (ácido desoxirribonucleico) por su exactitud y en temas de seguridad por los elementos encontrados como “rastros”, también tiene su resistencia en aspectos de privacidad y manejo de la muestra así como sus usos que, en algunos países, se encuentran enmarcados solo para casos de delincuencia sexual o para reclamos de paternidad o parentesco, sumado a esto el costo y tiempo proveniente del análisis.

La Torre, debería decir, sería el registro facial. Si bien se ha dicho mucho de los registros biométricos y sobre cuáles serían de carácter privado y cuales públicos, se introduce aquí en un problema, pretendiendo que el rostro es de acceso “público” solo porque una gran porción de la humanidad lo lleva visible todo el tiempo. Y, ¿qué ha de pasar con aquellos que usan por razones religiosas o culturales algún elemento que obstruye o dificulta su registro? ¿Qué sucede cuando la luminosidad, ángulo, o fondo no satisface la calidad de la muestra impidiendo que cumpla con los estándares internacionales en la materia? Por estas razones es que el registro facial, otra vez manifestado como solución de registro biométrico universal, queda como un elemento más a ser utilizado pero no como la llave primaria del registro biométrico. El trabajo de campo ha hecho lugar a muchas experiencias pobres, muchos intentos de plagio, no solo con altas semejanzas en rostros más allá de gemelos, sino de etnias que logran una alta similitud sumando a esto las fallas en la calidad de su adquisición. Vale decir también que exitosas experiencias se han obtenido gracias a una rigurosa adquisición de imágenes faciales en ambientes controlados de enrolamiento en posición, luminosidad y fondo, pero esto no se da en todos los casos.

⁷ Introducción a la Biometría por huella dactilar, Tecnologías Biométricas de Identificación, <http://www.algdrainvac.com/PRESENTA-TECNOBIO-TB-distribuidores-2.pdf>

Por último, por su versatilidad, disposición, cantidad de información y rapidez de cotejo, diríamos que el Alfil sería el iris. Su usabilidad en controles de identificación tanto de documentos de viaje como de controles migratorios y controles de acceso no solo da fiabilidad sino también agilidad y velocidad en sus procesos. El estándar que rige su condición de adquisición es cumplimentado por varios proveedores y ya se puede ver implementado en varios lugares con gran éxito. Es sin duda una gran herramienta de validación de identidad. Pero, siempre hay un pero, es denostado por aquellos que persiguen muestras delictuales dado que “no se dejan” registros de iris en escenas de crímenes, mientras que si imágenes faciales en video o fotos, y como señalábamos anteriormente, ADN, huellas dactilares, plantares y palmares.

Como podrán ver, los registros dactilares, faciales, ADN e iris son los datos biométricos que podrían contarse con los cuales registrar a un individuo a los fines de custodiar y verificar su única identidad. Pero todas estas, dependiendo de la legislación vigente, su forma de adquisición, y otros factores, pueden sufrir de engaños. La implantación de una huella dactilar moldeada, la imagen fotográfica de un registro facial, y hasta la construcción de un globo ocular con un registro de iris con tinta infrarroja han sido partes de las pruebas de madurez de los sistemas automatizados biométricos para la comprensión de los límites y alcances en sus usos, procedimientos y procesos. Todas y cada una pueden ser utilizadas con eficacia dependiendo del ambiente donde se realicen, su combinación y otros factores que permitan elevar al máximo posible su eficacia.

Se podría aquí entonces, hablar del porqué de la Pirámide Biométrica.

El registro biométrico de un individuo lleva procedimientos y procesos que “ocupan” a la persona a desplazarse a algún lugar, llenar formularios y en algunos casos pagar por el trámite iniciado. ¿Qué tal si en ese mismo momento registráramos más de una elemento biométrico para la protección de su identidad? ¿Qué tal si más allá del dactilograma y la imagen facial registráramos los iris? De esta forma los organismos estatales de incumbencia podrían ofrecer diferentes formas de validar la identidad y es más, podría hacerla más certera y menos factible de usurpación requiriendo más de un dato biométrico a verificar, por ejemplo, facial más iris, iris más dactilar, etc.

Se estaría de esta forma constituyendo un triángulo de datos biométricos (dactilar-facial-iris) con que el individuo podrá, en diferentes situaciones y circunstancias, hacer valer y certificar su identidad biométrica. Ahora bien, quien le da la dimensionalidad a este triángulo es el ADN, puesto que su registro (en las ocasiones que la Ley lo permita) brindará el último de los datos biométricos a explorar.

Estas cuatro facetas biométricas constituyen cada una de los planos de una pirámide donde su vértice logra que en toda ocasión, registro, verificación para trámites, accidentes y actos vinculados con la seguridad, entre otros, el ciudadano y el Estado posea las herramientas con que poder hacer valer sus derechos y obligaciones en forma certera y ágil integrando a todo individuo incluyéndolo socialmente y equitativamente a sus pares.

Ciberidentidad

Hoy se vive en un mundo digital, y es cierto que “internet” ha crecido como un gran bazar. Sin embargo, todo bazar tiene códigos, estructuras y reglas. Internet no es la excepción. Dominios, subdominios, clases, protocolos y otros; hacen a la organización de este gran canal de comunicación que acerca fronteras y brinda la libertad de participación y opinión.

Internet nació con un objetivo: intercambiar información y compartir conocimientos. Pero excedió a sus propios clientes, de una “elite” paso a convertirse en la herramienta popular que es hoy. Y por ser la herramienta principal de la “democracia digital” es que debemos conocer y difundir sus riesgos, facilitar su utilización haciendo usable y accesible para todos y establecer los mecanismos para cuidar su ecosistema.

Para proteger esta herramienta, habría que definir qué la sustenta y qué la limita. Por el lado tecnológico, se da un paso más allá, debiendo definir proyectos que garanticen la sustentabilidad y garantice su usabilidad y accesibilidad, su “calidad de servicio y sus garantías”.

A estos fines cabe señalar que, como es de público conocimiento, el acceso a “Internet” se ha vuelto cada vez más de perfil crítico a la sensibilidad de su uso y contenidos, así como a las estrategias de comunicación, transacciones, tramitaciones, bancarización, entre otros, y esto hace que se deba formular un marco de protección de “la Red” y del material más importante que ella posee, NOSOTROS las personas.

La faceta tecnológica se viene cuidando y reforzando, como se señaló anteriormente, desde varias capas, desde la electrónica, las comunicaciones y los centros de datos, emprendiendo para esto las “**Políticas de Calificación de Datacenters**” parte integrante del esfuerzo de “**Protección de Infraestructuras de Información Críticas**” y el proyecto “**Argentina Conectada**”. Pero, ¿qué hay de los usuarios?

Ya en 2010, la Jefatura de Gabinete de Ministros anunció y puso en marcha el sitio “**Internet Sano**” con el fin de promover el conocimiento de los riesgos del uso “no cuidado” de Internet, con el fin de alertar a padres, madres y/o tutores, sobre la necesidad de que se involucren en este mundo con sus hijos. Pero hay más.

En este “cibermundo” hay cuestiones a tener en cuenta y donde el mundo real y el virtual tienen un nexo en común, EL USUARIO. El uso de las tecnologías digitales (e-x) en la relaciones ciudadano-gobierno, ciudadano-ciudadano, y otras relaciones digitales, afines a las clases de relaciones y comercios electrónicos, hacen que se necesite, más que nunca, resguardar nuestra identidad.

Para esto se deberá entender dos principios básicos: el derecho a ser “**anónimo**” y el derecho a tener una “**identidad digital confiable**”. El primero refiere a que el individuo que accede a las tecnologías debe tener la libertad de acceder a la información que las mismas brindan sin necesidad de estar siendo “trazabilizado”. O sea, salvo que el individuo viole alguna Ley, el individuo digital debe ser libre de transitar, expresarse y comunicarse por el mundo virtual resguardando su privacidad. Ahora también, a lo que se refiere a “**datos sensibles**” el individuo

tiene el derecho de tener una “identidad digital confiable” donde él y solo él pueda reclamar acceso a sus datos, procesos o trámites garantizándose que ningún otro, sin derechos sobre esos datos, pudiere obtenerlos.

En los primeros meses del 2011, fue de público conocimiento que se pusieron en riesgo, en diferentes partes del mundo, más de once mil millones de datos de personas a nivel mundial, compuestos de nombres, direcciones, tarjetas de crédito y sus suscripciones asociadas, y hasta de salud. Esto pone en riesgo la identidad del ciudadano, empresas y hasta de gobiernos.

A estos fines, en diferentes latitudes, se llevan adelante proyectos que permitan garantizar la forma confiable, interoperable y estándar para que el ciudadano pueda acceder en forma digital y confiable a la información que el Estado tiene de él, siendo esta una de las aristas de un Gobierno Electrónico eficaz y eficiente.

De lo expuesto, surge la necesidad de poseer herramientas de triple factor en el accionar del individuo con sus pares, empresas, organizaciones o gobiernos.

Sumar las claves a elementos con firma electrónica confiable (PKI) y a datos biométricos, brindará un ecosistema de identidad confiable, iniciativa que podrá ser adherida por gobiernos, organismos propulsores de estándares, y empresas validadoras de identidades en el ciberespacio.

Como se ha señalado, el 2011 nos encuentra cosechando aquellas semillas que desde el 2003 se venían sembrando. Inclusión social, inclusión digital, educación con equipos y herramientas informáticas, generación de contenidos digitales, televisión digital abierta y libre, hot-spots de Wi-Fi gratuitos y tendidos de Fibra Óptica que permitan integrar a toda la Nación en una gran red de comunicaciones y donde la distancia no sea un problema para compartir información, opinar libremente, transmitir ideas y participar activamente.

Desde el Gobierno Nacional se han hecho, se están haciendo y se seguirán haciendo proyectos en pos de la erradicación de la brecha digital que permitan llegar al mayor porcentaje de implementación de aquellos títulos tan enunciados como Gobierno Electrónico, Gobierno Abierto, Ventanilla Única, Despapelización, entre otros y todas aquellas nuevas iniciativas que den el marco de seguridad a todas las acciones planteadas.

Conclusión

En estos años dedicados a la gestión pública, he visto cumplir los objetivos planteados fortaleciendo al Estado con la implementación de proyectos tecnológicos de alta complejidad en la Administración Nacional y el uso de tecnologías en las políticas de identidad y seguridad.

Es nuestro camino el de seguir incorporando herramientas para asegurar los procesos y utilización de la identidad en cualquiera de sus formas. Fortalecer las herramientas biométricas que se vean implícitas en cada eslabón en cada acción, situación y trámite que sirva al ciudadano para su mejor bienestar social.

Tratar de superar esquemas simplificadores y lineales que, en general, relacionan el tema de

la identidad solo al ámbito de la seguridad, olvidando todo lo que la identidad brinda como persona como ser social al individuo.

Es nuestra meta para el año 2016 lograr la total inclusión digital como corolario de la inclusión social.

Es necesario incluir a la biometría dentro de la realidad social Argentina y mundial, trabajando no solo con los grupos afectados, sino con todos los actores sociales para lograr la mayor diversidad de opiniones y propender a una elevada calidad institucional para sustentar este nuevo pacto social donde el ciudadano es participante y actor principal en un gobierno abierto, igualitario y eficaz.

Normas y Biometría

Bradford Wing



Bradford Wing

Coordinador de Estándares de Biometría. NIST (National Institute of Standards and Technology).



Brad ha estado trabajando en el campo de la biometría desde comienzos de los '90. Se unió al National Institute of Standards and Technology (NIST) en 2008 luego de 20 años de carrera en el Department of Homeland Security (DHS), Programa US-VISIT, y en uno de los predecesores del DHS, el Immigration and Naturalization Service. En el NIST, Brad se desempeña como Coordinador de Estándares de Biometría con la responsabilidad de dirigir el desarrollo del estándar ANSI/NIST-ITL y dando soporte sobre esta tecnología a otras agencias federales. El ANSI/NIST-ITL es el estándar utilizado para la transmisión de datos biométricos e información asociada utilizado por las fuerzas y organismos de seguridad tanto dentro de los EEUU como internacionalmente. Participa activamente en otras organizaciones donde se desarrollan estándares de biometría, entre ellos OASIS, INCITS/M1 e ISO/SC37.

Trabajó como Ingeniero de Biometría en el programa US-VISIT del DHS. Allí fundó el Biometrics Coordination Group que reúne a los diversos componentes del DHS para garantizar un enfoque coherente para la biometría en todo el departamento. También se desempeñó como representante técnico para los EEUU ante la International Civil Aviation Organization (ICAO) en el desarrollo de pasaportes electrónicos, coordinando la ejecución de tests de interoperabilidad y conformidad.

Sirvió como copresidente del National Science and Technology Council's Subcommittee on Biometrics and Identity Management, el cual agrupa a representantes de distintos organismos gubernamentales de los EEUU para coordinar la investigación en biometría y estándares para su implementación.

Resumen

Este documento se referirá a la importancia de las normas en la aplicación o el uso de sistemas biométricos. Las normas o estándares han sido desarrollados para asegurar que los sistemas biométricos puedan ser efectivos y precisos frente a las necesidades de los usuarios, tales como la protección de la integridad de los datos, la privacidad y la seguridad.

En este artículo se encontrarán ejemplos que ilustran 18 aspectos de los sistemas biométricos como la captura de datos biométricos, la transmisión de datos, y los factores humanos. Se describirán las normas principales que son utilizadas en la comunidad biométrica, y se identifican las áreas insuficientes en la cobertura de los estándares biométricos.

Enviado a: Congreso Internacional de Biometría de la República Argentina (CIBRA), "Biometrías II" -- una contribución invitada.

Normas y Biometría

1. ¿Por qué tener un sistema biométrico?

La razón básica para tener un sistema biométrico es descubrir la identidad de una persona o verificar la identidad declarada de una persona. Un sistema biométrico está diseñado para responder las siguientes preguntas:

¿Es la persona la que dice ser?

a. Verificación (comparación de 1 a 1): Tengo un pasaporte con mi imagen digital del rostro almacenada en él, y afirmo que el pasaporte fue emitido para mí. Puedo usar la “vía de inspección automática” con éxito, sólo si una imagen que me fue tomada coincide con la información almacenada en mi pasaporte electrónico (“true match”). Un “false non-match” ocurre si el sistema no encuentra coincidencia.

b. Identificación: (comparación de 1 a muchos): Soy un empleado de una fábrica que utiliza el reconocimiento del iris para conceder la entrada a las instalaciones. Sólo puede entrar si la imagen de mi iris coincide con aquella en la base de datos (“true match”).

¿La persona no es quien dice no ser?

c. Verificación negativa: (comparación de 1 a 1): Se me ha acusado de un delito. Le proporcioné a la policía una muestra de mi ADN¹, quien lo comparará con el ADN de la escena del crimen. Estaré en libertad si no hay ninguna coincidencia (“true non-match”).

d. Identificación negativa: (comparación de 1 a muchos): En un cierto país, a todas las personas que son deportadas, se les capturaron los datos del iris y la información está en una base de datos. Al llegar al aeropuerto del país, el sistema biométrico escaneó mi iris. Pude entrar al país porque mi iris no coincidía con ninguno de los presentes en la base de datos. (“true non-match”)

¿Puede la persona ser identificada debido a la información en el sistema?

e. Identificación: Un paciente con “Alzheimer”² se encuentra vagando por las calles. Se toma una huella digital de la persona en una estación de policía cercana y se compara con una base de datos de personas desaparecidas. La impresión coincide con una impresión de la base de datos. La persona es identificada y devuelta a la familia que había presentado la denuncia de desaparición.

f. Clasificación: En el lugar de una catástrofe se encuentra parte de un cuerpo. Se obtiene una muestra de ADN del cuerpo y se la compara con el ADN de posibles familiares. En este caso, el

¹ ADN es el ácido desoxirribonucleico. Es una sustancia química que se forma una doble hélice, que es único para todos con la excepción de los hermanos idénticos.

² La enfermedad ‘Alzheimer’ es la forma más común de demencia. Es incurable.

³ ADN mitocondrial son pequeñas moléculas circulares de ADN situado en estructuras que se utilizan para proporcionar energía a la célula (mitocondrias). Su tamaño pequeño y su cantidad las hace especialmente útiles cuando hay solamente una pequeña cantidad de material biológico o el material está deteriorado. Se puede utilizar para rastrear los linajes maternos, ya que sólo se hereda de la madre.

que proveyó muestras de su ADN es un tío de dos de las víctimas. Se produce una coincidencia de ADN mitocondrial³ con dos de las víctimas, lo que significa que el pariente y dos de las víctimas tienen un ancestro común por parte de madre. En este caso, el ancestro común es la abuela, como se muestra en la figura 1. La identificación positiva del cadáver no podrá ser establecida porque el cuerpo podría haber pertenecido tanto a víctima 1 como a víctima 2, pero el cuerpo es clasificado como perteneciente a uno de los dos primos, con exclusión del resto de las víctimas.

Nótese que si el supuesto familiar (el tío) hubiese sido el hermano de los padres de las víctimas, como se muestra en la figura 2, entonces el test del ADN mitocondrial no hubiera mostrado ningún resultado utilizable. Si el tío hubiera sido el hermano de la madre de una de las víctimas y hermano del padre de la segunda, como en la figura 3, y hubiese una coincidencia del ADN mitocondrial del cadáver y del tío, entonces la identificación positiva de la víctima 1 como el hijo de la madre 1, podría ser establecida.

Figura 1. Árbol Familiar A

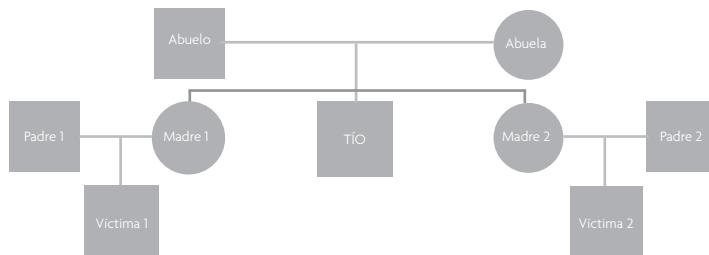


Figura 1. Árbol Familiar B

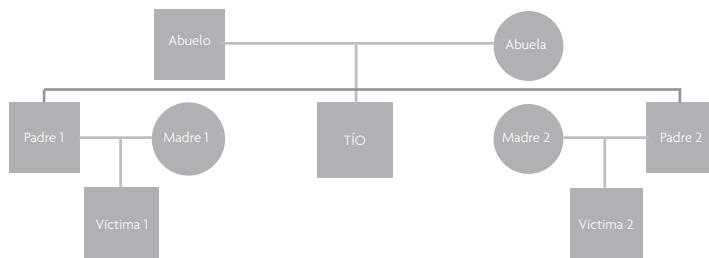
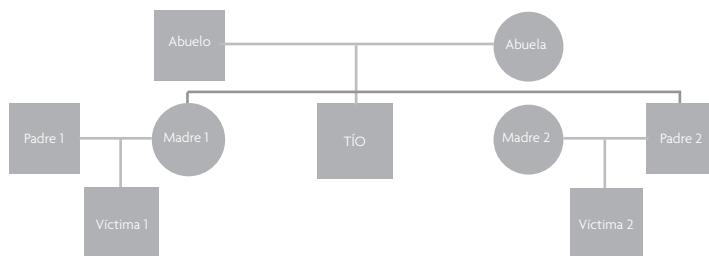


Figura 1. Árbol Familiar C



Hay variantes sobre los usos de la biometría arriba mencionados, pero todos tienen en común que la gente confía en que el sistema proporcionará un nivel de seguridad de que el resultado es correcto dentro de los niveles de tolerancia aceptables para ese sistema.

Los operadores de un sistema implementado deben considerar las limitaciones operativas y el costo. Las restricciones operativas incluyen: la política, la legislación, la integridad de los datos, la seguridad y la protección de la privacidad, la interoperabilidad con otros sistemas, las consideraciones ergonómicas, las condiciones ambientales, etc. Los datos recogidos, almacenados, transmitidos y usados en un sistema biométrico deberían:

- Mantener la fidelidad a las características biométricas del individuo (la persona que proporciona la muestra, es decir el sujeto);
- Describir el entorno y procedimientos de recolección; y
- Describir los datos pertinentes sobre el sujeto.

Además, el sistema debería:

- Tener un alto grado de fiabilidad con :
Niveles tolerables de “False matches” y “false non-matches” ⁴;
- Un tiempo medio entre fallos aceptable ((MTBF ⁵); y
- Requisitos de mantenimiento razonables ⁶;
- Proteger la privacidad de los datos del sujeto.

2 ¿Por qué se necesitan normas o estándares?

Las Organizaciones para el Desarrollo de Estándares (SDO por sus siglas en inglés) ⁷ han creado y crearán normas que puedan ser incorporadas en el diseño de sistemas y en los estándares que delinean los procedimientos operativos. Las normas ayudan a asegurar que un sistema biométrico funcionará correctamente y es capaz de intercambiar datos con otros sistemas. Estas normas han sido desarrolladas por expertos provenientes del gobierno, la academia y la actividad privada. Como resultado de incorporar estándares en el diseño de un sistema biométrico, el sistema tiene menos probabilidades de estar atado a una “solución propietaria” de un vendedor específico. Las soluciones propietarias pueden resultar en altos costos y posiblemente provocarán un fallo del sistema, si el proveedor deja de mantener el producto. Si los estándares no han sido incluidos en el diseño, existe la posibilidad de degradar seriamente la integridad del sistema.

Los perfiles de aplicación (“application profiles”) se basan en los estándares publicados. Una organización adapta los estándares a sus requerimientos particulares. Un campo de datos opcional puede ser requerido por un tipo de aplicación particular. Por ejemplo, el FBI, el Departamento de Defensa de Estados Unidos, la Policía Real Montada de Canadá, el Gobierno de Argentina, INTERPOL y otros han desarrollado perfiles de aplicación del estándar “Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information”, que comúnmente se

⁴ Los rangos tolerables representan una decisión clave del propietario del sistema.

⁵ El “MTBF” depende de la definición de fallo del propietario del sistema.

⁶ Algunos de los requisitos de mantenimiento puede implicar la limpieza de una placa de huella digital después de cada uso. El reemplazo de la batería para las unidades móviles es parte del mantenimiento, por lo que la vida de la batería es una consideración importante. El propietario del sistema define lo que es “razonable”.

⁷ La sección 4 describe las SDOs y estándares que éstas han desarrollado que son particularmente relevantes para la biometría.

conoce como el estándar ANSI/NIST-ITL⁸.

También existen las Recomendaciones de las Mejores Prácticas (BPR por su sigla en inglés) que describen la selección más adecuada de opciones y normas para los distintos tipos de escenarios. Un ejemplo es la “Recomendación de la mejor práctica de dispositivo de identificación móvil”⁹ para la policía y el ejército.

No todos los pasos en un sistema biométrico requieren un estándar. Muchas cosas pueden ser resueltas por los Procedimientos Regulares de Operación (SOP por sus siglas en inglés) e incluso el sentido común. Sin embargo, como ilustran los siguientes ejemplos, hay una necesidad de normas en ámbitos específicos. Los ejemplos que se dan a continuación no están listados en orden de importancia ni en el orden de procesamiento dentro de un sistema.

A) Recolección de una muestra biométrica

Los algoritmos para el reconocimiento del rostro funcionan mejor con una imagen totalmente frontal. Hay un elevado índice de falla en el reconocimiento cuando la cara no permanece en la posición completamente frontal. Es por eso que las fotos de pasaporte deben ser tomadas en una posición frontal completa con una expresión neutra, lo que se ha formalizado en el estándar para documentos de viaje internacional de la Organización de Aviación Civil Internacional (OACI)¹⁰. Los sitios de tomas fotográficas han sido diseñados para capturar todas las imágenes faciales en posición frontal en las instalaciones de viaje automáticas como RAPID¹¹ en Portugal, y SmartGate en Australia¹².

B) Registro de información asociada (metadatos)

Cuando se recoge un conjunto de huellas dactilares de un individuo es importante indicar, para cada impresión, de qué dedo se capturó la imagen. Los grandes sistemas de huellas dactilares normalmente comparan las huellas dactilares sólo contra aquellas que sean del mismo grupo (tal como espiral) para un tipo de dedo (por ejemplo, el dedo índice de la mano derecha). Si no hay metadatos que especifiquen el número de la posición del dedo, el sistema habrá comparado todas las imágenes de huellas dactilares en la base de datos; un proceso costoso y lento. Las normas como ANSI/NIST-ITL 1-2011 tienen campos que incluyen la información asociada a una imagen de la huella, como la posición de los dedos y el método de captura de la impresión (por ejemplo, impresiones de tinta o “livescan”).

En el ejemplo de “clasificación” consignado en la sección 1.0, la información asociada es extremadamente importante. Si el tío hubiese sido hermano de los padres de las dos víctimas, las pruebas mitocondriales no hubiesen servido para establecer una relación. Se habría tenido

⁸ ANSI / NIST-ITL el es acrónimo de American National Standards Institute / National Institute of Standards and Technology, Information Technology Laboratory. Esto significa que el NIST-ITL está acreditado por ANSI como una SDO. ANSI/NIST-ITL 1-2011 y sus predecesores se encuentran disponibles en inglés en: http://www.nist.gov/itl/iad/ig/ansi_standard/cfm. El gobierno de Argentina traducirá la norma en Español.

⁹ La BPR se encuentra disponible en <http://www.nist.gov/itl/iad/ig/mobileid.cfm>. Está disponible sólo en Inglés.

¹⁰ El estándar de la OACI para documentos de viaje, Documento 9303, está disponible en <http://www2.icao.int/en/MRTD/Pages/Document9303.aspx>. Esta disponible en árabe, chino, Inglés, francés, ruso y español.

¹¹ RAPID es un acrónimo en Portugués para “Identificación Automática de Pasajeros con documentos de viaje”.

¹² Ver Frontex informe técnico nº1 / 2010 “BIOPASS II, Automated Biometric Border Crossing Systems Base don Electronic Passports and Facial Recognition: RAPID and SmartGate” que está disponible en http://www.frontex.europa.eu/gfx/frontex/files/other_documents/biopass_ll.pdf

que utilizar un test totalmente diferente (Y-Short Tandem Repeat¹³⁾.

C) La recuperación de datos biométricos

Cuando una muestra biométrica (llamada “prueba”) se envía a un sistema a gran escala, la prueba puede ser comparada con un subconjunto de la base de datos, llamado galería o “target set”. Esta galería puede ser seleccionada según las características de los datos biométricos y también, según los metadatos tales como sexo y edad aproximada del sujeto. Si la información asociada es incorrecta o está incompleta, como se describe en la sección B) más arriba, el “target set” puede excluir los datos asociados con la identidad correcta en la base de datos, impidiendo una coincidencia.

Algunos sistemas recuperan la galería de una ficha (“token”) como una tarjeta de identificación con un chip, o un pasaporte electrónico. La galería en este ejemplo contiene datos para una sola persona, o sea para el propietario para el documento de identificación. Para asegurar que la ficha sea correctamente utilizada y que los datos biométricos en la tarjeta sólo estén disponibles para los sistemas autorizados, usualmente hay un sistema de control inserto en la ficha. Existe normalmente un sistema de control integrado en la ficha para asegurar que ésta se utilice correctamente y que los datos biométricos estén disponibles sólo para sistemas autorizados. En el caso de la tarjeta de identificación, el propietario puede ingresar un número de identificación personal PIN que autoriza el acceso al chip. Para un pasaporte electrónico, la información impresa en la “zona legible por la máquina” (MRZ, por sus siglas en inglés) sobre la página de datos, se escanea y se utiliza para generar una “clave” que el chip aceptará. Sólo entonces, podrá el sistema recuperar los datos biométricos.

Los ejemplos anteriores ilustran diferentes aspectos de la creación de una galería o “target set”. Los estándares afectan los sistemas biométricos de diversas maneras.

D) Factores no-biométricos

Este es un tópico muy amplio y puede resultar en la incorporación de otros estándares “no biométricos” en las especificaciones de un sistema biométrico.

Por ejemplo, la norma OACI para documentación de viaje incorpora la norma ISO para el reconocimiento de caracteres ópticos (Optical Character Recognition), en formato B (OCR-B)¹⁴. La información impresa en OCR-B es utilizada para generar una clave para acceder al chip contenido en el pasaporte digital. Sin esta clave no es posible leer los datos. Este proceso asegura que no sea posible acceder clandestinamente a los datos con un equipo en la proximidad del pasaporte electrónico sin que la página con el OCR-B sea deliberadamente presentada a una distancia cercana (10 cm.) del lector autorizado.

E) Análisis de la calidad de las muestras

La calidad de una muestra biométrica afecta dramáticamente su utilidad. Esto se aplica tanto a la muestra como a la galería. Si una huella dactilar está manchada, o si no se le aplicó suficiente presión cuando fue capturada, puede que no haya suficientes características distintivas, como por ejemplo las minucias o pequeños detalles. Un sistema necesita minucias para hacer coincidir

¹³ Repeticiones cortas en tandem (STR) son secuencias cortas de ADN que se repiten varias veces en sucesión directa. El número de unidades repetidas pueden variar ampliamente entre los individuos y el alto nivel de variación de STR hace especialmente útil para discriminar entre las personas. El cromosoma Y está presente sólo en los hombres.

¹⁴ ISO 1073-21976 está disponible en http://www.iso.org/iso_catalogue_detail.htm?csnumber=5568

con exactitud la muestra contra la galería. El análisis de la calidad de la imagen de la huella puede ser incorporado en un dispositivo de captura y proporciona información al operador. Por ejemplo, el programa US-VISIT¹⁵ de los Estados Unidos en los puertos de entrada del país, controla la calidad de las huellas dactilares capturadas en el momento de la captura. Se recogen hasta tres muestras que se analizan de forma automática por el sistema, utilizando la mejor. El operador también tiene la opción de retomar la huella dactilar del viajero si la calidad es de un nivel insuficiente. El nivel de calidad de la huella digital se almacena con la huella digital.

F) Almacenamiento inicial de datos

Si se llevan a cabo incorrectamente, el método y el proceso de almacenamiento de datos pueden anular por completo la utilidad de una muestra biométrica. Por ejemplo, cuando se toma una imagen de la huella debe almacenarse por lo menos con 19,69 píxeles por milímetro, lo que equivale a 500 píxeles por pulgada (pixels per inch-ppi). [1000 ppi se recomienda para las huellas latentes]. Algoritmos de compresión reducirá la imagen original de hasta 500 ppi para un almacenamiento y transmisión más eficientes. Algunos algoritmos de compresión, como JPEG¹⁶, no fueron diseñados para las huellas dactilares. JPEG forma cuadros a través de la imagen y comprime cada cuadro individualmente. Cuando se reconstruyen se puede introducir “artefactos”, como líneas pequeñas o puntos al lado del cuadro. Lo cual es un peligro, ya que estos artefactos podrían ser interpretados como minucias causando una falsa coincidencia (“false match”) o no produciendo una coincidencia válida (“false non-match”). Por lo tanto, un algoritmo de compresión especializado, llamado Wavelet Scalar Quantization (WSQ) almacena una imagen de 500 ppi. Existen especificaciones para WSQ¹⁷. Varios proveedores han desarrollado versiones diferentes de software que puede realizar esta compresión.

En EE.UU, la policía utiliza WSQ de proveedores múltiples al presentar muestras de huellas al FBI. El NIST convalida estos algoritmos frente a las especificaciones del FBI. El FBI publica una lista de productos del vendedor de WSQ que el FBI ha aprobado.

G) La transmisión a otra ubicación

Muchos sistemas biométricos incluyen procesos en lugares diferentes. El proceso de transmisión debe estar claramente especificado para mantener la integridad de los datos.

Por ejemplo, existía un sistema gubernamental de huellas dactilares que parecía estar bien diseñado. Sin embargo cuando se lo examinó, los procesos se mostraron deficientes. La imagen de la huella original fue almacenada en WSQ pero a continuación, se descomprimió y envío por fax a otro sitio. En ese otro lugar, la imagen fue escaneada después de ser impresa desde el aparato de fax, comprimida en formato JPEG y se transmitió al sitio central donde se descomprimió y se volvió a comprimir con WSQ. La captura original se almacenó utilizando WSQ así como el almacenamiento final (por lo que podría decirse entonces que la captura y el almacenamiento final fueron correctos), pero los datos de huellas dactilares habían sido destruidos por la compresión y descompresión de los múltiples pasos de la transmisión.

¹⁵ El documento “Biometric Standards Requirements for US-VISIT” está disponible en http://www.dhs.gov/files/programs/gc_1213298547634.shtml

¹⁶ JPEG es un acrónimo para el Joint Photographic Experts Group. Ellos crearon el estándar, que es: JPEG Interchange Format, Version 1.02 (JIF) que está disponible en: <http://www.hjpeg.org/public/jif.pdf>

¹⁷ IAFIS-IC-0110 (V3.1) “WSQ en escala de grises de huellas dactilares especificación de compresión, 4 de octubre de 2010” está disponible en: <https://www.frbiospecs.org>

Hay formatos de compresión que conllevan una parte de pérdida (lo que se conoce como “lossy”). Esto quiere decir que cierta cantidad de información contenida en la imagen original se pierde durante la compresión. Cuando se la descomprime, la imagen resultante no tendrá tantos detalles como la imagen original. Para las huellas dactilares, esto puede tener resultados extremadamente negativos.

A fin de abordar este problema, la norma ANSI/NIST-ITL 1-2011 establece que “las imágenes se comprimen sólo de una imagen original. Si una imagen ha sido recibida en un formato comprimido no se pueden descomprimir y volver a comprimir en el mismo o diferente formato.”

H) La comparación de la prueba frente a la galería

La comparación de la información biométrica puede ser automatizada, parcialmente automatizada o manual. Los sistemas automatizados de huella digital normalmente se basan en un conjunto específico de características dentro de la huella digital. La necesidad de codificar estos pequeños detalles (minucias) para el uso de computadoras fue reconocida como una necesidad de forma temprana. En 1986, la primera versión de lo que eventualmente se convirtió en la norma ANSI/NIST-ITL codificó minucias de huellas dactilares. El objetivo fue transmitir datos sin una recodificación extensiva.

Sin embargo, los especialistas forenses deben confiar en más tipos de información que el lugar donde las crestas terminan y se dividen (bifurcaciones), lo que forma la base de las minucias. También deben poder expresar sus hallazgos en una forma que puedan ser entendidas años más tarde por otros examinadores. Esto llevó al desarrollo del conjunto de características extendidas (Extended Feature Set – EFS) que se ha incorporado en la norma ANSI/NIST-ITL 1-2011. Especialistas forenses pueden especificar las características de una manera fija como: la ubicación de los poros, el número de crestas en una zona y otras características importantes. Los examinadores en otros lugares, y quizás separados por el tiempo, pueden hacer referencia a estas características en una forma que podría tener resultados muy importantes en los procesos penales.

I) Almacenamiento de los meta datos y las muestras

En muchas aplicaciones, existe el requisito de utilizar un mínimo de espacio, como los datos biométricos almacenados en una tarjeta de identificación. Los datos utilizados por comparadores en los sistemas biométricos del iris se pueden almacenar de una manera muy eficiente (en algunos casos tan poco como 3 kilobytes). Esto ha sido demostrado a través de la investigación realizada en el NIST¹⁸. Este análisis también encontró que una forma de almacenamiento compacto (el formato ‘polar’) resultó en la disminución de la exactitud de los sistemas. Ahora, ambas normas ISO y ANSI/NIST ITL permiten utilizar el formato “crop and mask” (cortar y ocultar) que ha demostrado mantener la fidelidad a la muestra biométrica original, pero al mismo tiempo reducir los requisitos de almacenamiento. Con el fin de mantener la exactitud del sistema, ni ISO ni ANSI/NIST-ITL permiten el formato “polar”.

J) Presentación de informes y uso de los resultados de la comparación

El producto de un sistema biométrico no es necesariamente un “sí” o un “no”. Una prueba siempre tiene características ligeramente diferentes a los datos de galería, por lo que una

¹⁸ Ver <http://www.nist.gov/itl/iad/ig/irex.cfm>

coincidencia no es exacta.¹⁹ De hecho, si es exacta, eso significa que la prueba y los datos de la galería provienen, exactamente, de la misma muestra, lo cual debería levantar sospechas sobre intentos de dañar el sistema. En muchos casos, sólo hay un conjunto de datos en la galería que están “cerca” en comparación con la muestra. En otros casos, puede haber varios conjuntos de datos de la galería que sean relativamente similares a la muestra. Las normas en general no cubren la presentación de los resultados directamente. Por lo general, esta es especificada por el usuario en base a los requerimientos del propietario del sistema. Por ejemplo, el Departamento de Estado de Estados Unidos tiene un sistema de reconocimiento facial para verificar que las personas no estén “comprando una visa” expresión que se aplica a las personas que solicitan una visa con distintos nombres en distintos consulados esperando que alguna de las solicitudes sea aprobada.²⁰ El sistema automatizado proporciona una lista de las “mejores” coincidencias frente a la galería de los candidatos anteriores. Un equipo de analistas se determina si hay una verdadera coincidencia (“true match”) o un match muy probable.

Otros sistemas, tales como el control de acceso o de activación del equipo (control de acceso lógico) requieren una decisión de “sí o no”. Se establece un “umbral” para una coincidencia. Es decir que tiene que haber suficientes características en común entre los datos de la muestra y los de la galería. Si se alcanza este umbral, entonces se concede el acceso. Ya que siempre hay un equilibrio entre el “false match” y “false non-match”, este umbral puede ser diferente para circunstancias distintas.

Una instalación nuclear establecerá el umbral de manera tal que el acceso no pueda ser concedido, a menos que haya una coincidencia muy cercana en las características biométricas. Esto significa que a alguna persona de vez en cuando se le negará la entrada a pesar de estar efectivamente autorizada para entrar. Es por eso que un procedimiento de “back-up” debería estar siempre en funcionamiento para los sistemas biométricos. Otro ejemplo es el de un parque de diversiones con una entrada automática para sus clientes con abonos para no incomodar a sus clientes. El parque de diversiones por lo general establecerá un umbral más bajo y aceptará el hecho de que algunas transacciones podrían ser realizadas por impostores y reconocidas como auténticas por el sistema biométrico. A medida que los sistemas biométricos mejoren, el mismo nivel de “true match” podrá ser alcanzado con niveles cada vez más bajos de “false match”. Esto significa que el umbral puede ser elevado manteniendo el mismo nivel de servicio a los clientes y con un nivel aún más bajo de pérdida de dinero potencial para el parque de diversiones a través del uso no autorizado de abonos.

Los procesos y procedimientos de información y el establecimiento de los umbrales se basan en las necesidades específicas del usuario y tienen en cuenta los estudios científicos sobre el rendimiento del sistema biométrico. Esto no se considera actualmente como un área para los esfuerzos de estandarización.

K) El análisis de bases de datos

El análisis de las bases de datos es crítico para mantener un sistema biométrico que sea confiable y eficiente. El análisis de las bases de datos abarca varias cosas, tales como la revisión de los datos asociados con la muestra biométrica, el análisis de la calidad de los datos biométricos y la ponderación de la importancia relativa de los valores de calidad y varios temas relacionados

¹⁹ Bajo ciertas circunstancias, es posible tener una coincidencia exacta con ADN

²⁰ Ver <http://www.nist.gov/itl/iad/ig/irex.cfm>

directamente con la eficiencia de la estructura de almacenamiento de datos y el mecanismo de recuperación de los mismos.

Uno de los aspectos del análisis de bases de datos que es fundamental es “la reconciliación de las bases de datos”. Esto también puede ser denominado como “el establecimiento de la verdad fundamental” Por ejemplo, la Patrulla Fronteriza (Border Patrol) de los EE.UU. puede detener a la misma persona en las diferentes ocasiones que intente ingresar ilegalmente en los EE.UU. Es poco probable que una persona del mismo nombre, en cada una de las detenciones, exista y tenga la posibilidad de ser enviado a la cárcel (en lugar de ser simplemente expulsado de los Estados Unidos) si se detectan múltiples intentos de entrada ilegal. Las huellas dactilares del sujeto se comparan en un sistema central (IDENT). Una fotografía del sujeto se asocia con cada captura y las muestras de las huellas dactilares. El agente de la Patrulla Fronteriza puede “vincular” dos identidades diferentes en IDENT basándose en los resultados que se presentan - estableciendo así que (al menos) dos alias diferentes existen para el mismo individuo.

Nótese que también es posible “desvincular” dos registros de detención si se demuestra que las huellas, en realidad se refieren a sujetos diferentes.

L) Confiabilidad del software y el hardware

Esta es un área extremadamente complicada. Hay varios normas que se aplican a los sistemas tanto biométricos como no biométricos. Por ejemplo, en el “Mobile Device ID Best Practice Recommendation Version 1.0” (BPR) hay una sección que se ocupa de las condiciones ambientales. Dice: “Es responsabilidad de la Agencia decidir, en la fase de adquisición de los dispositivos de identificación móvil, qué perfil pedir ... Es importante elegir el perfil adecuado ya que un perfil más bajo podría significar que los dispositivos no sean capaces de soportar el entorno operativo, causando fallas costosas y la disminución de los niveles de servicio, mientras que la elección de perfil demasiado alto puede causar un aumento innecesario en el tamaño, peso y costo de los dispositivos.”

Para los distintos perfiles que figuran en las Recomendaciones de las mejores prácticas, se remite a estándares que abordan las pruebas de equipos para ciertas condiciones ambientales. Un ejemplo es el perfil militar cuando se hacen pruebas para el funcionamiento de la supervivencia de los dispositivos biométricos móviles, operando a diferentes temperaturas: ensayo con la norma MIL-STD-810F método 502.4 procedimiento II a -20 grados Celsius y el uso de la norma MIL-STD-810 Método 501.4 Procedimiento II a los 60 grados centígrados²¹.

Las áreas evaluadas incluyen las temperaturas de funcionamiento, las temperaturas de almacenamiento, la humedad relativa, la protección del ingreso (resistencia a la infiltración de agua), y la resistencia a la caída.

M) Análisis del nivel de función del sistema

Los propietarios de sistemas desean tener el mejor sistema que puedan pagar y que sea adecuado a sus condiciones operativas. Las evaluaciones de la función del sistema pueden ayudar a los desarrolladores del algoritmo biométrico y de los componentes del sistema, así como a los propietarios. Es posible determinar el nivel de función de los algoritmos y componentes con un análisis en circunstancias controladas.

²¹ Los estándares para el método de prueba para la ingeniería del medio ambiente del Departamento de Defensa de Estados Unidos están disponibles en <http://www.dtc.army.mil/navigator>

Un ejemplo es la “Slap Fingerprint Segmentation Evaluation II”²², dirigida por el NIST. Se trata de una evaluación continua. Los participantes pueden presentar sus algoritmos en cualquier momento al NIST. El concepto es que algunos dispositivos de captura de huellas dactilares puedan capturar las imágenes de cuatro dedos de una sola vez, en un rodillo grande. Las huellas dactilares individuales deben ser segmentadas. Varios problemas complican la segmentación, como la rotación de la mano en el rodillo, que los dedos estén muy juntos, los imágenes “fantasmas” de impresiones residuales en el rodillo, imágenes apenas perceptibles de los dedos individuales, que falten dedos, las “aureolas” de calor alrededor de las impresiones.

N) Análisis de las repercusiones legales y de la privacidad

Las expectativas y los requisitos de protección legal, cultural y de la privacidad varían considerablemente en las distintas jurisdicciones. Las regulaciones y los SOP (“Estándares de procedimientos de operación”) que se ocupan de estas cuestiones son desarrollados a nivel jurisdiccional y no formalizados en estándares, dadas las variedades de requerimientos y expectativas.

Ciertas viajeras, por razones culturales, pueden mantener la cara parcialmente cubierta. Sin embargo, la imagen de la cara descubierta debe estar en el pasaporte. Con el fin de realizar una comparación de las viajeras con la imagen en el pasaporte, muchas jurisdicciones han establecido procedimientos especiales para llevar a la viajera a una zona de control especial.

O) Los factores humanos / el diseño de la interfaz humana

Esta es un área que sólo recientemente ha tenido estándares y recomendaciones de las mejores prácticas.

Esta área abarca temas tan diversos como figuran en esta lista. Los que se mencionan a continuación son sólo ejemplos y no una cobertura exhaustiva de los problemas²³.

- ¿Qué ángulo debe tener un dispositivo de captura de huellas dactilares en relación con el viajero y a qué altura debe ser colocada?
- ¿Qué símbolos (iconos) en los dispositivos biométricos interpretan más fácilmente las personas?
- ¿Cómo mejorar la interfaz con una persona que toma una foto para asegurar que la cara del sujeto esté en el centro del foto y el sujeto esté a la distancia apropiada de la cámara?
- ¿Cómo se diseñarán los dispositivos móviles de captura de huellas dactilares de modo que los sujetos no los vean como armas? ¿Cómo utilizar la máquina con una sola mano?

P) Diseño de la interoperabilidad (datos usados en otros sistemas)

Este es uno de los factores principales en el desarrollo de estándares biométricos. Un sistema biométrico aislado (como el control de acceso para una empresa pequeña) por lo general no tiene la obligación de enviar los datos a otros sitios ni recibe los datos biométricos de los otros sistemas. Cuando un sistema es grande y/o necesita datos biométricos de otros sistemas, debe utilizar un formato de datos común y hay un entendimiento común sobre el contenido de los

²² Ver: <http://www.nist.gov/itl/iad/ig/slapsegii.cfm>

²³ Ver <http://zing.ncsl.nist.gov/biousa/> para estudios en human factors.

datos biométricos. Necesita asegurar un uso adecuado de los mismos así como la posibilidad de la utilización efectiva en otro sistema.

Un ejemplo es un escenario del “primero en responder” (“first responder”). En el lugar donde haya sucedido una catástrofe ayudará el personal de varias agencias diferentes. En el sitio no debería haber personas no autorizadas. Los bomberos de una jurisdicción tienen sus huellas digitales registradas en la base de datos de su empleo. Los profesionales de la medicina de un hospital cercano tienen sus huellas digitales registradas en la base de datos del hospital. Si cada uno de estos sistemas fue diseñado para almacenar los datos de las huellas dactilares de una forma “estandarizada”, un sistema móvil en el lugar del desastre cargará los datos de las huellas dactilares de las personas autorizadas y verificará los “primeros en responder” para acceder al sitio utilizando las huellas dactilares.

Otro ejemplo es el de INTERPOL. INTERPOL ha establecido una base de datos de huellas dactilares de personas buscadas por delitos muy graves. Las huellas dactilares provienen de una variedad de agencias gubernamentales de todo el mundo. Gracias a los estándares biométricos es posible utilizar las huellas de otras agencias en todo el mundo para determinar si se han encontrado a una persona en la base de datos de INTERPOL²⁴.

Q) La certificación de los productos biométricos, los laboratorios de testeo de sistemas, y los procedimientos de prueba

Al adquirir equipos, los propietarios del sistema quieren estar seguros de que éste funcionará y cumplirá con las especificaciones. En el proceso de adquisición de sistemas grandes, el propietario del sistema puede probar los productos de diferentes proveedores en condiciones simuladas antes de tomar una decisión de compra. Esta opción es demasiado costosa y consume mucho tiempo cuando se compra una cantidad pequeña.

Las variedades de pruebas y los métodos para realizarlas es algo en lo que se han concentrado las actividades de estandarización. NIST ha establecido el National Voluntary Laboratory Accreditation Program (NVLAP)²⁵. Está diseñado para verificar que los laboratorios que realizan pruebas de conformidad con las normas, pruebas de interoperabilidad, tecnología de pruebas, pruebas de hipótesis y pruebas de funcionamiento y facilidad de uso para los productos biométricos, sigan estándares de prueba reconocidos nacional e internacionalmente.

R) Seguridad (vitalidad, detección de fraudes, seguridad de la información)

Ciertos aspectos de la seguridad, como la garantía de la información, tienen varias normas aplicables a los sistemas biométricos. Estos incluyen la encriptación, el “hashing” de los datos, la firma digital, y mucho más.

La OACI estableció una versión modificada de la “Public Key Infrastructure” (PKI) (Cifrado de Clave Pública) para su uso en los pasaportes electrónicos. Hay un “certificado de la firma de documento” que comprueba que los datos no se han modificado desde que fueron escritos en el chip que está en el pasaporte. Sin embargo, esto no garantiza qué organización escribió los datos en el chip. Un “certificado del país firmante” también se utiliza en los pasaportes electrónicos para indicar que el pasaporte es un producto válido de esa nación. La “clave” para

²⁴ La implementación de INTERPOL de la norma ANSI / NIST-ITL está disponible en <http://www.interpol.int/Public/Forensic/fingerprints/RefDoc/ImplementationV5.pdf>

²⁵ Ver: <http://www.nist.gov/pml/nvlap/nvlap-bio-lap.cfm>

leer este certificado es compartida a nivel nacional. Si ambos certificados son válidos para el pasaporte, entonces la información en el chip del pasaporte puede ser considerada verdadera. Otras variedades de controles son efectuados para garantizar que los datos impresos en el pasaporte no hayan sido alterados.

Un área de investigación nueva y que aún no posee estándares es la detección de vitalidad y la detección de fraudes. Queremos saber si una muestra biométrica fue capturada de un sujeto vivo y del sujeto correcto. Por ejemplo, algunos dispositivos de huellas digitales tienen competencia para la detección de las venas en la mano para ayudar a asegurar que el sujeto esté vivo y que no se haya presentado un dedo accidentado o artificial.

Nótese que ciertas situaciones no necesitan la detección de vitalidad, tal como la captura de las huellas dactilares de una persona difunta.

3. ¿Qué normas existen y cómo se utilizan?

Los estándares biométricos fueron desarrollados para cumplir con necesidades específicas de los usuarios y para reflejar los diversos requerimientos técnicos inherentes a las modalidades biométricas, tal como el ADN y el reconocimiento facial.

Los sistemas biométricos pueden también necesitar confiar en otros estándares que fueron desarrollados para un amplio espectro de aplicaciones, tales como el Federal Information Processing Standard 180, Secure Hash Standard²⁶.

Existe publicada una lista de las normas biométricas y sus áreas de uso para el Gobierno de Estados Unidos que se encuentra disponible públicamente. El “Registry of USG Recommended Biometric Standards”²⁷ tiene las siguientes categorías:

- colección de datos biométricos, almacenamiento y registros de intercambio;
- perfiles de transmisión de datos biométricos;
- perfiles biométricos de credenciales de identidad;
- normas técnicas de interfaz;
- métodos de prueba para la prueba de conformidad con los estándares biométricos;
- estándares para la metodología de prueba de rendimiento de sistemas biométricos.

Las principales normas que se utilizan en todo el mundo son las siguientes:

1. ANSI/NIST-ITL²⁸ Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information

(Centrado en la aplicación de la ley, para la comunidades de inteligencia y militares, y aplicaciones de seguridad.)

Perfiles de Aplicación desarrollados para usos específicos tales como:

- FBI / agencias de policía de EE.UU.
- EE.UU. Department of Defense
- Royal Canadian Mounted Police
- Terrorist Watchlist Person Data Exchange

²⁶ SHA-256 hashes are described in this document and are the basis for some of the data fields in the ANSI/NIST-ITL 1-2011 standard.
The standard is available at http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

²⁷ Ver: <http://www.biometrics.gov/Standards/Default.aspx>

²⁸ Ver: http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

- US-VISIT
- INTERPOL
- United Kingdom National Policing Improvement Agency
- Bundeskriminalamt (Alemania)
- La Unión Europea – Visa Information System
- Western Identification Network

Cubre ejemplares e impresiones latentes por crestas de fricción (huellas dactilares, palmares y pies); imágenes de marca facial / cicatriz / distribución de puntos de aguja / tatuaje / iris / y las características distintivas de otra partes del cuerpo; marcas forenses de huellas dactilares, imágenes faciales y las imágenes del iris; ADN; metadatos y datos de referencia asociados, tales como fotografías de la escena del crimen.

Modalidades múltiples pueden ser incluidos en una sola transacción

- ISO / IEC 19794-x (normas) e ISO 29794-x (conformidad)²⁹

Orientado a aplicaciones civiles

Implementaciones de las normas a gran escala con la cara, los dedos y del iris, como:

La tarjeta de la India de identificación único (UID) y

Las especificaciones para pasaportes electrónicos de la OACI

Cubre varias modalidades por separado (minucias del dedo, la imagen y los datos espectrales y del patrón esquelético; imagen de la cara, imagen del iris, firma / signo; vascular; geometría de la mano) para la transmisión y las pruebas de conformidad

- CBEFF – Common Biometric Exchange File Format

Define un conjunto de información “de cabecera” para una transmisión.

Permite la incorporación de datos biométricos y meta datos conformes con varios estándares.

- a. INCITS 381 (imágenes de huellas dactilares), INCITS 378 (plantillas de huellas dactilares), INCITS 385 (imágenes faciales)

Desarrollado como las normas de EE.UU. antes de los estándares ISO / IEC 19794-x internacionales.

Es usado por las especificaciones para la Personal Identification Verification (PIV) tarjetas del Gobierno de los EE.UU. para los empleados de Gobierno de los EE.UU. y contratistas.

4.0 ¿Qué queda por hacer?

Aunque existen normas para especificar varios aspectos de los sistemas de biometría, aún existen lagunas. Además, las normas existentes deben actualizarse para reflejar las necesidades

²⁹ La lista de normas y estándares en desarrollo en SC37 está disponible en:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45020

y requerimientos de los propietarios de sistemas biométricos y sus usuarios. Actualmente existen tres foros principales para el desarrollo y la modificación de los estándares biométricos:

A) ANSI / NIST-ITL grupos de trabajo

ANSI/NIST-ITL publicó recientemente una nueva versión (ANSI/NIST-ITL 1-2011).

Ya hay 3 grupos de trabajo en marcha:

Análisis dental (forense) y de mordedura humana

El reconocimiento de voz

Pruebas de conformidad

B) ISO / SC37 (Subcomité³⁰ - Biometría³¹)

ISO / SC37 tiene en marcha varios proyectos. Estos incluyen:

Revisões de las normas existentes

El reconocimiento de voz

Datos de ADN

Pictogramas o iconos y símbolos para los sistemas biométricos

C) Comité Técnico para la Integración OASIS BIAS (Organization for the Advancement of Structured Information Standards, Biometric Identity Assurance Services Integration Technical Committee)³²

El comité Técnico BIASOASIS se concentra en proveer un marco documentado y abierto para desplegar e invocar las capacidades del aseguramiento de la identidad que pueden ser accedidas desde los servicios de internet. El comité técnico define y describe métodos y enlaces que pueden ser usados dentro de los servicios de web transaccionales basados en XML y arquitectura orientadas al servicio.

La siguiente lista es sólo una muestra de proyectos que existen para mejorar o introducir las normas biométricas:

- Las huellas dactilares sin contacto
- La transformación de datos dactilares en 3 dimensiones para ser comparados con las bases de datos de dos dimensiones
- Forma del oído
- Modelos de marcha
- Olor humano
- Biometría ocular: incluyendo la región alrededor del ojo, así como el ojo
- Onda infrarroja corta y media por la imagen facial
- Envejecimiento de sujetos y muestras biométricas
- Detección de cambios deliberados de una característica biométrica, incluyendo:
 - La Cirugía plástica de la cara, o la mutilación de las huellas dactilares
 - Detección de vitalidad
 - Técnicas contra la falsificación
 - Optimización del diseño de los sistemas biométricos de gran escala
 - Uso adecuado de los “soft biometrics” (tales como altura, peso, color de la piel, etc.)

³⁰ INCITS normas están disponibles en <http://www.incits.org>

³¹ Ver http://www.iso.org/iso/iso_technical_committee.html?commid=313770

³² Ver <http://www.oasis-open.org/committees/bias>

- Fusión de datos biométricos de tipos multi-modal / multi-muestra / multi-instancias
- Análisis de la calidad en el momento de la captura y de la base de datos
- La integración de los procesos de otras disciplinas y procedimientos de los datos biométricos como: la detección facial de micro-movimientos típicos del engaño) y la inteligencia artificial para ayudar a los analistas forenses
- Diseño de métodos para el funcionamiento óptimo de los usuarios y los operadores
- Nuevos métodos y capacidades de comunicación
- “Toma de decisión dinámica”, incluyendo: la modificación automática o asistida de los parámetros del sistema operativo biométrico basado en la demanda actual al sistema.

Conclusión

Los estándares sólo tiene sentido si son usados. Los estándares sólo serán usados si sirven a un propósito y cubren las necesidades de los usuarios y propietarios de los sistemas biométricos. Este es un proceso continuo, pero las normas deben permanecer lo suficientemente estables como para poder ser efectivamente usadas durante un lapso de tiempo. No todos los sistemas serán capaces de adaptarse a las nuevas normas en la misma proporción.

Es importante que los propietarios y usuarios de los sistemas biométricos se acerquen a los organismos de estandarización y participen en el proceso de desarrollo.

Por ejemplo, ANSI/NIST-ITL opera con el método “canvass” y está abierto a todas las partes interesadas. La membresía de OASIS está abierta a todas las organizaciones interesadas. ISO/SC37 y se organiza en torno a la representación de organizaciones nacionales. Cada organización nacional establece sus reglas propias para la participación, pero pueden estar constituidas por representantes de la industria, el gobierno y la academia. OASIS está abierto a todas las organizaciones interesadas.

Es el trabajo permanente de los organismos de normalización, el garantizar que tengan una representación adecuada todos los grupos afectados así como garantizar que las normas que los SDO desarrollan son un reflejo de las necesidades de la comunidad y están al mismo tiempo basadas en la investigación científica sólida.

La cooperación internacional y las iniciativas de seguridad en la identificación de individuos usando el ADN o las huellas dactilares propuesta por INTERPOL

Mark Branchflower / Jess Maltby



Mark Branchflower

Jefe de la Unidad de Dactiloscopia. INTERPOL.



Fue entrenado en Scotland Yard desde 1984 hasta 1990, año en el que fue premiado por sus méritos. Ha trabajado en diversos aspectos con huellas digitales incluyendo: 10 impresiones, procesamiento de impresión latente, evaluación de escena del crimen y trabajo de laboratorio. Luego de 6 años junto a la Policía Metropolitana, incluyendo también 1 año en la Unidad de Huella Digital Anti Terrorismo, se postuló para un cargo en la INTERPOL.

Se inició como perito en huellas digitales con INTERPOL en 1990, luego de dos años ascendió a Examinador Senior de Huellas Digitales y en 2005 fue nominado para Jefe de la Unidad de Huellas Digitales.

Durante estos 17 años estuvo involucrado como organizador y participante de INTERPOL en: Grupos de trabajo para INTERPOL de Europa e Internacional (6 por año). Presidente y Organizador de Simposios de Huella Digital de Interpol. Presencia en numerosas conferencias en más 35 países alrededor del mundo. Entrenamiento de personal en uso de AFIS para DVI. Participación en seminarios, grupos de trabajo y colocación de sistemas AFIS para DVI. Miembro del grupo de trabajo de ADN para INTERPOL. Desarrollo de estándares para la transmisión de registros de huella digital internacionalmente. Desarrollo y promoción de servicios AFIS de INTERPOL.

En la actualidad, sus tareas incluyen la dirección de un grupo de 6 especialistas en huellas digitales, intercambio y procesamiento de emparejamiento de información, promoción de servicios AFIS para INTERPOL y actualización constante en los últimos desarrollos. Recientemente, fue nominado a Presidente para el grupo de Usuarios de Sagem Internacional, lo que implica trabajar junto con la Dirección de Sagem y a la vez, junto con los delegados de países miembros para lograr el mejor rendimiento del sistema AFIS y mirar hacia el futuro.



Jess Maltby

Oficina de Registros Criminales, ACPO.



Jess Maltby es empleada de la agencia del Reino Unido en la Oficina de Registros Criminales ACPO (ACRO por sus siglas en inglés) y se encuentra actualmente asignada a la Unidad de huellas dactilares de INTERPOL con varios proyectos para promover el uso de AFIS de INTERPOL, por un periodo de 6 meses.

Resumen

Este paper ha sido escrito por Mark Branchflower y Jess Maltby e incluye conocimiento funcional en la materia de las dos personas a cargo del área de huellas dactilares de INTERPOL.

Este paper se referirá a dos de las bases forenses de INTERPOL, huellas dactilares y ADN y examinará cómo los países miembros de INTERPOL pueden usar los servicios y qué beneficios pueden obtenerse de ellos.

La conclusión es un sueño personal que creemos puede volverse realidad si todos los participantes involucrados en la esfera forense, a nivel mundial toman la decisión de cumplir el pedido de la Organización de poblar las bases de datos e investigar en ellas.

La cooperación internacional y las iniciativas de seguridad en la identificación de individuos usando el ADN o las huellas dactilares propuesta por INTERPOL

Introducción

INTERPOL es la organización policial internacional más grande del mundo, con 188 países miembros. Creada en 1923, hace posible la cooperación policial internacional y apoya y colabora con todas las organizaciones, autoridades y servicios cuya misión sea prevenir o combatir el delito internacional.

El objetivo de INTERPOL es el de facilitar la cooperación policial incluso en aquellos casos en los que no existen relaciones diplomáticas entre países particulares. La acción se lleva a cabo dentro de los límites de las leyes existentes en diferentes países y en el espíritu de la Declaración Universal de los Derechos Humanos. La constitución de INTERPOL prohíbe “cualquier intervención o actividad de carácter político, militar, religioso o racial.”

Uno de las funciones principales de INTERPOL es la de posibilitar que las policías del mundo intercambien información de forma segura y rápida. El sistema de comunicaciones global I-24/7 conecta a funcionarios de la seguridad en los 188 países miembros, y los provee de los medios para compartir información crucial sobre delincuentes y actividades delictivas.

Dado que los delincuentes y las organizaciones delictivas están, por lo general, involucradas en múltiples actividades, I-24/7 puede cambiar de forma fundamental la manera en la que las autoridades policiales trabajan juntas alrededor del mundo. Fragmentos de información aparentemente no relacionados pueden ayudar a crear una imagen y resolver una investigación criminal transnacional.

El uso de las Oficinas Nacionales Centrales de I-24/7 puede buscar y verificar datos en una cuestión de segundos, con acceso directo a bases de datos que contienen información sobre sospechosos de terrorismo, personas buscadas, huellas dactilares, perfiles de ADN, documentos de viaje perdidos o robados, vehículos robados, obras de arte robadas, etc. Estos múltiples recursos le otorgan a la policía acceso instantáneo a información potencialmente importante, facilitando así las investigaciones sobre delitos.

El sistema I-24/7 también les permite a los países miembros acceder a las bases de datos nacionales de unos y otros usando una conexión “business-to-business” (B2B). Los países miembros administran y mantienen sus propios datos criminales a nivel nacional. Estos países tienen la opción de hacerlos accesibles a la comunidad de la seguridad internacional a través del sistema I-24/7.

Aunque el I-24/7 está inicialmente instalado en las Oficinas Centrales Nacionales, INTERPOL está alentando a los países miembros a extender sus conexiones con las entidades nacionales de seguridad tales como la policía fronteriza, la aduana y las agencias de inmigración, etc. Las

Oficinas Centrales Nacionales controlan el nivel de acceso que otros usuarios autorizados tienen a los servicios de INTERPOL y pueden requerir que se les informe de consultas hechas por otros países a sus bases de datos nacionales.

Perspectiva general forense

Identificar el rol de un individuo en un delito, y si está o no vinculado a ofensas previas a veces puede poner a prueba el sistema de verificación. Es más, si un individuo comete un delito en un país y es condenado por él, cumple su condena y después se traslada a otro país y comete otro delito, entonces es importante que existan redes de comunicación e intercambio entre países. Esta es la principal función de INTERPOL que trabaja para posibilitar ese tipo de comunicación policial más allá de las fronteras.

Así como las huellas dactilares y el ADN son importantes para establecer una identidad sospechada en el primer momento, también es central que esa información biométrica esté disponible para otros países para establecer coincidencias (“matches”) si un individuo comete un delito en un lugar diferente al del delito inicial en el que se estableció el registro de las huellas dactilares. Por lo tanto es necesario que los registros estén disponibles a nivel global (a individuos autorizados), dado que hoy el delito ha adquirido crecientemente una naturaleza transnacional.

Ciertos delitos tienen a suceder a través de una serie de países debido a su naturaleza. Estos incluyen fenómenos tan diversos como el terrorismo internacional, el tráfico de drogas, el tráfico ilegal de armas, el contrabando de material radioactivo, el tráfico de personas, el tráfico global de sexo, el crimen organizado, el tráfico de órganos humanos, la falsificación de documentos e identidades, la extorsión y muchos otras formas de delitos estatales y corporativos.

La importancia de compartir información biométrica fue subrayada en abril de 2011 cuando se informó que cientos de prisioneros (aproximadamente 480), incluyendo miembros del Talibán, habían escapado de una prisión afgana. Desafortunadamente se supo que las autoridades afganas no habían sido entrenadas ni tenían equipamiento para tomar, almacenar y tener acceso a fotos, huellas dactilares o muestras de ADN de posibles terroristas internacionales, que pudieran ser compartidas internacionalmente. Esto presentó un enorme riesgo global y subraya la necesidad del intercambio de esta información y la cooperación en la identificación de individuos que puedan ser una amenaza a la seguridad pública.

Por otro lado, este episodio sucede tres años después de otra fuga en masa de la misma prisión de casi el doble de internos de la cual INTERPOL todavía no ha recibido información identificatoria para su circulación en la comunidad policial internacional. Luego de la última fuga, el Secretario General de INTERPOL notificó a los países vecinos de Afganistán pero con la poca información identificatoria será muy difícil para ellos poder hacer algo con los potenciales sospechosos.

Las huellas dactilares y el ADN son también de extrema importancia en el momento posterior a una catástrofe.

Luego del tsunami en Phuket, en 2004, INTERPOL trabajó activamente en la coordinación de los esfuerzos por identificar a las víctimas internacionales. La respuesta de INTERPOL al desastre

fue puesta en marcha la misma mañana del tsunami, el 26 de diciembre de 2004, cuando su comando y centro de control activos 24 horas por día se contactaron con los países afectados para ayudarlos. INTERPOL también informó a su red de equipos internacionales DVI y envió un equipo de respuesta a incidentes (IRT, por sus siglas en inglés) a Tailandia para comenzar la tarea de manejo de datos en terreno.

De las 3750 víctimas registradas, casi 3000 fueron identificadas durante el año posterior al desastre. INTERPOL jugó un rol central en coordinar la identificación internacional de víctimas y en proveer apoyo logístico y comunicacional. Más de 2000 funcionarios de 31 naciones participaron del proceso de identificación, tomando muestras de ADN, realizando análisis forenses, clasificando información y ayudando con la repatriación de los restos de las víctimas del tsunami. Aproximadamente 45% de las identificaciones realizadas durante el año siguiente, fueron hechas vía registros dentales, 35%, a través de huellas dactilares, y el 20% a través del ADN. Se espera que el número de las identificaciones de ADN aumente significativamente durante las etapas finales del proceso.

Nuevamente, esto demuestra la importancia de la esfera forense en ayudar a la identificación de individuos lo que ayudó a otorgarles un cierre al proceso de duelo experimentado por sus seres amados.

Huellas dactilares

En las investigaciones de delitos la evidencia de las huellas dactilares se ha vuelto un área de extrema importancia. Dado que las huellas dactilares son únicas en cada individuo y no cambian a lo largo de la vida, resultan extremadamente útiles en confirmar o descartar la identidad de un individuo. Se han usado para la identificación por más de un siglo y debido a los avances en la tecnología se han automatizado (esto, la biometría). Son una fuente de identificación exitosa por una cantidad de razones que incluyen “la facilidad inherente de la adquisición, las numerosas fuentes (diez dedos) disponibles para la recolección, y su uso establecido por las fuerzas de seguridad e inmigración (Subcomité de Biometría del NSTC: 2006 : 1)

Además, las huellas dactilares pueden ser recogidas en una escena del delito y tienen el potencial de vincular una serie de delitos y/o ubicar a un individuo en la escena. Son también muy útiles en la Identificación de Víctimas en desastres (DVI, por sus siglas en inglés) en los que las víctimas pueden ser identificados luego de una catástrofe como un terremoto o un bombardeo.

INTERPOL maneja una base de datos que contiene más de 146. registros de huellas dactilares y más de 3500 marcas de escenas de delitos. Los individuos autorizados de los países miembros pueden acceder a la red global de comunicaciones policiales I-24/7 para ver, enviar o verificar registros vía el sistema automático de identificación de huellas dactilares AFIS.

Las huellas dactilares pueden ser tomadas por los funcionarios de seguridad usando un aparato electrónico, o de forma manual usando tinta y papel, registro que es luego escaneado y almacenado en el formato apropiado.

DNA – ácido desoxirribonucleico

Al igual que las huellas dactilares, el ADN es extremadamente vital para las investigaciones del delito. Estas moléculas contienen la información que todas las células vivientes en el cuerpo humano necesitan para funcionar. Con la excepción de los gemelos idénticos, el ADN es único en cada individuo por lo que, al igual que las huellas dactilares, es muy útil para reconocer la identidad de una víctima en un desastre y en la resolución de delitos.

El primer paso para obtener perfiles de ADN es la recolección de muestras de la escena del delito y muestras de referencia de los sospechosos. Normalmente, las muestras se obtienen de la sangre, el pelo y los fluidos corporales. Usando métodos científicos forenses, la muestra se analiza para crear un perfil de ADN que puede ser comparado frente a otros perfiles de ADN dentro de una base de datos. Esto crea la posibilidad de que se encuentren coincidencias, coincidencias con otra persona, coincidencias con una persona en la escena, o coincidencias entre la escena del delito y otro delito.

La base de datos automatizada de ADN de INTERPOL hace posible que las policías de los países miembros puedan enviar un perfil de ADN de infractores, escenas del crimen, personas extraviadas y cuerpos no identificados. Esta base de datos se llama “DNA Gateway” (puerta de acceso de ADN) y fue creada en 2002 con un sólo perfil de ADN. Los países miembros pueden acceder a la base de datos a través del sistema de comunicación policial global I-24/7.

INTERPOL sólo actúa como el conducto para compartir y comparar información. No mantiene ningún dato nominal relacionado con el perfil de ADN de ningún individuo. Un perfil de ADN es un código numérico basado en el patrón de ADN del individuo, este código numérico puede ser usado para diferenciar individuos.

La unidad de huellas dactilares de INTERPOL

INTERPOL posee una larga historia con las huellas dactilares, y el uso de huellas dactilares para identificar fugitivos se remonta a los primeros días de la Organización. En la Unidad trabajan hoy 7 expertos de Francia, el Reino Unido y Portugal y se busca ampliar el personal a medida que crezca el volumen de trabajo. El personal es responsable de asegurar que todas las búsquedas se realicen de forma oportuna y que AFIS responda a las necesidades de la Organización. El personal también organiza y asiste a conferencias y grupos de trabajo en todo el mundo para promover el uso de los servicios AFIS de INTERPOL. La mayor parte del trabajo procesado son pedidos de impresiones de los diez dedos, sin embargo estamos viendo un aumento en la búsqueda de marcas de escenas del delito, y ya hemos tenido algunos resultados exitosos en este respecto.

Estadísticas (2011)

Nos gustaría compartir con ustedes algunas estadísticas de este año (de enero a septiembre) que le darán a lector una idea rápida del volumen de trabajo y del modo en que el servicio AFIS se viene desarrollando.

Tamaño total de la base de datos – 146.000

Huellas dactilares agregadas – 30.500

Búsqueda de huellas dactilares exclusivamente - 950

Identificaciones - 1615

En 2010 la UNIDAD realizó 958 Identificaciones e insertó 16.000 huellas dactilares. Esto demuestra que al agregar más datos somos capaces de devolver más resultados positivos a los países miembros.

AFIS – Sistema automatizado de identificación de huellas dactilares

La identificación automatizada de huellas dactilares es el proceso de hacer coincidir automáticamente una o muchas huellas dactilares desconocidas frente a una base de datos de impresiones conocidas y desconocidas.

INTERPOL administra una base de datos AFIS a la que los individuos autorizados de los países miembros pueden acceder. Los datos de huellas dactilares, ya sea los formularios de diez impresiones o marcas de escenas del delito son recibidas en la Unidad de huellas dactilares enviadas por los países miembros de INTERPOL. La Unidad de huellas dactilares utiliza un AFIS que ha sido desarrollado y es mantenido por SAGEM. Actualmente la base de datos contienen 146.000 registros de huellas dactilares y 3500 marcas de escenas del delito. Los funcionarios alrededor del mundo tomarán las huellas de un sospechoso y los datos serán luego remitidos a INTERPOL, donde serán cargados a la base de datos. Los registros son guardados e intercambiados en el formato establecido por el NIST. Los usuarios autorizados de los países miembros pueden ver, enviar y verificar información usando la red I-24/7, la red segura de comunicaciones policiales globales de INTERPOL.

La Unidad de huellas dactilares de INTERPOL alienta activamente a los países miembros a usar la base de datos en la mayor medida posible y a incrementar el número de huellas dactilares relevantes en el sistema. Es altamente recomendable que todas las huellas dactilares de extranjeros arrestados o de sujetos de la misma nación sospechados de delitos transnacionales, y marcas de escenas de delitos no resueltos sean enviadas a la Unidad de huellas dactilares.

Transmisión de Datos

Dada su naturaleza, la Unidad de huellas dactilares de INTERPOL recibe huellas de todas partes del mundo. Hasta 1999 todos los archivos de huellas dactilares se recibían en formato de papel, y estos formularios eran luego cortados y pegados en una tarjeta diseñada por INTERPOL. Esta tarjeta funcionaba bien, sin embargo llevaba mucho tiempo y dejaba margen de error cuando la huella dactilar recibida no era pegada en la posición correcta en el formulario. Un grupo de trabajo europeo decidió desarrollar un formulario que pudiera ser utilizado por los países miembros para intercambiar huellas dactilares internacionalmente. Luego de un periodo de 18 meses, expertos de varios países europeos crearon el formulario de transmisión de huellas dactilares de INTERPOL para los países europeos, más tarde este formulario fue presentado en una asamblea general y fue aceptado como el estándar para el intercambio de huellas dactilares a través de INTERPOL.

El formulario fue utilizado con éxito limitado por parte de los países miembros, varios países

europeos lo adoptaron como su formulario estándar nacional. Sin embargo, debido al número limitado de países utilizando este formulario, la Unidad de huellas dactilares de INTERPOL seguía enfrentándose al hecho de tener que procesar muchos tipos diferentes de formularios. El grupo de trabajo no se dio por vencido y con más países utilizando AFIS de modo creciente, decidió crear una versión electrónica del formulario en el formato ANSI/NIST. Aprovechando el trabajo previo realizado en este respecto por el Reino Unido, el grupo de trabajo observó cada parte del formulario y le otorgó el número correspondiente al archivo de NIST. Este formulario fue presentado en la Asamblea General en India y los delegados votaron de manera unánime el uso de este formulario para el intercambio de registros de huellas dactilares. Este formulario ha existido durante 12 años y se ha vuelto el formulario reconocido para la transmisión internacional de huellas dactilares. La implementación de INTERPOL es ampliamente utilizada por los países miembros y también recibe el apoyo de los líderes de la industria en AFIS.

¿Qué enviar?

Todos los países miembros están invitados a enviar la siguiente información a la base de datos para ser investigados y comparados.

- b. Huellas dactilares de extranjeros arrestados
- c. Huellas dactilares de ciudadanos nacionales sospechados de estar involucrados en el delito internacional.
- d. Marcas de escenas de delitos no resueltos.

INTERPOL cree que si los países miembros envían los datos arriba listados a AFIS para ser investigados y almacenados, esto ayudará a identificar a fugitivos internacionales, resolver crímenes y logrando que los países miembros vuelvan sus países más seguros. Algunos ejemplos de éxito que hemos observado en países que enviaron datos se explican brevemente a continuación.

Historias de éxito de las huellas dactilares

La importancia de intercambiar datos forenses, tales como huellas dactilares se comprueba regularmente aquí en INTERPOL. Por ejemplo en un periodo de una semana (28 de julio) se produjeron seis coincidencias.

Estas incluyeron huellas dactilares que fueran enviadas desde Colombia para su identificación. Fueron comparadas con las huellas en la base de datos y produjeron una coincidencia con una serie de impresiones en AFIS de Portugal donde el individuo había cometido una violación; las impresiones estaban bajo distintos nombres.

Una segunda coincidencia se produjo entre huellas dactilares recibidas de Los Países Bajos por tráfico de drogas, que coincidieron con impresiones en AFIS recibidas de Portugal por robo.

Otra coincidencia incluyó huellas dactilares recibidas desde Mónaco por robo. Fueron ingresadas a la base de datos de AFIS y coincidieron con un conjunto de impresiones recibidas de Austria por robo.

Otro ejemplo de éxito en el intercambio de datos biométricos tuvo lugar en 2008. Un individuo fue arrestado en Brasil bajo el cargo de comportamiento amenazante. Había cumplido con una sentencia previa por daño físico severo y estaba bajo investigación por pedofilia. Las huellas dactilares del sospechoso fueron enviadas a INTERPOL por las autoridades brasileras, y se realizó una búsqueda en AFIS lo cual otorgó una identificación positiva. Las huellas dactilares coincidieron con un registro bajo otro nombre, un alias. En esa ocasión había sido arrestado por intentar cruzar ilegalmente la frontera entre Bielorusia y Polonia utilizando un documento falsificado.

Áreas para mejorar

INTERPOL posee 188 países miembros que pueden utilizar esta base de datos central para al almacenamiento y búsqueda de personas, pero no todos los países miembros aprovechan esta posibilidad. Esta es un área en la que necesitamos ver una mejora ya que la Organización cree que sólo si esta base de datos se puebla y se utiliza, descubriremos su potencial completo. La Unidad contacta constantemente a los países miembros para explicarles la utilidad de AFIS y cómo con esta vía en funcionamiento pueden obtener altos beneficios del uso de AFIS. En 2012 lanzaremos un proyecto para apuntar a 6 países de los cuales creemos que con un poco más de información de INTERPOL y ayuda en el intercambio de datos poblarán AFIS.

MorphoEVA, visor del NIST

La Unidad trata constantemente mejorar la calidad de los datos de huellas dactilares enviados a su AFIS y también entre los países miembros. Notamos que uno 20% de estos archivos son de una muy pobre calidad y son escaneados con una baja resolución y sin escalas. INTERPOL trabajando con Morpho, un comercializador de AFIS, ha desarrollado un proyecto para proveer a los países miembros de hardware y software que hará posible que el país escanee un formulario de huella dactilar, y cree un archivo del NIST para su transmisión a INTERPOL AFIS. Además de permitir el envío de archivos de NIST, INTERPOL ofrece un software sin cargo para sus usuarios para ver los archivos del NIST.

El portal de acceso AFIS

El proyecto más importante de la Unidad de huellas dactilares en 2011 y 2012 fue el desarrollo de una herramienta que le permita a AFIS recibir y enviar respuestas automáticas a los países miembros.

Esta herramienta será desarrollada por la firma 3M Cogent, basándose en especificaciones escritas por la Unidad de huellas dactilares y el servicio de tecnología de INTERPOL, el puerto de acceso interactuará con las bases de datos de historias de casos de INTERPOL, lo que les permitirá a los países miembros recibir información valiosa relacionada con coincidencias encontradas en el sistema AFIS. Cuando este puerto de acceso entre en operaciones se estima que el 80% de todas las solicitudes a AFIS estarán automatizadas y los países miembros recibirán una respuesta a su pedido en minutos, la capacidad de procesamiento de este servicio también

será incrementado para permitir volúmenes más altos de comparaciones por parte de nuestros países miembros. Se espera tener este servicio funcionando a mediados de junio de 2012, el desarrollo ya ha comenzado y pronto se iniciará el testeo del servicio. Este servicio constituirá una gran mejora para la Unidad al permitir un alto volumen de respuestas rápidas a los países miembros, esto alentará a los países miembros a enviar más solicitudes.

Las huellas dactilares en el control fronterizo

INTERPOL observa una necesidad creciente de control de personas en los cruces fronterizos; esto se realiza verificando el pasaporte frente a una base de datos de pasaportes robados o perdidos. Creemos que si también se realiza la verificación de las huellas dactilares de la persona frente a una lista de personas a observar, esto dará como resultado un modo más seguro y completo de controlar los cruces de frontera. (entrada y salida). Observando el ejemplo de un país miembro que añadió la búsqueda de huellas dactilares contra una lista nacional de personas non grata en ese país, se vio que en la primera semana se le impidió la entrada a 50 personas. En todos estos casos, las personas tenían documentos de viaje genuinos bajo identidades asumidas.

El sueño de la Unidad de huellas dactilares de INTERPOL

Los autores creen que hay un gran futuro para la Unidad de huellas dactilares de INTERPOL y para el uso de las huellas dactilares en general, en todo el mundo. Para asegurarse que esto suceda es vital que las oficinas de huellas dactilares de los países miembros pueblen e investiguen el sistema AFIS central de INTERPOL con datos que tengan relevancia para otros Estados miembros. Creemos que los fugitivos, los delitos no resueltos y la entrada y salida de personas pueden ser controlados si esta base de datos y este intercambio de datos se incrementan. El ámbito en el que la Unidad de huellas dactilares realmente desea ver una mejora es en la calidad de la transmisión de las huellas dactilares, y con esto en mente, ha puesto en funcionamiento un proyecto piloto para apuntar a seis países. A partir del resultado obtenido en estos países veremos cómo podemos continuar con todos los países miembros. **Algo importante para tener siempre presente es que la base de datos AFIS no es la base de datos de la Unidad de huellas dactilares de INTERPOL, es la base de datos de todos los países miembros, y ellos son responsables de poblarla y usarla.** La Unidad de huellas dactilares de INTERPOL sólo puede alentar a los países miembros a usarla.

Conclusión

Esperamos que luego de leer este documento el lector tenga una idea del trabajo realizado por la Unidad de huellas dactilares de INTERPOL y entienda por qué es importante que exista este servicio, y por qué es necesario utilizarlo.

INTERPOL apoya completamente el intercambio de datos forenses entre los países miembros ya sea de modo bilateral o a través de diversos servicios regionales, en conclusión INTERPOL AFIS es una de muchas posibilidades, sin embargo es una posibilidad que debería ser utilizada siempre.

Los registros dentales: su importancia en la identificación

Virginia Kannemann



Virginia Kannemann

Asistente Ejecutiva. Oficina Nacional de Tecnologías de Información



Odontóloga egresada de la Universidad Argentina John F. Kennedy de Buenos Aires. Expositora del V Congreso Internacional de Biometría de la República Argentina, e integrante del workshop del estándar ANSI/NIST-ITL 1-2011 en Maryland, USA. Coordina el grupo para el desarrollo de la estandarización de los registros dentales de dicho estándar.

Actualmente realizando el curso de Odontología Forense en el Instituto Universitario de la PFA (IUPFA).

Información de contacto: *VKannemann@jefatura.gob.ar*

Resumen

La identificación humana es un proceso que compromete el accionar de muchas ciencias. Los medios más comunes de identificación son los reconocimientos visuales, realizado por parientes o conocidos y la dactiloscopia. Sin embargo, cuando los cuerpos se hallan carbonizados, en un alto grado de descomposición o esqueletizados, ambos métodos son limitados. La Odontología se destaca como una ciencia plenamente capacitada para ofrecer datos en la identificación de cuerpos, pues no solo el aparato estomatognártico¹, sino también el cráneo pueden ofrecer elementos valiosos para la identificación.

La odontología forense es el área dentro de la odontología que tiene como misión auxiliar a la administración de la justicia determinando a través del estudio del aparato estomatognártico, la mayor cantidad de información posible sobre las características físicas, edad, género, hábitos, posición socioeconómica, raza, origen geográfico y actividades del individuo o individuos en cuestión. Con esto la aplicación de la odontología se constituye en auxilio del derecho estudiando la resolución de problemas jurídicos mediante la aplicación de los conocimientos odontológicos, ya sea de los fueros civil, penal o laboral.

Palabras clave: odontología forense, identificación.

¹ Se denomina “sistema estomatognártico” a la integración anatómica y funcional de los componentes de la cavidad bucal, con elementos dentarios y articulares, como la articulación temporo-mandibular y los músculos paraprotéticos. Integrado por: labios, mejillas, lengua, paladar, piezas dentarias, periodonto de protección, glándulas salivales y huesos maxilares.

Los registros dentales: su importancia en la identificación

Introducción

La identificación de los individuos reúne diversas áreas del conocimiento, tales como la medicina, la antropología, la biología molecular y la odontología. Cuando la misma es realizada por las condiciones y caracteres específicos de los elementos dentales se torna imprescindible, pues los dientes y sus restauraciones son resistentes al fuego y a otras alteraciones que pueden acontecer después de la muerte del individuo constituyendo, algunas veces, los únicos elementos con los cuales cuenta el perito. Es de mucha importancia que, para que el proceso de identificación por los dientes sea efectivo, exista una buena documentación del tratamiento realizado en cada paciente. Los registros de los tratamientos ejecutados deben ser realizados de forma estandarizada y con un nomenclador universal para que los mismos puedan ser utilizados y entendidos por todo aquel que lo necesite.^(I)

En virtud de lo mencionado anteriormente, es que la Argentina mediante la Oficina Nacional de Tecnologías de Información (ONTI)² ha propuesto incluir la información biométrica que se obtiene del mencionado sistema a fin de que al realizar los intercambios de datos de los registros dentales todos hablen el mismo idioma. Dicha propuesta fue considerada por el canvasse del National Institute of Standards and Technologies (NIST)³ y por unanimidad se aprobó la inclusión de los registros dentales dentro del documento de Estándares para el intercambio de datos biométricos.

Liderando el grupo para el desarrollo de los “Registros Dentales” la Dirección Nacional de la ONTI se encuentra actualmente trabajando para la definición del mismo.

Reseña histórica

Desde tiempos pasados, se han utilizado los conocimientos odontológicos para la resolución de casos identificativos que por otros medios no podrían llevarse a cabo, ya sea por el alto grado de descomposición, por tratarse de catástrofes en masa o por el hecho de ser irreconocibles debido a la acción del fuego o si ha pasado mucho tiempo de la muerte y solo se encuentran restos óseos.

Quien fuera considerado el padre de la odontología forense, el Dr. Oscar Amoedo y Valdez, identificó 40 cadáveres víctimas de un incendio en el bazar de la caridad en París, en el que fallecieron 126 personas en el año 1897.^(II)

² Oficina Nacional de Tecnologías de Información (ONTI): Oficina Nacional que depende de la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros, tiene entre sus funciones la implementación de las estrategias de innovación informática en la administración pública. Desarrollar sistemas que son utilizados en procedimientos de gestión, fijar los estándares a utilizar en los organismos públicos al incorporar nuevas tecnologías, colabora con otras dependencias en la creación de portales informativos y promueve la interoperabilidad de las redes de información de las instituciones estatales. <http://www.igm.gov.ar/sgp/paginas.dhtml?pagina=27>

³ National Institute of Standards and Technologies (NIST): agencia federal no reguladora dentro del Departamento de Comercio de los Estados Unidos. Su misión consiste en promover la innovación del Estado y la competitividad industrial mediante la mejora de la dimensión de las ciencias, los estándares y la tecnología en forma que mejoren la seguridad económica y la calidad de vida. http://www.nist.gov/public_affairs/general_information.cfm

Sin embargo, la primera víctima identificada por la dentadura se remonta al año 69 AC, cuando Agripina, madre de Nerón, identificó a la amante de su marido por unas características de la cavidad bucal.^(III)

En el año 1905, Guillermo Beckert Frambauer, segundo secretario de la delegación Alemana en Santiago de Chile, asesinó a Ezequiel Tapia, el cual era portero del edificio donde habitaba. Luego de apuñalarlo, fracturarle el frontal y la base del cráneo, provocó un incendio en la delegación. El cuerpo carbonizado fue identificado por el Dr. Germán Valenzuela Basterrica por la comparación de los restos con la historia clínica dental de las prácticas odontológicas realizadas a Ezequiel Tapia en el ejército.^(IV)

Víctimas del atentado a la sede de la Asociación de Mutuales Israelitas Argentinas (AMIA) en julio del año 1994 fueron reconocidas por sus fichas odontológicas, así como 39 víctimas del accidente de la aeronave de la empresa LAPA en agosto del año 1999.^{(V)(VI)}

La identificación de Ernesto "Che" Guevara en el año 1997 se realizó con el método odontológico mediante la comparación de la ficha odontológica ante mortem que enviaron desde Argentina a los antropólogos y odontólogos cubanos que dirigían las excavaciones, y el estudio de los restos hallados. Una amalgama y la particular disposición de las piezas dentales, desde el punto de vista odontológico, y la presencia de un mega seno frontal, fueron los puntos de coincidencia que determinaron la identificación positiva treinta años después de su muerte.

Estructuras que determinan la identificación

Las medidas que resultan de los distintos puntos y planos antropométricos, las disposiciones que adoptan las piezas dentarias, el momento evolutivo en el que se encuentran, las particulares morfológicas y las restauraciones realizadas a lo largo de la vida, nos dan indicios de: sexo, raza, hábitos, enfermedades, edad posición económica e incluso individualidad.

Se dará un breve detalle de cada una de ellas.

A. Medidas antropométricas

Las relaciones del estudio antropológico de los maxilares superior e inferior y del cráneo en general, junto con las medidas y morfología dental, permite mediante mediciones y una serie de fórmulas e índices obtener la identificación de los individuos.

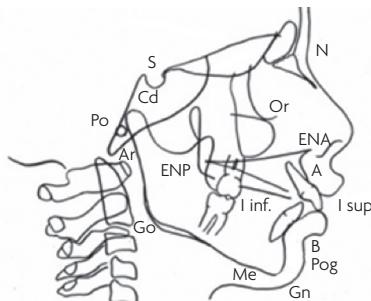


Fig. 1. Puntos cefalométricos utilizados para realizar las mediciones de los huesos craneales y maxilares.

Un ejemplo de esa relación es el índice dentario de Flower, utilizado para la determinación de la raza. El mismo corresponde a la relación que existe entre el largo dentario⁴ y la línea nasión-basión.⁵

La fórmula utilizada es: Índice dentario= (largo dentario/línea nasión-basión) x 100

El resultado de la misma puede variar entre los siguientes valores, que pertenecen a los grupos raciales más importantes:

- Microdontes: < 42 Raza caucasoide
- Mesodontes: 42-44 Razas mongoloide o amarilla
- Macrodontes: > 44 Razas negras y australianas

B. Piezas dentarias

Las piezas dentarias son las estructuras más duras del organismo. El tejido que los cubre, el esmalte, está formado por 5 a 12 millones de cristales del mineral hidroxiapatita ($\text{Ca}_{10}(\text{PO}_4)_6(\text{OH})_2$), con un 94% de sustancia inorgánica, 1,5% de sustancia orgánica y 4,5% de agua. Dichos cristales, están organizados en prismas y se disponen en forma oblicua y en dirección ondulada dándole resistencia a las fuerzas de la masticación que pueden llegar a 45 kg por m^2 .

El patrón dental es único en cada individuo y las fórmulas dentarias son:

Dentición temporaria o primaria:⁶ compuesta de 20 piezas dentales divididas en 3 grupos: incisivos (centrales (CI) y laterales (CL)), caninos (C) y molares (M).

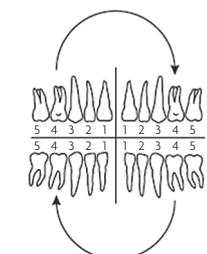


Fig. 2: Fórmula dentaria para la dentición temporaria o primaria

Dentición permanente:⁷ compuesta de 32 piezas dentarias divididas en 4 grupos: incisivos (centrales (IC) y laterales (IL)), caninos (C), premolares (PM) y molares (M).

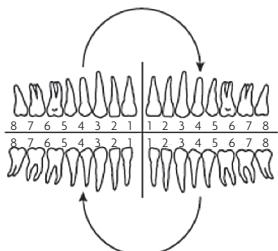


Fig. 3: Formula dentaria para la dentición permanente

⁴ Largo dentario: línea recta desde la cara mesial del primer premolar hasta la cara distal del tercer molar.

⁵ Línea nasión-basión: línea recta que va desde la raíz de la nariz (unión de huesos propios con frontal) hasta el punto más basilar de la apófisis basilar del esfenoides (hueso de la parte media de la base de cráneo).

⁶ Se considera dentición temporal a la primera dentición la cual comienza su periodo de erupción a partir de los 6 meses de vida extrauterina hasta completarse alrededor de los 2 años.

⁷ Se considera dentición permanente a la segunda dentición, que comienza con la erupción de los primeros molares permanentes.

Cada pieza dental tiene 5 caras visibles ⁸: mesial, distal, oclusal o incisal, vestibular, lingual o palatina, por lo que se puede encontrar innumerables combinaciones posibles, dados por: caries, restauraciones, piezas ausentes, anomalías de posición, de forma, de número, etc.

Con el objeto de utilizar un nomenclador unificado y reconocido internacionalmente, los odontólogos en la República Argentina utilizan el aprobado por la FDI⁹ e Interpol¹⁰, denominado Sistema Dígito Dos. El mismo consiste en dividir cada maxilar en dos hemiarcadas que se numeran de derecha a izquierda desde el número 1 al número 4, quedando un total de 4 hemiarcadas. Cada hemiarcada está compuesta por 8 piezas dentales que se numeran desde la línea media hacia el tercer molar. Siendo el 1C el número 1 y el tercer molar el 8. Esta numeración correspondería a la dentición permanente.

Ej.: Incisivo Central Superior Derecho: 1.1 Para la dentición temporaria la numeración de los hemimaxilares comienza en el 5 hasta el 8 de derecha a izquierda. La numeración de las piezas dentarias va del 1 al 5, también desde el incisivo central.

Ej: Incisivo Central Superior Derecho: 5.1, donde el primer número corresponde a la hemiarcada superior derecha y el segundo número al incisivo central.

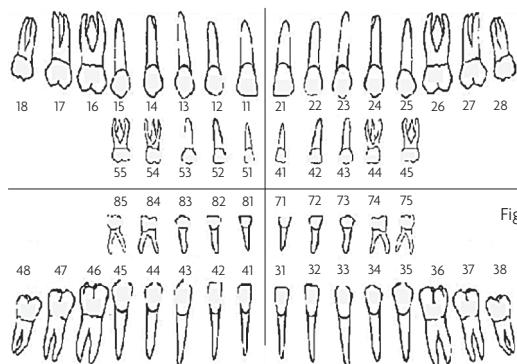


Fig. 4: Odontograma utilizando sistema dígito dos

Al encontrarse protegidas por estructuras óseas y mucosas, como el cráneo, los maxilares, músculos, aponeurosis; la cavidad bucal en su conjunto, por hallarse en un medio húmedo y por su alto contenido de materia inorgánica son capaces de soportar hasta 1000 grados de temperatura, por lo que es el método ideal de identificación en casos de calcinaciones y grandes catástrofes.

Al ser sometidos a la acción del fuego, se pueden observar distintos estados, tales como:

- Presentarse intactos (hasta 100° C)
- Presentarse quemados (cambio de color en la superficie entre los 150° C hasta 270° C)
- Presentarse estallados o carbonizados (reducido a carbón por combustión incompleta entre 300° C y 1100° C)
- Presentarse incinerados (reducido a cenizas temperaturas mayores de 1100°C) ^(VII)

⁸ Todas las caras cercanas a la línea media se denominan mesial, y sus opuestas se denominan distal. Las caras cortantes se denominan borde incisal en incisivos y oclusales en premolares y molares. Los caninos tienen 2 vertientes (una mesial y otra distal) pero se la considera como bordes incisales. Las caras que se orientan al vestíbulo de la boca, hacia afuera, se denominan vestibulares y las que se orientan hacia el interior, dependiendo si son del maxilar superior, caras palatinas, próximas al paladar y si son del maxilar inferior, caras lingüales, próximas hacia la lengua.

⁹ Federación Dental Internacional (FDI): es una organización compuesta por más de 200 miembros de asociaciones nacionales y grupos de especialistas que representan a más de un millón de odontólogos en el mundo. <http://www.fdiworlddental.org/>

¹⁰ Interpol: es la mayor organización mundial de policía internacional, con 188 países miembros. Creada en 1923 con el objeto de facilitar la cooperación internacional en los pasos fronterizos, apoya y ayuda a las organizaciones, autoridades y servicios cuya misión es prevenir o combatir la delincuencia internacional. <http://www.interpol.int/public/icpo/default.asp>

Determinación de la edad

El momento evolutivo y la cronología de las piezas dentarias así como ciertas medidas antropométricas permiten determinar la edad.

Cronología dental ^(VIII)

Dentición primaria o temporalia

- Incisivos centrales inferiores: 6 meses
- Incisivos centrales superiores: 7 meses
- Incisivos laterales superiores: 8 meses
- Incisivos laterales inferiores: 9 meses
- Primer molar inferior: 12 meses
- Primer molar superior: 13 meses
- Caninos: 18 meses
- Segundos molares: 24 meses

Dentición permanente

- Primer molar permanente: 6 años
- Incisivos centrales: 7 años
- Incisivos laterales: 8 años
- Primer premolar: 9-11 años
- Segundo premolar: 11-12 años
- Segundo molar: 12 años
- Caninos: 13 años
- Terceros molares: 18-25 años

Sin embargo, debido a que puede haber ciertas variaciones, se deberá complementar con otros estudios, tales como: tablas de Carmen Nolla ¹¹, radiografía carpal ¹², mediciones del cráneo y maxilares, entre otros.

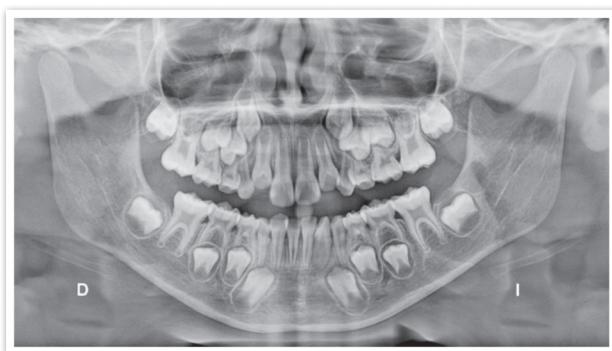


Fig. 5: Radiografía panorámica de un niño de aproximadamente 8 años de acuerdo a la cronología dental.

¹¹ Describen los distintos estadios de la formación del diente, se dividen en 10 períodos que van desde la formación de la corona, calcificación, formación de la raíz, calcificación y cierre apical. Todos tienen un momento preciso e indican la edad estimada. Se deben tomar radiografías para realizar el diagnóstico.

¹² Corresponde a la evaluación del desarrollo esquelético del cuerpo. Utilizado para evaluar la edad esquelética y el potencial de crecimiento.

Para determinar la edad en los adultos, una vez que ha pasado el periodo de erupción de las piezas dentarias se suele utilizar el análisis de Gusftason. El mismo consiste en el estudio de 6 características presentes en la edad adulta, a las cuales el autor a numerado del 0 al 3, donde el 0 es ausencia de los mismos y 3 es el estado avanzado.

El siguiente cuadro refleja las características con sus escalas respectivas:

	0	1	2	3
Atricción (A)	Ausencia	Afecta esmalte	Afecta dentina	Afecta pulpa
Periodontitis (P)	Ausencia	Comienza periodontitis	Afecta primer 1/3 de raíz	Afecta más de 2/3 de raíz
Dentina secundaria (D)	Ausencia	Formación en la parte superior de la cavidad pulpar	Cavidad pulpar ocupada hasta la mitad	Cavidad pulpar ocupada completamente
Aposición del cemento (C)	Ausencia	Aposición algo mayor a lo normal	Gran capa de cemento	La capa de cemento es de gran consistencia
Reabsorción de Raíz (R)	Ausencia	Reabsorción en pequeños grupos aislados	Mayor cantidad de perdida de sustancia	Cemento y dentina afectados
Transparencia de raíz (T)	Ausencia	Se nota la transparencia de la raíz	Supera el tercio apical	Supera los dos tercios de la raíz

La suma de los puntos y el ordenamiento en un eje cartesiano, permite realizar una estimación de la edad.

Determinación del sexo

Las piezas dentales poseen ciertas características que al relacionarse con los huesos maxilares y craneales, pueden ayudar a la determinación del sexo. Se nombran en los siguientes cuadros algunas de ellas.

Piezas dentarias	Masculino	Femenino
Diámetro M-D incisivos	Desproporcionados y desalineados	Uniformes y alineados
Ángulos	Robustos y cuadrangulares	Delicados y redondeados
Color	Más oscuros	Más claros
Tamaño	Grandes	Pequeños

Mandíbula	Masculino	Femenino
Peso medio	80g	63g
Angulo goníaco	<125°	>125°
Sínfisis mentoniana	Más alta	Más baja
Tamaño	mayor	menor
Cóndilos	mayor	menor
Inserciones musculares	Más marcadas	Menos marcadas
Anchura bicondilea	125mm	<105mm
Paladar	Ancho y poco profundo	Estrecho y profundo
Arcada dentaria	Gruesa	Fina y delicada

Determinación de la talla

El cálculo de la talla a partir de las dimensiones de las piezas dentarias se relaciona con la proporcionalidad de los dientes con la altura del individuo, relacionando las medidas dentarias con las del esqueleto óseo.

Uno de los métodos utilizados es el propuesto por el Dr. Ubaldo Carrea quien comprobó que la suma de los milímetros de las distancias mesiodistales de un incisivo central, un incisivo lateral y un canino del arco inferior, constituye un arco de circunferencia, la cuerda de ese arco es la medida fundamental del diagrama dental, el cual el autor ha denominado “radio-cuerda inferior”^(IX)

De ahí que se considera que la talla humana se encuentra entre dos medidas una máxima proporcional al arco y una mínima proporcional al radio cuerda.

La fórmula matemática utilizada es la siguiente:

$$\text{Talla máxima (cm)} = (\text{arco} \times 6 \times 10 \times 3,1416) / 2$$

$$\text{Talla mínima (cm)} = (\text{radio-cuerda} \times 6 \times 10 \times 3,1416) / 2$$

$$\text{Radio-cuerda} = \text{arco} \times 0,954$$

El hombre se acerca más a la talla máxima en cambio la mujer se acerca más a la talla mínima.

C. Rugas palatinas

Las rugas palatinas son elevaciones de la mucosa palatina ubicadas en el paladar anterior, inmediatamente detrás de las piezas dentales anterosuperiores y a ambos lados de la línea media.

En cantidad de 3 a 5, adoptan diferentes disposiciones las cuales son únicas en cada individuo incluso en gemelos homocigotos. Desde su desarrollo en la 3ra semana de vida intrauterina, son perennes, inmutables e invariables durante el tránscurso de la vida. Aunque sufran alguna alteración por lesiones, se regeneran según su patrón original.

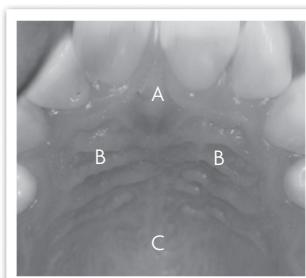


Fig. 6. Detalle de rugosidades o rugas palatinas: A) papila inter incisiva, B) Rugas palatinas, C) Línea media o rafe medio

Son valiosas y aceptadas en la identificación dada su perennidad e invariabilidad, su unicidad y por encontrarse protegidas de las agresiones externas, de la descomposición y de la incineración. Al igual que las huellas dactilares, permiten, por cotejo de muestras, obtener la identidad del individuo.^(X)

Debido a las diversas disposiciones que adoptan, su tamaño, forma y número, las mismas son pláciles de clasificación. Existiendo varias clasificaciones de diversos autores.

El estudio de las rugas palatinas se denomina rugoscopía. El estudio del paladar en todo su conjunto (rafe medio, papila inter incisiva y rugas palatinas) se denomina palatoscopía.

D. Huellas labiales

Las huellas labiales son las impresiones de los pliegues, fisuras y surcos de la cara mucosa de los labios y las cuales pueden encontrarse en superficies más o menos lisas cuando estos se encuentran cubiertos de maquillaje haciéndolas visibles, o latentes cuando están cubiertas de saliva. Su importancia trasciende la impresión física, siendo estas fuentes de material genético. De todos los indicios que se pueden ubicar en la escena de un crimen, las huellas corporales en general son las más comunes y entre ellas las huellas labiales, las cuales se pueden encontrar en una colilla de cigarrillo, en un vaso, incluso en una huella de mordedura por la presencia de saliva. ^(x)

Su estudio no solo considera el patrón de la semimucosa labial, sino también su grosor, la dirección de las comisuras y las huellas labiales, de las cuales existen muchas clasificaciones que no se tocarán en este artículo.

Entre sus características, lo cual las hacen importantes en la identificación, es que son: perennes, inmutables, invariables, únicas para cada individuo salvo en gemelos homocigotos, caso en el que suelen ser similares a alguno de los padres.

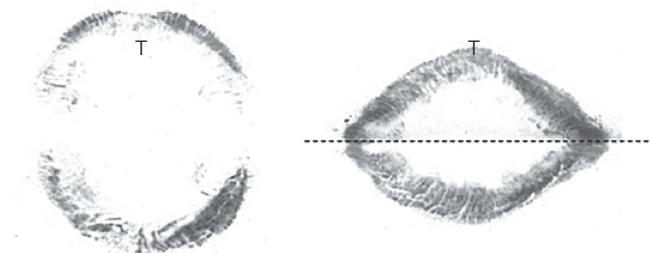


Fig. 7: Ejemplo de impresión labial. Nótese los surcos marcados y la dirección de las comisuras.

E. ADN extraído de la pulpa dental

Todas las características identificativas de los individuos se encuentran en el código genético. El ADN, soporte del código genético, se encuentra en el núcleo de todas las células del organismo, aunque también se encuentra ADN en las mitocondrias (ADN mitocondrial) con características y utilidades forenses distintas a la nuclear.

El genoma humano está formado por 6000 millones de pares de bases distribuidas en 23 pares de cromosomas, en dos cadenas superenrolladas, una perteneciente a la línea materna y la otra a la línea paterna conteniendo las características hereditarias que hacen único a los individuos paro unidos a sus familiares.

Habitualmente el estudio de ADN se realiza en muestras de saliva, semen y cabello con bulbo capilar. Sin embargo, el diente es una fuente confiable de ADN por encontrarse protegido del medio ambiente y de las agresiones ambientales como ya se ha explicado en el presente artículo. Dado que la pulpa dental, tejido blando del interior del diente, contiene diferentes tipos de células, tales como: fibroblastos, células madres de la pulpa dental, macrófagos, odontoblastos, células sanguíneas, células nerviosas periféricas, entre otras, se puede obtener la cantidad necesaria para realizar un estudio de ADN. La cantidad de celular y la así como la cámara pulpar

decrecen con la edad. No todas las piezas dentarias contienen la misma cantidad de pulpa dental, dependiendo de ello un diente puede rendir 15 a 20 microgramos de ADN.^(X)

Se contemplan básicamente dos métodos de extracción del ADN de la pulpa dental: la pulverización total del diente y la sección transversal u horizontal de la pieza dental.^(XI)

Estudio de las mordeduras

Las huellas de mordeduras son las impresiones de las piezas dentarias sobre diferentes sustratos capaces de deformarse. Esta deformación permite que las características de las piezas dentarias sean transferidas a la superficie.

Cada diente deja una huella característica, tales como:

- Incisivos: rectángulos elongados
- Canino superior: triángulo ancho
- Canino inferior: triángulo angosto
- Premolares superiores: triángulos dobles
- Premolares inferiores: triángulos simples
- Molares: no suelen ser frecuentes, pero al encontrarse se ven como rectángulos anchos.

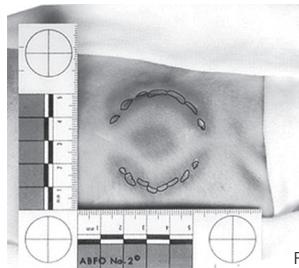


Fig. 8: Huella de mordedura

Es un método de gran utilidad en criminalística, dado que los dientes pueden ser utilizados como armas de defensa o ataque. Dichas marcas suelen encontrarse en delitos de naturaleza sexual, abuso de menores o riñas.

Las mismas pueden ser fuente de ADN también, dado que en las mismas se puede encontrar saliva y/o sangre del atacante.

De estas huellas se puede determinar la especie, si son realizadas por defensa o ataque, de acuerdo al lugar donde hayan sido producidas se puede determinar el tipo de delito, se puede identificar si las huellas fueron realizadas por terceros o por sí mismos, orientan a la investigación, se puede asociar a un sospechoso en el crimen, junto con la valoración psicológica se puede construir el perfil psicológico del agresor.

Conclusión

Como se ha visto, los registros dentales y el sistema estomatognático en su conjunto, pueden brindar información para identificar a las personas. Dicho método es útil cuando la identificación por otros medios no es posible y en este sentido, la función del odontólogo forense se torna

imprescindible cuando se disponen de datos parciales producidos por catástrofes o cuando se encuentran cuerpos esqueletizados y no tenemos otro dato más que el ADN que se pueda obtener de los huesos y el registro de las piezas dentales.

En estos años se ha dado importancia a los registros dentales para la identificación. Distintos organismos, han empezado a trabajar con el apoyo del odontólogo forense dentro de los cuerpos médicos como Interpol, desde su grupo de identificación de víctimas de desastres (DVI) en el cual utilizan la comparación dental para la identificación o desde el NIST en su interés de incluir en el estándar ANSI/NIST – ITL de intercambio de datos biométricos los registros dentales. Sin embargo, cabe aclarar que es un método que necesita registros anteriores para hacer el cotejo, lo que nos compromete como odontólogos a llevar registros claros, completos y de acuerdo a las normas y nomenclatura internacional.

Viendo la importancia de dichos registros, la ONTI en colaboración con el NIST ha comenzado a trabajar en el desarrollo de dicho estándar.

Bibliografía

- I R. F. Da Silva, De la Cruz, B.V.M, E. Daruge Jr., et al. La importancia de la documentación odontológica en la identificación humana – Relato de un caso. Acta odont. Venez, Mayo 2005, Vol. 42, Nro. 2, p. 159-164.
- II Garay Crespo MI, García Rodríguez I, Hernández Falcón L. Dr. Oscar Luis Amoedo y Valdez. Aportes a la Odontología. Rev méd electrón. 2007; 29 (5).
- III Moya Pueyo V., Roldán Garrido B. y Sánchez Sánchez J. A. Odontología Legal y Forense, Ed. Masson, 1994.
- IV Spadácio, Célio. Análisis de dos principales materiales restauradores dentales sometidos a la acción del fuego y su importancia en el proceso de identificación. 2007. <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000429262&fd=>
- V Eleta G. Odzak J., et al. Identificación en desastres de masas. Corte Suprema de Justicia de la Nación. Cuadernos de Medicina Forense. 2002. Año 1, Nº3, Pág. 167-187.
- VI Estrategia Médico Legal frente a una Catástrofe Colectiva. El Caso A.M.I.A. Editorial JR, Abril 1996, Cuerpo Médico Forense.
- VII Delattre V: Burned beyond recognition: Systematic approach to the dental identification of charred humans remains. J Forensic Sci. 2000; 45(3): 589-596.
- VIII Gómez de Ferraris, Ma. E, Campos Muñoz, A. Histología y Embriología Bucodental. Ed. Médica Panamericana. 2002. 2da Edición. Pág. 387-403.
- IX Ortigoza Ruiz, Juan Francisco. Identificación Humana y Análisis de ADN en pulpa dental. Instituto de Medicina legal de Catalunya. <http://www.odontochile.cl/trabajos/reconyadnpulpar.pdf>
- X Grimaldo-Carjevski Moses. Rugoscopía, queiloscopía, oclusografía y oclusoradiografía como métodos de identificación en odontología forense. Una revisión de la literatura. Acta Venezolana Odontológica. 2010. Volumen 48 (2). www.actaodontologica.com/ediciones/2010/2/art23.asp.
- XI González Andrade Fabricio, et al. El estudio de polimorfismo de ADN a partir de restos óseos y dientes

y sus aplicaciones en la identificación de desaparecidos. Ciencia Forense. Rev Aragonesa de Medicina Legal. 2007. (5) pág. 163-182.

Tendencias Biométricas, desafíos y oportunidades

Julio Fuoco



Julio Fuoco

Licenciado en Comercialización.



Actualmente se desempeña como Director de BITCompany, empresa que ofrece servicios de consultoría, coaching, capacitación, que van desde la definición de la estrategia de TI (debidamente alineada al negocio) hasta la implantación del gobierno y los sistemas de gestión de calidad de procesos, seguridad de la información, servicios de TI, basados en normas y buenas prácticas . También es director de ETSA Consulting, empresa especializada en management, tecnología y procesos.

Cuenta con más de 30 años de experiencia en el mercado TIC. Su desarrollo se enmarca en temas relacionados con asesoramiento y consultoría estratégica en managment y tecnología, tanto para empresas públicas, como privadas. Fundador del Grupo ETSA de Argentina (especializada en Outsourcing de TI, consultoría y Reingeniería de empresas), IDS (consultora especializada para el sector turismo) y ECU (portal de compras del mercado de consumo masivo) portal BtoB.

Expositor Internacional en Seminarios y Congresos en temas de Procesos, Tecnología y Negocios. Autor de varios artículos para revistas especializadas y portales de tecnología. En el campo docente es Director de la diplomatura de Procesos con Calidad en las TIC's y docente en varias materias de postgrado en temas relacionados con su especialidad. Fue Director del ISIPE "Instituto de Tecnología de la Universidad Siglo 21 de Córdoba" y profesor de Cátedras de Management en el IBAHRS y la Fundación de Altos estudios de Ciencias Comerciales.

Resumen

Revisaremos algunos de los factores necesarios para el éxito de un proyecto Biométrico. Ahondaremos en temas que van más allá de la tecnología, como son los procesos, las personas y la cultura. Todo esto enmarcado en un contexto donde los estándares internacionales, serán una pieza importante a tener en cuenta a la hora de planificar la solución a implantar.

Palabras clave: procesos, transformación gubernamental, estándares nacionales.

Tendencias Biométricas, desafíos y oportunidades

Introducción

En los últimos años la ubicuidad y penetración de la tecnología, la reducción de costos, el aumento de velocidad en las comunicaciones, la capacidad de almacenamiento y la alta disponibilidad de los equipos, hacen factible que pensemos en el uso de la Biometría Informática¹ como un proceso que complementa la verificación de la identidad de las personas o identificación electrónica.

En Latinoamérica los gobiernos ya han comenzado a vislumbrar un futuro donde la tecnología jugara un rol importante, como herramienta efectiva para el Gobierno Electrónico, la Inclusión Social, y los Derechos de las Personas (Carta Iberoamericana de Identificación Electrónica Social, Lisboa 2010²) y en particular, la Biometría será un eslabón que facilitara muchos de esos objetivos, ya que la biometría es al día de hoy, la tecnología más apropiada para identificar y verificar identidades con el resguardo de la identidad de las personas.

Ahora, si bien ya existe mucha experiencia por parte de las empresas de la industria de la Tecnología de la Información y Comunicaciones (en adelante TIC), los clientes gubernamentales y privados, al pensar en la implementación de distintos tipos de soluciones tecnológicas cuando hablamos de proyectos de Biometría, pueden en algunos casos aparecer nuevos paradigmas respecto de la invasión a la privacidad de cada individuo/ciudadano. Esto implica prestar mucha atención en la etapa inicial de planificación, analizando los actores que serán parte de esta implantación.

Escribiendo sobre este tema, me viene a la mente una frase, que utilizo en las reuniones de lanzamiento de proyectos con alto nivel de innovación o importantes cambios culturales: “el cementerio de los fracasos está lleno de buenas ideas mal implementadas”, es por ello que sería importante repasar que elementos se ponen en juego en la implantación de herramientas Biométricas tanto a nivel gubernamental, como privado.

Para ello, como eje del análisis me valdré de un estudio –Benchmarking– realizado por Xerox hace ya muchos años, allá por la década de los ‘80. El mismo determinó la incidencia que tenían cuatro factores; tecnología, procesos, personas y cultura (ver figura 1), en el éxito de los proyectos cuya conclusión sigue siendo válida hoy en día. Pudiendo sintetizarlo con la frase de Saint-Exupéry en el Principito, “lo esencial es invisible a los ojos”.

Allí se pone de manifiesto la incidencia o importancia real que tienen cada una de las partes de un programa de cambio a través del uso de la tecnología, donde el componente tecnológico, tiene una incidencia de solo el **quince por ciento** (15%) dentro de los factores de éxito, si bien muchas veces es solo lo que se ve. En el resto de los elementos encontramos los procesos que

¹ Biometría; es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. La “biometría informática” es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.
<http://es.wikipedia.org/wiki/Biometria>

² www.clad.org

incidirán en un porcentaje del **treinta y cinco por ciento** (35%), las personas (que los operen, como las que hagan uso de los beneficios) y la cultura, ya sea organizacional como del lugar donde se vaya a implantar la solución, tendrán una incidencia en el éxito del proyecto de un **veinticinco por ciento** (25%) cada una.

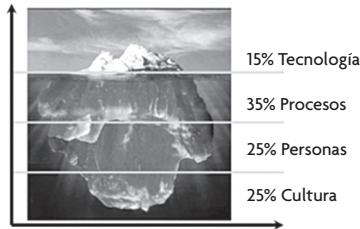


Figura 1

Entonces profundicemos sobre cada una de estas partes:

Tecnología

Como dijimos anteriormente, la tecnología (hardware, software, comunicaciones) es cada vez más accesible a nivel de costos y la convergencia tecnológica es una realidad. Esta regla también es válida para soluciones Biométricas, habiendo una gran cantidad de dispositivos para cada una de los métodos, ya sean:

- Físicos; huellas dactilares, venas de la mano, geometría de la palma de la mano, iris/retina, facial, ADN, voz, dental, palatoscopia, forma del oído
- De comportamiento; firma, reconocimiento del teclado (key stroke recognition), reconocimiento de la forma de caminar (gait recognition), gesticular

Con lo cual la factibilidad para encarar proyectos crece día a día.

Ahora bien, si hablamos de tecnología probada, con una amplia oferta de soluciones, sistemas y dispositivos, ¿cuáles serían entonces los temas que no deberían faltar en la etapa de planificación, para que los proyectos sean escalables? Que los mismos fuesen diseñados e implantados bajo estándares³ y buenas prácticas⁴ internacionales. Es decir, valerse de estos estándares para definir temas tales como la captura de la información, su almacenamiento, formato de comunicaciones e inclusive hasta la forma de llevar adelante el proyecto.

Es así que, si hablamos del intercambio de información entre sistemas de información y/o aplicaciones (interfaces de programación, API) deberían trabajar bajo el estándar **ANSI / NIST ITL 1-2011**⁵ de muy reciente aprobación, que define cómo trabajar para la interoperabilidad de datos biométricos entre los distintos sistemas.

Así mismo, también será importante que los gobiernos, a través de las direcciones responsables de definir estándares tecnológicos, fijen condiciones mínimas de certificación que deberían contar los equipos o dispositivos. Por ejemplo la que provee la Federal Bureau Investigation (FBI)⁶. Esto permitirá la escalabilidad de proyectos, desapareciendo las barreras de integración

3 <http://www.wordreference.com/definicion/estandar>

4 http://es.wikipedia.org/wiki/Mejores_practicas

5 http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

6 <http://www.fbi.gov/>

y que no sean los dispositivos, los que se transformen en críticos y responsables del fracaso.

Para ahondar aún más en la importancia de la adopción de estándares, para que los programas sean interoperables, escalables y con alto grado de seguridad en el intercambio de información, podemos analizar la experiencia de la industria de servicios financieros. La misma es históricamente una de las que cuenta con: el mayor número de centro de cómputos interconectados, la mayor cantidad de usuarios, una gran distribución física de dispositivos, un alto nivel de intercambio de información, un trabajo en tiempo real, manejo información crítica y confidencial, y me animaría a decir, el más alto nivel de seguridad de la información. Si por ejemplo, en el comienzo de la implantación de las redes de cajeros automáticos, no hubiesen utilizado estándares; para el formato de las bandas magnéticas de las tarjetas, el sistema de encripción, es decir, la decisión de trabajar bajo estándares internacionales, nada de lo que es hoy esa industria hubiese sido posible.

Por lo tanto, tomar la decisión de trabajar con estándares y buenas prácticas en el área de tecnología, es estar definiendo uno de los más importantes pilares para el éxito del proyecto. Un ejemplo reciente de las implicancias por una planificación no adecuada de uso de estándares, es el caso de la Policía Federal Argentina. Esta institución tempranamente en el año 1995, comenzó a guardar los datos de los ciudadanos (patrónicos y biométricos) no solo en papel, sino que también digitalmente en una base de datos. Recientemente por una necesidad de servicio y calidad, tuvo que hacer un salto tecnológico, y debió resolver el problema de compatibilizar la lectura de 5 millones de registros dactilares que existían en una base de datos propietaria, del sistema que tenían implantado.⁷

Obviamente hay otras decisiones tecnológicas más o tan importantes a evaluar en la etapa de planificación. Por ejemplo, respecto de los dispositivos y método biométrico utilizar, difícilmente se podría optar por un sistema de identificación dactilar, en proyectos donde las personas que deban identificarse tengan una actividad que haga que sus manos no estén limpias; en ese caso la calidad de identificación sería muy baja.

O el plan de contingencia ante fallas en la tecnología. Tema que ya está presente en todos los proyectos, pero que muchas veces, no se le da el tiempo adecuado, para el diseño de esa solución. Seguramente el proceso ante fallas, podrá ser más burocrático y lento, ya que estamos hablando de identificación de personas, pero a la hora del diseño deberá prestársele tanta atención a la contingencia, como al proyecto principal. Esto es consecuencia de que, en la medida que los procesos se hacen más lineales y agiles por el uso de la tecnología, la misma se vuelve crítica y difícil de reemplazar u obtener las mismas prestaciones o flexibilidad ante fallas.

Procesos

Quedo bien reflejado en la Fig. 1 que planificar y trabajar sobre los procesos (con una incidencia del 35%), será un factor importante para el éxito de los proyectos. Pero en la palabra procesos, se involucra también las políticas organizacionales y procedimientos que se deberán diseñar como parte de la solución integral a implantar.

⁷ (Biometrías, "Herramientas para la Identidad y Seguridad Pública", P. Janices, 42)

Una vez más, como cuando hablamos de Biometría, estamos hablando del involucramiento directo de los ciudadanos, por lo que, deberemos comenzar por analizar las leyes y estándares existentes (o que habrá que crear) y que serán la base para el diseño de las políticas, procesos y procedimientos de la solución.

Si nos situáramos en la Argentina, deberíamos hablar de la Ley 17.761 y sus modificatorias⁸ que regulan la identificación, registro y clasificación del potencial humano nacional, o la Ley 24.450 que establece el régimen de identificación de los recién nacidos, donde se obliga a la identificación de los mismos a través de datos patronímicos, como biométricos. Si hablásemos de los pasaportes, deberíamos referirnos a recomendaciones de la International Civil Aviation Organization (ICAO)⁹, tema importantísimo si pensamos en la necesidad imperiosa de poder identificar a una persona más allá de las fronteras de su país. Pero a nivel de documentación de los ciudadanos, existentes deudas como los estándares de los documentos únicos de identificación, inclusive habiendo países que no cuentan con normas que exijan la necesidad de los mismos. Es decir, deberemos analizar los distintos marcos legales y estándares para luego ver temas como que datos se están registrando, con qué formato (si existiese), etc.

Si bien jurídicamente la identificación de las personas está resuelta, creo que el avance de la tecnología y los sistemas de identificación biométricos, harán que aparezcan nuevos marcos legales para la identificación digital del ciudadano. Colaborando en el logro de los objetivos perseguidos por muchos países de la región; la inclusión social, los derechos de las personas y el gobierno electrónico, como mencionásemos en el comienzo de este capítulo.

Una vez que hemos revisado los aspectos legales correspondientes y teniendo en cuenta el área donde se va a desarrollar el proyecto biométrico, se deberá poner foco en el diseño de los procesos para que los mismos sean lineales y agiles, que son dos características viables con el uso de la Biometría. Las características de procesos agiles y lineales son principios de la reingeniería, planteados en el año 1994, por sus creadores Michael Hammer y James Champy, ambos provenientes del mundo tecnológico.

Ellos definían conceptos como “la necesidad de sencillez produce consecuencias enormes en cuanto a la manera de diseñar los procesos y de darles forma a las organizaciones¹⁰ o algunos de los postulados que se definieron a partir del surgimiento de la reingeniería, como son:

- Ingreso de la información en el origen; la tecnología biométrica hace participar directamente a la persona como parte actora de la acción de identificación digital.
- Eliminación de pasos intermedios; con identificación digital, el proceso se cumple en forma automatizada.
- Diseñar procesos que agregan valor, que más valor puede tener que él transparentar la identificación y hacer justa la inclusión social, aquí estoy asumiendo la premisa que la identificación biométrica me dará la mayor seguridad existente a la fecha en la identificación de las personas.

Esta nueva forma de hacer las cosas trae aparejado un cambio de valores tanto culturales como organizacionales, que las personas (tercer parte integrante de este proyecto) tendrá que afrontar.

⁸ <http://www.boletinoficial.gov.ar/institucional/index.castle>

⁹ <http://www2.icao.int>

¹⁰ (Reingeniería, M Hammer & J Champy, 1994, 54);

Además de lo dicho hasta aquí en materia de reingeniería para el rediseño de estos procesos y procedimientos, uno no podrá basarse en la experiencia de quien lleva a cabo su implantación, ya que hace varios años esto dejó de ser la fuente de conocimiento, debiéndose trabajar (cuando estos existen) con los estándares internacionales existentes, Por ejemplo los estándares ISO/IEC¹¹ que definen que debería hacerse en particular para la solución específica.

En Biometría, existe la norma ISO/IEC 19794¹² que describe desde los aspectos generales y los requisitos para la definición de formatos de intercambio de datos biométricos. Su notación, los formatos de transferencia (que deben proveer independencia de la plataforma) y la separación de la sintaxis de transferencia de la definición del contenido. Esta norma define lo que comúnmente se aplica en los datos biométricos, es decir, la estandarización de los contenidos comunes, lo que significa, el formato de intercambio, como la representación de los formatos de los datos, teniendo especificaciones para los distintos sistemas de identificación biométricos. Una descripción más detallada de estos estándares se puede encontrar en la página de Biometría del Gobierno Argentino.¹³

Volviendo a procesos ágiles y además seguros para la identificación de ciudadanos, si lo hiciésemos a través de un documento y alguna característica física del mismo (sistema biométrico), será una tarea más ágil y segura que si fuese través del documento y algún dispositivo. Simplemente y sin entrar en más detalles, con solo pensar que ese dispositivo, debe estar junto a la persona en el momento de realizar la acción. Aquí no mencionamos el uso de un nombre de usuario y una clave, ya que directamente no es considerado seguro como identificación digital.

Personas

Si estas líneas hubiesen sido escrita diez años atrás, tal vez debería haber ocupado un capítulo completo hablando de las personas. Por suerte, cada vez más, empieza a desaparecer el miedo a la tecnología, a su seguridad y uso.

El trabajo que vienen realizando muchos Gobiernos, entre ellos, el argentino por achicar la brecha digital, hace que podamos pensar que en mediano plazo desaparecerá definitivamente la “ignorancia tecnológica”¹⁴ y por lo tanto, el miedo a lo desconocido dejará de ser un factor relevante.

Pero cuando hablamos de personas y su influencia en el éxito de los proyectos con base tecnológica, no solo debemos detenernos en el conocimiento de la misma. Hay otros factores asociados que pueden influenciar positiva o negativamente de acuerdo a como se los planifique. Por ejemplo, debemos distinguir, entre aquellas que manejarán la solución, de las que serán usuarios de la misma (en este caso los ciudadanos).

Comencemos por el más conocido “la resistencia al cambio”, en el caso de los usuarios esta condición no se pondrá de manifiesto, ya que las técnicas de identificación biométricas más

¹¹ <http://www.iso.org/>

¹² http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50862

¹³ <http://www.biometria.gov.ar/metodos-biometricos/dactilar.aspx>

¹⁴ Cuando se aplica a un contenido concreto significa «no saber algo determinado», frente al conocimiento de otras muchas cosas o «tener un conocimiento imperfecto sobre...» <http://es.wikipedia.org/wiki/Ignorancia>,

comúnmente utilizadas no son invasivas. Es más, los ciudadanos argentinos ya encontraron positivo el hecho de no tener que pintarse los dedos para la identificación dactilar para la obtención de los nuevos DNI¹⁵ y pasaporte¹⁶. Proyecto exitoso que involucra el uso de la biometría, y donde se vieron reflejadas muchas de las ventajas de su uso.

Ahora bien, si hablamos de los usuarios del sistema, esta resistencia posiblemente sí se pondrá de manifiesto, sin hacer referencia a ningún proyecto en particular, sino a la experiencia vivida en muchos proyectos de rediseño de procesos, e innovación y los estudios realizados por muchos investigadores.

Kurt Lewin¹⁷, uno de los mayores estudiosos de los procesos de resistencia al cambio, reconocido como el fundador de la Psicología Social moderna, encontró tres causas comunes:

- Interés propio. Definidas como las razones personales que afectan o alimentan el deseo de cambio. Aquí se ubica la motivación, la costumbre a desarrollar un proceso definido de trabajo y la capacitación.
- Cultura organizacional. Entendido como la fuerza fundamental que guía la conducta de los trabajadores: A veces, se sienten amenazados cuando se trata de efectuar cambios radicales en la manera de hacer las cosas en determinadas actividades.
- Percepción de las metas y estrategias de la organización. Los miembros de un equipo no entienden que se necesita una meta nueva (un cambio), porque no cuentan con la misma información que manejan sus directivos.

Lamentablemente estas causas se ponen de manifiesto aún más cuando hablamos de estructuras gubernamentales, donde existen en muchos países estructuras poco flexibles, muy jerárquicas, donde conceptos como “cuantos más dependientes directos tenga yo, mas importante soy”¹⁸.

Y estas razones, donde el desafío está en el cambio de paradigma de las personas y/o usuarios, serán seguramente uno de los mayores problemas a enfrentar a la hora de implementar un proyecto tecnológico, y más aún cuando el mismo involucre aplinar el proceso para su agilización.

Lo dicho hasta aquí acerca de las personas parece muy obvio y que hoy en día a nadie se le escapa; sin embargo lamento decirle al lector, que esto no concuerda con lo que vivimos a diario en la implantación de proyectos que involucran cambios organizacionales. Por lo que, habrá que recurrir a metodologías y formas de implantar un proyecto, que permiten minimizar estos los factores negativos. En el final de este capítulo enunciaremos algunos de los mismos.

Cultura

Esta parte que tiene una incidencia del veinticinco por ciento, es decir, mayor que la propia tecnología, al igual que cuando hablamos de las personas tiene dos visiones.

15 <http://www.nuevodni.gov.ar/>

16 <http://www.mininterior.gov.ar/pasaporte/>

17 http://es.wikipedia.org/wiki/Kurt_Lewin

18 Reingeniería (M Hammer % J Champy, 1994, 80)

Nos referimos tanto a:

- Cultura Organizacional
- Cultura social¹⁹, que en proyectos de índole públicos y/o regionales juegan un papel mucho más importante.

Respecto de la cultura organizacional, podemos afirmar que su incidencia en el éxito del proyecto biométrico estará dada básicamente por el estilo de liderazgo que tenga el sponsor del proyecto y el director del mismo. Temas como la estabilidad laboral de los empleados públicos, los tiempos limitados de los funcionarios en su cargo; como así también, la falta de premios y castigos de los empleados, hacen poco posible pensar en un cambio cultural de esa organización o dependencia. Por lo tanto, a la hora de la planificación del proyecto, se deberá tener en cuenta esa cultura para que el proyecto no fracase.

A nivel de cultura social, considero que el tema es distinto. Si bien los países e individuos tienen culturas bien definidas hay estrategias que se pueden implantar a la hora de encarar la puesta en marcha de un proyecto Biométrico. Normalmente los usuarios y/o ciudadanos se resisten a los cambios por falta de comunicación, de explicación de las ventajas que traerán aparejado esta solución.

Si quisiésemos que, a nivel organizacional, las mismas estén más preparadas para el cambio, deberían existir buenas políticas, como dice L. Schvarstein, “una buena política sería dotar a las organizaciones de la capacidad necesaria para sostener buenas utopías. Las utopías son signos de insatisfacción con el presente, su sometimiento es un factor de desequilibrio que no puede sino favorecer el desarrollo de la organización y de sus miembros, que dará espacio al sujeto.”²⁰

Como así también, “dotarlas de una plasticidad estructural que permita disposicionalmente abordar situaciones de cambio, será entonces esta preocupación algo que no deberá estar ausente en el diseño de las estructuras”.²¹

Factores de Éxito de los proyectos

Habiendo ya repasado sucintamente cuatro de los factores de éxito de un proyecto biométrico, que aunque no son los únicos, si son normalmente los que más varían de acuerdo a la solución a implantar. Volvemos a remarcar la necesidad de que formen parte importante en la etapa de planificación, ya que a veces por falta de conocimiento, necesidad política, o simplemente por desconocimiento no se le asignan el grado de análisis y tiempo suficiente, pasando a ser luego las razones que dichos proyectos pasen a engrosar los definidos como “A prueba”. Esta denominación, se corresponde a proyectos que fueron rediseñados en su alcance, objetivos, especificaciones u otro elemento que modificaron su concepción inicial y que finalmente pudieron terminar. Si analizamos los estudios realizados por Standish Group en Estados Unidos (Standish 2001) y la Universidad de Oxford en el Reino Unido²² (figura 2), casi el cincuenta por

¹⁹ Definición; El medio ambiente social de las creencias creadas por los seres humanos, las costumbres, los conocimientos, y las prácticas que definen la conducta convencional en una sociedad. (Newstrom & Davis, 1993)

²⁰ Psicología Social de las Organizaciones (Leonardo Schvarstein, 2002, 268)

²¹ Psicología Social de las Organizaciones (Leonardo Schvarstein, 2002, 246)

²² http://www.alejandrobarros.com/media/users/1/50369/files/4363/Proyectos_TIC_GOV.pdf (pag. 4)

ciento (50 %) de se corresponden con “a prueba”, frente a un dieciséis por ciento (16%) exitosos, y el resto fracasados.

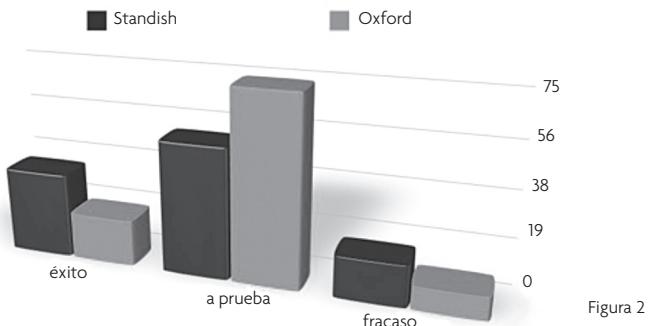


Figura 2

Otro informe que también habla sobre los factores que afectan al desempeño de proyectos TIC's en Gobiernos, es el realizado por Alejandro Barros, donde aparecen causas como la adopción de metodologías de desarrollo/diseño no probadas y con poca experiencia ²³. Que traducido en términos de lo que venimos definiendo en este capítulo, sería por ejemplo; que los dispositivos no cuenten con alguna certificación internacional, no trabajar bajo estándares, normas y buenas prácticas internacionales. La Argentina por ejemplo, va camino a realizar bien las cosas en materia biométrica, siendo deseable que se haga realidad el “Programa Nacional de Estandarización de Datos Biométricos y Biométricos Forenses (comúnmente llamado bio.ar)” ²⁴, tarea que está siendo coordinada por la Oficina Nacional de Tecnología de la Información (ONTI). Dirección que tiene a su cargo las tareas necesarias para la homogeneización y coordinación de las herramientas tecnológicas para la optimización de la gestión.

Otro trabajo que podría ayudar en la etapa de planificación de un proyecto, es el realizado por la Parliamentary Office of Science and Technology (Government IT Projects) en el Reino Unido, cuya finalidad es evaluar los proyecto sobre la base de factores de éxito y fracaso en 16 áreas, las cuales determinaran la evolución de un proyecto TIC ²⁵. Destacando nuevamente, entre otras, el trabajar con soluciones establecidas y proyectos no complejos.

Como venimos hablando permanentemente de la utilización de estándares, normas y buenas prácticas, es indispensable también mencionar que el proyecto deberá gestionarse para su éxito, de acuerdo a los principios metodológicos definidos por el Project Management Institute (PMI[®])²⁶ o el Gobierno de Inglaterra (Prince 2[®])²⁷

Por último, como condición sine qua non, siendo que los grandes proyectos biométricos son los relacionados con los ciudadanos y el Estado, está la decisión política como clave del éxito de los mismos.

²³ http://www.alejandrobarros.com/media/users/1/50369/files/4363/Proyectos_TIC_GOV.pdf (pag. 6)

²⁴ http://www.biometria.gov.ar/media/14056/estandar_MININT_biométrico8.pdf

²⁵ http://www.alejandrobarros.com/media/users/1/50369/files/4363/Proyectos_TIC_GOV.pdf (pag. 7)

²⁶ <http://www.pmi.org/>

²⁷ <http://www.prince-officialsite.com/>

Conclusión

En la Argentina muchas de las tareas para convertir a la Biometría en la herramienta para identificación digital de individuos, ya se puso en marcha hace años. Pero tal vez, uno de los proyectos más ambiciosos, es la creación de un repositorio integral interABIS de resguardo e interconsulta Biométrica, que consolidara los datos biométricos existentes en los distintos Organismos Oficiales, Organismos Provinciales, y otras dependencias nacionales o provinciales con competencia en la materia, brindando servicios de interconsulta y verificación. Este proyecto fue concebido bajo los principios de manejarse con los estándares y buenas prácticas existentes a nivel internacional para este tipo de desafíos.

Pero en la Argentina, existen problemas que seguramente se repiten en otros países. De allí el repaso de esta lista de sugerencias y puntos críticos que deberán abordarse para no fallar:

- La adopción y estandarización de interfaces XML para la interoperabilidad de datos biométricos
- La definición de estándares Nacionales de certificación para los dispositivos.
- Trabajar en la implementación de una Verificación de Identidad Personal (PIV)²⁸, en el ámbito de la administración pública nacional.
- Armar una estructura computacional adecuada para el resguardo de datos críticos, que cumpla con los estándares correspondientes.
- Crear una autoridad de aplicación que bregue por la funcionalidad del sistema, incluyendo el intercambio de información.
- La integración de privacidad de todas las capas de la arquitectura del sistema a implantar.
- La definición de una guía de buenas prácticas, para la digitalización de formularios biométricos es decir la interoperabilidad biométrica.
- Trabajar sobre la calidad de los datos, donde es posible que existan duplicación de registros biométricos con diversa identidades patronímicas (nombres vs. datos biométricos) o que los registros no estén en formatos consumibles para aplicaciones automatizadas.
- Implementación de registros biométricos de personas NN, cadáveres NN o personas declaradas desaparecidas.
- Realizar un debate profundo entre el sector público y privado sobre donde, cuando y como debe aplicarse biometría, abordando temas como privacidad y seguridad.
- Difundir y sensibilizar al ciudadano acerca de los beneficios de la correcta identificación de los ciudadanos para la inclusión social lo no invasivo de estos métodos las leyes y normativas de privacidad existentes.

No olvidemos que el cementerio de los fracasos está lleno de buenas ideas, mal implementadas.

²⁸ <http://csrc.nist.gov/groups/SNS/piv/index.html>

Bibliografía

Centro Latinoamericano de Administración para el Desarrollo (CLAD), www.clad.org

National Institute of Standards and Technology Information Technology, www.nist.gov

Federal Bureau of Investigation <http://www.fbi.gov/>

Boletín Oficial de la República Argentina, <http://www.boletinoficial.gov.ar/institucional/index.castle>

International Civil Aviation Organization, <http://www.icao.int>

Michael Hammer & James Champy (1994) "Reingeniería", Colombia, Grupo Editorial Norma

International Organization for Standardization, <http://www.iso.org/>

Sitio web oficial de Biometria del Gobierno Argentino, <http://www.biometria.gov.ar>

Wikipedia, <http://es.wikipedia.org>

Sitio web oficial del nuevo Documento Nacional de Identidad de la República Argentina,
<http://www.nuevodni.gov.ar/>

Sitio web oficial del Ministerio del Interior de la Rep Argentina,
<http://www.mininterior.gov.ar/pasaporte/>

Leonardo Shvarstein (2002), "Psicología Social de las Organizaciones", Barcelona, Editorial Paidós
Davis, K y Newstrom, J (1993): Comportamiento Humano en el Trabajo. (8th ed.), México, D.F, Mc Graw-Hill

Blogs de Alejandro Barros, <http://www.alejandrobarros.com>

Project Management Institute, "PMBOK®", Fourth Edition

OGC, "Managing Successful Project with PRINCE 2™, 2009, Edition

Tecnología en Biometría y la Nueva Economía: Una Revisión del Campo y el Caso de los Emiratos Árabes Unidos

Ali M. Al-Khoury



Ali M. Al-Khoury

Director General Autoridad de Identidad de los Emiratos Árabes Unidos.



El doctor Al-Khoury posee un doctorado en ingeniería en el campo de la gestión de programas de gobierno estratégicos y de gran escala, en la Universidad de Warwick del Reino Unido. Actualmente se desempeña como Director General de la Autoridad de Identidad de los Emiratos. Durante los últimos 20 años ha estado involucrado en numerosos programas de gobierno estratégicos y de gran escala. Ha sido un investigador activo en desarrollos revolucionarios en el contexto gubernamental y ha publicado más de treinta artículos en los últimos cuatro años. Sus actuales áreas de investigación se relacionan con el desarrollo de mejores prácticas en la gestión pública y el desarrollo de sociedades de la información, con particular atención en las aplicaciones de gobierno electrónico.

Información de contacto: P.O. Box: 47999, Abu Dhabi, United Arab Emirates

Tel.: +971 2 495 5450

Fax: +971 2 495 5999

email: ali.alkhoury@emiratesid.ae

website: www.emiratesid.ae

Resumen

Durante la última década, la tecnología en biometría ha evolucionado desde una tecnología utilizada principalmente en el ámbito forense y un campo estrecho científico y tecnológico a una tecnología indispensable en los sectores públicos y privados que están expandiendo sus raíces en áreas que demandan una seguridad avanzada. Las tecnologías en biometría ofrecen altos niveles de seguridad y confiabilidad para tratar los requerimientos relacionados con la identificación y verificación de identidades personales. A la luz de las permanentes y crecientes demandas de un manejo de la identidad robusto, la industria de la biometría está evolucionando para jugar un rol central en diseñar la economía del futuro.

Este artículo presenta una visión global de las tecnologías biométricas, sus funciones y áreas de aplicación, estándares internacionales relacionados y los recientes avances en este campo. La segunda parte de este artículo muestra la aplicación de la biometría en los sectores gubernamentales, en todo el mundo y el rol pivote emergente de la biometría en la consolidación de las fundaciones de las economías digitales.

También arroja luz sobre las experiencias de los Emiratos Árabes Unidos en el despliegue e implementación de diferentes tecnologías avanzadas en un amplio rango de aplicaciones. Señala los planes del gobierno para desarrollar una infraestructura de manejo de la identidad dirigida a múltiples objetivos estratégicos, algunos de los cuales están relacionados con revolucionar los servicios públicos y sustentar el desarrollo de la economía digital.

Palabras clave: biometría, manejo de la identidad, economía digital, sociedad digital.

Tecnología en Biometría y la Nueva Economía: Una Revisión del Campo y el Caso de los Emiratos Árabes Unidos

Introducción: Historia de la Biometría y el Estado Actual

La raza humana siempre ha estado acosada por la necesidad de métodos altamente seguros para la identificación y verificación de personas, que surgen de varias razones en torno a: consideraciones sociales, económicas, comerciales y legales. La identificación es un proceso a través del cual uno asegura la identidad de otra persona o entidad. Siempre se ha reconocido que todo ser humano tiene rasgos únicos que pueden definir su identidad.

El reconocimiento comenzó por los rostros que son tan únicos como los que puedan aparecer. Sin embargo, con poblaciones más numerosas, los avances en alteraciones quirúrgicas y los modernos modelos de servicio centrados en el ciudadano han requerido variar los métodos de reconocimiento e identificación única.

Derivada de las palabras griegas Bios (vida) y Metron (Medición), la biometría representa la ciencia de reconocimiento de la identidad. La biometría como una ciencia y un medio automatizado de identificación tiene unas pocas décadas de antigüedad, pero como concepto, ha existido durante miles de años (Ver Figura 1, y Tabla 1). Hoy, la identificación biométrica está reconocida mundialmente como un método de identificación personal definitivo con métricas específicas que dan tanto al proveedor del servicio como al usuario final la garantía de una transacción rápida, segura, y práctica.

Referencia de Investigación	Evidencia
Renaghan (2005)	Detalles de una caverna que datan de 31.000 años atrás revelaron impresiones de la mano de prehistóricos humanos con figuras prehistóricas aparentemente firmadas con la estampa de las huellas dactilares de los autores.
McMahon (2005)	Historiadores chinos e indios tienen referencias de huellas dactilares usadas como firmas en transacciones que datan de 5 mil años atrás.
McMahon (2005)	Historiadores chinos e indios tienen referencias de huellas dactilares usadas como firmas en transacciones que datan de 5 mil años atrás.
“Dermatoglíficos”, (2005)	Las tablas de arcilla de Babilonia de 500 AC muestran evidencia de que la humanidad acostumbraba a registrar transacciones comerciales y firmar estampando la huella dactilar.

Tabla 1: Medios de reconocimiento en la historia de la civilización



Figura 1: Fines Antes de Cristo. Se descubrió la escritura de los patrones de las crestas de la palma en Nueva Escocia.

Claramente, la identificación de las personas se tornó un requerimiento para la actual economía global cada vez más digitalizada. En realidad, la confianza en las transacciones electrónicas es esencial para el fuerte crecimiento de la economía global. Aunque los mercados se achican y expanden en forma cíclica, las naciones emergentes continúan presentando nuevos mercados emergentes con oportunidades infinitas. Sin embargo, la globalización generalmente está elevando el nivel de intensidad y competencia para entregar servicios y productos mejores, más económicos y rápidos en un entorno seguro y confiable. Las empresas se encuentran en la necesidad de soluciones de identificación modernas más que antes para establecer tales bases de confianza, es decir, para negación y acuerdo, y para aceptación y rechazo.

Las empresas y los gobiernos también en la década pasada, por lo tanto, han prestado atención a la protección de sus infraestructuras desde las actividades de hacerse pasar por otra persona y/o infiltración; un delito que se informó que costó 35 billones de dólares en Estados Unidos solamente en 2011 (Vamosi et al., 2011). Con tal atención justificada a los requerimientos de identificación, los métodos de identificación cobraron mayor prominencia.

Además, como las iniciativas de gobierno electrónico y comercio electrónico proliferan, ofreciendo más servicios electrónicos online se requieren métodos de identificación y autenticación robustos para enfrentar los requerimientos de control y seguridad. La bibliografía existente se refirió extensamente al hecho de que uno de los temas principales que presentan un desafío frente al desarrollo de gobierno electrónico y de la sociedad electrónica es el manejo de la identidad y el tema de la confianza en las transacciones online e identidades digitales. Y por último, la identidad digital necesita pasar a ser lo mismo que la identidad del mundo real. El uso de identificadores biométricos para el manejo de la identidad ofrece fuertes credenciales y niveles de aseguramiento de la calidad más altos.

De acuerdo con un informe reciente publicado por los Servicios Electrónicos RNCOS (Servicios de Consultoría de Investigación de Mercados) se anticipa que el mercado biométrico mundial crecerá a un CAGR de alrededor del 22% entre 2011 y 2013 (RNCOS, 2011). A nivel regional, Norte América informó dominar la participación del Mercado biométrico global de más del 30% en 2010. Se esperaba que la región de Asia, Oriente Medio y África emergieran como mercados crecientes en biometría para el 2013.

El informe también indicó que el sector del gobierno representa la participación mayor del Mercado biométrico mientras que los sectores de atención de la salud y financieros están emergiendo como adoptadores potenciales de los sistemas biométricos. Muchos bancos en países desarrollados (específicamente las naciones de Asia, incluyendo India, China, Malasia, etc.) han adoptado la biometría para enfrentar los temas de fraude de identidad y para ofrecer a los clientes una alternativa de autenticación fácil y más práctica con respecto a las tarjetas y PINs para las transacciones, como por ejemplo las extracciones de los cajeros automáticos.

Nuevamente, la biometría es vista como un facilitador crítico para la nueva economía digital. Sólo comprendiendo sus potenciales, cómo funciona, y construyendo sobre las experiencias ganadas a partir de implementaciones internacionales podemos esperar alcanzar un progreso significativo en la creación de un futuro exitoso para nuestras sociedades. Como tal, este

Este artículo está escrito en el espectro de este diálogo.

Este artículo está estructurado como sigue. La primera sección brinda una visión general de la biometría, incluyendo sus características, campos de aplicación, normas internacionales relacionadas, y recientes avances que están modelando la industria de la biometría. La segunda sección observa cómo las tecnologías para biometría son adoptadas en el sector gubernamental, y su rol emergente en atender los requerimientos de identidad y construyendo la base para la nueva economía digital.

La tercera sección enfoca algunas iniciativas biométricas implementadas en los Emiratos Árabes Unidos en la última década para atender las necesidades relacionadas con el desarrollo de sistemas de infraestructura crítica. Finalmente, la cuarta sección presenta una visión general de uno de los programas multimillonarios en dólares implementados para desarrollar una infraestructura de manejo de la identidad para actuar como una única fuente para la provisión de identidad personal en el país.

Características Biométricas

Las características biométricas están divididas en dos amplias categorías: fisiológicas y de comportamiento. Las características fisiológicas son aquellas que están estrechamente ligadas al cuerpo humano. El Iris, la retina, los rasgos faciales, la huella dactilar, la impresión de la palma y el ADN son características físicas del cuerpo humano; ofrecen identificación positiva que es difícil de falsear. La voz, el habla, las firmas, la escritura, la secuencia de teclado son características usadas para los estudios de los patrones de conducta.

A fin de reconocer una persona por sus características biométricas y rasgos biométricos derivados, se debe hacer un proceso de inscripción. El proceso implica la construcción de un registro de datos de la persona registrada y almacenarlo en una base de datos de registros biométricos. El registro de datos de inscripción debe comprender una o múltiples referencias biométricas y datos no biométricos arbitrarios, por ejemplo, nombre, información personal, etc. Ver también la Figura 2.

Medición del Comportamiento	Descripción
Tasa de rechazo falso (non-match) (FRR) o error tipo I	La medición del porcentaje de veces que un sujeto válido ha sido rechazado falsamente por el sistema. FRR (%) = cantidad de rechazos falsos * 100/cantidad total de intentos únicos.
Tasa de aceptación de Falso (match) (FAR) o error tipo II	La medición del porcentaje de veces que un sujeto inválido ha sido falsamente aceptado por el sistema. FAR (%) = cantidad de aceptaciones falsas * 100/cantidad total de intentos únicos.
Tasa de error “cross-over” (CER)	Una medición que representa el porcentaje en que FRR iguala a FAR. Este es el punto con el gráfico donde se intersectan FAR y FRR. La tasa de cross-over indica un sistema con buen balance sobre sensibilidad y rendimiento.

Tabla 2: Mediciones de los comportamientos biométricos

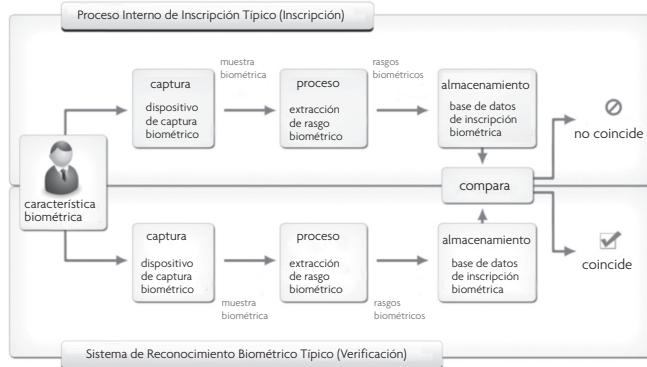


Figura 2: Procesos de inscripción y verificación.

El proceso de reconocimiento se inicia cuando la persona a ser reconocida presenta su característica biométrica en el dispositivo biométrico de captura. El dispositivo genera una muestra biométrica de reconocimiento con rasgos biométricos que son comparados con una o más plantillas biométricas de la base de datos de registros biométricos. Esto debería dar por resultado la aceptación o el rechazo del pedido de reconocimiento.

El proceso más común de captura en biometría hoy en día es óptico. En la mayoría de los casos se utilizan cámaras miniaturas CCD, que capturan luz visible o infrarroja (Brüderlin, 2001). Los métodos recientes, particularmente en la captura de huellas dactilares tratan de dejar de lado la captura biométrica para utilizar temperatura, presión y/o capacidad (*ibid*). Las principales medidas de evaluación del desempeño en los sistemas biométricos están descritos en la Tabla 2. Sin embargo, la precisión de estas mediciones varía, lo que tiene relevancia directa sobre los niveles de seguridad que ofrecen (Shoniregun y Crosier, 2008). Las tasas de error de los sistemas biométricos es ajustable, lo que permite que se configure de acuerdo con los objetivos de la empresa.

Las tasas de error en biometría no pueden ser totalmente disminuidas, sin embargo, reduciendo una tasa de error incrementará la otra. Se debe encontrar un balance entre riesgo (es decir, aceptación falsa) y operabilidad (es decir rechazo falso) que concuerde mejor con los objetivos de la empresa. Como se describe en la Figura 3, mayormente en biometría, una comparación de plantilla da por resultado un valor representado por la “Distancia de Hamming”, que es el porcentaje de bits de dos plantillas biométricas comparadas que son diferentes. Si este porcentaje es más bajo que un umbral establecido, se toma una decisión de coincidencia y viceversa.

En este ejemplo de arriba el umbral está establecido en 0.41 lo que significa que el sistema reconoce una biometría presentada como auténtica cuando no más del 41% de los bits capturados previamente durante el proceso de inscripción sean diferentes de los bits capturados en el momento de la verificación. Un auténtico con más de 41% de bits diferentes es denominado una no coincidencia falsa, un impostor con menos del 41% de bits diferentes es llamado coincidencia falsa.

Capacidad Biométrica	Explicación
Identificación	Es el proceso por medio del cual uno trata de ver si coincide una muestra presentada de información biométrica con una base de datos de identidades conocida.
Verificación	Si se establece una coincidencia, se establece la identidad de la persona. Es el proceso por el cual se establece una confirmación de un reclamo de identidad. Brinda una respuesta a “¿Soy realmente la persona que pretendo ser?”
Autenticación	Es el proceso por el cual se establece la veracidad de la muestra biométrica presentada. La autenticidad de la muestra biométrica presentada establece las credenciales de la persona.
Reconocimiento	Es el proceso que no es necesariamente para la identificación o verificación. Es para reconocer a un individuo – especialmente cuando no hay rasgos disponibles para detección. EL ADN es un ejemplo excelente de aplicación de Reconocimiento.

Tabla 3: Funciones biométricas

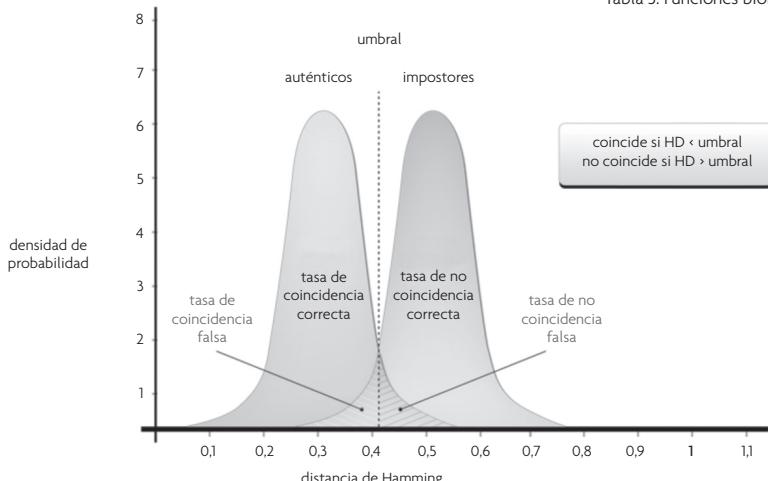


Figura 3: Ajuste de los sistemas biométricos

El diagrama (Figura 3) muestra cómo el umbral configurable determina el balance entre las tasas de coincidencia falsa y no coincidencia falsa. La probabilidad de una coincidencia falsa o una no coincidencia falsa es igual al área bajo la curva en ambos lados del umbral. Cambiando el umbral, un área se reduce mientras la otra se incrementa, determinando así el balance.

Las tecnologías actuales han evolucionado en el curso de las últimas cinco décadas hacia niveles de maduración más altos debido a los desarrollos en la tecnología de semiconductores sumado al poder de la computación. Sin embargo, los impedimentos de la biometría en primer lugar giran alrededor de los temas de complejidad y privacidad en el abuso de información.

El abuso de información biométrica ha provocado que varios libertarios civiles se indignaran por los riesgos presentados por la naturaleza personal de la información biométrica y cómo esta información puede ser manipulada o mal utilizada. Inversamente, la evolución de la biometría

hacia el estado actual en el mundo se entiende mejor en el contexto de las aplicaciones de la biometría. La siguiente sección da una visión de los usos diferentes de la biometría que también explican el concepto de identificación y autenticación.

1.2 Propósito de la Biometría

Los números de identificación personal, generalmente denominados números PIN, fueron uno de los identificadores iniciales para ofrecer un reconocimiento automatizado. El PIN es una clave numérica secreta compartida entre un usuario y un sistema que puede ser usado para autenticar al usuario. A pesar de su amplia aplicación, los métodos de autenticación basados en un PIN no ofrecen un reconocimiento de la persona que está realizando la transacción. La biometría, sin embargo, representa identificadores únicos y contrariamente a los PINs, no pueden ser fácilmente transferidos entre individuos. La mayoría de las aplicaciones biométricas actuales están relacionadas con la seguridad y se utilizan ampliamente en el sector del gobierno.

Las vastas aplicaciones de la biometría en el dominio público están siendo impulsadas debido a sus capacidades avanzadas de (1) identificación, (2) verificación, (3) autenticación y (4) reconocimiento. En la práctica se observa que muchos en el campo generalmente no comprenden la diferencia entre las funciones de estas capacidades. La Tabla 3 ofrece una definición de cada una.

En el contexto de las capacidades de arriba, la biometría ha recorrido un largo camino. Desde la catalogación impresa a mano en 1858 de los empleados Indios por día de paga por Sir William Herschel; a la impresión de huellas digitales de los delincuentes en La Prisión del Estado de Nueva York de 1903; al Programa de Visita de los Estados Unidos; a la base de datos biométricos más grande del mundo en la India para la entrega de beneficios sociales, la biometría está llegando a la mayoría de edad.

En la última década, la industria ha visto desarrollos notables en el campo de los métodos de almacenamiento y procedimientos de inscripción y verificación. Las huellas dactilares físicas tomadas pasando los dedos por tinta indeleble han cedido el paso a la captura de la imagen de las huellas dactilares por medio de sensores electrónicos. Las fotos que ofrecen un reconocimiento facial han cedido el paso a los sistemas de análisis que capturan la geometría interna del cráneo y la detección de la textura de la piel.

El reconocimiento del color de ojos/retina ha evolucionado hacia un reconocimiento del iris que no puede ser falseado. Se han desarrollado Sensores Electrónicos que capturan con precisión características biométricas diferentes para que puedan ser almacenadas como plantillas que pueden ser reconocidas electrónicamente. La Tabla 4 muestra una lista de las tecnologías biométricas que están evolucionando y ganando diversos niveles de aceptación en varios segmentos de la industria.

A la luz de la gran velocidad de los avances tecnológicos en biometría, la industria ha sido testigo de los acelerados esfuerzos de estandarización para sustentar el intercambio e interoperabilidad de los distintos sistemas. La próxima sección describe una breve visión de los estándares biométricos existentes que fueron desarrollados para facilitar la interoperabilidad de los sistemas biométricos y acrecentar la efectividad de los productos y procesos biométricos.

1.3 Evolución de los Estándares Biométricos

Desde el punto de vista técnico, los estándares fueron desarrollados de modo que las plantillas sean generadas, almacenadas y recuperadas en forma uniformada. El principal ímpetus de los estándares biométricos es definir las especificaciones de los requerimientos, formatos y software que permitan la interoperabilidad entre los sistemas biométricos, especialmente los sistemas de autenticación. Los estándares biométricos permiten diferentes flujos de interoperabilidad. Un flujo de los estándares permite la interoperabilidad de las recolecciones de datos y los procesos almacenados. El otro flujo permite la interoperabilidad del procesamiento de la señal y las tecnologías para verificar las coincidencias.

La evolución de los estándares significa la madurez de la tecnología y la tecnología está diseñada para permitir un vasta adopción de la biometría por parte del gobierno. Ofrece un campo de juego a nivel de los proveedores de dispositivos y un intercambio de información a niveles nacional e internacional. Esto equivale a decir que los estándares reducen el riesgo para el integrador y el usuario final también, porque simplifica la integración y permite la sustitución y actualización de las tecnologías, y reduce los efectos de las “restricciones de vendedor fijo” (Tilton, 2006). Esto probablemente conduca a un rango y disponibilidad más amplios de productos y movimientos hacia una mayor indiferenciación (comoditización) (*ibid*).

Aún hay un largo camino a recorrer para los estándares que se desarrollan para ser adoptados uniformemente en todo el mundo. Los estándares biométricos han sido desarrollados por organizaciones de estándares informales y formales. En general, las siguientes organizaciones están activamente involucradas en el desarrollo de los estándares y su adopción:

- Comité Internacional para Estándares de la Tecnología de la Información (INCITS) M1
- Instituto Nacional de Estándares y Tecnología (NIST)
- Comité Técnico Conjunto 1 (JTC 1)/Subcomité 37 (SC 37)
- Organización para el progreso de Estándares de Información Estructurados (OASIS)
- Organización de Estándares Internacionales (ISO)

Los estándares desarrollados por estas organizaciones ofrecen un buen indicio sobre el estado actual de las tecnologías biométricas. Actualmente, hay gran madurez y consenso y se han difundido documentos de estándares definitivos. Ellos incluyen, pero no están limitados a: Interfaces Técnicas, Formatos de Intercambio de Datos, Estándares de Perfil de Aplicación y Prueba de Comportamiento.¹ Estos se describirán brevemente a continuación.

1.3.1 Interfases Técnicas

Estos estándares están relacionados con la captura de interfaces biométricas e interacciones entre componentes biométricos y subsistemas junto con mecanismos de seguridad para proteger los datos almacenados y los datos transferidos entre sistemas. También incluyen especificaciones de arquitectura y operación de sistemas biométricos para sustentar los sistemas multi-vendedores y sus aplicaciones. La especificación v1.1ANSI INCITS 358-2002 BioAPI, ANSI INCITS 398-2005 [NISTIR 6529-A] el Formato de Archivo de Intercambio Biométrico en Compón (CBEFF) son ejemplos de los Estándares de Interfaz Técnica.

¹ Referirse a la pág. 138 Biometrics “Foundation Documents” y al documento “Biometric Standards” publicado por el Sub Comité de Biometría para Bio-Estandares de NISTC.

1.3.2 Formato de Intercambio de Datos

Estos estándares especifican el contenido, significado y representación de formatos para el intercambio de datos biométricos, por ej. Formato de Intercambio Basado en Patrón Dactilar, Formato de Minutiae Dactilar para Intercambio de Datos, Formato de Reconocimiento Facial para Intercambio de Datos, Formato de Intercambio Imagen del Iris, Formato de Intercambio Basado en Imagen Dactilar, Formato de intercambio Basado en Imagen de Firma/Signo, y Formato de Intercambio de Geometría de la Mano; y anotación de especificación y formatos de transferencia que ofrecen una independencia de plataforma y una separación de la sintaxis de transferencia de la definición del contenido. Los ejemplos incluyen Formato de intercambio Basado en Patrón Dactilar ANSI INCITS 377-2004, Formato de Minutiae Dactilar para Intercambio de Datos ANSI INCITS 378-2004, y Formato de Intercambio de Imagen del Iris ANSI INCITS 379-2004.

1.3.3 Estándares de Perfil de Aplicación

Estos estándares especifican uno o más estándares base y perfiles estandarizados, y donde fuere aplicable, la identificación de las clases elegidas, subjuegos en conformidad, opciones y parámetros de aquellos estándares base o perfiles estandarizados necesarios para cumplir con una función en particular. Algunos de estos estándares son: ANSI INCITS 383-2003 – Verificación e Identificación Basada en Biometría para los Trabajadores del Transporte – y ANSI INCITS 394-2004 – Intercambio de Datos e Integridad de Datos de la identificación de Personas Basada en Biometría para Gestión de Fronteras.

1.3.4 Prueba e Informe de Rendimiento (Performance): Estos juegos de estándares especifican definiciones y cálculos de métrica de performance biométrica, enfoques de la performance de las pruebas, y requerimientos para informar los resultados de estas pruebas. Los ejemplos incluyen ANSI INCITS 409.1-2005 – Prueba e Informe de Performance Biométrica Parte 1 – Marco de Principios; ANSI INCITS 409.2-2005 Prueba e Informe de Performance Biométrica Parte 2 – Metodología de Prueba de Tecnología; y ANSI INCITS 409.3-2005 Prueba e Informe de Performance Biométrica Parte 3 – Metodología de Prueba de Escenario.

Estos estándares junto con otros establecen la madurez de la biometría como una tecnología para la identificación de personas. Sin embargo, se debe observar que no hay ninguna característica biométrica que pueda ser considerada como una solución a prueba de bala. El uso de las características de la biometría dependen enteramente de la aplicación.

Las aplicaciones de la biometría están dictadas por las circunstancias, datos disponibles, evaluación de seguridad y riesgo, cantidad de gente a ser cubierta y sucesivamente. Por ejemplo, en los EEUU con una inmensa base de datos de huellas dactilares de delincuentes, la detección de los delitos resulta relativamente más fácil para que los Investigadores de la Escena del Crimen recolecten huellas dactilares de la escena del crimen y que busquen la coincidencia con huellas conocidas.

Con la recolección de los nuevos datos biométricos de visitantes (huella dactilar, rasgos faciales), los EEUU, el Reino Unido y otros países europeos están buscando asegurar sus fronteras contra ingresantes no autorizados. El proyecto de la India que está considerado como el ejercicio biométrico más grande del mundo busca capturar huellas dactilares de sus 1.3 billones de

habitantes con el fin de asegurar una entrega transparente de beneficios sociales a los individuos autorizados.

La tecnología de huella dactilar tiene más amplia aceptación mundialmente debido a que los costos de implementación son más bajos en comparación con otras biometrías, y la disponibilidad de un rango más amplio de aplicaciones comerciales en la industria. Sin embargo, la huella dactilar como una característica biométrica no está libre de problemas. Por ejemplo, cualquier daño en los dedos inutiliza las huellas dactilares existentes. Más aún, es muy difícil escanear huellas dactilares y construir plantillas para dedos ásperos o con cortes y lesiones.

Estos tipos de temas necesitan nuevas tecnologías biométricas, nuevos sensores para la detección y mejores algoritmos de computación para mejorar la calidad en la inscripción y detección. La siguiente sección intenta ofrecer una visión de alto nivel acerca de los desarrollos en la industria biométrica.

1.4 Avances en Biometría

Los recientes avances en las tecnologías y la computación han permitido que la biometría evolucionara y se convirtiera en un método definitivo y legalmente aceptado para la identificación de personas. Desde los días de la catalogación de las huellas dactilares y el establecimiento de una coincidencia en forma manual, las técnicas informáticas hoy han transformado a la biometría.

Impulsadas por la necesidad de tener características más auténticas para determinar la identidad, algunas tecnologías biométricas se han robustecido en la última década. La biometría facial multimodal con reconocimiento facial 3D es una de las técnicas que se han trasladado desde los laboratorios al dominio comercial para una producción masiva.

Por el otro lado, en la última mitad de la década, el iris ha avanzado enormemente como un rasgo biométrico definitivo. El iris es ahora un rasgo biométrico común utilizado en los controles fronterizos en muchos países del mundo. Complementado con el reconocimiento facial 3D, el tema de tomar el iris en vivo ha sido superado en un alto grado.

Sin embargo, aún no es completamente confiable en aplicaciones no supervisadas. En entornos supervisados, el reconocimiento del iris presenta resultados excelentes. Una de las conocidas implementaciones del iris son los Emiratos Árabes Unidos donde la detección del iris está implementada para monitorear a todos los visitantes. Esta implementación es una de las historias de éxitos más grande y reciente en cuanto a tecnología del iris en el mundo (Al-Raisi and Al-Khoury, 2006). Ver también la Sección 3 en este artículo.

Las tecnologías de huella dactilar ahora usan los diez dedos incluyendo la palma. Como las bases de datos de huella dactilar se tornan cada vez más grandes, ya no se considera definitiva con uno o dos dedos. Lo ultimo en geometría de la mano es el reconocimiento de las Venas de la Palma. Actualmente Fujitsu tiene la patente para el reconocimiento de las venas de la palma y los escáneres, detectores y lectores están comercialmente disponibles usando esta tecnología. El escáner de venas de la palma trabaja capturando las imágenes de los patrones venosos que están dentro del cuerpo sin contacto, que lo hace más estéril e higiénico para utilizar. Ver

también la Figura 4. Esto hace difícil falsear los patrones de las venas de la palma, y por lo tanto más es seguro. La tecnología de reconocimiento de las venas de la palma tiene una de las tasas de aceptación falsa (FAR) y tasas de rechazo falso (FRR) más bajas, es decir una tasa de rechazo falso de 0.01% y una tasa de aceptación falsa menor de 0.00008% (Sarkar et al., 2010).

Se espera que el Reconocimiento de las Venas de la Palma sea el determinante biométrico principal y que supere muchos inconvenientes que las actuales huellas dactilares conlleven. Ésta es la tecnología que promete un buen toque de entusiasmo en los días venideros.

Además de la tecnología, los avances más importantes han tenido lugar en el dominio de la computación. La habilidad para implementar grandes bases de datos relacionales con motores de búsqueda rápidos ha agilizado los tiempos de detección e identificación. La identificación de una persona se ha tornado más fácil y rápida con la habilidad de coincidencias 1:n en bases de datos inmensas.

Esto ayudó a las instituciones de orden público muchas veces. La tecnología de computación y redes ha colaborado para intercambiar datos y compartir información en forma más fácil y rápida. Esto dio por resultado que las naciones pudieran compartir mejor la inteligencia. Hay numerosas iniciativas mundiales para asegurar estándares en comunicación y protocolos para el intercambio de datos. Estos estándares han tornado la interoperabilidad de sistemas más fácil y eficiente.

Finalmente, pero no en menor grado, está el progreso alcanzado en el dominio de la calidad. Se han establecido estándares de calidad para la captura de plantillas biométricas. El NIST (National Institute of Standards & Technology) lanzó el NFIQ (NIST Calidad de la Imagen de Huella Dactilar) en 2004 y buscó estandarizar el algoritmo para la coincidencia de minutiae de huella dactilar. ISO estuvo activo a través de su Sub Comité SC 37 en la definición de varios estándares biométricos incluyendo el intercambio de datos, BioAPIs, formatos y almacenamiento de datos de huella dactilar.

Actualmente hay muchos más estándares bajo desarrollo bajo el SC 37- por ejemplo: metodología para las pruebas de conformidad (por ej. ISO/IEC 19794-9/PDAM 1); procedimientos para la operación de la Autoridad de Inscripción Biométrica - ISO/IEC DIS 19785-2, para citar unos pocos.² Otras dos organizaciones activamente involucradas en el desarrollo de estándares para biometría son el INCITS (International Committee on Information Technology Standards) MI, y OASIS (Organization for the Advancement of Structure Information Standards).

Estos estándares y la evolución de la calidad en biometría prometen mayores avances en la tecnología de detectores biométricos. Mejores sensores ofrecen mayor sensibilidad, mejor resolución y mayor repetitibilidad. Esto contribuye a valores más bajos de Tasas de Rechazo Falso (FRR), Tasa de Aceptación Falsa más baja (FAR) y mejores Tasas de Cross-over Error (CER). En los últimos años, los avances en las tecnologías de detección han permitido velocidades y resultados de rendimiento más altos. Las tasas de rendimiento más altas significaron mayor cantidad de capacidad de inscripción y procesamiento. Dichos avances han cimentado el

² Referirse al Sitio Web ISO: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770

camino para que varios gobiernos iniciaran programas de inscripción masivos a nivel nacional para capturar la biometría de su población.

Tecnología Biométrica	¿Cómo funciona?
Huellas dactilares	Una huella dactilar está compuesta de una serie de crestas y surcos sobre la superficie del dedo. La unicidad de una huella dactilar puede determinarse por el patrón de crestas y surcos tanto como por los puntos de minucia. Los puntos de minucia son características de crestas locales en la bifurcación de la cresta o en los extremos de una cresta.
Escaneo del Iris	Uno de los procesos biométricos más precisos en el cual se encuentra la estructura de las venas del iris que se utiliza como una muestra biométrica para identificar a una persona. Por ser un órgano interno del ojo cuya textura es estable a lo largo de toda la vida, el iris es inmune (a diferencia de las huellas dactilares) a las influencias del medioambiente, excepto por su respuesta papilar a la luz. Trabajando sobre principios completamente diferentes desde el escaneo de retina, el reconocimiento del iris es mucho más fácil de utilizar y ofrece una elevada precisión.
Reconocimiento facial	El reconocimiento facial es un método automático para registrar la geometría especial de rasgos distintivos del rostro. La falta de cooperación del usuario en factores ambientales, tales como condición de luz, pueden degradar el comportamiento de las tecnologías para reconocimiento facial.
Reconocimiento de la voz	Se enfoca sobre las diferencias que resultan de la forma de los tractos vocales y los hábitos de habla aprendidos. La tecnología no está bien desarrollada dado que el ruido de fondo afecta su comportamiento y confiabilidad.
Impresión palmar /geometría de mano	Captura de mediciones que comprenden al ancho, altura y longitud de los dedos, distancias entre las articulaciones y las formas de los nudillos. Aunque sean razonablemente diversas, la geometría de las manos de un individuo no es necesariamente única.
Escaneo de retina	Mediciones de los patrones venosos en la parte posterior del ojo. Como la retina puede cambiar con ciertas condiciones médicas, tales como embarazo, alta presión, y SIDA, su biometría tiene el potencial de revelar más datos sobre individuos que sólo su identidad, se la percibe como una tecnología invasiva y ha perdido popularidad en los usuarios finales.
Imagen del patrón venoso	La imagen del patrón venoso (vascular) de la mano de un individuo puede ser capturada por radiación de rayos infrarrojos cercanos. Puede realizarse usando el método de reflexión para fotografiar las venas en la mano iluminando la palma y fotografiando la luz reflejada desde la parte posterior de la palma.
ADN	Con excepción de los mellizos idénticos, el ADN de cada persona es único. Por lo tanto puede ser considerada como la modalidad 'perfecta' para verificación de la identidad. Las técnicas de identificación de ADN observan áreas específicas dentro de la larga secuencia de ADN humano, que se conoce que varían ampliamente entre personas. La precisión de esta técnica es por lo tanto muy alta, y permite tanto la identificación como la verificación.
Reconocimiento del andar	Captura una secuencia de imágenes para el análisis de como camina un individuo. Aún en una etapa temprana de investigación y desarrollo.

Reconocimiento del ritmo de tipo	Evaluá el estilo de tipo del usuario, incluyendo cuánto tiempo cada tecla es presionada (tiempo de detención), tiempo entre tipo de teclas (tiempo de vuelo) y errores de tipo típicos. Es más apropiado como una tecnología de seguridad interna, tal como suministrar el acceso a computadores dentro de una organización.
Reconocimiento de la firma	Analiza una serie de movimientos que contienen datos biométricos únicos tales como el ritmo personal, aceleración y flujo de presión. Dado que los movimientos pueden variar con cada firma, la diferenciación entre las partes consistentes y conductuales de una firma es difícil.

Tabla 4: Evolución de las tecnologías biométricas

Manos abajo, cómo funciona la identificación de escaneo de la palma:

el escáner emite luz infrarroja. La hemoglobina en las venas absorben la luz...



...creando una imagen del patrón venoso que es reflejado y capturado por el escáner

El escaneo se almacena en una base de datos. Un patrón venoso de un usuario que retorna se compara contra la base de datos para determinar si hay una coincidencia.

Figura 4: Reconocimiento de las Venas de la Palma

2. Programas de Biometría Gubernamentales: permitiendo las iniciativas de la nueva economía

El manejo de la identidad ha sido siempre un desafío clave para los gobiernos en todo el mundo. Los gobiernos se han esforzado para brindar a sus ciudadanos seguridad y protección, fácil acceso a través de las fronteras nacionales y asegurar que los beneficios sociales llegaran a los ciudadanos con derecho a y merecedores de ellos. Los gobiernos hoy en día y a esta edad buscan métodos probados para establecer las identidades de su población a fin de asegurar el acceso a las aplicaciones y servicios gubernamentales. La Tabla 5 resume un modelo genérico utilizado para identificar los requerimientos para la entrega de beneficios y acordar de privilegios.

En el pasado, los servicios o beneficios entregados a través de diferentes canales debían estar severamente limitados debido a la falta de una verificación creíble de la identidad de los beneficiarios. Los ciudadanos debían necesariamente presentarse en las oficinas gubernamentales que demandaban diferentes controles de identificación para verificar la identidad de quien reclamaba un beneficio. No es necesario decir que los gobiernos confiaban fuertemente en la información biográfica para manejar la identidad de sus ciudadanos. Los pasaportes, aunque eran considerados documentos de viaje, fueron considerados como el documento de identidad principal en varios países de todo el mundo.

Muchos países han hecho intentos de ofrecer métodos de identificación más simples en términos de papel basados en tarjetas de identidad que portaban la foto de la persona. Estos

documentos de identidad cumplían con un propósito limitado dado que la identidad en gran medida dependía de la foto y era fácil reproducir o falsear esos documentos. Las tarjetas de identidad en papel fueron luego reemplazadas por tarjetas plásticas. Se adoptaron las tarjetas plásticas con estampado en relieve, marcas de agua, hologramas para reducir el riesgo de tarjetas falseadas. Todos estos enfoques se encontraron con un éxito limitado debido a las limitaciones de uso y aplicaciones de diferentes necesidades comerciales.

Los gobiernos en el mundo implementaron copiosos programas de manejo de la identidad en los últimos 10 años que se dirigieron a necesidades estratégicas discretas. Una de las aplicaciones más tempranas e importantes fue en el dominio de la seguridad de frontera. Los sistemas de seguridad de frontera difieren entre los países, sin embargo, en general, todos los visitantes y residentes normalmente necesitan solicitar una visa o un equivalente de visa, con condiciones apropiadas con su estadía. Esta visa es verificada en la frontera y pasa a través de una cantidad de capas de control, muchas desconocidas para el viajero, y si se encuentra que es genuina y auténtica, se permite que la persona que porta la visa ingrese al país.

Las visas son producidas en forma de papel y adheridas a los pasaportes. Las visas de papel están plagadas de problemas. Hay una preocupación importante para la seguridad en la frontera. La necesidad de un manejo más efectivo de las fronteras nacionales y el fraude de identidad trajó aparejado una mayor demanda de sistemas de identidad punta-a-punta seguros.

Aplicación	Comentarios
Identificación simple	Verificación de Seguridad e Identificación Física.
Se requiere Documento de Identidad para ser ingresado como dato	Se requiere Documento de Identidad como elemento en los Formularios de Solicitud de Servicio.
Servicio requerido en mostrador <i>(over the counter)</i>	Se requiere Documento de Identidad para asegurar que es la persona correcta que presenta la solicitud.
Servicio a ser entregado en Mostrador <i>(over the counter)</i>	Se requiere Documento de Identidad para asegurar que es entregado a la persona correcta y requiere confirmación de entrega del servicio (firma del beneficiario del servicio).
Servicio Requerido Remotamente	Ingreso Manual del Documento de Identidad en Formularios de Solicitud.
Servicio a ser suministrado remotamente	Se requiere Documento de Identidad para asegurar que está siendo entregado a la persona correcta y que requiere confirmación de suministro del servicio.

Tabla 5: Requerimientos de identidad para el suministro de servicio por parte del gobierno

Las tecnologías biométricas han surgido como componentes críticos de los programas de identidad y seguridad. Con el tipo de confiabilidad y aceptación que las huellas dactilares, el reconocimiento facial y el reconocimiento del iris han ganado en la última década, complementados por los avances en las técnicas de computación, la biometría está siendo cada vez más utilizada internacionalmente como una herramienta de manejo de la identidad de alta tecnología para fortalecer los procesos de identificación. Ver también la Figura 5.

Evidentemente, hubo y continua habiendo numerosos intentos por parte de los países para enumerar sus ciudadanos, enlistarlos, registrarlos y lo que es más importante, identificarlos. La Tabla 6 ofrece una visión global de las aplicaciones biométricas por los gobiernos mundialmente. Los EEUU, la India, los EAU, Malasia, Corea del Sur, el Reino Unido y Francia han sido mencionados anteriormente en cuanto a que han tomado el liderazgo en la implementación de la biometría para la Seguridad de Fronteras. El ingreso de visitantes a estos países está regulado por las huellas dactilares a ser recolectadas en el momento de otorgar la aprobación para visitar el país (Emisión de Visa). Las huellas dactilares son verificadas al momento del ingreso real y si coinciden, se concede el ingreso.

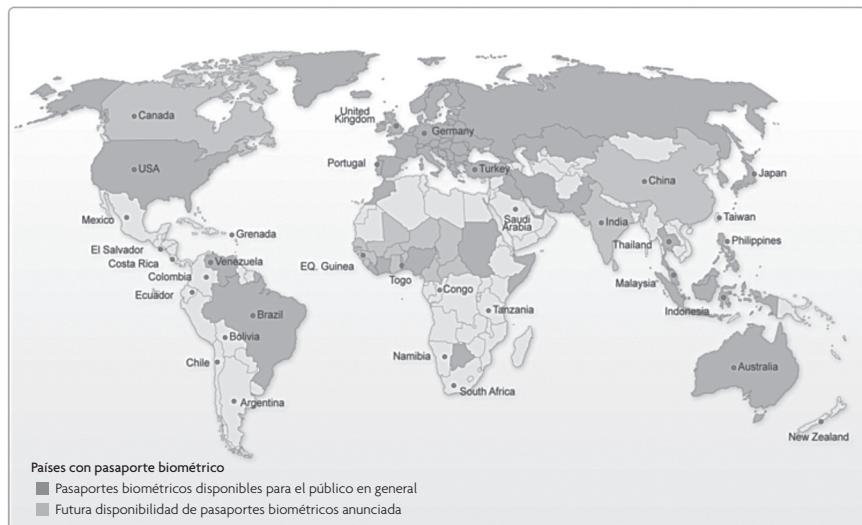


Figura 5: Adopción global de la biometría.

2.1 Roles emergentes de los gobiernos

La globalización y el rápido avance del desarrollo en las tecnologías de la información y las comunicaciones están redefiniendo la naturaleza de los gobiernos y sus relaciones con los ciudadanos (Guthrie, 2003). Con tales desarrollos, los servicios públicos tienen el desafío de reinventar al gobierno en la economía digital.

Esto requiere repensar la forma en que los gobiernos se han relacionado con los ciudadanos y empresas, hacer re-inginería de sus procesos de trabajo, y también facilitar una mayor colaboración entre instituciones para entregar servicios en una forma que el público aprecie (*ibid*). Como tal, el manejo de la identidad es un factor de éxito crítico para permitir tal transformación. Se diseñó una infraestructura de manejo de la identidad robusta para permitir la economía digital, con sistemas de identificación y autenticación con los cuales las personas puedan vivir, confiar y usar. (Stevens et al., 2010).

Hay evidencia acumulada de que los gobiernos son fuentes de fuerzas poderosas que influyen en el desarrollo de nuevas industrias (Ke and Wang, 2008). Aún, los gobiernos, como un contexto válido y poderoso tienen el potencial de influir en la creación de la economía digital (*ibid*).

País	Aplicaciones Biométricas
Canadá	<ul style="list-style-type: none"> • 2005: Reconocimiento del iris en aeropuertos para agilizar a los viajeros pre-aprobados para pasar aduana e inmigración • 2011: Lanzamiento del sistema fronterizo de ingreso e inmigración basado en huellas dactilares
EEUU	<ul style="list-style-type: none"> • 1999: Se pone en funcionamiento el IAFIS (Integrated Automated Fingerprint Identification System) del FBI con la base de datos más grande del mundo con cerca de 55 Millones de registros. • 2008: FBI expande su base de datos con NGI (Identificación de Nueva Generación) para incluir biometría multimodal (facial, iris, huellas digitales y patrones de la palma) • 2004: US-VISIT (US-Visitor and Immigrant Status Indicator Technology) lanzada para control fronterizo con total integración de IAFIS como el objetivo • 2007: Pasaportes electrónicos emitidos con Control de Acceso Básico y PKI
Méjico	<ul style="list-style-type: none"> • 2009: El gobierno mejicano anuncia una nueva tarjeta de identidad que portará las huellas dactilares, un escaneo de retina y una fotografía en la banda magnética para luchar contra la corrupción en los planes sociales bajo el Ministerio del Interior mejicano (Instituto Mexicano del Seguro Social).
Salvador	<ul style="list-style-type: none"> • 1999: Lanzamiento de la iniciativa de Licencias de conductor basadas en huellas dactilares • 2007: Comenzó la implementación del Pasaporte Biométrico Multimodal y luego extendido para incluir al sistema de justicia penal además del control Fronterizo.
Costa Rica	<ul style="list-style-type: none"> • 1998: Iniciativa del Documento de Identidad Nacional con huellas dactilares y fotos lanzado para reemplazar a las tarjetas de identidad con base papel • 2003: El Banco Central lanza un sistema de identificación biométrico para asegurar el acceso a las bases de datos del banco para bancos miembro • 2010: Iniciativa de Tarjetas Inteligentes lanzadas para asegurar la información biométrica en las tarjetas
Colombia	<ul style="list-style-type: none"> • 1995: Reforma de Identificación Digital para introducir información biométrica en formato digital para la inscripción Civil Nacional y emisión de nuevas tarjetas de identidad con fines electorales y de transacciones civiles. • 2005: Máquinas Automáticas para Bancos introducidas para transacciones de cajero automático usando biometría • 2009: El gobierno de Colombia hace cambios significativos a la Cédula y solicita a todos los ciudadanos que pasen al documento de identidad nacional para las elecciones presidenciales del 2010.
Granada	<ul style="list-style-type: none"> • 2009: Inicia el Programa de Registro de Identificación Civil como parte de la iniciativa del Caribe para fines Electorales y de Identificación Civil
Venezuela	<ul style="list-style-type: none"> • 2007: Lanza la Tarjeta de Identidad Nacional con datos faciales y huella dactilar modernizando el Registro Civil para el sistema electoral y las transacciones civiles..
Ecuador	<ul style="list-style-type: none"> • 2007: Parte de la iniciativa CLARIEV en preparar el registro civil con identificación biométrica de foto y huella dactilar. • 2009: Lanzó el Sistema de Escaneo Biométrico para Extranjeros en varios puntos de entrada para prevenir que ingresen ilegales de países vecinos.
Bolivia	<ul style="list-style-type: none"> • 2009: Se condujo la Inscripción Biométrica de ciudadanos elegibles y se creó una base de datos biométricos de la Lista de Votación Electoral. Condujo exitosamente las Elecciones Presidenciales usando base de datos biométricos.
Brasil	<ul style="list-style-type: none"> • 2007: Tarjeta de Identidad Nacional con Datos Biométricos para reemplazar a las tarjetas de cartón

	<ul style="list-style-type: none"> • 2011: Tarjetas Inteligentes de Nueva Generación – llamado el Registro de Identidad Civil (Registro de Identidade Civil – RIC) con características de seguridad mejoradas para los datos biométricos y huella dactilar y datos faciales que fueron lanzadas y se espera que reemplacen a todas las tarjetas existentes para el año 2019 • 2010: Usa base de datos biométricos para conducir las elecciones usando la biometría como la identificación principal para los votantes
Argentina	<ul style="list-style-type: none"> • 2010: Relanza el Documento de Identidad Nacional en la forma de libreta Pasaporte incluyendo información biométrica de datos de huella digital y faciales • 2011: Lanza la inscripción biométrica para Documento de Identidad y viajes para expatriados que viven fuera de la Argentina y también para visitas extranjeras que viajen a la Argentina.
Chile	<ul style="list-style-type: none"> • 1997: Uso ampliado de la Biometría para los registros Penales • 2007: Parte de CLARIEV- iniciativa de Registro Civil • 2007/8: Implementación del Laboratorio de Investigación Biométrica para validar la base de datos de identificación Facial/Iris, con punto de referencia para la búsqueda de algoritmos para 1:N en una base de datos de 16 Millones de registros
Togo	<ul style="list-style-type: none"> • 2009: De acuerdo con su compromiso con la Comunidad Económica de los Estados Africanos (ECOWAS), Togo adopta los Pasaportes Biométricos que contienen información no repudiada de huellas dactilares para fortalecer el acceso fronterizo. Los pasaportes que no pueden ser leídos por máquina se dejaron de usar en 2010, junto con las Naciones Africanas de ECOWAS (a saber Nigeria, Nigeria, Guinea, Senegal, Costa de Marfil, Liberia, Benín y Ghana) –Togo, ha emitido pasaportes Biométricos a sus ciudadanos.
EQ. Guinea	<ul style="list-style-type: none"> • 2010: Se establece la Comunidad Económica y Monetaria de los Estados Africanos Centrales (CEMAC) para poner en circulación los pasaportes biométricos dentro de sus estados miembro. Los miembros de CEMAC son Camerún, Congo, África Central Africana, Gabón, Guinea Ecuatorial y Chad.
Congo	<ul style="list-style-type: none"> • 2004: Congo lanza un sistema de identificación basado en el iris para la rehabilitación de ex-combatientes de la Guerra a la vida civil. Este programa - El Programa Nacional de Desarme, Desmovilización, y Reinscripción (PNDRR) demostró ser altamente exitoso. • 2010: Lanza los Pasaportes Biométricos bajo el programa CEMAC.
Tanzania	<ul style="list-style-type: none"> • 2011: La Autoridad Nacional de Identificación lanza el sistema para emitir 25 millones de tarjetas de identidad Inteligentes biométricas para identificación y uso civil. • 2011: Puestos de Autenticación Biométrica implementados como parte de las iniciativas de gobierno electrónico para permitir a los ciudadanos elegibles el acceso a los fondos de Seguridad Social y realizar transacciones electrónicamente a través de estos puestos.
Namibia	<ul style="list-style-type: none"> • 2007: Registro de Conductor Biométrico implementado y en acción
Sudáfrica	<ul style="list-style-type: none"> • 2002: Se introdujo el AFIS para colaborar en la justicia penal, digitalizando alrededor de 4.5 Millones de registros penales y huellas dactilares recolectadas desde 1920. • 1993: Se lanzó el HANIS (Sistema de identificación Nacional de Asuntos Internos) con la recolección de datos biométricos como parte de la libreta de identificación emitida con un Código de Barras 2D. • 2010: Se inició la Tarjeta de Identificación Inteligente con datos Biométricos
Alemania	<ul style="list-style-type: none"> • 2010: Se inició el uso de Tarjetas Inteligentes basadas en RFID con datos digitales incluyendo información biométrica para reemplazar las tarjetas de identificación plásticas normales • 2003: Se introdujo AFIS para visitantes a Alemania como parte de la Visa Schengen

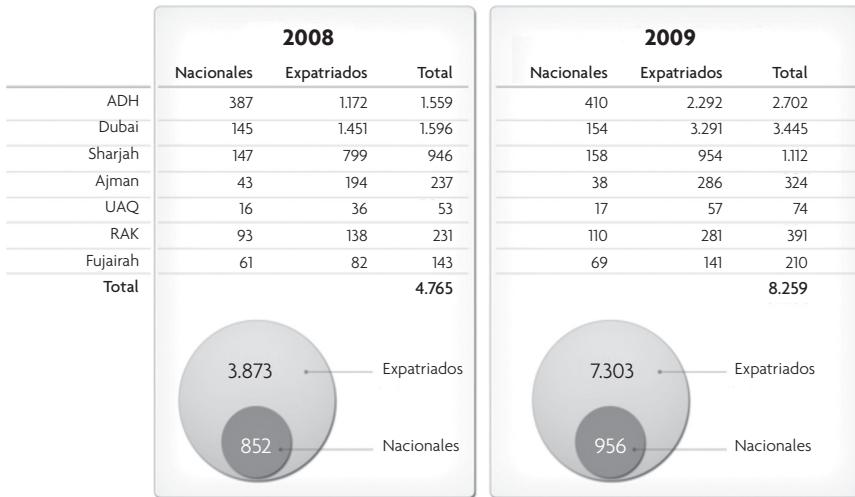
	<p>para identificación biométrica. Se registra el iris en los Aeropuertos a la entrada para monitorear a los visitantes</p> <ul style="list-style-type: none"> • 2005: El Sistema de Pasaportes electrónicos con datos biométricos integrados tiene imagen facial como principal identificador biométrico • 2007: Se entregó el Segundo Pasaportes electrónico Gen con huella dactilar como el principal identificador cumpliendo con las reglamentaciones de la UE en eMRTD • 2010: Los datos biométricos permitieron que se comenzara a emitir las Tarjetas Inteligentes RFID como Tarjetas de Identidad Nacionales
Reino Unido	<ul style="list-style-type: none"> • 2001: Una identidad formal - El BWG (Grupo de Trabajo Biométrico) establecido bajo el CESG (Grupo de Seguridad en Comunicaciones - Electrónica). El BWG del Reino Unido es un grupo gubernamental interdisciplinario enfocado en el uso de la tecnología biométrica en todo el gobierno y la Infraestructura Nacional Crítica (CNI). • 2005: Reconocimiento del Iris y Huella Dactilar para los poseedores de visa y viajeros frecuentes para el Control Fronterizo. • 2006: Pasaportes electrónicos con datos Biométricos, los datos de huella dactilar, iris y facial comenzaron a ser emitidos a los británicos en cumplimiento con el Programa de Exención de visa a US. • 2010: Segunda Generación de Pasaportes electrónicos con características de seguridad mejoradas.
Portugal	<ul style="list-style-type: none"> • 2006: Se emitieron pasaportes electrónicos en conformidad con los estándares de la UE. • 2007: Tarjetas de Identidad Nacionales con datos de huella dactilar, foto y firma digital emitidos a los ciudadanos. • 2007: El Aeropuerto Portugués Faro pasa a ser el primer aeropuerto en empezar a usar la lectura del pasaporte electrónico biométrico para un control de ingreso rápido al país seguido por Lisboa.
Turquía	<ul style="list-style-type: none"> • 2007: Tarjetas inteligentes con información personal y datos de huella dactilar lanzados para servicios de Atención de la Salud. • 2010: Pasaportes electrónicos con reconocimiento de huella dactilar y facial lanzados en Turquía
Arabia Saudita	<ul style="list-style-type: none"> • 2006: Comienza a emitir tarjetas inteligentes con datos biométricos como Tarjeta de Identidad Nacional para todos los ciudadanos y residentes como el primer Documento de Identidad para transacciones civiles. • 2010: A. Saudita anuncia el requerimiento de huellas dactilares para todos los visitantes como parte de la identificación para seguridad fronteriza. • 2003: Comienza a emitir la Tarjeta Inteligente basada en Tarjetas de Identidad Nacional con datos de huella dactilar.
EAU	<ul style="list-style-type: none"> • 2003: Los EAU es el primer país en comenzar el reconocimiento del iris para todos los visitantes en el aeropuerto de Dubai y subsiguientemente lo extendió a todos los aeropuertos internacionales del país. • 2005: Comienza a emitir Tarjetas Inteligentes como Tarjetas de Identidad Nacionales basadas en un chip con datos biométricos (huella dactilar), foto y firma digital para firmar. • 2010: Comienza a emitir Tarjetas de Identidad de segunda generación con capacidades RFID como una tarjeta combi (combi-card) • 2004: La tarjeta biométrica para Puerta de Embarque Electrónico fue lanzada y emitida a los residentes y ciudadanos para un rápido registro de entrada y salida de los aeropuertos del país basada en identificación de huella dactilar • 2009: Programa de Pasaporte Biométrico lanzado con RFID y datos de huella dactilar que pueda ser leído por máquinas.

	<ul style="list-style-type: none"> • 2011: Las Elecciones Nacionales se llevaron a cabo con la ayuda de las Tarjetas de Identidad Nacionales con verificación biométrica de los votantes.
Bahrein	<ul style="list-style-type: none"> • 2005: Introduce la Tarjeta de Identidad basada en Tarjeta Inteligente con datos de huella dactilar para identificación y autenticación para reemplazar la tarjeta CPR en forma progresiva. • 2009: Instala escáneres biométricos y puertas de inmigración altamente seguras en sus aeropuertos, siendo el tercer país luego del Reino Unido y Japón para hacerlo.
Qatar	<ul style="list-style-type: none"> • 2006: Introduce la Tarjeta de Identidad basada en Tarjeta Inteligente con datos de huella dactilar, rasgos faciales y datos del iris junto con datos personales para reemplazar su tarjeta de Identidad plástica existente.
Omán	<ul style="list-style-type: none"> • 2004: Lanza el Sistema de Registro Nacional para emitir tarjetas inteligentes como la Tarjeta de Identidad Electrónica con información biométrica embebida con seguridad en las tarjetas de identificación para todas las transacciones civiles
Kuwait	<ul style="list-style-type: none"> • 2009: Lanza las nuevas Tarjetas de Identidad inteligentes para las Tarjetas de Identidad Civiles que incluyen información de huella dactilar y ADN como datos biométricos para identificación de ciudadanos y residentes en el país. Los Datos Biométricos son parte del Registro Civil. Las capacidades incorporadas incluyen PKI para firmas digitales.
India	<ul style="list-style-type: none"> • 2009: India lanza el programa Bio-inscripción más ambicioso para la identificación de su población de 1,2 Billones. El programa apunta a suministrar una Identidad Única a todos los ciudadanos con huella dactilar como los identificadores primarios y también escaneo del iris. La meta principal del Documento de Identidad Biométrico es asegurar la distribución de los beneficios sociales a los ciudadanos con derechos y que se lo merecen y prevenir el robo de fondos sociales.
China	<ul style="list-style-type: none"> • 2005: Uno de los primeros adoptantes de la tecnología biométrica para el cruce de frontera automático – instala puertas de acceso biométrico entre Shenzhen y Hongkong, atendiendo cerca de 400.000 cruces diarios. Esto fue seguido en la frontera Zhejiang-Macau en 2006.
Tailandia	<ul style="list-style-type: none"> • 2005: Tarjetas de Identidad Inteligentes con datos biométricos de huella dactilar con capacidades Match-On-Card lanzadas para identificación personal.
Malasia	<ul style="list-style-type: none"> • 2011: Sistema de huella dactilar biométrico para todos los visitantes extranjeros ingresando a Malasia en los aeropuertos y otros puntos de ingreso (Singapore-Malaysia) • 2011: La Comisión Electoral adopta tecnología biométrica para la identificación del votante • 2005: MyKad- la Tarjeta de Identidad Nacional con capacidades de tarjeta inteligente lanzada con datos biométricos para la identificación de los titulares de las tarjetas que se extiende desde su iniciativa del 2011. • 2005: La Seguridad Informática de Malasia pasa a ser la única agencia de certificación para aplicaciones y lectores basados en tarjeta inteligente para la Certificación de Criterios Comunes en Malasia.
Japón	<ul style="list-style-type: none"> • 2007: Sistemas de Identificación Biométrica implementados en aeropuertos en todo el país y extendido a las fronteras en 2008 • 2006: Comenzaron a emitirse Pasaportes Biométricos cumpliendo el programa de Exención de Visa a EEUU a ciudadanos japoneses. • 2010: Uso extendido de Biometría en los Puestos y Cajeros Automáticos
Taiwán	<ul style="list-style-type: none"> • 2011: Sistemas de Control de Frontera Biométrico implementados a prueba • 2009: Pasaportes electrónicos biométricos lanzados para emitir pasaportes electrónicos a los ciudadanos Taiwaneses

Filipinas	<ul style="list-style-type: none"> • 1998: Tarjetas de Seguridad Social con datos biométricos emitidas a ciudadanos y residentes Filipinos para prevenir el fraude • 2009: Pasaportes electrónicos con datos biométricos para reemplazar a los pasaportes existentes. Todas las renovaciones se emitieron con nuevos pasaportes biométricos • 2010: El gobierno anuncia el registro biométrico para las Elecciones para el registro del Votante
Indonesia	<ul style="list-style-type: none"> • 2010: Lanza la verificación e identificación biométrica en el control de frontera de los aeropuertos • 2009: Se comienzan a usar los pasaportes biométricos como pasaportes electrónicos
Australia	<ul style="list-style-type: none"> • 2008: Se lanzaron los sistemas de control biométrico Puerta Inteligente • 2011: Australia busca establecer el Grupo de Trabajo en Biometría para guiar la implementación biométrica en toda la nación • 2006: Se lanzó el sistema de pasaporte electrónico biométrico
Nueva Zelanda	<ul style="list-style-type: none"> • 2006: Se lanzaron los sistemas de Inmigración Biométricos para control de frontera en los aeropuertos • 2009: Se implementó el Registro Biométrico para Inmigración y Pasaportes Biométricos para ciudadanos

Tabla 6: Prácticas internacionales de aplicaciones biométricas.

Población de Emiratos Árabes Unidos (en miles)



La literatura existente expresa que hay indicios suficientes de que debido a los efectos de externalidad de la red, los gobiernos necesitan tomar un rol activo en estimular un entorno para comenzar el camino hacia un nivel más alto de desarrollo electrónico.

De Meyer y Loh (2004) alegan que los gobiernos pueden jugar un rol importante en por lo menos cuatro áreas: (1) estimulando el acrecentamiento de la infraestructura que permite una sociedad electrónica (e-society); (2) invirtiendo en mejores servicios (e-government); (3) estimulando un entorno de negocios amigables con la electrónica (e-friendly); y (4) creando un sociedad de la

información inclusiva. Además sostiene que para que exista un entorno electrónico se necesita establecer una infraestructura TIC básica a fin de alcanzar a los ciudadanos y brindar una red robusta sobre la cual puedan operar las empresas.

La literatura en general, muestra gran desacuerdo con el concepto de dependencia del sector privado para construir tal infraestructura por su cuenta, y cree que si lo hiciera, produciría esfuerzos ineptos y llenos de obstáculos que serán insuficientes para ganar aceptación social y confianza (Al-Khoury & Bal, 2007; Al-Khoury, 2010; De Meyer and Loh, 2004).

Aparentemente la biometría ofrece tremendas oportunidades para crear nuevo valor, y para brindar conocimiento instantáneo y capacidad de procesamiento para pegar saltos gigantes en el manejo de la identidad y entrega de servicios. (Guthrie, 2003). Los gobiernos, por lo tanto, están asumiendo nuevos roles para construir confianza en las identidades online a fin de mejorar la entrega electrónica de los servicios del gobierno y las empresas. Esta confianza se considera un aliciente a la innovación en el mercado online e impulsa el crecimiento de la nueva economía digital.

Las redes son un componente clave de esta nueva sociedad, como lo ilustran el incremento de teléfonos móviles, el correo electrónico y los sitios web sociales, aún las redes en el mundo digital están cambiando constantemente (IMA, 2011). Los gobiernos han sido durante largo tiempo responsables de desarrollar métodos para la identificación física de identidades. En el mundo de hoy, los gobiernos³ están reconociendo que los límites de sus responsabilidades requieren expansión e incluir redes virtuales y digitales que revolucionen y/o creen nuevos negocios y paradigmas sociales.

“Modelar el mundo digital no es como modelar el mundo físico, donde ecuaciones establecidas gobiernan el movimiento de los átomos o el flujo de electrones. Las interacciones entre la gente y la información son más complicadas, y necesitamos desarrollar nuevos conceptos y modelos para comprender y predecir su comportamiento en la nueva sociedad digital.” El instituto de matemáticas y su aplicación, Reino Unido.

La biometría brinda una oportunidad estupenda para crear una nueva comprensión de las interacciones digitales. Muchos gobiernos en el mundo han invertido intensamente en la última década para desarrollar soluciones de manejo de la identidad para la identificación y autenticación de identidades físicas y virtuales. Estas soluciones están basadas en los medios de identificación y autenticación aceptados tradicionalmente, de uno o más de los tres principios generales: (1) lo que la persona sabe (alguna forma de secreto compartido como las contraseñas), lo que posee (algun tipo de token o clave, por ejemplo, tarjeta inteligente), o lo que es (algún aspecto de su ser físico, es decir, la biometría).

³ • La campaña presidencial Americana de Obama basada en tecnología cambió la cara de las elecciones de los EEUU y dejó claro que él ve tanto a la tecnología como a una fuerte infraestructura de comunicaciones vitales para la recuperación económica y el crecimiento. Esto incluye redefinir el servicio universal para extender su alcance a la banda ancha y desatar el poder del espectro de radio inalámbrica.

• El Gobierno de Francia recientemente lanzó su plan Francia Numerique 2012, una ambiciosa estrategia del sector de comunicaciones diseñada para fortalecer la posición digital de Francia y acrecentar su amplia competitividad en un momento de una desaceleración de la economía y crisis global. El mensaje que conlleva el plan es claro: la economía digital es el sector más dinámico del mundo y a medida que la recesión global avanza, es esencial nutrir aquellas partes de la economía que puedan generar un potencial de crecimiento y puestos de trabajos.

La aplicación de la tecnología de Infraestructura de Clave Pública con su capacidad de firma digital junto con los identificadores biométricos tienen el potencial de brindar una fuerte seguridad de autenticación y no repudiación en las redes digitales. Las firmas digitales identifican y autentican al creador de la información. Permiten que el receptor se asegure la identidad del emisor y a determinar si el mensaje cambió durante el tránsito (Uhlfelder, 2000). Además, permiten la verificación de que la información se mantuvo intacta luego de que el emisor firmó el mensaje y permite que el usuario mismo se identifique en la red (*ibid*).

El uso de las firmas digitales y los identificadores biométricos, cuando se implementan juntos pueden complementarse entre sí, con las fortalezas de cada tecnología contrarrestando las debilidades potenciales en la otra (Jueneman and Robertson, 1998). Habiendo dicho esto, la sección siguiente brinda una visión de las recientes implementaciones de las tecnologías biométricas en los Emiratos Árabes Unidos para atender las necesidades estratégicas nacionales.

3. Las iniciativas de los EAU en la Identificación Biométrica

Los EAU son pioneros en su implementación biométrica. Integraron múltiples tecnologías biométricas en sistemas de infraestructura críticos en la última década. A continuación se muestran ejemplos de proyectos recientes en el campo de la implementación de la biometría.

3.1 Reconocimiento del iris

En los puntos de entrada al país se solicita a todos los visitantes que pasen un escaneo del iris. A través de una infraestructura de red nacional segura, cada uno de los estimados 20.000 viajeros diarios ingresan al país a través de un escaneo del iris; donde cada iris de pasajero presentado es comparado exhaustivamente contra las plantillas en la base de datos de vigilancia de 2,3 millones de personas.

Los EAU comenzaron la implementación de la tecnología de reconocimiento del iris en sus fronteras en 2001 para inhibir el ingreso ilegal de personas en el país. Los EAU fueron los primeros en el mundo en introducir implementaciones de esta tecnología a tan gran escala. Hoy, toda la tierra, aire y puertos marítimos de los EAU, están equipados con sistemas para escanear el iris.

La base de datos de vigilancia para el iris de los EAU actualmente es la más grande del mundo, tanto en términos de cantidad de registros de iris inscriptos (más de 2,3 millones de personas) y en cantidad de comparaciones de iris realizadas diariamente es decir, más de 15 billones de cruzamiento de comparaciones en una comparación (1:n) exhaustiva. Más de 320.000 personas deportadas fueron capturadas en los aeropuertos tratando de volver a ingresar el país luego de haber sido deportados usando nuevos pasaportes con a veces información biográfica diferente.

3.2 Reconocimiento Facial

El reconocimiento facial (facial on the move) ha sido implementado recientemente en los aeropuertos de los EAU en 2008 para incrementar los procedimientos de seguridad y detectar personas que podrían presentar una amenaza al país. Este sistema permite que se realicen controles de identificación críticos a una distancia sin la participación activa de las personas. El sistema ayuda a los inspectores en los puntos de control dentro de los aeropuertos a que implementen controles continuos y preativos diseñados para detectar inmediatamente personas las que se les debería denegar el ingreso o ser detenidas.

El sistema puede identificar personas vivas o por fotografías. Puede identificar personas que se están moviendo con un alto grado de precisión. El sistema que aún está en fase de prueba se espera que esté desplegado en todos los puntos del país en los próximos 2 a 3 años.

3.3 Puertas de Embarque Electrónicas Basadas en Huellas Dactilares

Los EAU tienen otra aplicación biométrica funcionando en sus aeropuertos, principalmente las puertas de embarque electrónicas basadas en la biometría (e-gate). La instalación e-gate que fue introducida por primera vez en 2002 en el Aeropuerto Internacional de Dubai, es el primer aeropuerto de la región y el tercero en el mundo ofreciendo este servicio a los viajeros. El servicio está básicamente disponible para un pasaje rápido a través del control del pasaporte.

La puerta de embarque electrónica utiliza la biometría de huella dactilar para procesar automáticamente todos los pasajeros registrados que llegan y parten de cualquier de los aeropuertos de los EAU. Este es un sistema avanzado de control de pasajeros que acelera considerablemente el movimiento de tráfico con el escaneo de los datos de los pasajeros con la ayuda de una tarjeta inteligente. Se estima que más de 4 millones de viajeros usaron puertas de embarque electrónicas en 2010. El gobierno está trabajando en un plan para alentar el uso de puertas de embarque electrónicas y de hacerlo casi obligatorio para los adultos que viajan sin acompañantes menores.

3.4 Pasaporte Electrónico

El gobierno de los EAU está en proceso de lanzar su nuevo pasaporte electrónico en los próximos seis meses (también llamado pasaporte biométrico). El nuevo pasaporte contiene información biométrica principalmente huellas dactilares y una fotografía con el estándar ICAO que será utilizado para autenticar la autenticidad de los pasajeros. La información en los chips puede ser escaneada y verificada en los aeropuertos, otros puertos y puestos de frontera.

La tecnología PKI se utiliza para firmar los datos electrónicos almacenados en el chip microprocesador del pasaporte. Se espera que esto aumente los rasgos de seguridad actuales de los pasaportes, brinde mayor protección contra la adulteración y reduzca el riesgo de un fraude de identidad. El proceso de emisión está relacionado con la expiración de los pasaportes existentes dado que serán reemplazados por los electrónicos. Los datos biográficos y de huellas dactilares se extraen electrónicamente del registro de identidad nacional, detallado debajo.

3.5 Registro Nacional de Identidad

En el 2003 se lanzó otro programa biométrico ambicioso y de gran escala. El programa apunta a establecer un registro nacional de identidad e inscribir una población estimada de 9 millones. Este programa, que también es denominado por el gobierno de los EAU como la infraestructura nacional de manejo de la identidad, apunta a servir con múltiples objetivos estratégicos. El objetivo principal fue establecer una entidad gubernamental que tenga un rol imperativo como la única fuente para la otorgamiento de identidad personal en el país.

A través de un banco de datos integral, el gobierno busca ayudar a proteger billones de inversiones del gobierno en la duplicación de datos por parte de diferentes instituciones gubernamentales. Los mecanismos de identificación avanzados ofrecidos por este programa están diseñados para suministrar una base de identidad altamente creíble para revolucionar los servicios públicos

y sustentar la creación de la economía digital. La sección cuatro se refiere a este proyecto y muestra sus componentes y objetivos.

3.6 Proyecto Federal de ADN

El gobierno ha comenzado el desarrollo de una base de datos de identificación de ADN en 2010. El proyecto que aún se encuentra en su fase de piloto, apunta a recolectar muestras de ADN de 10 millones de personas tanto ciudadanos nacionales como residentes extranjeros en los próximos años. La base de datos federal de ADN es primeramente considerada como una contribución a las áreas relacionadas con la detección de delitos y la identificación de los delincuentes.

El campo total de la biometría en los Emiratos Árabes Unidos está ganando prominencia y el gobierno parece estar convencido de los potenciales de estas tecnologías para proporcionar una autenticación más fuerte y reducir el riesgo de fraude de identidad. Se han realizado grandes inversiones en soluciones biométricas en los recientes años, como ilustramos en los pocos ejemplos de arriba.

El mercado en los EAU ha visto algunas aplicaciones de biometría en sectores públicos y privados, sin embargo estuvieron primeramente limitados al campo del control del acceso físico. La aplicación de las capacidades de la nueva tarjeta de identidad biométrica de los EAU, de proporcionar soluciones de identificación y verificación personal seguras, está diseñada para mejorar la aceptación pública de la tecnología y vitalizar las transacciones electrónicas, como describe la siguiente sección.

4. El Programa del Registro Nacional de Identidad de los EAU

Los EAU tienen una demografía poblacional muy interesante. De un estimado de 8,2 millones, sólo tan poco como el 10% de su población son ciudadanos nacionales. El restante 90% representa la población residente extranjera que trabaja con permisos de trabajo de un máximo de 3 años o como acompañantes de familiares expatriados. Aproximadamente ciudadanos de 180 países de todo el mundo son residente legales en los EAU. El fuerte crecimiento económico en el país atrajo tal diversidad de trabajadores de todo el mundo, y continúa creciendo a un rápido ritmo. La Figura 6 muestra los patrones cambiantes de demografía en la población en los EAU.

Los EAU se dieron cuenta de la necesidad de un sistema de manejo de la identidad más sofisticado a la luz de la composición única o particular de su población. Los EAU lanzaron su programa de registro nacional de identidad a mediados del 2005.

El programa fue lanzado con el objetivo de construir una infraestructura de manejo de la identidad que tenga un rol derivativo como el único punto de autoridad para el suministro de la información de identidad en el país. Esto fue diseñado para permitir al gobierno que planifique mejor sus prioridades de desarrollo. Claramente, la tasa de crecimiento fue un factor determinante para atender estas necesidades de cambio de su gente para su infraestructura (por ejemplo, escuelas, hospitales, viviendas, rutas), recursos (por ejemplo, alimentos, agua, electricidad), y trabajos.

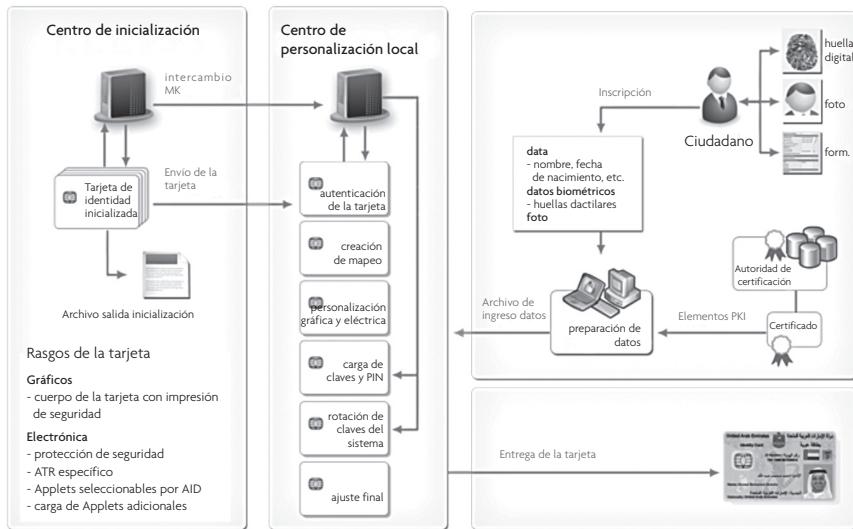


Figura 7: Proceso de emisión de la tarjeta de identidad de los EAU

Otro objetivo importante estaba relacionado con mejorar la entrega de servicio del gobierno, y desarrollar la infraestructura para la nueva economía digital. El programa con sus componentes tecnológicos de avanzada, intenta desarrollar y suministrar identidades digitales para cada ciudadano y residente en el país y en un intento de revolucionar sus iniciativas de gobierno electrónico y comercio electrónico, la identidad digital de una persona está establecida a través de una combinación de tres componentes críticos:

- Número de Identificación Nacional
- Un conjunto de rasgos biométricos (foto, huella dactilar, - el iris está en prueba piloto)
- Un certificado digital consistente en llaves Privada y Pública emitidas por un PKI Nacional (Infraestructura de Llave Pública).

Todos los atributos de la identidad personal se reúnen y se emiten en un solo instrumento de identidad; la Tarjeta de Identidad Nacional de los EAU. De una estimación de una población de 8,2 millones, más de la mitad se han inscrito en el esquema a la fecha. Se espera que la población restante se inscriba hacia fines del 2012.

El gobierno procura procesos de inscripción rigurosos que cumplan con estándares internacionales para la adquisición de datos biométricos de los ciudadanos. Los centros de inscripción están establecidos en todo el país brindando a los ciudadanos y residentes el servicio de inscripción en el Registro de Identidad Nacional.

Principalmente, las huellas dactilares (impresiones rodadas, impresiones de la palma, impresiones de la palma del redactor) y el reconocimiento facial son los rasgos biométricos capturados. Siguiendo los estándares de cumplimiento NFIQ, los datos biométricos son procesados y almacenados en una tarjeta junto con el certificado digital. Ver también la Figura 7. Se espera que el reconocimiento del iris complemente los datos biométricos actuales durante las

renovaciones. El motivo principal para no incluir un tercer dato biométrico fue debido a razones relacionadas con no provocar la interrupción del proceso de inscripción.

Applet	Interfaz	Funcionalidad
Applet de ID y E-monedero (e-purse)	Por contacto y sin contacto excepto para E-monedero la interfaz es sólo contacto	<p>Hay 10 carpetas de datos de identificación personal en el EEPROM de la Tarjeta de EAU. Esas 10 carpetas de identificación personal brindan varios datos de identificación acerca del titular de la Tarjeta de Identidad incluyendo datos de e-monedero. La función del “Applet ID” es manejar el acceso a esas carpetas. Otra función del “Applet ID” es suministrar servicios criptográficos principalmente autenticación mutua y verificación del certificado digital de datos personalizados. Las 10 carpetas de identificación (denominadas Carpetas de Datos de Aplicación ID) son las siguientes:</p> <ol style="list-style-type: none"> 1. Datos ID públicos 2. Datos de Monedero electrónico (E-Purse) 3. Datos de Trabajo 4. Datos de Salud 5. Datos de Defensa 6. Datos de la Licencia para Conducir 7. Datos del Libro de Familia 8. Datos de Servicios Sociales 9. Datos de domicilio 10. Datos de Calificación
Applet PKI	Contacto	<p>La función del applet PKI es facilitar la autenticación electrónica del titular de la Tarjeta de Identidad y facilitar la generación de firmas electrónicas por parte del titular de la Tarjeta de Identidad (dentro de una infraestructura de PKI).</p> <p>La Carpeta de Datos de Aplicación PKI en el EEPROM contiene disposiciones para Pares de Clave 5 RSA y disposiciones para los Certificados 5 RSA correspondientes. Durante la personalización, sólo 2 pares de Clave son personalizados y sus 2 certificados digitales correspondientes son construidos. Esos 2 Pares de Clave se utilizan para las funcionalidades de Autenticación y Firma Digital. Los archivos de los 3 Pares de Clave restantes y sus correspondientes 3 certificados digitales quedan vacíos (RFU). 3 PINs son personalizados (Usuario, Admin, & RFU).</p>
Applet e-viaje (Travel)	Contacto y sin Contacto	<p>Este es un applet que cumple con ICAO. Contiene 5 grupos de datos y un archivo elemental separado como sigue:</p> <p>DG1: MRZ contenido detalles personales básicos DG2: Retrato DG11: Información personal adicional DG13: Nombre completo (Arábico) y fecha de vencimiento DG15: Clave Pública de Autenticación Activa EF.SOD (Post Perso): Firma de datos</p> <p>La Fase 2 contendrá los siguientes grupos de datos adicionales y un archivo elemental:</p> <p>DG3: 2 huellas dactilares (ISO 19794-4) DG14: Parámetros RSA o ECDSH (Autenticación EAC) EF.CVCA: Referencia de Autoridad de Certificación</p>
Applet MIFARE	Sin Contacto	Este es un applet que emula la funcionalidad de la tarjeta sin contacto MIFARE.

4.1 Características de la Tarjeta de Identidad Nacional de los EAU

Adoptando un giro brusco en las características de seguridad, y los estándares biométricos reconocidos internacionalmente y las últimas técnicas de computación, los EAU emiten las tarjetas inteligentes más avanzadas a todos sus ciudadanos y residentes. La Figura 8 describe algunas de las características de seguridad física en la tarjeta.

La tarjeta con microprocesador está basada en Java y cumple el doble propósito de micro computación tanto como de almacenamiento seguro. La micro computación permite utilizar algoritmos de encriptación complejos para que funcionen en la tarjeta eficiente y efectivamente. Esto permite el almacenamiento seguro de los datos asegurándolos a prueba de falsificación de los datos de identidad, incluyendo los datos biométricos.

La EAU fueron uno de los que primeros adoptaron la característica match-on-card (tarjeta de coincidencia). Esta característica permite la autenticación de las huellas dactilares del usuario del Match-on-Card como una alternativa y para completar la verificación complementaria del PIN de la tarjeta inteligente. Esto a su vez brinda el acceso a certificados digitales en la tarjeta que luego pueden ser utilizados para “loguearse”, firma digital, encriptación de archivos, acceso seguro a VPN entre otros servicios.

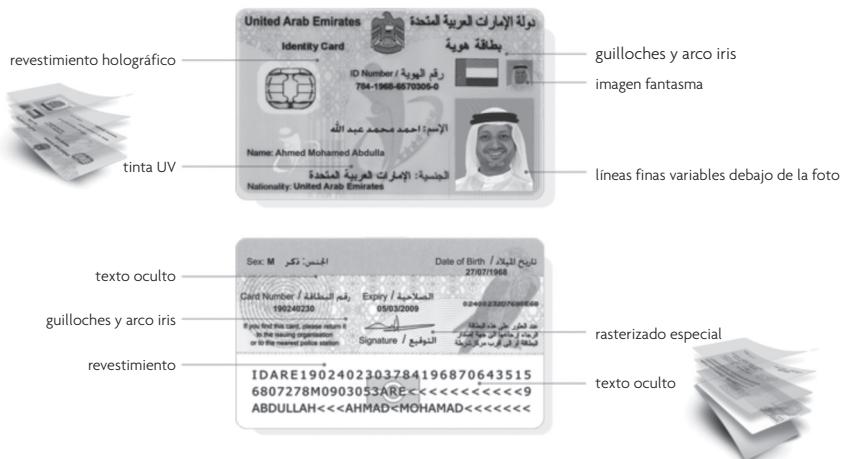


Figura 8: Tarjeta de identificación del proceso de emisión en EAU

Esta solución ofrece una capacidad de autenticación segura de dos o tres factores y es práctica para los usuarios, fácil de implementar y manejar, y totalmente compatible con los componentes de la tarjeta inteligente disponible en los sistemas operativos Windows. También es compatible con la mayoría de los sensores de huellas dactilares disponibles en el mercado.

La tarjeta es una tarjeta inteligente híbrida que también contiene datos personales protegidos por un PIN incluyendo certificados digitales, y los datos biográficos del titular y las dos mejores huellas dactilares. La tarjeta está pensada para que sea el único documento de identidad aceptable para acceder a cualquier servicio del gobierno y algunos críticos del sector privado. La tarjeta 144KB-combi es una tarjeta multi-aplicación y está diseñada para que cumpla totalmente con los dos estándares más importantes de la industria:

- La Especificación de Especificación de Tarjeta de Plataforma Global Versión 2.0.1⁴ define el manejo de la tarjeta; y
- Los Requerimientos de Implementación de la Tarjeta Visa Configuración 1-Compact” por virtud de las mejoras en la tarjeta por las características de seguridad adicionales descriptas en “Plataforma Abierta 2.0.1”.

Los estándares de Java Card Runtime Environment (JCER) y Plataforma Global (Global Platform - GP) contribuyen a las características de seguridad de la tarjeta de Identidad Nacional de los EAU. Java ofrece mecanismos criptográficos e impone firewalls para proteger las aplicaciones y mantener la seguridad de los datos y operación dentro de un espacio de tarjeta compartida multi-aplicación. Las especificaciones del GP 2.0.1 amplían los mecanismos de autenticación criptográficos de la Tarjeta Java para asegurar la carga/actualización de aplicaciones individuales en la Tarjeta Java multi-applet.

Servicio de Validación PKI	Servicio de Proveedor de Datos de Identidad	Servicios de Validación de Tarjeta
<ul style="list-style-type: none"> • Usado en un escenario de negocios donde el Proveedor de Servicios maneja el proceso de autenticación y necesita sólo validación PKI. • Un motor seguro de ‘válido/no válido’ que brinda validación en Tiempo Real de los certificados de Identidad a través de OCSP. 	<ul style="list-style-type: none"> • Para Proveedores de Servicio que transfieren el proceso de autenticación completo a la Autoridad de Entidad de los Emiratos.⁴ • Ofrece Autenticación como Servicio (por e . autenticación por Demanda). • Implementa los protocolos SAML IdP (Proveedores de Identidad) • Provee autenticación de Tarjeta de Identidad de factor 2. 	<ul style="list-style-type: none"> • Servicios de valor agregado tales como Cambio de PIN, Verificar si la Tarjeta es genuina y verificación biométrica

Tabla 8: Servicios de Portal de Validación Nacional (Gateway)

En la tarjeta se brindan tres características únicas que hacen a la tarjeta de identidad nacional de los EAU distinta en su aplicación en el mundo. Hay cinco applets en la tarjeta de identidad de los EAU: (1) applet ID y e-monedero (ePurse), (2) applet PKI, (3) applet Match on Card (MoC), (4) Applet e-Viaje (eTravel), y (5) Applet MIFARE. Ver también la Figura 9. Estos applets no comparten datos dentro de la tarjeta y son completamente seguros. La comunicación con la tarjeta se puede establecer únicamente usando el Kit SDK/Herramienta distribuido por el gobierno.

Los applets están auto-contenidos en la tarjeta y corren como aplicaciones sobre la tarjeta, y nunca los datos almacenados salen de la tarjeta. Estas características permiten una identificación/reconocimiento, validación de las credenciales, verificación instantánea y lo que es más importante da seguridad de la identidad establecida. Esto fue pensado para acrecentar fuertemente la aceptabilidad y confiabilidad de la tarjeta en el país.

⁴ Emiratos Identidad Autoridad es una organización independiente del gobierno federal creada en 2004 para gestionar la aplicación del registro de la identidad nacional.

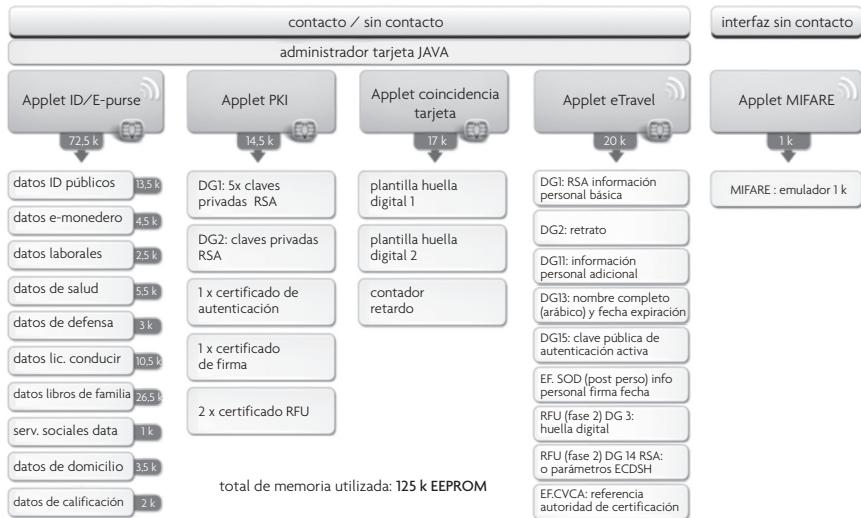


Figura 8: Applets de Identidad en la tarjeta de los EAU

4.2 Funciones de la Tarjeta de Identidad Nacional de los EAU

La principal función que cumple la tarjeta de los EAU es la de establecer una identificación irrefutable del titular de la tarjeta. La función Match on Card da una verificación instantánea de los datos biométricos del titular. Una de las tecnologías de infraestructura clave en los programas es la Infraestructura de Clave Pública (PKI). PKI tiene la funcionalidad de la firma digital permitiendo transacciones entre individuos y organizaciones en el espacio virtual de Internet.

La necesidad primaria surge de los requerimientos relacionados con el desarrollo de un mecanismo de comunicación (autenticación) seguro. El gobierno busca sustentar las iniciativas de gobierno electrónico y comercio electrónico (e-government y e-commerce) a través de esta tarjeta para actuar como el habilitador de las transacciones electrónica.

Además de las funciones principales, la tarjeta debe estar preparada para ser el sistema de identidad singular en el país suministrando un soporte de integración para los requerimientos de identidad inter-agencias. La tarjeta tiene múltiples contenedores de datos que podrían permitir y facilitar el gobierno electrónico. Los datos de Trabajo y Empleo, Autoridades Viales, agencias de Orden Público, Puerta de Embarque electrónica, Pasaporte electrónico, Monedero Electrónico, son algunos de los contenedores de datos disponibles en la tarjeta.

Distintos departamentos del gobierno pueden habilitar sus metadatos de identidad específicos para el titular de la tarjeta en estos contenedores. La Tabla 7 muestra un panorama de las capacidades y funciones de la tarjeta de identidad de los EAU.

4.3 Iniciativa de Gobierno Electrónico de los EAU

Un informe reciente realizado por la escuela de negocios INSEAD y el Foro Económico Mundial mostraron que los EAU están considerados primeros en el Oriente Medio y África del

Norte (Mena), y 24° en el mundo, en términos de estar preparados para las tecnologías de la información y comunicación (Dutta and Mia, 2011). El gobierno de los EAU se dieron cuenta de la necesidad de adoptar enfoques más efectivos para promover en principio, la autenticación de las identidades online, y atender los requerimientos generales de confianza, manejo de la identidad y privacidad y en el contexto del gobierno electrónico.

La tarjeta de identidad de los EAU, sumada a la tecnología de Infraestructura de Clave Pública, brinda capacidades de autenticación fuertes para soportar los servicios online. La tecnología PKI brinda bloques de construcción de llave de identidades digitales, es decir, generación, gestión y validación de certificados digitales, y estampillado de tiempo electrónico.

El gobierno de los EAU recientemente introdujo su solución de gestión de la identidad federada (también llamada Portal de Validación Nacional - National Validation Gateway) que está basada en su nueva tarjeta de identidad inteligente y las capacidades avanzadas de PKI. La solución brinda servicios de autenticación de identidad a los proveedores de servicios (por ejemplo, gobierno electrónico, bancos, hospitales, entidades comerciales). Está implementado como un servicio sobre la nube para brindar servicios diferentes como se describe en la Tabla 8.

La solución actualmente está disponible para las autoridades de gobierno electrónico. Hay ocho autoridades de gobierno electrónico en el país, una autoridad de gobierno electrónico federal y siete autoridades locales, una en cada emirato. Actualmente hay 48 servicios del gobierno⁵ que están integrados con esta infraestructura.

El usuario básicamente necesita bajar un applet en su computadora. Usando el lector de tarjeta, necesita usar su tarjeta para “loguearse” en el portal de gobierno electrónico. El método de autenticación puede variar dependiendo de los requerimientos del servicio. El portal puede realizar la función de autenticación en modo off-line, o puede redirigir al usuario al portal de validación nacional. La retroalimentación desde la última determinará la autorización pasa o no pasa (decisión del control de acceso) a los recursos deseados.

El gobierno federal de los EAU está trabajando en un borrador del marco legal para legalizar las identidades digitales y las firmas digitales. El gobierno está planeando hacer que todas las transacciones G2C de gobierno electrónico se realicen sólo a través de su nueva tarjeta de identidad inteligente en los próximos 3 a 5 años. El gobierno está planeando conducir el crecimiento económico digital a través de todo el país usando su nueva infraestructura de identidad basada en la biometría.

4.4 El Rol de la Biometría en la Tarjeta de Identidad Biométrica en G2G, G2B, G2C

Como los niveles de seguridad del sistema de información mundial es violado e incrementa el fraude en las transacciones, el gobierno de los EAU se está moviendo agresivamente hacia la transformación del gobierno electrónico, particularmente para desarrollar servicios combinados, sin fisuras, que son entregados electrónicamente a su población u otras entidades del sector público o privado (Westland and Al-Khoury, 2010). Esto se condice con su objetivo de mejorar la eficiencia, calidad y transparencia de los servicios del gobierno.

⁵ www.abudhabi.ae Uno se puede registrar para acceder al portal y sus servicios usando la Tarjeta de Identidad de los Emiratos.

El gobierno planea incluir el desarrollo de canales múltiples de auto-servicio, por ejemplo, sobre Internet, cabinas, canales inalámbricos e IVR. La autenticación biométrica de identidades personales es vista como más conveniente y considerablemente más precisa que los métodos corrientes tales como la utilización de contraseñas o PINs.

Como se mencionó anteriormente, la tarjeta de los EAU está habilitada con una aplicación Match-on-Card. Esto le permite a los proveedores de servicios tales como las instituciones del gobierno a verificar la identidad del titular y entregar servicios con total confianza sobre la identidad de la persona que recibe los servicios. Con tantas características seguras y transaccionales habilitadas en la tarjeta, la tarjeta de identidad nacional de los EAU está establecida para convertirse en la tarjeta más valiosa del país tanto en las transacciones físicas como las electrónicas.

La biometría en general está diseñada por el gobierno de los EAU para brindar altos niveles de aseguramiento de la identidad para la seguridad interior incluyendo aplicaciones para mejorar la seguridad aeroportuaria, y fortalecer las fronteras nacionales, y para la prevención de robo de identidad. Se ve que hay una creciente conciencia e interés en la biometría en el país y en la región en general, sobre su potencial en identificar y verificar la identidad de los individuos con mayor precisión y proteger los activos nacionales.

El gobierno recientemente ha lanzado y mejorado la versión del Software Development Tool Kit (SDK) – Kit de Herramientas de Desarrollo - para permitir a las organizaciones licenciadas que integren la nueva tarjeta de identidad inteligente y las aplicaciones biométricas a sus sistemas y desarrollen sistemas de firma electrónica y autenticación biométrica que cumplan con la legislación.

El kit de herramientas SDK brinda un alto nivel de API (Interfaz de Programación de Aplicaciones) que ayuda a realizar el desarrollo de software de aplicación fácil y rápidamente y UI (Interfaz Usuario) del tipo asistente para que ahorre tiempo y esfuerzos para desarrollar una aplicación. Se lo opera sobre varias plataformas, soportando diversos sistemas operativos y lenguajes de desarrollo (Al-Khoury, 2011).

Con tales acciones, se espera que el uso y alcance de la biometría en los EAU aumente considerablemente en pocos años. Se implementarán más sistemas de identificación y verificación para atender los requerimientos de varias industrias que posiblemente consideren a la biometría de sumo interés en términos de costo y necesidad para proteger sus datos y activos. El gobierno está planeando impulsar sus soluciones de tarjeta de identidad basada en biometría en múltiples dominios de aplicación. Recientemente ha lanzado varias iniciativas en cooperación con organizaciones del sector privado para alentar el desarrollo de una extensa gama de soluciones de identificación y verificación personal altamente seguras integrando las funciones de la nueva tarjeta de identidad en las aplicaciones del sector público, por ejemplo, (1) acceso a la red para controlar el acceso no autorizado a computadores y redes en organizaciones gubernamentales, (2) la industria financiera para promover el comercio electrónico y las transacciones online, (3) la industria de atención de la salud para brindar seguridad en las instalaciones hospitalarias y el reconocimiento de las identidades de los pacientes, (4) agencias de orden público y (5) inmigración y aeropuertos.

4.5 Marco de Interoperabilidad

Para incrementar aún más las transacciones que usan la nueva tarjeta de identidad inteligente, el gobierno de los EAU está trabajando activamente con distintos interesados en el país y en la región para definir las normas de interoperabilidad. Se ha definido un marco que determina el rol de la nueva tarjeta de identidad inteligente y la verificación biométrica que sería necesaria para autenticar a un interesado en cualquier transacción.

Se están definiendo normas para el intercambio de datos que permita a los departamentos del gobierno y distintas agencias que se comuniquen en forma segura. La tarjeta de identidad con su característica de PKI es central para tal comunicación. Se está brindando el Manejo de la Identidad Federada que actualmente está en su estado piloto, integrando el acceso de diferentes servicios web usando el sistema de manejo de la identidad establecido por el gobierno.

Llevando la interoperabilidad a un nuevo nivel, se están tomando acciones para establecer un Marco de Interoperabilidad del Golfo que permitirá el uso de las tarjetas de identidad inteligentes de los EAU y otras tarjetas de identidad nacionales en los países del GCC⁶ (Consejo de Cooperación del Golfo) en las fronteras. Estos han sido avances significativos en los últimos años para asegurar que las tarjetas de identidad en todos los países del GCC sean técnicamente compatibles e interoperables. Hay algunos desarrollos recientes de APIs relacionados con biometría, firmas calificadas digitales y autenticación digital para permitir las transacciones de comercio electrónico (e-business) cruzando las fronteras (Al-Khoury and Bechlaghem, 2011).

Conclusión

Las tecnologías biométricas que tienen una larga historia de uso en las aplicaciones de orden público, ahora están en transición con una aceptación social más amplia hacia el sector público y las aplicaciones comerciales. Utilizada con otras tecnologías de avanzada, tales como tarjetas inteligentes, claves de encriptación y firmas digitales, la biometría está establecida para dominar todos los aspectos de la economía y en nuestra vida diaria.

Sólo aprendiendo más sobre estas tecnologías y explorando sus potenciales y explotando las experiencias de programas exitosos y fallidos, los gobiernos pueden desarrollar una comunidad biométrica robusta y vibrante. Se requieren tales acciones para construir los sistemas de identificación y autenticación con los que la gente puede vivir, confiar y usar, que también deberían permitir que se generara la nueva economía digital.

La búsqueda exitosa de desafíos en biometría generará avances significativos en las capacidades diseñadas para mejorar la seguridad en la futura misión dentro del marco de la seguridad nacional, el orden público, la información personal y transacciones comerciales. La interoperabilidad aún será un obstáculo importante.

Desde un ángulo, la interoperabilidad a través de las fronteras geográficas y los sectores de

⁶ GCC es la sigla de Consejo de Cooperación del Golfo, también conocido como el Consejo de Cooperación para los Estados Árabes del Golfo (CCASG). Incluye seis países, a saber, Bahrein, Kuwait, Omán, Qatar, Arabia Saudita, y los Emiratos Árabes Unidos. La cantidad de población del GCC se estima en alrededor de 40 millones de personas (GCC Portal, 2011). Los ciudadanos del GCC generalmente pueden viajar libremente entre los estados miembro sin necesidad de visa, y pueden usar pasaportes o tarjetas de identidad nacionales para cruzar las fronteras.

negocios, a través de los procesos, dispositivos y sistemas es beneficiosa para la difusión de la biometría. Sin embargo, y mirándolo desde otro ángulo, se espera que los intereses nacionales en mantener las resistencia al control y los proveedores (aspirando a un dominio del mercado futuro debido a los efectos de proveedor fijo) desafíen los esfuerzos de interoperabilidad, a pesar del trabajo significativo en estandarización que se está haciendo a niveles nacionales e internacionales.

Aunque la interoperabilidad técnica esté recibiendo mayor atención en cierto grado, la interoperabilidad de los procesos puede ser un mayor desafío. Estos desafíos saldrán a la superficie cuando los intentos de innovar los modelos de entrega comiencen a operar desplazando los estrechos objetivos existentes y promoviendo más amplia difusión en nuestras sociedades. Como tal, cuando los sistemas se tornan más interoperables, la necesidad de construir un manejo de la identidad más robusto crece tanto como la de cumplir con las necesidades nacionales e internacionales.

El gobierno y las industrias probablemente se tornen más dependientes que nunca de las herramientas de manejo de la identidad y de los principios de gobierno de la identidad más robustos. La biometría jugará un rol clave en atender los nuevos desafíos de los años venideros.

Bibliografía

- Al-Khoury & Bal, J. (2007), "Electronic Government in GCC countries." in International Journal Of Social Sciences, 1(2), pp.83-98.
- Al-Khoury, A.M. (2011), "PKI in Governemt Identity management Systems." in International Journal of Network Security & Its Applications, 3(3), pp. 69-96.
- Al-Khoury, A.M. and Bechlaghem, M. (2011), "Towards federated e-Identity Management across GCC: A solution's Framework." in Global Journal of Strategies and Governance 4(1). pp. 1-20.
- Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002), "Biometric perils and patches." Pattern Recognition 35(12), pp. 2727-2738.
- Brüderlin, R. (2001)."What is Biometrics?" [Online]. Available from: <http://www.teleconseil.ch/english/introduction.html>. Accessed: August 12, 2011.
- Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005), "PalmHashing: a novel approach for cancelable biometrics." in Information Processing Letters, 93(1), pp. 1-5.
- De Meyer, A. and Loh, C. (2004), "Impact of ICT on government innovation policy: an international comparison," in International Journal of Internet and Enterprise Management 2(1).
- "Dermatoglyphics," Hand Analysis, International Institute of Hand Analysis, 24 January 2005.
- Dutta, S. and Mia, I. (ed.) (2011), "The Global Information Technology Report 2010-2011". [Online] Available from: http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf Accessed: August 15, 2011.
- GCC Portal: <http://www.gcc-sg.org/eng/index.html>. Accessed: August 12 2011.
- Guthrie, I. (2003), "Electronic Government in the Digital Society." Lomonosov Moscow State University,

- Russia. [Online] available from: egov_digital_society. Accessed: August 12, 2011.
- IMA (2011), "Building the Digital Society," The insitute of mathamtics and its application, UK. [Online]. Available from: building_the_digital_society_20101213122904. Accessed: August 12, 2011.
- Jueneman, R.R. and Robertson Jr, R.J. (1998), "Biometrics and Digital Signatures in Electronic Commerce," in 38 Jurimetrics J. [Online] Available from: <http://nma.com/mcg-mirror/mirrors/digsig.pdf>. Accessed: August 1, 2011.
- Ke, W. and Wang, X. (2008), "How do governments matter to the creation of digital economy?" in Fensel, Dieter and Werthner, Hannes (editors) Proceedings of the 10th international conference on Electronic commerce (ICEC), Innsbruck, Austria, August 19-22, 2008.
- McMahon, Z. (2005), "Biometrics: History," Indiana University, Indiana University Computer Science Department [Online]. Available from: <http://www.cs.indiana.edu/~zmcMahon/biometrics-history.htm>. Accessed: August 12 2011.
- Renaghan, J. (2005), "Etched in Stone," Zoogoer, August 1997, (Smithsonian National Zoological Park, 26 January 2005).
- Richardson, A. (2009), "Why Identification Cards are Important in Today's Economy," Articles Factory [Online]. Available from: <http://www.articlesfactory.com/articles/business/why-identification-cards-are-important-in-todays-economy.html>. Accessed August 21, 2011.
- RNCOS (2011), "Global Biometric Forecast to 2012" [Online]. Available from: http://pdf.marketpublishers.com/463/global_biometric_forecast_to_2012.pdf. Accessed August 30, 2011.
- Ross, A. & Jain, A. (2003). "Information fusion in biometrics." in Pattern Recognition Letter 24(13), pp. 2115-2125.
- Rukhin, A. L. & Malioutov, I. (2005). Fusion of biometric algorithms in the recognition problem. Pattern Recognition Letters, 26(5), 679-684.
- Sarkar, I., Alisherov, F., Kim, T., and Bhattacharyya, D. (2010), "Palm Vein Authentication System: A Review". International Journal of Control and Automation, Vol. 3, No. 1, pp. 27-34.
- Shoniregun, C.A., and Crosier, S. (2008). Securing Biometrics Applications. Springer-Verlag.
- Tilton, C. (2006), "Biometric Standards – An Overview." Daon. [Online]. Available from: http://www.securitydocumentworld.com/client_files/biometric_standards_white_paper_jan_06.pdf. Accessed: August 12, 2011.
- Uhlfelder, D. (2000), "Electronic Signatures and The New Economy" [Online]. Available from: <http://ubiquity.acm.org/article.cfm?id=354571>. Accessed: August 1, 2011.
- Vamosi, R., Monahan, M., Kim, R., Miceli, D., Van Dyke, A. and Kenderski, J. (2011) 2011 Identity Fraud Survey Report. Javelin Strategy and Research.
- Westland, D. and Al-Khoury, A.M. (2010), "Supporting gobierno electrónico progress in the United Arab Emirates," in Journal of Gobierno electrónicoStudies and Best Practices, pp.1-9.
- Woodward, J.D. (1997), "Biometrics: Privacy's foe or privacy's friend?," in Proceedings of the IEEE (Special Issue on Automated Biometrics), 85, pp. 1480-1492.

El Proyecto RIC como paradigma de la identificación civil brasilera

Marcos Elias Claudio Araujo



Marcos Elias Claudio Araujo

Director del Instituto Nacional de Identificación, INI Departamento de la Policía Federal de Brasil.



Nació en Brasilia/DF en 1963. Graduado en Ciencias Económicas por la Universidad Católica de Brasilia, posee un título de Extensión Universitaria en Análisis de Sistemas en la Universidad de Brasilia. Es co-autor del libro “Datalografía: a determinação dos dedos” (2007), fue director de la División de Identificación de Informaciones Criminales y de Extranjeros y actualmente es el Director del Instituto Nacional de Identificación.

Es miembro del Comité Gestor del Sistema Nacional de Registro de Identificación Civil - SINRIC, grupo responsable de la implantación de la nueva tarjeta de identidad brasileña, y participa de este proceso desde 1997 momento en que se promulgó la Ley 9.454 que instituyó el número único de Registro de Identidad Civil.

Resumen

Acompañando las más recientes innovaciones tecnológicas, el nuevo modelo de identificación civil adoptado por Brasil contempla la adopción de una tarjeta inteligente que contiene ítems de seguridad de última generación, configurando un documento de identidad moderno, práctico y seguro que posiciona a Brasil en la vanguardia mundial en lo que respecta a la identificación civil.

Palabras clave: identificación civil, seguridad.

El Proyecto RIC como paradigma de la identificación civil brasilera

Según el “Informe de las mejores prácticas mundiales” de la Agencia para la Sociedad del Conocimiento de Portugal(¹), a comienzo de los años 2000 varios países iniciaron estudios para el perfeccionamiento y la modernización de los servicios públicos prestados a la sociedad.

Estas iniciativas estaban, en su mayoría, centradas en la tecnología buscando la modernización de los servicios públicos. Actualmente, muchos de estos proyectos están en una segunda fase de operación, la cual consiste en la creación de servicios “inteligentes” focalizados en el ciudadano.

La implantación de una nueva forma de identificación del ciudadano-usuario fue el punto de partida para la modernización de la atención al público, y en ese contexto varios países vienen perfeccionando sus sistemas de identificación civil.

Acompañando esta tendencia internacional de modernización de los documentos, Brasil adhirió a la Convención de las Naciones Unidas contra la delincuencia organizada transnacional, conocida como la Convención de Palermo que fue promulgada por el Decreto nº 5015, del 12/03/2004. Los protocolos adicionales de esta convención, relacionales con la prevención del tráfico de migrantes por vía terrestre, marítima y aérea (promulgado por el Decreto nº 5016, del 12/03/2004) y la prevención, represión y castigo del tráfico de personas, en especial mujeres y niños (promulgado por el Decreto nº 5017, del 12/03/2004), prevén la creación de mecanismos de seguridad, control y validación de los documentos de identidad.

Artículo 12: Seguridad y control de los documentos

Cada Estado parte adoptará las medidas necesarias de acuerdo con los medios disponibles para:

- a) *Asegurar la calidad de los documentos de viaje o de identidad a emitir a fin de que no sean indebidamente utilizados ni fácilmente falsificados o modificados, reproducidos o emitidos de forma ilícita; y*
- b) *Asegurar la integridad y la seguridad de los documentos de viaje o de identidad por sí mismos o emitidos en su nombre e impedir su creación, emisión y utilización ilícitas.*

Artículo 13: Legitimidad y validez de los documentos

A pedido de otro Estado Parte, un Estado Parte verificará, en conformidad con su legislación interna y dentro de un plazo razonable, la legitimidad y validez de los documentos de viaje o de identidad emitidos o supuestamente emitidos en su nombre y de los que se sospeche haber sido utilizados para el tráfico de personas.

La identificación civil posee el objetivo de identificar a la población, garantizándole su individualidad en los diversos actos de la vida en sociedad. Actualmente, la identificación civil de los brasileros se realiza por medio de la emisión del Carné de Identidad (Carteira de Identidade), expedido por los Órganos e Institutos de Identificación de los estados y el Distrito Federal, conforme a la Ley nº 7.116, del 29 de agosto de 1983, reglamentada por el Decreto nº 89.250, del 27 de diciembre de 1983, siendo esta ley responsable de la estandarización del modelo nacional de identidad civil. Desde entonces, en la mayor parte de las unidades federativas brasileras no

hubo inversiones o proyectos relevantes en el campo de la identificación civil que acompañasen los avances tecnológicos y las necesidades de la sociedad contemporánea. Como resultado, el carné de identidad se volvió un documento obsoleto.

El sistema de identificación civil en vigor hace posible que un ciudadano obtenga, legalmente, documentos de identidad en varias unidades federativas pudiendo llegar a 27 registros de identidad civil, pero con numeraciones diferentes. A lo que se suma el hecho de que varios Institutos de Identificación presenten dificultades para realizar la investigación en sus archivos dactiloscópicos antes de la emisión de la cédula de identidad, generando que una persona pueda defraudar al sistema y obtener varios números de identidad con datos personales diferentes en un mismo estado o unidad de federación.

Otro factor que contribuye a la fragilidad de este sistema es la completa ausencia de integración sistémica, tanto a nivel nacional como de cada Estado, lo que impide la investigación de datos entre los órganos e institutos de Identificación. La fragmentación y desarticulación institucional perjudica al Estado, la sociedad y compromete la confiabilidad de todos los documentos emitidos.

El proyecto en marcha se basa en la condición especial de garantizar los derechos fundamentales del ciudadano. El artículo 5º de la Constitución establece que: *"Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándoles a los brasileros y a los extranjeros residentes en el país la inviolabilidad del derecho a la vida, la libertad, la igualdad, la seguridad y la propiedad"*. Su inciso X reglamenta que: *"son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurado el derecho a indemnización por el daño material o moral resultante de su violación"*.

A pesar de esto, las garantías constitucionales dejan de respetarse a diario y la vida, el honor y la imagen del ciudadano son perjudicadas cuando su nombre se utiliza indebidamente para la apertura de empresas fantasma, realización de préstamos y otros fines resultantes de sus relaciones sociales, generando deudas y la carga de tener que probar su identidad. Muchas personas responden por delitos que no cometieron a causa de la fragilidad del actual documento de identidad, otras son sepultadas como indigentes debido a la falta de integración entre los archivos de identificación civil.

Creado por la Ley nº 9.454 del 7 de abril de 1997, el número único de Registro de Identidad Civil – RIC, contenido en el documento, será generado y provisto por el Órgano Central luego de la confirmación de la unicidad de la identificación del ciudadano, basándose en sus impresiones dactilares. Conforme al Decreto nº 7.166, del 5 de mayo de 2010, con el nuevo documento, la persona tendrá un registro en el Catastro Nacional de Registro de Identificación Civil – CANRIC que se constituirá a partir de la utilización del RIC para la indexación de los datos necesarios para la identificación única de los ciudadanos.

Según el Decreto nº 7.166/2010, el Organismo Central del Sistema será responsable de la coordinación, almacenamiento y control del Catastro Nacional de Registro de Identificación Civil. Será tarea de los entes federados convenidos, en régimen de coparticipación con el Organismo

Central, poner en práctica y actualizar el Catastro Nacional de Registro de Identificación Civil, controlar el proceso de distribución del RIC, transmitir los datos de identificación reunidos para emisión del RIC al organismo central del sistema, y emitir el documento de identificación que contenga el RIC.

Bajo la coordinación del Ministerio de Justicia, el Registro de Identidad Civil nació con la misión de volverse un importante instrumento en la garantía de los derechos sociales y la protección del patrimonio. Su implantación hará posible, de forma rápida y segura, la identificación de cualquier ciudadano brasileño contribuyendo a evitar fraudes y facilitar la solución de conflictos sociales. El nuevo documento de identificación civil también tiene por objetivo modernizar el Sistema de Identificación Civil del país, garantizar la unicidad del ciudadano en una base de datos de alcance nacional, fortalecer las relaciones de la sociedad con los organismos gubernamentales y privados, contribuir con la promoción de la inclusión social y digital, y ampliar los mecanismos preventivos de seguridad pública.

El Proyecto propuesto prevé la emisión de 150 millones de Registros de Identidad Civil - RIC (generados luego de la certificación de la unicidad biométrica de las impresiones digitales en un sistema automatizado, centralizado e integrado en el ámbito nacional) insertados en los nuevos documentos de Identificación Civil con el uso de la tecnología aplicada a la identificación, modernos ítems de seguridad documental, chip microprocesador y certificado digital. El nuevo proceso de identificación civil podrá ser financiado a través del presupuesto público, el cobro de tasas de emisión del documento, la prestación de servicios por los órganos de Identificación en tanto Autoridad de Registro, y la utilización de los servicios de certificación digital; pudiendo también firmarse acuerdos de colaboración público-privadas.

Con el nuevo sistema de identificación civil, los registros dejarán de estar regionalizados, como ocurre hoy con el Registro General - RG y formarán un banco de datos centralizado contenido informaciones dactiloscópicas de ciudadanos de todo el país. Este sistema será administrado por el Ministerio de Justicia (Instituto Nacional de Identificación de la Policía Federal) y contendrá datos como fotografía, firma digital, números de otros documentos y datos personales como altura y color de los ojos. La implementación del nuevo documento de identidad civil es un proyecto de alcance nacional que alcanzará a todos los ciudadanos brasileños.

Luego de la implantación del Registro de Identidad Civil, el proyecto deberá transformarse en un proceso, es decir en una acción continua. Los órganos participantes del Sistema Nacional de Registro de Identificación Civil - SINRIC estarán estructurados física y tecnológicamente, y con recursos humanos adecuados de forma uniforme en todo el territorio nacional, garantizando la misma calidad de atención al ciudadano independientemente del lugar donde fuera prestado el servicio.

La adopción del Registro de Identidad Civil – RIC traerá innumerables beneficios a la sociedad garantizando la unicidad entre el ciudadano y su documento y utilizando la identificación dactiloscópica de forma automatizada. Esta medida fortalecerá los servicios públicos y privados que requieran la identificación del ciudadano contribuyendo efectivamente con la reducción de fraudes contra personas físicas, jurídicas y entes gubernamentales.

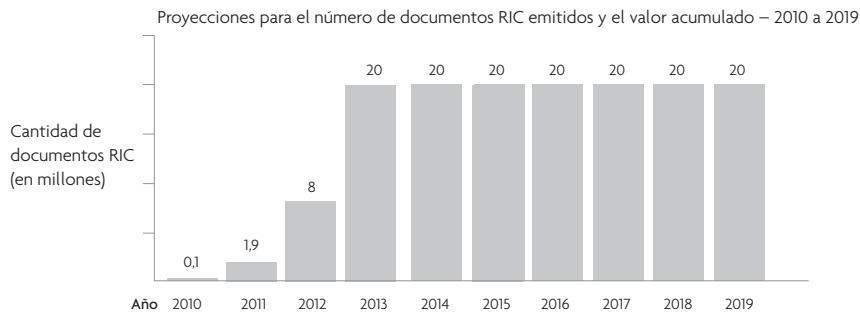
Además de la implantación del Registro de Identidad Civil, el Proyecto RIC propone la adopción de un nuevo documento de identificación civil con especificaciones tecnológicas, posicionando a Brasil en la vanguardia del Estado moderno. Los ítems de seguridad tecnológicos posibilitarán su utilización en diversas aplicaciones en la vida cotidiana de las personas y de las instituciones, proporcionando seguridad, agilidad y transparencia de los resultados.

La tarjeta RIC posee un formato semejante al de una tarjeta de crédito y se fabrica en un material de alta resistencia y durabilidad, llamado policarbonato. Otra importante innovación de la tarjeta RIC es que posee dos chips microprocesadores (uno con contacto y uno sin contacto), donde estarán grabados los datos biográficos (nombre, filiación, fecha de nacimiento, etc.) y biométricos (impresiones digitales), lo que posibilitará la identificación electrónica automatizada del titular y el uso de la certificación digital. En el futuro, los chips podrán recibir otras aplicaciones para ampliar las relaciones del ciudadano con instituciones públicas o privadas. Entre los ítems de seguridad documental presentes en el nuevo documento de identidad brasileño se encuentran (cuadro 1):



- Fondo de seguridad: Compuesto por líneas complejas de colores diferentes (duplex), entrelazadas y dispuestas en figuras geométricas (guillochés), formando imágenes tridimensionales por medio de la distorsión de las líneas (numismático), con una mezcla de colores que produce un efecto óptico exclusivo;
- Imagen en UV (ultravioleta): Imagen revelada bajo la incidencia de luz ultravioleta;
- Imagen oculta: Imagen revelada solamente bajo refracción da luz;
- OV: Tinta que cambia de color dependiendo del ángulo de visión;
- Relieve táctil: Diseño hecho en relieve perceptible a través del tacto;
- MLI: Imágenes múltiples grabadas por haces de rayo láser que, dispuestas en un ángulo específico, revelan el estado de origen de la tarjeta y el número de RIC. Con otro posicionamiento, se percibe la reproducción de la foto y la firma del titular de la tarjeta;
- DOV: Dispositivo Óptico Variable que produce efecto de transición de formas y colores. Se trata de un tipo de holograma desarrollado exclusivamente para el gobierno brasileño. La matriz de este diseño complejo es propiedad del Estado y queda bajo su custodia;
- Foto fantasma: Es la reproducción de la foto del titular en el reverso de la tarjeta en tamaño reducido;
- Personalización: Todos los datos de personalización de la tarjeta (como nombre, filiación, foto, firma e imagen de la impresión digital) son grabados por medio de haces de rayo láser que perforan las capas del policarbonato. Con esto, se formarán palabras e imágenes sin la utilización de tintas, evitando la remoción o adulteramiento de estos datos;
- Campo MRZ con código OCR estándar ICAO: Conjunto de números y letras que permiten la lectura en equipamientos utilizados, por ejemplo, en aeropuertos. Se trata del estándar internacional para la identificación de documentos de viaje.

Como resultado de la implementación del RIC un gran acuerdo está siendo firmado con los órganos estatales de Identificación que deberán recibir la inversión necesaria para promover la armonía tecnológica entre todos los participantes del Sistema Nacional de Registro de Identificación Civil - SINRIC, permitiendo una integración segura entre las bases de datos, lo que posibilitará la implementación del Proyecto en todo el territorio brasileño en el plazo de nueve años, con el registro de aproximadamente 150 millones de brasileros (cuadro 2).



Varias instituciones fueron invitadas a participar de la construcción de este proyecto, y pronto comprenderán la importancia del tema y de forma integrada, presentarán modelos de aplicaciones para sus respectivas áreas de acción fortaleciendo los lazos institucionales de coparticipación e integración, en torno al objetivo de reformular el concepto de identificación civil en el país.

El proyecto RIC apoyará diversas áreas como por ejemplo, la de Previsión Social que almacena datos de aproximadamente 36,5 millones de contribuyentes y 25 millones de beneficiarios que son atendidos y reciben pagos todos los meses en cualquier parte del territorio nacional. El CNIS, Catastro Nacional de Informaciones Sociales, contiene informaciones que garantizan los derechos laborales y previsionales. Con el RIC, varias aplicaciones que facilitan los procesos de atención serán agilizadas, proporcionando comodidad, seguridad y transparencia.

La justicia electoral cuenta, actualmente, con una base de datos civiles de aproximadamente 130 millones de personas. El proceso electoral brasileño, que se destaca internacionalmente, busca fortalecer su confiabilidad agregando la autenticación biométrica a las urnas electrónicas. Con el objetivo de garantizar el pleno ejercicio de la ciudadanía por parte de los electores brasileños, evitando que las personas emitan su voto más de una vez en el mismo padrón electoral, el Tribunal Superior Electoral inició en 2008 la ejecución de proyectos pilotos para el registro biométrico de los electores, en colaboración con el Instituto Nacional de Identificación de la Policía Federal.

Datos presentados por la Federación Brasileña de Bancos – FEBRABAN, señalan que los bancos e instituciones financieras invierten aproximadamente 1200 millones de reales por año para garantizar la seguridad en las transacciones bancaria, la protección de grabaciones electrónicas y la bancarización (acceso de personas de bajos ingresos a los servicios bancarios).

La ampliación de la distribución de renta resultante de los programas sociales del Gobierno Federal ha contribuido con el proceso de bancarización. El avance de este proceso es inevitable, teniendo en cuenta que varias rutinas del ciudadano pueden ser resueltas en cualquiera de las agencias bancarias o unidades correspondientes ubicadas por todo el país.

Por ello, el Proyecto RIC pasa a ser un mecanismo de fundamental importancia para este movimiento político de inclusión social y seguridad en los procesos de aperturas de cuentas, concesión de créditos y reducción de fraudes y perjuicios.

En 2008, el sector bancario invirtió R\$ 6400 en Tecnología de la Información (TI), y el número de cuentas de Net Banking aumentó casi un 300% en esta década, alcanzando en 2008, un total de 23,5 millones de cuentas. El número de agencias bancarias aumentó de 18600 a 19100 entre 2007 y 2008, un aumento de 3,1%. La suma de gastos e inversiones de los bancos en Tecnología de la Información (TI) llegó a R\$ 16200 millones, frente a los R\$ 14900 millones registrados en 2007. Estos números divulgados por la FEBRABAN revelan la dimensión del desafío a enfrentar.

El hecho es que con el proceso de bancarización, las transacciones “on-line” crecerán a una velocidad mayor a la de la emisión de certificados digitales. Especialistas del sector estiman que si todos tuviesen un certificado digital, el número de fraudes en internet podría caer hasta en un 80%.

En Brasil, el Instituto Nacional de Tecnología de la Información - ITI ha sido el principal promotor de la implementación del certificado digital, ofreciendo más aplicaciones y servicios a los ciudadanos en el mundo virtual. Los mejores ejemplos son: la utilización de la nota fiscal electrónica, la virtualización de los Procesos Judiciales el e-CPF (Censo de Personas Físicas) de la Hacienda Federal.

La adhesión de este resultado al Proyecto RIC hará posible la popularización de la certificación digital y con esto, el nuevo documento de Identificación Civil será también un instrumento de ciudadanía e inclusión digital en Brasil. Es decir, cada ciudadano brasileño tendrá acceso al medio tecnológico necesario para ser reconocido en redes de comunicación, de internet, y podrá utilizar los servicios del gobierno electrónico.

La certificación digital se ha vuelto la forma segura de resolver uno de los más antiguos dilemas de internet: la comprobación de la identidad de quien hace compras con tarjeta de crédito o accede a una cuenta bancaria. En las transacciones actuales esta certeza es muy precaria.

La combinación de la biometría de las impresiones digitales con la certificación digital se consolidará en un proceso de identificación personal más seguro que garantizará la mejora de la cadena de atención virtual de los bancos, la seguridad en las redes de comunicación, reducción de fraudes y delitos en internet.

Otro segmento que se beneficiará ampliamente es el comercial. Los establecimientos comerciales podrán certificar la identidad del cliente por medio del nuevo Documento de Identificación Civil y la utilización de lector biométrico, minimizando riesgos de prejuicios procedentes de acciones ilícitas.

Asociado a la utilización de tecnologías de punta, el RIC permitirá el registro de los ciudadanos brasileños luego de una investigación de las impresiones digitales en una única base de datos nacional, asegurando que para cada individuo sea emitido un número único de Registro de Identidad Civil por el que cada ciudadano brasileño, nacido o naturalizado, será identificado en sus relaciones con la sociedad y con organismos gubernamentales y privados; fortaleciendo todos los servicios que requieran a la identificación del ciudadano.

La herramienta para la investigación de impresiones digitales adoptada por Brasil y que será

utilizada para la investigación a gran escala en el Proyecto RIC, es el Sistema Automatizado de Identificación de Impresiones Digitales (acrónimo de Automated Fingerprint Identification System – AFIS) que es capaz de extraer con suficiente velocidad y precisión características particulares morfológicas, denominadas minucias, que permiten distinguir, entre si, las impresiones papilares, individualizando al ciudadano de forma inequívoca. Se trata, entonces, de la herramienta fundamental para la implementación del Registro de Identidad Civil.

El Departamento de Policía Federal ya dispone de un AFIS implementado y en operación en el Instituto Nacional de Identificación - INI y en sus veintisiete superintendencias regionales. El AFIS del INI posee una interfaz, llamada Inter-AFIS, que permite intercambiar informaciones con otros sistemas automatizados de Identificación de impresiones digitales que hayan adoptado el estándar ANSI/NIST-ITLI-2000 de la INTERPOL.

En otra vertiente, la Policía Federal posee una estructura tecnológica moderna, capaz de operacionalizar el sistema de comunicación e interoperabilidad entre los órganos participantes.

El Registro de Identidad Civil fue oficialmente lanzado el día 30 de diciembre de 2010, por el entonces Presidente de la República, Luiz Inácio Lula da Silva, y por el Ministro de Estado de Justicia, Luiz Paulo Teles Ferreira Barreto, con inversiones de cerca de 90 millones de reales proporcionados por el Ministerio de Justicia, y se basa en la condición especial de garantizar los derechos fundamentales del ciudadano.

El ministro de Justicia, Luiz Paulo Teles Ferreira Barreto, durante la ceremonia de lanzamiento del nuevo Registro de Identidad Civil, resaltó que el RIC es uno de los más modernos documentos de identificación del mundo: “El RIC es más seguro y más práctico, ya que incorpora en un solo documento diversos ítems de seguridad”. Su adopción traerá innumerables beneficios para la sociedad al garantizar la unicidad entre el ciudadano y su documento, utilizando la identificación dactiloscópica de forma automatizada. Esta medida fortalecerá los servicios públicos y privados que requieren la identificación del ciudadano, contribuyendo efectivamente para la reducción de fraudes contra personas físicas, jurídicas y entes gubernamentales.

Toda transición es un gran desafío y el punto de partida para este proceso exige un alto poder de articulación y de concentración de esfuerzos. En paralelo a esto, es necesario establecer directrices sólidas para su desarrollo y credibilidad. Debe considerarse, que en este proceso, las elecciones de estándares organizacionales y tecnológicos serán decisivos para direccionar el mercado y la propia evolución de las aplicaciones gubernamentales.

La implementación de una política de modernización del sistema de identificación civil, con la adopción de métodos, tecnologías, infraestructura y modelos de gestión contemporáneos, hará posible la introducción en la vida cotidiana del ciudadano de un documento de identidad civil inteligente y seguro que proporcionará mayor confiabilidad en sus relaciones con el Estado y con el sector privado, resguardando su privacidad y la integridad de las instituciones.

En este sentido, el Proyecto RIC se presenta como el resultado de la madurez técnica y gerencial adquirida en los años que antecedieron su inclusión efectiva con la agenda de Gobierno como Política Pública. Su propuesta y sus mecanismos de gestión fueron concebidos dentro de una

tendencia mundial y en el marco de la exigencia del Gobierno brasileño que vela por la garantía del estado democrático de derecho, por la seguridad y por el equilibrio social.

Brasil, país de dimensiones continentales que abriga realidades económicas y culturales muy diversas, ha ampliado su relevancia en el escenario internacional no sólo, por el potencial económico sino también, por la adopción de políticas públicas responsables que llevaron a la reciente inclusión social de millones de ciudadanos que vivían bajo la línea de pobreza. Tal contexto muestra las oportunidades y desafíos que requieren la adopción de acciones estructurantes para la adecuación del país a esta nueva realidad.

El proyecto RIC se encuadra estratégicamente en el rol de estas acciones al fortalecer su imagen en el ámbito internacional, y proporcionará el cambio de paradigma de las relaciones entre el Estado brasileño y la sociedad.

Bibliografía

1. Convención de Palermo, adoptada en Nueva York, el 15 de noviembre de 2000.
2. Decreto n.º 5.015, del 12 de marzo de 2004.
3. Decreto n.º 5.016, del 12 de marzo de 2004
4. Decreto n.º 5.017, del 12 de marzo de 2004
5. Decreto n.º 7.166, de 5 de mayo de 2010.
6. Decreto n.º 89.250, 27 de diciembre de 1983.
7. Ley n.º 7.116, del 29 de agosto de 1983.
8. Ley n.º 9.454, del 7 de abril de 1997.
9. Informe de las Mejores Prácticas Mundiales, de la Agencia para la Sociedad del Conocimiento de Portugal.
10. Término de Apertura del Proyecto de Registro de Identificación Civil.

Proyecto integral de renovación tecnológica del Registro Nacional de las personas de Honduras

Jorge Arturo Reina García



Jorge Arturo Reina García

Director del Registro Nacional de las Personas (RNP) y Presidente del Directorio del RNP.



Nacido el 8 de octubre de 1960 es Ingeniero Civil, con Maestría en Gerencia de Proyectos.

Se desempeñó como: Gerente de Empresas Productoras de Concreto (hormigón) y derivados fue Presidente de Ingeniería Gerencial, empresa pionera y líder en Honduras y C.A. en Gerencia de Proyectos y Sistemas de Información Geográfica (SIG o GIS). Capacitado como usuario de GIS y como Secretario de Organización del Consejo Central Ejecutivo del Partido Liberal (2,009 en ese momento era Partido de Gobierno).

Actualmente Director del Registro Nacional de las Personas, donde se está desarrollando un proceso de Reingeniería y Fortalecimiento institucional.

Información de contacto: 6to piso, Edf. Villatoro, Blvd Morazán,

Tegucigalpa MDC, Honduras;

Tel.: (504)22214425, (504)22215520

email: direcciónejecutiva@rnp.hn

jorgereina@hotmail.com

website: www.rnp.hn

Resumen

El Registro Nacional de las Personas (RNP) es un órgano especial, autónomo e independiente con autoridad nacional, con funciones y procesos por los que fue declarado Institución de Seguridad Nacional. Tiene por finalidad: planificar, organizar, dirigir y administrar con la más alta seguridad, el sistema integrado de registro civil e identificación de las personas naturales; para el manejo seguro, integral, eficiente y eficaz de la información y documentación. Su misión es la de garantizar la veracidad de la inscripción a perpetuidad de los hechos y actos relativos al estado civil de las personas naturales, el derecho universal a la identidad con un enfoque de derechos humanos, desarrollando y fortaleciendo el sistema democrático de Honduras; con el compromiso de prestar servicios de excelencia para alcanzar la confianza ciudadana.

El **Proyecto Integral de Renovación Tecnológica** del RNP de Honduras, consiste en la solución de los problemas estructurales de la Institución, de conformidad con su Naturaleza y Finalidad de Derechos Humanos (Inclusión Social), Seguridad Pública, así como el apoyo básico como institución relevante del sector Información Nacional, para los nacientes programas estatales: Gobierno Electrónico y Firma Electrónica.

El Proyecto Integral se desglosa de la siguiente forma:

Proceso de Modernización

- Reingeniería de procesos y Fortalecimiento institucional
- Adopción de Plan Estratégico, Políticas, Normas y Procedimientos;
- Reorganización de la Estructura administrativa;
- Capacitación.
- Proyecto Renovación Tarjeta de Identidad
- Actualizar y Homologar Bases de Datos de Registro Civil e Identificación;
- Mejoramiento de la Capacidad Instalada de los Registros Civiles Municipales;
- Renovación del Hardware Central;
- Actualización y ampliación del software del Sistemas de Registro Civil y del AFIS;
- Cambio de Línea de Impresión.

Interacción con otras Instituciones Públicas y Privadas

- Consulta Externa.
- Gobierno Electrónico.

Palabras clave: programas biométricos de gobierno; identificación de los ciudadanos; identificación para la inclusión social, seguridad pública, gobierno electrónico.

Proyecto integral de renovación tecnológica del Registro Nacional de las personas de Honduras

Antecedentes

En Honduras, el Registro Civil nace adscrito a las parroquias católicas del país en la década de 1890, trasladándose luego esta a las Alcaldías Municipales, donde se continuó realizando, en forma descentralizada hasta el año 1982 en que por Decreto del Congreso Nacional se creó y se transfirió esta responsabilidad al Registro Nacional de las Personas, dependiente del Tribunal Nacional de Elecciones, atribuyéndole las funciones de Registro Civil, Identificación Nacional de Personas y elaboración del Censo Nacional Electoral.

En el 2004 y mediante el decreto del Congreso Nacional se creó el Registro Nacional de las Personas (RNP) como órgano especial autónomo e independiente, con autoridad en todo el territorio nacional, con funciones y procesos de registro del Estado civil, administración y emisión de la documentación regstral, por los que se lo declaró Institución de Seguridad Nacional, al estar estrechamente vinculados a la seguridad de la sociedad teniendo por finalidad la planificación, organización, dirección y administración con la más alta seguridad desarrollando, para su logro métodos, técnicas, procedimientos modernos, controles tecnológicos, científicos y especializados, para el manejo seguro, integral, eficiente y eficaz de la información y documentación regstral. De aquí que la actividad principal del RNP es la administración eficiente y permanente del Sistema de Registro Civil, el registro de los actos y hechos del ciudadano del que se deriva el Sistema de Identificación Nacional que genera la Tarjeta de Identidad y es la base para que el Tribunal Supremo Electoral elabore el Censo Nacional Electoral como registro de los ciudadanos (as) aptos para ejercer el sufragio en los Comicios internos, primarios y generales del país.

En 1984 se levantó un inventario de inscripciones a nivel nacional y se creó un código numérico de trece (13) dígitos único para cada persona, se foliaron los libros de inscripción para seguridad de que estos no pudiesen modificarse y facilitar la captura de los códigos de Departamento, Municipio, año de inscripción y numero correlativo de acta de inscripción, el que se asigna dentro del municipio y se restaura cada año.

La estructura de dicho Código es la siguiente:

- Los cuatro (4) primeros dígitos identifican el departamento y municipio de inscripción;
- Los siguientes cuatro (4) dígitos designan el año de la inscripción y
- Los restantes cinco (5) dígitos corresponden al número de acta de inscripción en cada municipio, asignado en orden cronológica de presentación y reiniciándose cada año.

El código de Departamento es de dos dígitos (01 al 18 y 20 para los hondureños nacidos en USA) la variante del número se establece por el orden alfabético del nombre del Departamento. Está previsto que si se crea un nuevo departamento o se fusionan algunos existentes, se le asignará el código siguiente al último vigente.

El código de Municipio se estableció con similares criterios: a la cabecera departamental se

le asignó el código 01, a los demás Municipios se les asignó un correlativo en base al orden alfabético dentro del Departamento. A los nuevos municipios se les asignará el número a continuación del último vigente aplicándose la misma norma cuando se fusionen Municipios.

Hay códigos especiales para los hondureños por naturalización, a quienes se les asignó un código de Departamento y Municipio: 0890. El código 0880 se le otorgó a las personas que se acogen a tratados de doble nacionalidad y el 1292 para las personas que viven en las zonas recuperadas mediante sentencia de la Corte Internacional de Justicia en la Haya, Holanda.

A los hondureños reinscritos sin sentencia judicial, en base a la certificación que portaban de su inscripción de nacimiento emitida por el Registro Civil, pero que no constaba en los registros del RNP, se les asignó el código Departamental con la suma de 20 dígitos al código del departamento de inscripción.

El estado de Honduras, a través del RNP ha realizado esfuerzos permanentes para regularizar las inconsistencias, la integridad de los datos y la actualización del Registro Civil, para lo que ha ejecutado varios proyectos de reajuste de la información:

1. En 1983 Proyecto financiado por el AID y el Gobierno de Honduras para trasladar el Registro Civil de las Alcaldías municipales al RNP y crear la primera Tarjeta de Identidad con registro de Huellas Dactilares,
2. 1987 Proyecto de Actualización del Registro Civil (PARC), financiado por el AID,
3. 1991 Proyecto DEPUR, financiado por el TNE / RNP.
4. 1996 Proyecto OEA de Fortalecimiento al Registro Civil,
5. 2005 Proyecto OEA de Fortalecimiento a las Instituciones Democráticas, y
6. 2011 proyecto PNUD para reducir el Subregistro, digitalizar la información registral faltante.

Nota: Los Proyectos de actualización no han logrado concluir su labor y han generado información y Bases de Datos incompletas que se deben Homologar.

En materia de Identificación Nacional de personas se han ejecutado tres (3) proyectos:

1. En 1984 que crea la primera Tarjeta de Identidad con control Biométrico,
2. En 1996 que crea la primera Tarjeta de Identidad en el Mundo con control Biométrico y AFIS combinados, y
3. En el 2005 un Proyecto de actualización y Modernización del Documento de Identificación (Decadactilar) y del RNP.

El proyecto de 1996 inicio la identificación de los ciudadanos, usando un sistema biométrico dactilar, con dos bases de datos: la de las inscripciones del Registro Civil (nacimientos, defunciones, matrimonios, adopciones, etc.) con aproximadamente 12 millones de registros y la segunda con la información de emisión de aproximadamente 3,700,000 Tarjetas de Identidad única para igual cantidad de ciudadanos, con sus datos demográficos e imágenes (fotografía y huellas de los dedos índices). Desde esa fecha, se han incorporado más de 5 millones de emisiones para igual cantidad de ciudadanos de los que se dispone de datos demográficos e imágenes (fotografía y huellas de 3,234,927 registros con huellas dactilares de los dos dedos índices) y vectores de minucia. El proyecto del año 2005 implementó un sistema biométrico

decadactilar, por el que se dispone de datos demográficos e imágenes (fotografía y huellas de 1,802,730 con los 10 dedos de la mano), vectores de minucia y se mantiene en la base de datos de las inscripciones del Registro Civil (nacimientos, defunciones, matrimonios, adopciones etc.) la que se ha poblado con aproximadamente 16,000,000 de registros. La Tarjeta de Identidad vigente incluye información en el código de barras bidimensional (datos generales del ciudadano, departamento y municipio de solicitud, nombres de los padres).

Operación de los sistemas de RNP

El RNP atiende a 8,215,000 personas y opera con 333 oficinas y 1430 empleados a nivel nacional. Cuenta con 76 Registros Civiles Municipales (RCM) computarizados de los que 22, están en línea cubriendo el 70% de la población del país y 222 RCM que operan manualmente. Se dispone además de 20 Oficialías Civiles Departamentales, 15 Registro Civiles Auxiliares y algunas tareas en los Consulados hondureños a nivel mundial. La operación centralizada de desarrolla en 3 edificios y 1 bodega en la capital Tegucigalpa.

El sistema de Registro Civil se administra centralizadamente, aunque capta la información de manera descentralizada, basado en un número único de inscripción de nacimiento o naturalización que posteriormente se convierte en el número de tarjeta de identidad, complementado con un método de identificación biométrica de cada ciudadano. El sistema vincula la inscripción de nacimientos o naturalización con los datos de las demás inscripciones relativas al estado civil de las personas y la emisión de sus documentos de identificación.

Las Tarjetas de Identidad se emiten usando la información de la solicitud de la certificación de la inscripción de nacimiento, su domicilio actual, la Fotografía del ciudadano, sus huellas dactilares (pueden ser repuestas a petición del propietario) y se envían al municipio donde se solicitaron.

El Registro Civil opera en 312 locales, con por lo menos uno en cada Municipio del país.

El RNP tiene 23 ciudades conectadas en línea a la sede central, con equipo de captura de imágenes digital, (foto, huellas y firma) de los solicitantes de tarjetas de identidad. Además hay 53 ciudades que cuentan con equipo de captura de datos para trámites de Registro Civil y con los recursos para captura de imágenes digitales, (foto, huellas y firma) de los solicitantes de tarjetas de identidad, pero estas guardan la información en los equipos y posteriormente es enviada en CD's a la sede central para su procesamiento.

Así mismo, el RNP cuenta con 75 unidades móviles de captura de datos e imágenes en medio digital, (foto, huellas y firma), las cuales se desplazan a los lugares donde se necesite. Sin requerir facilidades, tienen su propia infraestructura y son capaces de atender solicitudes de identificación de ciudadanos; los datos se guardan y envían a la sede central en CD, o por Internet.

En el resto de oficinas se procesan las inscripciones de las personas naturales, en los libros correspondientes y se toma la huella de los ciudadanos con procedimientos manuales. La información se remite a la sede central por mecanismos tradicionales, para que esta se digitalice

y procese. Los Libros de Inscripción se envían hasta que están llenos. Las inscripciones se vinculan con los registros de nacimientos mediante las comunicaciones de anotaciones marginales, las que se remiten a los municipios y con copia al archivo central.

El sistema se complementa con las reposiciones por omisión y las rectificaciones o adiciones a las inscripciones originales por resolución especial, emitidas por los Registros Civiles Regionales u Oficialías Civiles, los que ordenan la inscripción en el registro respectivo. Actualmente no existe comunicación informática entre los Registros y Oficialías Civiles.

Sistemas informáticos implementados

El RNP atiende a los ciudadanos en todo el territorio nacional mediante las siguientes aplicaciones informáticas:

- **Registro Civil**

1. Captura y Certifica inscripciones en línea en RCM's Mecanizados y los libros digitales.
2. Captura de las Inscripciones, desde los libros de los Registros no Mecanizados.
3. Cruce de información de nacimientos, defunciones, matrimonios, etc., generando notas marginales a las inscripciones en las bases de datos.
4. Homologación de las Bases de Datos en los Registros Civiles.
5. Generación de estadísticas vitales
6. Construcción de árbol genealógico de cada persona
7. Generación de expediente u hoja de vida de cada persona
8. Extensión de certificaciones de inscripciones desde la Base de Datos
9. Mecanismos de consulta a la base de datos del Registro Civil
10. Procesos de auditoría a cambios, ingresos y modificaciones en Bases de Datos
11. Control de la producción
12. Multimedia (digitalización de las imágenes de los libros de inscripción)

- **Programa de Identificación Nacional**

1. Captura digital de datos e imágenes huellas, fotografía y firma y envío por Internet.
2. Trascipción de la información de los Registros Civiles no Mecanizados.
3. Digitalización de las huellas y la fotografía de los Municipios no Mecanizados
4. Integrar datos biográficos, demográficos, e imágenes, para envío al AFIS, por Internet.
5. Cotejo de huellas de las personas que solicitan por primera vez su Tarjeta de Identidad, contra las que ya están registradas en la base de datos AFIS.
6. Impresión de las tarjetas de identidad de primera vez, de reposición o renovación
7. Control de usuarios actuales
8. Control de solicitudes de emisión de tarjeta de identidad
9. Control de emisión y rechazos de tarjetas de identidad
10. Control de solicitudes de reposición de tarjetas de identidad
11. Respaldar la base de datos de tarjetas emitidas por primera vez

- **Consulta externa Sistema de Identificación Nacional y de Registro Civil**

1. Identificación cuenta con 3 componentes de búsqueda:
 - Autenticación:

- Identificación;
 - Consulta;
2. Registro Civil cuenta con 4 Módulos:
- Consulta por número de identidad;
 - Consulta por nombre;
 - Consulta del Árbol Genealógico;
 - Impresión de inscripciones de nacimiento;

El RNP presta estos servicios a entidades estatales con las que ha suscrito convenios:

1. Ministerio de Relaciones Exteriores con sus consulados en el extranjero;
2. Ministerio de Seguridad;
3. Ministerio de Finanzas;
4. Ministerio Público;
5. Dirección General de Migración y Extranjería;
6. Programa de Asignación Familiar PRAF;
7. Procuraduría General de la República;
8. Comisión Nacional de Bancos y Seguros;
9. Corte Suprema de Justicia, etc.

Situación actual

El RNP enfrenta la necesidad de renovar el actual documento de identificación, lo que implica un proceso masivo de enrolamiento, proceso e impresión del Documento de Identificación para más de 5 Millones de Ciudadanos (as), sumado a la necesidad de actualización y la implícita modernización de sus sistemas de información e infraestructura y la estructura administrativa, para mejorar la eficiencia operativa, mantener un proceso de mejora continua y liderar el proceso de implementación del Gobierno Electrónico. El rol preponderante que le corresponde jugar en el mismo la eventual implementación de la firma electrónica, combinado con un elemento distorsionante de tipo político, por la realización de las elecciones internas y primarias en Noviembre 2012 y de las Elecciones Generales en Noviembre 2013, que se superpone en tiempo con la probable implementación del proceso de renovación del Documento de Identificación Nacional, habida cuenta que el mismo sirve como Documento Electoral para que el ciudadano ejerza el sufragio en ambos procesos.

Esto ha llevado a la necesidad de iniciar un proceso de Reingeniería y Fortalecimiento Institucional que involucre toda la estructura del RNP, el que hemos iniciado con un diagnóstico que se realizó durante el año del 2010 y que demostró la situación siguiente:

1. La Exclusión Social de las personas que conforman en Honduras el Subregistro y la Subidentificación (oscila entre el 6% y el 8% de la población);
2. Falta o debilidad en el equipamiento, apoyo logístico, supervisión y calidad y capacitación de los recursos humanos debido a las Limitaciones Presupuestarias;
3. Problemas de Procedimientos Técnicos y Administrativos derivados de la inexistencia de Políticas, Normas y Procedimientos oficializados;
4. Problemas de Fraude documental (Inscripción, Usurpación Identidad, etc.)

5. La estructura administrativa es inadecuada para disponer de la cobertura geográfica, los servicios, la eficiencia operativa y mantener un proceso de mejora continua;
6. Debilidad de las capacidades que permitan la modernización de los sistemas de información, tanto en su Sistema de Registro Civil, de Identificación y el área administrativa;
7. La desactualización, dispersión e inconsistencia de las Bases de Datos tanto de Registro Civil como de Identificación, ya que aun los RCMs automatizados cuentan con equipos de capacidades limitadas y reducido numero en relación a la demanda;
8. Debilidad en la capacidad de proceso automatizado por la obsolescencia, desactualización o carencia de infraestructura informática y de comunicaciones en los sus Registros Civiles a nivel nacional,
9. Debilidad de la infraestructura de comunicaciones en todos los Registros Civiles a nivel nacional, lo que genera deficiencias en la Seguridad del proceso y en la agilidad y flexibilidad de la atención a los trámites;
10. La necesidad de incorporación como Institución relevante en el naciente proceso de implementación a mediano plazo del Gobierno Electrónico y la Firma Electrónica, ya que ambos se apoyan fuertemente en la identificación ciudadana, la certificación de usuarios y el intercambio de información, tareas que se deberán ejecutar en plataformas de comunicación robustas;
11. Renovación el Documento de Identificación (Tarjeta de Identidad), lo que implica la renovación o cambio para actualizar su capacidad informática en el Sistema de Identificación, en la línea de personalización del documento, en el enrolamiento y el proceso de las huellas;
12. Desactualización de recursos informáticos en la Sede Central para mejorar y fortalecer la seguridad del Sistema de Identificación;
13. Debilidad en las capacidades de Consulta Externa y de intercambio de información, para apoyar la gestión de las entidades estatales de los sectores de seguridad, Justicia, Ministerio Público, y de las instituciones privadas de servicios como telefonía celular, Banca, etc.,
14. Debilidad en las capacidades de los empleados para producir la generación de relevo;
15. Necesidad de nuevos Ingresos por servicios al Sector Privado como elemento de sostenibilidad del Proyecto y del RNP.

Plan de solución integral

El Plan para la Solución Integral de los problemas estructurales del RNP derivados del diagnóstico de las actividades obligatorias que se hacen mal, o que se hacen de forma incompleta o simplemente las que no se hacen; está sostenido en los Pilares siguientes:

- **Lucha contra el Fraude Documental**
 - Creación Comisión Antifraude (Secretarías de Seguridad, Interior, Migración, Ministerio Público y RNP)
 - Establecimiento de Controles internos y Coerción
- **Proceso de Modernización**
 - Reingeniería de procesos y Fortalecimiento institucional
- Adopción de Plan Estratégico, Políticas, Normas, Procedimientos técnicos y administrativos (Reglamentos, Manuales, etc.);

- Reorganización de la Estructura administrativa (Organigrama y Reclasificación de puestos y salarios)
 - Proyecto Renovación Tarjeta de Identidad
- Atualizar y Homologar Bases de Datos de Registro Civil e Identificación;
- Equipamiento y mejoramiento de comunicaciones de los Registros Civiles Municipales;
- Renovación del Hardware Central;
- Actualización (upgrade) y ampliación del software de el Sistemas de Registro Civil y el Biométrico de Identificación (matriz de rasgos faciales);
- Cambiar Línea de Impresión
 - Proyecto Identificación de Menores
 - Interacción con otras Instituciones Públicas y Privadas
- Consulta Externa
- Gobierno Electrónico

Acciones emprendidas en cumplimiento del plan integral

El RNP, a pesar de las grandes limitaciones presupuestarias ha estado trabajando con una nueva y amplia participación del personal más experimentado y capacitado de la Institución, con el Sindicato de Trabajadores del RNP y también actuando de cerca con el apoyo y confianza de Organismos Internacionales como el PNUD, la Cooperación Española y Sueca para el desarrollo, UNICEF, la embajada de EUA, las ONG Plan en Honduras, Visión Mundial.

Es importante destacar que en la ejecución de Proyecto “Fortalecimiento Institucional de RNP y la disminución del Subregistro y la Subidentificación en Zonas Excluidas de Honduras” (PNUD, AGDI, AECID, RNP) se logró el honor de ser calificados como el **Mejor Proyecto** en Honduras (PNUD), en virtud de la innovación de figuras y registrales para la solución del problema de las personas que aún no han tenido el universal derecho a “un nombre y una nacionalidad”, debido a la exclusión económica, social o geográfica, entre las que destacan:

- La creación del Promotor Registral
- La creación del Libro de Subregistro
- La disminución o agilización de requisitos de inscripción para personas excluidas (incluyendo anteproyecto de ley junto con Secretaría de la Presidencia)
- Adquisición de recursos (Vehículos de Inscripción Ciudadana, equipos móviles automatizados, etc.) para las Brigadas Móviles de Inscripción e Identificación
- Coordinación con Instituciones vinculadas (Programas estatales sociales, PRAF, ONGs, Organizaciones sociales locales, Alcaldías, etc.)

Así mismo, en la ruta del cumplimiento del Plan Integral del RNP, se han ejecutado una amplia serie de acciones que se resumen a continuación:

- **Lucha contra Fraude Documental**
 - Reactivación de Comisión Antifraude (Secretarías de Seguridad, Interior, Migración, Ministerio Público y RNP)
 - La Depuración del personal vinculado con actos de corrupción esta en marcha con resultados preliminares producto del “Secuestro de Documentos”, mas de 100 mil expedientes y solicitudes de identificación en oficinas de todo el país con indicios racionales de fraude.

Dicho operativo a dado como resultado hasta el momento acciones correctivas de recursos humanos así: 20 destituciones, 65 suspensiones, 225 llamados de atención y inicio de procesos judiciales. Además, ya se vive una nueva cultura antifraude en el RNP.

- **Reingeniería y Fortalecimiento Institucional**

- El Proceso de Reingeniería,

Inicio el RNP revisando la Estructura Organizacional y elaborando los controles, los procedimientos operativos administrativos y técnicos, mediante los siguientes productos:

- Borrador de Reformas a la ley del RNP
- Reglamentos (Ley, Régimen Carrera Registral)
- 19 Manuales de Seguridad, procedimientos (administrativos y técnicos), funciones, puestos y salarios, etc.
- Nueva Estructura Administrativa (Organigrama)
 - Creación del Instituto Superior de Estudios Registrales (PNUD y AECID), al mismo tiempo hemos iniciado un proceso de Capacitación del Personal como nunca antes sucedió.
 - Emitir un Documento de Identificación para menores de 18 años, cuyo rango comienza al cumplir 12 años el niño, lo que evitara la usurpación de los números de identidad, al obtener el registro Decadactilar tempranamente;
 - Proyecto Renovación de la Tarjeta de Identidad
- Actualización de las Bases de Datos de Registro Civil incorporando los Libros del 2004 a la fecha;
- Iniciar el proceso de revisión de los Logs de Auditoria de actualización de las Bases de Datos de Registro Civil;
- Identificar las inconsistencias entre Bases de Datos de Registro Civil e Identificación para corrección conjunta con los Registros Civiles Municipales
- Análisis preliminar de alternativas para homologar las Bases de Datos de Registro Civil primero y después las Bases de Datos de Registro Civil e Identificación, combinadas con las Bases de Datos de Imágenes de Archivo Central;
- Iniciar el Desarrollo de un nuevo Sistema de Registro Civil, (PNUD y Departamento de Informática y Registro Civil)
- Mejora del Sistema de Comunicaciones utilizando tecnología de punta, mediante infraestructura de Internet y VoIP
- Se ha definido el Plan de Renovación Tecnológica del RNP que comprende las áreas siguientes:
 - Elaborar planes;
 - Normalizar los tipos de locales, Mobiliario y configurar los equipos;
 - Determinar las necesidades de Software;
 - Diseño del Sistema de Comunicación Integral requerido para cada Registro Civil Municipal, áreas Administrativa, Técnica Informática, Registral y de Identificación;
 - Elaborar e Implementar la Pagina Web con Sistemas de Consulta a Registro Civil e Identificación, Trámites institucionales a nivel informático en el Marco de la estrategia de Gobierno Electrónico (en conjunto con PNUD);
 - Definir Proyecto de Renovación de la Tarjeta de Identidad, estableciendo la estrategia y planes para el proceso:
 - Seleccionar el Material y Medidas de Seguridad del Documento de Identidad.
 - Definir Estrategias de Enrolamiento e Impresión

- Elaborar Plan de Mecanización de Registros Civiles por etapas
- Crear Estructura Administrativa (Comité) temporal del Proyecto.
- Elaborar Términos de Referencia para la Adquisición de los recursos del Proyecto
- Elaborar Metodología Transparente de Evaluación de Ofertas y adjudicación de Contrato(s) con alta Concurrencia de proponentes; proceso de licitación Internacional con intermediación (contratación) de un Organismo Externo experto (PNUD, OEA, etc.) y Supervisión Nacional e Internacional (Tribunal Superior de Cuentas, Comisión Nacional Anticorrupción, Iglesias, Tribunal Supremo Electoral, OEA, ONU, etc.)
- Informar el Proyecto de Renovación de Tarjeta de Identidad a 15 empresas Internacionales interesadas
 - Presentación de el Proyecto Integral de Renovación Tecnológica del RNP al Congreso Nacional,

Para someterlo discusión y aprobación de los recursos financieros. Los Componentes Relevantes para la ejecución por etapas son:

- Actualización, Depuración, Unificación y Homologación de las Bases de Datos de Registro Civil e Identificación;
- Transcripción de Libros;
- Depuración de Bases de Datos de Archivo Central, Registro Civil e Identificación;
- Homologación de Bases de Datos del RNP
- Modernización y Fortalecimiento de Registros Civiles Municipales
- Locales adecuados;
- Equipamiento;
- Comunicaciones;
- Enrolamiento o Captura de Información
- Foto;
- Huellas;
- Actualización domiciliar, Datos personales, etc.
- Sistema biométrico de identificación (AFIS)
- Actualización de software (upgrade);
- Reposición de hardware;
- Línea de Impresión
- Maquinas Impresoras de Tarjetas de Identidad
- Material de Tarjetas de Identidad
 - Beneficios del Proyecto
- Inclusión Social
- Seguridad en Documentos y Base de Datos;
- Servicios de Calidad al Pueblo, Instituciones Públicas y Privadas;
- Censo Electoral Depurado;
- Estadísticas Vitales oportunas y confiables (desde 89 no hay en Honduras);
- RNP convertido en verdadera Institución de Seguridad Nacional
- Confiabilidad;
- Ahorros adicionales del Estado;
- Nuevos Ingresos;

- Capacidad de respuesta inmediata del RNP para la Implementación gubernamental de Gobierno Electrónico.

Ciudades mecanizadas no en línea

Cod. Depto	Cod. Mun.	Departamento	Municipio
01	04	Atlántida	Jutiapa
01	06	Atlántida	San Francisco
01	08	Atlántida	Arizona
02	01	Colón	Trujillo
02	02	Colón	Balfate
02	05	Colón	Saba
02	08	Colón	Sonaguera
04	04	Copan	Copan Ruinas
04	09	Copan	El Paraiso
05	02	Cortés	Omoa
06	04	Choluteca	Duyure
06	06	Choluteca	El Triunfo
06	15	Choluteca	San Marcos de Colón
07	01	El Paraiso	Yuscaran
07	04	El Paraiso	El Paraiso
07	19	El Paraiso	Trojes
08	06	Fco. Morazán	Guaimaca
08	16	Fco. Morazán	Sabanagrande
08	24	Fco. Morazán	Talanga
09	01	Gracias a Dios	Puerto Lempira
10	01	Intibuca	La Esperanza
10	04	Intibuca	Concepción
10	06	Intibuca	Intibuca
10	09	Intibuca	Masaguara
11	01	Isla de la Bahía	Roatan
12	08	La Paz	Marcala
13	01	Lempira	Gracias
13	07	Lempira	Guarita
13	09	Lempira	La Iguala
13	10	Lempira	Las Flores
13	11	Lempira	La Unión
13	12	Lempira	La Virtud
13	13	Lempira	Lepaera
13	16	Lempira	San Andres
13	18	Lempira	Sn Juan Guarita
13	20	Lempira	San Rafael
13	26	Lempira	Valladolid
14	01	Ocotepeque	Ocotepeque
14	07	Ocotepeque	La Labor
14	13	Ocotepeque	San Marcos
14	06	Ocotepeque	La Encarnacion
14	08	Ocotepeque	Lucerna
14	16	Ocotepeque	Sinuapa
15	02	Olancho	Campamento

15	05	Olancho	Dulce Nombre de Culmi
15	23	Olancho	Froylan Turcios (Patuca)
16	13	Santa Barbara	Macuelizo
16	16	Santa Barbara	Petoa
16	17	Santa Barbara	Protección
16	25	Santa Barbara	San Vicente Centenario
17	07	Valle	Langue
18	01	Yoro	Yoro

Ciudades conectadas

Cod. Depto	Cod. Mun.	Departamento	Municipio
01	01	Atlántida	La Ceiba
01	07	Atlántida	Tela
02	09	Colón	Tocoa
03	01	Comayagua	Comayagua
03	18	Comayagua	Siguatepeque
04	01	Copan	Sta. Rosa de Copan
04	13	Copan	Nueva Arcadia
05	01	Cortés	San Pedro Sula
05	02	Cortés	Choloma
05	06	Cortés	Puerto Cortes
05	11	Cortés	Villa Nueva
05	12	Cortés	La Lima
06	01	Choluteca	Choluteca
07	01	El Paraizo	Danli
08	01	Fco. Morazan	Distrito Central
12	01	La Paz	La Paz (sólo Registro Civil)
15	01	Olancho	Juticalpa
15	03	Olancho	Catacamas
16	01	Santa Barbara	Santa Barbara (sólo Registro Civil)
17	01	Valle	Nacaome (sólo Registro Civil)
17	09	Valle	San Lorenzo
18	04	Yoro	El Progreso
18	07	Yoro	Olanchito



Mapa RCM automatizados y en línea

Bibliografía

Términos de referencia Proyecto de actualización tecnológica del Registro Nacional de las Personas.

“Ley del Registro nacional de las Personas”.

Identificación para la inclusión social y digital

Dra. Mónica Litzá



Dra. Mónica Litza

Directora Nacional del Registro Nacional de Reincidencia.



La Dra. Mónica Litza, graduada de la carrera de abogacía, se ha desempeñado como Senadora de la Provincia de Buenos Aires durante el periodo 2003-2007. Actualmente, ocupa el cargo de Directora Nacional del Registro Nacional de Reincidencia dependiente del Ministerio de Justicia y Derechos Humanos. Es Autora de la Ley 13.666 “Firma Digital, Digitalización de Procedimientos de la Administración Pública Provincial”.

Ha sido expositora en diversos Seminarios y Congresos, destacándose el III, IV y V Congreso Internacional de Biometría de la República Argentina; la III Reunión Regional de Usuarios de AFIS de América Latina y el Caribe “Nuevos parámetros de identificación biométrica”, Perú, 2010; el Biometric Consortium Conference, Tampa, E.E.U.U; 2010 y Biometrics 2010, Londres, Reino Unido, “Argentinean Biometrics: One Step Forward”.

Información de contacto: Tucumán N° 1353. C.P.: 1050

Ciudad Autónoma de Buenos Aires

email: mlitza@dnrec.jus.gov.ar

web (personal): <http://www.monicalitza.com.ar>

Resumen

Esta nueva participación nos permite una vez más profundizar sobre el acontecer biométrico dentro de Administración Pública Argentina.

El haber planteado en el trabajo anterior la descripción de las funciones que desempeña el Registro Nacional de Reincidencia nos exime abundar acerca del análisis funcional y hace posible avanzar sobre aspectos coyunturales de la realidad biométrica de nuestro país.

En tal sentido, nos permitimos a lo largo del capítulo analizar en forma integral los aspectos económicos, políticos y sociales que determinaron la construcción del modelo biométrico y la conexidad que presenta con las actuales políticas de Estado.

También hemos considerado oportuno resaltar el papel de las Tecnologías de la Información y las Comunicaciones en la elección del paradigma para avanzar luego, desde lo empírico, en la elaboración de un diagnóstico de esa realidad biométrica por la que transitamos, destacando su importancia como instrumento que trasciende la mera identificación para convertirse en una herramienta política de inclusión social.

El desarrollo de plataformas informáticas y el avance de los medios digitales de almacenamiento han permitido repensar los modelos de gestión y reasignar funciones a los sistemas existentes de identificación biométrica.

En esa sintonía, hemos presentado al lector dos desarrollos que permitirán articular la interoperabilidad de las bases públicas biométricas, con el propósito de diseñar políticas de seguridad que optimicen el cumplimiento de las funciones que le son propias al Estado.

Identificación para la inclusión social y digital

Introducción

"Yo soy yo y mi circunstancia..."

Sin duda esa frase aparecida en la obra de Ortega y Gasset (1883- 1955), “Meditaciones del Quijote”, constituye el punto de partida para desentrañar la importancia de la biometría, sus tendencias y la trascendencia como herramienta política de inclusión social y digital dentro del trazado de la Agenda Digital Nacional.

De este modo esa “realidad circundante” elaborada por el hombre, integra la otra mitad de la persona y constituye la técnica, es decir, la reforma que el hombre impone a la naturaleza en vista de la satisfacción de sus necesidades. Solo así el hombre es un ser compuesto de realidades circunstanciales creadas como fuente inspiradora de las culturas neo-pensantes.

Entonces, “esa realidad” no es más que una proyección de la creación humana y como tal trasciende a la misma sin dejar de integrarla.

Así, poder hablar de biometría implica hablar de esa realidad técnica y efectuar a lo largo del capítulo un análisis integral para aproximarnos a su ubicación como componente de la realidad social, en el marco del diseño de políticas de Estado inclusivas, sin soslayar el papel que cumplen las Tecnologías de la Información y las Comunicaciones (TIC's).

Podemos afirmar que la biometría ha trascendido a la ciencia de la identificación de personas para transformarse en una herramienta de inclusión social, desde el momento que posibilita al ciudadano una mejor integración dentro de la actividad estatal cotidiana.

No podría avanzarse en un análisis sobre la “realidad biométrica”, sin definir previamente su “realidad circundante”.

La biometría como método dedicado a la identificación de las personas valora aspectos fisonómicos o conductuales, materializa el Derecho a la Identidad y a través de ese derecho basal que debe garantizar el Estado, se articula un nuevo plexo de derechos que resultan indispensables para la existencia e integración de la persona como “ser social”.

En la actualidad, todo proceso que se cumple dentro de los sistemas biométricos requiere de un desarrollo tecnológico adecuado en el cual la mayoría de las instancias de captura, cotejo y resultado se efectúan en entornos íntegramente digitales.

Debemos adelantar que nos inclinamos por entender a la biometría como una herramienta inclusiva desde lo social e integrativa desde lo digital, que forma parte de un concierto de recursos establecidos en el marco de políticas de Estado, donde la idea de reforma y reparación están dirigidas a satisfacer las necesidades sociales y garantizar los derechos ciudadanos.

Para valorar la importancia de la biometría como herramienta es imprescindible establecer la

prioridad que esta tiene dentro de las políticas de Estado que determinan la Agenda Digital Nacional. De esta planificación participan el revisionismo crítico, la elección de un modelo con horizonte de universalidad, la integración regional y la propia identidad soberana.

Los principios rectores del gobierno electrónico, las normas que aseguran la ciberseguridad de redes, los programas destinados a asegurar la disminución de las brechas digitales, aquellos que fomentan la alfabetización digital, los destinados a tender nuevas plataformas informáticas, los programas de protección a la industria del software y los que atienden al desarrollo del hardware, son protagonistas de la Agenda Digital.

Desde la Subsecretaría de Tecnologías de Gestión de la Jefatura de Gabinete de Ministros se coordina el uso de las tecnologías, observando los estándares de interoperabilidad y compatibilidad que resulta el denominador común en el proceso de integración que permite potenciar y revalorizar la información que resguarda el Estado Nacional. Esta coordinación es fundamental al momento de proyectar y planificar las políticas a mediano y largo plazo.

La incorporación tecnológica en los organismos estatales

“La tecnología solo encuentra sentido en la medida que esté provista de contenido”

Como hemos mencionado, la biometría como método de identificación, autentica datos en un entorno digital. Por lo tanto resulta de utilidad hacer un análisis retrospectivo sobre el avance tecnológico de las últimas décadas acontecido en la sociedad en su conjunto y su correlato dentro de la Administración Pública.

La necesidad de ser interoperables, es un diagnóstico de nuestra “realidad circundante” y por lo tanto debemos atender sus causas.

Las políticas neoliberales de la década de los '90 produjeron una de las mayores regresiones en la distribución del ingreso y como consecuencia inmediata se incrementaron las desigualdades sociales, en un contexto de apertura comercial y financiera producto de la desregulación económica.

En ese marco, se incorporaron al mercado en forma masiva bienes de capital importados, entre los cuales se encontraban el software y hardware. Por otra parte, la demanda de mayor complejidad de software y de servicios informáticos se abastecía desde el exterior, en lo que puede considerarse una clara dependencia tecnológica, acentuándose la brecha existente, en particular dentro de los organismos públicos.

Hacia fines de esa década, una encuesta efectuada por Microsoft, establecía que en nuestro país sobre el 74 por ciento de las personas que poseían televisión, solo el 7,4 por ciento era propietario de computadoras, cifra alarmante que debe integrarse con el dato de que el 67 por ciento del parque de computadoras se ubicaba en la Capital Federal.

Hoy la realidad da cuenta que “En el año 2001 el 30 por ciento de los hogares tenía acceso a Internet y, en 2010, ello se elevó al 47 por ciento, es decir, benefició a más de 5 millones de ciudadanos”, según expresara la presidenta Cristina Fernández de Kirchner en la casa de Gobierno

al presentar el sitio web Infojus, del Servicio Argentino de Información Jurídica del ministerio de Justicia, que permitirá el acceso libre y gratuito de los ciudadanos a toda la información jurídica del país.

Si nos detenemos por un instante en el párrafo anterior podemos comprender, sin lugar a dudas, que el desafío ha sido extender la inclusión a la mayor cantidad de ciudadanos y organismos estatales en la agenda digital nacional, para lo cual se han establecido estrategias que entienden la inclusión digital como una herramienta fundamental para la inclusión social.

El cambio cultural que deviene de acercar los recursos tecnológicos a la ciudadanía ha sido complementado con programas de alfabetización digital destinados a asegurar las condiciones de acceso y mejorar su calidad de uso.

Analizar el impacto de la construcción digital, dentro de los organismos de la Administración Pública, significa hablar de los distintos niveles de desarrollo tecnológico y de la utilidad en función del servicio específico que presta en relación con la potencialidad del usuario para acceder a ese servicio digital.

Pensar la inclusión digital desde un organismo estatal, es pensar en acortar las brechas sociales existentes en cuanto al acceso a los servicios por parte de los ciudadanos y también poder establecer entre los estamentos de la Administración Pública Nacional, verdaderos puentes digitales que conecten la sociedad de la información.

En lo que respecta al Registro Nacional de Reincidencia, el proceso de informatización y digitalización lleva más de una década. A través del “Programa de Reforma del Sistema de Justicia” se adquirió el software y hardware que posibilitó la digitalización de los archivos de antecedentes penales respetándose los estándares internacionales respecto de los datos biométricos allí contenidos, permitiendo asegurar la interoperabilidad a futuro con otras bases de datos.

Además, la implementación de la Firma Digital Ley Nº 25.506 ha permitido certificar los Informes de Antecedentes Penales de manera más segura y que, conjuntamente con la aplicación de nuevos sistemas de captura de datos ha posibilitado ampliar los parámetros de identificación, lo que finalmente redunda en una mejor utilización de los datos que administra el organismo.

Nos encontramos transitando el camino hacia una cultura dospuntocerista, donde participan los conceptos de apertura, cooperación e interoperabilidad, es decir la construcción de un Registro abierto e inteligente dentro del concepto de gobierno abierto.

Es importante resaltar que la incorporación de tecnología solo encuentra sentido en la medida que esté provista de contenido, razón por la cual debe ser conducida con claridad desde la política, dado que constituye una herramienta imprescindible en los procesos de transformación.

Las Tecnologías de la Información y las Comunicaciones aplicadas en un contexto de innovaciones constantes vienen a suprimir una amplia franja de tareas que conllevan un ritual burocrático.

Promover el desarrollo digital como plataforma operativa de los sistemas biométricos desde el Estado, requiere crear un contexto que fomente la instalación de nuevos emprendimientos destinados a proveer hardware y software, lo que implica determinar estrategias de crecimiento que alienten desde la ciencia y la educación.

Esos nuevos emprendimientos se materializan de diversas maneras, a través de medidas protectoras que promueven la industria nacional o bien mediante normas como la recientemente sancionada Ley 26.685 de Expedientes Digitales que autoriza la utilización de expedientes, documentos, firmas, comunicaciones, domicilios electrónicos y firmas digitales en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales.

El gerenciamiento público implica diseñar en forma constante nuevos instrumentos que acompañen esa “realidad circundante” que se encuentra en constante evolución. Es por ello, que al momento de proponer la reforma a la Ley 22.117 del Registro Nacional de Reincidencia, hemos resaltado el valor que la biometría presenta como componente fundamental en la lucha contra el delito, reafirmando que resulta de singular importancia en el diseño de las políticas de seguridad.

Entendemos que el éxito en la definición de las estrategias de simplificación de los procedimientos dentro de la Administración Pública, reside en la capacidad para establecer un modelo de gestión acorde a la especificidad de las funciones, lo cual implica el abandono de políticas anacrónicas para dar paso al concepto de organismo abierto y proactivo.

Los conceptos rectores de cooperación, interconexión e interoperabilidad, motores de las actuales políticas públicas, la constante innovación tecnológica en entornos digitales, han posibilitado la construcción de nuevas plataformas destinadas a ampliar el servicio que tradicionalmente prestaba el Registro Nacional de Reincidencia con el objeto de ampliar la interacción con las fuerzas de seguridad a través del Sistema de Consulta Nacional de Rebeldías y Capturas (Co.Na.R.C.), con la Agencia Nacional de Seguridad Vial, mediante la Consulta Nacional de Inhabilitados para conducir (Co.N.I.C.) y con el Registro Nacional de las Personas para la emisión de los nuevos pasaportes (Co.N.A.A.P.).

Nuevos instrumentos que posibilitan la integración e interactuación

“Ese dato que necesito, otro ya lo tiene”

Plataforma de enlace de bases públicas

La nueva arquitectura social que establece Internet, impulsada por el actual Gobierno y materializada a través del Plan Nacional de Telecomunicaciones “Argentina Conectada”, tiene como eje estratégico la inclusión digital. Esto hace posible pensar en uniones estratégicas dentro de la Administración Pública que concentren la información para el cumplimiento de las funciones específicas de cada uno de los órganos estatales.

La coordinación e integración de las bases de datos biométricos a través de plataformas

tecnológicas ubica al Estado frente a nuevos escenarios donde resulta imperiosa la correcta y ágil identificación de las personas. Para aquellos organismos que, como en nuestro caso, se vinculan con la identificación de personas, dicha integración resulta estratégica dado que permite conectar e intercambiar información biométrica que en la actualidad se presenta en compartimentos estancos.

La puesta en marcha de una Plataforma potenciará el tratamiento de los datos biométricos mediante la utilización de entornos digitales donde se pone de relieve el mejor funcionamiento del Estado.

Estos desarrollos constituyen de alguna manera el puntapié inicial para seguir construyendo un Estado en red donde participan modelos organizacionales flexibles

Los actores que integrarán dicha Plataforma son el Registro Nacional de las Personas, la Dirección Nacional de Migraciones, el Registro Nacional de Reincidencia y la Policía Federal Argentina, y poseen como denominador común la existencia de bases de datos biométricos digitalizadas que a pesar de ser plenamente interoperables en la actualidad, aún no han interactuado.

Por otra parte, la Plataforma de Enlace de Bases Públicas constituye la piedra basal sobre la cual se sustenta la implementación de diversos sistemas como el que presentaremos a continuación.

Un registro que trabaja en red



Consultas Nacional de Inhabilitados para Conducir (CONIC): El RNR brinda los antecedentes referidos a las inhabilitaciones para conducir para la obtención de todas las licencias.



Consultas desde Móviles Policiales: El RNR participa junto a otros organismos como el RENAPER, el RENAR y el Registro Automotor. Concretamente los efectivos policiales pueden acceder directamente desde sus móviles a la CONARC.



Consulta Nacional Antecedentes Penales para Pasaporte: El RNR trabaja conjuntamente con el RENAPER, el Ministerio del Interior consulta antecedentes penales y la base CONARC para los ciudadanos que tramitan el pasaporte.

REGISTRO NACIONAL DE REINCIDENCIA

Un nuevo paradigma de Estado

CONIC
Consulta Nacional de Inhabilitados para Conducir

CONARC
Consulta Nacional de Rebeldías y Capturas

CONAPP
Consulta Nacional de Antecedentes Penales para Pasaportes

SINABIP
Consulta Nacional de Búsqueda e Identificación de Personas

PLATAFORMA DE ENLACE DE BASES PÚBLICAS

Sistema Nacional de Busqueda e Identificacion de Personas – Si.Na.B.I.P.

Este sistema constituye el primer desarrollo a nivel nacional destinado a la búsqueda e identificación de personas, mediante el cual el Estado brinda una respuesta genuina a las necesidades sociales salvaguardando la debida identificación y asegurando el Derecho a la Identidad.

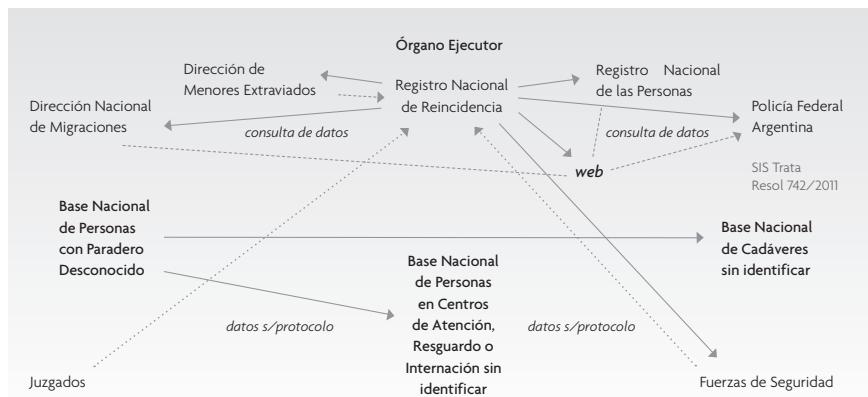
El objetivo es interconectar a diversos organismos que manejan información biométrica como el Registro Nacional de Reincidencia, el Registro Nacional de Información de Personas Menores Extraviadas, el Registro Nacional de las Personas, la Dirección Nacional de Migraciones y la Policía Federal Argentina.

Los datos biométricos de las personas incluidas en el sistema serán almacenados en tres bases independientes, las que además de entrecruzarse en forma permanente, serán cotejadas con aquella información que obra en las bases de los organismos que integran el sistema. Su dinámica funcional, sumada a la proyección de la información útil, asegura a través de las constantes búsquedas la probabilidad de éxito.

En el caso concreto, las autoridades judiciales, las Fuerzas Federales y de Seguridad del país representan los canales comunicacionales del sistema, ya que mediante estos actores se recepciona y trasmite la información, que resulta de vital importancia para adoptar con la mayor celeridad las medidas conducentes para cada caso.

Esta herramienta brindará asistencia a potenciales víctimas de delitos complejos, como la trata de personas, la privación ilegal de la libertad o el secuestro extorsivo. Constituye de este modo un aporte significativo en materia de políticas de seguridad pública.

Esquema funcional del Sistema Nacional de Búsqueda e Identificación de Personas



Conclusión

En los últimos años se han implementado políticas de gestión tendientes a estandarizar el manejo de los datos biométricos, obrantes en bases públicas digitales, con el propósito de asegurar su interoperabilidad.

Los que participamos de la gerencia pública entendemos que sólo a través un fuerte liderazgo político es posible conducir los procesos de transformación.

El uso de la biometría, como método de identificación no invasivo, requiere de una serie de acciones coordinadas para fomentar el desarrollo tecnológico como también la capacitación en el uso de esas nuevas tecnologías.

Por otra parte, tal como lo hemos sostenido a lo largo del presente capítulo, podemos afirmar que la biometría trasciende a la ciencia de la identificación de personas para transformarse en una herramienta de inclusión social, desde el momento que posibilita al ciudadano una mejor integración dentro de la actividad estatal cotidiana, como lo es su identificación para la obtención de beneficios de la seguridad social, el Certificado de antecedentes penales, la tramitación de la licencia de conducir, radicación, ciudadanía, la obtención del documento de Identidad y el pasaporte.

Para finalizar podemos intentar una analogía respecto de la máxima “somos lo que compartimos” la cual traslada al acontecer biométrico nos permite tomar conciencia que “en la actual realidad biométrica compartir nos da seguridad”.

Bibliografía

Criado, J.I. y Ramilo, M.C.: “E-Administración: ¿Un reto o una nueva moda? Problemas y perspectivas de futuro en torno a internet y las tecnologías de la información y la comunicación en las administraciones públicas del siglo XXI”. Instituto Vasco de la Administración Pública.

Achiary, Carlos (2005): “Interoperabilidad para el gobierno electrónico”, X Congreso Internacional del CLAD sobre Reforma del Estado y la Administración Pública, Santiago, Chile, 18-21 de octubre de 2005

Calderón, Cesar ; Lorenzo, Sebastián (2010): “Open Government - Gobierno Abierto” 1 ed. Buenos Aires, Capital Intelectual.

Cabello, Roxana (2003): “Argentina Digital” Ed. Universidad Nacional de General Sarmiento. Biblioteca Nacional.

Avance de los proyectos biométricos en el Servicio Penitenciario Federal

Néstor Matosian



Néstor Matosian

Director del COPIC - Servicio Penitenciario Federal.



Nacido el 10-02-1954 en Buenos Aires, ingreso a la Escuela Penitenciaria de la Nación en septiembre de 1975 obteniendo el título de Perito Dactiloscopo en 1978. (Colegio de Dactiloscopos de Capital Federal).

Funciones relevantes:

Año 1995/97: Jefe Centro Recuperación Enfermos de S.I.D.A., Instituto de Detención de la Cap. Fed. (U.2) Devoto.

1998/99: Jefe de Área- División Seguridad Interna del mismo Instituto.

2000: Secretario y Jefe de División Jóvenes Adultos en la Ex prisión de la Cap-Fed. (U:16)

2001: Jefe División Seguridad Externa Centro de detención de mujeres Ntra. Señora del Rosario de San Nicolás (U.31), el mismo año secretario del Complejo Penitenciario Federal I-Ezeiza.

2002: Subdirector Instituto Correccional de Mujeres (U.3)-Ezeiza.

2003: Curso de perfeccionamiento para oficiales Jefes.

2004: Subdirector Colonia Penal de Viedma (U.12)

2005: Director de la Dirección de Judicial, año 2006 Director del Instituto de Detención de la Cap.Fed. (U.2) Devoto, hoy Complejo C.A.B.A.

2007: Director General de Régimen Correccional

2008/2009: Director General del Cuerpo Penitenciario.

2010: Subdirector Nacional del Servicio Penitenciario Federal.

A partir del mes de agosto de 2010 miembro del Consejo de Planificación y Coordinación del S.P.F.

Resumen

En la actualidad la Biometría es una herramienta que se utiliza en el Servicio Penitenciario Federal con el objetivo de lograr la inclusión social, en pos de la reinserción que la Nación necesita.

El control de acceso de visitas, el enrolamiento de internos, la telefonía pública multi-biométrica, la visita virtual biométrica, internet con PIV, son algunos de los proyectos que el Servicio Penitenciario Federal está desarrollando junto al Ministerio de Justicia y la ONTI, con el fin de trabajar con mayor celo y eficiencia en la reinserción social, facilitando el acceso a las nuevas tecnologías y simplificando las visitas familiares.

Avance de los proyectos biométricos en el Servicio Penitenciario Federal

En el año 2005, el ex presidente Dr. Néstor Kirchner designó con el nombre de *Roberto Pettinato* a la Academia Superior de Estudios Penitenciarios. En esa oportunidad, el ex mandatario recordó que fue el Inspector General Pettinato quien promovió, a principios de la década del '50, las reformas que introdujeron el principio de socialización como pilar en el trato hacia las personas recluidas en el sistema penitenciario.

Desde el nombramiento del Inspector General Pettinato al frente de la Institución, el Servicio Penitenciario Federal (SPF) es signo del esfuerzo en el tratamiento educativo y socializador, con el fin de lograr la reinserción social, dándole este sentido y nunca el castigo, a la pena privativa de libertad. Desde entonces, es función de la propia Institución superarse y mejorar día a día en esta tarea dificultosa, pero de una enorme importancia en el contexto de la seguridad de todos los habitantes de la Nación.

El SPF, en 1947, inicia lo que se conoce como el Período de la Reglamentación Progresista de la Ley 11.833. Esta ley, entre otras cosas, crea la Escuela Penitenciaria con la idea de formar cuadros para la socialización de los internos.

Es con la llegada del Inspector General Pettinato que el SPF procura, no sólo plasmar en la realidad todas las conquistas ya iniciadas por la ley 11.833, sino acentuar aún más los principios correccionales y humanistas que siempre han servido de norte al penitenciarismo argentino.

Si bien la consolidación como Institución se realiza a comienzos de 1958 con la sanción de la Ley Penitenciaria Nacional complementaria del Código Penal (Decreto ley N° 412, del 14 de enero de 1958, ratificado el 23 de octubre del mismo año por el Congreso de la Nación mediante Ley 14.467) dentro de la normativa penitenciaria nosotros, denominamos a ese período, como la unificación legal del régimen penitenciario. Esta antigua ley perduró y sirvió de base al desarrollo y modernización de nuestros centros penales y a la instauración de lo que hoy se conoce como el Servicio Penitenciario Federal.

Ya avanzada la Nación en su consolidación democrática y con el espíritu de la renovación constitucional, en el año 1996 se dicta la Ley de Ejecución de las Penas Privativas de la Libertad N° 24.660 que es la norma más destacada en legislación penitenciaria con que cuenta nuestro país. Sin lugar a dudas, esta norma y sus complementarias marcan el inicio de un periodo moderno, abierto y con mayor participación social.

Pero sin lugar a dudas, es en estos últimos años donde los cambios se hacen más profundos y por ende más notorios. Roberto Pettinato, sin duda fue un revolucionario en materia penitenciaria, nombrar en su honor a nuestra Academia Superior, es marcar un norte, señalar un camino. Sin duda, esa fue la intención del ex Presidente y sin dudarlo ese fue el camino que siguió el SPF. En este sentido nos obligó desde ese momento, a pensar hoy en el futuro, previéndolo.

Fue en su gestión de gobierno, y obviamente en el período actual, bajo la presidencia de Cristina

Kirchner donde la posibilidad de incorporar nuevas tecnologías a nuestra tarea nos obligó a pensar distinto, ya que estas tecnologías modifican fuertemente la situación en la que nos desarrollamos, y así como produjo una revolución en la vida mundial, también la produjo en la vida penitenciaria.

El trabajo del Servicio Penitenciario a partir de la llegada de Pettinato a su conducción no fue otro que el de posibilitar la socialización y la reinserción del interno. Hoy esta misión se está profundizando. En estos últimos años, pensar en la cuestión penal es también pensar en la inclusión social, y en la igualdad de oportunidades. Ese es el desafío de la época, ese es el mandato gubernamental que el SPF abrazó e hizo suyo.

Pero esta reintegración no puede ser llevada con éxito por el Servicio Penitenciario Federal, si no nos adaptamos a los cambios tecnológicos y culturales de un mundo que evoluciona muy rápidamente.

La Biometría es hoy una herramienta que nos ayuda a trabajar para la inclusión social, para esta reinserción social que la Nación necesita. En ese sentido, en el Complejo Penitenciario de Ezeiza está funcionando el primer paso del Sistema de Control de Acceso Biométrico que lleva adelante nuestra Institución. No fue poco esfuerzo implementarlo, primero porque debimos vencer la resistencia de nuestro propio personal; segundo, afrontar ciertos temores que generó en el sistema judicial, y por último en las familias de los internos.

Todos hicimos un gran esfuerzo, no solo la Institución sino también el propio Ministerio de Justicia, a través de la Dirección de Gestión Informática (DGGI), y la Oficina Nacional de Tecnología e Informática, (ONTI), dependiente de la Jefatura de Gabinete de Ministros.

Fue una voluntad protagonizada por todos: familiares de los internos, la Justicia, nuestros hombres, los internos que terminó siendo un éxito que hoy forma parte de la cotidianidad y que ha logrado agilizar y simplificar el trámite de la visita, tornándolo mucho más sencillo, seguro y rápido.

Esto nos ha llevado a estudiar y desarrollar la segunda etapa de este ambicioso plan, el que se está implementando en ocho sistemas penitenciarios más.

Pero no se agotan aquí los planes y proyectos biométricos que lleva adelante nuestra Institución. Son muchos. Nos llenan de orgullo porque permitirán un mejor trabajo institucional de educación, formación y entrenamiento en las nuevas tecnologías para que los internos puedan sumarse e incluirse en una sociedad que avanza y que requiere individuos formados en tecnologías modernas, aptos para trabajar en este mundo cada vez más informatizado.

Pero para lograrlo, debemos hacer un gran esfuerzo y diferenciar a aquellos que no quieren reinsertarse de aquellos que se han equivocado y que viven ese periodo en el que la Justicia nos encarga su tutela, como una oportunidad para mejorar, perfeccionarse, formarse y así poder reinsertarse en la sociedad, junto a su familia.

No es una tarea fácil porque nuestro país absorbe cambios importantes desde hace años.

Tomemos como un ejemplo tecnológico a las comunicaciones telefónicas.

Para entender nuestra dedicación, nuestro celo en el tema, debemos comprender primero que nuestra Nación, a través del artículo 75 inciso 22 de la Constitución Nacional, ha sumado pactos internacionales a nuestra Carta Orgánica y ha reconocido nuevos derechos que hoy tienen categoría constitucional.

Así, cuando un individuo es condenado no debe sufrir restricciones en sus comunicaciones, en su derecho a la información sino en su libertad ambulatoria.

En los ámbitos del SPF, el interno puede comunicarse con quien desee, sin restricciones. No hay un límite a los números de teléfonos a los que pueda llamar al igual que nosotros, que estamos en libertad y no tenemos esas restricciones. En algunas naciones, un condenado solo puede elegir cinco números, en otras a familiares directos y al abogado previamente identificado. Pero en nuestro país esa libertad no se restringe y estamos de acuerdo en no restringirla, pero eso nos ha traído muchos inconvenientes.

Están prohibidas, como en todos los sistemas penitenciarios del mundo, las comunicaciones por celular. Pero la introducción ilegítima de celulares al establecimiento penitenciario se hizo enorme, muchos que no quieren reinsertarse delinquen desde los teléfonos realizando secuestros virtuales, estafas, etc. La mayoría de estos delitos son realizados con celulares, pero otros desde los teléfonos públicos que poseen a su disposición los internos.

Es por esta dura realidad que en este momento estamos implementando un sistema de control, ubicación e inhibición de celulares de alta tecnología y en poco tiempo mas no se podrá realizar ninguna llamada desde celular sin que la misma sea detectada, ubicada e inmediatamente interrumpida.

Pero entonces se agravarán los delitos que se cometen desde los teléfonos públicos, y esto el SPF lo sabe, y lo prevé. La telefonía pública instalada en los establecimientos penitenciarios tiene un sistema previsto y provisto por el operador que advierte que la llamada que se recibe es efectuada desde un establecimiento penitenciario. Esta comunicación debería aparecer siempre que se realice una llamada saliente. Pero resulta ser, que con los sistemas de tarjetas que existen en el mercado muchos internos han logrado saltar esa advertencia y entonces se producen secuestros virtuales, y otros tipos de delitos desde estos teléfonos.

Al día de hoy, las prestadoras del servicio no han podido resolver el problema y ante esta falta de resolución, por parte de las prestadoras, hemos encontrado a través de la biometría una forma de solventar este grave trastorno. Así, decidimos implementar teléfonos públicos biométricos y anti vandálicos en la totalidad de los establecimientos penitenciarios. Son más de mil teléfonos públicos.

Estamos avanzando en la provisión de este nuevo sistema de telefonía pública que tendrá reconocimiento por huella digital y por voz, fotografía del individuo que habla cada breves intervalos, y registro de hora, tiempo de duración y número al que se realizó la llamada; pero para garantizar la privacidad del interno, toda esta información solo será de acceso judicial, es

decir, sólo se podrá acceder a esa información en el marco de una investigación judicial y previa orden del magistrado actuante.

Así, la biometría ayuda a garantizar los derechos de aquellos que quieren vivir bien, permitiendo individualizar a aquellos que quieren delinquir. Sin restringir, sin cercenar el ejercicio del derecho, pero sabiendo que aquel que delinque podrá ser fácilmente identificado y castigado.

Hemos avanzados considerablemente en la realización de este sistema, el cual consideramos sumamente importante y no tenemos dudas que en el próximo CIBRA, podremos comentarles sobre su implementación.

También estamos diligentes en la implementación de las estaciones biométricas de enrolamiento de internos. Como en todos estos desarrollos, iremos por etapas, pero sin duda, esta implementación será de gran utilidad no solo para la verificación permanente de la identidad del interno y la certera ubicación del mismo, sino para un proyecto ambicioso que están encarando las autoridades nacionales, que es la Red Nacional de Biometría y que el SPF será junto con el Registro Nacional de Reincidencias, uno de los primeros en sumarse.

Otro de los temas que estamos abordando, y que está en un avanzado estado de diseño, es el sistema de visita virtual. Desde ya hace varios años, y muy especialmente desde que estalló este fenómeno que conocemos como globalización, la población extranjera en institutos penales ha aumentado en forma muy significativa.

Hace un momento, comentaba sobre lo difícil que es lograr la reinserción social del interno. Pues esta reinserción, es mucho más difícil aun cuando el interno pierde su vínculo familiar. Es por eso que el SPF trabaja en forma denodada para que el interno logre mantener e incluso fortifique su vínculo familiar. Sin este vínculo la reinserción es casi inasequible.

Estamos diseñando este sistema tanto para el extranjero, como para el ciudadano del país que vive alejado del interno. Así, en todas las dependencias del SPF tendremos una sala de visita virtual biométrica, donde luego de enrolar a la visita y al interno se podrá tener una visita virtual, de alta calidad en imagen y sonido, compartiendo así un acercamiento que la distancia y los costos hoy hacen imposible, o al menos muy espaciados en el tiempo. En el caso de los extranjeros serán los consulados o las embajadas de los respectivos países quienes tendrán que validar la identidad de los familiares y visitantes virtuales.

Somos una Institución que con un gran apoyo gubernamental está iniciando un cambio revolucionario. Sin duda somos la Institución con más desarrollo biométrico, no sólo de la Nación, sino de la región. Por eso es necesario comentar el proyecto más ambicioso y revolucionario de los últimos tiempos en materia penal.

Las Tecnologías de la Información y la Comunicación (TIC) son incuestionables y están aquí, forman parte de la cultura tecnológica que nos rodea y con la que debemos convivir y aprender a sacarle provecho para una ágil gestión, por parte de los procesos gubernamentales. Su avance es incuestionable en la totalidad de la sociedad, sean estos aspectos laborales, de seguridad, gobierno, universitario, empresarial y de la sociedad toda. Amplían nuestras capacidades físicas

y mentales y las posibilidades de la inclusión y desarrollo social y digital. No sumarse a las tecnologías, en los avances que propone, sería negar los beneficios que redundan al Estado en su conjunto y a la sociedad toda.

Hoy, pensar en la cuestión penal es también pensar en la inclusión social y en la igualdad de oportunidades. Esta es la verdadera reinserción. No tendremos posibilidades de socializar, no podremos reinsertar sino trabajamos en la inclusión social. No habrá política de reinserción social exitosa que pueda ser llevada con éxito por el Servicio Penitenciario Federal si no nos adaptamos a los cambios tecnológicos y culturales del mundo en que evoluciona.

La cuestión del acceso a las nuevas tecnologías de la información se ha instalado en el imaginario social, independientemente de la condición socio-cultural, como una necesidad indiscutible, que día a día profundiza más el abismo entre quienes acceden y quiénes no.

Existe un íntimo y profundo convencimiento que si no se poseen los conocimientos para utilizar y convivir con una computadora, en el futuro se va a quedar marginado de todos sus beneficios, lo que a su vez va a marcar una profunda diferenciación social entre los que tienen acceso y los que no lo tienen.

En este sentido, el Gobierno Nacional lleva algunos años trabajando en la Agenda Digital Argentina, un plan de mirada federal promovido por el Gobierno Nacional, que se propone dar direccionalidad estratégica al uso y aplicación de las Tecnologías de la Información y Comunicación (TIC) para generar mayor inclusión y fomentar el desarrollo.

Recientemente, la Asamblea General de las Naciones Unidas declaró el acceso a Internet como un “derecho humano” altamente protegido. En una declaración sin precedentes, la organización estableció que los gobiernos de todas las partes del globo tendrán la obligación de facilitar un servicio “accesible y asequible para todos” y deberá de ser una prioridad asegurar la conexión a internet.

Entre otras cosas, la ONU establece que impedir el acceso Internet es una violación del artículo 19, párrafo 3, del Pacto Internacional sobre Derechos Civiles y Políticos y sostiene que los Estados deben asegurar el acceso a Internet a todos los segmentos de la población. Ese pacto, está garantizado en nuestra Constitución.

Pero no es menos cierto que nuestra tarea, también consiste en coadyuvar al mantenimiento de la seguridad de la Nación e impedir la comisión de delitos con estas nuevas tecnologías, de modo que deberemos estudiar los mecanismos para evitarlos, teniendo presente el mandato Constitucional de que se aplique la mínima restricción posible al flujo de información por Internet.

Hemos estado evaluando largamente el problema y contestes con el pensamiento oficial, hoy crece el temor en el seno del SPF de que la falta de interacción con las computadoras se convierta en un nuevo factor de exclusión social y como tal, limite o dificulte aún más nuestra tarea, que no es otra que trabajar por la reinserción y resocialización del interno.

En este contexto y comprendiendo el futuro en que nos adentramos, el Servicio Penitenciario Federal se esfuerza en sumarse al Proyecto Nacional, que no es otro que lograr una Argentina de igualdad, inclusión, progreso y desarrollo, para lo cual está trabajando junto a la DGII y la ONTI en la implementación de un sistema computarizado completo con acceso al servicio de Internet para la totalidad de los internos del sistema penitenciario. Este sistema, que está siendo desarrollado y contendrá un técnicas biométricas de *personal identification verification (piv)*, *Face recognition* y, como ya dijimos, será una forma de capacitar y preparar al interno para la reinserción social y laboral.

En el ámbito de la biometría, estos son los temas que tenemos en desarrollo. Son muchos, ambiciosos y todos ellos de una gran importancia institucional y nacional.

No hace muchos años, cuando iniciamos estos proyectos en el SPF, hablar de Biometría era hablar de algo químérico, fantasioso. Hoy, con el esfuerzo gubernamental e institucional es una realidad, con la que estamos conviviendo y la que sin duda se está transformando en una herramienta eficaz para una mejor gestión y por lo tanto un mayor éxito en la reinserción e inclusión social, pudiendo de esta manera estar un poco más cerca del mandato constitucional; fundamentalmente en lo que ordena a través del artículo 75 inciso 23: *"promover medidas de acción positiva que garanticen la igualdad real de oportunidades y de trato, y el pleno goce y ejercicio de los derechos reconocidos por esta Constitución y por los tratados internacionales vigentes sobre derechos humanos"*.

Herramientas biométricas en la Provincia de Buenos Aires: Casos de Éxito

Gustavo Donato



Gustavo Donato

Director Oficina Provincial de Biometría



Gustavo Fabián Donato nació el 8 de octubre de 1970. Curso sus estudios secundarios en el Liceo Militar General San Martín y en el Colegio Militar de la Nación. Desde 1993 se desempeñó en el Ministerio de Seguridad de la Provincia de Buenos Aires como oficial de la Policía de la provincia de Buenos Aires llegando al cargo de Subcomisario. Paralelamente curso estudios de grado en la Universidad Nacional de Lanús, siendo el primer egresado como Licenciado en Seguridad Ciudadana. Entre los estudios de postgrado curso la Especialización en Administración y Derecho de la Seguridad Pública en la Universidad Carlos III de Madrid y en la Universidad del Salvador, la Maestría en Defensa Nacional en la Escuela de Defensa Nacional y el Doctorado en Ciencia Política en la Universidad del Salvador, entre otros. También es socio fundador de la asociación civil denominada Asociación Argentina de Seguridad (personería jurídica 1059 de la IGJ). A partir de 2008 comenzó a trabajar en el Ministerio de Jefatura de Gabinete de Ministros para posteriormente ser nombrado a cargo de la Oficina Provincial de Biometría.

Información de contacto: gfdonato@gmail.com | gdonato@gob.gba.gov.ar

Resumen

Sin lugar a dudas, durante todo el siglo XX y principios del siglo XXI la humanidad fue testigo de los mayores avances en todos los campos, en especial el tecnológico. Cada día aparecen más y mejores tecnologías que modifican sustancialmente la vida de las personas. Paralelamente, los Estados no quedaron ajenos a estos cambios y decidieron incorporar nuevas herramientas tecnológicas que permitan perfeccionar su gestión. El surgimiento de la biometría y de los sistemas de reconocimiento biométricos no pasaron desapercibidos y los Estados comenzaron a utilizarlos para mejorar la seguridad en el manejo de la información, particularmente en lo referente a la identificación de sus habitantes. La República Argentina ha implementado satisfactoriamente el uso de herramientas biométricas y la provincia de Buenos Aires se ha acoplado a este proyecto iniciando un proceso de crecimiento continuo para el desarrollo de bases biométricas alimentadas a través del enrolamiento biométrico de individuos que pertenecen a distintos ámbitos gubernamentales. En el siguiente paper, se describirá sucintamente el avance en esta área de la Provincia con mayor cantidad de habitantes del país, abarcando tanto la creación de la Oficina Provincial de Biometría, única en su especie a nivel Nacional, como algunos de los proyectos implementados que impulsan tantos otros en los cuales estamos trabajando diariamente para mejorar la calidad de vida de los bonaerenses.

Palabras clave: biometría, bases, tecnología, información, objetivos, datos, huellas, dactilares, enrolamiento, Afis. seguridad, interoperatividad.

Herramientas biométricas en la Provincia de Buenos Aires: Casos de Éxito

“Dios pone un sello en la mano de todos los hombres,

para que cada uno conozca sus obras”

Comisario Alberto Pérez; Manual Práctico de Papiloscoopia

El gobernador de la provincia de Buenos Aires, Daniel Scioli, dispuso a través de la Jefatura de Gabinetes de Ministros a cargo del Lic. Alberto Pérez, cuyo progenitor fallecido Comisario Alberto Pérez hiciera un valioso aporte al campo de la biometría con su libro *Manual Práctico de Papiloscoopia*, la creación de la Oficina Provincial de Biometría a efectos de implementar e impulsar nuevas técnicas y aplicar estándares internacionales en la materia con un alcance integrador para las distintas dependencias que conforman el Estado Provincial. De esta manera, se ha facilitado la difusión de buenas prácticas en la toma de datos biométricos, con miras a lograr la interoperatividad en las bases de datos biométricos creadas, y a crearse.

Tomando a la Biometría como el estudio de métodos y técnicas para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos, consideramos de suma importancia la utilización de herramientas biométricas y la consecuente fijación de estándares provinciales para mejorar la seguridad en el manejo de la información.

Dentro de las tecnologías de la información (TI), la autenticación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humano con propósito de autenticación. Las huellas dactilares, el iris, los patrones faciales, el ADN, las venas o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye: la firma, el paso y el tacleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

Por ejemplo la *Tecnología utilizada para el reconocimiento de la Huella Dactilar* es la que tiene como finalidad identificar, de manera rápida y precisa, a una persona por medio de su huella dactilar certificando la autenticidad de las personas de manera única e inconfundible por medio de un dispositivo electrónico que captura las huellas dactilares y de un programa que realiza la verificación, ya sea 1 a 1 o 1 a N pudiendo estos dispositivos ser estáticos o móviles.

Los principales objetivos de la Oficina Provincial de Biometría son:

- Jerarquizar a la Provincia de Buenos Aires en la seguridad, manipulación y resguardo de la información de personas.
- Lograr la integración de los distintos Ministerios Provinciales para unificar los datos personales de cada individuo que en los mismos se obtengan.
- Fijar estándares en la aplicación de técnicas biométricas para la seguridad en la información.
- Generar una base de datos biométricos como herramienta fundamental para el resguardo de la identidad de todo habitante de la Provincia.

- Conjuntamente con la estandarización de la toma de datos biométricos lograr en un plazo programado la operatividad de la unificación de plataformas entre las bases de datos de las distintas jurisdicciones provinciales.
- Elaborar capacitaciones y seminarios en forma permanente para promover, inculcar y comunicar los beneficios de las herramientas biométricas y hacer escuela sobre las buenas y mejores prácticas en la toma de datos biométricos.

Acciones tendientes al fortalecimiento institucional de la Oficina Provincial de Biometría.

- * Diseñar un Plan de Desarrollo Tecnológico e Informatización Integral del Organismo.
- * Coordinar y gestionar los pasos operativos para la ampliación de la red informática (estándares biométricos) con las distintas dependencias conectadas en la integración de información.
- * Diagramar el desarrollo e instalación de sistemas de bases de datos, programas operativos y aplicaciones para: carga, almacenamiento y manejo de información, relacionada con la gestión de los trámites realizados en distintos organismos.
- * Organizar capacitaciones de recursos humanos en el uso de nuevas herramientas, sistemas y aplicaciones biométricas.
- * Evaluar el sistema de calidad en áreas consideradas clave de la gestión local.
- * Coordinar y administrar el establecimiento de estándares biométricos en el marco de las normas internacionales que regulan la materia (ANSI – NIST)
- * Controlar y verificar el diseño, diagramación y planificación de proyectos adicionales que eventualmente sea menester arbitrar para la instrumentación de los sistemas enunciados. (de acuerdo al expediente N° 2208-358/10 que regula la creación de la Oficina Provincial de Biometria).

En términos generales, el fortalecimiento de la Oficina Provincial de Biometría de la provincia de Buenos Aires, permitirá institucionalizar la modernización en el funcionamiento del Organismo. Todo ello, enmarcado en el proceso de creación de la capacidad técnica y de gestión en cuanto a su desarrollo organizativo, procesos gerenciales y técnicos, incorporación de tecnología, marco normativo, metodológico e instrumentos orientados a la prestación de apoyo, capacitación y monitoreo de las actividades.

Casos de éxito implementados

Dirección Provincial de Política y Seguridad Vial

La Dirección Provincial de Política y Seguridad Vial, dependiente del Ministerio de Jefatura de Gabinete de Ministros ha desarrollado un programa de modernización de procesos de seguridad en la emisión de licencias de conducir en los 135 municipios, distribuidos geográficamente en todo el territorio provincial.

El Sistema de Emisión Centralizada de Licencias de Conducir tiene por objeto acentuar la agilidad, la transparencia y la seguridad que contemplan tecnológicamente las mejores prácticas nacionales e internacionales en esta materia. A tal efecto, se están rediseñando y modernizando los procedimientos de expedición de licencias. Para su implementación, la Provincia ha realizado

una importante inversión en estudios de validación y seguridad de la nueva documentación, que contiene 32 medidas de seguridad que impiden cualquier tipo de adulteración, falsificación y le otorgan una invulnerabilidad similar a la de un pasaporte internacional.

La seguridad de un documento de identificación, como lo es un registro de conducir está determinada por una serie de elementos que intentan hacerlo inmune a la falsificación, adulteración, duplicación y simulación. En este sentido tiene incorporados elementos de seguridad visible y no visible.

En primer lugar, la información está impresa con técnicas especiales que permiten grabar o imprimir y penetrar profundamente el material. En el anverso cuenta con un número de serie único especial de control de producción y un código bidimensional para la verificación automática de identificación, a la que pueden optar instituciones públicas y privadas, lo que permite verificar en forma inmediata si la persona que porta el documento es su titular.

En condiciones normales de uso este nuevo registro de conducir tiene una duración mayor a sus cinco (5) años de vigencia.

El soporte base está constituido por un innovador material que respeta el concepto de elemento monolítico imposible de desmembrar dado que se amalgama constituyendo un soporte íntegro. Los llamados elementos de seguridad de primera línea son visibles a simple vista, mientras que para controlar los elementos de seguridad de segunda línea se necesitan medios auxiliares, dejando una tercera línea al laboratorio forense.

Medidas de Seguridad Nivel I o primera línea.

1. Proceso de termo formado de amalgama en un único elemento plástico
2. Monoelemento que ante todo intento de alterar los datos impresos provocará daños irreparables al recubrimiento, claramente manifiestos
3. Fondo genuinos y exclusivos Guilloches
4. Fondos genuinos y exclusivos Numismáticos de principio lineal
5. Fondos genuinos y exclusivos Numismáticos de principio circular sinusoidal
6. Fondo impreso exclusivo en sistema iris
7. Mapa provincial que varía su color según el ángulo de observación impreso en tinta OVI/OVP
8. Dorso grabado en láser de microfoto y número de DNI
9. Imagen latente con la leyenda dual Valido/BsAs en el reverso
10. Roseta Guilloches en relieve en registro perfecto con imagen preimpresa
11. Números y letras táctiles por estructuras en relieve
12. Banda OVD que varía su color según el ángulo de observación
13. Foto digital del titular
14. Trama base en líneas de curvas que se superponen a la fotografía del titular.
15. Foto y datos variables en la masa misma del sustrato plástico
16. Firma digital del titular
17. Firma digital de funcionario firmante

Medidas de Seguridad Nivel II o segunda línea

18. Nanotexto en líneas del fondo de seguridad en positivo y en negativo

19. Nanotexto en contorno de caja de imagen fotográfica
20. Imagen latente en el anverso, visible con la interpolación de una lente decodificadora
21. Sustrato sintético opaco a la luz UV
22. Grabado láser con reacción al UV

Medidas de Seguridad Nivel III o tercera línea

23. Medidas criptográficas solo perceptibles en laboratorio.
24. Medidas biométricas solo perceptibles en laboratorio.
25. Fondo de seguridad reactivo al infrarrojo IR en forma parcial, resultando el resto no visible.
26. Textos impresos fragmentados donde uno de los fragmentos resulta invisible al infrarrojo IR.
27. Clave única de relación de datos impresos con información alfanumérica e imágenes de la base de datos centralizada.
28. Código de barras 2D tipo PDF-417 con datos del titular de la licencia y de funcionario firmante
29. Código de barras 2D tipo PDF-417 con datos del funcionario firmante (código interno).
30. Código de barras 2D tipo PDF-417 con datos de código AFIS de la huella dactilar del titular.
31. Código de barras 2D tipo PDF-417 con datos de código HCS (Hash Code Security) calculado sobre la información relevante de la licencia para verificación de datos variables.
32. Código de barras 2D tipo PDF-417 con datos de código de versión del programa que produce la licencia.

Como se puede apreciar, se ha incorporado tecnología biométrica para la emisión de la licencia de conducir. Los sistemas de identificación biométricos introducen sin duda una revolución en el sistema de seguridad provincial ya que supone métodos de identificación y autenticación de los seres humanos a través de características fisiológicas o de comportamiento.

En el caso de la licencia de conducir, la característica física e intransferible que se identifica son las huellas dactilares de las personas.

La identificación por medio de huellas dactilares constituye una de las formas más representativas de la utilización de la biometría. Una huella dactilar está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados 'puntos de minucia'. Cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona.

Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. En el caso del reconocimiento de la huella dactilar, se ha de tener en cuenta que en ningún caso se extrae la imagen de la huella, sino sus minucias, representadas en una secuencia de números que se guardan



en formato PDF 417 y/o BIDI. Actualmente en la Provincia contamos con más de trescientos puestos de enrolamiento biométrico que se distribuyen geográficamente en los 135 municipios que componen a la provincia de Buenos Aires. Conjunto a ésto, se procedió a la compra y puesta en marcha de un motor AFIS (Automated Fingerprint Identification System) para poder almacenar las bases con los datos biométricos de los cinco millones de usuarios de licencias de conducir

que posee la provincia de Buenos Aires para poder realizar verificaciones y autenticaciones 1:N (comparar una única imagen dactilar con una base de datos de imágenes de huellas). También se han adquirido equipos del tipo PDA (dispositivos portátiles multibiométricos) para proveer a la Policía y a los Municipios a los fines de que puedan realizar operativos de identificación 1:1 en la vía pública.

El empleo de la biometría para identificar las características únicas de un individuo brinda una serie de cualidades que no han pasado desapercibidas por los Gobiernos de muchas Naciones. En los últimos años, las autoridades gubernamentales han iniciado la investigación e implementación de programas piloto y registros biométricos para la identificación ciudadana, como documentos, pasaportes, cédulas de identidad y licencias de conducir.

ReCAP (Registro de Controladores de Admisión y Permanencia)

En el año 2008 se sancionó y promulgó la Ley Nacional Nº 26.370, por medio de la cual se establecieron las reglas de habilitación del personal que realiza tareas de admisión y permanencia de público en general, y para empleados cuya actividad consista en la organización y explotación de eventos y espectáculos públicos.

En el ámbito de la Provincia de Buenos Aires se dictó la Ley Nº 13.964, a través de la cual la misma adhiere al régimen establecido por la normativa precedentemente mencionada, dictándose posteriormente el Decreto Reglamentario 1096/09, por medio del cual se crea el Registro Público Provincial de Personal de Control de Admisión y Permanencia, el que está a cargo de un responsable designado por el Poder Ejecutivo, bajo la órbita de la Subsecretaría de Planificación del Ministerio de Justicia y Seguridad, para la habilitación de las personas que se desempeñen como personal de control de admisión y permanencia de público en general. Estructuralmente el Registro está organizado en dos Departamentos:

Departamento Registro: Se encarga de todo el procedimiento para la habilitación de los controladores, y la expedición del carnet profesional y credencial identificatoria, por lo que cada controlador deberá exhibir esta credencial siempre que se encuentre trabajando y el carnet profesional, título habilitante para ejercer la función de controlador.

Departamento Habilitaciones: Es el área que se encarga de la recepción de toda la documentación de empresas y establecimientos, así como de realizar los actos de habilitación de empresas y registro de establecimientos.

La Oficina Provincial de Biometría, ha tipificado un protocolo de tomas de datos para el Departamento de Registro. En el mismo se estipula el enrolamiento biométrico de todo el personal a través de la toma de huellas decadactilares, fotografía y firma digital.

Dirección General de Agencias de Seguridad Privada

La Dirección General de Agencias de Seguridad Privada es un organismo que depende del Ministerio de Seguridad de la provincia de Buenos Aires y tiene la función de ser el contralor sobre las empresas que prestan servicios de seguridad en todo el territorio Provincial. Tiene

injerencia sobre cuestiones administrativas relacionadas con la habilitación de estas empresas y operativas, tanto sobre la cantidad de objetivos que poseen como sobre el personal que trabajan en esos objetivos. Cabe aclarar que los vigiladores de empresas de seguridad privada ascienden a más de ciento veinte mil personas, duplicando en su conjunto a los miembros de la Policía de la provincia de Buenos Aires. Al igual que los vigiladores y controladores de admisión y permanencia, los vigiladores de empresas de seguridad privada deben cumplimentar la requisitoria legal que los habilita a tal efecto. En ese orden la Oficina Provincial de Biometría ha realizado un protocolo de toma de datos para el enrolamiento biométrico de estos trabajadores para poder identificarlos y verificar que estén autorizados a realizar tareas de seguridad. Recientemente se ha adquirido un motor AFIS para almacenar las bases de datos creadas por el ReCAP y por la Dirección General de Agencias de Seguridad Privada y para poder realizar comparaciones 1:N.

Servicio Penitenciario Bonaerense

A principios de 2011, desde la Oficina Provincial de Biometría se comenzó a trabajar con el Servicio Penitenciario Bonaerense para tratar de resolver dos cuestiones fundamentales para el desarrollo de la actividad carcelaria: por un lado los traslados intracárceles y los movimientos a sede judicial de las personas (denominados internos) alojadas en las más de sesenta cárceles y alcaidías provinciales, y por otro el ingreso y egreso de familiares de los mismos a unidades carcelarias.

Por lo expuesto ut supra se implementó, en una primera etapa, en el complejo denominado Florencio Varela (este complejo está compuesto por la alcaidía departamental La Plata, la unidad 8 de mujeres, la unidad 9 de La Plata, la unidad 10 Melchor Romero, la unidad 12 Gorina, la unidad 18 Gorina, la unidad 29 (operativa Melchor Romero), la unidad 33 de mujeres, la unidad 34 Melchor Romero y la unidad 45 Melchor Romero), la instalación y puesta en marcha de treinta equipos biométricos para enrolar a más de cuatro mil internos y treinta mil visitas.

Para ello la Oficina Provincial de Biometría entregó tres equipos por unidad, de los cuales uno fue utilizado para obtener los registros biométricos de los internos y los otros para obtener los datos biométricos de los familiares que los visitan segmentadas en hombres y mujeres. Los registros están compuestos por la captura de huellas decadactilares, fotografía y firma digital y serán almacenados en el servidor Afis adquirido para uso del Servicio Penitenciario Provincial.

Todas las bases creadas hasta el momento, es decir las de la Dirección Provincial de Política y Seguridad Vial, del Registro de Controladores de Admisión y Permanencias, de la Dirección General de Agencias de Seguridad Privada y del Servicio Penitenciario son perfectamente interoperables entre si, ya que fueron abastecidas bajo protocolos y estándares certificados por el NIST (National Institute of Standards and Technology), el ANSI (American National Standards Institute) y el FBI (Federal Bureau of Investigation) siendo integrables a las bases alimentadas por las quinientas delegaciones del Registro Provincial de las personas y Centros de Documentación Rápida (CDR) donde se expide el nuevo DNI y Pasaporte.

Indudablemente, con el avance de las nuevas tecnologías aplicadas a la biometría, hoy día es

viable poder realizar proyectos biométricos de gran escala en el campo civil, aptos para que se complemente con el campo penal. Ya los costos no se presentan como una barrera de magnitud. De hecho, el principal inconveniente reside en los recursos humanos especializados en esta área y no hablamos solo de programadores, sino también de personas que sepan y conozcan las reglas de negocio, sobre estándares y experiencias en otros países.

No obstante, creemos que vamos por el buen camino. Debemos seguir trabajando para mejorar las buenas y mejores prácticas y asegurar la interoperabilidad de las bases de datos biométricas independientemente del lugar donde residan o del organismo que la administre. Estamos convencidos que la aplicación de herramientas biométricas mejorara notablemente la capacidad del Estado Provincial para proteger la identidad de las personas.

**Identidad, biometría y firma digital en la región.
El marco iberoamericano de Identificación Electrónica Social**

Gabriel Casal / Mercedes Rivolta



Gabriel Casal

Jefe de Asesores de la Subsecretaría de Tecnologías de Gestión, Jefatura de Gabinete de Ministros.



Abogado y Profesor de la Universidad Nacional de La Plata. Ha sido Asesor de la Dirección General de Cultura y Educación de la Provincia de Buenos Aires entre 1994 y 1999. Jefe de la Comisión de Asuntos Legales del Consejo General de Cultura y Educación de la Provincia de Buenos Aires. Subsecretario del Consejo Nacional de Coordinación de Políticas Sociales de la Presidencia de la Nación. Consultor del Ministerio del Interior para la Dirección General de Gestión Informática. Asesor en el Ministerio de Justicia, Seguridad y Derechos Humanos de la Nación, en la Dirección General de Gestión Informática. Miembro de la Comisión Técnica Redactora del proyecto de Código Procesal Penal de la Nación. Experto designado por el Presidente del CLAD en la Comisión redactora del nuevo documento doctrinal del CLAD. Coordinador argentino en el Proyecto Mercosur Digital. Representante alterno en el Subgrupo 13 de Comercio Electrónico en el Mercosur. Miembro del Comité Organizador del Congreso Internacional de Biometría en la República Argentina desde 2006.

Información de contacto: gabrielcasal@sgp.gov.ar
gcasal@jefatura.gob.ar | <http://ar.linkedin.com/pub/gabriel-casal/4/264/756>



Mercedes Rivolta

Asesora del Subsecretario de Tecnologías de Gestión, Jefatura de Gabinete de Ministros.



Abogada (UBA), Magister en Administración Pública (FCE UBA). Miembro del Cuerpo de Administradores Gubernamentales de la Jefatura de Gabinete de Ministros. Ha sido miembro de las comisiones técnicas redactoras de la Ley Nº 25.506 de firma digital, del Decreto Nº 1023/01 que establece el régimen de compras públicas de la Administración Nacional, coordinadora del Comité Técnico redactor del Decreto Nº 2628/02 reglamentario de la ley de firma digital, en Argentina. Como consultora internacional, ha brindado asistencia a los gobiernos del Panamá, República Dominicana, Perú, Paraguay, Colombia, Ecuador, Banco Interamericano de Desarrollo y Banco Mundial en materia de regulación de sistemas electrónicos de compras públicas e Infraestructuras de firma digital.

Información de contacto: mrivolta@jefatura.gob.ar
mercedesrivolta@yahoo.com.ar | <http://ar.linkedin.com/in/mercedesrivolta>

Resumen

El Marco para la Identificación Electrónica Social Iberoamericana, complementario de la Carta Iberoamericana de Gobierno Electrónico de 2007, es una iniciativa que fue presentada por Argentina, en la XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), durante la cual se trataron temas vinculados con la Participación de los Ciudadanos en la era del Gobierno Electrónico: Educación para la Ciudadanía e Inclusión Digital.

Consideramos que el Marco e-ID Social es relevante por varias razones:

- a. Es la primera expresión de un entendimiento entre los países iberoamericanos que aborda la temática de la identificación y el uso de las tecnologías.
- b. Introduce el concepto de autenticación electrónica, como eslabón entre los conceptos de identificación de personas en entornos físicos y el de firma electrónica/digital.
- c. Es la primera vez que un documento aborda en forma conjunta la temática de la identificación de personas en entornos físicos y la identificación de personas en entornos electrónicos.
- d. Es la primera expresión de entendimiento entre todos los países iberoamericanos que logran conformar un glosario común sobre temas vinculados con el comercio electrónico, el gobierno digital y la autenticación en entornos electrónicos.
- e. Constituye un valioso antecedente para lograr futuros acuerdos de reconocimiento mutuo de firmas digitales.

En consecuencia, entendemos entonces que el Marco e-ID Social constituye un gran avance. En este artículo analizamos el marco citado desde una mirada jurídica, identificando aquellos aspectos que resultan relevantes desde nuestro ordenamiento legal.

Nos proponemos dar inicio a un intercambio de opiniones sobre estos aspectos, con el deseo de contribuir, en el mediano plazo, al logro de acuerdos que faciliten el acceso de las personas a las aplicaciones de comercio y gobierno electrónico.

Palabras clave: Argentina, Marco Iberoamericano Identificación Electrónica Social, biometría, firma digital, firma electrónica, documento digital, administración pública, documento identidad, Tecnologías Información y Comunicaciones, Gobierno Electrónico, Carta Iberoamericana de Gobierno Electrónico.

Identidad, biometría y firma digital en la región

El marco iberoamericano de identificación electrónica social

Introducción

“Hoy, ni escena ni espejo, sino pantalla y red”

Jean Baudrillard

Desde la 1^a edición del libro Biometrías, que acompañó al V Congreso Internacional de Biometría de la República Argentina – CIBRA 10, ha transcurrido sólo un año. Sin embargo, se ha producido una novedad que, a nuestro entender, constituye un gran avance en la materia.

Nos referimos al Marco para la Identificación Electrónica Social Iberoamericana, al cual en adelante llamaremos Marco e-ID Social, complementario de la Carta Iberoamericana de Gobierno Electrónico de 2007.

El Marco e-ID Social es una iniciativa que fue presentada por Argentina, en la XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), durante la cual se trataron temas vinculados con la Participación de los Ciudadanos en la era del Gobierno Electrónico: Educación para la Ciudadanía e Inclusión Digital.

Como resultado de esta reunión, se aprobó la Declaración de Lisboa, la cual recomienda *“el desarrollo de mecanismos de identificación y autenticación electrónica seguros, es otra de las condiciones para el cambio pretendido, destacándose su papel en la promoción de simplificación de procedimientos y en el fomento de la utilización de los servicios electrónicos.”*

Dicha Declaración de Lisboa reconoce que *“los objetivos del gobierno electrónico deben trascender la mera eficacia y eficiencia de los procesos de administración, hacia formas que permitan cambios sociales, políticos, económicos en pro del desarrollo humano, la igualdad de oportunidades y la justicia social.”*

Como consecuencia, el 1° de julio de 2011 el Marco e-ID Social fue aprobado en Asunción, Paraguay, durante la XIII Conferencia Iberoamericana de Ministros y Ministras de Administración Pública y Reforma del Estado, a la que asistieron 18 países con más de 40 delegados, en el marco de la “XXI Cumbre Iberoamericana de Jefes y Jefas de Estado y de Gobierno”. En dicha oportunidad, los países declararon *“Continuar la adopción de la Carta Iberoamericana de Gobierno Electrónico, la cual promueve el reconocimiento del derecho al acceso electrónico a la administración... Para ello resulta necesario incentivar la inclusión digital de todos los habitantes de la región, impulsar políticas de identificación electrónica social y convertir la Sociedad de la Información y del Conocimiento en una oportunidad para todos y todas, especialmente de aquellos en peligro de quedar rezagados.”*

Los países signatarios de la Declaración de Asunción resolvieron “Aprobar el Marco para la Identificación Electrónica Social Iberoamericana” como addendum de la Carta Iberoamericana de Gobierno Electrónico.

El Marco e-ID Social no constituye una norma positiva, ya que no ha sido internalizado por cada uno de los países. Sin embargo, es un gran avance pues representa la voluntad de los países iberoamericanos de lograr puntos de encuentro para el tratamiento de la temática de la identificación de personas en entornos físicos y digitales, expresada por primera vez.

Consideramos que el Marco e-ID Social es relevante por varias razones:

- a. Es la primera expresión de un entendimiento entre los países iberoamericanos que aborda la temática de la identificación y el uso de las tecnologías.
- b. Introduce el concepto de autenticación electrónica, como eslabón entre los conceptos de identificación de personas en entornos físicos y el de firma electrónica/digital.
- c. Es la primera vez que un documento aborda en forma conjunta la temática de la identificación de personas en entornos físicos y la identificación de personas en entornos electrónicos.
- d. Es la primera expresión de entendimiento entre todos los países iberoamericanos que logran conformar un glosario común sobre temas vinculados con el comercio electrónico, el gobierno digital y la autenticación en entornos electrónicos.
- e. Constituye un valioso antecedente para lograr futuros acuerdos de reconocimiento mutuo de firmas digitales.

En consecuencia, entendemos entonces que el Marco e-ID Social constituye un gran avance. En este artículo analizamos el marco citado desde una mirada jurídica, identificando aquellos aspectos que resultan relevantes desde nuestro ordenamiento legal.

Nos proponemos dar inicio a un intercambio de opiniones sobre estos aspectos, con el deseo de contribuir, en el mediano plazo, al logro de acuerdos que faciliten el acceso de las personas a las aplicaciones de comercio y gobierno electrónico.

Estamos convencidos que el avance del comercio electrónico es altamente positivo para el desarrollo de la economía, especialmente para las pequeñas y medianas empresas, con el consecuente aumento de empleos dignos y el desarrollo de las economías regionales. Y entendemos que en la medida que el gobierno electrónico avanza, se incrementa el acceso de la gente a su gobierno, a la administración, al Estado, y ello significa más democracia, más participación, más transparencia, mejor gobierno. Pero fundamentalmente, estamos persuadidos de que las políticas de inclusión social que despliegan nuestros gobiernos, necesitan para ser efectivas, de la identificación de las personas. Y que el efectivo ejercicio de los derechos comienza cuando una persona ha sido identificada, posee una identidad y dicha identidad es reconocida.

El Capítulo II describe brevemente el marco legal argentino en materia de identificación de personas y de firma digital. Se tratan los principales conceptos, su relación con biometría y firma digital, y su naturaleza jurídica.

El Capítulo III presenta el Marco e-ID Social, y en particular, sus principales contenidos desde la perspectiva legal.

En ambos Capítulos se relacionan los conceptos legales argentinos y los del Marco e-ID Social, intentando identificar consistencias, coincidencias y discrepancias, si las hubiera.

El Capítulo IV contiene las conclusiones y nuevas oportunidades que se abren a partir del Marco e-ID Social.

II.- Marco Legal Argentino

El Marco e-ID Social aborda el tema de la identificación desde distintas perspectivas. Trata sobre el proceso de identificación de las personas y los documentos que acreditan dicha identidad en el mundo físico. También, contempla la cuestión de la identificación de personas en entornos virtuales, para lo cual alude a los conceptos de firma electrónica y de firma digital, e introduce el concepto de autenticación electrónica. En ambos casos, es decir, aplicable a ambas situaciones (identificación en entornos físicos mediante documentos de identidad e identificación en entornos digitales) el Marco e-ID Social contempla el uso de biometrías.

En el presente artículo abordaremos la normativa argentina referida a estos temas.

a. Identificación de personas en entornos físicos

Tal como menciona el Marco e-ID, la identificación de las personas es, simultáneamente, una obligación y un derecho que habilita el ejercicio de otros derechos: electorales, sociales, educativos, a la salud, tributarios, etc. Es un derecho para las personas y una obligación para el Estado, en su doble rol: establecer los mecanismos que acrediten la identidad y garantizar su pleno ejercicio. Sin identificación no hay posibilidad de hacer valer los derechos.

El reconocimiento de la personalidad jurídica de un ser humano es una condición necesaria para el efectivo ejercicio de sus derechos económicos, culturales, sociales, políticos, etc. La República Argentina considera estratégica la identificación y documentación de todas las personas físicas.

A tal fin, nuestro país ha sancionado una ley que regula la identificación de personas, la Ley N° 17.671. Esta norma asigna a un organismo de la administración pública nacional, con alcance federal, la función de identificar, registrar y emitir el documento nacional de identidad a todos los habitantes del país y a los argentinos que residen en el extranjero. (CASAL; 2010)

La ley asigna dicha función al Registro Nacional de las Personas, organismo que depende del Ministerio del Interior de la Nación. La identificación de todas las personas de existencia visible que se domicilien en el país, o en jurisdicción argentina y de todos los argentinos sea cual fuere el lugar donde se domiciliaren (art. 1º ley 17.671), son parte de sus funciones. En su articulado, la Ley regula las competencias del Registro, creado anteriormente por la Ley N° 13.482.

Esta Ley N° 17.671, emitida en el año 1968 y denominada de Identificación, Registro y Clasificación del Potencial Humano Nacional, crea además el Documento Nacional de Identidad, único documento válido en toda la extensión del territorio nacional para la identificación de personas. Asigna al Registro la potestad “exclusiva” de emitir el Documento Nacional de Identidad (artículo 11).

Este Documento Nacional de Identidad es el único documento que acredita la identidad de las personas en Argentina, aunque es admisible para viajar a países limítrofes. Vemos entonces cómo en Argentina existe una ley que regula el procedimiento de identificación de las personas, otorga dicha competencia a un organismo de la administración pública nacional, crea el documento

nacional de identidad, contempla el uso de tecnologías biométricas en dicho proceso y dispone que dicho documento sea el único medio válido para probar la identidad de las personas físicas. En efecto, la Ley dispone:

"Artículo 13: La presentación del documento nacional de identidad expedido por el Registro Nacional de las Personas será obligatoria en todas las circunstancias en que sea necesario probar la identidad de las personas comprendidas en esta ley, sin que pueda ser suplido por ningún otro documento de identidad cualquiera fuere su naturaleza y origen."

La mencionada norma establece el procedimiento por el cual el Registro realizará la función de identificación de personas, previendo a tal fin las siguientes acciones que le son encomendadas:

"Artículo 2º... a) la inscripción e identificación de las personas comprendidas en el artículo 1º mediante el registro de sus antecedentes de mayor importancia desde el nacimiento y a través de las distintas etapas de la vida, los que se mantendrán permanentemente actualizados;

b) la clasificación y procesamiento de la información relacionada con ese potencial humano, con vistas a satisfacer las siguientes exigencias:

Proporcionar las Gobierno Nacional las bases de información necesarias que le permita fijar, con intervención de los organismos técnicos especializados, la política demográfica que más convenga a los intereses de la Nación.

Poner a disposición de los organismos del Estado y entes particulares que lo soliciten, los elementos de juicio necesarios para realizar una adecuada administración del potencial humano; posibilitando se participación activa en los planes de defensa y desarrollo de la Nación.

c) la expedición de los documentos nacionales de identidad, con carácter exclusivo, así como todos aquellos otros informes, certificados o testimonios previstos por la presente ley, otorgados en base a la identificación dactiloscópica..."

Por otra parte, la Ley citada crea el denominado “Legajo de Identificación”, el cual es regulado en su artículo 7º, y contempla el uso de tecnologías biométricas aplicables al proceso de identificación de personas, lo cual es, considerando la época de su sanción, un elemento extremadamente novedoso que se ha mantenido actualizado hasta nuestros días. (CASAL; 2010) En efecto, el artículo 7 mencionado dispone que:

"Las personas comprendidas en el artículo 1º deberán ser inscritas por el Registro Nacional de las Personas, asignándoseles en el mismo un legajo de identificación con un número fijo, exclusivo e inmutable, el que sólo podrá modificarse en caso de error fehacientemente comprobado. Dicho legajo se irá formando desde el nacimiento de aquellas y en el mismo se acumularán todos los antecedentes personales de mayor importancia que configuran su actividad en las distintas etapas de su vida. Todo identificado tiene derecho a exigir que conste en su legajo los antecedentes, méritos y títulos que considere favorable a su persona."

Las constancias del legajo de identificación deberán puntualizar con precisión los comprobantes que las justifiquen. En la sede central del Registro Nacional de las Personas se llevarán por lo

menos ficheros patronímicos, numéricos y dactiloscópicos según el sistema argentino Vucetich u otro que en el futuro aconseje la evolución de la técnica”.

Como en la casi totalidad de los ordenamientos jurídicos que contemplan la registración y documentación de las personas físicas, la norma argentina previó la conformación de un archivo personal que consta de datos patronímicos de las personas –sus datos biográficos trascendentales-, su identificación física dada por el registro dactiloscópico de los diez dedos de las manos y la asignación de un número “fijo, exclusivo e inmutable” según las propias palabras de la Ley. (CASAL; 2010)

El uso de tecnologías digitales en la identificación de los ciudadanos nacionales y extranjeros como así también en la emisión del Documento Nacional de Identidad es autorizado por el Decreto N° 1501/2009, reglamentario de la Ley N° 17.671. El mencionado Decreto establece el Nuevo Documento Nacional de Identidad, en dos formatos: libreta y tarjeta. Dicho Decreto, habilita a la Dirección Nacional del Registro Nacional de las Personas, dependiente del Ministerio del Interior de la Nación, a establecer el diseño, características y detalle del nuevo Documento Nacional de Identidad, tanto en formato libreta como tarjeta, con su nomenclatura, descripción y elementos de seguridad e inviolabilidad.

Por su parte, la Resolución N° 1800/2009, regulatoria del Decreto mencionado ut supra, prevé el carácter reservado con exclusividad a las autoridades con alcance pericial sobre aquellos contenidos que refieren a aspectos y elementos de seguridad del DNI, a fin de resguardar la constatación y validación de los mismos por parte de actores competentes en la materia en condiciones de máxima seguridad.

En consecuencia, el nuevo documento nacional de identidad contiene los datos patronímicos, impresión dactilar y fotografía, y un código de barras bidimensional que incorpora los datos biográficos y biométricos del titular del documento. Esta nueva regulación que habilita al Registro Nacional de las Personas a la digitalización del trámite y la modernización documental, es sustancial como paso previo al documento de identidad electrónico.

La Ley de 1968, como se desprende de la parte final de su artículo 7º, ha previsto la evolución de la técnica para el tratamiento de los datos dactiloscópicos en la identificación de las personas, más concretamente en los procesos que lleva adelante el ReNaPer (Registro Nacional de las Personas).

El proceso de registración y la posterior comparación de huellas dactilares, de acuerdo a lo previsto por la ley citada, puede realizarse válidamente, mediante la acción manual de un perito papiloscópico, o por medio de la utilización de un sistema automatizado, conocido por su sigla en inglés AFIS (Automatic Fingerprint Identification System). (CASAL; 2010)

En Argentina, entonces, contamos con un marco legal específico que regula el proceso de identificación de las personas, asigna la función a un organismo de alcance federal – el Registro Nacional de las Personas, y admite el uso de tecnologías biométricas. La identificación de las personas de existencia visible en la República Argentina se apoya por imperio legal en el uso de tecnologías biométricas.

La protección del derecho a la identidad

El ordenamiento jurídico argentino reconoce el derecho a la identidad y, en consecuencia, la obligación del Estado de garantizar la plena identificación de las personas. La materia está regulada en las Leyes Nº 24.540, que establece el régimen de identificación de los recién nacidos, su modificatoria, Nº 24.884 y la Ley Nº 26.061 de protección integral de los derechos de niñas, niños y adolescentes, reglamentada por el Decreto Nº 415/06.

El derecho a la identidad está expresamente reconocido por la Ley Nº 26.061. En su artículo 11, la ley engloba dentro del concepto de identidad, al derecho al nombre, a la lengua de origen, al conocimiento de sus padres biológicos (salvo el caso de procesos de adopción plena en los términos de los artículos 327 y 328 del Código Civil), a la cultura del lugar de origen y a preservar su identidad e idiosincrasia.

ARTICULO 11. — DERECHO A LA IDENTIDAD. *Las niñas, niños y adolescentes tienen derecho a un nombre, a una nacionalidad, a su lengua de origen, al conocimiento de quiénes son sus padres, a la preservación de sus relaciones familiares de conformidad con la ley, a la cultura de su lugar de origen y a preservar su identidad e idiosincrasia, salvo la excepción prevista en los artículos 327 y 328 del Código Civil.*

Este derecho a la identidad encuentra su correlato en la obligación que la misma ley pone en cabeza del Estado en el artículo siguiente, el cual establece la garantía estatal de identificación e inscripción en el Registro del Estado Civil y Capacidad de las Personas. Esta norma incorpora una garantía de identificación de recién nacidos por parte del Estado. La ley prescribe que los procedimientos de identificación deben ser:

- Sencillos
- Rápidos
- Gratuitos
- Obligatorios
- Oportunos
- Inmediatos

La ley citada establece que dicho proceso de identificación del recién nacido debe necesariamente establecer el vínculo filial con la madre, conforme al procedimiento establecido por la Ley Nº 24.540. En tal sentido, la Ley prevé que si los padres no tuvieran documentos que acrediten su propia identidad, los organismos del estado deberán arbitrar los medios necesarios para la obtención de la identificación obligatoria. La norma establece la inscripción gratuita de aquellos adolescentes y madres que no hayan sido inscriptos oportunamente, por parte del Registro del Estado y Capacidad de las Personas. (Artículo 12)

ARTICULO 12. — GARANTIA ESTATAL DE IDENTIFICACION. INSCRIPCION EN EL REGISTRO DEL ESTADO Y CAPACIDAD DE LAS PERSONAS. *Los Organismos del Estado deben garantizar procedimientos sencillos y rápidos para que los recién nacidos sean identificados en forma gratuita, obligatoria, oportuna e inmediatamente después de su nacimiento, estableciendo el vínculo filial con la madre, conforme al procedimiento previsto en la Ley Nº 24.540.*

Ante la falta de documento que acredite la identidad de la madre o del padre, los Organismos del Estado deberán arbitrar los medios necesarios para la obtención de la identificación obligatoria consignada en el párrafo anterior, circunstancia que deberá ser tenida especialmente en cuenta por la reglamentación de esta ley.

Debe facilitar la adopción de medidas específicas para la inscripción gratuita en el Registro del Estado y Capacidad de las Personas, de todos aquellos adolescentes y madres, que no hayan sido inscriptos oportunamente.

Este artículo ha sido reglamentado por el Decreto N° 415/06, que contempla la situación en la cual el padre es desconocido. En ese caso, el Decreto prevé la intervención de funcionarios del Registro Civil para orientar a la madre en esta situación, según el siguiente procedimiento:

ARTICULO 12: En todos los casos en que se proceda a inscribir a un niño o niña con padre desconocido, el jefe u oficial del Registro Civil deberá mantener una entrevista reservada con la madre en la que se le hará saber que es un derecho humano de la persona menor de edad conocer su identidad; que, declarar quién es el padre, le permitirá a la niña o niño ejercer el derecho a los alimentos y que esa manifestación no privará a la madre del derecho a mantener la guarda y brindar protección. A esos efectos, se deberá entregar a la madre la documentación en la cual consten estos derechos humanos del niño, pudiendo el funcionario interviniente, en su caso, solicitar la colaboración de la autoridad administrativa local de aplicación correspondiente, para que personal especializado amplíe la información y la asesore. Asimismo se comunicará a la presentante que, en caso de que mantenga la inscripción con padre desconocido, se procederá conforme lo dispone el artículo 255 del Código Civil.

El Código Civil en su artículo 255 instruye al Registro Civil a comunicar al Ministerio Público de Menores acerca de todos los casos de menores inscriptos como hijo de padre desconocido, a fin de que esta instancia impulse las acciones necesarias para la determinación de la paternidad y el posterior reconocimiento del hijo por parte del presunto padre, pudiendo iniciar la acción judicial correspondiente si mediara autorización expresa de la madre.

Código Civil, Art. 255. En todos los casos en que un menor aparezca inscripto como hijo de padre desconocido, el Registro Civil efectuará la comunicación al Ministerio Público de Menores, quien deberá procurar la determinación de la paternidad y el reconocimiento del hijo por el presunto padre. En su defecto podrá promover la acción judicial correspondiente si media conformidad expresa de la madre para hacerlo.

Siguiendo el procedimiento establecido por el Decreto N° 415/06 reglamentario de la Ley N° 26.061, se prevé la situación de que alguno de los padres del niño por nacer carezca de documento de identidad. En esta situación, la norma prevé que en ocasión de los controles prenatales o de ingreso al centro de salud para el parto, las autoridades del mismo deben informar de la indocumentación referida a los organismos competentes para que le expidan el documento. En caso de imposibilidad, la norma prevé que si llegara el momento del parto sin que los progenitores hayan obtenido su documento de identidad, las autoridades del centro de salud deberán consignar en el Certificado de constatación del parto el nombre, apellido,

fecha de nacimiento, domicilio, edad, huellas dactilares y nacionalidad del padre o madre indocumentado.

Dicha norma prevé la aplicación de la ley N° 24.540 en relación con la identificación de los recién nacidos. El Decreto propicia la localización de oficinas del Registro Civil en todas las maternidades y establecimiento que atienden nacimientos, a fin de facilitar la identificación del recién nacido y de sus padres indocumentados.

Por otra parte, la Ley N° 26.061 establece el derecho a la documentación en su artículo 13. Expresamente, reconoce el derecho a obtener los documentos públicos que comprueben su identidad a todos los niños, niñas, adolescentes y madres indocumentadas, de acuerdo con los términos de la Ley N° 24.540.

ARTICULO 13. — DERECHO A LA DOCUMENTACION. Las niñas, niños, adolescentes y madres indocumentadas, tienen derecho a obtener los documentos públicos que comprueben su identidad, de conformidad con la normativa vigente y en los términos que establece el procedimiento previsto en la Ley N° 24.540.

El Decreto N° 415/06 reglamentario de la Ley citada, dispone la gratuitad de los Documentos nacionales de identidad a todos los niños, niñas y adolescentes nacidos en el territorio nacional, es decir, hasta los 18 años.

ARTICULO 13: Declárese la gratuitad del otorgamiento del primer Documento Nacional de Identidad a todos los niños y niñas y adolescentes nacidos en el territorio nacional.

Procedimiento de identificación del recién nacido

La Ley N° 24.540 establece el procedimiento para la identificación de los recién nacidos, aplicable a todos los niños nacidos en el territorio nacional, vivos o muertos, y a su madre. En los casos que el nacimiento se produjera en un establecimiento de salud, el artículo 2 dispone que durante el trabajo de parto deberá identificarse a la madre, y luego del nacimiento y antes del corte del cordón umbilical, al recién nacido, de acuerdo con los procedimientos previstos en el artículo 6º.

La Ley contempla situaciones anómalas como el nacimiento prematuro o con malformaciones que impiden levantar la huella plantar y papilar del recién nacido. Dispone que la autoridad de aplicación sea el Registro Nacional de las Personas, organismo rector en materia de identificación personal en nuestro país. (CASAL; 2010)

En su artículo 6º, la Ley N° 26.061 establece el procedimiento a seguir para la identificación del recién nacido, y su vinculación con la madre.

ARTICULO 6º — La identificación deberá hacerse en una ficha única, numerada por el Registro Nacional de las Personas, en tres ejemplares, en la que constarán los siguientes datos:

— *De la madre: nombre y apellido, tipo y número de documento de identidad e impresión decodactilar.*

— *Del niño: nombre con el que se lo inscribirá, sexo, calcos papilares palmares y plantares*

derechos, y clasificación de ambos.

- *Si el niño ha nacido con vida.*
- *Nombre, apellido y firma del identificador interviniente.*
- *Nombre, apellido y firma del profesional que asistió el parto.*
- *Fecha, hora y lugar del nacimiento y de la confección de la ficha.*
- *Calclos tomados al egreso.*
- *Datos del establecimiento médico asistencial: nombre y domicilio.*
- *Observaciones*

La Ley establece un procedimiento de identificación del binomio madre-hijo, el cual se apoya en la recolección de datos biométricos en el momento del parto, tanto de la progenitora como del niño. Estos datos biométricos permitirán garantizar posteriormente la identidad del recién nacido y luego de la persona en su vida adulta.

En la Ciudad Autónoma de Buenos Aires, en el año 2003 se dictó la Ley N° 1226 que crea el Sistema de Identificación del Recién Nacido y de su Madre, de aplicación obligatoria, que tiene por objeto asegurar a las personas su legítimo derecho a la identidad así como garantizar la indemnidad del vínculo materno filial.

El sistema de identificación previsto por la Ley N° 1226 se propone garantizar la indemnidad e integridad del binomio madre – hijo, para lo cual dispone la identificación de todo niño nacido vivo o muerto y de su madre. Además, la Ley prevé la toma y archivo de huellas genéticas sanguíneas correspondientes al niño y a su madre, con el propósito de garantizar el derecho a la identidad del recién nacido.

La Ley citada prevé los procedimientos de identificación tanto de la madre como del niño, contemplando a tal fin la toma y archivo de huellas genéticas sanguíneas correspondientes al recién nacido y a su madre en orden a garantizar el derecho a la identidad del recién nacido.

La Ley de la Ciudad de Buenos Aires no incluye la obtención de las huellas dactilares de la madre y del niño, con lo cual surge la pregunta acerca de cuál es el procedimiento correcto, dado que la Ley N° 26.061 es de alcance nacional. Una posible respuesta es que la ley porteña es complementaria de la ley nacional, por lo tanto, el proceso de identificación del binomio madre-recién nacido en la ciudad de Buenos Aires debe contemplar necesariamente tanto la obtención de la huella genética sanguínea prevista en la Ley N° 1226, y además, los datos requeridos en la Ley N° 26.061, esto es, datos filiatorios, nombre, domicilio y huellas decadactilares de la madre y plantares del recién nacido. (CASAL; 2010)

Esta interpretación se ve abonada por el artículo 16 de la citada Ley porteña, el cual prevé expresamente que la misma es una ley complementaria de la Ley N° 24.540 de la Nación, antecesora de la Ley N° 26.061.

En la provincia de Formosa rige la Ley N° 1129, la cual prevé el sistema de identificación del recién nacido, en el marco de los derechos del niño, uno de los cuales es la preservación de su identidad. El Ministerio de Desarrollo Humano ha implementado un sistema que consiste en la identificación del recién nacido a través de la impresión dactilar –también a la madre- y plantar

del bebé, además de una pulsera con un código único, con la finalidad de asegurar la identidad del binomio madre-hijo y evitar cambios o confusiones.

El sistema contempla dos momentos en la identificación: Uno es antes del corte del cordón umbilical del bebé, cuando el pediatra así lo solicite y, el segundo momento es antes del alta de la madre junto a su chico. Se utiliza una ficha, en cuyo reverso el identificador colocará los datos de la mamá y se le tomarán las impresiones dactilares a la misma (el pulgar), la palma derecha del bebé y también la impresión del pie derecho del bebé. Se confeccionan dos fichas conteniendo todos los datos, una queda archivada en el hospital y la otra se envía al Registro Civil.

Uso de tecnologías biométricas en el proceso de identificación

Si bien en el presente libro se ha hablado de biometrías, explicando su definición y alcances, recordamos una definición que hemos dado en trabajos anteriores, entendiendo por biometría aquellos métodos de identificación y autenticación de los seres humanos a través de características fisiológicas y de comportamiento. La individualidad es aquello que hace que una cosa sea diferente de todas las otras similares de la misma especie; y para determinar la individualidad hay que comparar, colocando una cosa al lado de la otra para poder observar similitudes y diferencias entre ellas. (CASAL; 2010).

El Marco e-ID Social contempla una definición de tecnologías biométricas, entendiendo por tal al “*reconocimiento biométrico a los métodos automatizados que aseguran el reconocimiento de individuos con base en rasgos físicos o conductuales distinguibles. Las tecnologías que se usan en biometría incluyen el reconocimiento de huellas dactilares, de rostros, de patrones de las venas, del iris, de voz y del teclado, entre otros.*”

El mencionado Marco Iberoamericano incluye en su glosario la definición de sistema biométrico, considerando tal al “*sistema informático de reconocimiento con base en uno o varios patrones, que opera requiriendo datos biométricos a un individuo, extractando un patrón de estos datos adquiridos y comparando el ejemplo contra una plantilla previamente registrada. Dependiendo de la aplicación, esta plantilla puede estar almacenada en una base de datos centralizada o en un dispositivo individual, como un token o una tarjeta inteligente.*”

Existen dos tipos de identidad, la identidad absoluta y la identidad práctica; esta última es la que se establece demostrando suficientes similitudes y es, en definitiva, la relevante a la hora de hablar de sistemas biométricos.

La identidad es entonces el conjunto de caracteres que individualizan a una persona: nombre, edad, nacionalidad, estado civil, profesión, señas personales, dibujos de impresiones digitales, etc. (SILVEYRA; 2006)

En épocas recientes, se identificó el término biometría con los métodos automáticos que analizan determinadas características humanas con el fin de identificar y autenticar a las personas (SIGÜENZA PIZARRO Y TAPIADOR MATEOS; 2005)

La biometría permite efectuar el reconocimiento de una característica física o conductual

de la persona. Existen distintos tipos de reconocimientos posibles actualmente: de huellas dactilares, de iris, de la mano, del ADN, de las venas, del trazo de escritura, del tecleo, etc. En los últimos cinco años, las tecnologías biométricas han avanzado enormemente, brindando hoy una multiplicidad de soluciones que los gobiernos pueden utilizar para la identificación de las personas. Estos datos biométricos son la base para el desarrollo e implementación de distintas políticas públicas: de seguridad, de gobierno electrónico, de tránsito fronterizo, y también para la puesta en operación de políticas sociales.

Cualquier política social requiere como un elemento básico, la identificación de la persona. Es un derecho de la persona y un deber del Estado. Es por ello que las decisiones que tomen los gobiernos en la materia tendrán un impacto directo sobre otras políticas públicas que se instrumenten. Esta consideración debería estar presente a la hora de elaborar proyectos de bases de datos biométricas, ya que serán la base sobre la cual podrán edificarse eficientemente otras políticas: de inclusión social, de lucha contra el delito, de gobierno electrónico, etc.

Otro elemento central es la interoperabilidad de las bases de datos biométricos. De poco sirve contar con datos si no pueden ser compartidos. En este sentido, el Marco e-ID Social constituye un importante avance para el futuro establecimiento de estándares de interoperabilidad en materia de tecnologías biométricas, de modo de facilitar el intercambio de información entre las administraciones de los países de la región.

b. Identificación de personas en entornos virtuales

Argentina cuenta con un marco normativo completo relativo a la validez de las transacciones electrónicas. La Ley N° 25.506 de firma digital, reconoce “el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece” dicha ley. (Artículo 1º) La Ley N° 25.506 de firma digital, cuyo antecedente es Decreto Nro. 427 de abril de 1998, constituye el marco legal que otorga validez jurídica al documento digital, la firma electrónica y la firma digital. Contiene en su primer capítulo una serie de disposiciones que intentan eliminar los obstáculos presentes en el derecho civil y comercial tradicional para el reconocimiento de la validez de actos jurídicos. Acorde con las leyes modelo de UNCITRAL sobre comercio electrónico y de firma electrónica, la ley argentina contiene una serie de disposiciones que, basadas en el concepto de equivalente funcional, dotan de virtualidad jurídica a transacciones realizadas en un soporte distinto al papel. (BUGONI, RIVOLTA; 2007)

Los principales obstáculos estaban representados por: a) la exigencia de que los documentos constaran por escrito, b) la necesidad de que estuvieran firmados, y c) su carácter de original y la guarda de documentación. (RIVOLTA; 2008)

Argentina cuenta con un marco normativo completo en materia de transacciones electrónicas: Ley N° 25.506 (B.O. 14/12/2001), el Decreto N° 2628/02 (B.O. 20/12/2002), el Decreto N° 724/06 modificadorio del Decreto N° 2628/02 (B.O. 13/06/06) y la Decisión Administrativa de la Jefatura de Gabinete de Ministros N° 6/07 (B.O. 12-02-07)

La ley de Firma Digital N° 25.506 reconoce el valor jurídico del documento electrónico, la firma electrónica y la firma digital en todo el territorio nacional. Es una ley que complementa las

disposiciones del Código Civil, con el objetivo de facilitar el uso de medios digitales para la realización de transacciones, tanto entre particulares como por parte de los organismos del Estado. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

La Ley N° 25.506 incorpora el concepto de documento digital, equiparándolo con el concepto de documento tradicional en soporte papel, aclarando que el documento electrónico satisface el requerimiento de escritura que los códigos tradicionales incluyen. Reza la Ley:

ARTÍCULO 6º — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

Respecto de la firma, la Ley N° 25.506 incorpora dos conceptos: la firma electrónica y la firma digital. (MASON, 2006). Ambas especies de firma son válidas, de acuerdo con el artículo 1º de la Ley. Más precisamente, existe una amplia gama de alternativas para la firma electrónica, que van desde un simple correo electrónico, el uso de tecnologías de clave pública compartidas (PGP), el uso de palabras clave basadas en criptografía simétrica, hasta el uso de tecnología de clave pública basada en certificados digitales emitidos por una entidad de certificación que no se encuentre licenciada por la autoridad pública. Una firma digital que utilice criptografía asimétrica y tecnología de clave pública, puede ser considerada como una firma electrónica, tanto como la mera inclusión del nombre como parte del texto de un mensaje de correo electrónico, en la medida que el firmante haya ejecutado o adoptado el símbolo con la intención de firmar, esto es, como declaración de voluntad respecto del contenido del mensaje. (RIVOLTA, SCHAPPER, 2004).

La diferencia entre una firma electrónica y una firma digital, desde el punto de vista jurídico, radica en la carga de la prueba de su validez. En el artículo 5º la Ley define como firma electrónica “*al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.*”

La firma digital es aquella que se basa en certificados digitales emitidos por una autoridad certificante habilitada por la Autoridad de Aplicación de la ley. El artículo 2 define como firma digital al “*resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.*”

La Ley otorga una fuerza probatoria superior a la firma digital respecto de la firma electrónica. Le asigna dos presunciones iuris tantum, es decir, que admiten prueba en contrario. En efecto, el artículo 7º dispone que un documento firmado digitalmente goza de la presunción de autoría

respecto de la persona titular del certificado digital, y por su parte, el artículo 8º establece la presunción de integridad del documento electrónico firmado digitalmente, es decir, que se presume que dicho documento no ha sido alterado. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Sin embargo, debe destacarse que la firma digital de un documento no impide que el mismo sea modificado. Simplemente asegura que, si el documento electrónico firmado digitalmente sufre alguna alteración, esta circunstancia queda en evidencia. Es por ello que el legislador le asigna una presunción de integridad. (RIVOLTA; 2008)

Además de lo dicho, la Ley contiene disposiciones sobre la calidad de “original” de un documento electrónico en el artículo 11 y sobre la conservación de los documentos digitales en el artículo 12. Contiene disposiciones relativas a la consideración de original y a la forma escrita, destacando que un documento electrónico cumple dichos requisitos en la medida que sea accesible para su posterior consulta. (RIVOLTA; 2010)

El sistema establecido por la Ley N° 25.506 se basa en un esquema de Infraestructura de Firma Digital, en el cual solamente se consideran firmas digitales a aquellas que han sido producidas mediante el uso de certificados de clave pública emitidos por certificadores previamente licenciados por la Autoridad de Aplicación, la Jefatura de Gabinete de Ministros,

Sin embargo, la Ley contempla el caso de aquellos certificados que han sido emitidos por certificadores extranjeros. Tal situación está prevista en el artículo 16, admitiendo su validez bajo condiciones. En efecto, con respecto a la validez de los certificados emitidos por certificadores extranjeros, la ley dispone que:

Artículo 16: Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

- a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero, o
- b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.

La Ley N° 25.506 establece un esquema de Infraestructura de Clave Pública, constituyendo un sistema basado en criptografía asimétrica, con un órgano público que licencia y autoriza a funcionar a las autoridades certificantes emisoras de certificados de firma digital, y cuyos elementos son detallados en los siguientes capítulos, los cuales se refieren ya específicamente a los componentes de la Infraestructura de Firma Digital: certificados digitales, certificadores licenciados, titulares de certificados, organización institucional, autoridades, sistema de auditoría, responsabilidad, régimen de sanciones, etc. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Dada la limitación de extensión del artículo, simplemente detallaremos los principales

conceptos que nuestra ley contempla.

Infraestructura de Firma Digital

Una Infraestructura de Firma Digital, o PKI por sus siglas en inglés (Public Key Infrastructure) es “una combinación de tecnología (hardware y software), procesos (políticas, prácticas y procedimientos) y componentes legales (acuerdos) que asocian la identidad del poseedor de una clave privada con su correspondiente clave pública, usando la tecnología de criptografía asimétrica”. Los usos de una PKI en entornos digitales pueden ser múltiples: proteger la confidencialidad (mediante la encripción de comunicaciones o de datos almacenados), autenticar la identidad de una persona u organización, informar sobre la integridad de un mensaje o documento electrónico, y garantizar el no repudio de mensajes o transacciones electrónicas. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Componentes de la Infraestructura de Firma Digital

Las tecnologías de clave pública no pueden garantizar por sí solas la identificación de las personas en el mundo real, ya sea la identificación de personas físicas, organizaciones públicas y privadas o atributos de entidades de todo tipo, tales como servidores.

Para ello, deben adoptarse adicionalmente otras medidas, además de la tecnología de clave pública. Cuando se habla de Infraestructura de Claves Públicas (sinónimo de Infraestructura de Firma Digital), se está aludiendo a este conjunto de elementos que comprende a los pares de claves asociados con una identificación en el mundo real. Asimismo, abarca los mecanismos para generar los pares de claves, los resguardos de seguridad para alojar la clave privada, y en este sentido cabe mencionar los dispositivos de generación y almacenamiento de la clave privada, así como los mecanismos de resguardo de la clave privada, que pueden ser desde una simple password, una passphrase, o bien basarse en biometría (por ejemplo, la huella dactilar). (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Una característica distintiva de la PKI es que el receptor del mensaje debe tener acceso a la clave pública de la persona que lo remite. Es así como surge el concepto de certificado digital, así como la necesidad de contar con directorios en los cuales se publiquen dichos certificados digitales, y que sean accesibles para su consulta pública.

A fin de satisfacer los requerimientos detallados en el punto precedente, una PKI contempla los siguientes elementos:

- Estándares y protocolos;
- Software para implementar un gran número de funciones y protocolos;
- Protección de las claves privadas;
- Un repositorio de claves públicas, su creación, mantenimiento y uso;
- Los elementos que permitan firmar digitalmente los certificados por la entidad de certificación;
- Un marco legal que regule y apoye la infraestructura y su operación y
- Servicios para apoyar la operación de aplicaciones que utilicen firma digital.

En síntesis, una infraestructura de clave pública incluye:

- Una Autoridad Certificante (CA por sus siglas en inglés), también denominada Entidad de Certificación o Certificador, según la distinta legislación. La CA emite y garantiza la autenticidad de sus Certificados Digitales. Un Certificado Digital incluye la clave pública u otra información respecto de la clave pública.
- Una Autoridad de Registro (RA por sus siglas en inglés) – valida los requerimientos de Certificados Digitales. La Autoridad de Registro autoriza la emisión del certificado de clave pública al solicitante por parte de la Autoridad Certificante.
- Un sistema de administración de certificados – una aplicación de software provisto por el vendedor de PKI.
- Un directorio en el cual los certificados y sus claves públicas son almacenados.
- El Certificado Digital incluye el nombre de su titular y su clave pública, la firma digital de la Autoridad Certificante que emite el certificado, un número de serie y la fecha de expiración.
- Suscriptores: son las personas o entidades nombrados o identificados en los certificados de clave pública, tenedores de las claves privadas correspondientes a las claves públicas de los certificados digitales.
- Usuarios: son las personas que validan la integridad y autenticidad de un documento digital o mensaje de datos, en base al certificado digital del firmante. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Qué es una firma digital

Según la Ley argentina, el proceso de firmado digital de un documento electrónico presenta dos momentos:

- un primer momento en el cual el suscriptor de un certificado digital firma digitalmente un documento electrónico
- un segundo momento en el cual un tercero, receptor de ese documento electrónico firmado digitalmente, verifica la autoría e integridad del mensaje.

Las firmas digitales son una aplicación muy importante de esta tecnología de claves públicas. En efecto, la persona que remite un mensaje utiliza su clave privada para encriptar el digesto seguro del mensaje (obtenido mediante el cálculo de la función de hash del mensaje). Remite al receptor el mensaje, el digesto seguro encriptado y su certificado digital que contiene su clave pública. El receptor desencripta el digesto utilizando la clave pública del emisor del mensaje, la cual se corresponde con la clave privada del mismo. El receptor del mensaje, verifica la firma digital del mensaje, para lo cual recalcula la función de hash de este, y si ambos resultados coinciden, verifica que el mensaje no ha sido alterado, con lo cual puede tener certeza de su integridad. Si fue posible desencriptar el digesto con la clave pública correspondiente al emisor del mensaje, verifica la autoría del documento electrónico firmado digitalmente. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Estándares Tecnológicos

Tal como sucede en otros ámbitos, las tecnologías de clave pública se apoyan en estándares. A medida que las iniciativas e infraestructuras de clave pública van proliferando, comienzan

a aparecer modificaciones a los estándares utilizados inicialmente para poder ampliar su funcionalidad o para hacerlos más específicos y con un contenido semántico mas claro. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Los estándares se refieren, entre otros, a los siguientes componentes:

- Estándares para algoritmos de encripción y algoritmos de hash.
- Protocolos para parámetros acordados asociados con los algoritmos de encripción y algoritmos de hash.
- Protocolos para facilitar el acceso de usuarios a las claves públicas.
- Protocolos para facilitar el acceso de usuarios a las noticias de revocación
- Estándares para la generación segura de pares de claves
- Estándares y protocolos para apoyar el mecanismo de sincronización y fechado con valor probatorio (time stamping)
- Estándares para el software de:
 - Generación de pares de claves
 - Almacenamiento de claves privadas
 - Almacenamiento de claves públicas
 - Acceso de usuarios a claves públicas
 - Generación de digestos seguros de mensajes
 - De encripción de mensajes
 - De creación de mensajes
 - De solicitud de claves públicas
 - De verificación de claves públicas: de su validez, de su vigencia, de no haber sido revocadas
 - De desencripción de mensajes
 - De desencripción de digestos seguros
 - De comparación de digestos descriptados
 - De tiempo
 - De protección de claves privadas
 - Contra intrusiones cuando están almacenadas
 - Contra intrusiones cuando están en la memoria principal
 - Contra invocaciones no autorizadas
- De Directorio si es utilizado como Repositorio de claves públicas:
 - Protocolos para insertar datos y mantener datos en el repositorio
 - Protocolos para acceder a los datos del repositorio
- De los certificados de la Autoridad de Certificación:
 - Estándares para formatos de certificados
 - Perfiles para aplicación de los estándares en contextos particulares
- Protocolos para la comunicación de certificados a las partes que los necesiten
- Medios por los cuales los receptores de mensajes pueden evaluar si chequean la firma digital del certificado
- Medios por los cuales los receptores de mensajes pueden chequear la firma digital del certificado
- Medios por los cuales los receptores de mensajes pueden evaluar la extensión de las afirmaciones contenidas en el certificado

- Si los certificados son firmados por Autoridades de Certificación:
- Estándares para Autoridades de Certificación
- Estándares y procedimientos para registro y auditoría de Autoridades de Certificación
- Procedimientos para recurrir contra la Autoridades de Certificación
- Seguros que deben contratar las Autoridades de Certificación

Si el marco legal vincula un par de claves con algo del mundo real como parte de una PKI, más allá de un nivel de aplicación informática (como es el caso argentino y la mayoría de las legislaciones latinoamericanas), entonces la PKI debe contener los medios para establecer la asociación del par de claves con un dispositivo, persona física, persona jurídica, atributo, agencia pública o lugar. (RIVOLTA, SCHAPPER; 2004)

III. Marco para la Identificación Electrónica Social Iberoamericana

A partir del explosivo desarrollo de las TIC, el principal objetivo de la legislación sobre comercio electrónico o firma electrónica, ha sido remover los obstáculos para el uso de la legislación tradicional interna de cada país, en las nuevas aplicaciones basadas en transacciones electrónicas.

Con ese propósito, los países han desarrollado legislación específica que proporciona nuevas alternativas a las firmas manuscritas, basadas tanto en las Leyes Modelo de Uncitral sobre Comercio Electrónico (1996) y sobre Firma Electrónica (2001), cuanto en la Directiva 99/93 de la Unión Europea, en la Ley de Firma Electrónica de Estados Unidos conocida como E-Sign, o en una combinación de ellas. (RIVOLTA, SCHAPPER; 2004), (UNCITRAL; 2009).

Los países de la región han desarrollado legislación específica sobre comercio electrónico o sobre firmas electrónicas. Los enfoques que se adoptaron están basados en cada sistema legal en particular de cada uno de los países. En aquellos países cuyos regímenes jurídicos pertenecen al common law, en los cuales la regulación es más abierta, a menudo ha sido necesario solamente reconocer el no repudio de un documento electrónico (electronic record) o de una firma electrónica (tal como lo establece la Ley de Firma Electrónica de Estados Unidos de América – E-Sign). En aquellos países con regímenes de derecho civil codificado, se han formulado tipos muy prescriptivos de legislación sobre firmas electrónicas o comercio electrónico, con énfasis en normas técnicas y operacionales y en las formalidades de los actos, específicamente basados en firmas digitales (RIVOLTA, SCHAPPER; 2004).

Sin embargo, a pesar del gran avance alcanzado en la materia, las legislaciones nacionales no trascienden las fronteras, con lo cual, pensar un escenario de transacciones internacionales y regionales, generó la necesidad de construir consensos mínimos que faciliten la celebración de acuerdos tendientes a establecer normativas de alcance trasnacional.

El propósito del Marco e-ID Social es establecer un conjunto de conceptos, fundamentos, principios y orientaciones de utilidad para el diseño, implantación y desarrollo de una Identificación Electrónica Social Iberoamericana que consolide en la región el reconocimiento, ejercicio y goce efectivo de los derechos sociales de los ciudadanos iberoamericanos.

a. Identificación electrónica social y autenticación electrónica

El Marco e-ID Social distingue dos conceptos, los cuales define:

1.- “**Identificación Electrónica Social**”: entendiendo por tal al “*procedimiento que mediante elementos externos, permite asignar una identidad con determinados atributos a una persona concreta, esto es, a la comprobación de los datos que acreditan que un individuo es efectivamente la persona que dice ser, sujeto de derecho, con determinados atributos.*”

2.- “**Autenticación Electrónica**”: entendiendo por tal al “*proceso de verificación de la autenticidad de las identificaciones realizadas o solicitadas por una persona física o entidad, sobre los datos tales como un mensaje u otros medios de transmisión electrónica. El proceso de autenticación es la segunda de dos etapas que comprenden: 1) La presentación de un medio que acredita la identificación ante el sistema y, 2) La presentación o generación de información que corrobora la relación entre el medio presentado y la persona o entidad identificada.*”

En este sentido, el Marco e-ID Social conjuga en su texto dos conceptos que usualmente aparecen disociados. En efecto, el concepto de “**identificación electrónica social**” alude al procedimiento de asociación entre los atributos de una persona y la persona misma, y también al proceso de comprobación de dichos datos con la persona concreta. Esto señala dos momentos, que estarían comprendidos en el concepto de identificación electrónica social. Un primer momento en el cual una autoridad certifica la identidad de una persona, después de haber asociado determinados atributos (nombre, lugar de nacimiento, datos filiatorios, datos biométricos) con la persona física en sí, mediante un procedimiento establecido. Un segundo momento, en el cual alguien verifica que la correlación de dichos datos con la persona en sí.

Este procedimiento debe basarse en elementos externos a la persona, los cuales constarán en un documento oficial que acredite en adelante dicha identidad. Este documento deberá contener estos datos de modo tal que permita el proceso de identificación a terceras partes.

El concepto de “**autenticación electrónica**” es innovador. Por primera vez aparece en documentos vinculados con la identificación. Este concepto, alude a un tercer momento: el de la verificación de la autenticidad de las identificaciones realizadas o solicitadas por una persona física o entidad, sobre los datos tales como un mensaje de datos u otros medios de identificación electrónica. Este concepto introduce algunos elementos novedosos que nos gustaría destacar.

Por una parte, se aplica tanto a personas físicas como a entidades, esto es, a dispositivos electrónicos automatizados, como servidores, sistemas informáticos, etc. Que interactúen entre sí o con particulares. Se incluye así el valor de la acción realizada por un sistema informático, aún sin la actividad humana directa. Este elemento ya figura en la Ley argentina de firma digital, que reconoce en su artículo 10, la presunción de remitente. Esta norma dispone que se presume, salvo prueba en contrario, que el documento firmado digitalmente proviene del remitente, en aquellos casos que este documento digital haya sido enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente.

Por otra parte, el concepto de “**autenticación electrónica**” que alude al proceso de verificación

de la autenticidad de las identificaciones realizadas por medio de mensajes de datos u otros medios de transmisión electrónica, es un concepto que respeta totalmente el principio de neutralidad tecnológica que debe imperar en toda norma. En efecto, dado que el tiempo de evolución de la tecnología es sumamente acelerado, mientras que los procesos de elaboración normativa por definición son largos, dado que requieren de consensos complejos, una adecuada técnica normativa indica el beneficio de contar con regulaciones tecnológicamente neutras, esto es, que no se definan por una tecnología u otra, ya que seguramente quedarán obsoletas en el corto plazo. En los casos en que las leyes adoptan una solución tecnológica, ya no forman parte de la solución sino que pasan a constituir parte del problema. (SCHAPPER, RIVOLTA, VEIGA MALTA; 2006)

El concepto de autenticación electrónica que contiene el Marco e-ID Social, es tecnológicamente neutro. Cuando se refiere a “otros medios de transmisión electrónica” deja abierta la posibilidad de incluir a cualquier otro medio que no sea el soporte físico en papel, sin establecer una u otra tecnología.

En este sentido, el Marco e-ID Social, admite como formas de autenticación electrónica a lo que nosotros conocemos como firmas electrónicas, firmas digitales, tecnologías biométricas, y todo otro mecanismo electrónico de acreditación de identidad. Lo novedoso de esta iniciativa es que nombra correctamente las funciones: por un lado, la identificación, que incluye elementos tecnológicos como biometría. Y por otra parte, el proceso de autenticación electrónica, que admite todo tipo de procedimientos electrónicos.

Esta visión es superadora de la actual. En efecto, el marco normativo actual, proveniente de las leyes de comercio electrónico, firma electrónica y firma digital, han puesto el acento en la función de firmado de documentos. Sin desconocer que constituyen un avance importantísimo para el desarrollo del comercio electrónico y el gobierno digital, las leyes de firma electrónica o firma digital se refieren a dos situaciones distintas. Por un lado, el sustituto electrónico de la firma manuscrita, como expresión del consentimiento de la persona con el otorgamiento de un acto jurídico. Y por el otro, el proceso de identificarse ante un sistema informático.

Un ejemplo lo podemos ver en el caso de la factura electrónica. La factura en papel no requiere la firma del comerciante que la emite. Sin embargo, cuando algunas iniciativas de factura electrónica incluían la firma digital. Esto significa que se le pedían más formalidades a la solución digital que a la tradicional.

El Marco e-ID Social, correctamente a nuestro juicio, define la instancia de autenticación electrónica en forma independiente de los conceptos de firma electrónica y de firma digital que define en el glosario, ya que se trata de institutos diferentes. A modo de ejemplo, cuando deseo ingresar al edificio del Registro Civil para contraer matrimonio, en la puerta no tengo que presentar credenciales, pero al momento de firmar el acta, mi firma manuscrita perfecciona la expresión del consentimiento.

El Marco e-ID Social se inspira en la Convención de UNCITRAL sobre comunicaciones electrónicas en contratos internacionales, que contempla el principio del equivalente funcional, admitiendo el uso de variadas técnicas de autenticación electrónica. En cuanto a las razones

jurídicas, es posible afirmar que la evolución del derecho ha superado la visión inicial proclive a admitir solamente las firmas digitales. (UNCITRAL; 2007)

En ese sentido, el panorama jurídico es lo suficientemente amplio como para dar validez a cualquier método de autenticación electrónica que esté acordado entre las partes o cuyo procedimiento cuente con algún marco procedural. Así se admiten las claves simétricas, tecnologías biométricas, firmas digitales emitidas por certificadores no licenciados, todas ellas con el valor jurídico de una firma electrónica susceptible de dar por satisfecho el requisito legal de “firma” como expresión del consentimiento de la persona.

b. Factores de autenticación

El Marco e-ID Social contiene un glosario de términos que constituye un punto de partida para el establecimiento de acuerdos entre nuestros países.

Define a los **factores de autenticación** como aquellos “elementos que integran el proceso de identificación”, a saber:

- *Algo que sé*: la persona se autentica mediante algo que sabe: una clave, un número que la identifica – PIN, una frase o una respuesta a una pregunta de seguridad.
- *Algo que tengo*: la persona se autentica utilizando algo que posee: un token, una tarjeta inteligente, un certificado digital.
- *Algo que soy*: el individuo se autentica con base en una característica que tiene su persona, esto es, un dato biométrico.

El glosario también define el concepto de tecnologías biométricas, como aquellos “*métodos automatizados que aseguran el reconocimiento de individuos con base en rasgos físicos o conductuales distinguibles.* Las tecnologías utilizadas en biometría incluyen el reconocimiento de huellas dactilares, de rostros, de patrones de las venas, del iris, de voz y del tecleo, entre otros.” (MARCO; 2011)

En cuanto a los sistemas biométricos, el Marco e-ID Social, lo define como el “*sistema informático de reconocimiento con base en uno o varios patrones, que opera requiriendo datos biométricos a un individuo, extractando un patrón de estos datos adquiridos y comparando el ejemplo contra una plantilla previamente registrada. Dependiendo de la aplicación, esta plantilla puede estar almacenada en una base de datos centralizada o en un dispositivo individual, como un token o una tarjeta inteligente.*” (MARCO; 2011)

A continuación, el Marco e-ID Social define las **Infraestructuras de Clave Pública**, también conocidas como Infraestructuras de Firma Digital o PKI por sus siglas en inglés - Public Key Infrastructure. Entiende por tal al “*conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de clave pública basados en criptografía asimétrica, que facilitan la creación de una asociación verificable entre una clave pública y la identidad del tenedor de su correspondiente clave privada.*” (MARCO; 2011)

Seguidamente, se refiere a la **firma digital**, también conocida como firma electrónica segura, firma electrónica avanzada o firma electrónica reconocida. El Marco e-ID Social reconoce dos

acepciones de la firma digital: un aspecto jurídico y un aspecto tecnológico. En cuanto a la acepción tecnológica, está vinculada con las tecnologías de clave pública. El aspecto jurídico responde a la definición que las leyes nacionales han incluido como equivalente a la firma manuscrita. El Marco e-ID Social introduce esta doble mirada a fin de superar los inconvenientes que a veces se producen debido a distintas interpretaciones.

Expresamente contempla ambas acepciones del concepto de firma digital:

Desde el punto de vista **tecnológico**, una firma digital es el mecanismo de autenticación que, sustentado en criptografía asimétrica, esto es, que usa dos claves, una pública y una privada, permite identificar al firmante y garantizar la integridad del contenido del documento electrónico firmado.

Desde el punto de vista **jurídico**, las leyes incluyen un requisito administrativo. Ello significa que para ser considerada legalmente firma digital, ese mecanismo debe haber sido aplicado mediante el uso de un certificado digital emitido por una entidad de certificación acreditada por el órgano rector del Estado en dicha materia

Pero no debe confundirse este tema de la firma digital, que permite asegurar la autoría de un documento electrónico, con el tema de la verificación de la identidad en entornos digitales. Así como en el derecho civil, la firma es la expresión del consentimiento de la persona en una determinada transacción, distinta de la identificación de dicha persona, que se realiza mediante el cotejo con su documento nacional de identidad. En el entorno digital, suele confundirse la función de firma digital con la función de identificación de las personas en entornos electrónicos. La función de identificación de las personas está asignada al Registro Nacional de las Personas según la legislación nacional.

En tal sentido, la posibilidad de instrumentar documentos nacionales de identidad con dispositivos electrónicos que alberguen datos biométricos de sus titulares, será un gran avance para la identificación de personas en entornos digitales. Mientras eso no suceda, deberemos continuar con sistemas de autenticación electrónica tradicionales.

Finalmente, el Glosario contempla la definición de “**firma electrónica**”. El Marco e-ID Social entiende por tal *“a cualquier sonido, símbolo o proceso, adjunto o lógicamente asociado a un documento electrónico que exprese el consentimiento de una persona emitido en formato digital, y ejecutado o adoptado por dicha persona con el propósito de firmar el documento electrónico. En general, las leyes denominan ‘firma electrónica’ a cualquier mecanismo de autenticación que no cumpla alguno de los requisitos exigidos para una firma digital. ‘Firma electrónica’ es el término genérico y neutral para referirse al universo de tecnologías que una persona puede utilizar para expresar su consentimiento con el contenido de un documento.”* (MARCO; 2011)

c. Acuerdos de reconocimiento mutuo

En su capítulo 3, el Marco e-ID Social contempla los acuerdos de reconocimiento mutuo entre los países signatarios de la Declaración de Asunción. El Marco e-ID Social, se propone abordar los aspectos vinculados a los procesos de identificación electrónica de personas en entornos físicos o virtuales, con el fin de sentar las bases para lograr futuros acuerdos de reconocimiento mutuo

que permitan establecer un medio común de Identificación Electrónica Social Iberoamericana. (MARCO; 2011)

El Marco e-ID Social intenta ser un punto de partida que oriente la discusión de los aspectos legales y técnicos necesarios para la celebración de acuerdos de intercambio de datos, la interoperabilidad de sistemas y el establecimiento de estándares tecnológicos comunes en materia de identificación electrónica, incluyendo tecnologías biométricas y certificados de firma digital.

IV. Conclusiones

Como decíamos en un trabajo anterior (CASAL; 2010), el tema de la identificación en entornos digitales no está resuelto aún. Por el contrario, debido al desarrollo de plataformas transaccionales de gobierno electrónico, es un aspecto que comienza a ser analizado.

Por un lado, los países disponen de sistemas de identificación ciudadana tradicionales, que se concretan en documentos de identidad y en documentos de viaje para el tránsito fronterizo.

Por otra parte, los sistemas informáticos usan distintos elementos tecnológicos para autenticar a las personas en dichas aplicaciones.

Actualmente, en materia de gobierno electrónico, la tendencia es a utilizar mecanismos de autenticación basados en claves compartidas, y un movimiento incipiente que tiende al uso de certificados digitales, básicamente para identificar sitios web seguros.

Pero por otra parte, desde hace pocos años los sistemas de identificación biométrica han irrumpido en la escena. Han surgido poderosas tecnologías que permiten el reconocimiento de personas a partir de datos biométricos: el iris, las huellas dactilares, el rostro, la mano, las venas, el ADN, etc.

Estas tecnologías biométricas están siendo contempladas por los países para la emisión de los documentos de identidad, mediante la inclusión en dichos documentos de dispositivos que almacenan información biométrica de las personas, datos que permiten la posterior verificación de su identidad.

El uso de biometría es beneficioso para los gobiernos en la medida que facilita la identificación indubitable de la persona, y que, si se incluyen dispositivos tecnológicos, permitiría ampliar el alcance de políticas de gobierno electrónico. Pero por sobre todo, es un instrumento necesario para la protección de la identidad de cada uno de nosotros. Siendo el robo de identidad uno de los males de nuestro tiempo, nada mejor que la identificación biométrica para proteger nuestro derecho a la identidad. (CASAL; 2010)

El derecho a la identidad es un derecho personalísimo. Compartimos con Bustamante Donas que “No puede haber justicia social sin inclusión social, y no se puede entender en estos días la inclusión social sin inclusión digital.” El concepto de identidad está íntimamente vinculado con el de ciudadanía, entendida como capacidad para interactuar con las administraciones a través de redes de información y para acceder a servicios más completos y simples de utilizar. (BUSTAMANTE DONAS; 2007)

El Marco e-ID introduce por primera vez una distinción y una relación. La distinción tiene que ver con clarificar los conceptos de firma, identificación y autenticación. Decimos que establece por primera vez una relación por cuanto al introducir el concepto de autenticación electrónica, establece un vínculo entre los conceptos de identificación y de firma electrónica/digital.

El Marco e-ID por primera vez nos permite distinguir los conceptos de firma, como elemento que representa la expresión del consentimiento de una persona con un acto jurídico, de la noción de identificación en entornos electrónicos, contenida en el concepto de autenticación electrónica.

En efecto, en nuestro derecho positivo, la firma es un medio que la ley reconoce para vincular un documento con su autor. En un sentido amplio, la firma es cualquier método o símbolo utilizado por una persona con la intención de vincularse o autenticar un documento. (LORENZETTI; 2001). Las técnicas que se utilizan para firmar pueden ser variadas: desde el trazo de la mano en un papel (firma manuscrita), la firma manual contenida en un sello, la firma manuscrita digitalizada, una clave compartida (por ejemplo, en los cajeros automáticos de los Bancos), una identificación biométrica o una clave asimétrica reconocida o no en un esquema PKI. Pero cualquiera de estas técnicas son jurídicamente reconocidas como “firma” de la persona. (RIVOLTA; 2010)

Nuestro derecho de fondo, el Código Civil, dispone que la firma sea un requisito para el otorgamiento de instrumentos privados y públicos, como manifestación del consentimiento de la persona con el objeto del acto jurídico. (RIVOLTA; 2010) El Código de Vélez, del año 1869, no requiere en su articulado que la firma sea manuscrita, salvo en cuanto al testamento ológrafo. En efecto, el artículo 3639 dispone que:

Art. 3.639. El testamento ológrafo para ser válido en cuanto a sus formas, debe ser escrito todo entero, fechado y firmado por la mano misma del testador. La falta de alguna de estas formalidades lo anula en todo su contenido.

Por otra parte, nuestro Código Civil establece que las formas y solemnidades de los actos jurídicos serán aquellas que se establezcan por las leyes del lugar de celebración.

Art. 950. Respecto a las formas y solemnidades de los actos jurídicos, su validez o nulidad será juzgada por las leyes y usos del lugar en que los actos se realizaran.

A su vez, el Código prevé la existencia de instrumentos públicos y de instrumentos privados. En cada caso, la firma constituye un requisito esencial. La ausencia de firma torna al acto anulable.

Art. 988. El instrumento público requiere esencialmente para su validez, que esté firmado por todos los interesados que aparezcan como parte en él. Si alguno o algunos de los cointeresados solidarios o meramente mancomunados no lo firmasen, el acto sería de ningún valor para todos los que lo hubiesen firmado.

Art. 989. Son anulables los instrumentos públicos, cuando algunas de las partes que aparecen firmadas en ellos, los arguyesen de falsos en el todo, o en parte principal, o cuando tuviesen enmiendas, palabras entre líneas, borraduras o alteraciones en partes esenciales, como la fecha, nombres, cantidades, cosas, etcétera, no salvadas al fin.

Art. 1.012. La firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos

El Código contempla el principio de libertad de las formas para los actos jurídicos celebrados por instrumentos privados.

Art. 1.020. Para los actos bajo firma privada no hay forma alguna especial. Las partes pueden formarlos en el idioma y con las solemnidades que juzguen más convenientes.

El Código Civil prevé el repudio del acto, habilitando al signatario a desconocer el contenido del mismo, mediante los elementos probatorios que considere convenientes, excepto el de testigos.

Art. 1.017. El signatario puede, sin embargo, oponerse al contenido del acto, probando que las declaraciones u obligaciones que se encuentran en él, no son las que ha tenido intención de hacer o de contratar. Esta prueba no puede ser hecha con testigos.

En síntesis, la introducción del concepto de autenticación electrónica que promueve el Marco e-ID Social, nos permite ir distinguiendo la diferencia entre el proceso de identificación de una persona en un entorno digital, y el acto de firmar un documento. La firma de un documento, tanto en un soporte papel como digital, es un acto de manifestación de la voluntad de una persona que expresa su consentimiento con el otorgamiento de un determinado acto jurídico.

La autenticación electrónica, por el contrario, es un estadio previo, en el cual la persona se presenta ante un sistema y acredita su identidad. No manifiesta su voluntad, ni expresa su consentimiento con acto jurídico alguno.

El Marco e-ID Social es un importante avance. Establece una matriz común para iniciar el diálogo que facilite el reconocimiento mutuo de identificadores electrónicos, y el recorrido de un camino coherente en materia de identificación de personas. Nuestros países están avanzando en lograr superar la brecha digital, mediante acciones efectivas en materia de inclusión social.

Se presenta entonces un nuevo escenario en el cual la identificación de personas es un requisito impostergable para lograr la ejecución eficaz de las políticas públicas de inclusión. Al mismo tiempo, el aumento de usuarios de las TIC que se está logrando gracias a los programas de inclusión digital educativa y de ampliación del acceso a medios electrónicos nos pone frente al desafío de prepararnos para un aumento de la demanda de servicios digitales. Ello implica lograr mecanismos de autenticación electrónica ágiles y a la vez seguros.

Sería deseable que las normas nacionales se inspiren en este Marco Iberoamericano, así como los acuerdos que se logren respondan a esquemas internacionales, es decir, abrevan en fuentes comunitarias o tratados internacionales que fijen criterios mínimos comunes, con un enfoque tecnológicamente neutro que las dote de la capacidad de mantener su vigencia a pesar del constante avance tecnológico (LORENZETTI, 2001), (RIVOLTA; 2008).

El Marco e-ID es un primer paso.

V. Bibliografía

- BUSTAMANTE DONAS, J. (2007): "Los nuevos derechos humanos: gobierno electrónico e informática comunitaria", Enlace: Revista Venezolana de Información, Tecnología y Conocimiento – Mayo Agosto, 2007, volumen 4, número 002, Universidad de Zulia, Venezuela. Disponible en internet en <http://redalyc.uaemex.mx/redalyc/pdf/823/82340202.pdf>.
- BUGONI, M. y RIVOLTA, M. (2007): "e-autenticación. Firma Digital y Firma Electrónica. Panorama en la República Argentina", Observatorio de Políticas Públicas de la Jefatura de Gabinete de Ministros, Buenos Aires, Septiembre 2007.
- BUGONI, M.; RIVOLTA, M. y FERNANDEZ, J. (2010): "Políticas de Tecnologías de la Información y las Comunicaciones en la Gestión Pública", en "Políticas Públicas en Democracia", Secretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros de Argentina, Buenos Aires, 2010.
- CASAL, G. (2010): "Derecho a la identidad y biometría en la Argentina" Ponencia presentada en el XV Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Santo Domingo, Noviembre 2010.
- CASAL, G. (2010): "Derecho a la identidad y biometría en la Argentina", en Biometrías. Herramientas para la Identidad y la Seguridad Pública, Jefatura de Gabinete de Ministros, Buenos Aires, 2010.
- CARTA IBEROAMERICANA DE GOBIERNO ELECTRONICO, CLAD, 2007. Disponible en internet en <http://www.clad.org/documentos/declaraciones/cartagobelec.pdf>.
- MARCO PARA LA IDENTIFICACION ELECTRONICA SOCIAL IBEROAMERICANA (2011), disponible en internet en <http://www.clad.org/documentos/otros-documentos/marco-para-la-identificacion-electronica-social-iberoamericana>
- MASON, S. (2006): "Electronic Signatures in Practice" Journal of High Technology Law, Volume 6, Number 2, 148 – 164. J. High Tech L. 148 Disponible en Internet en <http://www.jhtl.org/docs/pdf/Mason.pdf>.
- RIVOLTA, Mercedes y SCHAPPER, Paul (2004): "Autenticación & Firmas Digitales en E-Legislación y Seguridad. Guía para la regulación y el gerenciamiento de aplicaciones de comercio electrónico y de compras públicas electrónicas", Banco Interamericano de Desarrollo, 2004. Disponible en Internet en <http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=645510>
- RIVOLTA, M., SCHAPPER, P. y VEIGA MALTA, J. (2006): "Risk and Law in Authentication", Digital Evidence Journal, Vol 3 number 1, London, UK, 2006.
- RIVOLTA, M. (2008): "Leyes de 3^a generación: hacia el pleno reconocimiento del derecho a la administración electrónica" Ponencia presentada en el XIII Congreso del CLAD para la reforma del Estado y de la Administración, Buenos Aires, noviembre 2008.
- RIVOLTA, M. (2010): "Biometría y autenticación digital: firma electrónica segura o firma digital", en "Biometrías. Herramientas para la Identidad y la Seguridad Pública", Jefatura de Gabinete de Ministros, Buenos Aires, 2010.
- SILVEYRA, J. (2006): "Sistemas de Identificación Humana", Ediciones La Rocca, Buenos Aires 2006.
- SIGÜENZA PIZARRO Y TAPIADOR MATEOS (2005): "Tecnologías Biométricas aplicadas a la Seguridad", Alfaomega – Ra-Ma, México 2005.
- UNCITRAL (2001): "Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al

derecho interno 2001”, Naciones Unidas, Nueva York, 2002. Disponible en Internet en <http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf>.

UNCITRAL (2007): “Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en Contratos Internacionales”, Naciones Unidas, Nueva York, 2007. Disponible en Internet en http://www.uncitral.org/pdf/spanish/texts/electcom/06-57455_Ebook.pdf

UNCITRAL (2009): “Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica”, Naciones Unidas, Viena, 2009. Disponible en Internet en http://www.uncitral.org/pdf/spanish/publications/sales_publications/Promoting_confidenceS.pdf.

Anexo

Marco para la Identificación Electrónica Social Iberoamericana

Aprobado por la XIII Conferencia Iberoamericana
de Ministros y Ministras de Administración Pública
y Reforma del Estado
Asunción, Paraguay, 30 de junio - 1º de julio de 2011

Contenido

I.	Resumen Ejecutivo	243
II.	Antecedentes	244
	Declaración de Lisboa	244
	Conferencias Sectoriales de Ministros	245
	Declaración de Mar Del Plata	247
	Carta Iberoamericana de Gobierno Electrónico	248
III.	Elementos de la Identificación Electrónica	250
	Importancia de la Identificación Electrónica para el Pleno Ejercicio de los Derechos	250
	Elementos que Permiten la Identificación	251
	Documento de Identidad Electrónico	252
	Hacia un Intercambio de Datos Biométricos	252
	Las Infraestructuras de Firma Digital	253
	Normas de UNCITRAL	253
	Normas del MERCOSUR	254
IV.	Desafíos y Conclusiones	254
V.	Marco para la Identificación Electrónica Social Iberoamericana	256

I. Resumen Ejecutivo

El presente documento tiene por objetivo presentar el “MARCO PARA LA IDENTIFICACIÓN ELECTRÓNICA SOCIAL IBEROAMERICANA”, como un instrumento necesario para el efectivo ejercicio de los derechos de las personas en nuestra región. Responde a las recomendaciones efectuadas en la Declaración de Lisboa 2010. Su inicial presentación se produjo en la primera reunión del Grupo de Trabajo intergubernamental sobre Gobierno Electrónico que promovió la pasada Red Iberoamericana de Ministros de la Presidencia y Equivalentes, realizada en Lisboa, Portugal, los días 9 y 10 de septiembre de 2010. Esta primera reunión del Grupo de Trabajo Intergubernamental se efectuó el día 12 de abril del presente año, en Cartagena de Indias, Colombia.

Sin identificación no existen derechos. El ejercicio de los derechos requiere necesariamente la identificación plena de las personas, función que corresponde al Estado. El Estado es el responsable de la identificación de las personas, y de garantizar la identidad a cada uno. En un mundo cada vez más informatizado, los gobiernos utilizan las TIC's para la implementación de las políticas públicas sustantivas. Cómo lograr la plena identificación de las personas, cómo reconocer entre países dichas identificaciones, cómo facilitar el acceso remoto a los servicios que brinda la Administración, son

cuestiones que tienen que ver con una adecuada identificación electrónica de las personas. Esta identificación electrónica es necesaria para el acceso a sistemas informáticos, a las aplicaciones de gobierno electrónico, de comercio electrónico, pero también para la ejecución de políticas sociales. Además de este uso, los modernos documentos de identidad, básicamente los pasaportes y los documentos nacionales, están utilizando elementos de identificación electrónica, lo cual lleva a considerar que aún en los supuestos de identificación presencial, las tecnologías de la información y las comunicaciones cobran un rol relevante.

En consecuencia, resulta necesario contar con un marco conceptual en la región que se refiera a la identificación electrónica social, que pueda ser tomado como guía por nuestros países para la identificación de las personas y la autenticación electrónica, elemento básico para el pleno ejercicio de los derechos y la efectiva implementación de políticas públicas de inclusión social.

En la Sección II de esta presentación se indican los antecedentes sobre los que se apoya el Marco, básicamente las recomendaciones emanadas de las distintas reuniones de ministros realizadas en el año 2010 y la Carta Iberoamericana de Gobierno Electrónico aprobada en 2007.

En la Sección III se enumeran las consideraciones que motivan el presente Marco. Se exponen los principales conceptos jurídicos y tecnológicos involucrados en el tema de identificación de personas y autenticación electrónica.

En la Sección IV se presentan las conclusiones, mencionando los desafíos que nuestros países afrontan en materia de identificación de personas y posibles caminos a seguir.

Finalmente, se agrega el “Marco para la Identificación Electrónica Social Iberoamericana”, el que fuera considerado y discutido por los representantes de los Estados de la región.

II. Antecedentes

Durante el año 2010, se desarrolló una intensa agenda de reuniones de la Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Se realizaron reuniones ministeriales sectoriales que convocaron a los responsables de las áreas de Agricultura, Salud, Trabajo, Administración Pública y Reforma del Estado, Turismo, Educación, Infancia y Adolescencia, Justicia, Presidencia, Vivienda y Urbanismo. Dichas actividades concluyeron en la XX Cumbre Iberoamericana, que emitió la Declaración de Mar del Plata “Educación para la Inclusión Social”.

En todas las reuniones ministeriales sectoriales, de una u otra manera, se abordó el tema de la inclusión social como eje de las políticas públicas de la región. Especialmente, en la XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), celebrada en Lisboa, Portugal, se abordó el tema de la Participación de los Ciudadanos en la era del Gobierno electrónico. En dicho encuentro, los países acordaron que “los objetivos del gobierno electrónico deben trascender la mera eficacia y eficiencia de los procesos de administración, hacia formas que permitan cambios sociales, políticos, económicos en pro del desarrollo humano, la igualdad de oportunidades y la justicia social.”

Declaración de Lisboa

La XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), giró en torno a la Participación de los Ciudadanos en la era del Gobierno Electrónico: Educación para la Ciudadanía e Inclusión Digital. Los ministros acordaron reforzar la cooperación, información y coordinación en el área del Gobierno Electrónico en el espacio iberoamericano. Asimismo, se acordó la recogida de información sobre programas, acciones y buenas prácticas en el área de la simplificación, la modernización administrativa y la inclusión digital llevados a cabo en diversos países iberoamericanos, con el fin de desarrollar proyectos de cooperación de interés común.

Entre otras, la Declaración de Lisboa, contiene recomendaciones a los Gobiernos relativas a lograr “un modelo de Administración más abierto, transparente y colaborativo, que permita responder

eficazmente a los desafíos económicos, sociales, culturales y ambientales que se plantean a nivel mundial". Para ello, la Declaración contempla el uso de las TIC's para transformar la Administración. En ese sentido, los países signatarios consideran que "las políticas de administración electrónica y simplificación administrativa deben contribuir, de manera articulada, al desarrollo de servicios públicos con mayor calidad".

A tal fin, la Declaración de Lisboa reconoce que "el desarrollo de mecanismos de identificación y autenticación electrónica seguros, es otra de las condiciones para el cambio pretendido, destacándose su papel en la promoción de simplificación de procedimientos y en el fomento de la utilización de los servicios electrónicos." Finalmente, la Declaración de Lisboa reconoce que "los objetivos del gobierno electrónico deben trascender la mera eficacia y eficiencia de los procesos de administración, hacia formas que permitan cambios sociales, políticos, económicos en pro del desarrollo humano, la igualdad de oportunidades y la justicia social."

En consecuencia, los países signatarios de la Declaración de Lisboa acordaron:

- Impulsar programas que relacionen la administración electrónica con la simplificación administrativa, con el objetivo de hacer más simples, rápidas y eficaces las interacciones de los ciudadanos y de las empresas con la Administración, disminuyendo los costes de operación y tiempo, para el ejercicio de las actividades económicas y aumentando la eficiencia de la Administración Pública,
- Intercambiar experiencias entre la comunidad iberoamericana, en lo que concierne a la creación de servicios integrados únicos, físicos o virtuales, que se organicen en función de la demanda ciudadana y de las empresas,
- Intercambiar experiencias relativas a la implementación de formas de identificación electrónica y biométricas seguras y de mecanismos de articulación para el desarrollo de los servicios electrónicos transfronterizos, en el espacio iberoamericano,
- Articular el Intercambio de experiencias de utilización de las TIC's, para asegurar la transparencia de los procesos de decisión pública y para ofrecer nuevas formas de participación democrática,
- Promover políticas y prácticas de inclusión digital y otros mecanismos que faciliten el acceso a los servicios electrónicos, para que los ciudadanos puedan beneficiarse de las potencialidades de las TIC's, en condiciones de igualdad y universalidad, de forma de asegurar la cohesión social y territorial.

Conferencias Sectoriales de Ministros

En todas las reuniones ministeriales sectoriales, se abordó el tema de la inclusión social como eje de las políticas públicas de la región, y el uso de las tecnologías de la información y las comunicaciones para el pleno despliegue de las políticas públicas sustantivas.

En efecto, en la X Conferencia Iberoamericana de Ministros de Agricultura en Mar del Plata, realizada bajo el lema "Educación y Agricultura para el Desarrollo Inclusivo", se plantearon los objetivos de establecer acuerdos transversales para mejorar las condiciones de vida de los pobladores rurales, promover la agricultura familiar, garantizar su seguridad alimentaria, favorecer el acceso a los sistemas educativos y a un trabajo digno y remunerado.

Por su parte, la XII Conferencia Iberoamericana de Ministros y Altos Responsables de Infancia y Adolescencia celebrada en Buenos Aires, fijó su compromiso para la adopción de medidas legislativas, políticas y prácticas institucionales que faciliten la construcción de sistemas integrales de protección a la infancia y la adolescencia.

Asimismo, los Ministros acordaron la puesta en marcha de una plataforma virtual, alojada en la Web institucional de la SEGIB, que facilite el acceso y puesta a disposición de material y experiencias.

En la XII Conferencia Iberoamericana de Ministros de Salud, celebrada en Buenos Aires, se resolvió impulsar una agenda integrada de Salud y Educación para la inclusión social y se acordó la realización de acciones conjuntas para fomentar el impulso de la formación y la capacitación de recursos humanos.

En igual sentido, la XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, realizada en Buenos Aires, impulsó la promoción de la implantación de la Carta Iberoamericana de la Función Pública y de la Carta Iberoamericana de Calidad en la Gestión Pública. Los 18 países participantes además acordaron impulsar decididamente la Carta Iberoamericana de Gobierno Electrónico.

Debido al impacto que en la actualidad posee el empleo de las tecnologías de la información y la comunicación sobre el desarrollo de las sociedades, y a que su utilización por parte de los gobiernos puede significar un resultado positivo en la gestión pública, la Carta Iberoamericana de Gobierno Electrónico reconoce el derecho de los ciudadanos de relacionarse electrónicamente con las administraciones públicas para facilitar su participación y hacer que éstas sean más transparentes, eficaces y eficientes.

La Carta también promueve, con los mismos propósitos, la construcción de una sociedad de información y conocimiento, inclusiva, centrada en las personas y orientada al desarrollo, considerando el rol insustituible de los Estados para garantizar la universalización a toda la población y la continuidad de los servicios electrónicos y el fortalecimiento de la democracia. En consecuencia, los participantes del encuentro acordaron apoyar la adopción de los principios y orientaciones de la Carta Iberoamericana por parte de los Estados de la región, para lo cual decidieron desarrollar políticas y herramientas que faciliten la interoperabilidad de las comunicaciones y servicios, así como que promuevan el uso de software público en las administraciones públicas.

Por su parte, en el XIV Foro Iberoamericano de Ministros y Autoridades Máximas del Sector de Vivienda y Desarrollo Urbano, celebrado en Buenos Aires, los 15 países iberoamericanos participantes acordaron dar la máxima prioridad a que las acciones de vivienda en áreas urbanas formen parte de programas integrales que aseguren en su entorno equipamientos públicos, especialmente edificios educacionales.

De manera similar, la X Conferencia Iberoamericana de Ministros de Turismo, realizada en Córdoba, Argentina, bajo el lema “Turismo, Educación e Inclusión Social”, acordó continuar trabajando en la sensibilización y concientización acerca de la importancia del turismo como herramienta de reactivación económica y de estímulo de las economías nacionales y locales de Iberoamérica. Decidieron igualmente continuar los esfuerzos para la creación de la Red Iberoamericana de Formación en Turismo y se constituyó un grupo formado por Argentina, Brasil, Costa Rica, España y Paraguay, con objeto de elaborar un proyecto que viabilice la concreción de la mencionada Red.

También se resolvió impulsar el concepto de sostenibilidad en la educación, capacitación y práctica turística, a fin de favorecer la armonía del hombre con la naturaleza, alentando -a su vez- la promoción de las nuevas tecnologías y prácticas innovadoras que permitan elevar los actuales niveles de competitividad del sector.

Por otra parte, e inspirados en el eje de inclusión social presente en todas las reuniones sectoriales ministeriales, en la XIII Conferencia Iberoamericana de Cultura que se llevó a cabo en Buenos Aires, los ministros analizaron la constitución de un Mercado Común Iberoamericano de la Música, la creación del Fondo Iberoamericano de Cooperación para la Música y la conformación de un Portal de Músicas Iberoamericanas. Los países participantes trataron también la Carta Cultural Iberoamericana, el proyecto Cumbres, un programa de educación artística y cultural para la región, y la cultura como

herramienta de inclusión social.

En materia educativa, la XX Conferencia Iberoamericana de Educación, reunida en Buenos Aires, giró en torno al Proyecto Metas Educativas 2021: la educación que queremos para la generación de los bicentenarios. En la Declaración de Buenos Aires, los ministros de Educación coincidieron en que “nuestro compromiso a favor de la educación y la inclusión, así como hacia las políticas públicas en esta materia, requiere el apoyo del conjunto de nuestras sociedades para hacer posible su universalización en condiciones de calidad y equidad”.

Destacaron que “el programa Metas Educativas 2021: la educación que queremos para la generación de los bicentenarios, ..., contribuirá estratégicamente a hacer frente a los retos pendientes del siglo XX, sobre todo en el campo de la alfabetización y educación básica de jóvenes y de adultos, del acceso a la educación y de la calidad de la enseñanza, y a los desafíos del siglo XXI, especialmente en lo referido a la innovación, al desarrollo científico y tecnológico y a la incorporación a la sociedad de la información y del conocimiento”.

Finalmente, la Declaración contempla solicitar a la SEGIB y a la OEI, que en el marco de los objetivos de las Metas 2021, y de manera específica de la meta general quinta, continúen elaborando un programa de cooperación iberoamericana en la introducción de las TIC's en el sistema educativo, con el objetivo de difundir las distintas experiencias nacionales, evaluar las diferentes metodologías educativas, promover la cooperación horizontal entre los países iberoamericanos y apoyar la formación de los educadores en el uso de las TIC's.

En similar sentido, en el II Foro Iberoamericano de Ministros de Trabajo, realizado en Buenos Aires, Argentina bajo el lema “Trabajo decente y Educación para la Inclusión Social”, se trattaron los siguientes temas: el desarrollo con trabajo decente e inclusión social (el rol de la educación y la formación profesional); los modelos productivos; innovación y tecnología (educación y aprendizaje a lo largo de la vida); los actores del mundo del trabajo frente al trabajo decente; la educación para la inclusión social; la cooperación iberoamericana y las redes (avances en la construcción de la Red Iberoamericana de Inspección del Trabajo).

En el encuentro, los ministros analizaron los desafíos de la crisis y la necesidad de poner en marcha políticas innovadoras para la inclusión social. Por otra parte, se debatió la necesidad de políticas que permitan articular los varios modelos productivos y la innovación y la tecnología como desafíos para la educación y el aprendizaje a lo largo de la vida. Finalmente, se trató la cuestión de los actores del mundo del trabajo frente a la educación, la cooperación iberoamericana y la visión estratégica en la construcción del espacio regional.

En cuanto a la XVII Conferencia de Ministros de Justicia de Iberoamérica, realizada en la Ciudad de México, se aprobó el texto del Convenio Iberoamericano sobre el uso de la Videoconferencia en la cooperación jurídica entre sistemas de justicia, así como el Programa Iberoamericano de Acceso a la Justicia. Los Ministros aprobaron una serie de Recomendaciones relativas a la lucha contra el crimen organizado, la promoción de los derechos humanos de los grupos vulnerables y la modernización de los procesos. En la reunión se fijaron como ejes centrales del trabajo de la COMIIB para el próximo bienio: el acceso a la justicia, las reformas en el sistema penitenciario, la modernización de la justicia y la lucha contra el crimen organizado. Asimismo se apoyó la puesta en marcha del Portal Iberoamericano de Justicia Electrónica, así como el desarrollo del Observatorio de Justicia Iberoamericano y de la tarea desarrollada por IberRed.

Declaración de Mar Del Plata

En la XX Cumbre Iberoamericana, bajo el tema “Educación para la Inclusión Social”, los Jefes y Jefas de Estado y de Gobierno reiteraron el objetivo común de avanzar en la construcción de sociedades justas, democráticas, participativas y solidarias en el marco de la cooperación e integración cultural,

histórica y educativa iberoamericanas, lograr una educación con inclusión social intra e intercultural en la región iberoamericana de calidad para todos y todas, para promover una Iberoamérica más justa, con desarrollo económico, social y cultural en el marco de sociedades democráticas, solidarias y participativas que promuevan el bienestar de todos los habitantes de nuestra región.

Asimismo, el documento enfatiza el rol de los gobiernos, que “deben facilitar el acceso y la comprensión de las leyes a los ciudadanos y caminar hacia un modelo de Administración más abierto, transparente y colaborativo, que permita responder eficazmente a los desafíos económicos, sociales, culturales y ambientales que se plantean a nivel mundial.”

Entre otros, la Declaración de Mar del Plata refleja el compromiso de los países de la región para lograr los objetivos siguientes:

- Incorporar en los sistemas educativos el principio de la inclusión de tal manera que ninguna persona deje de tener una oferta educativa pertinente y oportuna a sus necesidades, expectativas, intereses e identidad, ya sea bajo la modalidad de educación formal o de educación no formal e informal. (Objetivo 7)
- Alcanzar plena alfabetización en todos los países de la región antes de 2015. (Objetivo 11)
- Promover el acceso universal de las y los alumnos y docentes, a las tecnologías de la información y de la comunicación y a una educación informática de calidad teniendo en cuenta su papel fundamental en la educación, la cultura, la salud, la inclusión social, el crecimiento económico y el desarrollo sostenible. (Objetivo 23)
- Fomentar la investigación y el desarrollo de estrategias innovadoras para la incorporación de las tecnologías de la información en el proceso de enseñanza-aprendizaje y en la formación docente inicial y continua a través del desarrollo de contenidos de programas de alfabetización digital y tecnológica. (Objetivo 24)
- Alentar el intercambio de experiencias y fortalecer la cooperación iberoamericana en ciencia, tecnología e innovación y de formación de recursos humanos calificados, desarrollando acciones nacionales e internacionales para promover la inclusión social y el desarrollo sostenible. (Objetivo 25).

Carta Iberoamericana de Gobierno Electrónico

Los Ministros de Administración Pública y de la Reforma del Estado y los Jefes de Delegación de los Gobiernos Iberoamericanos, reunidos los días 31 de mayo y 1º de junio de 2007, en Pucón, Chile, en ocasión de la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, reconocieron la brecha digital existente entre países desarrollados y en desarrollo, y expresaron su compromiso a reducir la brecha digital y convertir la Sociedad de la información y el Conocimiento en una oportunidad para todos, especialmente mediante la inclusión de los más rezagados.

Desde esta perspectiva, las autoridades iberoamericanas abordaron el empleo de las nuevas tecnologías por los gobiernos y las administraciones públicas, emitiendo una Carta Iberoamericana de Gobierno Electrónico como herramienta para la mejora de la gestión pública. En dicho documento, expresaron “Estamos firmemente comprometidos a reducir la brecha digital y convertir la Sociedad de la información y el Conocimiento en una oportunidad para todos, especialmente mediante la inclusión de aquellos que corren peligro de quedar rezagados.”

La Carta subraya que la perspectiva desde la que se tiene que abordar el empleo de las TIC's en la gestión pública es la del ciudadano y sus derechos, considerando como “ciudadano” a “cualquier persona natural o jurídica que tenga que relacionarse con una Administración Pública y se encuentre en territorio del país o posea el derecho a hacerlo aunque esté fuera de dicho país.”

La Carta Iberoamericana de Gobierno Electrónico enfatiza el rol central de la persona, no de la tecnología. En tal sentido, la Carta impulsa el reconocimiento del derecho del ciudadano a relacionarse

electrónicamente con la Administración Pública. Este reconocimiento, implica abrirle múltiples posibilidades de acceder más fácilmente a las Administraciones Públicas, con los consecuentes beneficios:

- Conocer qué están haciendo las Administraciones.
- Sentar las bases que permiten un gobierno más abierto.
- Superar las barreras físicas y de espacio, que por estar situados en lugares remotos o por otras cuestiones muchas veces dificultan el acceso de las personas a sus administraciones.
- Promover la inclusión y la igualdad de oportunidades de forma que todos los ciudadanos puedan acceder, cualquiera que sea su situación territorial o social, a los beneficios que procura la sociedad del conocimiento.
- Participar activamente de la cosa pública.

La Carta de Pucón se propone dos objetivos: un objetivo final y directo que es reconocer a los ciudadanos un derecho que les facilite su participación en la gestión pública y sus relaciones con la Administración. Este derecho, a su vez, será un elemento coadyuvante para incrementar la transparencia de la Administración, garantizar el respeto al principio de igualdad, y generar una gestión más eficaz y eficiente.

Por otra parte, la Carta persigue un objetivo estratégico indirecto: promover la construcción de una sociedad de información y conocimiento, inclusiva, centrada en las personas y orientada al desarrollo. En tal sentido, y en lo que constituye un paso extraordinario en cuando al reconocimiento de los derechos sociales, la Carta Iberoamericana de Gobierno Electrónico señala expresamente como objetivo “Definir los contenidos del derecho de los ciudadanos a relacionarse de forma electrónica con sus Gobiernos y Administraciones Públicas.” (inciso b) del artículo 1º)

En ese sentido, la Carta Iberoamericana de Gobierno Electrónico destaca “el rol insustituible que le corresponde a los Estados en estas materias, para garantizar la universalización a toda la población y la continuidad de los servicios electrónicos y el fortalecimiento de la democracia.”

Define el concepto de “gobierno electrónico” como sinónimo de “administración electrónica”, entendiendo por tal al “uso de las TIC’s en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustancialmente la transparencia del sector público y la participación de los ciudadanos.” Como parte de los instrumentos del gobierno electrónico, la Carta contempla el tema de la identificación de las personas. En tal sentido, destaca la obligación de los gobiernos de contar con instrumentos esenciales que posibiliten a los ciudadanos (en sentido amplio) el acceso electrónico a la administración. Dentro de estas herramientas, considera como un factor fundamental “la identificación de los ciudadanos, Administraciones Públicas, funcionarios y agentes de éstas que empleen medios electrónicos, así como la autenticidad de los documentos electrónicos en que se contiene la voluntad o manifestaciones de todos ellos.”

Asimismo, el tema de la identificación electrónica es abordado en relación al principio de seguridad del gobierno electrónico. En efecto, la Carta recomienda a los Estados a emitir las normas jurídicas y técnicas que aseguren a los ciudadanos y a las Administraciones Públicas las condiciones necesarias para que “en sus relaciones electrónicas puedan tener seguridad y confianza, tanto en lo que se refiere a la identidad de la persona, órgano o institución que se comunica, como en lo que se refiere a la autenticidad e integridad del contenido de la comunicación, así como, consecuentemente, en la imposibilidad de ser repudiada por el emisor.”

A continuación, la Carta define el concepto de autenticidad e integridad de la comunicación, como aquel en el cual ésta se corresponde con la originalmente emitida sin que sus contenidos hayan sido alterados. Recomienda en tal sentido a los Estados, que contemplen en la regulación sobre seguridad del Gobierno Electrónico los “sistemas físicos, sistemas de firma electrónica, incluso avanzada, así

como otros sistemas alternativos a la firma electrónica, cuanto la naturaleza del trámite lo aconseje, que permitan identificar al comunicante y asegurar la autenticidad del contenido de la comunicación.” Como se advierte, para la Carta Iberoamericana de Gobierno Electrónico, la identificación de las personas es un elemento central para la implementación de políticas de gobierno electrónico, tanto como un instrumento esencial básico para la ejecución de políticas públicas, como en su rol vinculado con la identificación en entornos electrónicos. En ese sentido, cobra especial relevancia el tema de la firma digital como instrumento que permite, por una parte, identificar la autoría de documentos electrónicos, y simultáneamente, confirmar la integridad de dichos documentos digitales.

III. Elementos de la Identificación Electrónica

Esta sección aborda los aspectos que explican el porqué la identificación electrónica es un elemento clave para la implementación de políticas públicas de inclusión social. Asimismo, contiene una sintética descripción de las tecnologías involucradas.

Importancia de la Identificación Electrónica para el Pleno Ejercicio de los Derechos

Nuestros países avanzan cada día en reconocer explícitamente derechos sociales a sus habitantes. La búsqueda de la inclusión social implica no solamente el reconocimiento de estos derechos, sino brindar las condiciones necesarias para garantizar su efectivo ejercicio.

Desde una perspectiva jurídica, la identidad de la persona es la base sobre la que se construye el andamiaje de derechos y obligaciones. Si bien los derechos están establecidos erga omnes, vale decir, para todos en general, la apropiación de una situación particular amparada por el marco normativo con sus respectivos derechos y obligaciones, surge a partir de la identidad específica de cada persona. En otro sentido, el concepto de identidad de la persona hace referencia a la comprobación de los datos que acreditan que un individuo es efectivamente la persona que dice ser, sujeto de derecho, con determinados atributos. Esta comprobación de los datos que acreditan la identidad es conocida por “identificación”, es decir, el procedimiento que mediante elementos externos, permite asignar una identidad con determinados atributos a una persona concreta.

En una relación entre dos personas o más, con efectos jurídicos, es necesario acreditar la identidad de las partes que intervienen en ella. Un contrato, una demanda, un matrimonio, una adquisición, una venta, en fin, cada operación con efectos jurídicos requiere la identificación de las personas que participan de ella como paso previo a su celebración. En la administración pública, ocurre algo similar. Los trámites que se realizan ante la Administración requieren la identificación de la persona que lo inicia y de los funcionarios que intervienen. Una compra requiere la identificación de los que participan del acto licitatorio, la notificación de un acto administrativo se hace a una persona determinada y es hecha por un funcionario competente para ello, en fin, cada actividad de la Administración involucra alguien que la realiza, y ese alguien debe poder ser identificado.

La implementación de políticas públicas de alcance social requiere también la identificación de sus beneficiarios. Las políticas educativas, las de salud, las de inclusión digital, todas se apoyan en una correcta identificación de las personas que son beneficiarias. Para acceder a estas políticas sociales, las personas deben identificarse ante los órganos administrativos, mediante algún documento, a fin de acceder a los beneficios y ejercer plenamente sus derechos. En consecuencia, si alguien no cuenta con un documento que lo identifique, no puede acceder a sus derechos, no puede reclamar por ellos, en una palabra, no existe para el Estado.

La identificación de las personas es un elemento esencial de los actos jurídicos, ya que el error sobre la identidad de la persona, acarrea la nulidad del acto, al constituir un vicio del consentimiento que invalida la relación jurídica.

La identidad y la identificación de las personas, son materia del derecho sustantivo y del derecho

procesal. La identificación hace referencia tanto a los datos de identidad de una persona (nombre, apellidos, naturaleza, edad, sexo, domicilio y nacionalidad), como al acto y procedimiento de comprobación y acreditación de la identidad. La identificación de la persona supone su individualización dentro del colectivo social. El nombre es uno de los criterios principales de identificación, al referirse a la filiación de la persona. Lo identifican otros datos, como se verá más adelante, que son los datos objeto de la biometría. Rasgos personales, únicos, que sirven para identificar indubitablemente a la persona.

Ahora bien, es el derecho el que define qué instrumentos y procedimientos serán considerados válidos para la identificación de una persona. Es el Estado el encargado de identificar a las personas, a partir de distintos procedimientos según la legislación del país de que se trate. En Argentina, la identificación de las personas está regulada por la Ley Nro. 17.671 (Ley de Identificación, Registro y Clasificación del Potencial Humano Nacional), y se realiza mediante un Documento Nacional de Identidad. Además, están los documentos de identificación transfronteriza, los pasaportes. No todos los países cuentan con normas que establecen documentos únicos de identificación. Sí en cambio, existen estándares para los pasaportes, debido a la necesidad de ser reconocidos más allá de las fronteras del país emisor. Una persona que no ha sido identificada por el Estado, es una persona “inexistente”. Es una persona que no posee acta de nacimiento, ni, consecuentemente, documento que acredite su identidad. Es presa fácil para la trata de personas, apropiación de menores, pornografía y abuso infantil, tráfico de órganos, entre otros delitos. Una de las funciones básicas del Estado es garantizar la identificación de las personas. Una persona sin acta de nacimiento, no puede ejercer sus derechos. No accede a los servicios de salud, ni a la educación, no puede recibir planes sociales, no puede insertarse en el mercado de trabajo: en una palabra, no existe para el derecho. La falta de inscripción es una de las causas de exclusión social, porque un niño sin inscripción, es un niño sin nombre, sin rostro y sin identidad.

Elementos que Permiten la Identificación

Históricamente, el proceso de identificación de una persona se basó en la comparación de un rasgo con un dato, pero a medida que las aplicaciones fueron creciendo se hizo necesario contar con mecanismos no personales de reconocimiento. Por ejemplo, hasta no hace mucho tiempo, en Argentina el Documento Nacional de Identidad era otorgado después de que un perito dactiloscópico cotejara la huella tomada al solicitante contra la huella dactilar que obraba en la primera ficha. Este proceso llevaba su tiempo. Hoy, en el nuevo esquema de trabajo que puso en marcha el Ministerio del Interior de Argentina, el cotejo está automatizado, acelerando el tiempo de entrega del nuevo Documento Nacional de Identidad.

Con el avance de la tecnología, el proceso de autenticación e identificación se fue apoyando en nuevas herramientas. Hoy pagar con una tarjeta de crédito en un comercio requiere de la tarjeta, del Documento de Identidad y del rostro de la persona, el cual será cotejado por el comerciante. Sin embargo, al no haber un proceso de verificación de la identidad que esté automatizado y que se apoye en la tecnología, puede ocurrir que alguien que ha hurtado mi tarjeta y mi Documento de Identidad, cambie la foto, usurpe mi identidad y salga alegramente a comprar.

Las tecnologías biométricas fueron utilizadas en sus orígenes con fines legales, básicamente, de investigación criminal. Pero el avance de las TIC's en todos los órdenes ha ampliado su utilización con otros fines. La biometría aporta aquellas técnicas de identificación basadas en las características físicas de un individuo: el ADN, las huellas digitales, los rasgos faciales o las características del iris. En suma, lo que hace a una persona única.

Los gobiernos se apoyan en la biometría para identificar a las personas, autenticar su identidad en sistemas informáticos, reforzar la seguridad pública en aeropuertos y ciudades, y restringir el acceso a sitios seguros, tanto físicos (edificios) como virtuales (sistemas y aplicaciones informáticas).

Los sistemas de reconocimiento que utilizan tecnologías biométricas reconocen a una persona con base en características físicas (huellas dactilares, rasgos de la mano o de la cara, patrones del iris) o características conductuales aprendidas o adquiridas (patrones de voz, patrones de firma ológrafo, patrones de tipo).

El uso de tecnologías biométricas para la identificación de personas se apoya en el uso de dispositivos que contienen sus datos y de lectores de éstos. Los dispositivos pueden ser tarjetas inteligentes, que almacenan los datos biométricos en un Chip de Circuito Integrado (ICC), protegido a su vez por tecnologías de clave pública (utilizadas por la autoridad que emite el dispositivo de identificación personal para firmar el ICC) y por tecnologías de clave simétrica (un PIN – Personal Identification Number), para aquellas aplicaciones que así lo requieran, como por ejemplo, el acceso a sistemas informáticos o a centros de cómputos.

Este dispositivo es un artefacto físico (por ejemplo, una tarjeta de identidad, una tarjeta inteligente) emitida por la autoridad competente para ello a un individuo, y que contiene datos almacenados que prueban su identidad (por ejemplo, fotografía, huella dactilar, etc.) de modo tal que la identidad del portador pueda ser verificada contra los datos almacenados por otra persona (es decir, que sean accesibles a la lectura humana) o por un sistema automatizado (o sea, que pueda ser accedido y verificado electrónicamente).

Los factores de autenticación que se utilizan actualmente son tres, que se basan en:

1. *Algo que sé*: la persona se autentica mediante algo que sabe: una clave, un número que la identifica – PIN, una frase o una respuesta a una pregunta de seguridad.
2. *Algo que tengo*: la persona se autentica utilizando algo que posee: un token, una tarjeta inteligente, un certificado digital.
3. *Algo que soy*: el individuo se autentica con base en una característica que tiene su persona, esto es, un dato biométrico.

Los factores basados en conocimiento y en posesión requieren que la persona que se va a autenticar ante un sistema recuerde o lleve consigo el dispositivo. En cambio, cuando se aplican tecnologías biométricas, el dato lo lleva consigo, y resulta casi imposible que se lo falsee, o sea, que sea utilizado por otra persona para suplantar su identidad. Se dice que en los dos primeros factores, el vínculo entre el dato y su verificación es débil, lo cual facilita la usurpación de identidad, ya que el sistema no puede distinguir entre el legítimo poseedor del dispositivo y alguien que lo haya sustraído, lo mismo se aplica a la clave.

La principal función de la biometría aplicada se refiere a la identificación de personas, tanto en el entorno real como virtual.

Documento de Identidad Electrónico

La identificación de las personas que habitan en su territorio es una de las funciones básicas del Estado en algunos países, la cual en general es responsabilidad de los Registros Civiles. En la región, los gobiernos han encarado procesos de modernización de sus administraciones, los cuales consideran la posibilidad de incorporar TIC's para cumplir con dicha función de identificación.

Pero además de cumplir con esta función de identificación de personas, el uso de la biometría en los documentos nacionales electrónicos, conlleva el despliegue de otras funcionalidades adicionales. En ese contexto, el uso de la biometría con este fin permitiría contar con bases de datos interoperable sobre los datos de identificación de las personas. Disponer de esta información facilitaría el cumplimiento de otras funciones del Estado, tales como educación, seguridad social, asistencia social, y en general, toda otra política pública que requiera para su instrumentación la identificación de las personas beneficiarias.

Hacia un Intercambio de Datos Biométricos

Los gobiernos necesitan disponer de mecanismos de identificación seguros para poder implementar políticas públicas. La identificación permite a las personas acceder a planes sociales, beneficios de seguridad social, anotar a los hijos en los colegios, ser atendido en hospitales, ejercer sus derechos electorales, etc. El Estado debe garantizar el pleno ejercicio de los derechos sociales, electorales, civiles de las personas, el tránsito fronterizo. Para todas estas políticas públicas, el dato biométrico asociado a los datos biográficos constituye una de las claves de éxito. Disponer de una base de datos biométricos asociados con datos biográficos permite y facilita la implementación de las principales políticas públicas.

Desde el punto de vista del usuario, es simplemente garantizar su identidad. Desde la perspectiva de los gobiernos, es contar con una herramienta esencial para facilitar la ejecución de las políticas públicas relevantes. No alcanza con disponer de los datos biométricos que responden a diferentes estándares, alojados en distintas bases de datos administradas por diferentes organismos, sino de cooperar y compartir la información para un uso racional, apoyado por las TIC's, de fácil acceso para no expertos y acorde con los tiempos que corren.

Se trata entonces de establecer mecanismos de colaboración que permitan contar con rápida información a partir de la integración de los datos biográficos y los datos biométricos de una persona en un formato digitalizado, susceptible de ser utilizada en tiempo real por distintos organismos del Estado. En la actualidad, en general la única información que se tiene almacenada en formato digital son los datos biográficos de una persona: nombre y apellido, sexo, fecha de nacimiento, etc.

En cambio los datos biométricos (las huellas dactilares) históricamente se han conservado en fichero de papel. No se utilizan en un sistema automático de verificación de identidad. Al no contar con esas herramientas, estamos ante el riesgo de que una persona física pueda tener más de una identidad porque no hay forma de hacer lo que se denominan controles 'uno a n', es decir contra el total.

Además de los usos en el sistema crediticio, de salud y prestaciones sociales, un empleo evidente del sistema sería en las elecciones. Contando con esto, es natural la creación de padrones electorales con patrones biométricos que verifiquen la identidad del elector previa a la emisión del voto y totalmente disociada del acto del sufragio. De este modo habría garantías de que nadie podría ir a votar en nombre de otro.

Las Infraestructuras de Firma Digital

Los países de la región han avanzado en el reconocimiento legal del documento y la firma electrónica.¹ En algunos países, las legislaciones han contemplado esquemas de firma digital, es decir, de sistemas de autenticación electrónica basados en tecnologías de clave pública. Esto significa la existencia de Infraestructuras de Firma Digital, de alcance nacional. Sin embargo, en un escenario en el cual las transacciones comerciales y de gobierno son transfronterizas, esta legislación no cubre dichos intercambios, existiendo un vacío legal.

Normas de UNCITRAL

Resulta necesario entonces, promover el establecimiento de acuerdos entre los países de la región que, tomando en consideración sus propias normas nacionales, establezcan las bases para el reconocimiento mutuo de firmas digitales.

En ese sentido, existen antecedentes como la Convención sobre Comunicaciones Electrónicas en

¹ Ver la Ley Argentina sobre Firma Digital N° 25.506; la Ley de la República Dominicana sobre Comercio Electrónico, Documentos Electrónicos y Firmas Digitales N° 126-02; la Ley Peruana sobre Firma Digital N° 27269; la Medida Provisoria de Brasil N° 2200-2; la Ley de Chile sobre Firmas Electrónicas N° 19979; la Ley Colombiana sobre Comercio Electrónico y Firmas Digitales N° 527-1999; la Ley de Ecuador sobre Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; la Ley Venezolana de Mensajes de Datos y Firmas Electrónicas; México, Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de protección al consumidor (2000); Panamá, Ley de firma digital (2001); y Uruguay, la Ley N° 18.600 (2009) sobre Documento Electrónico y de Firma Electrónica.

Contratos Internacionales de UNCITRAL. Desde que surgió la Ley Modelo de Comercio Electrónico en 1996, los países han ido adoptando leyes sobre la materia. Sin embargo, dichas leyes tienen un alcance limitado, pues se aplican a las transacciones internas de cada país, quedando sin regular una amplia gama de operaciones transfronterizas, que se realizan a través de Internet.

Para superar este problema, UNCITRAL elaboró la Convención sobre Comunicaciones Electrónicas Internacionales que actualmente ha sido firmado por 18 naciones entre las que se encuentran China, Rusia y Corea, y de la Región, Paraguay, Colombia, Honduras y Panamá.

Dicha Convención, adoptada por la Asamblea General el 23 de noviembre de 2005, tiene por objeto fomentar la seguridad jurídica y la previsibilidad comercial cuando se utilicen comunicaciones electrónicas en la negociación de contratos internacionales. Regula la determinación de la ubicación de la parte en un entorno electrónico; el momento y lugar de envío y de recepción de las comunicaciones electrónicas; la utilización de sistemas de mensajes automatizados para la formación de contratos; y los criterios a que debe recurrirse para establecer la equivalencia funcional entre las comunicaciones electrónicas y los documentos sobre papel, incluidos los documentos sobre papel "originales", así como entre los métodos de autenticación electrónica y las firmas manuscritas.

La Convención de UNCITRAL se apoya en el principio de neutralidad tecnológica, admitiendo todo método de autenticación que permita por una parte, establecer la identidad de la persona y por la otra, establecer la manifestación de la voluntad de esa persona. Admite asimismo, los acuerdos de parte, los antecedentes, la proporcionalidad entre medios y fines, la prueba posterior inclusiva. Considera a tales métodos como el equivalente funcional de la firma que solicitan las leyes tradicionales.

Normas del MERCOSUR

En el ámbito del MERCOSUR, con su conformación original de cuatro miembros (Argentina, Brasil, Paraguay y Uruguay), se comenzó a tratar el tema de firma digital en el Subgrupo de Trabajo N° 13 de Comercio Electrónico, en cuyo marco se aprobaron dos resoluciones relativas a la firma digital.

Resoluciones sobre Comercio Electrónico

En 2006, el Subgrupo de Trabajo N° 13 de Comercio Electrónico del MERCOSUR, aprobó dos Resoluciones sobre Firma Digital. La primera de ellas, la Resolución N° 34/06, establece las Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR.² La segunda, la Resolución Nro. 37/06, contempla la eficacia jurídica del documento electrónico, de la firma electrónica y de la firma electrónica avanzada en el ámbito del MERCOSUR.³

Ninguna de estas Resoluciones tiene efecto práctico, por cuanto la primera, si bien no requiere la incorporación al derecho interno, no establece un acuerdo de reconocimiento en sí mismo sino que fija pautas a tal fin. La segunda, requiere su incorporación al derecho interno para tener eficacia jurídica, con lo cual, representa solamente una declaración general sin efectos jurídicos.

IV. Desafíos y Conclusiones

Actualmente los países de la región han encarado proyectos de inclusión digital que permitirán en breve superar la brecha existente. Proyectos educativos apoyados en computadoras para estudiantes, facilidades para el acceso a la banda ancha, políticas de accesibilidad, impacto de las redes sociales, presentes en las agendas digitales de nuestros países, nos muestran una realidad: más gente conectada, más servicios en Internet, más necesidad de garantizar la identificación de las personas en los medios electrónicos.

² Disponible en http://www.mercosur.int/msweb/Normas/normas_web/Resoluciones/ES/RES034-2006.pdf

³ Disponible en http://www.mercosur.int/msweb/Normas/normas_web/Resoluciones/ES/GMC_2006_RES-037_ES_EficaciaFirmaDigital.pdf

Para cumplir las recomendaciones de la Declaración de Lisboa, tendientes a lograr “*un modelo de Administración más abierto, transparente y colaborativo, que permita responder eficazmente a los desafíos económicos, sociales, culturales y ambientales que se plantean a nivel mundial*”, los países signatarios reconocen que “el desarrollo de mecanismos de identificación y autenticación electrónica seguros, es otra de las condiciones para el cambio pretendido, destacándose su papel en la promoción de simplificación de procedimientos y en el fomento de la utilización de los servicios electrónicos.” En tal sentido, en el presente documento se ha presentado un panorama de las cuestiones involucradas en los procesos de identificación electrónica, y su relevancia para el pleno ejercicio de los derechos de las personas. Se abordaron sencillamente las tecnologías biométricas involucradas, especialmente las relativas al documento de identidad electrónico.

Las dificultades para su implementación no están vinculadas con la tecnología, que ya existe con un suficiente grado de madurez. Tampoco con la existencia de estándares internacionales, que han sido desarrollados y aceptados. Como todo proyecto que implica implantar Tecnologías de la Información y las Comunicaciones en la gestión administrativa del Estado, los proyectos orientados a construir una base de datos biométricos o a reemplazar los documentos de identidad actuales por otros electrónicos, enfrentan los mismos factores de riesgo que cualquier otro proyecto tecnológico transversal.

El desafío que nuestros países enfrentan a la hora de implementar proyectos tecnológicos en el sector público que permitan desarrollar el Gobierno Electrónico⁴, no se relaciona tanto con la escasez de recursos, ni con una infraestructura insuficiente ni tampoco con la carencia de profesionales, sino más bien con la falta de coordinación entre las organizaciones públicas. En efecto, los esfuerzos que realizan los gobiernos muchas veces no obtienen los resultados esperados no por falta de recursos sino porque los distintos organismos realizan proyectos en forma descoordinada, lo cual genera comportamientos estancos.

Es claro que el logro de resultados en la implementación de proyectos tecnológicos en la gestión pública requiere una planificación adecuada y un monitoreo y evaluación que acompañe su desarrollo. Pero esto no alcanza para garantizar el éxito del proyecto, sobre todo en aquellos que involucran a varios organismos, o sea, que son transversales en la Administración. Un elemento crucial es el rol de los decisores políticos, especialmente de aquellos que intervienen en los procesos de definición de las políticas públicas vinculadas al uso de las tecnologías en la Administración o a la modernización del Estado.

El factor “liderazgo” es el factor de éxito más importante en el diseño e implementación de estrategias electrónicas. Sin un decidido liderazgo no se podrán superar las resistencias al cambio que naturalmente implica la modificación de las formas de trabajo derivadas de la incorporación de TIC’s en la gestión pública.

En tal sentido, proponemos este documento sobre Identificación Electrónica Social Iberoamericana, que contenga el marco general, lineamientos básicos a seguir por nuestros países para implementar sistemas de autenticación e identificación de personas ágiles y efectivos, como un insumo de base para la implementación de políticas públicas de inclusión social, y que garantice el derecho a la identidad de cada habitante de nuestra región.

Con base en la justificación anterior, se adjunta el **Marco para la Identificación Electrónica Social Iberoamericana**, considerado por los Estados de la región en Asunción, Paraguay.

⁴ Este documento adopta la definición de “gobierno electrónico”, como sinónimo de “administración electrónica”, contenida en la Carta Iberoamericana de Gobierno Electrónico, 2007. La Carta de Pucón entiende por tal al “uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos.”

V. Marco para la Identificación Electrónica Social Iberoamericana

Preámbulo

Los países de la región han avanzado en el establecimiento de políticas públicas de inclusión social que requieren el uso de tecnologías de la información y de las comunicaciones (TIC's) para su implementación.

La IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado reunida en Pucón, Chile, aprobó el 1º de junio de 2007 la Carta Iberoamericana de Gobierno Electrónico que establece un conjunto de conceptos, valores y orientaciones de utilidad para su diseño, implantación, desarrollo y consolidación como herramienta coadyuvante de la mejora de la gestión pública iberoamericana, mientras que en muchas legislaciones nacionales vigentes se reconoce el valor legal de los documentos electrónicos, las firmas electrónicas y las firmas digitales.

La identificación de las personas constituye un requisito esencial para el pleno ejercicio de sus derechos. Como una obligación ineludible de los Estados iberoamericanos, se tiene que garantizar la correcta identificación de las personas, así como salvaguardar y proteger el derecho a la identidad de cada uno de los habitantes de su suelo.

La XIII Reunión de la Red Iberoamericana de Ministros de La Presidencia y Equivalentes (RIMPE), celebrada en Lisboa, Portugal, giró en torno a la Participación de los Ciudadanos en la era del Gobierno Electrónico: Educación para la Ciudadanía e Inclusión Digital y, en la Declaración de Lisboa, se reconoce que “los objetivos del gobierno electrónico deben trascender la mera eficacia y eficiencia de los procesos de administración, hacia formas que permitan cambios sociales, políticos, económicos en pro del desarrollo humano, la igualdad de oportunidades y la justicia social.”

También la Declaración de Lisboa reconoce que “el desarrollo de mecanismos de identificación y autenticación electrónica seguros, es otra de las condiciones para el cambio pretendido, destacándose su papel en la promoción de simplificación de procedimientos y en el fomento de la utilización de los servicios electrónicos.”

En consecuencia, el presente Marco tiene el propósito de establecer un conjunto de conceptos, fundamentos, principios y orientaciones de utilidad para el diseño, implantación y desarrollo de una Identificación Electrónica Social Iberoamericana que consolide en la región el reconocimiento, ejercicio y goce efectivo de los derechos sociales de los ciudadanos iberoamericanos.

Capítulo primero. Finalidad y ámbito de la Identificación Electrónica Social Iberoamericana

- Objetivos 1 El presente Marco para la Identificación Electrónica Social Iberoamericana tiene los objetivos siguientes:
- a. Brindar un marco conceptual y los componentes que participan de los procesos de identificación de las personas que, involucrando elementos tecnológicos, facilitan el desarrollo del Gobierno Electrónico y la implementación de políticas públicas de inclusión social en Iberoamérica.
 - b. Promover el uso de documentos electrónicos de identificación en los países de la región, incluyendo pasaportes electrónicos y documentos nacionales de identidad.
 - c. Proveer recomendaciones técnicas a las administraciones públicas para los procesos de autenticación electrónica, cubriendo autenticación remota

		de usuarios sobre redes abiertas.
		d. Conformar un marco genérico de principios rectores, políticas y procedimientos de gestión, que siente las bases para el establecimiento de un futuro esquema de reconocimiento mutuo de dispositivos de identificación electrónica social en los países de la comunidad iberoamericana.
		e. Servir como orientación para el diseño, regulación, implantación, desarrollo, mejora y consolidación de modelos nacionales de identificación electrónica de personas por parte de las administraciones públicas de la región.
Finalidades	2	<p>Los objetivos previstos en el apartado anterior se orientan a múltiples fines:</p> <ul style="list-style-type: none"> a. Promover la participación ciudadana en la gestión pública, mediante la implementación de servicios electrónicos de calidad y de pautas para la interacción entre los habitantes y las administraciones públicas por medios electrónicos. b. Propender al reconocimiento del derecho a relacionarse electrónicamente con la Administración propugnado en la Carta Iberoamericana de Gobierno Electrónico. c. Facilitar la comunicación y relación de las personas con las administraciones públicas por medios electrónicos. d. Establecer un marco de reconocimiento transfronterizo de dispositivos de identificación y autenticación electrónica. e. Promover el uso y reconocimiento mutuo de documentos de identidad electrónicos. f. Garantizar la protección del derecho a la identidad de las personas. g. Facilitar el intercambio de datos entre los países de la región, en un todo de acuerdo con las normas nacionales de protección de datos personales. h. Contribuir a que los pueblos de nuestros países accedan en plenitud a la sociedad de la información y del conocimiento mediante la implementación de programas de inclusión digital. i. Superar la brecha digital interna y externa, promoviendo el acceso igualitario a la sociedad de la información de todos los habitantes de los países de la región.
Concepto de Identificación Electrónica Social	3	<p>Sin perjuicio de las denominaciones adoptadas en las legislaciones nacionales, se entiende por “Identificación Electrónica Social” al procedimiento que mediante elementos externos, permite asignar una identidad con determinados atributos a una persona concreta, esto es, a la comprobación de los datos que acreditan que un individuo es efectivamente la persona que dice ser, sujeto de derecho, con determinados atributos.</p> <p>En el presente marco, se entiende por “Autenticación Electrónica” al proceso de verificación de la autenticidad de las identificaciones realizadas o solicitadas por una persona física o entidad, sobre los datos tales como un mensaje u otros medios de transmisión electrónica. El proceso de autenticación es la segunda de dos etapas que comprenden: 1) La presentación de un medio que acredita la identificación ante el sistema y,</p>

		2) La presentación o generación de información que corrobora la relación entre el medio presentado y la persona o entidad identificada.
Fundamentos de la Identificación Social	4	<p>La Identificación Electrónica Social Iberoamericana se apoya en los fundamentos siguientes:</p> <ul style="list-style-type: none"> a. La identificación de las personas es una obligación indelegable de los Estados, así como la protección de su inviolabilidad. b. El reconocimiento del derecho a la identidad que gozan todas las personas, así como a la protección de su integridad y la garantía de su pleno ejercicio. c. El acceso igualitario a la sociedad de la información como bien público relevante, que debe ser impulsado por los gobiernos de la región. d. El reconocimiento de los principios definidos en la Carta Iberoamericana de Gobierno Electrónico.
Principios para el marco de la Identificación electrónica social	5	<p>Con base en los fundamentos anteriores, la Identificación Electrónica Social Iberoamericana se orienta por los principios siguientes:</p> <ul style="list-style-type: none"> a. Principio de igualdad o no discriminación: en ningún caso el uso de medios electrónicos puede implicar la existencia de restricciones o discriminaciones para los habitantes que se relacionen con las administraciones públicas. b. Principio de legalidad: mantener las garantías previstas en los modos tradicionales de relación de las personas con el Gobierno y la Administración cuando se realice por medios electrónicos. c. Principio de conservación: garantiza que las comunicaciones y documentos electrónicos se conserven accesibles para su posterior consulta, en las similares condiciones que por los medios tradicionales. d. Principio de transparencia y accesibilidad: garantiza que la información de las administraciones públicas y el conocimiento de los servicios por medios electrónicos se haga en un lenguaje comprensible según el perfil del destinatario. e. Principio de proporcionalidad: de modo que los requerimientos de seguridad sean adecuados a la naturaleza de la relación que se establezca con la Administración. f. Principio de responsabilidad: de forma que la Administración y el Gobierno respondan por sus actos realizados por medios electrónicos de la misma manera que de los realizados por medios tradicionales. g. Principio de adecuación tecnológica: las administraciones elegirán las tecnologías más adecuadas para satisfacer sus necesidades.
Capítulo Segundo. Elementos Involucrados en el Proceso de Identificación		
Garantía al derecho a relacionarse electrónicamente con la Administración	6	Las Estados iberoamericanos están en la obligación de atender el ejercicio efectivo del derecho de las personas a relacionarse electrónicamente con la Administración, lo que requiere que garanticen la identificación electrónica social de sus habitantes.
Adopción de	7	A los efectos de la identificación electrónica social de los habitantes de la

un glosario común

Comunidad Iberoamericana, los Estados Iberoamericanos entenderán por:

b. **Factores de autenticación:** Son aquellos elementos que integran el proceso de identificación.

Los factores de autenticación que se utilizan actualmente son tres, que se basan en:

- *Algo que sé:* la persona se autentica mediante algo que sabe: una clave, un número que la identifica – PIN, una frase o una respuesta a una pregunta de seguridad.

- *Algo que tengo:* la persona se autentica utilizando algo que posee: un token, una tarjeta inteligente, un certificado digital.

- *Algo que soy:* el individuo se autentica con base en una característica que tiene su persona, esto es, un dato biométrico.

Los factores sustentados en conocimiento y en posesión requieren que la persona que se va a autenticar ante un sistema recuerde o lleve consigo el dispositivo. En cambio, cuando se aplican tecnologías biométricas, el dato lo lleva consigo, y resulta casi imposible que se lo falsee, esto es, que sea utilizado por otra persona para suplantar su identidad. Se dice que en los dos primeros factores, el vínculo entre el dato y su verificación es débil, lo cual facilita la usurpación de identidad, ya que el sistema no puede distinguir entre el legítimo poseedor del dispositivo y alguien que lo haya sustraído, lo mismo se aplica a la clave.

b. **Tecnologías Biométricas:** Se entiende por reconocimiento biométrico a los métodos automatizados que aseguran el reconocimiento de individuos con base en rasgos físicos o conductuales distinguibles. Las tecnologías que se usan en biometría incluyen el reconocimiento de huellas dactilares, de rostros, de patrones de las venas, del iris, de voz y del tecleo, entre otros.

c. **Sistema Biométrico:** Es un sistema informático de reconocimiento con base en uno o varios patrones, que opera requiriendo datos biométricos a un individuo, extractando un patrón de estos datos adquiridos y comparando el ejemplo contra una plantilla previamente registrada. Dependiendo de la aplicación, esta plantilla puede estar almacenada en una base de datos centralizada o en un dispositivo individual, como un token o una tarjeta inteligente.

d. **Infraestructuras de Clave Pública:** (también conocidas como Infraestructuras de Firma Digital o PKI por sus siglas en inglés -Public Key Infrastructure. Puede definirse como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de clave pública basados en criptografía asimétrica, que facilitan la creación de una asociación verificable entre una clave pública y la identidad del tenedor de su correspondiente clave privada.

e. **Firma Digital** -también llamada firma electrónica segura, firma electrónica avanzada o firma electrónica reconocida-. El concepto de firma digital tiene al menos dos acepciones: una tecnológica, vinculada con las tecnologías de clave pública, y otra jurídica, que responde a la definición que las leyes nacionales han incluido como equivalente a la firma manuscrita.

Desde el punto de vista tecnológico, una firma digital es el mecanismo de autenticación que, sustentado en criptografía asimétrica, esto es, que usa dos claves, una pública y una privada, permite identificar al firmante y garantizar la integridad del contenido del documento electrónico firmado. Desde el punto de vista jurídico, las leyes incluyen un requisito administrativo. Ello significa que para ser considerada legalmente firma digital, ese mecanismo debe haber sido aplicado mediante el uso de un certificado digital emitido por una entidad de certificación acreditada por el órgano rector del Estado en dicha materia.

f. **Firma Electrónica:** el concepto se aplica a cualquier sonido, símbolo o proceso, adjunto o lógicamente asociado a un documento electrónico que exprese el consentimiento de una persona emitido en formato digital, y ejecutado o adoptado por dicha persona con el propósito de firmar el documento electrónico. En general, las leyes denominan “firma electrónica” a cualquier mecanismo de autenticación que no cumpla alguno de los requisitos exigidos para una firma digital. “Firma electrónica” es el término genérico y neutral para referirse al universo de tecnologías que una persona puede utilizar para expresar su consentimiento con el contenido de un documento.

Capítulo Tercero. Acuerdos de Reconocimiento Mutuo

- | | |
|---|---|
| Adopción de compromisos regionales | <p>8 El presente Marco promueve todos aquellos asuntos que, vinculados a los procesos de identificación electrónica de personas en entornos físicos o virtuales, constituyen las bases para los futuros acuerdos de reconocimiento mutuo entre Estados iberoamericanos, que son indispensables para alcanzar un efectivo medio común de Identificación Electrónica Social Iberoamericana.</p> <p>9 Mediante este Marco los Estados Iberoamericanos orientarán la discusión de los aspectos legales y técnicos necesarios para la celebración de acuerdos de intercambio de datos, la interoperabilidad de sistemas y el establecimiento de estándares tecnológicos comunes.</p> <p>10 Los Estados Iberoamericanos se comprometen al intercambio de experiencias nacionales en materia de implementación del documento de identidad electrónico y del pasaporte electrónico, y de todo otro mecanismo de autenticación digital.</p> <p>11 Por último, este Marco incluye los contenidos de entendimiento para que los Estados iberoamericanos celebren acuerdos de reconocimiento mutuo de certificados digitales.</p> |
| Adendum a la Carta Iberoamericana de Gobierno Electrónico | <p>12 El presente Marco para la Identificación Electrónica Social Iberoamericana consiste en un desarrollo de los fines y propósitos de la Carta Iberoamericana de Gobierno Electrónico, por lo que se considerará un adendum de la misma.</p> |

BIOMETRÍAS 2

Eduardo Thill

Pedro Janices

Bradford Wing

Mark Branchflower

Jess Maltby

Virginia Kannemann

Julio Fuoco

Ali M. Al – Khouri

Marcos Elías Claudio de Araujo

Jorge Arturo Reina García

Mónica Litza

Néstor Mastosian

Gustavo Donato

Gabriel Casal

Mercedes Rivolta

Compiled by: Natalia Aguerre, Virginia Kannemann | Traduction: Liliana Bosch, Cécilia Pavón

Index

The role of individuals' identification in the development and digital inclusion policies: the framework for the Ibero American social electronic identification Eduardo Thill	267
Biometrics Tools for Social and Digital Inclusion Pedro Janices	289
Standards and Biometrics Bradford J. Wing	307
The International Co-operation and Safety Initiatives in Individuals Identification and Verification using DNA or Fingerprints proposed by INTERPOL Mark Branchflower / Jess Maltby	327
The importance of dental records in identification Virginia Kannemann	339
Biometric Trends, Challenges and Opportunities Julio Fuoco	355
Biometrics technology and the new economy: A Review of the field and the case of the United Arab Emirates Ali M. Al - Khouri	371
The RIC Project as a new paradigm in Brazilian civil identification Marcos Elías Claudio de Araujo	409
Comprehensive project for technological upgrade in the General Register Office of Honduras Jorge Arturo Reina García	419
The Role of Identification in Social and digital inclusion Mónica Litza	435
Advances in the Federal Penitentiary Service´s biometrics project Néstor Mastosian	447
Biometrics Tools in the Province of Buenos Aires: successful cases Gustavo Donato	457
Identity, biometrics and digital signature in the region. Framework for the Ibero-American Social Electronic Identification Gabriel Casal / Mercedes Rivolta	467
Annex: Framework for the Ibero-American Social Electronic Identification	497

The role of individuals' identification in the development and digital inclusion policies: the framework for the Ibero American social electronic identification

Eduardo Thill



Eduardo Thill

Under-Secretary for Technology Management. Cabinet Secretariat. Office of the Cabinet Chief



Eduardo Thill is currently Under-Secretary for Technology Management in the government of the Republic of Argentina. Between 2003 and 2009 was Director General of Information Management in the Interior Ministry and subsequently in the Ministry of Justice and Human Rights.

During his time at the Interior Ministry he had responsibility for the technical aspects of the project to create a database of the entire population to facilitate universal personal identification. In 2002, while Director of Information Management in the President's General Secretariat, he supplemented his duties with responsibility for liaising between the Secretariat, the government of the province of Tucumán and the National Council for Coordination of Social Policy, and was in charge of Operation Rescue in that province.

He participated as a co-speaker on behalf of the Argentine Government at the 2008 Biometric Consortium Conference, as well as attending the 2007 and 2009 BCC events and Biometrics 2005 in London. He is the co-founder and organiser of CIBRA, the Argentine International Biometrics Congress, which has taken place every year since 2006.

Contact mail: ethill@jefatura.gob.ar

Abstract

With no identification there are no rights. The exercise of rights necessarily requires full identification of individuals, a function for which the State is responsible. The State is responsible for individuals' identification and for ensuring the identity of every individual. In an increasingly computerized world, governments make use of ICT's for the implementation of substantive public policies. How to attain the full identification of all individuals, how to recognize these identifications among countries and how to facilitate the remote access to the services rendered by government agencies are issues related to an accurate electronic identification of individuals.

This electronic identification is necessary to have access to computerized systems, e-government applications, e-commerce and also to execute social policies. Besides this use, the modern identity documents, basically passports and national documents, are using electronic identification what demands considering that even for in-person identification, information and communications technologies play a relevant role.

This article presents the recently approved “**Framework for the Iberoamerican Social Electronic Identification**”, the difficulties that this issue brings about and the main aspects involved.

The role of individuals' identification in the development and digital inclusion policies: the framework for the Ibero-American social electronic identification

Introduction

"E-government objectives shall go further than mere efficacy and efficiency of administration processes towards ways that allow social, political and economical changes focused on human development, equal opportunities and social justice" (DECLARATION OF LISBOA; 2010)

Our region's governments are pursuing a course of economic growth combined with social justice. To do that, they are introducing public policies to support development aimed at improving the daily lives of their citizens and achieving the complete social inclusion of those who had previously been left behind.

This new Latin American approach, centred on the individual, is borne out by the range of sectors (Agriculture, Health, Labour, Public Administration and Reform of the State, Tourism, Education, Children and Young People, Justice, Presidency, Housing and Town Planning) covered by the ministerial meetings held during the 20th Ibero-American Summit of Heads of State and Governments in 2010, which resulted in the Declaration of Mar del Plata ("Education for Social Inclusion").

Each of the ministerial meetings covering the different policy areas treated social inclusion as the core issue of public policy in the region. This was also particularly the case at the 13th Meeting of the Ibero-American Network of Presidential Ministers or Equivalents (RIMPE), held in Lisbon, Portugal, whose theme was the Participation of Citizens in the Age of Electronic Government. Here the concept of "social justice" as the inspiration for public policy across the Ibero-American region was first adopted multilaterally.

At that meeting it was agreed to work on the design of "*a more open, transparent and collaborative model of government that allows the economic, social, cultural and environmental challenges facing the world to be answered more effectively*". To that end, the Declaration envisages the use of information and communications technology (ICT) to transform the administration of government, and recommends that countries promote "*policies of electronic government and simplified administration which should contribute, in the manner described, to the development of better quality public services*". (FRAMEWORK, 2011).

The Lisbon Declaration recognises that "*the development of secure methods of electronic identification and authentication is another of the prerequisites for the desired change, with a fundamental role in the promotion of simplified processes and the encouragement of the use of electronic services*".

This is a very special time for the countries of Latin America. Each one is advancing its digital agenda, with one clear vision: to achieve the greatest possible digital inclusion among its citizens. In Argentina, for example, the governments of both Dr. Kirchner and current President Cristina Fernández de Kirchner have since 2003 constructed a national policy of digital inclusion in order to guarantee equal opportunities for all. This policy, inspired by the principle of social justice, has been translated into numerous programs and initiatives of the federal government: Universal Child Benefit, Argentina Connected, Freeview Digital Television, Internet for All, and so on. In turn, these programs are constantly being interconnected, reviewed in terms of feedback, and reconfigured. They represent the social model of Argentina's digital agenda: digital inclusion, equality of opportunities and social justice.

Implementing these programs effectively over such a short period of time has required a major effort on the part of public bodies. This would not have been possible had the relevant agencies not been ready. Their preparation obviously included the technical aspects of electronic government, which equipped them not just for internal management but also for their relationship with claimants and other citizens.

Ibero-American countries are each developing their own agendas for ensuring social inclusion for their inhabitants, with the aim of achieving the effective entry of our countries into the knowledge society. In general, our governments have underlined the importance of implementing public policies designed to bridge existing gaps in our societies. The region is therefore implementing education, health and social development policies with socio-economic development objectives based on inclusion, justice and fairness.

In this context, the identification of individuals takes on an important role. Firstly, because without identification there are no rights. The exercise of rights needs complete identification. In our country this role is performed by the State. The State is responsible for identifying individuals, and for guaranteeing their identities. Secondly, the implementation of fundamental public policies involving mass interaction with the population, especially those policies which are social in nature or relate to digital inclusion, require the identification of individuals in an electronic environment.

Electronic identification is necessary for access to computer systems and e-government and e-business applications, but also for the implementation of social policy. In addition to this use, modern identity documents (mainly passports and national identity cards) are using electronic identification features, leading one to conclude that, even in the case of face-to-face identification, information and communications technology plays an important part.

At regional level, the following issues also arise: how to achieve the complete identification of individuals, how to recognise those identifications in different countries, and how to facilitate remote access to government services. These are questions that involve the proper electronic identification of individuals.

This article outlines the Ibero-American Framework for Social Electronic Identification, which

complements the terms of the Ibero-American Charter on Electronic Government.

Social Inclusion Policies

In this second decade of the 21st century, with an economic crisis affecting the entire developed world, Argentina and its fellow nations in the region are pursuing a different course to that of the 90s. The aim of our governments is to give the State an active role, both as regards the economy and in other aspects of social life. We are thus witnessing a reconstruction of the relationship between the State and society.

At this moment in time we are together rethinking the concept of the nation state. After the crisis at the end of the last century, we faced the challenge of rebuilding an ethical, political and socio-economic community. "That involves once more putting the question of equality centre stage." (CEPAL; 2010)

We are at a veritable tipping point between the neoliberal model, in which the State plays a subsidiary role, and the social model, in which it has an active role. A change of this magnitude demands a change in the underlying values shared by society as a whole.

In effect, the new social model revolves around the general public interest and the provision of public goods. According to the Economic Commission for Latin America and the Caribbean (CEPAL) (2010), the general interest "*refers to the creation and provision by the State of public goods that benefit the whole of society. These goods require considerable investment whose results are often only seen in the long term. Public goods can be found in areas as diverse as education, health, production infrastructure, transport, communications, energy, the environment, investment in science and technology, domestic and external social harmony, the administration of justice, democratic elections and public security.*"

Our countries have made significant progress in this regard. A useful example are the agreements reached by the governments of the region at successive inter-governmental meetings. The Declaration of Mar del Plata in 2010 reflects this resolve. In it, the signatories expressed their agreement on the need to tackle "the challenge of consolidating models of economic growth which extend fairness and social inclusion", and observed that "education is an essential means of achieving such objectives" (DECLARATION OF MAR DEL PLATA; 2010).

Governments further reinforced this idea through this year's Asunción Consensus, in which the ministers of Public Administration and Government Reform agreed that "*the State is a basic and irreplaceable instrument for promoting and guaranteeing the sustainable development of Ibero-America. In this sense development means an increase in the quality of life and happiness of the population, both publicly and privately and both collectively and as individuals, and across all aspects of society, including political, social, cultural, economic, and environmental: development for the good of all of society, with inclusion, fairness and social justice*" (ASUNCION CONSENSUS, 2011).

Another of the values which to our minds must be present is the value of the strategic

vision agreed upon for the State's new role, which involves being active, taking the initiative, coordinating resources, and anticipating and avoiding crises, all in a context of broad social participation. Thinking about the future, taking action in the present, learning from the past, in order to build going forward. *"Like peoples' lives, the future of societies is built over time: a society which does not educate itself, which does not invest in social cohesion, which does not innovate, which does not build consensus and strong, stable institutions, has little chance of prospering. In the face of these challenges, the State must be capable of providing a long-term strategy for public administration, of adopting an anticipatory role and of taking part in the design of strategies for national development. It should be borne in mind that State action takes place in a setting of shared power, so that the negotiation and construction of a strategic national consensus are at once both the means and the end".* (CEPAL; 2010)

Put simply, the times have revaluated the importance of policy. Experience has shown that the market-based model is insufficient and in the long term leads to deep crises. A model based on the individual involves the State in guaranteeing equality of access to public goods for all citizens: the individual as a person with rights, the State as guarantor of equality of opportunity, and equal access to education, health, social security and the knowledge society.

Following this line of thought, our governments have promoted policies that have reintroduced the public as the relevant collective, by making those policies about all citizens rather than just the government or the State.

Starting in 2003 with the presidency of Dr. Néstor Kirchner, Argentina embarked on a period of social reconstruction. On taking the oath of office before the Legislative Assembly, President Kirchner signalled the central policy themes that would guide his government. After pointing out that in the 80s the emphasis was placed on reclaiming democracy, while in the 90s the market took a central place in government policy, with well-known consequences, he indicated his intention to *"promote active policies that would permit the development and economic growth of the country, the creation of new jobs and the better and fairer distribution of income. Clearly the State has a primary role in this, and the presence or absence of the State represents an entirely political stance."* (KIRCHNER; 2003).

Later, President Kirchner stated that *"it is all about having what is needed for our development, to re-engineer an intelligent State. We want to rediscover the values of solidarity and social justice which will allow us to change the way things currently are, and move towards the creation of a more balanced, more mature, fairer society. We know that the market operates economically, but doesn't express itself socially; we must arrange for the State to impose equality where the market excludes and abandons."* (KIRCHNER; 2003). With this thought, he turned the page on the country's history of constant crisis.

Based on that idea, with social justice at its heart, his government started out on the path towards providing equal access to public goods and the possibility of social integration. It did a lot of work on social, educational and health issues, and special emphasis was placed on creating public policies aimed at closing the digital gap. In that regard, it was seven years ahead of CEPAL's observation in 2010 when, referring to values, it claimed a new role for the State

in conditions of full democracy (CEPAL; 2010). In his inauguration address, President Kirchner said: *"It is the State which must take the greatest role in repairing social inequality, working constantly to secure inclusion, creating opportunities through strengthening the possibility of access to education, health and housing and promoting social progress based on the effort and industry of each individual."* (KIRCHNER; 2003)

Based on this vision, inclusive policies, especially in respect of education, employment and infrastructure, were created by the government on a consensual basis. The implementation of these policies presented a significant challenge. One of the first issues to be resolved was the ability to identify those to be benefited. Another important aspect was that digital inclusion was contemplated from the very beginning. The State was considered to have a predominant role in guaranteeing equal access to public goods, one of which relates to closing the digital gap and facilitating the participation of everyone in the knowledge society.

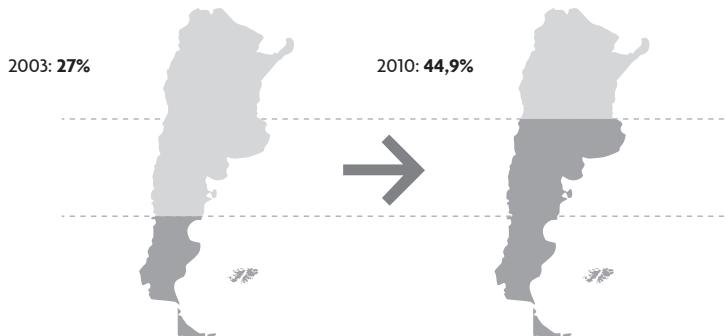
As a consequence, as CEPAL has pointed out, the policies developed by the Argentine government succeeded in transforming the structure of production on the basis of coordinated policies. Improvement was achieved in the country's industrial profile, stimulating those sectors with greatest innovation; its technological profile, strengthening offer and matching it with demand; and its education profile, through the provision of computer equipment in public schools and investment equivalent to 6.7% of GDP (CEPAL; 2010). As a consequence of these policies, unemployment fell by 50% (see Diagram No.1) and the size of the workforce contributing to GDP grew significantly, reaching 44.9% in 2010 (see Diagram No. 2).

Diagram No. 1: Evolution of employment levels



Source: Indec. <http://www.presidencia.gov.ar/component/content/article/138-indicadores/6177-desempleo>

Diagram No. 2 – Level of workforce contribution to GDP



Source: Indec. <http://www.presidencia.gov.ar/component/content/article/138-indicadores/6191-mayor-participacion-de-los-trabajadores-en-el-pbi>

As regards Latin America as a whole, meetings took place throughout 2010 in preparation for the Ibero-American Summit of Heads of State and Governments at which ministers with responsibility for the different participating portfolios, namely Agriculture, Health, Employment, Public Administration and Government Reform, Tourism, Education, Children and Young People, Justice, Presidency, Housing and Town Planning, agreed the objectives to be met by each country, resulting in the Mar del Plata Declaration "Education for Social Inclusion".

On that occasion, the heads of state and government reiterated the common goal of advancing the building of fair, democratic, participatory and collective societies in the context of cultural, historical and educational cooperation and integration across the Ibero-American region to secure for everyone in that region a quality education based on intra- and intercultural social inclusion, in order to promote a fairer Ibero-America, with greater economic, social and cultural development within democratic, collective and participatory societies that promote the wellbeing of all of the region's inhabitants.

The challenges of social inclusion as a central plank of the region's public policies were brought up in the various preparatory ministerial meetings. The 13th Meeting of the Ibero-American Network of Presidential Ministers and Equivalents (RIMPE), held in Lisbon, Portugal, dealt with the theme of the Participation of Citizens in the Age of Electronic Government, and it was agreed that "the goals of E-Government must extend beyond the mere effectiveness and efficiency of administrative processes towards forms which permit social, political and economic change in support of human development, equality of opportunity and social justice." (DECLARATION OF LISBON; 2010)

At the Lisbon conference, the delegate countries agreed desirability of advancing electronic government initiatives. Specifically, they declared their intention to tackle the following points:

- To promote programs linking electronic government and simplified administration, with the aim of making interaction between individuals and businesses and the public sector simpler, faster and more efficient,
- To share experience within the Ibero-American community as regards the creation of unique

- integrated services, whether real or virtual, to meet the needs of individuals and businesses,
- To share experience relative to the implementation of secure forms of electronic and biometric identification and methods of integration for the development of cross-border electronic services within the Ibero-American region,
 - To coordinate the sharing of experience of using ICT in order to ensure the transparency of public decision-making processes and to offer new forms of participation in the democratic process,
 - To promote digital inclusion policies and practices which facilitate access to electronic services, so that all citizens can take equal advantage of the potential of ICT as a means of ensuring social and territorial cohesion.

In summary, we are witnessing a re-evaluation of the State to give it an active role aimed at improving the living conditions of the region's citizens; an active State which promotes social inclusion through effective public policies. These initiatives go hand in hand with the conviction that the knowledge society is the future, and with a belief in the need for a closer relationship between the State and the citizen, for which electronic government is an effective tool.

Importance of the identification of individuals

In this context, with the region's countries implementing active public policies of social inclusion, the issue of the correct identification of individuals represents an important key to success, both for the implementation of large-scale policies of social inclusion and for the authentication of the identity of citizens by electronic means. As our countries have progressed the implementation of e-government measures, one of the issues that have emerged is the correct identification of individuals in computerised platforms.

In 2007 the Ibero-American Charter on Electronic Government highlighted the need for the use of ICT in public administration to be centred on the citizen and his rights, the term "*citizen*" being understood to mean "*such natural or juridical person as requires to deal with a government either within the country or, having the right to do so, from outwith the country.*"

The Ibero-American Charter on Electronic Government emphasises the central role of the individual, rather than the technology; consequently, it encourages the recognition of the right of citizens to deal with the government electronically. This recognition of the right of every citizen to use electronic means to conduct his or her business with the government involves establishing a portal for access to information, laying the foundations for open government and removing physical and geographic barriers to a closer relationship between the citizen and the State.

In that regard, the Ibero-American Charter on Electronic Government highlighted "*the unique role of States in these matters in order to guarantee the availability of electronic services to all citizens, and the continuity of those services, and the strengthening of democracy.*" We can see therefore the link between digital inclusion and the development of public policies in general in a democratic society.

The Charter defines the concept of "*electronic government*" as a synonym of "*electronic administration*", by which is understood "*the use of information and communications*

technology in government organisations to improve the information and services offered to citizens, to regulate the effectiveness and efficiency of public administration, and to increase substantially the transparency of the public sector and the participation therein of citizens."

The Charter addresses the question of the identification of individuals as a tool of electronic government. It points out the obligation of the State to facilitate access by citizens (in a wide sense) to the electronic information held by the government. Among the fundamental elements identified by the Charter are "*the identification of the citizens, government organisations and their officials and agents who use electronic media, as well as the authenticity of those electronic documents that contain their consent or authority.*" (CHARTER; 2007).

The Charter recommends that States issue legal and technical regulations which guarantee for both citizens and the government the conditions necessary for "security and confidence in their electronic transactions, both as regards the identity of the person, organisation or institution one is dealing with and as regards the authenticity and integrity of the content of the communication and, consequently, in the impossibility of it being repudiated by the issuer."

The Charter considers that a communication has such authenticity and integrity if it is received as transmitted, without its contents having been altered. The recommendation to States in this respect is that in their regulations on the security of electronic government they consider "*physical systems, and systems of electronic signature, including advanced and other alternative systems of electronic signature as may be required by the nature of the transaction, which permit the person communicating to be identified and the authenticity of the content of the communication to be verified.*"

We can see therefore that the Ibero-American Charter on Electronic Government highlights the identification of individuals as a core element in the implementation of policies of electronic government. The role of the State is central to achieving the correct identification of individuals to enable the implementation of public policies to be implemented, as in its role in identification in electronic settings.

In the virtual environment, the Charter recognises the basic electronic signature and the digital, or advanced electronic, signature as elements of authentication. These are tools which allow the authorship of an electronic document to be identified, and its integrity confirmed, and in addition the identity of a person to be confirmed in a virtual setting.

In this respect, and following the recommendations of the Lisbon Declaration, Ibero-American governments considered it necessary to supplement the Ibero-American Charter on Electronic Government with a specific framework for social electronic identification to provide the region with a conceptual framework as a guide to the identification of individuals and electronic authentication, which are fundamental to the full exercise of rights and the effective implementation of public policies of social inclusion. (FRAMEWORK; 2011)

IV. Ibero-american framework for social electronic identification

As a result of the foregoing, the Ibero-American Framework for Social Electronic Identification

was presented for consideration at the 13th Ibero-American Conference of Ministers of Public Administration and Government Reform held in Asunción, Paraguay, on 1st July 2011, at which the text was approved.

The Framework addresses the problems of the identification of individuals from a technological perspective, and considers it necessary to start to establish common standards in order to coordinate the correct identification of individuals across the region. The document then presents an explanatory section which describes the elements involved in the identification of individuals, and the relevant legal framework and its consequences.

In addition, it describes in simple terms the biometric and digital signature technology involved. Why only this technology? Because there has been a lot of progress worldwide in the use of biometric technology in documentation which vouches a person's identity, such as a passport; and because new laws have been passed across the region which recognise the legal value of digital signatures and their use in e-commerce and e-government. However since each country has its own set of rules governing these matters, it becomes necessary to start to establish common standards that allow for the cross-border recognition of such digital signatures.

Features of electronic identification

Identification and the Full Exercise of Rights

A person's rights and obligations are based on his or her identity. The ability to assert and exercise a right belongs to a particular person, with certain attributes and identity. The process of assigning an identity and particular attributes to a specific person by extraneous means is what we call "*identification*". (FRAMEWORK; 2011)

This relationship between a specific person and certain attributes that define his identity, such as his name, place of birth, fingerprints and distinguishing features, permit on the one hand the unequivocal identification of each individual; and on the other hand, verify his identity whenever necessary, whether for exercising a right, accessing social security benefits, or moving from one country to another, and so on.

In this country, that process of identification is a function that the State cannot delegate. It is the State which identifies people, which verifies the information that enables that identification that issues the document that provides proof of identity, and that protects the exercise of the right to an identity.

Separately, the State relies on this identification for the proper and effective implementation of social-based public policies. The identification of individuals is an essential element of legal acts, since any error in the identification of an individual constitutes defective consent and leads to the transaction being void and the legal relationship invalid.

In Argentina, the identification of individuals is regulated by Law No. 17.671 (Law of Identification, Registration and Classification of National Manpower) and achieved by means of a National Identity Document. For that reason work has been proceeding since 2003 on the digitalisation of the identity card transaction, initially using existing paper-based biometric

details, which involved the electronic conversion of 50 million index cards. This then allowed the computerisation of the processes of applying for and issuing the document, which today is complete.

Internationally, the identity document that is used for entering other countries is the passport. Some countries have made provision for a single identification document; but those all meet the standards for passports, in order to be recognised in other countries.

In summary, a person who has not been identified by the State does not exist from a legal point of view. The implementation of substantive public policies, especially of a social nature, require correct identification of individuals for their implementation. And in the second decade of the 21st century, that is not possible without the help of technology, specifically, existing biometric technology which meets accepted international standards.

Biometrics and Identification

The process of identification of a person is based on a comparison of characteristics with data. Today there is technology that allows this comparison of data to be automated, speeding up the processes of issuing documentation and verifying identity.

Even for paper-based documentation – in other words, for face-to-face identification – automated biometric technology has been incorporated which, since it observes international standards, facilitates the traceability of data.

Biometric technology allows identification based on an individual's physical characteristics: DNA, fingerprints, facial features or the characteristics of the iris, details which are personal and unique to a particular individual.

Today there is biometric technology in multiple public and private applications. For example in social networks, the application automatically assigns a name to a person when his or her photo is uploaded which, depending on the facial recognition information available, the system interprets as correct. Some have questioned this application, since it identifies individuals without authorisation and with a high degree of error, and could affect the right to privacy.

In the public realm, biometry is used both for the identification of individuals and for the authentication of identity in computerised systems, the strengthening of public security at airports and in cities, and the restriction of access to secure sites (both in the physical sense – buildings – and the virtual – computer systems and applications). Recognition is conducted using physical characteristics (fingerprints, features of the face or hand, and iris patterns) or learned or acquired behavioural characteristics (voice patterns, handwriting and keystroke patterns).

There are various devices for housing biometric technology and identifying individuals. These devices rely on various factors, depending on the level of security the application requires. Typically, authentication factors will be something we know (a password, for example), something we have (such as a smart card) and something we are (in other words, some biometric detail). The use of the three factors for authentication makes the process secure.

The Framework for Social Electronic Identification contains a description of these authentication factors, and defines the concepts of biometry and biometric technology.

Digital Signature Infrastructures

The countries of the region have made progress towards consolidating their laws on the legal status to electronic and digital documents and signatures. In this process, many of them have adopted digital signature schemes, in other words public key infrastructures in which a State organisation licenses providers of digital certificates.

However these public key infrastructures have legal scope only within each country's borders. This is not because of technological difficulties but due to the nature of national legal systems, in which laws only apply within national boundaries, except to the extent covered by existing international treaties.

In the case of digital signature recognition there is no agreement for mutual recognition among countries, despite the laws of most countries acknowledging that possibility.

This makes it difficult to reach agreement on transnational applications, whether public or private. Thus arose the idea of establishing a shared conceptual framework to delineate minimum common denominators that would allow further agreement on digital signatures and electronic authentication to be reached.

Purpose and scope of ibero-american social electronic identification

Chapter 1 of the Ibero-American Framework defines its founding objectives, principles and aims.

Its objectives include drawing up a generic framework of guiding principles, policies and administrative procedures to lay the foundations for the future design of a scheme of mutual recognition of electronic recognition devices across the countries of the region. A further objective proposes the promotion of the use of electronic identification documentation across the region, including electronic passports and national identity documents, in a way that respects each country's characteristics and peculiarities.

Likewise the Framework seeks to set down technical recommendations for governments in connection with electronic authentication processes, particularly for the creation of processes of remote user authentication over open networks.

The aims which inspired the Framework are those of the Ibero-American Charter on Electronic Government, of which it forms part. Consequently, the aim of the Framework is to bring citizen and government closer together, to recognise the right of the former to connect himself electronically with the latter, and to facilitate access to and participation in the process of government.

In relation to the issue of identification, the Framework expresses the aims of establishing a framework of cross-border recognition of electronic identification and authentication devices;

promoting the use and mutual recognition of electronic identity documents; guaranteeing the protection of the right to identity and facilitating the intra-regional exchange of information.

In addition, the Framework includes aims linked to closure of the digital gap and to equal access to the knowledge society. In this context, the proposed aims include contributing to our populations having full access to the information and knowledge society through the implementation of digital inclusion programs, and closing both internal and external digital gaps.

Concept of electronic identification

Without prejudice to the designations adopted in national legislation, the Framework adopts a common definition for the concept of “*Social Electronic Identification*”. It is understood as “*the process which through external elements allows an identity with certain attributes to be assigned to a specific person, that is the verification of the information that proves that an individual is indeed who he claims to be, a legal person, with certain attributes*”.

At the same time it defines the concept of “Electronic Authentication” as “the process of verifying the authenticity of identification carried out or requested by a natural person or organisation of information such as a message or other means of electronic transmission. The process of authentication is the second of two stages comprising: 1) The introduction of a means of accrediting the identification [in the system and 2) the presentation or generation of information which corroborates the relationship between that means of accreditation and the person or organisation identified”. The introduction of the concept of “electronic authentication” is an innovation. Until now, national legislation recognised the concepts of “identification” and “electronic signature” or “digital signature”. The concept of “electronic authentication” is common in the vocabulary of technology, but hadn’t yet been introduced in government or e-commerce regulations. This is the first initiative in that context, and we believe that it constitutes a major contribution to the Ibero-American Framework of Social Electronic Identification.

The Framework sets out a series of fundamentals which inspire it, linked to the role of the State, namely:

1. The identification of individuals, as well as protection of the inviolability of their identities, as non-transferable obligations of the State.
2. Recognition of the right of every person to an identity, as well as the right to protection of its integrity and the guarantee of its unfettered exercise.
3. Equal access to the information society as an important public good which must be promoted by the governments of the region.
4. Recognition of the principles defined in the Ibero-American Charter on Electronic Government.

Finally, Chapter 1 of the Ibero-American Framework reviews the principles to which it subscribes. Those principles, recognised by the Ibero-American Charter on Electronic Government of which the Framework forms part, are as follows:

- Principle of equality or non-discrimination:** the use of electronic means may never involve restricting or discriminating against citizens in their dealings with the government.
- Principle of legality:** keeping the same guarantees for electronic transactions as are expected in traditional modes of transacting with the government.
- Principle of conservation:** guaranteeing that electronic communications and documents remain accessible for subsequent consultation under conditions similar to those applicable in traditional forms of transaction.
- Principle of transparency and accessibility:** guaranteeing that information about government and its electronic services is written in language easily understood by those receiving it.
- Principle of proportionality:** ensuring that security requirements are appropriate to the nature of the relevant administrative transaction.
- Principle of responsibility:** making the government answerable for actions carried out by electronic means to the same extent as it would be answerable in traditional forms of transacting.
- Principle of technological capacity:** governments must select the most appropriate technology to meet their requirements.

Technical aspects of social electronic identification

Chapter 2 of the Ibero-American Framework promotes the recognition of the right to transact electronically with the government, echoing the Ibero-American Charter on Electronic Government.

Specifically, article 6 states: "*Ibero-American States have an obligation to facilitate the effective exercise of the right of individuals to transact with the government, which means guaranteeing the social electronic identification of their inhabitants*".

The Framework then provides a glossary aimed at establishing a common set of definitions of the technical aspects of the electronic identification process.

Article 7 sets out a common glossary which, by standardising the terminology used and establishing common criteria on those important technical issues, will allow future agreements of mutual understanding to be drawn up.

The Framework's glossary defines the following terms:

- Authentication factors:** these are those elements that make up the identification progress. Three authentication factors are currently used, based on:
 - *Something I know:* the person is authenticated using something known to him: a password, an identifying number (PIN), a phrase or the answer to a security question.
 - *Something I have:* the person is authenticated using something he possesses: a token, a smart card or a digital certificate.
 - *Something I am:* the person is authenticated on the basis of a personal characteristic, i.e. a biometric detail.

The factors based on knowledge and possession requires the person being authenticated to

remember something or to take an item (such as a card) with him. In contrast, when biometric technology is used the information is with him permanently so that it is therefore almost impossible for it to be falsified (that is, for it to be used by someone else for impersonation purposes). It is said that in the first two factors, the link between information and verification is weak, which makes stealing identities easier, since the system cannot distinguish between the legitimate possessor of the device or password and someone who has stolen it.

2. **Biometric technology:** biometric recognition means the automated methods that guarantee the identification of an individual based on physical features or distinguishable behaviour. Biometric technology includes the recognition of fingerprints, the face, vein patterns, the iris, the voice and keystroke patterns.
3. **Biometric system:** this is a computerised recognition system, based on one or more patterns, which extracts one of those patterns from an individual's biometric data and compares the sample with a previously created template. Depending on the application, this template can be stored in a centralised database or in a separate device, such as a token or a smart card.
4. **Public Key Infrastructure:** also known as Digital Signature Infrastructure or PKI, this can be defined as the combination of hardware, software, people, policies and procedures necessary to create, administer, store, distribute and revoke public key certificates using asymmetric cryptography, which facilitates the creation of a verifiable association between a public key and the identity of the holder of the corresponding private key.
5. **Digital Signature:** also known as secure electronic signature, advanced electronic signature or recognised electronic signature, the concept of the digital signature has at least two meanings: one technological, linked to public key technology, and the other legal, reflecting its definition in national laws as equivalent to a handwritten signature.
From a technological point of view, a digital signature is the means of authentication which, supported by asymmetric cryptography (meaning the use of two keys, one public and one private), enables the signer to be identified and the integrity of the contents of the signed electronic document to be guaranteed.
From a legal point of view, laws include an administrative requirement. This means that in order for a document to be considered legally completed with a digital signature, the signature must have been applied using a digital certificate issued by a certificate authority accredited by the relevant supervising State organisation.
6. **Electronic Signature:** this concept is applied to any sound, symbol or process attached to or logically associated with an electronic document which expresses the giving of a person's consent in digital form, and is performed or adopted by that person for the purpose of signing the electronic document. In general, laws give the name "electronic signature" to any means of authentication that does not comply with one of the requirements necessary to be a digital signature. "Electronic signature" is the generic, neutral term for referring to all technology that a person can use to express his agreement with the content of a document.

Basis of agreement on mutual recognition

Finally, Chapter 3 of the Framework lays down a series of considerations relating to the establishment of common criteria to allow for a future common means of social electronic

identification across the Ibero-American region.

Accordingly it promotes the establishment of agreements on mutual recognition linked to processes of electronic identification of individuals in physical or virtual settings.

The Framework advocates discussion, based on its contents, of the legal and technical aspects needed for concluding information exchange agreements, for ensuring the interoperability of systems, and for establishing common technological standards among Ibero-American countries.

Furthermore, it promotes the sharing of each country's experience of the implementation of electronic identity documents, electronic passports and any other means of digital authentication.

Finally, in a significant step towards the strengthening of electronic commerce and digital government, the Framework states that it shall form a basis of understanding for Ibero-American States to enter into agreements for the mutual recognition of digital certificates, setting the foundations for future agreements that permit the coordination of digital signature infrastructures across the region.

Conclusions

We have seen that the countries of the region are rolling out public policies designed to achieve full digital inclusion for their citizens. The Ibero-American Framework of Social Electronic Identification is a further step towards achieving this goal. For our countries, it is a starting point for moving forward in a coordinated and structured manner in a subject of great importance for the effective implementation of social policy: the identification of individuals.

However the Framework also represents a major advance in the introduction of electronic government initiatives across the region, and for the effective implementation of the Ibero-American Charter on Electronic Government.

In this regard, the Framework will allow us to make progress in the recognition of electronic and digital signatures, aiding the development of open government and electronic commerce.

If we make progress towards closing the digital gap, and towards establishing electronic government, our countries will, put briefly, be in a position to recognise the right of their inhabitants to transact electronically with their governments.

We must however reiterate certain ideas that we have set out at other times during this Congress of the Latin American Centre for Development Administration (CLAD) regarding the safeguards that must be provided in order for the implementation of these projects to be successful.

We have mentioned that the difficulties in implementation are not related to the technology, which is already sufficiently developed. Nor is the problem the question of international standards, which have already been developed and accepted. As with every project that involves introducing information and communication technology to the administration of government, projects aimed at building a biometric database or replacing existing identity documents with electronic ones

face the same risks as any other cross-government technological project. (THILL; 2010)

The challenge facing our countries when implementing technological projects in the public sector that will permit the development of e-Government is related not so much with a lack of resources, nor with inadequate infrastructure, nor even with a shortage of qualified personnel, but with a lack of coordination among public bodies. In effect, the efforts of governments often do not produce the expected results not through lack of resources but because the different organisations implement projects in an uncoordinated manner, resulting in each operating in total isolation.

It is clear that in order to achieve results in the implementation of technological projects in the field of public administration, adequate planning is required, along with monitoring and evaluation of their development. That alone is not sufficient to guarantee success, however, particularly where projects involve a number of organisations, in other words where they are being implemented across various different parts of government. A crucial factor is the role of policy decision-makers, particularly those involved in defining public policy in relation to the use of technology in government or to the modernisation of the State.

We would highlight the central role of “leadership” in the design and implementation of electronic strategies. Without determined leadership it will not be possible to overcome the natural resistance to changes in working methods resulting from the incorporation of information and communications technology into the business of government. (THILL; 2010)

In summary, the consensus achieved between the countries of the region on means of electronic authentication and identification using technological tools, to which the Ibero-American Framework on Social Electronic Identification gives expression, constitutes a step forward towards electronic government. It is also an important step in starting to formulate agreements on the mutual recognition of electronic certification of digital signatures. However the most significant achievement lies in the fact that it is the first joint initiative aimed at achieving common standards in respect of identity documents, identification processes and biometric technology.

This initiative will allow us to start sharing experience and achieve common guidelines to improve the quality of performance of public services and achieve the full identification of our citizens, which is an essential requirement for the deployment of social inclusion policies.

Bibliography

- CEPAL (2010), "La hora de la igualdad: Brechas por cerrar, caminos por abrir", United Nations, May 2010. Available online at http://www.eclac.org/publicaciones/xml/0/39710/100604_2010-114-SES.33-3_La_hora_de_la_igualdad_doc_completo.pdf
- CLAD (2007), "Carta Iberoamericana de Gobierno Electrónico". Available online at <http://www.clad.org/documentos/declaraciones/cartagobelec.pdf/view>
- CLAD (2011), "Consenso de Asunción", Available online at <http://www.clad.org/documentos/declaraciones/consenso-de-asuncion/view>
- CLAD (2011), "Marco Iberoamericano de Identificación Electrónica Social", ratified at the 13th Ibero-American Conference for Ministers of Public Administration and Government Reform, Asunción, July 2011. Available online at http://www.agendadigital.ar/docs/identificacion_electronica_social_iberoamericana.pdf
- KIRCHNER, Néstor (2003). Inauguration speech to the Legislative Assembly, 25 May 2003. Available online at <http://www.anibalfernandez.com.ar/Documentos/Asunción de 20Nestor Kirchner.pdf>
- ORGANIZACIÓN DE ESTADOS IBEROAMERICANOS (2009), "Declaración de Lisboa", 19th Ibero-American Conference Argentina 2010, December 2010. Available online at http://www.oei.es/Declaracion_Lisboa.pdf
- ORGANIZACIÓN DE ESTADOS IBEROAMERICANOS (2010), "Declaración de Mar del Plata", 20th Ibero-American Conference Argentina 2010, December 2010. Available online at <http://www.oei.es/declaraciondemardelplata.php>
- THILL, Eduardo (2010): "Identidad, Identificación Electrónica y Ciudadanía Digital". Paper on Reform of the State and Government Administration presented to the 15th International Congress of CLAD, Santo Domingo, November 2010

Biometrics tools for social and digital inclusion

Pedro Janices



Pedro Janices

National Director. National Office of Information Technologies



In 1995 he started his career in the Federal Administration with diverse positions in the National Government in which, through different projects, he has been building experience and knowledge on issues related to public management, technology and identity. Over all these years he was able to gather the experiences and needs of the National Government and know what the society demands.

At present, his functions are oriented to the coordination of projects on e-government implementation, the relationship and strengthening of the tools promoting the creation of the digital citizen (e-citizen), the development and approval of the digital signature implementation plans (pki), the development of policies for the implementation of actions to protect of critical information infrastructures (CIP), and the development of hardware, software and data standards of the Federal Administration, among other tasks.

Contact e-mail: Pjanices@jefatura.gob.ar

Abstract

Digital inclusion policies shall be based on providing individuals the necessary knowledge and capacities for an improved government-citizen communication and on the democratization of information through ICT's with the goal of bridging inequalities, opening new possibilities of social growth and turning citizens aware on the use of networks and their content to gain knowledge and develop competences. For the attainment of this, it is first necessary to know and identify users univocally.

To speak about digital inclusion it is necessary to refer to social inclusion and security policies. The first ones have to be supported on favouring excluded individuals providing them with the necessary mechanisms and tools to improve their life quality. Social welfare shall be ensured to all citizens, with special attention to those in need that suffer from the lack of them, for which the Government needs to know and identify every citizen who is granted such benefit and be sure that it was received by those in need.

Citizen security policies must be based on policies for the prevention and dissuasion of possible crimes; and a substantial part of this policy is the correct and accurate identification of individuals, an essential function of the State for a precise verification of the identity.

The common denominator for these three scenarios is the citizen, the one who the State has to know, to be capable to identify and to provide an accurate LEGAL identity and, to preserve the privacy of this information.

Key Words: digital inclusion, ciber identity, biomectic, security

Biometrics tools for social and digital inclusion

Introduction

The present work aims at showing the experience gained in the last 7 years on the biometric field through diverse projects implemented by the National Government and to present the new action plans for the next 5 years, understanding the use of biometric tools as an integral process that demands commitment and responsibility in the application of the model by different actors of society.

For this purpose, different issues will be described as social indicators of the work that the Argentine Government is carrying out in relation to the “*2011 -2016. Biometrics: a key tool for social and digital inclusion*” program.

Current situation

To start dealing with this issue, it is necessary to go back to the past. As of 2005, the National Government promoted the adoption of international standards in biometrics to allow sharing information among agencies competent on this issue as well as between provincial governments and the Nation. Likewise, it fostered the implementation of equipment with the biometric quality certifications necessary to obtain the raw material to ensure and guard citizen identity.

The adoption of ANSI-NIST type standards for the transmission of biometric data for identification was a step studied and assimilated considering the benefits that this type of communication provided in systems interoperability. Law 17.671 for “*Identification, Registration and Classification of National Human Potential*” in its chapter II, Section I, Art. 7 considers the record of biometric patterns but not the means to transmit or guard them, defining only their classification in the following manner “*at least patronymic, numerical and dactyloscopic cards will be kept in compliance with the Argentine Vucetich system or another that in the future the technical evolution might consider*”. This allows the constant and necessary evolution of the systems for keeping, classifying, comparing and recording biometric data to optimize processes and procedures in order to provide an identity and, to issue the National Identity Documents.¹

Also, the adoption of these standards enables the inter-consultation with other Agencies (provincial and foreign) to support national and international public security policies.

These are based on the accurate identification of individuals; and it is worth stressing that they are mandatory for the constitution of a Nation as they allow defending individual identification. They are an essential instrument against identity theft, and they contribute in the prevention and fight against crime, the optimization of border registration systems, the authentication in commercial transactions and the exercise of social and electoral rights, among others.

Then, the identification and security policies, for being a central axis in government management, enabled the application of biometric tools to the projects that require identity identification by

¹ <http://www.infoleg.gov.ar/infolegInternet/anexos/25000-29999/28130/texact.htm>

agencies of the Federal Administration.

Therefore, having social and digital inclusion as a conceptual framework in the Citizen-Government relation (C2G), the following basic objectives were established:

- To ensure a full and univocal identity.
- To ensure privacy of personal data.
- To optimize citizen registration and identification mechanisms.
- To optimize public security processes within the scientific framework of recognition in crime investigation.
- To strengthen the State's capacity through ICT's.
- To continue with the ongoing improvement policies for the insertion of biometric tools.

Therefore, projects such as the following ones were implemented: improvement in the circuit for the issuance of the National Identity Document and the Argentine Passport, technological update of the automated fingerprint identification system (AFIS) at the Argentine Federal Police, the creation of a multi-biometrical record for the access to the Federal Penitentiary Service premises, update of the National Recidivism Registry system and the creation of the "*National Program for the standardization of biometric data and forensic data*".

In the last 8 years, there has been an extraordinary development of biometric technologies in general and of its different branches in particular: verification and identification through fingerprints, facial, iris, vascular, voice and DNA, among others, as well as new combinations: multi-biometrics, fusion, etc. bringing about even more accurate results.

Following the same path, we have collaborated with NIST (National Institute of Standards and Technology - USA) participating very actively in the elaboration of open biometric standards (ANSI NIST-ILT 1-2011) and successfully promoting the incorporation of records of the estomatognathic system (dental comparison, lip prints, palatal rugae and bite marks) leading the group of dental records, with agencies such as the Federal Bureau of Investigation (FBI), INTERPOL, Bundeskriminalamt, and Miami Dade, among others.

Also the sixth "*International Biometrics Conference of the Argentine Republic*" called CIBRA was organized, where projects at national and international levels are presented. In this event there is an interchange of knowledge and experiences with provinces and other nations in the world. The fifth edition of the Conference, in 2010, published the book "Biometrics" (2010), that compiles some of the many papers presented.

2011 -2016: Biometrics as social inclusion

But stressing the objectives of the current State policy, it is necessary to bear in mind that security is one of the dimensions of human development that includes the environmental, education and socio economic situation of the population, these being the basic components for the construction of citizenship and to strengthen the State and its institutions.

Social exclusion is an issue that generates permanent conflicts in the countries of our region: human trafficking including minors, school desertion, illegal labour market, disappearance of people with deprivation of life, identity theft, among others. In face of this situation future fields to approach it are under study, analyzing the external and internal contexts where this situation is taking place to determine how to attain the proposed objectives.

Programs such as the Argentine Digital Agenda, promotes the elimination of the so called "digital divide" providing communications and technological tools so that citizens at school age and the family group can be part of the digital world. The access to school, cultural and information contents are part of the improvement of citizenship quality in its relation with governments, provincial and national, providing equal opportunities and generating more and better jobs thanks to the initiatives of the national production of technological equipment that foster higher investments. All this, is a constituent part of a stable and strong government that promotes social and digital inclusion.

For this reason, when analyzing the sustainable development of these projects, we are faced with the certainty that biometrics should not be focused only from a technological perspective for application and use, but also it should be part of the progress in social inclusion issues.

The security pursued should not be based on more prisons, or on providing more weapons to fight against crime, but on inserting those least protected to a social ecosystem where they can be trained, they can have an opinion and be part of a growth model; and for this purpose, digital inclusion is undoubtedly the following step in social inclusion, allowing citizens to be part of the society since their infancy.

Childhood

Taking as a conceptual framework the "*XII Ibero American Conference of Ministers and Responsible Staff for Infancy and Adolescence*" held on June 23 and 24, 2011, in the Autonomous City of Buenos Aires, in which a commitment to take legislative actions to facilitate the construction of integral systems for the protection of infancy and adolescence was taken, it was decided to accompany this process from the environment of our competence.²

It is known that it is a State obligation to protect, and if it is the case, to restore the fundamental aspects of a child's identity as name, nationality and family relationships.

But, why is it important to have a name? Because it is the most common social way of introducing oneself to other people, to declare an identity. Every person, every human being is born with biometric features such as fingerprints but that individual needs to be identified before him/herself and for other individuals with his/her own biographical data (first name, last name, etc.) and to perform necessary administrative procedures with his/her documents and identity number. An individual with no name and nationality cannot have access to other rights; a name and a nationality are the pillars that contribute to the exercise of other rights such as the access to medical care, education, information, recreation, etc.

² <http://www.xcumbreiberoamericana.mrecic.gov.ar/?q=node/17>

The Convention on the Rights of the Child incorporated to the National Constitution under the 1994 Amendment (art. 75 par.22) states in its Article 7 that “The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents”. On the other hand, article 8 states that *“States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name and family relations (...)”*³.

In our internal law, Law N° 26.061 for the integral protection of the rights of girls, boys and adolescents rules under Article 11 that *“Girls, boys and adolescents shall have the right to a name, a nationality, their mother tongue, to know who their parents are, and to preserve family relations in accomplishment of the law, the culture of the place of origin and to preserve their identity and idiosyncrasy, with the exception of the provisions of the articles 327 and 328 of the Civil Code”*.⁴

Girls and Boys present a series of difficulties when they do not have an identity document. A child with no identification document does not have full access to the protection that public powers have the obligation to provide to every individual. The child is confined to a world with no opportunities to have access to the juridical, legal and social protection system in a country if the State does not protect him or her or does not recognize his or her rights.

Although it is true that this corresponds to a management decision in the interior policy, as it has already been mentioned, it is inserted in the foreign policy to pursue the attainment of the commitments subscribed in the *“World Summit and Millennium Development”*, as it is the *“World Status of Infancy”* where statistics pose that millions of children are denied their basic rights to identity, quality education, health, protection from abuse and labour exploitation.

But children are not only in our political agenda but also in our health agenda.

Health

In the *“XII Ibero American Conference of Ministers of Health”*, held on December 3 and 4, 2010 in the City of Mar del Plata, it was decided to foster an integrated agenda on health and education for social inclusion and it was agreed to implement joint actions to promote human resources training.⁵

The sanitary information system is one of the essential basis of the activities in public health. A few developing countries have effective systems although knowledge is boosted by the new communications and information tools. There is a considerable and evident gap between what those who plan sanitary policies know and what it is necessary to know to improve health projects. Needless to say those among the necessary issues to be considered are patient’s identification, medical records and confidentiality of their identity and associated data.

Difficulties are not only due to financial constraints. In this area, measurement is a conceptual

³ La CDN y el derecho a la identidad: <http://www.unicef.es/infancia/derechos-del-nino/convencion-derechos-nino>

⁴ Ley 26061: <http://www.infoleg.gob.ar/infolegInternet/anexos/110000-114999/110778/norma.htm>

⁵ <http://www.xxcumbreiberamericana.mrecic.gov.ar/>

and technically complex work that demands sound data about sanitary results (for example, diseases, treatments, drugs and mortality), inputs from the health system (such as human resources, infrastructure and financing) and health determinants. A portion of sanitary information is not only a matter of a determined state entity; it is produced and used by diverse institutions, such as health ministries and secretariats, national census agencies, ministries of labour, social welfare, planning and finance and the private sector, among others.

Childhood and health are one of the first social indicators, but also the sector of housing and urban development, tourism and education integrate the work dynamics of the Federal Administration as well as Universities and institutions of the third sector such as NGO's, which undertake the task of designing projects and programs focused on solving the society's demands, considering that many of them can be implemented with the human resources obtained from social inclusion, their protection and training.

As previously stated, there are other rights, as the access to information, education and free speech, which are currently closely related to the access and use of ICT's.

Social and digital inclusion

The access to the different factors that allow accomplishing this can be reflected on diverse projects being carried out by current Argentine Government that promote social inclusion and establish the links of the Digital Agenda focused on closing the Digital Divide.

Connecting every link of this chain of projects we can start from the inclusion of minors who lacked resources into school, to social assistance implemented through the projects belonging to the plan called "*Universal Allowance for Pregnancy*" and "*Universal Child Allowance*" with over 4.5 million families assisted, to which the "*New Argentine Identity Document*" is added with over 8.2 new identity documents issued up to date, as well as public and free access to the Internet through the "*Argentina Connected*" project, followed by the over 1 million personal computers provided to the new school-age generation for education and approach to ICT's through the "*Egalitarian Connection*" project and the access to free and egalitarian information of the "*Open Digital Television*" that currently has over 16 information, training, education and cultural contents.

It is worth mentioning that these projects are accompanied by programs such as the "*Social Self-employed Taxpayer*" through which the individuals with social and economic vulnerabilities can be directly contracted by agencies of the Federal Administration, these being selected from a database of public access, providing transparency and allowing inclusion to the labour market in a quick and effective manner.

As above mentioned, these links give soundness to the chains of facts focused on the social inclusion of the more needy and provide, at the same time, the technological tools not only related to information but also to training, opinion and participation.

This inclusion is closely connected to the need to offer a more accessible, usable, responsive and effective interface for the access to information, fostering an e-government that has to

allow citizens to access to the information the government possess about them.

For this purpose, the Government needs to have certainty about “*who*” is requesting information and “*what*” private information about a citizen that individual is receiving, in other words, “*who*” is on the other side of the computer.

This is the point where the identification factor is relevant and on which the strategy that such digital information be forged through the “*triple factor*” is based.

“*Something that I know, something that I have and something that I am*” is the expression coined by those who support the use of a key, a device of the token/card type and a verifiable biometric record as the elements to reinforce the integrity of identity verification through digital means. Moreover, it can be found that depending on the information to which it is intended to access, the IT world speaks about a fourth factor, “*where I am*”, and its usefulness, security and privacy are under discussion.

Further than digital inclusion policies and the path started towards the “*Open Data*” and the “*Open Government*”, there is no doubt that the axis of every administration, its support and service are centred in citizens, the care of them, their protection, their education and their opinion. For this reason, including them socially, including them digitally and recognizing them univocally protecting their cyber identity it is not an alternative but an obligation.

Identification, biometrics and the biometric pyramid

It is very important to understand that the validation methods applied for known users and dealt with in various documents along different times in human evolution were based on digital security, protection by a key (something that I know) and a device (something that I have) that “*authorises*” the possessor to have access to a system, for example.

When speaking of a third factor, the biometric factor, certainty is higher but “*of whom?*” As an example and briefly, we are going to describe the paths followed by an Argentine citizen in line with current legislation.

Every individual is born with biometric patterns (e.g. fingerprints, plantar prints), then that plantar print is recorded in the hospital (plantar print of the new born) and his or her parents, tutors or person in charge report it to the National Citizen Registry, through its corresponding offices, declaring the name they give to him/her, and where he/she is given an identity number and in turn he/she receives a legal entity materialized in a National Identity Document that entitles him/her, if needed, to request social and sanitary assistance, among others, within the competent legal framework.

At school age this identity document is renewed for the first time, and now, bearing a facial photo, the new Identity Document is issued with the first biometric identifier (facial photo) associated to biographical information (First names, last names, etc.).

As of 16 years old, the third Document is issued, now including fingerprints that enable to check through automated fingerprint identification systems that those fingerprints are univocally

associated to the identity document, facial image and first and last names.

$$\text{NAMES} + \text{NUM_IDENTITY} + \text{BIOMETRICS} = \text{IDENTITY}$$

From the last step on, that citizen is associated to a unique identity in the universe of registers of individuals that the Government has for identification purposes.

Then, going back to the query posed above, it can be said that we have to VERIFY the citizen's identity through the comparison of any of the biometric factors that the Government possess, against those submitted at the moment of requiring this information, thus attaining the certainty sought for.

At this point, it is necessary to go deeper into some definitions that are merely for information purposes and substantially necessary for a correct interpretation of the statements, and based on what Don Arturo Jauretche defined, our intention is that the language used be free of "nonsense".

When speaking about **biometrics**, it is about those unique and measurable identifying features that an individual has. Fingerprints, iris conformation, face configuration, particular features that are intrinsic to that individual. The other features, such as first and last names, are imposed by the individual's parents; the individual's identity number is assigned by the State; but biometric features belong to that individual since in the womb.

When speaking about **registering** an individual, also known as "enrolling", it is when at the moment of identification no identical record is found in all records, so those biometric records are added to the existing ones.

When speaking about **identity**, within the biometric framework, it is referred to a bi-univocal association or of a univocal correspondence (the first one refers to the other, and the latter to the first one with no ambiguities and unequivocally) between an individual and his/her biometric records, which are given (registered) after a verification that there is no one with identical biometric patterns. In other words, and as an example, "*this print belongs only to an individual and only that individual has that print*".

When speaking about verifying the biometric identity, it is said that that individual is in the records and the registered biometric particularities are compared against those that the individual presents; if they match there is a positive verification.

Having explained this, it still has to be mentioned that there is no biometric method that is not vulnerable to tricks or actions of human nature (e.g. diseases or accidents) or at least cheated if usability and security conditions are not taken into account. We are not pretending to make this text a manual for biometric identity theft but to show that biometrics is not a "silver bullet" that is a solution in itself or that acts to the detriment of the other measures to be taken into account, but it only acts according to what it is, a tool that facilitates, speeds up and ensures an identity.

For this reason is that we actively participate in the elaboration, debates, proposals and votes in

NIST (National Institute of Standards and Technology - USA), to gain more knowledge on the issue of biometric standards and to be able to express our position on this respect.

We have to bear in mind how much quicker it would have been the work of “Mothers and Grandmothers of the Plaza de Mayo” to find the children and grandchildren of their disappeared relatives during the military regime in our country, if they had had more biometric records and methods in the database with automated identification verification systems that collect this information in an inviolable manner.

The point is that now to ensure a biometric identity one method is not enough (for example only fingerprints) but what has been called “*the biometric pyramid*” has to be considered.

The Biometric Pyramid

Human beings since their origin, that some researches date back to the old Chinese dynasties or at least “before Christ”, have been using fingerprints as an additional element to “sign” their work of art or possessions, allowing the verification of this fingerprint against the ones of the individual who was claiming authorship or property.⁶

A fingerprint is undoubtedly the most effective biometric method in the history of humanity, as up to now, and considering the hundred million automated fingerprint records in the world, there has not been found one single fingerprint identical to another individual’s fingerprint, not even in the same individual.⁷

If static biometric methods (because there are also dynamic ones or also called behavioural) are represented by chess pieces we could say that the “Queen” would be the fingerprint. As in other methods, its qualities of being perennial (since the moment they are formed they are kept invariable in number, position, shape and direction), immutable (they do not mutate, since they are formed at the sixth week of intrauterine life they do not change and they regenerate to their original design) invariable (they cannot vary and also, depending on the cut produced by an injure, they either regenerate or the design is invalidated by the scar, but their shape does not change) and diversiform (they are all different), they are given supremacy over other identification methods, moreover on the base that in crimes the biometric elements (traces) are the most found. Nevertheless, it has to be taken into account that there is no religion or “uses and customs” that oblige an individual to wear gloves or to cover them, for which a fingerprint is the most exposed identification elements in everyday life.

Being able to approach the highest accuracy degree is a matter of usability, practicality and statistics. For this reason it is not necessary to add any other biometric methods for not being essential nowadays.

Following with the chessboard, although the “King” could be the DNA (Deoxyribonucleic Acid) for its accuracy, and in security issues by the elements found as “traces”, it also has some resistance in privacy aspects and sample handling as well as its use that, in some countries, is

only applied for sexual-related crimes or to claim paternity or family relationship, having to add the cost of the analysis and the time involved.

The Rook, we should say, would be the facial record. Although a lot has been said about biometric records and about which ones would be private or public, here there is a problem when pretending that the face is of “public” access only because a great portion of human beings displays it all time. And what would happen with those who for religious or cultural reasons cover their faces with an element that blocks it or makes it difficult to register? What happens when the luminosity, angle or background does not satisfy the quality of the sample and so it does not comply with the international standards on this issue? For these reasons, is that the facial record, in the past considered as a universal biometric solution, it is only another element to be used but not as the primary key of a biometric record. The field work carried out shows many marginal experiences, many intents of plagiarism not only with high similarities in faces further than the identical twin brothers but with ethnics that attain a high degree of similitude; also the flaws in capturing quality have to be added. It is also worth mentioning that successful experiences have been reported thanks to a strict acquisition of facial images in enrolling environments with controlled position, luminosity and background, but this is not common in all cases.

At last, for its versatility, availability, amount of information and quickness to compare, we would say that the Bishop would be the iris. Its usability in identification control in travel documents and immigration and access controls provides not only reliability but speed and quickness in the process. The Standard that rules the conditions for its acquisition is complied with by various vendors and it can already be seen successfully implemented in various places. Undoubtedly, it is a tool for identity validation. But there is always a “but”, it is disregarded by those who pursue crime samples as iris records “are not left” in crime scenes, while facial images are left in video or photos, and as already mentioned, DNA, fingerprints, plantar and palmar prints leave traces.

As it can be seen, fingerprint, facial, DNA and iris records are the biometric data available with which to record an individual in order to custody and keep his or her unique identity. But all of them, depending on current legislation, their manner of acquisition, and other factors, can be cheated. The implantation of a moulded fingerprint, the photo image of a facial record and also the construction of an eye globe with an iris record with infrared ink have been part of the maturity tests of the automated biometric systems to comprehend the limits and scopes in their use, procedures and processes. All and every one can be used effectively depending on the environment where they are done, their combination and other factors that allow to increase as much as possible their efficacy.

Here the reason for the Biometric Pyramid can be dealt with.

An individual’s biometric record involves procedures and processes that “require” the individual to move to a certain place, to fill in forms and in some cases to pay for the administrative

⁶ <http://www.applied-biometrics.com/spanish/tecnologia/huella-dactilar/posicion-del-desarrollo.html>

⁷ Introducción a la Biometría por huella dactilar, Tecnologías Biométricas de Identificación,
<http://www.algdrainvac.com/PRESENTA-TECNOBIO-TB-distribuidores-2.pdf>

procedures started. What about recording more than one biometric element to protect that individual's identity? What about recording the iris apart from the fingerprints and facial image? In this way incumbency government agencies could offer different forms of validating the identity and moreover, it could turn it more accurate and less feasible to theft when more than one biometric data is required to verify, for example, facial plus iris, iris plus fingerprint, etc.

In this manner a triangle of biometric data is constituted (*dactyl-facial-iris*) with which the individual, in different situations and circumstances will be able to assert and certify his or her biometric identity. Now then, what gives this triangle the dimensionality is the DNA as its record (*on the occasions allowed by the Law*) will provide the last biometric data to explore.

These four biometric aspects constitute each of the planes of a pyramid where its vertex achieves that in every occasion, registration, verification for administrative procedures, accidents and acts related to security, among others, the citizen and the State have the tools with which they can assert their rights and obligations in an effective and quick manner integrating every individual and including him or her socially and equitably to his or her pairs.

Ciber identity

Today we live in a digital world, and it is true that the "*Internet*" has grown as a big bazaar. Nevertheless, every bazaar has codes, structures and rules. The Internet is not the exception. Domains, class subdomains, protocols and others integrate the organization of these huge communications channels that brings frontiers closer and provides freedom of participation and opinion.

The Internet was born with one objective: to interchange information and to share knowledge. But it exceeded its own clients, from an "*elite*" it turned to be the popular tool it is today. And for being the main tool of the "*digital democracy*" we have to know and spread its risks, facilitate its use making it usable and accessible for everybody and to establish the mechanisms to take care our ecosystem.

To protect this tool, it would be necessary to define what supports it and what constrains it. From the technological point of view we further have to define projects to ensure sustainability and to ensure its usability and accessibility, its "*service qualities and its guarantees*".

To this regards it is worth mentioning that, as it is of public knowledge, the access to the "*Internet*" has increasingly become more critical to the sensitiveness of its use and contents, as well as to the communications, transactions, administrative procedures, and on-line banking strategies, among others, and this demands the development of a protection framework of "the Network" and of the most important material it possesses, WE the persons.

The technological aspect is being taken care of and strengthened, as it was mentioned above, from various layers; from the electronics, communications and data centres, undertaking the "*Policies of Datacenters Qualifications*" that integrate part of the efforts for "Protection of Critical Information Infrastructures" and the "*Argentina Connected*" project. But, what about the users?

Already in 2010, the Chief of the Cabinet Office announced and implemented the site named “*Healthy Internet*” in order to promote knowledge about the “*non careful*” use of the Internet, in order to alert parents and/or tutors on the need to be involved in this world together with their children. But there is still more.

In this “*cyber world*” there are issues that have to be taken into account and where the real and the virtual world have a common nexus, THE USER. The use of digital technologies (e-x) in the citizen-government, citizen-citizen relations and other digital relations, with similarities to the classes of relation and electronic commerce, turn it necessary, more than ever, to protect our identity.

For this, two basic principles have to be understood: the right to be “*anonymous*” and the right to have a “*reliable digital identity*”. The first one is referred to the fact that an individual who accesses these technologies shall have the freedom to access the information that these provide with no need of being “traced”. That is, except that the individual violates any Law, the digital individual has to be free to surf, express him/herself and to communicate in the virtual world having his privacy protected. Now then, with respect to “*sensitive data*” the individual has the right to have a “*reliable digital identity*” where he or she and only he or she can claim access to his or her data, processes or administrative procedures being ensured that no other individual, with no right on these data, may obtain them.

In the first months of 2011, it was publicly known, in different parts of the world over eleven thousand millions of data about individuals worldwide, containing names, addresses, credit cards and associated subscriptions, and even health records were put at risk.

To this effect, and in different latitudes, there are projects being carried out to ensure a reliable, interoperable and standard structure so that citizens can access to the information that the State has about them in a digital and reliable manner, being this one of the characteristics of an efficient and effective E-Government.

From what was mentioned, there emerges the need to have triple factor tools in the interaction of individuals with their pairs, businesses, organizations or governments.

Adding up keys to elements with reliable electronic signature (PKI) and to biometric data will bring about a reliable identity ecosystem, an initiative that can be adhered to by governments, organizations that promote standards and companies that validate identities in the cyber space.

As it has been stated, year 2011 finds us harvesting those seeds that have been planted since 2003. Social inclusion, digital inclusion, education with IT equipment and tools, the generation of digital contents, the open and free digital television, free Wi-Fi hot-spots and the extension of Optic Fibre that allow integrating the whole Nation in a huge network of communications and where distance is not a problem to share information, give free opinion, convey ideas and participate actively.

From the Federal Government there are projects already accomplished, others under progress and there will more in the future aiming at eradicating the digital divide to be able to attain

the highest percentage of implementation of those issues repeatedly announced such as E-Government, Open Government, Single Point of Contact, Paperless Procedures, among others and all those new initiatives to ensure a legal framework for all the actions posed.

Conclusion

Along this 2003-2011 government period, the objectives posed have been attained strengthening the State with the implementation of highly complex technological projects in the Federal Administration and the use of technologies in identity and security policies.

Our mission is to care for our citizens' needs, to understand expenses as an investment through measurable and tangible results in our society.

Our path is to continue incorporating tools to ensure identity processes and use in any of its forms. To strengthen the biometric tools that are implicit in every link of the chain, situation and procedure that improve citizen welfare.

Trying to exceed simplifying and linear schemes that, in general, relate the issue of identity only to the environment of security forgetting all that identity provides an individual as a person, as a social being.

Our goal for 2016 is to attain total digital inclusion as a corollary of social inclusion.

It is necessary to include biometrics in the tools that generate and help Argentine and the world's social reality, working not only with the affected groups, but also with lawyers, journalists, technicians, officers from diverse governments and organizations, undoubtedly, to attain the most diverse opinions and to promote the highest institutional quality and to support this new social pact where citizens are participants and main actors in an open, egalitarian and effective government.

Standards and Biometrics

Bradford Wing



Bradford Wing

Coordinator of Biometrics Standards NIST (National Institute of Standards and Technology)



Bradford Wing has been working in the field of biometrics since the beginning of the 1990's. He joined the National Institute of Standards and Technology (NIST) in 2008 after 20 years of career in the Department of Homeland Security (DHS), US-VISIT Program and in one of its predecessors of the DHS, the Immigration and Naturalization Service. In NIST Brad is the Coordinator of Biometrics Standards, responsible for conducting the ANSI/NIST-ITL standard development and providing support on this technology to other federal agencies. The ANSI/NIST-ITL is the standard used for the transmission of biometric data and related information used by security forces and institutions both, in the EEUU and internationally. He actively participates in these institutions where the biometric standards are developed, OASIS, INCITS/M1 and ISO/SC37, among them.

We worked as the Chief Biometrics Engineer in the US-VISIT Program of the Department of Homeland Security. There he founded the Biometrics Coordination Group that holds the diverse components of the DHS to ensure a coherent approach to biometrics in the whole department. He has also been the technical representative for the EEUU at the International Civil Aviation Organization (ICAO) in the development of Electronic passports, coordinating the execution of the interoperability and conformance tests.

He also served as Co-President of the National Science and Technology Council's Subcommittee on Biometrics and Identity Management, which gathers the representatives of the different governmental institutions of the EEUU to coordinate research on biometrics and standards for its implementation.

Abstract

This paper addresses the importance of standards when implementing or using biometric systems. Standards have been developed to ensure that biometric systems can effectively and accurately meet users' needs such as protecting data integrity, privacy, and security. Examples are given to illustrate the problems addressed by standards in 18 aspects of biometric systems, such as biometric data capture, data transmission, and human factors. The principal standards used in the biometrics community are described and gaps in biometrics standards coverage are identified.

Submitted to: Congreso International de Biometría de la República Argentina (CIBRA), "Biometrias II" as an invited contribution.

Standards and Biometrics

1. Why have a biometric system?

The basic reason to have a biometric system is to verify the claimed identity of a person or to discover the identity of a person. A biometric system is designed to provide an answer to one of the following questions:

Is the person who he claims to be?

- a. *Verification (1 to 1 comparison)*: I have a passport with my facial image stored on the chip contained in the passport (an e-passport), and I claim that the e-passport was issued to me. I can use the 'facilitated travel inspection lane' successfully only if a picture taken of me at the kiosk matches the facial information stored in my e-passport.
- b. *Identification: (1 to many comparison)*: I am an employee at a factory that uses iris recognition to grant entrance to the facility. I can only enter if my iris image matches one in the database.

Is the person not who he claims not to be?

- c. *Negative verification: (1 to 1 comparison)*: I have been accused of a crime and I provide a DNA sample to match against the DNA¹ recovered from a crime scene. I am able to show that I am not the person whose DNA was left at the crime scene if there is no match.
- d. *Negative identification: (1 to many identification)*: In a certain nation, all persons that are deported have iris data captured at release. I arrive at the country's airport, have my iris scanned and can enter if my iris does not match one in the deportation database.

Can the person be identified, given the information in the system?

- e. *Identification*: An Alzheimer's² patient is found wandering the streets. A fingerprint is taken from the person at a nearby police station, and it is compared against a database of missing persons. The print matches one in the database and the person is identified and returned to the family that had filed the missing person report.
- f. *Classification*: Part of a body is found at a disaster site. A DNA sample is collected from the body and compared to DNA from possible relatives. In this case, the claimed relative is an uncle to two of the victims, and he provided a DNA sample. A match occurs for his mitochondrial DNA³ to that of both of the victims. This means that the claimed relative and

¹ DNA is an acronym for deoxyribonucleic acid. It is a chemical that forms a double helix, which is unique for all persons except identical siblings, for whom it is the same.

² Alzheimer's disease is the most common form of dementia. It is incurable.

³ Mitochondrial DNA are small circular DNA molecules located in structures used to provide energy to the cell (mitochondria). Their small size and abundant nature make them particularly useful when examining small or severely damaged biological material. It can be used to trace maternal lineages as it is only inherited from one's mother.

the two victims all have a common maternal ancestor. Mitochondrial DNA is only passed to a child from the mother. In this case, the common maternal ancestor is the grandmother, as shown in Figure 1. Positive identification of the corpse could not be established because the body could have belonged to either Victim 1 or Victim 2, but the body is classified as being one of the two cousins, to the exclusion of all others.

Note that if the claimed relative (the uncle) had been a brother of the fathers of the victims, as shown in Figure 2, then the mitochondrial DNA test would not have revealed any usable results. If the uncle had been brother to a mother of one victim and father of the second, as in Figure 3, and there was a mitochondrial DNA match of the corpse and the uncle, then positive identification of Victim 1 as the son of Mother 1 could be established.

Figure 1. Family Tree A

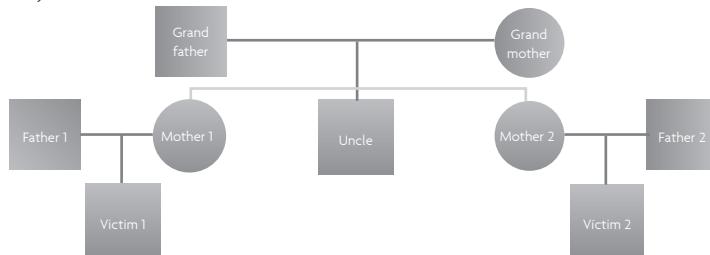


Figure 1. Family Tree B

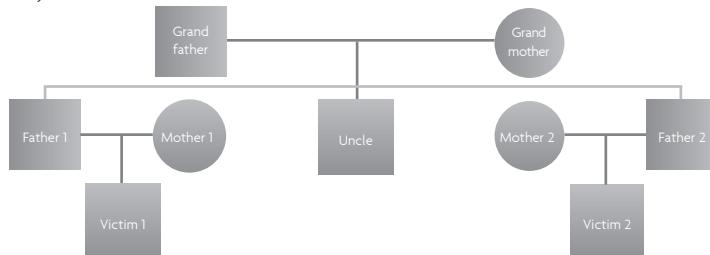
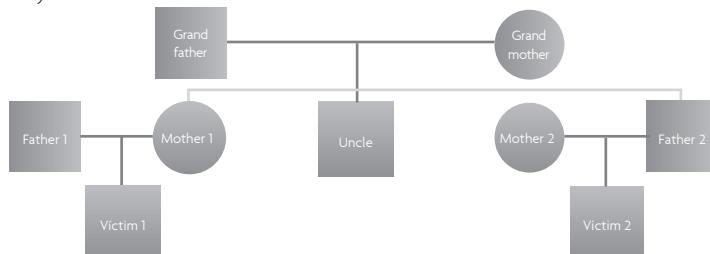


Figure 1. Family Tree C



There are many variants on the above uses for biometrics, but they all have in common the fact that people rely upon the system providing a level of assurance that the result is correct.

A deployed system must take into account operational and cost constraints. Operational constraints include policy, legal, data integrity, security and privacy protections, interoperability with other systems, ergonomic considerations, environmental conditions, and many other factors. The data collected, stored, transmitted and used in a biometric system should:

- maintain fidelity to the biometric characteristics of the subject (the person providing the sample);
- describe the collection environment and procedures; and
- describe pertinent facts about the subject.

In addition, the system should:

- have a high degree of reliability, with
 - false match and non-match rates that are within tolerable ranges⁴,
 - mean time between failure (MTBF⁵) that is acceptable, and
 - maintenance requirements that are reasonable⁶; and
- appropriately protect the subject's data.

2. What is the need for standards?

In order to help ensure that a biometric system is accurate, meets the system owner and user needs, and is able to interface with other systems (where appropriate), standards developing organizations (SDOs)⁷ have created standards that can be incorporated into system design and standard operating procedures. Experts in the field, from government, academia, and private industry developed these standards. As a result of implementing standards in a biometric system's design, the system is less likely to be tied to a 'proprietary solution' of a specific vendor. Proprietary solutions can result in much higher costs, and possibly result in system failure if the vendor ceases to support the product. Failure to adhere to standards can also seriously degrade the integrity of the system. '*Application profiles*' are based upon published standards. An organization tailors the standard to its particular requirements. An optional data field may be required for a particular type of application. Certain options allowed in the standard may be inapplicable to the needs of a particular organization. For instance the US Federal Bureau of Investigation (FBI), the US Department of Defense, the Royal Canadian Mounted Police, the Government of Argentina, INTERPOL, and others have developed application profiles of the standard "Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information" that is commonly called the ANSI/NIST-ITL standard⁸.

⁴ What the tolerable ranges are is a key decision of the system owner.

⁵ The MTBF is dependent upon the system owner's definition of a failure.

⁶ Some maintenance requirements can involve cleaning a fingerprint platen after every use. Battery replacement for mobile units is part of maintenance, so battery life is an important consideration. The system owner defines 'reasonable.'

⁷ Section 4 describes the SDOs and standards that they have developed that are particularly relevant to the biometrics industry.

There are also ‘Best Practice Recommendations’ (BPR) that describe the most appropriate selection of options and appropriate standards for various types of operational scenarios. An example is “Mobile ID Device Best Practice Recommendation Version 1.0”⁹.

Not every step in a biometric system requires a standard. Many things can be addressed by “Standard Operating Procedures” and even common sense. However, there is a strong need for standards for certain parts of biometric systems, due to the severe impact that a failure to use a common format or procedure can have.

An operational (or designed) biometrics system can be discussed by examining it from different perspectives. Not all of the perspectives are relevant to every transaction or each biometric system. The key perspectives are addressed below using examples. They are not listed in order of importance or processing order within a system.

A) Biometric sample collection

Facial recognition algorithms work best with a full-frontal image. There is deterioration in the rate in recognition as the face moves away from the full frontal position. That is why passport facial pictures are required to be a full-frontal pose with a neutral expression, which has been formalized in the standard for international travel documents of the International Civil Aviation Organization (ICAO)¹⁰. Kiosks have been designed to capture full-frontal facial images in facilitated travel installations such as RAPID¹¹ in Portugal and SmartGate in Australia¹².

B) Associated metadata recordation

When a set of fingerprints is captured from an individual, it is important to label each print to indicate from which finger the image was captured. Large fingerprint systems may compare fingerprints only against those labeled as the same group (such as whorl) for a particular digit (such as index finger of the right hand). If there is no label, the systems may have to compare against all of the fingerprint images that have been stored – a costly and time-consuming process that increases the risk of error. Thus, standards like ANSI/NIST-ITL 1-2011 have fields that allow the entry of information associated with a fingerprint image, such as the finger position and the method of capture of the print (for example, rolled ink prints or livescan units).

In the ‘classification’ example described in Section 1.0, the metadata is extremely important. If the uncle were possibly related to the victims as shown in Figure 2, then a mitochondrial DNA would not have been run. An entirely different test (Y-Short Tandem Repeat¹³) would have been used.

⁸ ANSI/NIST-ITL stands for American National Standards Institute / National Institute of Standards and Technology, Information Technology Laboratory. This means that NIST-ITL is accredited by ANSI as an SDO. ANSI/NIST-ITL 1-2011 and its predecessors are available at http://www.nist.gov/itl/iad/ig/ansi_standard.cfm. It is available in English only.

⁹ The BPR is available at <http://www.nist.gov/itl/iad/ig/mobileid.cfm>. It is available in English only.

¹⁰ The ICAO travel document standard, Document 9303, is available at <http://www2.icao.int/en/MRTD/Pages/Document9303.aspx>. It is available in Arabic, Chinese, English, French, Russian and Spanish.

¹¹ RAPID is a Portuguese Acronym for the phrase “Automatic Identification of Passengers Holding Travelling Documents”

¹² See Frontex technical report No 1/2010 “BIOPASS II, Automated Biometric Border Crossing Systems Based on Electronic Passports and Facial Recognition: RAPID and SmartGate” It is available at http://www.frontex.europa.eu/gfx/frontex/files/other_documents/biopass_II.pdf

¹³ Short tandem repeats (STR) are short sequences of DNA that are repeated numerous times in direct succession. The number of repeated units may vary widely between individuals and this high degree of variation makes STRs particularly useful for discriminating between people. The Y-chromosome is only in males.

C) Retrieval of biometric data to compare against

When a biometric sample (called the ‘probe’ sample) is sent to a large-scale system, the probe may be compared against a subset of the entire database, called the target set. This target set may be selected based upon characteristics of the biometric data as well as its metadata, such as the sex and approximate age of the subject. If the accompanying information is incorrect or incomplete, as described in B) above, the target set may exclude the data associated with the correct identity in the database, causing a match not to be possible.

Some systems retrieve the target set from a ‘token’ such as an identification card with a chip embedded in it, or an e-passport. The target set in this example consists only of data for one person, the owner of the identifying document. In order to ensure that the token is properly used and that the biometric data on the card is only available to authorized systems, there is typically a control system built into the token. In the case of the identification card, the owner may enter a personal identification number (PIN) that authorizes access to the chip. For an e-passport, the information printed in the ‘machine readable zone’ on the data page is scanned and used to generate a ‘key’ to open the chip. Only then can the biometric data be retrieved.

The examples above illustrate different aspects of target set creation. Standards affect biometric systems in different ways.

D) Non-biometric factors affecting the biometric system

This is a very broad topic, and may result in the incorporation of other ‘non-biometric’ standards into a biometric system’s specifications. As an example, the ICAO standard for travel documents incorporates the ISO standard for optical character recognition, format B (OCR-B)¹⁴. The information stored using OCR-B printing on the ‘information page’ of the passport is used to generate a ‘key’ to open the chip contained in the e-passport in order to read the data stored on it. Without this key, the data cannot be read. This was done to ensure that the data on the chip could not be ‘skimmed’ by equipment in proximity to the e-passport without the information page being deliberately presented in close range to the authorized e-passport reader.

E) Sample quality analysis

The quality of a biometric sample dramatically affects its usefulness. This applies to both the probe and the target set. If a fingerprint is smudged or if there was not enough pressure applied when it was captured, there may not be enough distinguishing features, such as minutiae, to enable a system to accurately match the sample against other samples. Automated quality analysis of the captured sample can be built into a capture device and provide feedback to the operator. For instance, the US-VISIT program¹⁵ and United States ports-of-entry check the quality of the fingerprint captured at the time of capture. Up to three samples are collected and analyzed automatically by the system, and the best one is

¹⁴ ISO 1073-2:1976 is available at http://www.iso.org/iso_catalogue_detail.htm?csnumber=5568

¹⁵ Document “Biometric Standards Requirements for US-VISIT” is available at http://www.dhs.gov/files/programs/gc_1213298547634.shtm

used. The operator also has the option to re-take the fingerprint of the traveler if the quality is of a poor level. The quality level of the fingerprint is stored with the fingerprint.

F) Initial data storage

The method and process of data storage, if done improperly, can negate the usefulness of a biometric sample. For instance, when a fingerprint image is taken, it should be stored with at least 19.69 pixels per millimeter, which equates to 500 pixels per inch (ppi). [1000 ppi is recommended for latent prints]. Compression algorithms are used to reduce the original image for more efficient storage and transmission. Certain compression algorithms, such as JPEG¹⁶, were not specifically designed for fingerprints. JPEG forms squares across the image and compresses each square individually. When they are reconstructed, it is possible to introduce ‘artifacts,’ such as small line segments along the edges of these boxes. That is a real danger for fingerprints, since these artifacts could be interpreted as minutia and may cause a false match to occur or a valid match not to occur. A compression algorithm optimized for 500 ppi fingerprint images, called Wavelet Scalar Quantization (WSQ), is used to store those images. There are specifications for WSQ¹⁷. Vendors have developed different versions of software that does this compression.

Fingerprints are submitted, for instance, to the US FBI from state and local police departments using a variety of implementations of WSQ. NIST validates these algorithms against the specifications. The FBI then publishes a list of approved vendor products for WSQ for use by law enforcement organizations when submitting fingerprints to the FBI.

G) Transmission to another location

The application of biometrics is not confined to one specific location. The capture of a biometric sample can happen at one location, and the matching of it against a database can be performed at a different location. The process of transmission must be clearly specified to maintain the integrity of the data.

For instance, there was a governmental fingerprint system that appeared to be well designed. Upon examination, the overall process was flawed. The original fingerprint image was stored in WSQ. Then it was decompressed, printed, and faxed to another site. At that location, the printed image from the fax machine was compressed in JPEG and transmitted to the central site, where it was decompressed and re-compressed using WSQ. The original sample was stored using WSQ and the final image was also stored in WSQ (so they could claim compliance with the recommended capture and storage compression procedures), but the fingerprint data had effectively been destroyed by the multiple format conversions during the steps of the transmission.

Many forms of compression are ‘lossy.’ This means that a certain amount of information contained in the original image is lost during compression. When decompressed, the resulting image will not be as detailed as the original image. For fingerprints, this can have extremely negative results.

¹⁶ JPEG is an acronym for the Joint Photographic Experts Group. They created the standard, which is: “JPEG File Interchange Format, Version 1.02 (JFIF).” It is available at <http://www.jpeg.org/public/jfif.pdf>

¹⁷ IAFIS-IC-0110 (V3.1) “WSQ Gray-scale Fingerprint Image Compression Specification, October 4, 2010” is available at <https://www.fbibiospecs.org>

To address this problem, the ANSI/NIST-ITL 1-2011 standard states: “*Images shall be compressed only from an original uncompressed image. If an image has been received in compressed format, it shall not be uncompressed and re-compressed in the same or different format.*”

H) Comparison of the probe to the target set

The actual comparison of biometric information may be automated, partially automated, or manual. Automated fingerprint matching systems typically rely on a specified set of features within the fingerprint. The need to standardize the encoding of these ‘fingerprint minutiae’ for use by multiple matchers was recognised very early. In 1986, the first version of what eventually became the ANSI/NIST-ITL standard addressed fingerprint minutiae with the goal of ensuring that law enforcement organizations would be able to send information to one another without extensive re-coding of the data.

However, forensic examiners must rely upon more types of information than where ridges end and divide (bifurcations), which form the basis for minutiae. They must also be able to state their findings in a way that can be understood years later by other examiners. This led to the development of the Extended Feature Set, which is now incorporated into the ANSI/NIST-ITL 1-2011 standard. Forensic examiners can now specify in a fixed manner features such as the location of pores, the number of ridges in an area and other important characteristics. Fingerprint examiners in other locations, and perhaps separated by time, can refer to these features in a way that could have very important results in criminal prosecutions.

I) Biometric sample and metadata storage

In many applications, there is a requirement to use a minimum amount of space. An example is biometric data stored on an identification card used for building access. The data used by iris matchers can be stored in a very efficient manner (in some cases in as little as 3 kilobytes). This has been demonstrated through research conducted at NIST¹⁸. This analysis also found that one form of compact storage (polar format) resulted in degraded performance. The ISO and ANSI/NIST-ITL standards now both allow the ‘crop and mask’ format that has been shown to retain fidelity to the original biometric sample yet simultaneously reduce storage requirements. In order to maintain system accuracy, both the ISO and ANSI/NIST-ITL standard do not allow iris data to be stored in the ‘polar’ format.

J) Reporting and use of comparison results

The output of a biometric system is not necessarily a ‘yes’ or a ‘no.’ A probe of a biometric will always have slightly different characteristics than data in the target set, so a ‘match’ is never exact¹⁹. In fact, if it is exact, then that means that the probe and the target set data are from the exact same sample, which should raise suspicions about attempts to compromise the system. In many cases, there is only one set of data in the target set that is ‘close’ in comparison to the probe. In other cases, there may be several sets of data in the target set

¹⁸ See <http://www.nist.gov/itl/iad/ig/irex.cfm>

¹⁹ It is possible under certain circumstances to have an exact match with DNA.

that are relatively similar to the probe. The presentation of results is generally not covered by standards. It is typically user-specified, based upon the system owner's requirements. For instance, the U.S. Department of State has a facial recognition system²⁰ used to verify that persons are not 'visa shopping' (applying at multiple consulates under different names in the hope that one application will be approved). The automated system provides a list of the 'best' matches of an applicant against the target set, which is comprised of previous visa applicants. A team of analysts then determines if there is a true or highly likely match.

Other systems, such as access control or computer activation (logical access control) require a yes/no decision. A 'threshold' is set for a match. That is, there have to be enough characteristics in common between the probe and the target set data. If that threshold is met, then access is granted. Since there is always a trade-off between false match rate and false non-match rate, this threshold may be different for different circumstances.

A nuclear facility will set the threshold such that access cannot be granted unless there is a VERY close match in biometric characteristics. This means that a person will occasionally be denied entrance even though they really are authorized for entry. That is why a backup procedure should always be in place for biometric systems. On the other hand, an amusement park using a biometric verification system for season pass holders does not want to inconvenience its customers. The amusement park will usually set a lower threshold and accept that some transactions could possibly be performed by imposters and recognised as authentic by the biometric system. As biometric systems improve, the same level of true match can be achieved with lower and lower levels of associated possible false matches. In the amusement park example, this means that the threshold can be increased while still maintaining the same level of service to the customer, and with an even lower level of loss of revenue through unauthorized use of season passes.

The reporting processes and procedures and the setting of thresholds are based upon specific user needs and usually take into account scientific studies on biometric system performance. However, this is not currently seen as an area for standardization efforts.

K) Database analysis

Database analysis is critical in order to maintain a reliable and efficient biometric system. Database analysis encompasses several things, such as review of data associated with the biometric sample, quality analysis of the biometric data, and possible weighting of the matching results based upon those quality values and several issues directly related to the efficiency of the data storage structure and retrieval mechanism.

One aspect of database analysis that is critical is '*database reconciliation*.' This can also be referred to as '*establishing ground truth*.' For instance, the U.S. Border Patrol can apprehend the same individual multiple times as he or she attempts to illegally enter the U.S. A subject will often give the same name upon subsequent apprehensions since there is a potential for being sent to jail (instead of simply being expelled from the U.S.) if multiple attempts at illegal entry are detected. When fingerprints are taken of the subject, they are compared against a central system (in this example, IDENT). A photograph of the subject is linked to the metadata for the apprehension and to the fingerprint sample. The Border Patrol agent

²⁰ See <http://www.nist.gov/itl/iad/ig/irex.cfm>

can 'link' two different claimed identities in IDENT based upon the results that are presented – thus establishing that at least two different aliases exist for the same individual. Note that it is also possible to unlink two apprehension records if it can be shown that they really do refer to different individuals.

L) Software and hardware reliability

This is an extremely complicated area. Several standards have been developed that apply to both biometric and non-biometric systems.

For instance, in the "Mobile ID Device Best Practice Recommendation Version 1.0" (BPR), there is a section that addresses environmental concerns. In the BPR there is a profile for law enforcement applications and a more stringent profile for military applications. A profile is a set of specifications. The BPR states: "It is the responsibility of the Agency to decide, in the procurement phase of the Mobile ID devices, which profile to request... It is important to choose the right profile since a lower profile could mean that the devices are not able to withstand the operating environment, causing costly failures and decreasing service levels, while choosing too high profile is likely to cause an unnecessary increase in the size, weight and cost of the devices."

For the different profiles listed in the BPR, standards are referenced that address testing of equipment for certain environmental conditions. An example is for the military profile, when testing for survival of mobile biometric devices at different operating temperatures: test using MIL-STD-810F Method 502.4 Procedure II at -20 degrees Celsius and use MIL-STD-810 Method 501.4 Procedure II at 60 degrees Celsius²¹.

Categories of testing include operating temperatures, storage temperatures, relative humidity, ingress protection (resistance to water infiltration), and drop resistance / shock tolerance.

M) System performance analysis

System owners want to have the best performing system that they can afford while being suitable to their operating conditions. System performance evaluations can assist the algorithm and biometric system component developers as well as the systems owners. By running algorithms and components in controlled tests, their relative performance can be evaluated.

An example is the Slap Fingerprint Segmentation Evaluation II²², run by NIST. It is an ongoing evaluation. Participants can submit their algorithms at any time to NIST. The concept is that certain fingerprint capture devices can acquire the images of four fingers at one time on a large platen. Then, the individual fingerprints must be 'segmented.' There can be several issues that complicate the segmentation, such as rotation of the hand on the platen, fingers being very close together, 'ghost' images of prints from residue on the platen, smudged or light images of individual fingers, missing fingers, and heat 'halos' around the prints.

²¹ The US Department of Defense test method standards for environmental engineering are available at <http://www.dtc.army.mil/navigator>

²² See: <http://www.nist.gov/itl/iad/ig/slapsegii.cfm>

N) Legal and privacy impact analysis

The expectations and requirements for legal, cultural and privacy protection vary considerably in different jurisdictions. Regulation and SOPs to address these concerns are often written at the jurisdictional level, rather than formalizing the requirements into standards, due to these varying expectations and requirements.

For example, certain travelers, for cultural reasons, may wish to keep their face partially covered. However, their uncovered face image must be printed in the passport, according to ICAO travel document specifications. In order to perform a comparison of the traveler to the image in the passport, many jurisdictions have established special procedures to bring the traveler to a special screening area.

O) Human factors / human interface design

Only recently have standards and best practice documents been developed covering this aspect of biometric systems .

This area covers such diverse topics as listed below. These are only a few examples and are not an exhaustive coverage of the types of issues²³.

- What angle should the angle of the platen on a fingerprint capture device be relative to the subject? At what height should the device be placed?
- What symbols (icons) on biometric devices are most easily interpreted across cultures?
- How can the camera best assist the photographer to ensure that the subject's face is centered and is at the proper distance from the camera?
- How can mobile fingerprint capture devices be designed so that they do not appear to be weapons to subjects, yet they can be operated using one hand by an officer?

P) Interoperability design

This is a major driver behind the development of biometric standards. Isolated biometric systems (for example, access control for a small company) usually do not have a need to send data to other sites. However, as systems become larger, or there is a need to exchange biometric data with other systems. A common data format and understanding of the content of the biometric data ensure its proper use and allow for effective use in another system.

One example is a 'first responder' scenario. At a disaster site, personnel from several different organizations may respond. However, unauthorized persons should not be within the disaster zone. Firefighters from one jurisdiction may have had their fingerprints enrolled in their employment database. Medical practitioners at a local hospital may have had their fingerprints enrolled in the hospital's database. If each system had been designed to store fingerprint data in a standardized format, then a mobile system at the disaster site could be loaded with the fingerprint data of authorized persons. This eliminates the need to submit fingerprint samples of persons accessing the site to multiple systems for verification.

Another example involves INTERPOL. INTERPOL has established a database consisting of fingerprints of persons who are wanted for very serious crimes. The fingerprint data come

²³ Ver <http://zing.ncsl.nist.gov/biousa/> para estudios en human factors.

from a variety of government agencies all over the world. Only because biometric standards are in place and used, can these prints be used by other agencies around the world to determine if they have encountered an individual in the INTERPOL database²⁴.

Q) Certification of biometric products, system testing laboratories, and testing procedures

When procuring equipment, system owners need to be assured that the equipment will work and will meet requirements. In the procurement process for large systems, the system owner can test the different vendor products in simulated conditions prior to making a purchase decision. However, such extensive testing is often too costly and time-consuming for smaller purchases.

The types of tests and the methods of performing those tests have become a focus for standardization activities. NIST has established the Biometrics Laboratory Accreditation Program²⁵. It is designed to verify that those laboratories that perform conformance tests, interoperability testing, technology testing, scenario testing, and operational and usability testing for biometric products follow nationally and internationally recognised biometric testing standards.

R) Security (information assurance, liveness and fraud detection.)

Certain aspects of security, such as information assurance, have several standards applicable to biometrics systems. These include encryption, hashing, digital signatures, and more.

The ICAO established a modified version of public key infrastructure (PKI) for use in e-passports. There is a document-signing certificate that verifies that the data have not been changed since it was written to the chip in the passport; this, however, does not guarantee which organization wrote the data to the chip. A country-signing certificate is also used in e-passports. The key to read the country-signing certificate is shared at the national level. If both certificates are valid, then the information on the chip in the passport can be considered genuine. Other types of checks must be performed to ensure that the printed data on the passport has not been altered.

Research into liveness detection and fraud analysis is underway at several universities and private companies. This involves detecting, for instance whether the biometric sample being captured is from a live subject and from the correct subject. For example, some fingerprint sensors may have heat-detection or vein-detection capabilities to help ensure that the subject is alive and that a severed finger or an artificial finger has not been presented.

Note that certain scenarios do not require or want liveness detection, such as when taking fingerprints from deceased individuals in order to identify a corpse.

3. What standards exist and how are they used?

Biometric standards were developed to meet specific needs of communities of users and to reflect the vastly different technological requirements inherent to the biometric modalities, such as DNA and facial recognition.

²⁴ La implementación de INTERPOL de la norma ANSI / NIST-ITL está disponible en <http://www.interpol.int/Public/Forensic/fingerprints/RefDoc/ImplementationV5.pdf>

²⁵ Ver: <http://www.nist.gov/pml/nvlap/nvlap-bio-lap.cfm>

Biometric systems may need to also rely upon other standards that were developed for a broad range of applications – such as the Federal Information Processing Standard 180, Secure Hash Standard²⁶.

The U.S. Government developed a publicly available list of relevant biometric standards. This “Registry of USG Recommended Biometric Standards”²⁷ has the following sub-registries:

- biometric data collection, storage, and exchange records;
- biometric transmission profiles;
- biometric identity credentialing profiles;
- biometric technical interface standards;
- biometric conformance testing methodology standards;
- biometric performance testing methodology standards.

The principal standards that are used internationally are:

- ANSI/NIST-ITL²⁸ Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information
 - Focused on law enforcement, military, intelligence, and homeland security applications
 - Application profiles developed for specific uses, such as:
 - FBI / U.S. police agencies
 - U.S. Department of Defense
 - Royal Canadian Mounted Police
 - Terrorist Watchlist Person Data Exchange Package
 - US-VISIT
 - INTERPOL
 - United Kingdom National Policing Improvement Agency
 - German Bundeskriminalamt
 - European Union Visa Information System
 - Western Identification Network
 - Covers exemplar and latent friction ridge prints (fingerprint, palmprint, and footprints); images of facial / scar / needle mark / tattoo / iris / other body part and distinguishing characteristics; forensic markups of fingerprints, facial images, and iris images; DNA; associated metadata; and, associated reference information, such as crime scene photographs.
 - Multiple modalities can be included in a single transaction
- ISO/IEC 19794-x (standards) and ISO 29794-x (conformance)²⁹
 - Oriented toward civilian applications
 - Large-scale implementations using face, finger, and iris standards, such as
 - The Indian Unique Identification card (UID)³⁰ and
 - ICAO specifications for e-passports.

²⁶ SHA-256 hashes are described in this document and are the basis for some of the data fields in the ANSI/NIST-ITL 1-2011 standard. The standard is available at http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

²⁷ See: <http://www.biometrics.gov/Standards/Default.aspx>

²⁸ See: http://www.nist.gov/itl/ig/ansi_standard.cfm

²⁹ The list of published biometric standards and standards under development in ISO is available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45020

³⁰ Unique Identification Authority of India, “Biometric Design Standards for UID Applications”. It is available at http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf.

- Covers several modalities and formats separately (finger minutiae, image, and spectral and skeletal pattern data; face image; iris image; signature / sign; vascular; hand geometry) for transmission and conformance testing
- CBEFF – Common Biometric Exchange File Format
 - Defines a set of 'header' information for a transmission
 - Allows the incorporation of biometric data and metadata conformant to several standards
- INCITS 381 (fingerprint images), INCITS 378 (fingerprint templates), INCITS 385 (facial images)³¹
 - Developed as US standards prior to the publication of the ISO/IEC 19794-x international standards
 - Used by the U.S. Government for the Personal Identity Verification (PIV) card³².

4. What still needs to be done?

Although standards do exist to address several aspects of biometrics systems, there are still gaps to be filled. Additionally, existing standards need to be updated to reflect the changing requirements of biometrics system owners and users as well as to reflect the results of research that has been conducted.

There are three principal forums that are currently developing and maintaining biometrics standards at the international level:

A) ANSI / NIST-ITL working groups.

ANSI/NIST-ITL has recently published an updated version (ANSI/NIST-ITL 1-2011). Work is already underway to enhance the standard. Three working groups are now established to address:

- Dental and bitemark analysis;
- Voice recognition; and,
- Conformance testing.

B) ISO / SC37³³ (Subcommittee - Biometrics)

ISO / SC37 has several projects underway. They include:

- Revisions to the existing standards;
- Voice recognition;
- DNA data; and,
- Pictograms, icons and symbols for use with biometric systems.

³¹ INCITS standards are available at <http://www.incits.org>.

³² PIV standards and supporting documents are available at: <http://csrc.nist.gov/groups/SNS/piv/standards.html>.

³³ Information is available at http://www.iso.org/iso/iso_technical_committee.html?comnid=313770

C) OASIS BIAS Integration TC³⁴ (Organization for the Advancement of Structured Information Standards, Biometric Identity Assurance Services Integration Technical Committee)

The following list is a sample of the topics under examination that may result in new or updated biometrics standards in one of the forums described above:

- touchless fingerprints;
- transformation of a 3-dimensional fingerprint data set to be compared against 2-dimensional databases;
- ear shape;
- gait;
- human odor;
- ocular biometrics: the region around the eye as well as the eye;
- near- and mid-wave infrared facial imaging;
- aging of the subject and of the biometric sample;
- detection of deliberate changes to a biometric characteristic, including
 - plastic surgery of the face or
 - mutilation of fingerprints;
- detection of liveness of the subject;
- anti-spoofing techniques;
- optimization of the design of large-scale biometric systems;
- appropriate use of 'soft biometrics', including
 - height,
 - weight, and
 - skin colour;
- multi-modal / multi-sample / multi-instance biometric data fusion;
- data quality analysis, at time of capture and once in the database;
- integration of other processes and procedures with biometrics, including
 - detection of facial micro-movements typical of deceit, and
 - artificial intelligence to assist forensic analysts;
- biometric system design for optimum performance by users and operators (usability and accessibility);
- new communication methods and capabilities; and
- dynamic decision making, including
 - automated or assisted modification of biometric system operational parameters based on current demands upon the system.

³⁴ Information is available at <http://www.oasis-open.org/committees/bias>

Conclusion

Standards are only meaningful if they are used. Standards will only be used if they serve a purpose and meet the needs of the biometric system owners and users. This is an ongoing process, but standards should remain stable enough that they can be effectively used over a period of years. Not all systems will be able to adapt to new standards at the same rate.

It is important for biometric system owners, developers, designers and users as well as researchers to reach out to the SDOs and participate in the development process.

For example, ANSI/NIST-ITL operates on the canvass method and is open to all interested parties. ISO / SC37 is organized around national body representation. Each participating national body establishes its own rules for participation, but they may be comprised of industry, government and academic experts. OASIS membership is open to all interested organizations.

It is an ongoing responsibility of SDOs to ensure that they have adequate representation from all interested groups in order to ensure that the standards that they develop are truly reflective of the community's needs and are simultaneously based upon solid scientific research.

The International Co-operation and Safety Initiatives in Individuals Identification and Verification using DNA or Fingerprints proposed by INTERPOL

Mark Branchflower / Jess Maltby



Mark Branchflower

Head of Fingerprint Unit, Interpol



Mark Branchflower trained at Scotland Yard from 1984 to 1990, in which year his expertise in the field was recognised. Qualified in numerous aspects of fingerprint work including: tenprints, processing of latent prints, crime scene evaluation and laboratory work. After six years with the Metropolitan Police, including one year in the Anti-Terrorism Fingerprint Unit, he applied for a position with INTERPOL.

He began working as a fingerprint examiner for INTERPOL in 1990, was promoted to Senior Fingerprint Examiner after two years, and in 2005 was appointed Head of the Fingerprint Unit.

For the past 17 years he has been involved in organising and participating on behalf of INTERPOL: in 6 INTERPOL Europe and International working groups per year; as President and organiser of INTERPOL Symposia on Fingerprints; at numerous conferences in more than 35 countries around the world; in the training of staff in the use of AFIS for DVI; as a member of INTERPOL's DNA working group; in the development of international standards governing the transmission of fingerprint records; and in the development and promotion of INTERPOL's AFIS services.

Currently his responsibilities include leading a group of six fingerprint specialists, the exchange and processing of matching information, promotion of INTERPOL's AFIS services, and keeping up to date at all times with the latest developments. Recently, he was named President of the Sagem International Users Group, which involves working with both the management of Sagem and the delegates of the group's member countries to achieve the best results possible from AFIS and to plan future developments.



Jess Maltby

Criminal Record Office (ACPO)



Jess MALTBY is employed by the UK agency ACPO Criminal Records Office (ACRO) and is currently assigned to the INTERPOL Fingerprint Unit with various projects to promote the use of the INTERPOL AFIS for a 6 month period.

Abstract

This paper has been written by Mark BRANCHFLOWER and Jess MALTBY, the information has been adapted from INTERPOL documents and includes subject working knowledge of the two persons in the Fingerprint area.

This paper will cover two of INTERPOL Forensic databases, Fingerprints and DNA and will look at how INTERPOL member countries can use these services and what benefits can be gained from them. The conclusion is a personal dream which we believe can become reality if all the concerned players in Forensics worldwide take the decision to respect the request of the Organization to populate and search the databases.

The International Co-operation and Safety Initiatives in Individuals Identification and Verification using DNA or Fingerprints proposed by INTERPOL

Introduction

INTERPOL is the world's largest international police organization, with 188 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.

INTERPOL aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. INTERPOL's constitution prohibits 'any intervention or activities of a political, military, religious or racial character.'

One of INTERPOL's core functions is to enable the world's police to exchange information securely and rapidly. The organization's I-24/7 global police communications system connects law enforcement officials in all 188 member countries and provides them with the means to share crucial information on criminals and criminal activities.

As criminals and criminal organizations are typically involved in multiple activities, I-24/7 can fundamentally change the way law enforcement authorities around the world work together. Pieces of seemingly unrelated information can help create a picture and solve a trans-national criminal investigation.

Using I-24/7, National Central Bureaus (NCBs) can search and cross-check data in a matter of seconds, with direct access to databases containing information on suspected terrorists, wanted persons, fingerprints, DNA profiles, lost or stolen travel documents, stolen motor vehicles, stolen works of art, etc. These multiple resources provide police with instant access to potentially important information, thereby facilitating criminal investigations.

The I-24/7 system also enables member countries to access each other's national databases using a business-to-business (B2B) connection. Member countries manage and maintain their own national criminal data. They also have the option to make it accessible to the international law enforcement community through I-24/7.

Although I-24/7 is initially installed in NCBs, INTERPOL is encouraging member countries to extend their connections to national law enforcement entities such as border police, customs and immigration, etc. NCBs control the level of access other authorized users have to INTERPOL services and can request to be informed of enquiries made to their national databases by other countries.

Forensic Overview

Identifying an individual's role in a crime and whether they are linked to previous offences can sometimes prove testing. Furthermore, if an individual commits a crime in one country and is convicted for this, serves their punishment and then goes to another country and commits another crime then it is important for networks of communication and an exchange of information to be in place between countries. This is a main function of INTERPOL who serve to facilitate such cross border police communication.

Just as fingerprints and DNA are important for establishing a suspect identity in the first place it is also paramount that such biometric information is available to other countries in order to ascertain matches if an individual commits a crime in a different place to the initial crime for which the fingerprints and record was set up for. Therefore it needs to be available on a global level (to authorized individuals) as crime today is increasingly transnational.

Certain crimes tend to occur across a series of different countries due to their nature, these include phenomena as diverse as international terrorism, drug trafficking, illegal arms deals, the smuggling of radioactive material, human trafficking, the global sex trade, racketeering, trading in human organs, counterfeiting of documents and identities, extortion and many different forms of state and corporate crime.

The importance of sharing biometric information was highlighted back in April of 2011 when it was reported that hundreds of prisoners (approximately 480), including members of the Taliban, escaped an Afghan prison. Unfortunately it emerged that the Afghan authorities have not been trained or equipped to take, store and access photographs and most importantly, fingerprints and DNA of possible dangerous terrorists for international sharing. This presented a huge global security risk and further highlights the need for such information sharing and co-operation in identifying individuals who are a possible threat to public safety.

Furthermore, it comes three years after a mass break out of almost double the amount of inmates from the same prison and for whom INTERPOL has still not received identifying information for circulation to the global law enforcement community. Following the recent breakout INTERPOL General Secretariat notified the neighboring countries of Afghanistan but with little strong identifying information it would prove extremely difficult for them to do anything with potential suspects.

Fingerprints and DNA are also of extreme importance in the aftermath of a disaster.

Following the Tsunami in Phuket in 2004 INTERPOL provided much support in coordinating the international victim identification effort. INTERPOL's response to the disaster was set in motion on the morning of the tsunami, 26 December 2004, when its 24-hour-a-day command and control centre immediately contacted the affected countries to offer assistance. INTERPOL also informed its network of international DVI teams and deployed an incident response team (IRT) to Thailand to begin co-ordination and data management efforts on the ground.

Nearly 3,000 victims of the 3,750 recorded were identified in the year that followed the

disaster. INTERPOL played a key role in coordinating the international victim identification effort and in providing logistical and communications support. More than 2,000 personnel from 31 nations were involved in the identification process, collecting DNA samples, conducting forensic analysis, logging data and helping with the repatriation of tsunami victims' remains. Of the identifications in the year following, approximately 45 per cent were made via dental records, 35 per cent by fingerprints and the remaining 20 per cent by DNA. The number of DNA identifications is expected to rise significantly during the final stages of the process.

Again, this demonstrates the importance of forensic matter in assisting the identification of individuals which assisted in providing closure for their loved ones.

Fingerprints

In criminal investigations the evidence of fingerprints has become an extremely important area. Since fingerprints are unique to the individual and do not change throughout their life they are extremely useful in either proving or disproving an individual's identity. They have been used for identification purposes for over a century and due to the advancements in technology have more recently become automated (i.e. a biometric). They are a popular source of identification for a number of reasons these include 'their inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration' (NSTC Subcommittee on Biometrics: 2006 : 1)

Furthermore, fingerprints can also be collected at a crime scene and have the potential to either link a series of crimes together and/or place an individual at the scene. They are also extremely helpful in Disaster Victim Identification (DVI) where victims can be identified after a disaster such as an earthquake or a bombing.

INTERPOL manages a database which contains over 146,000 fingerprint records and over 3,500 crime scene marks. Authorized individuals in member countries can access INTERPOL's secure global police communications network I-24/7 in order to view, submit and cross-check records via the automatic fingerprint identification system – AFIS.

Fingerprints can be taken by law enforcement officers using an electronic device or manually using ink and paper which is then scanned and saved in the appropriate format.

DNA – Deoxyribonucleic acid

Like fingerprints, DNA is also extremely vital in assisting criminal investigations. These molecules contain the information all living cells in the human body require to function. With the exception of identical twins, DNA is unique to an individual so in the same way as fingerprints it is very useful in ascertaining a victim's identity in a disaster and useful for solving crimes.

The first step in obtaining DNA profiles for comparison is the collection of samples from crime scenes and reference samples from suspects. Samples are commonly obtained from blood, hair or body fluids. Using forensic science methods, the sample is analyzed which then creates a

DNA profile that can be compared against other DNA profiles within a database. This creates the possibility for 'hits' to be made, hits with another person, hits with a person to a scene or hits with a crime scene to another crime scene.

INTERPOL's automated DNA database enables police in member countries to submit a DNA profile from offenders, crime scenes, missing persons and unidentified bodies. This is called the DNA Gateway and was created in 2002 with a single DNA profile. Member countries can access the database via INTERPOL's I-24/7 global police communications system.

INTERPOL serves only as the conduit for the sharing and comparison of information. It does not keep any nominal data related to a DNA profile of any individual. A DNA profile is a numerical code based on the pattern of the individual's DNA, this numerical code can be used to differentiate individuals.

The INTERPOL Fingerprint Unit

INTERPOL has a long history with Fingerprints and the use of Fingerprints to identify fugitives can be traced back to the early days of the Organization. The Unit is currently staffed with 7 experts from France, UK and Portugal and is looking to expand as the workload increases. The staff are responsible for ensuring that all searches are carried out in a timely manner and ensuring that the AFIS responds to the needs of the Organization. The staff also organize and attend conferences and working groups worldwide to promote the use of INTERPOL AFIS services. The majority of work processed is ten print requests however we are seeing an increase in crime scene mark search requests and have already had some successful results from this.

Statistics (2011)

We would like to share with you some statistics from this year (January – September) which will give the reader a quick resume of the workload and how the AFIS service is developing.

Total Database size - 146,000

Fingerprints added - 30,500

Fingerprints search only - 950

Identifications - 1615

For information in 2010 the Unit made 958 identifications and inserted 16,000 Fingerprint records. This shows that by adding more data we are able to return more positive results to member countries.

AFIS – Automated Fingerprint Identification System

Automated fingerprint identification is the process of automatically matching one or many unknown fingerprints against a database of known and unknown prints.

INTERPOL manages an AFIS database which authorized individuals in member countries can

access. The fingerprint data, either ten print forms or crime scene marks are received into the Fingerprint Unit from the member countries of INTERPOL. The Fingerprint Unit uses an AFIS which was developed and is maintained by SAGEM. Presently the database contains 146000 fingerprint records and 3500 crime scene marks. Officers worldwide will take fingerprints of a suspect and the data is then submitted to INTERPOL where it is uploaded on to the database. Records are saved and exchanged in the format set by the National Institute of Standards and Technology (NIST). Authorized users in member countries can view, submit and cross-check records using I-24/7, INTERPOL's secure global police communications network.

The Fingerprints Unit at INTERPOL actively encourages member countries to use the database as extensively as possible, and increase the number of relevant fingerprints in the system. It is highly recommended that all fingerprints of foreign nationals arrested or nationals suspected of transnational crimes, and unsolved crime scene marks are submitted to the Fingerprint Unit.

Transmission of Data

Due to its nature, INTERPOL's Fingerprint unit receives fingerprints from all over the world, up until 1999 all fingerprint files were received in paper format and these forms were then cut and pasted onto an INTERPOL designed support card. This card worked well, however was very time consuming and left room for error by not pasting the received fingerprints in the correct position in the form. Through a European working group it was decided to try and develop a form that could be used by member countries for the international exchange of fingerprints, over a period of 18 months experts from several European countries met and created the INTERPOL fingerprint transmission form for European countries, later this form was presented at a General Assembly and was accepted as the standard for Fingerprint exchange through INTERPOL.

The form was met with limited success from member countries, several European countries adopted it as their National standard form however due to the limited number of countries using this form the INTERPOL fingerprint unit was still faced with processing many different types of fingerprint forms. The working group did not give up however and with more and more countries now using AFIS decided to create an electronic version of the form in the ANSI/NIST format, taking advantage of previous work done on this by the UK, the working group looked at each part of the form and gave it the corresponding NIST file record number. This form was presented at the General Assembly in India and the delegates voted unanimously to use this form for the exchange of fingerprint records. For 12 years this form has been in existence and it has now become the recognised form for the transmission of fingerprint data internationally and the INTERPOL Implementation is widely used by member countries and is also supported by industry leaders in AFIS.

What to send?

All member countries are invited to submit the following information to the database for search and comparison.

- Fingerprints of arrested non nationals
- Fingerprints of nationals suspected of involvement in International crime
- Unsolved crime scene marks.

INTERPOL believes that if member countries were to send the above data to the AFIS for search and storage then this would assist in identifying international fugitives, solve crime and assist member countries in making their countries safer. Examples of the success we have seen from countries sending data are briefly outlined in the next section.

Success Stories of Fingerprints

The importance of sharing forensic data such as fingerprints is regularly proven here at INTERPOL. For example, over a period of one week (July 28th) six hits were made. These included fingerprints that were sent over from Columbia for identification. They were run through the database which produced a hit to a set of prints in AFIS from Portugal where the individuals had committed rape; the prints were under a different name.

A second hit was made between fingerprints received from The Netherlands for drug trafficking which were matched to prints in the AFIS received from Portugal for theft.

Another hit included fingerprints received from Monaco for burglary. They were run through the AFIS database and matched to a set of prints received from Austria for theft.

A further example of success of sharing biometric data was proven in 2008. An individual was arrested in Brazil on the charge of threatening behavior. He had served a previous sentence for grievous bodily harm and was also under investigation for pedophilia. The fingerprints of the suspect were submitted by Brazilian authorities to INTERPOL and a search was conducted in the AFIS and returned a positive identification. The fingerprints matched a record held under a different name, an alias, to the one the Brazilian authorities had for him. The offence he was caught for on that occasion was attempting to illegally cross the border between Belarus and Poland by train using a forged identity document.

Areas for Improvement

INTERPOL has 188 member countries that can use this central database for the storage and searching of persons however it is noted that not all member countries take advantage of this possibility. This is an area where we need to see improvement as the organization believes that it is only by populating and using this database that its full potential can be discovered. The Unit is always contacting member countries to explain the usefulness of the AFIS and how with the gateway in place they can get high benefits from using the AFIS. In 2012 we will launch a project to target 6 countries who we believe with some more information from INTERPOL and help in exchanging data will populate the AFIS.

MorphoEVA, NIST viewer

The Unit is continually trying to improve the quality of Fingerprint data submitted to its

AFIS and also between member countries, we see that 20% of files are of a very poor quality and are scanned with low dots per inch and without scales. INTERPOL working with its AFIS vendor Morpho has developed a project to provide member countries with hardware and software which will enable the country to scan a Fingerprint form and create a NIST file for the transmission to INTERPOL AFIS. In addition to enabling the sending of NIST files, INTERPOL offers a free of charge software to its users to view the NIST files; to date in excess of 1200 viewers have been downloaded.

The AFIS gateway

The major project for the Fingerprint Unit in 2011 and 2012 has been the development of a tool to enable the AFIS to receive and send automated replies to member countries. This tool will be developed by 3M Cogent based on specifications written by the Fingerprint Unit and INTERPOL technology service, the gateway will interact with the INTERPOL case history databases therefore enabling member countries to receive valuable information relating to hits on the AFIS system. When this gateway is in operation it is estimated that 80% of all requests to the AFIS will be automated and the member countries will receive a reply to their request within minutes, the throughput of this service will also be increased to enable higher volumes of comparisons by our member countries. It is hoped to have this service in place by mid-June 2012, the development has already started and the testing of the service will soon begin, this service will be a vast improvement for the Unit as it will enable high volume and fast responses to member countries, this should encourage member countries to submit more requests.

Fingerprints at border control

INTERPOL is seeing an increased need for the control of persons at border control; this is being achieved by verifying the passport against a database of stolen and lost passports. We believe that if a verification of the person's fingerprints against a look out list of persons could also be done this would ensure a more complete and sure way of controlling border crossings (exit and entry). Looking recently at one member country that has now added the searching of fingerprints against a National list of persons who are non grata in that country it was seen that in the first week over 50 persons were stopped from entering, in all these cases the persons had genuine travel documents under assumed identities.

The INTERPOL Fingerprint Unit dream

The authors believe there is still very much a future for the Fingerprint Unit at INTERPOL and Fingerprints in general worldwide. To ensure that this is the case it is vital that the Fingerprint Bureau in member countries populate and search the INTERPOL central AFIS with data that is of relevance to other member states. We believe that fugitives, unsolved crimes and the entry and exit of persons can be controlled if this database and exchange of data are increased.

The area where the Fingerprint unit really wants to see an improvement is in the quality of Fingerprint transmission and with this in mind has put in place a pilot project to target 6 countries. Based on the result from this pilot we will see how we proceed with all the other

member countries. An important fact to always keep in one's mind is that the AFIS database is not the INTERPOL Fingerprint Units database it is the database of all member countries, they are the ones responsible for populating it and using it the INTERPOL Fingerprint unit can only encourage the member countries to use it.

Conclusion

We hope by reading this document that the reader now has an insight into the workings of the INTERPOL Fingerprint Unit and understands why it is important that this service exists and why it needs to be used. INTERPOL fully supports the exchange of Forensic data between member countries either bilateral or by various regional services, in conclusion INTERPOL AFIS is just one of many possibilities however it is one that should always be used.

The importance of dental records in identification

Virginia Kannemann



Virginia Kannemann

National Office of Information Technology



Virginia Kannemann has a degree in odontology from the John F. Kennedy Argentine University of Buenos Aires. She was a speaker at the 5th Argentine International Biometrics Congress, and participated in the workshop on the ANSI/NIST-ITL 1-2011 international standard in Maryland, USA. She coordinates a group on the development of standardisation of dental records to that international standard.

She is currently studying Forensic Odontology at the Institute Universitary of the PFA (IUPFA)

Contact: VKannemann@jefatura.gob.ar

Abstract

Human identification involves many different sciences. The most common means of identification are visual recognition, by family or friends, and fingerprinting. However when a body is recovered badly burnt, in an advanced state of decomposition, or skeletonised, both of these methods are of limited use. Dentistry is a particularly suitable science for providing data for the identification of corpses, since both the stomatognathic apparatus and the skull can offer valuable features to aid identification.

Forensic dentistry is the area of dentistry whose mission is to assist the administration of justice by determining, through examination of the stomatognathic apparatus¹, as much information as possible regarding the physical characteristics, age, gender, habits, socio-economic status, racial and geographical origins and activities of the individual or individuals in question. Dentistry is also applied in support of the law by considering solutions for legal problems, whether civil, criminal or occupational, through the application of dental knowledge.

Key words: forensic dentistry, identification.

¹ The “stomatognathic system” is the name given to the combined anatomy and functions of the component parts of the oral cavity, with dental and joint features such as the temporomandibular joint and paraprosthetic muscles. The system comprises the lips, cheeks, tongue, palate, teeth, periodontium, salivary glands and jawbones.

The importance of dental records in identification

Introduction

The identification of individuals brings together different areas of knowledge such as medicine, anthropology, molecular biology and dentistry. Identification using the specific condition and characteristics of dental features becomes indispensable, since teeth and restorative dental work are resistant to fire and other changes that can take place following a person's death, and are therefore sometimes the only features on which the forensic examiner can rely. It is very important, in order for dental identification to be effective, for good dental records to be kept for each patient. Dental records need to be kept in a standardised format, using universal nomenclature, so that they can be used and understood by everyone who might need to use them.⁽ⁱ⁾

In view of the foregoing Argentina, through the National Office of Information Technology (ONTI)² proposed the inclusion of biometric information to create a uniform language for dental records to aid interpretation when those records are shared. That proposal was considered by the National Institute of Standards and Technologies (NIST)³ and the inclusion of dental records in the standards document for the exchange of biometric data was unanimously approved.

The National Directorate of the ONTI is leading the "Dental Records" development group and is currently working on defining the issue.

Historical summary

Dental knowledge has long been used in cases where identification by other means could not be done, whether because of the advanced state of decomposition of the body, because one is dealing with a large-scale catastrophe, because the individual is unrecognisable due to the action of fire, or because, due to the length of time since death, only skeletal remains have been found.

The man considered to be the father of forensic dentistry, Dr. Oscar Amoedo y Valdez, identified the corpses of 40 victims of a fire at a charity bazaar in Paris in 1897 in which 126 people died.⁽ⁱⁱ⁾

However the first case of identification using the victim's teeth dates back to 69 BC, when Agrippina, the mother of Nero, identified her husband's lover by certain characteristics of her oral cavity.⁽ⁱⁱⁱ⁾

In 1905, Guillermo Beckert Frambauer, second secretary of the German delegation in Santiago,

² National Office of Information Technology (ONTI): National Office with responsibility to the Under Secretariat of Management Technology in the Cabinet Secretariat in the Office of the Cabinet Chief of Staff, whose functions include the implementation of strategies for technological innovation in government administration, the development of systems used in management procedures, the setting of standards in connection with the incorporation of new technology into public organisations, collaboration with other government agencies in the creation of information portals, and the promotion of the interoperability of the information networks of State institutions. <http://www.jgm.gov.ar/sgp/paginas.dhtml?pagina=27>

³ National Institute of Standards and Technologies (NIST): non-regulatory federal agency within the US Department of Commerce. Its mission is to promote State innovation and industrial competitiveness through improvement of measurement science, standards and technology in ways that improve economic security and quality of life. http://www.nist.gov/public_affairs/general_information.cfm

Chile, murdered Ezequiel Tapia, the doorman in the building where he lived. After stabbing him and fracturing his frontal bone and the base of his skull, he started a fire in the building. The charred body was identified by Dr. Germán Valenzuela Basterrica through comparison of the remains with records of dental work carried out on Ezequiel Tapia in the army.^(iv)

The victims of the attack on the headquarters of the Argentine Israeli Mutual Association (AMIA) in July 1994 were identified from their dental records, as were 39 victims of the LAPA plane crash in August 1999.^{(v)(vi)}

The identification of Ernesto "Che" Guevara in 1997 was done through comparison of his ante mortem dental records, sent from Argentina to the Cuban anthropologists and dentists who conducted the excavation, with the remains discovered. A filling, the particular layout of the teeth, from an odontological point of view, and the presence of an extra-large frontal sinus were the points of coincidence that indicated a positive identification thirty years after his death.

Structures which determine identification

The measurements of the various anthropological points and planes, the layout of the teeth, their current degree of development, their precise morphology and the restorative work carried out in the course of life give us indications of sex, race, habits, illnesses, age, economic status and even individual identity.

A brief description of each of these will be given.

A. Anthropometric measurements

Relationships identified through the anthropological analysis of the upper and lower jawbones, and of the skull generally, together with dental measurements and morphology, enables individuals to be identified using measurement and a series of formulae and indexes.

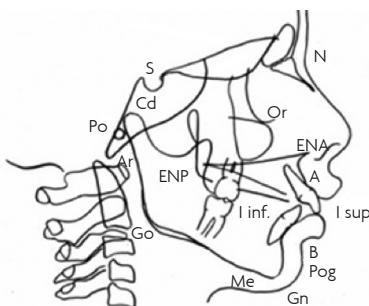


Fig. 1. Cephalometric points used to measure the bones of the cranium and jaws

One such relationship is Flower's dental index, used for the determination of race. This is based on the relationship between dental length⁴ and the basinasal line⁵.

The formula used is: dental index = (length of tooth/basinasal line) x 100

The result can vary between the following values for the principal racial groups:

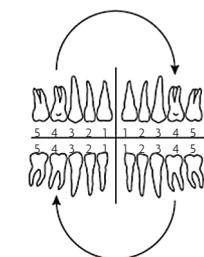
- Microdont: < 42 Caucasoid races
- Mesodont: 42-44 Mongoloid races
- Macrodont: > 44 Negroid and Australoid races

B. Teeth

The teeth are the body's hardest structures. The tissue which covers them, enamel, is formed by 5 to 12 million crystals of the mineral hydroxyapatite ($\text{Ca}_{10}(\text{PO}_4)_6(\text{OH})_2$), and is 94% inorganic, 1.5% organic and 4.5% water. These crystals are arranged in prisms with an oblique format and irregular direction, making them resistant to masticatory forces, which can reach 45 kg/m^2 .

Each individual's dental pattern is unique, and the dental formulae are:

*Temporary or primary dentition:*⁶ composed of 20 teeth divided into 3 groups: incisors (central (CI) and lateral (LI)), canines (C) and molars (M).

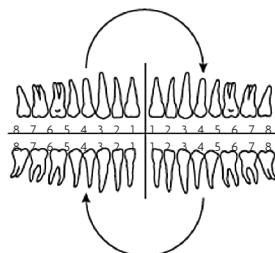


Dental formula for temporary dentition:

$$\text{MS: } (1\text{CI} + 1\text{IL} + 1\text{C} + 2\text{M}) + \text{MI: } (1\text{IC} + 1\text{IL} + 1\text{C} + 2\text{M}) \times 2 = 20$$

Fig. 2: Dental formula for temporary or primary dentition

*Dentición permanente:*⁷ composed of 32 teeth divided into 4 groups: incisors (central (CI) and lateral (LI)), canines (C), premolars (PM) and molars (M).



Dental formula for permanent dentition:

$$\text{MS: } (1\text{CI} + 1\text{LI} + 1\text{C} + 2\text{PM} + 3\text{M}) + \text{MI: } (1\text{CI} + 1\text{LI} + 1\text{C} + 2\text{PM} + 3\text{M}) \times 2 = 32$$

Fig. 3: Dental formula for permanent dentition:

4 Dental length: a straight line between the mesial surface of the first premolar and the distal surface of the third molar.

5 Basinasal line: a straight line from the summit of the nose (the intersection of the frontal bone and the two nasal bones) to the most basilar point of the basilar apophysis of the sphenoid (a bone situated in the middle part of the base of the skull).

6 Temporary dentition is the first dentition, which begins to erupt from the age of six months and ends around the age of two.

7 Permanent dentition is the second dentition, which starts with the eruption of the first permanent molars.

Each tooth has five visible surfaces⁸: mesial, distal, occlusal or incisal, vestibular, and lingual or palatal, so that one can come across innumerable possible combinations of cavities, restorations, missing teeth, and anomalies in the position, form or number of the teeth, and so on. With a view to using standardised and internationally recognised nomenclature, Argentina's dentists use the Two-Digit notation system approved by the FDI⁹ and Interpol¹⁰. This consists in dividing each jaw into two quadrants which are numbered from right to left from 1 to 4, giving a total of four quadrants. Each quadrant comprises eight teeth, which are numbered from the midline towards the third molar, the central incisor being numbered 1 and the third molar 8. This numbering applies to the permanent dentition. For example, Upper Right Central Incisor: 1.1 : For the temporary dentition, the quadrants are numbered right to left from 5 to 8; the teeth are numbered from 1 to 5, again starting from the central incisor.

For example, Upper Right Central Incisor: 5.1, where the first number corresponds to the upper right quadrant and the second number to the central incisor.

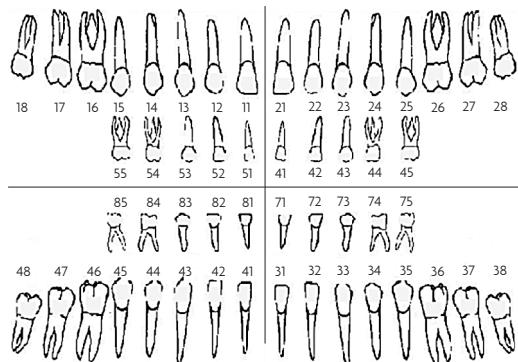


Fig. 4 : Odontogram using two-digit notation

Being protected by bone and mucous structures, such as the skull, the jaws, muscles and aponeuroses, the entire oral cavity, situated in a humid environment and largely comprised of inorganic material, is capable of withstanding temperatures of up to 1,000 degrees, making it the ideal means of identification of the victims of fire or disaster.

When teeth are subjected to fire, various states can be seen, as follows:

- The teeth remain intact (up to 100°C)
- The teeth are burnt (change of surface coloration between 150°C and 270°C)
- The teeth are broken or carbonised (reduced to charcoal by incomplete combustion at temperatures of between 300°C and 1100°C)
- The teeth are incinerated (reduced to ash by temperatures in excess of 1100°C).^(vii)

⁸ All of the surfaces closest to the midline are designated mesial, and the opposite surfaces are designated distal. The biting surfaces of incisors are called incisal, and those of premolars and molars are called occlusal. The canines have two sides, one mesial, the other distal, but they are considered incisal edges. The surfaces which face outwards to the vestibule of the mouth are described as vestibular, and those which face inwards are either palatal, if they are connected to the upper jaw and therefore close to the palate, or lingual, if they are of the lower jaw and therefore close to the tongue.

⁹ The World Dental Federation (FDI) is an organisation with more than 200 members comprising national associations and specialist groups representing more than a million dentists worldwide. <http://www.fdiworlddental.org/> <http://www.fdiworlddental.org/>

¹⁰ Interpol is the largest international police organisation in the world, with 188 member countries. Created in 1923 with the aim of facilitating international cooperation between neighbouring countries, it supports or assists the agencies, authorities and services whose mission is to prevent or fight international crime. <http://www.interpol.int/public/icpo/default.asp>

Determination of age

Age can be determined using the degree of development of the teeth and certain anthropometric measurements. Dental development timeline^(VIII)

Primary or temporary dentition

- Lower central incisors: 6 months
- Upper central incisors: 7 months
- Upper lateral incisors: 8 months
- Lower lateral incisors: 9 months
- Lower first molar: 12 months
- Upper first molar: 13 months
- Canines: 18 months
- Second molars: 24 months

Permanent dentition

- First permanent molar: 6 years
- Central incisors: 7 years
- Lateral incisors: 8 years
- First premolar: 9-11 years
- Second premolar: 11-12 years
- Second molar: 12 years
- Canines: 13 years
- Third molars: 18-25 years

Since this may vary, however, other studies should also be conducted, such as Carmen Nolla tables¹¹, carpal X-ray¹², and measurement of the skull and jawbones.



Fig. 5: Panoramic X-ray of the dental chronology of a child of approximately eight years of age

¹¹ These trace the different stages of formation of the tooth, divided into 10 periods from the formation of the crown through calcification, formation of the root, calcification and apical closure. Each one occurs at a precise time and indicates estimated age. Diagnosis requires X-rays to be taken.

¹² This involves assessment of the degree of development of the carpal bone, which helps calculate bone age and potential for growth.

To determine the age of adults after the permanent teeth have erupted, it is common to use Gusftason analysis, which consists of studying six characteristics present in adulthood which that author numbered from 0 to 3, where 0 represents absence of the feature and 3 represents its presence in an advanced state.

The following table shows those characteristics and the respective values:

	0	1	2	3
Attrition (A)	Absence	Enamel affected	Dentin affected	Dental pulp affected
Periodontitis (P)	Absence	Onset of periodontitis	First third of root affected	More than two thirds of root affected
Secondary dentin (D)	Absence	Formation in the upper part of the pulp cavity	Pulp cavity up to half filled	Pulp cavity completely filled
Build-up of cementum (C)	Absence	Build up somewhat greater than normal	Large covering of cementum	Cementum layer is largely consistent
Root resorption (R)	Absence	Resorption in small isolated areas	Greater degree of loss of substance	Cementum and dentin affected
Root transparency (T)	Absence	Root transparency noted	Apical third exceeded	Two thirds of root exceeded

Plotting the combined points in a Cartesian graph provides an estimate of age.

Determination of sex

Teeth possess certain characteristics which, when combined with features of the skull and jawbones, can help to determine sex. Some of those characteristics are shown in the following charts.

Teeth	Masculine	Femenine
Diameter M-D incisors	Disproportionate and misaligned	Uniform and aligned
Angles	Robustsand quadrangular	Delicate and rounded
Colour	Darker	Clearer
Size	Large	Small

Jaw	Masculine	Femenine
Average weight	80g	63g
Gonial angle	<125°	>125°
Symphysis menti	Higher	Lower
Size	larger	smaller
Condyles	larger	smaller
Inserciones musculares	More marked	Less marked
Bicondylar width	125mm	<105mm
Palate	Wide and not generally deep	Narrow and deep
Dental arch	Thick	Fine and delicate

Determination of height

The calculation of height on the basis of the dimensions of the teeth involves the proportionality of the teeth to the height of the individual, comparing dental measurements with those of the skeletal remains. One of the methods used is that proposed by Dr. Ubaldo Carrea, who proved that the sum in millimetres of the mesiodistal distances of a central incisor, a lateral incisor and a canine in the lower arch constitutes an arc of circumference whose chord is the central measurement of the dental diagram, which the author called “lower radial chord”.

That is why human height is considered to lie between two measurements, the maximum proportional to the arch and the minimum to the radial chord.^(ix)

The mathematical formula used is as follows:

$$\text{Maximum height (cm)} = (\text{arc} \times 6 \times 10 \times 3.1416) / 2$$

$$\text{Minimum height (cm)} = (\text{radial chord} \times 6 \times 10 \times 3.1416) / 2$$

$$\text{Radial chord} = \text{arc} \times 0.954$$

Men are closer to the maximum height while women are closer to the minimum.

C. Palatine folds

The palatine folds, or rugae, are ridges in the mucosa of the hard palate, immediately behind the antero-superior teeth on both sides of the midline.

Numbering between three and five, they adopt a different and unique position in each individual, even in identical twins. From the moment of their development in the third week of intrauterine life they are permanent and unchanging throughout life. Even if altered by injury, they regenerate according to their original pattern.

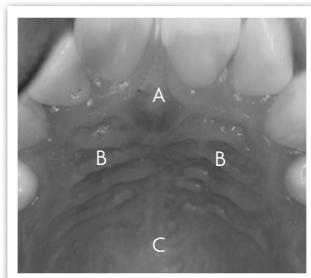


Fig. 6: Detail of rugosity or palatine folds:

A) Incisive papilla – B) Palatine folds – C) Midline or median raphe

Their value in identification, given their permanence, invariability and uniqueness and because they are protected from external damage, decomposition and incineration, is recognised and accepted. As with fingerprints, comparison with a specimen allows an individual's identity to be obtained.^(x)

Due to the different positions they adopt, as well as their size, shape and number, they are easily classified, and there are a number of classifications by different authors.

The study of the palatine folds is called rugoscopy. The study of the entire palate (median raphe, incisive papilla and palatine rugae) is called palatoscopy.

D. Lip prints

Lip prints are impressions of the folds, fissures and grooves of the mucous surface of the lips, which are visible on largely smooth surfaces when the lips are covered in lipstick and are latent on such surfaces when the lips are covered in saliva. As well as providing a physical impression, they are an important source of genetic material.

Of all the clues to be found at a crime scene, body marks in general are the most common, including lip prints, which can be found on a cigarette butt, a glass and even on a bite mark due to the presence of saliva.^(x)

Their analysis extends not only to the pattern of the labial semi-mucosa but also to its thickness, and the direction of the corners of the mouth and the lip prints, of which there are many classifications with which this article is not concerned.

Among the characteristics which are important for identification purposes are their permanence and invariability, and their uniqueness in each individual (except in identical twins, in which they are often similar to those of a parent).

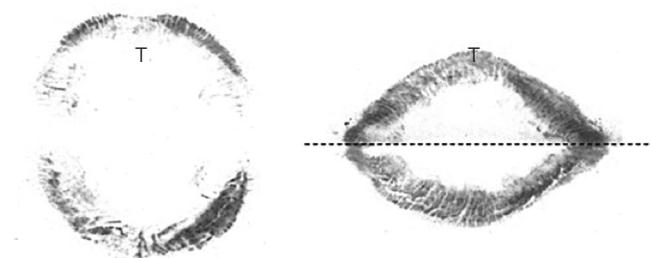


Fig. 7: Example of lip impression. Note the marked grooves and the direction of the corners of the mouth

E. DNA extracted from dental pulp

All of a person's identifying characteristics are found in their genetic code. DNA, which contains that genetic code, is found in the nucleus of each of the body's cells, although it is also found in the mitochondria (mitochondrial DNA) with different characteristics and forensic uses to those of nuclear DNA.

The human genome is made up of 6 billion base pairs distributed across 23 pairs of chromosomes in two supercoiled strands, one belonging to the maternal line and the other to the paternal line, containing the hereditary characteristics that make individuals unique yet similar to their relatives.

The study of DNA is usually done using samples of saliva, semen and hair (including the bulb). However teeth are also a reliable source of DNA because they are protected from the environment and from environmental damage, as already explained in this article.

Since dental pulp, the soft tissue within the tooth, contains different types of cell (such as fibroblasts, the mother cells of dental pulp, macrophage, odontoblasts, blood cells and peripheral nerve cells), enough can be obtained to carry out a DNA analysis. The number of cells in the pulp organs decreases with age. Not all teeth contain the same amount of dental pulp, so that a single tooth can provide between 15 and 20 micrograms of DNA. ^(xi)

Two methods of extracting DNA from dental pulp are used: total pulverisation of the tooth, and transversal or horizontal sectioning of the tooth. ^(xi)

Analysis of bites

Bite marks are the impressions made by the teeth on different substrata capable of becoming deformed. That deformation allows the characteristics of the teeth to be transferred to the surface.

Each tooth leaves a characteristic trace, such as:

- Incisor: elongated rectangle
- Upper canine: wide triangle
- Lower canine: narrow triangle
- Upper premolar: double triangle
- Lower premolar: single triangle
- Molar: rare, but when found it looks like a wide rectangle.

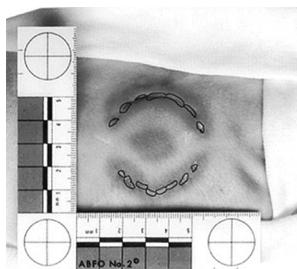


Fig. 7: Bite mark

This is a very useful crime lab method, since the teeth may have been used as weapons of either defence or attack. Bite marks are often found in crimes of a sexual nature, cases of child abuse, and fights. They can also be a source of DNA since they may also contain the attacker's saliva and/or blood.

Bite marks can indicate the type of bite – whether done in defence or attack – and depending on the location of the bite the type of crime can be determined. It is also possible to identify whether the marks were made by third parties or by the parties themselves, guiding the investigation; they can be used to link a suspect with a crime, and, along with psychological evaluation, they can be used to build a psychological profile of an attacker. ^(xii)

Conclusion

As we have seen, dental records, along with the entire stomatognathic system, can provide information for the identification of individuals. This method is useful when identification by other means is not possible, and in that event forensic dentistry becomes indispensable in respect of partial data obtained from disaster sites, or when bodies are found in skeletal condition and the only available information comes from DNA in the bones and from dental records.

In recent years dental records have been given importance in matters of identification. Different organisations have started to work with forensic dentists, such as Interpol with its disaster victims identification unit, which uses dental comparison for identification purposes, and the NIST, with its interest in including dental records in the ANSI/NIST – ITL standard for the exchange of biometric data. However, it should be pointed out that the method only works if there are prior records with which to compare, which obliges us as dentists to keep clear complete records that comply with international standards and nomenclature.

Given the importance of those records, the National Office of Information Technology is working with the NIST on the development of the appropriate standard.

Bibliography

- I R. F. Da Silva, De la Cruz, B.V.M, E. Daruge Jr., et al. La importancia de la documentación odontológica en la identificación humana – Relato de un caso. *Acta odont. Venez*, Mayo 2005, Vol. 42, Nro. 2, p. 159-164.
- II Garay Crespo MI, García Rodríguez I, Hernández Falcón L. Dr. Oscar Luis Amoedo y Valdez. Aportes a la Odontología. *Rev méd electrón*. 2007; 29(5). Moya Pueyo V., Roldán Garrido B. y Sánchez Sánchez J. A. *Odontología Legal y Forense*, Ed. Masson, 1994.
- III Spadacio, Célio. Análisis de dos principales materiales restauradores dentales sometidos a la acción del fuego y su importancia en el proceso de identificación. 2007. <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000429262&fd=y>
- IV Eleta G. Odzak J., et al. Identificación en desastres de masas. *Corte Suprema de Justicia de la Nación. Cuadernos de Medicina Forense*. 2002. Año 1, Nº3, Pág.167-187.
- V Estrategia Médico Legal frente a una Catástrofe Colectiva. El Caso A.M.I.A. Editorial JR, Abril 1996, Cuerpo Médico Forense.
- VI Delattre V: Burned beyond recognition: Systematic approach to the dental identification of charred humans remains. *J Forensic Sci*. 2000; 45(3): 589-596.
- VII Gómez de Ferraris, Ma. E, Campos Muñoz, A. *Histología y Embriología Bucodental*. Ed. Médica Panamericana. 2002. 2da Edición. Pág. 387-403.
- VIII Ortigoza Ruiz, Juan Francisco. Identificación Humana y Análisis de ADN en pulpa dental. Instituto de Medicina legal de Catalunya.<http://www.odontochile.cl/trabajos/reconyadnpulpar.pdf>

- IX** Grimaldo-Carjevschi Moses. Rugoscopía, queiloscopía, oclusografía y oclusoradiografía como métodos de identificación en odontología forense. Una revisión de la literatura. *Acta Venezolana Odontológica*. 2010. Volumen 48 (2). www.actaodontologica.com/ediciones/2010/2/art23.asp.
- X** González Andrade Fabricio, et al. El estudio de polimorfismo de ADN a partir de restos óseos y dientes y sus aplicaciones en la identificación de desaparecidos. *Ciencia Forense. Rev Aragonesa de Medicina Legal*. 2007. (5) pág. 163-182.

Biometric Trends, Challenges and Opportunities

Julio Fuoco



Julio Fuoco

Degree in Marketing. Certified Consultant in ISO 2000 and ITIL.



Currently, he is the Director of BITCompany, a firm that offers consulting, coaching and training services that go from the definition of IT strategies properly aligned with the business, to the implementation of government and systems of process quality management, information security, IT services based upon standards and good practices. He is also the director of ETSA Consulting, a company specialized in management, technology and processes.

He has more than 30 years of experience in the market of ICT. His has a wide expertise in themes related with advice and strategical consulting in management and technology, both for the public and private sector. Founder of the ETSA group of Argentina (specialized in IT outsourcing, consulting and reengineering of companies), IDS (specialized consultancy firm for the tourism sector) and ECU (purchase portal of the mass market).

Speaker at international seminars and conferences about processes, technology and business. Author of several articles for specialized magazines and technology portals. In the education field, he is Director of a Diploma Course in Processes with Quality in ICT and professor in several postgraduate courses in areas related with his speciality. He was the Director of ISIPE (Institute of Technology, Siglo XXI University, Córdoba) and professor of Management at IBAHRS and the Foundation for Commercial Sciences High Studies.

Abstract

We will examine some of the factors necessary for the success of a Biometrics project. We will examine in depth themes that go beyond technology, such as processing, people and culture. All of this framed in a context where international standards will be an essential element to keep in mind at the time of planning a solution to be implemented.

Key words: Processing, Government Transformation, National Standards

Biometric Trends, Challenges and Opportunities

Introduction

In recent years, the pervasiveness and incisiveness of technology, the reduction of costs, the rise in speed of communications, storage capacity and heightened availability of equipment have all made possible that we consider the use of Biometrics Technology¹ as a process that complements the verification of personal identity or electronic identification.

In Latin America, governments have already begun to discern a future where technology plays a central role, as an effective tool for E-Government, Social Inclusion, and Law of Persons (Ibero-American Letter of Social Electronic Identification, Lisbon 2010) and in particular, Biometrics will be a link that facilitates many of these objectives, given that Biometrics is state of the art, the most appropriate technology for identifying and verifying identities against the database of personal identities.

Given, while there is already a wide-scale familiarity with Information and Communications Technology (henceforth, ICT) on the part of industry enterprises and clients in the government and private sectors, on consideration of the implementation of distinct types of technological solutions when Biometrics projects are discussed, there can appear in some cases new paradigms with regards to the invasion of individual or citizens' privacy. This implies that great care be paid in the initial stages of planning, analyzing the players that will participate in this implementation.

Writing on this topic, a phrase comes to mind that I often use in meetings for project launches with a high degree of innovation or culturally significant changes: "*the graveyard of failures is filled with great ideas that were poorly implemented.*" This is precisely why it would be essential to go over the elements put into play in the implementation of biometric tools in both the governmental and the private sphere.

In order to do that, as the core of analysis I'll make use of a study – Benchmarking – done by Xerox several years back, in the 1980's. That study determined the impact of four factors; technology, processing, people and culture (see figure 1), on the success of projects whose results continue to be valid today. The results can be summarized aptly by Saint-Exupéry's phrase in The Little Prince, "*what is essential is invisible to the eye.*"

¹ Biometrics: is the study of automated methods for unique recognition of humans based on one or many intrinsic behavioral or physical traits. "Biometrics technology" is the application of mathematical and statistical techniques on the physical or behavioral traits of a person for the sake of "verifying" identities or "identifying" individuals.
<http://es.wikipedia.org/wiki/Biometria>

² www.clad.org

Here the real impact or importance of each of the parts of a program that seeks change through the use of technology is presented, where the technological component has a mere impact of fifteen percent (15%) in the factors of success, even though it is oftentimes the only one that can be seen. Among the rest of the elements we find processing, which has a bearing of thirty-five

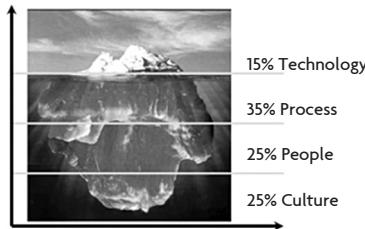


Figure 1

percent (35%), people (those who operate the new technology as well as those who make use of its benefits) and culture, be it organizational such as the place where the solution is to be implemented, will have a twenty-five percent (25%) impact each on the success of the project.

Hence let us examine with more depth each one of these parts:

Technology

As we stated previously, technology (hardware, software, and communications) is becoming more and more accessible with regards to costs and technological convergence is a reality.

This rule also holds true for biometric solutions, being that there is a large quantity of devices for each one of its methods, those being:

- *Physical*; finger prints, veins of the hand, hand geometry, palm print, iris/retina recognition, face recognition, DNA, voice, dental recognition, palatoscopy, ear shape
- *Behavioral*; signature, key stroke recognition, gait recognition, gestures

With which the feasibility of taking on projects is growing day to day. That being given, if we speak of technology that has been tested, with an ample range of solutions, systems and devices, what would the themes then be that could not be foreseen in the planning stage, so that the projects be scalable? So that they be designed and implemented under international standards³ and best practices⁴ (that is to say, valuing these standards for the sake of giving shape to issues such as information capture, its storage, communications formats and even the means by which to develop forth a project)?

It is thus that, if we speak of exchange of information among information systems and/or applications (programming interface, API), they ought to work under the ANSI / NIST ITL 1-2011

3 <http://www.wordreference.com/definicion/estandar>

4 http://es.wikipedia.org/wiki/Mejores_practicas

5 http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

6 <http://www.fbi.gov/>

standard⁵ of very recent approval, that defines how to work towards the interoperability of biometric data across different systems.

Likewise, it will also be important that governments, in line with the responsible directions for defining technological standards, set minimum conditions for certification that shall outline the equipment or devices (for example, that which is provided by the Federal Bureau of Investigation (FBI)⁶). This will allow for project scalability, with roadblocks to integration erased, and also ensure that the devices not be those whose condition becomes critical and responsible for failure.

To enter into even more depth regarding the importance of adoption of standards, in order for the programs to be interoperable, scalable and with a high grade of security in the exchange of information, we may analyze the experience of the financial services sector. This is a sector that historically has had the greatest number of networked calculations, the highest quantity of users, a large physical distribution of equipment, a high level of information exchange, real time labor, management of critical and confidential information, and I would go so far as to say, the highest level of information security. If for example, in the beginning of the rollout of ATM networks, there had not been standards set in place; for the format of magnetic strips on cards, encryption systems, or rather, the decision to work under international standards, nothing of what that industry is today would have been possible.

Therefore, making the decision to work under standards and best practices in the area of technology is giving definition to one of the most important pillars of success for the project.

A recent example of the implications of planning that does not adequately apply the use of standards is the case of the Argentine Federal Police. In early 1995, this institution began to collect data of its citizens (patronymic and biometric) not only on paper, but also digitally in a database. Recently, due to a necessity for service and quality, they had to make a technologic leap and they were forced to resolve the problem of reading compatibility of 5 million fingerprint entries that were stored in a proprietary database from the system they already had in place⁷.

There are obviously other technological decisions equally or of greater importance to evaluating the planning stage. For example, regarding the devices and biometrical methods to be used, it could prove difficult to opt for a fingerprint system of identification in projects where the people to be identified may have to engage in activities that leave their hands dirty; in that case the quality would be quite low.

Or the contingency plan in the event of defects in the technology. An issue that is already present in all projects, but if oftentimes not given the adequate amount of time for planning a solution. Certainly the process facing defects could be more bureaucratic and slow, given that we are speaking of the identification of people, but at the time for planning equal attention ought to be paid to the contingency as is to the main project. This is a consequence of the fact that, as the processing become more linear and flexible through the use of technology,

⁷ (Biometrías, "Herramientas para la Identidad y Seguridad Pública", P. Janices, 42)

the technology becomes critical and difficult to replace or obtain the same performance or flexibility against defects.

3. Processing

It remained evident from Fig. 1 that planning and working on the processing (at an impact of 35%) will be an important factor in the success of projects. But organizational politics and procedures, ones that ought to be designed as a part of any comprehensive solution to be implemented, are also a part of the term “*processing*.”

Once again, when we speak of Biometrics, we are speaking of the direct participation of citizens, for which we ought to begin by reviewing the extant laws and standards (or those which are to be created), which will be the basis for planning the politics, processing and procedures of the solution.

If we were to situate ourselves in Argentina, we could speak of Law 17.761 and its amendments⁸ that regulate the identification, registry and classification of national human potential, or Law 24.450 that establishes the system of identification for newborns, wherein they are obliged to identification through patronymic and biometrical data. If we were to speak of passports, we could refer to the recommendations of the International Civil Aviation Organization (ICAO)⁹, an exceedingly important issue if we take into account the pressing need to be able to identify a person beyond the borders of their home country, but in the domain of documentation of citizens, we must heed existing debts like the standards of unique documents of identification, realizing also the existence of countries where it is not the norm to require these documents universally. That is to say, we shall analyze the different legal marks and standards in order to then entertain issues such as which data is being registered, with what format (if one even exists), etc.

Identification of persons may be juridically resolved, but I believe that the advance of technology and Biometrics systems of identification will make possible the appearance of new legal marks for the digital identification of the citizen, collaborating in the achievement of the objectives sought by many nations in the region – social inclusion, law of persons, and e-government, as we mentioned in the beginning of this chapter.

Once we have revised the corresponding legal aspects, having in mind as well the area in which the Biometrics project is to be developed, the focus ought to be placed on the planning of the processing with the intent that it be linear and flexible, for these are two viable characteristics in the use of Biometrics. These characteristics, the flexibility and linearity of processing, are the beginnings of reengineering, set out in 1994 by its creators Michael Hammer and James Champy, both coming from the technological world.

They defined concepts, saying, for example, “*the need for simplicity produces enormous consequences with regards to the manner of planning processing and giving shape to organizations*”¹⁰; or, some of the postulates that were defined following the emergence of

⁸ <http://www.boletinoficial.gov.ar/institucional/index.castle>

⁹ <http://www2.icao.int>

¹⁰ (Reingeniería, M Hammer & J Champy, 1994, 54);

reengineering, for example:

- Entry of information at the beginning; the biometric technology makes the person a participant as an acting part of the digital identification process
- Elimination of intermediary steps; with digital identification, the process is completed in an automatized fashion
- Planning processing that adds value, for what more value can be had than the transparency of the identification and making social inclusion fair, here I am assuming the premise that biometric identification will give me the best security in existence at the time of identification of citizens

This new way of doing things brings with it a change in values equally cultural as organizational, that people (the third integral part of this project) will have to face.

In addition to what has been said until now regarding reengineering for the overhaul of these processing and procedures, one will no longer be able to base himself on the experience of whoever brings to fruition its implementation, given that for several years now this has no longer been the source of knowledge, given the necessity to work (when they exist) with the extant international standards (for example, the ISO/IEC¹¹ standards that delineate what ought to be done in particular for the specific solution).

In Biometrics, the ISO/IEC regulation 19794¹² is set forth, outlining the general aspects and requirements for the definition of formats for the exchange of biometric data – the notation, transfer methods (which should provide platform independence) and the separation of transfer syntax from the definition of the content. This standard defines what is commonly applied in biometric data, that is to say, the standardization of common content, what it means, the exchange format, and the presentation of data format, having specifications for the different systems of biometric identification. A more detailed description of these standards can be found on the Biometrics page of the Argentine Government¹³.

Returning to processing that is both flexible and secure for citizen identification, if we were to do this via a legal document and some physical characteristic of the person (a biometric system), it would prove to be a more flexible and secure task than if it were being done through a legal document and some sort of equipment. Quite simply, and without going into more details, the mere thought of any device brings to mind that it would have to be on the person at the time of identification. Here we are not mentioning the use of a user name and password, given that it is flat out rejected as insecure like digital identification.

4. People

If these lines had been written ten years ago, perhaps an entire chapter would have been dedicated to speaking of people. Fortunately, over time, the fear of technology has begun to diminish, the fear of its security and its use.

¹¹ <http://www.iso.org/>

¹² http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50862

¹³ <http://www.biometria.gov.ar/metodos-biometricos/dactilar.aspx>

The work that many governments (among them, the Argentine) have been bringing to fruition to shrink the digital gap has made it possible to think of the “disappearance of “technological ignorance”¹⁴ in the medium term, and as a consequence, the fear of the unknown will cease to be a relevant factor.

But when we speak of people and their influence on the success of projects with a technological base, we should not simply pause at familiarity they have with the projects. There are other associated factors that can influence positively or negatively in accordance with how the projects are planned out. For example, we ought distinguish between those who will actually manage the solution from those who will merely be the users of it (in this case, the citizens).

Let's begin with the best known: “resistance to change.” In the case of the users, this condition won't be put into play, since the most commonly used techniques of biometric identification are not invasive. Furthermore, Argentine citizens will already see the benefit of not having to ink fingers any longer for the fingerprint identification required for new government ID's (DNI¹⁵) and passports¹⁶. A successful project that involves the use of Biometrics and where many of the advantages of its used are visibly reflected.

Now, if we speak of the system users, this hesitance could possibly arise, without referring to any project in particular, simply the experiences lived out in many of the processing redesign projects, as well as innovation and studies brought forth by many researchers.

Kurt Lewin¹⁷, one of the top researchers on the processes of resistance to change, recognised as the founder of modern Social Psychology, found three common causes:

- *Self interest*. Defined as the personal motives that affect or feed the desire for change. Here we may place motivation, the habit of developing a defined work and training process.
- *Organizational culture*. Understood as the fundamental force that guides the workers' conduct: occasionally, they feel threatened when radical changes in the way things are done in certain activities come about.
- *Perception of goals and organizational strategies*. The members of a team do not understand that a new goal is needed (a change), because they haven't received the same information as their higher ups.

Unfortunately, these causes come about even more frequently when we're speaking of governmental structures, where in many countries these structures are little flexible, very hierarchical, where concepts like “*the more workers I have under me, the more important I am*”¹⁸ dominate.

And these motives, where the challenge lies in the paradigm change of the people and/or users, will certainly be one of the biggest problems to face when implementation of a technological project comes about, and even more so when that project involves leveling out the process for

¹⁴ When it is applied to a concrete context it means “not knowing something determined” in light of many other things or “having an imperfect knowledge of.” <http://es.wikipedia.org/wiki/Ignorancia>,

¹⁵ <http://www.nuevodni.gov.ar/>

¹⁶ <http://www.mininterior.gov.ar/pasaporte/>

¹⁷ http://es.wikipedia.org/wiki/Kurt_Lewin

the sake of its own flexibility.

What has been said up to this point regarding people seems very obvious and is not beyond anybody's comprehension today; nevertheless, I regret to inform the reader that this is not in line with what we live on a daily basis in the rollout of projects that involve organizational change. Due to which, it will be necessary to resort to methodologies and means of implementing a project that work to minimize these negative factors. At the end of this chapter we will list some of those means.

5. Culture

This portion which has an impact of twenty-five percent, or rather, larger than the technology itself, just as when we speak of people, has two focal points.

We refer equally to:

- a. Organizational culture
- b. Social culture¹⁹, which in projects of a public and/or regional nature plays a much more important role.

Regarding organizational culture, we can state with certainty that its impact on the success of the biometric project will be yielded by the leadership style that the project's sponsor and director employ. Issues like the work stability of public employees, the time limits for government officials in their post, likewise the lack of rewards and reprimands for the employees, make it barely possible to think of a cultural change in that organization or dependency. Therefore, when the time for project planning arrives, it will be essential to keep that culture in mind lest the project fail.

On the level of social culture, I believe the issue is distinct. Even though nations and individuals have well defined cultures, there are strategies that can be implemented at the time of taking on a proposal en route to a Biometrics project. Normally, users and/or citizens resist changes due to lack of communication, the lack of an explanation of the benefits that will accompany said solution.

If we sought that, on an organizational level, they would be better prepared for the change, a good policy would be necessary, as L. Schvarstein says, "*a good policy would be to provide organizations with the necessary capacity to maintain good utopias. Utopias are the sign of dissatisfaction with the present; its submission is a factor of unbalance that cannot but favor the development of the organization and its members that will give the subject space.*"²⁰ Likewise, "*granting them a structural elasticity that allows them to dispositionally take on situations of change, this concern will then be something that shan't be excluded from the planning of structures.*"²⁰

¹⁸ Reingeniería (M Hammer & J Champy, 1994, 80)

¹⁹ Definition: The social environment of beliefs created by human beings, customs, areas of knowledge, and the practices that define conventional conduct in a society. (Newstrom & Davis, 1993)

²⁰ Psicología Social de las Organizaciones (Leonardo Schvarstein, 2002, 246)

6. Factors in the Success of Projects

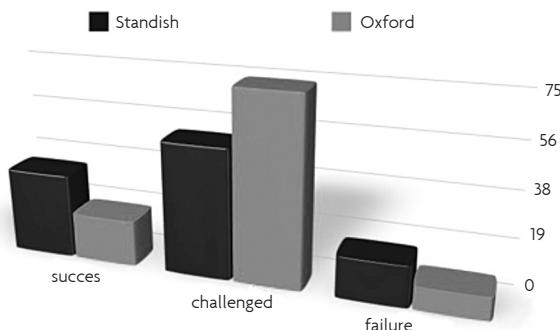


Figure 2

Having already concisely reviewed four of the factors in the success of a biometric project, that while they are not the only ones, they are indeed normally those that have most altered the solution to be developed, let's reemphasize the necessity that they form an integral part of planning stage, seeing as some times lack of awareness, political necessity or simply ignorance results in them being denied the sufficient degree of analysis and time, then going on to become the reasons that said projects end up becoming too large and we label them as "*challenged*."

This label corresponds to project that were redesigned in their reach, objectives, specifications or any other element that altered the initial conception and that at the end they were able to finish. If we review the studies performed by the Standish Group in the United States (Standish 2001) and by Oxford University in the U.K.²²(figure 2), almost fifty percent (50%) of projects fall under the category "*challenged*," while sixteen percent (16%) are successful, and the rest failed.

Another report that also discusses the factors that affect the performance of ICT projects in governments was done by Alejandro Barros, where causes such as the adoption of development or planning methodologies that had not been tried or with little experience were admitted²³.Translated into the terms we've come about defining in this chapter, these would be, for example; that the devices do not carry any international certification, not working under international standards, norms or best practices. Argentina, for example, is on its way towards implementing things in the Biometrics field, making it desirable that the "National Program of Standardization of Biometric Data and Forensic Biometrics" (commonly called bio.ar)²³ become a reality, a task that is being coordinated by the National Office of Information Technology

21 http://www.alejandrobarros.com/media/users/1/50369/files/4363/Proyectos_TIC_GOV.pdf (pag. 4)

22 http://www.alejandrobarros.com/media/users/1/50369/files/4363/Proyectos_TIC_GOV.pdf (pag. 6)

23 http://www.biometria.gov.ar/media/14056/estandar_MININT_biemetrico8.pdf

(ONTI), an organization that has under its command the tasks essential for the homogenization and coordination of technological tools for the managerial optimization.

Another task that could help in the planning stage of a project is realized by the Parliamentary Office of Science and Technology (Government IT Projects) in the United Kingdom, which has as its ends the evaluation of projects against a baseline of factors in success and failure in sixteen areas, those which will determine the evolution of an ICT project²⁴, highlighting again, amongst others, the area of working with established solutions and uncomplicated projects.

Seeing that we've been continually mentioning the use of standards, norms and best practices, we cannot leave out that the project ought to be administered for success, in agreement with the methodological principles defined by the Project Management Institute (PMI[®])²⁵ or the English Government (PRINCE2[®])²⁶.

Finally, as a sine qua non, being a given that the greatest biometric projects are those related to citizens and the State, political decision is also a key factor of success for these projects.

7. Conclusion

In Argentina, much of the work toward making Biometrics the tool for digital identification of the individual have already been in development for years. Still perhaps one of the most ambitious projects is the creation of an interABIS integral database system for biometric storage and consulting that would consolidate the existing biometric data entries stored by various official organizations, provincial organizations and other national or provincial dependencies with material competence, providing consultation and verification services. This project was conceived under the principles of operating within the existing international standards and best practices for these types of challenges.

But in Argentina, problems exist that must certainly repeat in other nations as well. From there comes this list of suggestions and critical points that ought to be accounted for in order to avoid critical flaws.

- The adoption and standardization of XML interfaces for the interoperability of biometric data entries
- The definition of national standards of certification for equipment
- Working on the implementation of a Personal Identify Verification (PIV)²⁷, in the scope of national public administration
- Putting together a computational structure adequate for the storage of critical data, that meets the corresponding standards

²⁴ http://www.alejandrobarras.com/media/users/1/50369/files/4363/Proyectos_TIC_GOV.pdf (pag. 7)

²⁵ <http://www.pmi.org/>

²⁶ <http://www.prince-officialsite.com/>

²⁷ <http://csrc.nist.gov/groups/SNS/piv/index.html>

- Creating an authority over application works towards the better functioning of the system, including exchange of information
- The integration of privacy on all levels of the system design to be implemented
- The creation of a guide for best practices, for the digitalization of biometric forms, that is, biometric interoperability
- Working on the quality of data, where it is possible that there exist duplications of biometric registries with diverse patronymic identities (names vs. biometric data); also possible is that the registries are not in a format recognised by automated applications
- The implementation of biometric registries for unnamed people, unnamed corpses or persons declared missing.
- Harvesting a profound discussion between the public and the private sectors over where, when and how to apply Biometrics, taking into account issues such as privacy and security
- Raising awareness and providing citizens with information about the benefits of accurate identification of citizens in regards to social inclusion
- the lack of invasiveness of these methods
- the current laws and regulations over privacy

Don't forget that the graveyard of failures is filled with great ideas that were poorly implemented.

Bibliography

- Latin American Center of Administration for the Development (CLAD), www.clad.org
- National Institute of Standards and Technology Information Technology, www.nist.gov
- Federal Bureau of Investigation <http://www.fbi.gov/>
- Official Bulletin of the Republic of Argentina, <http://www.boletinoficial.gov.ar/institucional/index.castle>
- International Civil Aviation Organization, <http://www.icao.int>
- Michael Hammer & James Champy (1994) "Reingeniería", Colombia, Grupo Editorial Norma
- International Organization for Standardization, <http://www.iso.org/>
- Official web site for Biometrics of the Government of Argentina, <http://www.biometria.gov.ar>
- Wikipedia*, <http://es.wikipedia.org>
- Official web site of the new National Document of Identification of the Republic of Argentina, <http://www.nuevodni.gov.ar/>
- Official web site of the Ministry of Interior of the Republic of Argentina, <http://www.mininterior.gov.ar/pasaporte/>
- Leonardo Shvarstein (2002), "Psicología Social de las Organizaciones", Barcelona, Editorial Paidós
- Davis, K y Newstrom, J (1993): Comportamiento Humano en el Trabajo. (8º ed.), México, D.F, Mc Graw-Hill
- Blogs of Alejandro Barros, <http://www.alejandrobarros.com>
- Project Management Institute, "PMBOK®", Fourth Edition
- OGC, "Managing Successful Project with PRINCE 2™", 2009, Edition
- Sitio web oficial del Ministerio del Interior de la Rep Argentina,
<http://www.mininterior.gov.ar/pasaporte/>
- Leonardo Shvarstein (2002), "Psicología Social de las Organizaciones", Barcelona, Editorial Paidós
- Davis, K y Newstrom, J (1993): Comportamiento Humano en el Trabajo. (8º ed.), México, D.F, Mc Graw-Hill
- Blog de Alejandro Barros, <http://www.alejandrobarros.com>
- Project Management Institute, "PMBOK®", Fourth Edition
- OGC, "Managing Sucessful Project with PRINCE 2™", 2009, Edition

Biometrics technology and the new economy: A Review of the field and the case of the United Arab Emirates

Ali M. Al-Khoury



Ali M. Al-Khoury

Emirates Identity Authority



Dr. Al-Khoury holds an Engineering Doctorate (EngD) in the field of large scale and strategic government programs management from Warwick University in UK. He is currently working with Emirates Identity Authority as the Director General. During the past 20 years, he has been involved in many strategic and large scale government programs. He has been an active researcher in the field of revolutionary developments in government context and has published more than 30 articles in the last 4 years. His recent research areas focus on developing best practices in public sector management and the development of information societies with particular attention to e-government applications.

Información de contacto: P.O. Box: 47999, Abu Dhabi, United Arab Emirates

Tel.: +971 2 495 5450

Fax: +971 2 495 5999

email: ali.alkhouri@emiratesid.ae

website: www.emiratesid.ae

Abstract

Over the past decade, biometrics technology has evolved from a technology used primarily in forensics and a narrow scientific and technological field to an indispensable technology in public and private sectors expanding its roots in areas calling for advanced security. Biometric technologies provide high levels of security and reliability to address requirements related to identification and verification of personal identities. In light of the ever increasing requirements for robust identity management, biometrics industry is evolving to play a central role in shaping the future economy.

This article provides a comprehensive overview of biometrics technologies, its functions, and areas of application, related international standards, and recent advances in the field. The second part of the article looks at the application of biometrics in the government sector worldwide, and the emerging pivotal role of biometrics in consolidating the foundations of the digital economies.

It also sheds light on the experiences of the United Arab Emirates in deploying different advanced biometrics technologies in a wide range of applications. It also outlines the government plans to develop an identity management infrastructure to address multiple strategic objectives, some of which are related to revolutionising public services and supporting the development of the digital economy.

Key words: Biometrics, identity management, digital economy, digital society.

Biometrics technology and the new economy: A Review of the field and the case of the United Arab Emirates

Introduction: Biometrics History and Current State

Human race has always been beset with the need for highly secure identification and personal verification methods, arising from various reasons spanning social, economic, commercial and legal considerations. Identification is a process through which one ascertains the identity of another person or entity. It has always been recognised that every human being has unique traits that can define his or her identity.

Recognition started from the faces that are as unique as they may appear. However, larger populations, advances in surgical alterations and modern citizen centric service models have necessitated varying methods of recognition and unique identification.

Derived from the Greek words: Bios (Life) and Metron (Measurement), biometrics represents the science of identity recognition. Biometrics as a science and an automated means of identification may only be a few decades old, but as a concept, it has been in existence for thousands of years (See Figure 1, and Table 1). Today, biometrics identification is recognised worldwide as a definitive personal identification method with specific metrics that gives both the service provider and the end user the assurance of a rapid, secure, and convenient transaction.

Research Reference	Evidence
Renaghan (2005)	Details of a cave dating 31,000 years back revealed hand prints of pre-historic humans with pre-historical pictures apparently signed by fingerprint stamps of authors.
McMahon (2005)	Chinese and Indian historians have references of fingerprints used as signatures in transactions going back five thousand years.
McMahon (2005)	Historiadores chinos e indios tienen referencias de huellas dactilares usadas como firmas en transacciones que datan de 5 mil años atrás.
“Dermatoglyphics”, (2005)	The Babylonian clay tablets of 500 BC show evidence that human kind used to record business transactions and sign it using fingerprint stamps.

Table 1: recognition means in the history of civilisation



Figure 1: Late B.C. - Picture writing of a hand with ridge patterns was discovered in Nova Scotia.

Clearly, personal identification has become a key requirement for today's increasingly digitised global economy. Indeed, trust in electronic transactions is essential to the vigorous growth of the global economy. As markets tend to shrink and get tougher, businesses find themselves in need for modern identification solutions ever than before to establish such trust basis, i.e., for denial and accordance, and for acceptance and refusal.

Businesses and governments alike in the past decade have therefore paid high attention to protecting their infrastructures from impersonating and/or infiltrating activities; a crime that was reported to cost 35 billion dollars in the United States alone in 2011 (Vamosi et al., 2011). With such justified attention to identification requirements, methods of identification assumed greater prominence.

In addition, as e-government and e-commerce initiatives proliferate, offering more online electronic services, robust identification and authentication methods are needed to address control and security requirements. The existing literature referred widely to the fact that one of the main challenging issues facing e-government and electronic society's development is identity management and the issue of trust in online transactions and digital identities. Ultimately the digital identity needs to become the same as real-world human identity. Using biometric identifiers for identity management provide strong credentials and higher levels of identity assurance.

According to a recent research report by RNCOS E-Services, the global biometric market is anticipated to grow at a CAGR of around 22% between 2011 and 2013 (RNCOS, 2011). At a regional level, North America was reported to dominate the global biometric market share of over 30% in 2010. The Asian, Middle East and Africa region were expected to emerge as growing markets for biometrics by 2013.

The report has also indicated that the government sector accounts for the major share of the biometrics market whereas the healthcare and financial sectors emerging as the potential adopters of biometrics systems. Many banks in developing countries (specifically Asian nations, including India, China, Malaysia, etc.) have adopted biometrics to address identity fraud issues and to offer customers an easy and more convenient authentication alternative to cards and PINs for transactions like ATM withdrawals.

Once again, biometrics is seen to be a critical enabler for the new digital economy. Only by understanding its potentials, how it works, and building on the experiences gained from international implementations, we can expect to make significant progress in creating successful future for our societies. As such, this article is written in this scope of dialogue.

This article is structured as follows. The first section provides a general overview of biometrics, including its characteristics, applications fields, related international standards, and recent advances that are shaping the biometrics industry. The second section looks at how biometrics technologies are adopted in the government sector, and its emerging role in addressing identity management requirements and forming the basis for the new digital economy.

The third section then looks at some biometrics initiatives implemented in the United Arab

Emirates over the past decade to address needs related to critical infrastructure systems development. Finally, the fourth section presents an overview of one of the recent multi-billion dollar programs implemented to develop an identity management infrastructure to act as a single source for personal identity provision in the country.

1.1 Biometric Characteristics

Biometric characteristics are divided into two broad categories; physiological and behavioural. Physiological characteristics are the ones that are closely linked to the human body. Iris, retina, facial features, fingerprint, palm print and DNA are physiological characteristics of the human body; offering positive identification that is difficult to counterfeit. Voice, speech, signatures, handwriting, key stroke sequences are characteristics used for behavioural pattern studies.

In order to recognize a person by his or her biometric characteristics and derived biometric features, an enrolment process must take place. The process entails the construction of a data record of the enrolled person and to store it in a biometric enrolment database. The enrolment data record may comprise one or multiple biometric references and arbitrary non-biometric data e.g., name, and personal information, etc. See also Figure 2.

Table 2: Biometric performance measures

Performance Measure	Description
False (non-match) rejection rate (FRR) or type I error	The measure of the percentage of times a valid subject has been falsely rejected by the system. FRR (%) = number of false rejections * 100 / total number of unique attempts.
False (match) acceptance rate (FAR) or type II error	The measure of the percentage of times an invalid subject has been falsely accepted by the system. FAR (%) = number of false acceptance * 100 / total number of unique attempts.
Cross-over error rate (CER)	A measure representing the percent at which FRR equals FAR. This is the point on the graph where the FAR and FRR intersect. The cross-over rate indicates a system with good balance over sensitivity and performance.
Enrolment time	The time taken to initially enrol a new subject with a system by providing samples for creation of reference templates.
Failure to enrol rate (FTER)	Used to determine the rate of failed enrolment attempts. FTER = number of unsuccessful enrolments / total number of users attempting to enrol.
Throughput rate	The time taken by the system to validate transaction data with the data in repository to process the identification or authentication function. This is the rate at which enrolled subjects are processed for acceptance or rejection by the system.

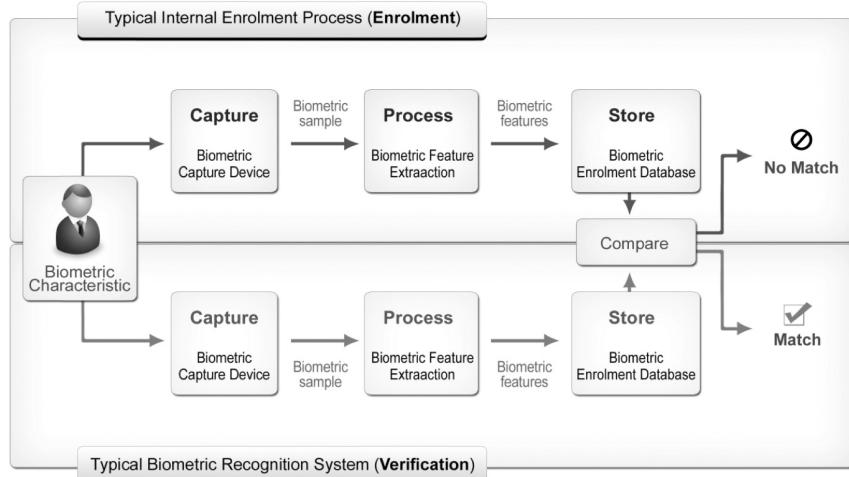


Figure 2: Enrolment and verification processes

The recognition process is initiated when the person to be recognised presents his or her biometric characteristic to the biometric capture device. The device generates a recognition biometric sample with biometric features which are compared with one or multiple biometric templates from the biometric enrolment database. This should result in acceptance or rejection of the recognition request.

The most common capturing process in biometrics today is optical. In most cases miniaturised CCD cameras are used, which capture either visible or infrared light (Brüderlin, 2001). Recent methods, particularly in fingerprint capturing, try to get away from the optical capture to use temperature, pressure and/or capacitance (*ibid*). The primary performance evaluation measures in biometric systems are depicted in Table 2.

However, the accuracy of these measurements varies, which has a direct relevance on the levels of security they offer (Shoniregun and Crosier, 2008). The error rates of biometrics systems are tuneable, which allows it to be configured according to the business objectives.

The error rates in biometrics cannot be entirely tuned down, however reducing one error rate will increase the other. A balance between risk (i.e. false accept) and operability (i.e. false reject) must be found which matches the business objectives best. As depicted in Figure 3, for most biometrics, a template comparison results in a score represented by the “Hamming Distance”, which is the percentage of bits of two compared biometric templates that are different. If this percentage is lower than a set threshold, a match decision is made and vice versa.

In this example above the threshold is set to 0.41 which means, that the system recognises a presented biometric as an authentic when no more than 41% of the previous captured bits during the enrolment process are different from the captured bits at verification time. An authentic with more than 41% different bits is called a false non match, an impostor with less than 41% different bits is called a false match.

Biometric Capability	Explanation
Identification	is the process whereby one tries to match a submitted sample of biometric information with an existing database of known identities. If a match is established, the identity of the person is established.
Verification	is the process by whereby a confirmation to an identity claim is established. It provides an answer to "Am I really who I claim I am?"
Authentication	is the process by which the truthfulness of the submitted biometric sample is established. The authenticity of the biometric sample submitted establishes the credentials of the person.
Recognition	is the process which is not necessarily for identification or verification. It is meant for recognizing an individual – especially when no features are available for detection. DNA is an excellent example of Recognition application.

Table 3: Biometric functions

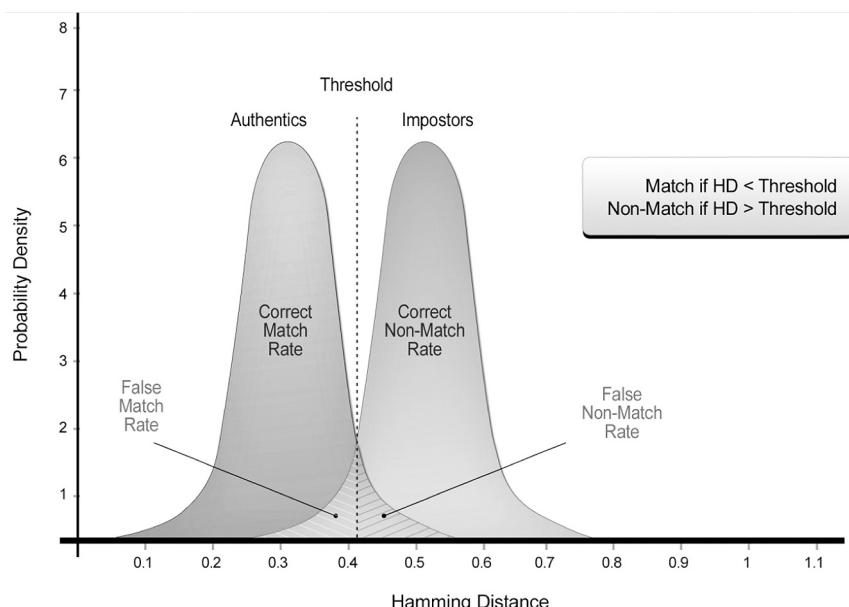


Figure 3: Tuning biometric systems

The diagram (Figure 3) shows how the configurable threshold determines the balance between false match and false non-match rates. The probability for a false match or a false non-match equals the area under the curve on either side of the threshold. By changing the threshold, one area reduces while the other increases, hence determining the balance.

Current technologies have evolved over the past five decades to higher mature levels due to the developments in the semi-conductor technology coupled with computing power. However, the foremost impediments of biometrics rotate around the complexity and privacy issues surrounding information abuse.

Biometric information abuse has caused some civil libertarians to be incensed by the risks posed by the personal nature of biometric information and how this information can be manipulated or misused. Conversely, the evolution of the biometrics to the current state in the world is best understood in the context of the applications of the biometrics. The next section looks at some different uses of biometrics which also explain the concept of identification and authentication.

1.2 Purpose of Biometrics

Personal identification numbers; often referred to as PIN numbers, were one of the earliest identifiers to offer automated recognition. PIN is a secret numeric password shared between a user and a system that can be used to authenticate the user. Despite its wide application, PIN-based authentication methods do not provide recognition of the person performing the transaction. Biometrics however represent unique identifiers and unlike PINs, it cannot be easily transferred between individuals. Most of current biometric applications are related to security and are used extensively in government sector.

The wide applications of biometrics in public domain are being motivated because of its advanced capabilities of (1) identification, (2) verification, (3) authentication and (4) recognition. In practice, it is noted that many in the field often do not understand the difference between the functions of these capabilities. Table 3 provides definition of each.

In the context of the above capabilities, biometrics has come a long way. From the 1858 hand print cataloguing of the Indian employees for pay day by Sir William Herschel; to the 1903 fingerprinting of criminals in New York State Prison; to the Visit Program of the United States; to the World's largest biometric database in India for social benefit delivery, biometric are coming of age.

In the past decade, the industry has seen remarkable developments in the field of storage methods and enrolment and verification procedures. Physical fingerprints taken by fingers dipped in indelible ink have given way to electronic sensors that capture the fingerprint image. Photographs that provide facial recognition have given way to face analysis system capturing internal skull geometry and skin texture sensing.

Eye colour/ retina recognition has evolved into iris recognition that cannot be tampered with. Electronic Sensors have been developed to accurately capture the different biometric characteristics so that they can be stored as electronically recognizable templates. Table 4 provides a list of evolving biometrics technologies that are gaining varying acceptance levels in various industry segments.

In the light of rapid speed of technological advancements of biometrics, the industry has witnessed accelerated standardization efforts to support inter-changeability and

interoperability of different systems. The next section provides a short overview of existing biometric standards that were developed to facilitate biometric systems interoperability, and enhance the effectiveness of biometrics products and processes.

1.3 Biometric Standards Evolution

Technically speaking, standards have been developed so that the electronic templates are generated, stored and retrieved in a uniformed way. The main impetus of biometrics standards is to define requirements, formats and software specification enabling interoperability between biometric systems, especially authentication systems. Biometric standards enable different streams of interoperability. One stream of standards enables interoperability of data collections and storage processes. The other steam enables interoperability of signal processing and matching technologies.

Evolution of standards signifies maturity of the technology, and standardization is envisaged to enable wide governmental adoption of biometrics. It provides a level playing field for device vendors and exchanging information at the national and international levels. This is to say that standards reduces risk to the integrator and the end user alike, primarily because it simplifies integration, and allows for substitution and upgrade of technologies, and reduces “vendor lock-in” effects (Tilton, 2006). This is likely to lead to a broader range and availability of products and movement towards commoditization (*ibid*).

There is still a long way to go for the standards that are developed to be uniformly adopted across the world. Biometrics standards have been developed by informal and formal standards organizations. In general, the following organizations are actively involved in the development of the standards and their adoption:

- International Committee for Information Technology Standards (INCITS) M1
- National Institute of Standards and Technology (NIST)
- Joint Technical Committee 1 (JTC 1)/Subcommittee 37 (SC 37)
- Organization for the Advancement of Structured Information Standards (OASIS)
- International Standards Organization (ISO)

The standards developed by these organizations provide a good indication to the current state of the biometric technologies. Currently, there exists a great maturity and consensus and definitive standards documents that have been released. They include, but are not limited to: Technical Interfaces, Data Interchange Formats, Application Profile Standards and Performance Testing.¹ These are briefly discussed next.

1.3.1 Technical Interfaces

These standards are related to the data capture of biometrics interfaces and interactions between biometric components and subsystems along with security mechanisms to protect stored data and data transferred between systems. They also include specifications of

¹ Refer to pg 138 Biometrics “Foundation Documents” & the document “Biometric Standards” published by NSTC Sub Committee on Biometrics for Bio-Standards.

architecture and operation of biometric systems for supporting multi-vendor systems and their applications. ANSI INCITS 358-2002 BioAPI Specification v1.1, ANSI INCITS 398-2005 [NISTIR 6529-A] Common Biometric Exchange File Format (CBEFF) are examples of Technical Interface Standards.

1.3.2 Data Interchange Formats

These standards specify the content, meaning, and representation of formats for the interchange of biometric data, e.g., Finger Pattern Based Interchange Format, Finger Minutiae Format for Data Interchange, Face Recognition Format for Data Interchange, Iris Interchange Format, Finger Image Based Interchange Format, Signature/Sign Image Based Interchange Format, and Hand Geometry Interchange Format; and specify notation and transfer formats that provide platform independence and separation of transfer syntax from content definition. Examples include ANSI INCITS 377-2004 Finger Pattern Based Interchange Format, ANSI INCITS 378-2004 Finger Minutiae Format for Data Interchange, and ANSI INCITS 379-2004 Iris Image Interchange Format.

1.3.3 Application Profile Standards

These standards specify one or more base standards and standardized profiles, and where applicable, the identification of chosen classes, conforming subsets, options, and parameters of those base standards or standardized profiles necessary to accomplish a particular function. Some of these standards are: ANSI INCITS 383-2003 Biometrics-Based Verification and Identification of Transportation workers and ANSI INCITS 394-2004 Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management.

1.3.4 Performance Testing and Reporting

These set of standards specify biometric performance metric definitions and calculations, approaches to test performance, and requirements for reporting the results of these tests. Examples include ANSI INCITS 409.1-2005 Biometric Performance Testing and Reporting Part 1 - Principles Framework; ANSI INCITS 409.2-2005 Biometric Performance Testing a Reporting Part 2 - Technology Testing Methodology; and ANSI INCITS 409.3-2005 Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies.

These standards among others establish the maturity of biometrics as a technology for personal identification. However, it is to be noted here that there is no one biometric characteristic that can be considered as a bullet proof solution. Usage of the biometrics characteristics depends entirely on the application.

Applications of biometrics are dictated by the circumstances, available data, security and risk assessment, number of people to be covered and so on. For example, in the US with a huge database of fingerprints of criminals, crime detection is relatively easier for Crime Scene Investigators to pick the fingerprints from the crime scene and match them with known prints.

With the new visitor biometric data (fingerprint, facial features) being collected, the USA, UK and other European countries are seeking to secure their borders from unauthorized entrants.

The Indian project which is billed as the world's largest biometric exercise seeks to collect the fingerprints of its 1.3 billion populations with the aim of ensuring transparent social benefit delivery to authorized individuals.

Fingerprint technology has wider acceptability worldwide due to its relatively lower implementation costs in comparison with other biometrics, and the availability of wider range of commercial applications in the industry. Nevertheless, the fingerprint as a biometric characteristic is not fraught without issues. For instance, any damage to the fingers renders the existing fingerprints useless. Further, it is very difficult to scan fingerprints and build templates for rough fingers or with cuts and damages.

These kinds of issues necessitate newer biometric technologies, newer sensors for detection and better computing algorithms for improvement of quality in enrolment and detection. The next section attempts to provide a highly level overview of developments in the biometric industry.

1.4 Advances in Biometrics

Recent advances in technologies and computing have enabled biometrics to evolve into a definitive and legally accepted means of personal identification. From the days of cataloguing fingerprints and establishing a match manually, computing techniques today have transformed biometrics.

Driven by the need to have more authentic characteristics for determining the identity, some biometric technologies are noticeably enhanced in the past decade. Multi-modal facial biometric with 3D face recognition is one of the techniques that have moved from laboratories to the commercial domain for mass production.

On the other hand, in the last half a decade, iris as a definitive biometric has advanced immensely. Iris is now a common biometric used to control borders in many countries in the world. Complemented by 3D facial recognition, the issue of live sensing of iris has been overcome to a large extent.

However, it is still not completely reliable in unsupervised applications. In supervised environments, iris recognition proffers excellent results. One of the well-known deployments of iris is UAE where iris detection is in place for monitoring all the visitors. This deployment is one the biggest and early success stories of iris technology in the world (Al-Raisi and Al-Khoury, 2006). See also Section 3 in this article.

Fingerprinting technologies now uses all ten fingers including the palm. As fingerprint databases growing bigger, it is no longer considered definitive with one or two fingers. The latest in hand geometry is Palm Vein recognition. Currently Fujitsu holds the patent for Palm vein recognition and scanners, detectors, and readers are commercially available using this technology.

The palm vein scanner works by capturing the images of vein patterns that are inside the body in a contactless manner, which makes it more sterile and hygienic to use. See also Figure 4.

This makes palm vein patterns difficult to forge, and thus more secure. Palm vein recognition technology also has one of the lowest false acceptance rates (FAR) and false rejection rates (FRR) i.e. false rejection rate of 0.01% and a false acceptance rate of less than 0.00008% (Sarkar et al., 2010).

Palm Vein Recognition is expected to be the major determinant in biometrics and to overcome many drawbacks that current fingerprints carry. This is the technology that promises a good touch of excitement in the days to come.

Besides technology, the major advancements have been in the domain of computing. The ability to deploy large relational databases with fast search engines has resulted in faster detection and identification times. Identification of a person has become easier and faster with the ability of 1:n matches in huge databases.

This has helped the law enforcement agencies big time. Computing and network technology has helped data exchange and information sharing easier and faster. This has resulted in better intelligence sharing among nations. There are numerous initiatives worldwide in ensuring standards in communication and protocols for data exchange. These standards have made interoperability of diverse systems easier and more efficient.

Last, but not the least is the progress made in the quality domain. Quality standards have been put in place for the capture of biometric templates. NIST (National Institute of Standards & Technology) launched the NFIQ (NIST Fingerprint Image Quality) in 2004 and sought to standardize the algorithm for fingerprint minutiae matching. ISO has been active through its Sub Committee SC 37 in defining various standards for biometrics including data exchange, BioAPIs, fingerprint data formats and storage.

Currently many more standards are under development under the SC 37- for example: Conformance testing methodologies (eg ISO/IEC 19794-9/PDAM 1); Procedures for the operation of the Biometric Registration Authority- ISO/IEC DIS 19785-2, to cite a few². Two other organizations actively involved in the standards development for biometrics are the INCITS (International Committee on Information Technology Standards) M1, and OASIS (Organization for the Advancement of Structure Information Standards).

These standards and the evolution of quality in biometrics promise major advances in biometric sensing technology. Better sensors provide higher sensitivity, better resolution and higher repeatability. This contributes to lower False Rejection Rate (FRR) figures, lower False Acceptance Rate (FAR) and better Cross-over Error Rates (CER).

Over the past few years, advancements in sensing technologies have enabled higher speed and throughput rates. Higher throughput rates meant larger number of enrolment capacity and processing. Such advancements have paved the way for many governments to initiate mass enrolment programs at a national level to capture the biometrics of their population.

² Refer to ISO Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770

Table 4: Evolving biometrical technologies

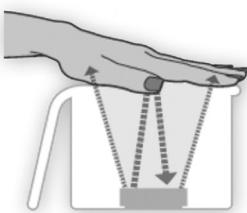
Biometric Technology	How it operates ?
Fingerprints	A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.
Iris Scan	One of the most accurate biometric processes in which the veins structure in the iris is used as biometric sample to identify a person. Being an internal organ of the eye whose random texture is stable throughout life, the iris is immune (unlike fingerprints) to environmental influences, except for its papillary response to light. Working on completely different principles from retinal scanning, iris recognition is far more user friendly and offers very high accuracy.
Facial recognition	Facial recognition is an automated method to record the spatial geometry of distinguishing features of the face. Non-cooperative behaviour by the user and environmental factors, such as lighting conditions, can degrade performance for facial recognition technologies.
Voice Recognition	Focuses on differences resulting from the shape of vocal tracts and learned speaking habits. The technology is not well-developed as background noise may affect its performance and reliability.
Palm print./hand geometry	The capture of measurements encompassing the width, height and length of the fingers, distances between joints and shapes of the knuckles. While reasonably diverse, the geometry of an individual's hands is not necessarily unique.
Retinal Scan	Measures the blood vessel patterns in the back of the eye. Because the retina can change with certain medical conditions, such as pregnancy, high blood pressure, and AIDS, this biometric has the potential to reveal more data about individuals than only their identity, and is perceived an intrusive technology, and has lost popularity with end-users.
Vein pattern image	The vein (vascular) pattern image of an individual's hand can be captured by radiation of near-infrared rays. It can be done by using the reflection method to photograph the veins in the hand by illuminating the palm and photographing the reflected light from the back of the palm.
DNA	Except for identical twins, each person's DNA is unique. It can thus be considered a 'perfect' modality for identity verification. DNA identification techniques look at specific areas within the long human DNA sequence, which are known to vary widely between people. The accuracy of this technique is thus very high, and allows both identification and verification.
Gait recognition	Captures a sequence of images for analysis of how an individual walks. Still in an early stage of research & development.

Biometric Technology	How it operates ?
Keystroke recognition	Assesses the user's typing style, including how long each key is depressed (dwell time), time between key strokes (flight time) and typical typing errors. This is more suited as an internal security technology, such as providing computer access within an organisation.
Signature recognition	Analyses a series of movements that contain unique biometric data such as personal rhythm, acceleration and pressure flow. Since these movements can vary with each signing, differentiating between the consistent and the behavioural parts of a signature is difficult.

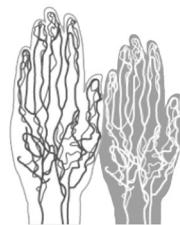
Hands Down

How palm-scanning identification works:

The scanner emits infrared light. Hemoglobin in the veins absorbs the light...



...enerating an image of the vein pattern that is reflected back and captured by the scanner.



The scan is stored in a database. A returning user's vein pattern is compared against the database to determine if there is a match.

Figure 4: Palm Vein Recognition

2. Government Biometric Programmes: enabling initiatives of the new economy

Identity management has always been a key challenge for governments across the globe. Governments have striven to provide its citizens security and protection, ease of access across its national borders, and ensure that social benefits reach the rightful and deserving citizens. Governments in this day and age seek proven methods to establish the identities of their population in order to provide secure access to government applications and services. Table 5 summarizes a generic model used for identity requirements for benefit delivery and privilege accordance.

In the past, services or benefits delivered across different channels had to be severely limited owing to lack of credible verification of identity of the beneficiaries. Citizens had to necessarily walk into government offices that demanded different identification checks to verify the identity of a benefit claimant. Needless to say governments relied heavily on biographical information to manage the identity of their citizens. Passports, although considered as travel documents, were considered as a primary identity document in many countries around the world.

Many countries have made attempts to provide simpler identification methods in terms of paper based identity cards carrying the photograph of the person. These identity documents served a limited purpose since the identity largely depended on the photograph and it was easy to reproduce or fake such documents. Paper ID cards were then replaced by plastic cards. Plastic cards with embossing, watermarks, holograms were adopted to reduce the risk of fake cards. All of these approaches met with limited success due to the limitations of usage and applications of different business needs.

Governments around the world implemented copious identity management programs in the last 10 years that addressed discrete strategic needs. One of the early and major applications was in border security domain. Border security systems differ between countries, however, in general, all visitors and residents are normally needed to apply for a visa or a visa equivalent, with conditions appropriate to their stay. This visa is verified at the border and passes through a number of checking layers, many unknown to the traveler, and if found genuine and authentic, the person carrying the visa is allowed into the country.

Visas are produced in the form of a paper and attached to passports. Paper visas are fraught with issues. This is a major concern for the border security. The need for more effective management of national borders and identity fraud has brought about an increased demand for secure end-to-end identity systems

Application	Remarks
Simple Identification	Security Check and Physical Identification
ID Required to be entered as data	ID required as entry in Service Application Forms
Service Requested OTC (Over the Counter)	ID required to ensure that it is being delivered to the correct person and require confirmation of service delivery (signature of service beneficiary)
Service Requested Remotely	Manual Entry of ID in Application Forms
Service to be delivered remotely	ID required to ensure it is being delivered to the correct person and require confirmation of service delivery

Table 5: Identity requirements for government service delivery

Biometric technologies have emerged as critical components of identity and security programs. With the kind of reliability and acceptance that fingerprints, facial recognition and iris recognition have gained in the last decade, complemented by the advances in computing techniques, biometrics is being increasingly used internationally as a high-technology identity management tool to strengthen identification processes. See also Figure 5.

Evidently, there have been and continue to be numerous attempts by countries to enumerate their citizens, enlist them, register them and more importantly identify them. Table 6 provides a global overview of biometrics applications by governments worldwide.

The USA, India, UAE, Malaysia, South Korea, UK, France have been mentioned before that have taken a lead in biometric implementation. USA, UAE and UK are early adopters and leading examples of biometric implementations for Border Security. Entry of visitors to these countries is mandated by fingerprints to be collected at the time of granting of approval to visit the country (Visa Issuance). Fingerprints are verified at the time of actual entry and if found matching, entry is granted.

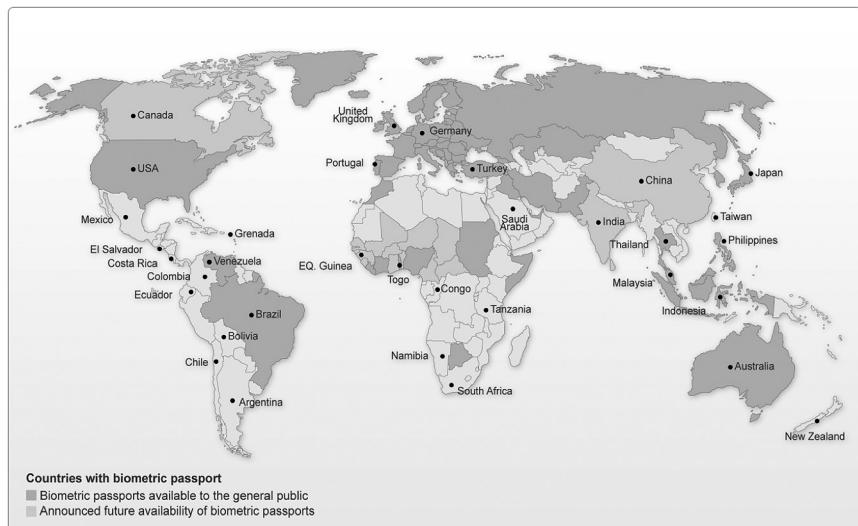


Figure 5: Global biometric adoption

2.1 Emerging roles of governments

The globalisation and the rapid pace of development in information and communication technologies are redefining the nature of governments and their relationship with citizens (Guthrie, 2003). With such developments, public services are challenged to re-invent the government in the digital economy.

This necessitates re-thinking the way governments have been dealing with citizens and business, re-engineering their work processes and as well as enabling greater cross-agency collaboration to deliver services in a way which the public appreciates (*ibid*). As such, identity management is a critical success factor to enable such transformation. Robust identity management infrastructure is envisaged to enable digital economy, with identification and authentication systems that people can live with, trust and use (Stevens et al., 2010). There is accumulating evidence that governments are sources of powerful forces influencing the development of new industries (Ke and Wang, 2008). Yet, governments, as a valid and powerful context have the potential to influence the digital economy creation (*ibid*). Existing literature argue that there is enough indication that due to network externality effects, governments need to take an active role in stimulating an e-environment to jump-start the move toward a higher level of e-readiness.

Country	Biometrics Applications
Canada	<ul style="list-style-type: none"> • 2005: Iris recognition at airports to expedite pre-approved travelers through customs and immigration • 2011: Fingerprints-based immigration and border entry system launched
USA	<ul style="list-style-type: none"> • 1999: FBI's IAFIS (Integrated Automated Fingerprint Identification System) becomes operational with the world's largest biometric database with about 55Million records. • 2008: FBI expands this databasewith NGI (Next Generation Identification to include multimodal biometrics (faces, iris, fingerprints and palm patterns) • 2004: US-VISIT (US-Visitor and Immigrant Status Indicator Technology) launched for border control with full integration to IAFIS as the goal • 2007: e-Passports issued with Basic Access Control and PKI
Mexico	<ul style="list-style-type: none"> • 2009: The Mexican government announces new biometric identity card which will carry fingerprints, a retina scan and a photograph on a magnetic strip to fight corruption in social programs under Mexican Interior Ministry (Instituto Mexicano del Seguro Social).
Salvador	<ul style="list-style-type: none"> • 1999: Fingerprints based drivers license initiative launched • 2007: Multimodal Biometric passport deployment started and later expanded to include criminal justice system apart from Border control.
Costa Rica	<ul style="list-style-type: none"> • 1998: National ID Card initiative with fingerprints and photographs launched to replace paper based ID cards • 2003: Central Bank launches biometric identification system for secure access to central bank databases for member banks • 2010: Smart Cards initiative launched for secure biometric information on the cards
Colombia	<ul style="list-style-type: none"> • 1995: Digital Identification reform brought in for introducing biometric information in digital format for National Civil registration and issue of new ID cards for the purpose of Elections and Civil transactions. • 2005: Automated Banking Machines introduced for ATM transactions using biometrics • 2009: The Colombian government makes significant changes to the Cedula and it requires all citizens to change to the new national ID for the presidential elections in 2010.
Grenada	<ul style="list-style-type: none"> • 2009: Initiates the Civil Identification Registration Program as a part of the Caribbean initiative for Electoral and Civil Identification purposes
Venezuela	<ul style="list-style-type: none"> • 2007: launches National ID Card with facial and fingerprint data modernizing the Civil Registry for the purpose of electoral system and civil transactions.
Ecuador	<ul style="list-style-type: none"> • 2007: Part of the CLARIEV initiative in preparing digital civil registry with biometric identification of photograph and fingerprints. • 2009: Launched the Biometric Screening System for Foreigners at various points of entry to prevent illegals from neighboring countries to enter
Bolivia	<ul style="list-style-type: none"> • 2009: Biometric Registration of all eligible citizens conducted and a biometric database of Electoral Voter List is created. Successfully conducts Presidential Elections using the biometric database.
Brazil	<ul style="list-style-type: none"> • 2007: National ID Cards with Biometric Data provided to replace paper cards • 2011: New Generation Smart Cards- called the Civil Identity Registry (Registro de Identidade Civil – RIC) with enhanced security features for biometric data of fingerprints and facial data launched and expected to replace all existing cards by 2019 • 2010: Uses Biometric database for conducting elections using biometrics as a primary identification for voters

Country	Biometrics Applications
Argentina	<ul style="list-style-type: none"> • 2010: Re launches National ID in the form of the Passport booklet including biometric information of fingerprints and facial data • 2011: launches Biometric enrollment for travel and ID documents for expats living outside of Argentina and also for foreign visitors intending to travel to Argentina
Chile	<ul style="list-style-type: none"> • 1997: Wide spread use of Biometrics in Criminal records • 2007: Part of CLARIEV- initiative in Civil Registry • 2007/8: Implementation of Biometric Research Laboratory to validate facial/Iris identification database, benchmarking of search algorithms for 1:N in a 16Million records database
Togo	<ul style="list-style-type: none"> • 2009: Keeping in line with their commitment to the Economic Community of African States (ECOWAS), Togo adopts the Biometric Passports containing non-repudiated fingerprint information to enhance border access. Non-machine readable passports phased out in 2010, along with other African Nations of ECOWAS (namely Nigeria, Niger, Guinea, Senegal, Cote D'Ivoire, Liberia, Benin and Ghana) –Togo, has issued Biometric passports to its citizens
EQ. Guinea	<ul style="list-style-type: none"> • 2010: The Economic and Monetary Community of Central African States (CEMAC) is set to put biometric passports into circulation within its member states. Members of CEMAC are Cameroon, Congo, Central African Republic, Gabon, Equatorial Guinea and Chad.
Congo	<ul style="list-style-type: none"> • 2004: Congo launches a unique Iris based identification system for rehabilitation of the ex-combatants of wars to civil life. This program- The Programme National de Désarmement, Démobilisation, et Reinsertion (PNDDR) has proved immensely successful. • 2010: Launches Biometric Passports under the CEMAC program.
Tanzania	<ul style="list-style-type: none"> • 2011: National Identification Authority launches system for issuing of 25 Million Smart ID Cards with biometric for national identification and civil use. • 2011: Biometric authentication based Kiosks deployed as part of e-Government initiatives for enabling eligible citizens to access the Social Security funds and conduct transactions electronically through the kiosks.
Namibia	<ul style="list-style-type: none"> • 2007: Biometric Driver's license deployed and in action
South Africa	<ul style="list-style-type: none"> • 2002: Automatic Fingerprint Identification System introduced for aiding criminal justice, digitizing about 4.5Million criminal records and fingerprints collected from 1920 • 1993: HANIS (Home Affairs National Identification System) launched with biometric data collection as part of Identification booklet issued with a 2D Barcode • 2010: Smart ID Card with Biometric data initiated
Germany	<ul style="list-style-type: none"> • 2010: RFID based Smart cards with digital data including biometric information initiated to replace normal plastic ID Cards • 2003: AFIS introduced for visitors to Germany as part of Schengen Visa for biometric identification. Iris recorded at Airports on entry for monitoring visitors • 2005: e-Passport System with integrated biometric data goes live with facial image as primary biometric identifier • 2007: Second Gen e-Passport released with fingerprint as the primary identifier complying with EU regulations on eMRTD • 2010: Biometric data enabled RFID Smart Cards started to be issued as National ID Cards

Country	Biometrics Applications
UK	<ul style="list-style-type: none"> 2001: A formal entity- The BWG (Biometrics Working Group) established under the CESG (Communications-Electronics Security Group). The UK Biometrics Working Group (BWG) is a cross government group focused on the use of biometric technology across government and Critical National Infrastructure (CNI) 2005: Iris and Fingerprint recognition for visa holders and frequent travelers for Border Control 2006: e-Passports with Biometric data – fingerprint, iris and facial data started to be issued to British citizens compliant with US Visa Waiver Program 2010: Second Generation e-Passports with enhanced security features introduced.
Portugal	<ul style="list-style-type: none"> 2006: e-Passports compliant with EU standards issued. 2007: National ID Cards with fingerprint data, photograph and digital signature issued to citizens. 2007: Portugal's Faro Airport becomes the first airport to begin using e-Passport biometric reading for fast track entry into the country followed by Lisbon.
Turkey	<ul style="list-style-type: none"> 2007: Smart cards with personal information and fingerprint data launched for Healthcare services. 2010: e-Passports with fingerprint and facial recognition launched in Turkey
Saudi Arabia	<ul style="list-style-type: none"> 2006: Starts issuing Biometric data enabled smart cards as National ID Card for all citizens and residents for primary ID for civil transactions. 2010: Saudi announces requirement of fingerprints for all visitors as part of identification for border security. 2003: Starts issuing Smart Card based National ID Cards with fingerprint data
UAE	<ul style="list-style-type: none"> 2003: UAE is the first country to Start Iris recognition for all visitors at Dubai airport and subsequently extends it to all International airports in the country. 2005: Starts issuing chip based Smart Cards as National ID Cards with biometric data (fingerprint), photograph and digital signature for signing. 2010: Starts issuing second generation ID Cards with RFID capabilities as a combi-card 2004: Biometric enabled e-Gate card launched and issued to residents and citizens enabling fast track entry and exit from the Country's airports based on fingerprint identification 2009: Biometric e-Passports program launched with RFID and fingerprint data that can be read by machines. 2011: National Elections being held with the help of National ID Cards with Biometric verification for voters.
Bahrain	<ul style="list-style-type: none"> 2005: Introduces the Smart Card based ID Card with fingerprint data for identification and authentication to replace the CPR card in a phased manner. 2009: Installs biometric scanners and high security immigration gates at its airport, becoming the third country after UK and Japan to do so
Qatar	<ul style="list-style-type: none"> 2006: Introduces Smart Card based ID Card with fingerprint, facial features and iris data along with personal data to replace their existing plastic ID Card.
Oman	<ul style="list-style-type: none"> 2004: Launches National Registry System for issuance of smart cards as Electronic ID Card with biometric information securely embedded in the ID cards for all civil transactions. 2006: Issues Smart ID Cards to all citizens
Kuwait	<ul style="list-style-type: none"> 2009: Launches new smart card ID Cards for Civil ID Cards that include fingerprint and DNA information as biometric data for identification of citizens and residents in the country. Biometric Data is part of the Civil Register. Enhanced capabilities include PKI for digital signatures.

Country	Biometrics Applications
India	<ul style="list-style-type: none"> • 2009: India launches the most ambitious Bio-enrollment program for identification of its 1.2 billion population. The program aims at providing a Unique Identity to all the citizens with the fingerprints as primary identifiers and iris scan as well. The primary goal of the Biometric ID is to ensure social benefits distribution to rightful and deserving citizens and prevent theft of social funds.
China	<ul style="list-style-type: none"> • 2005: One of the early adopters of Biometric technology for automated border crossing- installs biometric access gates between Shenzhen and Hongkong, catering to nearly 400,000 crossings every day. This is followed by Zhau-Macau border in 2006.
Thailand	<ul style="list-style-type: none"> • 2005: Smart ID Cards with fingerprint biometric data with Match-On-Card capabilities launched for personal Identification.
Malaysia	<ul style="list-style-type: none"> • 2011: Biometric fingerprint system introduced for all foreign visitors entering Malaysia at the Airports and other entry points (Singapore-Malaysia) • 2011: Election Commission adopts biometric technology for voter identification • 2005: MyKad- the National ID Card with smart card capabilities launched with biometric data for identification of card holders extending from their 2011 initiative. • 2005: Cyber Security Malaysia becomes the sole certification agency for smart card based applications and readers for Common Criteria certification in Malaysia.
Japan	<ul style="list-style-type: none"> • 2007: Biometric Identification systems deployed in airports across the country and extended to all borders in 2008 • 2006: Biometric Passports meeting US Visa Waiver program start being issued to Japanese Citizens • 2010: Widespread use of Biometrics in Kiosks, ATMs
Taiwan	<ul style="list-style-type: none"> • 2011: Biometric Border Control systems deployed on trial • 2009: Biometric e-Passports launched for issuing e-Passports to Taiwanese citizens
Philippines	<ul style="list-style-type: none"> • 1998: Social Security Cards with Biometric data issued to Philippines citizens and residents to prevent fraud • 2009: e-Passports with Biometric data introduced to replace all existing passports. All renewals issued with new Biometric passports • 2010: The Government announces Biometric registration for Elections for Voter registration
Indonesia	<ul style="list-style-type: none"> • 2010: Launches biometric verification and identification at the airports border control • 2009: Biometric Passports start being issued as e-Passports
Australia	<ul style="list-style-type: none"> • 2008: Smart gate- Biometric border control systems launched • 2011: Australia seeks to establish Biometrics Working Group to guide biometric implementation across the nation • 2006: Biometric e-Passport system launched
New Zealand	<ul style="list-style-type: none"> • 2006: Biometric Immigration systems for border control at airports launched • 2009: Biometric Registry for Immigration and Biometric Passports for citizens deployed

Table 6: International practices of biometrics applications

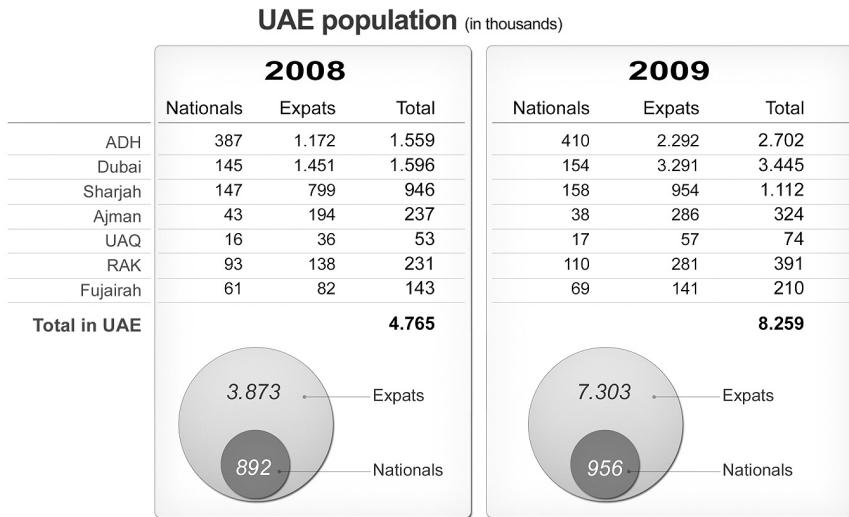


Figure 6: UAE population demographics

De Meyer and Loh (2004) allege that governments can play an important role in at least four areas: (1) stimulating the enhancement of the infrastructure that enable e-society; (2) investing in improved services (e-government); (3) stimulating an e-friendly business environment; and (4) creating an all-inclusive information society. He further elaborates that for an e-environment to exist, a basic ICT infrastructure need to be put in place in order to reach out to citizens and to provide a robust network over which business can operate.

The literature in general, widely disagrees with the concept of dependence on the private sector to build such infrastructure all alone, and believe that if it did, it will produce inept and hurdled efforts that will be insufficient to gain social acceptance and trust (Al-Khoury & Bal, 2007; Al-Khoury, 2010; De Meyer and Loh, 2004).

Apparently, biometrics offer tremendous opportunities to create new value, and to provide instant knowledge and processing capability to make quantum leaps in identity management and service delivery (Guthrie, 2003). Governments are therefore assuming new roles to build trust in online identities in order to improve electronic delivery of government and business services. This confidence is seen to encourage innovation in the online marketplace and foster the growth of the new digital economy.

Networks are a key component of this new society, as illustrated by the rise of mobile phones, email, and social networking websites, yet the networks in the digital world are constantly changing (IMA, 2011). Governments have for long been responsible to develop methods for physical identification of identities. In today's world, governments³ are recognizing that

their boundaries of responsibilities need to expand and include virtual and digital networks revolutionise and/or create new business and social paradigms.

"Modeling the digital world is not like modeling the physical world, where established equations govern the movement of atoms or the flow of electrons. Interactions between people and information are more complicated, and we need to develop new concepts and models to understand and predict their behaviour in the new digital society."

The institute of mathematics and its application, UK.

Biometrics provides a stupendous opportunity to create a new understanding of digital interactions. Many governments in the world have invested intensely in the last decade to develop identity management solutions for identification and authentication of physical and virtual identities. These solutions are based on the traditionally accepted means of identification and authentication of one or more of three general principles: (1) what the person knows (some form of shared secret like passwords), what he possesses (some kind of unique token or key e.g., smart card), or what he is (some aspect of his physical being i.e., biometrics).

The application of Public Key Infrastructure technology with its digital signature capability coupled with biometric identifiers have the potential to provide a strong authentication and non-repudiation assurances in digital networks. Digital signatures identify and authenticate the originator of the information. They allow the receiver to ascertain the identity of the sender and to determine whether the message changed during transit (Uhlfelder, 2000). In addition, they permit verification that the information has remained unchanged after the sender signed the message and allow a user to securely identify himself or herself on the network (*ibid*).

The use of digital signatures and biometric identifiers when implemented together may complement each other, with the strengths of each technology offsetting potential weaknesses in the other (Jueneman and Robertson, 1998). Having said this, the next section provides an overview of recent deployments of biometrics technologies in the United Arab Emirates to address different national strategic needs.

3. UAE initiatives in Biometric Identification

UAE is a pioneer in its biometric implementation. It has integrated multiple biometric technologies in critical infrastructure systems in the last decade. Following are few examples of recent projects in the field of biometrics implementation.

3.1 Iris recognition

At the country's entry points, all visitors are required to undergo an iris scan. Via secure national

- 3 • President Obama's technology-based American presidential campaign changed the face of US elections and he has made it clear that he sees both technology and a strong communications infrastructure as vital to economic recovery and growth. This includes a radical approach to the deployment of a modern communications infrastructure, including redefining universal service to extend its scope to broadband and unleashing the power of the wireless radio spectrum.
- The French Government has recently launched its France Numerique 2012 plan, an ambitious communications sector strategy designed to strengthen France's digital position and enhance its broader competitiveness at a time of global economic slowdown and crisis. The message laid out in the plan is clear: the digital economy is the most dynamic sector in the world and as the global recession bites, it is essential to nurture those parts of the economy that can generate growth potential and jobs.

network infrastructure, each of the daily estimated 20,000 travelers entering the country goes through iris screening; where each presented passenger's iris is compared exhaustively against all templates in the 2.3 million watch-list database.

The UAE began the implementation of iris recognition technology at its borders in 2001 to inhibit illegal entry of persons in the country. The UAE was the first in the world to introduce such a large scale deployment of this technology. Today, all of the UAE's land, air and sea ports of entry are equipped with iris systems.

UAE iris watch-list database is currently the largest in the world, both in terms of number of iris records enrolled (more than 2.3 million people) and number of iris comparisons performed daily i.e., more than 15 billion cross comparisons in an exhaustive (1:n) comparison. More than 320,000 deported people had been caught at airports trying to re-enter the country after being deported using new passports with sometimes different biographical information.

3.2 Facial Recognition

Facial recognition (facial on the move) has been implemented recently at UAE airports in 2008 to enhance security procedures and detect persons who might pose a threat to the country. The system allows critical identification checks to be performed from a distance without a person's active participation. The system helps inspectors at control points inside the airports to implement continuous and proactive checks designed to immediately detect persons who should be denied entry or detained.

The system can identify persons live or from photographs. It can identify persons while they are moving with a high degree of accuracy. The system which is still at a trial phase is expected to be rolled at all points of entry in the country in the coming 2 to 3 years.

3.3 Fingerprint based - Electronic Gates

UAE has another biometric application working at its airports; namely biometric based electronic gates (e-gate). The e-gate facility which was first introduced in 2002 in Dubai International Airport, is the first airport in the region and the third in the world offering this service to travelers. The service is basically available for quick passage through passport control.

The electronic gate uses fingerprint biometrics to automatically process all registered passengers arriving and leaving from any of the UAE airports. This is an advanced passenger clearance system that considerably accelerates the movement of traffic through electronic screening of passengers' data with the help of a smart card. It was estimated that more than 4 million travelers used electronic gates in 2010. The government is working on a plan to encourage the usage of electronic gates and to make it almost compulsory for travelling adults without children companions.

3.4 Electronic Passport

The UAE government is in the process of launching its new electronic passport in the coming six months (also referred to as a biometric passport). The new passport contains biometric

information mainly fingerprints and ICAO standard photograph, that will be used to authenticate the identity of travelers. The information on the chips can be scanned and verified at airports, other ports and border posts.

PKI technology is used to sign the electronic data stored in the passport microprocessor chip. This is expected to enhance the current security features of passports and provide greater protection against tampering and reduce the risk of identity fraud. The issuance process is linked with the expiry of the existing passports as it will be replaced with the electronic ones. The biographical and fingerprint data are pulled electronically from the national identity register, detailed below.

3.5 National Identity Register

Another ambitious and large scale biometric program was launched in 2003. The program aims to set up a national identity register and to enrol an estimated 9 million population in the country. This program, which is also referred to by the UAE government as the national identity management infrastructure, aims to serve multiple strategic objectives. The primary objective was to set up a government entity that has an imperative role as the single source for personal identity provision in the Country.

Through a comprehensive data bank, the government seeks to help conserve billions of government investments in the duplication of data by different government agencies. The advanced identification mechanisms offered by this program are envisaged to provide a highly credible identity base to revolutionise public services and support digital economy creation. Section four further elaborates on this project and discussed its key components and objectives.

3.6 Federal DNA Project

The government has begun a DNA identification database development in 2010. The project which is still in its pilot phase, targets to collect DNA samples of 10 million people both national citizens and foreign residents in the next few years. The federal DNA database is primarily seen to contribute to areas related to crime detection and identification of criminals.

The field of biometrics overall in the United Arab Emirates is gaining prominence and the government seems to be convinced of the potentials of these technologies to provide a stronger authentication and reduce the risk of identity fraud. It has invested substantially in biometrics solutions in the past few years as we have illustrated in the few examples above.

The market in the UAE has seen some trails of biometrics in public and private sectors however they were primarily limited to the field of physical access control. The application of the new UAE biometric identity card capabilities, to provide secure identification and personal verification solutions, is envisaged to improve public acceptance of the technology and vitalise electronic transactions, as the next section outlines.

4.The National Identity Register Program of UAE

The UAE has a very interesting population demographics. Out of an estimated 8.2 million,

only as little as 10% of its population are national citizens. The remaining 90% represents foreign resident population working on a maximum of 3 year work permits or as expats family companions. Nearly citizens of 180 countries across the globe are legal residents in the UAE. The strong economic growth in the country attracted such diverse workers from all over the world, and is continuing to grow at a rapid rate. Figure 6 shows the changing patterns of population demographics in the UAE.

The UAE realised the need for a more sophisticated identity management system in light of the unique composition of its population. The UAE launched its national identity register program in 2003. The actual population enrolment started in mid 2005.

The program was launched with the objective to build an identity management infrastructure that has a derivative role as the single point of authority for the provision of identity information in the country. This was envisaged to allow the government to better plan its development priorities. Clearly, the growth rate was a determining factor to address the changing needs of its people for infrastructure (e.g., schools, hospitals, housing, roads), resources (e.g., food, water, electricity), and jobs.

Another important objective was related to improving government service delivery, and to develop the infrastructure for the new digital economy. The program with its advanced technological components, intend to develop and provide digital identities to each citizen and resident in the country and in an attempt to revolutionise its e-government and e-commerce initiatives. The digital identity of a person is established through a combination of three critical components:

- National Identification Number
- A set of biometrics (photograph, fingerprints, - iris is being piloted)
- A Digital certificate consisting of Private and Public keys issued by a National PKI (Public Key Infrastructure).

All the attributes of the personal identity are packaged together and issued in a single instrument of identity; the UAE National Identity Card. Out of an estimated 8.2 million population, more than half have been enrolled in the scheme to date. The remaining population is expected to be enrolled by 2013.

The government follows a stringent enrolment processes compliant with international standards in acquiring the biometric data of the citizens. Registration centres are established all across the country serving the citizens and residents to enrol in the National Identity Register.

Mainly, fingerprints (rolled prints, palm prints, writer's palm prints) and facial recognition are captured biometrics. Following NFIQ compliant standards, the biometric data is processed and stored in the card along with the digital certificate. See also Figure 7. Iris recognition is expected to complement the current biometrics during renewals. The main reason for not including a third biometric was due to reasons related to not causing interruption to the enrolment process.

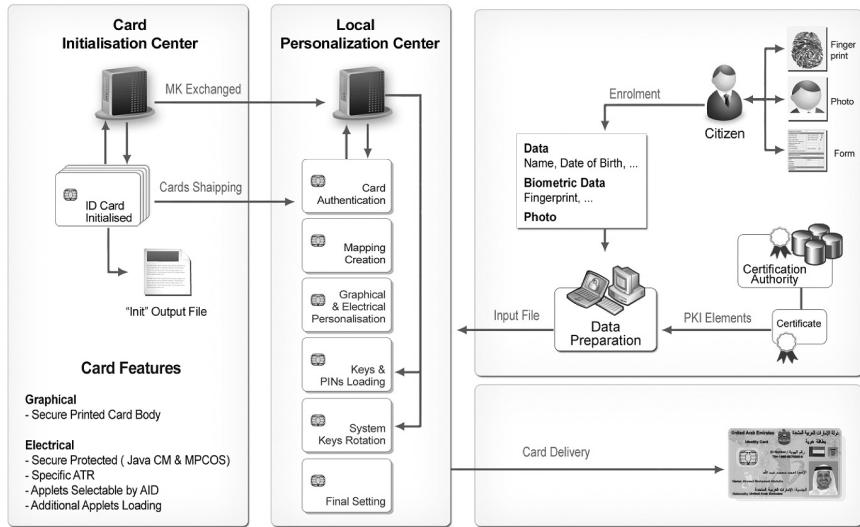


Figure 7: UAE ID card issuance process.

Applet	Interface	Functionality
ID & E-Purse Applet	Contact and Contactless except for E-Purse the interface is only Contact	<p>There are 10 personal identification data folders in the EEPROM of the UAE Card. Those 10 personal identification data folders provide various identification data about the ID Card holder including E-Purse data. The function of the "ID Applet" is to manage access to those folders. Another function of the "ID Applet" is to provide cryptographic services namely mutual authentication and verification of digital certificate of personalized data.</p> <p>The 10 identification folders (referred to as ID Application Data Folders) are as follows:</p> <ol style="list-style-type: none"> 1. Public ID Data 2. E-Purse Data 3. Labor Data 4. Health Data 5. Defense Data 6. Driving License Data 7. Family Book Data 8. Social Services Data 9. Address Data 10. Qualification Data

Table 7: Overview of UAE ID card capabilities and functions

Applet	Interface	Functionality
PKI Applet	Contact	<p>The function of the PKI applet is to facilitate the electronic authentication of the ID Card holder and to facilitate the generation of electronic signatures by the ID Card holder (within a PKI infrastructure).</p> <p>The PKI Application Data Folder in the EEPROM contains provision for 5 RSA Key Pairs and provision for the corresponding 5 RSA Certificates. During personalization, only 2 Key Pairs are personalized and their corresponding 2 digital certificates are constructed. Those 2 Key Pairs are used for the Authentication and Digital Signature functionalities. The files for the remaining 3 Key Pairs and their corresponding 3 digital certificates are left empty (RFU).</p> <p>3 PINs are personalized (User, Admin, & RFU)</p>
MOC Applet	Contact	<p>The MOC is a third party applet. Hence, the applet byte code is personalized in the EEPROM. The MOC applet stores two fingerprint templates of the ID Card holder. The applet facilitates the biometric authentication of the ID Card holder by comparing the ID Card holder fingerprint captured by a biometric terminal at a service counter against the fingerprint template stored inside the ID Card.</p>
eTravel Applet	Contact and contactless	<p>This is an ICAO compliant applet. It contains 5 data groups and a separate elementary file as follows:</p> <p>DG1: MRZ containing basic personal details DG2: Portrait DG11: Additional personal details DG13: Full name (Arabic) and date of expiry DG15: Active Authentication Public Key EF.SOD (Post Perso): Data signature Phase 2 will contain the following additional data groups and an elementary file: DG3: 2 fingerprints (ISO 19794-4) DG14: RSA or ECDH Parameters (EAC Authentication) EF.CVCA: Certification Authority Reference</p>
MIFARE Applet	Contactless	<p>This is an applet that emulates the functionality of the 1K MIFARE contactless card.</p>

4.1 The UAE National ID Card Features

Adopting a slew of security features, and internationally recognised biometric standards and the latest computing techniques, UAE issues the most advanced smart cards to all its citizens and residents. Figure 8 depicts some of the physical security features in the card.

The microprocessor card which is Java based serves a dual purpose of micro computing as well as secure storage. Micro computing allows complex encryption algorithms to run efficiently

and effectively on the card. This enables secure storage of data ensuring tamper proof identity data including biometric data.

The UAE was one of the early adopters of match-on-card feature. This feature enables fingerprint Match-on-Card user authentication as an alternative and to complement smart card PIN verification. This in turn gives access to the digital certificates on the card that can then be used for logon, digital signature, file encryption, secure VPN access among other services.

This solution provides a secure two or three factor authentication capability that is convenient for users, easy to deploy and manage, and fully compatible with the smart card security components available in Windows operating systems. It is also compatible, with the majority of fingerprint sensors available in the market.



The card is a hybrid smartcard that also contains PIN protected personal data including digital certificates, and the holder's biographical data and two best fingerprints. The card is envisaged to be the only acceptable identity document to access any government and some critical private sector services like the financial sector. The 144KB-combi card is a multi-application card and designed to be fully compliant with the two major industry standards:

- The Global Platform Card Specification Version 2.0.1', that defines the card management; and
- Visa Card Implementation Requirements Configuration 1-Compact" by virtue of the enhancement in the card by the additional security features described in the "Open Platform 2.0.1".

Both the Java Card Runtime Environment (JCER) and the Global Platform (GP) standards contribute to the security features of the UAE National ID card. Java provides cryptographic

mechanisms and enforces firewalls to protect applications and maintain data and operation security within the multi-application shared card space. The GP 2.0.1⁴ specifications extend the Java Card cryptographic authentication mechanisms to ensure dynamic and secure loading/updating of individual applications in the dynamic and multi-applet Java Card.

PKI Validation Services	Identity Data Provider Service	Card Validation Services
<ul style="list-style-type: none"> Used in a business scenario where a Service Provider handles the authentication process and needs only PKI validation. A secure '<i>valid/not valid</i>' engine providing Real Time validation of ID certificates through OCSP. 	<ul style="list-style-type: none"> For Service Providers that hand off the complete authentication process to Emirates Identity Authority . Offers Authentication as a Service (e.g. On-demand Authentication) Implements the SAML IdP (Identity Provider) protocols Provides 2-factor ID Card authentication 	<ul style="list-style-type: none"> Added-values services such as PIN Change, Verify Card Genuine and Biometric Verification.

Table 8: National Validation Gateway Services

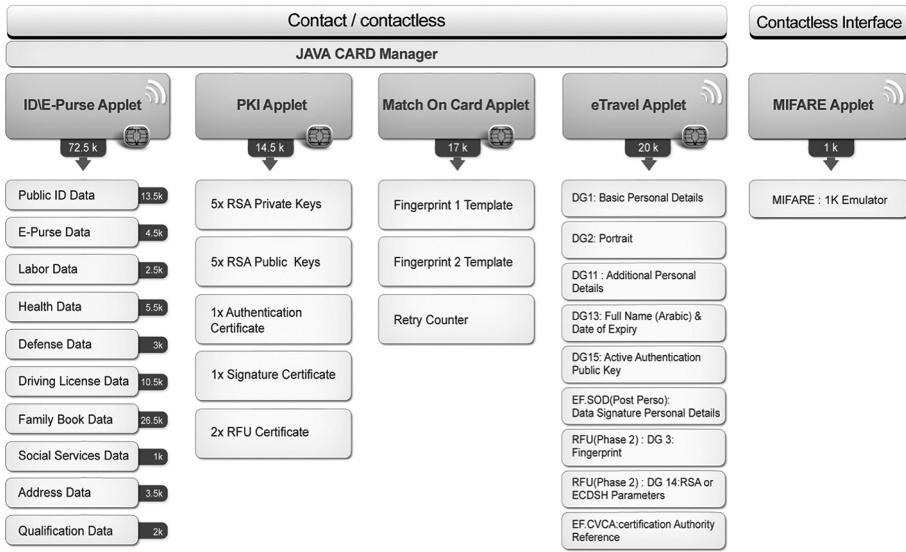
Three unique features are provided in the card that makes the UAE national identity card distinct in its application in the world. There are five applets in the UAE identity card: (1) ID and ePurse applet, (2) PKI applet, (3) Match on Card (MoC) applet, (4) eTravel Applet, and (5) MIFARE Applet. See also Figure 9. These applets do not share data inside the card and are completely secure. Communication with the card can only be established using the SDK/Tool Kit distributed by the government.

The applets are self-contained in the card and run as applications on the card, without the stored data ever leaving the card. These features enable instant identification/recognition, validation of credentials, verification and most importantly provide assurance of the established identity. This is envisaged to greatly enhance the acceptability and reliability of the card in the country.

4.2 Functions of the UAE National ID Card

The main function that the UAE card serves is that of establishing irrefutable identification of the cardholder. Match on Card function provides instant verification of the biometric data of the cardholder. One of the key infrastructure technologies in the program is Public Key Infrastructure (PKI). The PKI provides the functionality of digital signature enabling transactions between individuals and organizations on the virtual space of internet.

⁴ Emirates Identity Authority is an independent federal government organisation established in 2004 to manage the implementation of the national identity register.



Total memory utilized is: 125k EEPROM

Figure 8: Identity applets in UAE card

The primary need stems from requirements related to develop secure (authentication) communication mechanism. The government seeks to support e-government and e-commerce initiatives through this card to act as an enabler of electronic transactions.

In addition to the core functions, the card is poised to be the singular identity system in the country by providing integration support for inter-agency identity requirements. The card has multiple data containers that would enable and facilitate e-government. Labour and Employment data, Road Authorities, Law Enforcement agencies, e-Gate/ e-Passport, e-Purse are some of the important data containers available in the card.

Different government departments can enable their specific identity metadata for the card holder in these containers. Table 7 provides an overview of the capabilities and functions of the UAE identity card.

4.3 UAE e-Government Initiative

A recent report by the business school INSEAD and the World Economic Forum showed that the UAE ranked first in the Middle East and North Africa (Mena), and 24th worldwide, in terms of information and communication technology (ICT) readiness (Dutta and Mia, 2011). The UAE government realised the need to adopt more effective approaches to promote in principle, the authentication of online identities, and to address the overall requirements of trust, identity management and privacy and in the context of electronic governance.

The UAE ID card, coupled with the Public Key Infrastructure technology, provides strong authentication capabilities to support online services. PKI technology provides key building

blocks of digital identities, i.e., generation, management and validation of digital certificates, digital signatures, and electronic time-stamping.

The UAE government recently introduced its federated identity management solution (also referred to as the National Validation Gateway) which is based on its new smart identity card and advanced PKI capabilities. The solution provides identity authentication services to service providers (e.g., e-government, banks, hospitals, commercial entities). It is implemented as a service over the cloud to provide different services as depicted in Table 8.

The solution is currently available to e-government authorities. There are eight e-government authorities in the country; one federal e-government authority and seven local authorities, one in each emirate. Currently there are 48 government services⁵ that are integrated with this infrastructure.

The user basically needs to download an applet on his computer machine. Using the card reader, he needs to use his card to logon to the e-government portal. The method of authentication may vary depending on the service provider's requirements. The portal may perform the authentication function in offline mode, or it may redirect the user to the national validation gateway. The feedback from the latter will determine the go or no-go authorisation (access control decision) to desired resources.

The UAE federal government is working on drafting a legal framework to legalise digital identities and digital signatures. The government is planning to make all G2C e-government electronic transactions take place only through its new smart ID card in the coming 3 to 5 years. The government is planning to drive digital economy growth throughout the country using its new biometrics-based identity infrastructure.

4.4 Role of Biometrics in ID Card in G2G, G2B, G2C

As the levels of worldwide information system security breaches and transaction fraud increase, the UAE government is moving aggressively towards e-government transformation, particularly to develop combined, seamless services, which are electronically delivered to its population or other public or private sector entities (Westland and Al-Khoury, 2010). This comes in line with its objective to improve the efficiency, quality and transparency of government services.

The government plans include the development of multiple self-service channels e.g., over regular internet, kiosks, IVR and wireless channels. Biometric authentication of personal identities is seen more convenient and considerably more accurate than current methods such as the utilization of passwords or PINs.

As mentioned earlier, the UAE card is enabled with a Match-on-Card application. This allows service providers like government agencies to verify the identity of the cardholder and deliver services with complete confidence on the identity of the person receiving the services. With so many secure and transactional features enabled in the card, the UAE national identity card is set to become the country's most valued card both in physical and electronic transactions.

⁵ <http://www.abudhabi.ae> One can register to access the portal and its services using the Emirates ID Card

Biometrics in general is envisaged by the UAE government to provide high levels of identity assurance for homeland security including applications for improving airport security, and strengthening the national borders, and in preventing identity theft. There is seen to be a growing awareness and interest in biometrics in the country and in the region overall, of its potential in more accurately identifying and verifying the identity of individuals and protecting national assets.

The government has recently released an enhanced version of the Software Development Tool Kit (SDK) to enable licensed organisations to integrate the new smart identity card and biometric applications into their systems and develop legally compliant electronic signature and biometric authentication systems.

The SDK tool kit provides a high level API (Application Programming Interface) which help application software development easily and quickly made and UI (User Interface) of wizard type so that it saves time and efforts to develop an application. It is operated on various platforms, supporting diverse operating systems and development languages (Al-Khoury, 2011).

With such efforts, the use and reach of biometrics in the UAE is expected to increase considerably in the few years to come. As more identification and verification systems will be implemented to address various industries requirements who will likely find it in their best interest both in terms of cost and necessity to safeguard their data and assets.

The government is planning to push its biometric-based ID card solutions in multiple domains of applications. It has launched recently several initiatives in cooperation with private sector organisations to encourage the development of an extensive array of highly secure identification and personal verification solutions by integrating its new identity card functions in public sector applications, e.g., (1) network access to control unauthorized access to computers and networks in government organizations, (2) financial industry to promote e-commerce and online transactions, and (3) healthcare industry to provide security at hospital premises and recognition of patients identities, (4) law enforcement and (5) immigration and airports.

4.5 Interoperability Framework

To further enhance transactions using the new smart identity card, the UAE government is actively working with different stakeholders in the country and in the region to define interoperability standards. A framework has been defined that determines the role of the new smart identity card and the biometric verification that would be needed for authenticating a stakeholder in any transaction.

Standards are being defined for data interchange and exchange that will allow government departments and different agencies to communicate securely. The ID card with its PKI features is central to such a communication. Federated Identity Management is being provided and is currently in its pilot stage, integrating access of different web services using the identity management system set up by the government.

Taking the interoperability to a new level, initiatives are being taken to setup a Gulf

Interoperability Framework that will enable the UAE smart identity cards and other national ID cards in the GCC⁸ countries to be used across the borders. There have been serious moves in the recent years to ensure that identity cards across GCC countries are technically compatible and interoperable. There are some recent developments of APIs relating to biometrics, digital qualified signatures and digital authentication, to enable e-business transaction across borders (Al-Khoury and Bechlaghem, 2011).

5. Conclusion

Biometric technologies that have long history of use in law enforcement applications are now transitioning with wider social acceptance towards both public sector and commercial applications. Utilized with other advanced technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives.

Only by learning more about these technologies and exploring its potentials, and drawing on the experiences of successful and failed programs, governments can develop robust and vibrant biometrics community. Such efforts are needed to build identification and authentication systems that people can live with, trust and use, which should also enable the forming of the new digital economy.

Successful pursuit of biometrics challenges will generate significant advances in capabilities designed to improve safety and security in future mission within national and homeland security, law enforcement, and personal information and business transactions. Interoperability will still be a major hurdle.

From one angle, interoperability across geographical borders and business sectors, across processes, devices and systems is beneficial to biometrics diffusion. However, and looking at it from another angle, national interests in maintaining control and vendor resistance (aspiring to future market dominance due to lock-in effects) are expected to challenge interoperability efforts, despite the significant standardisation work being done at national and international levels.

Although technical interoperability is receiving increasing attention to some extent, the interoperability of processes may be more challenging. These challenges will come to surface as attempts of innovate service delivery models start taking place to push biometrics applications away from the existing narrowed objectives and promote wider diffusion in our societies. As such, when systems become more interoperable, the need for building more robust identity management grows as well as to meet national and international needs.

Government and industries are likely to become more dependent than ever on more robust identity management tools and identity governance principles. Biometrics will play a key role in addressing the new challenges of the years to come.

⁸ GCC is the acronym for Gulf Cooperation Council, also referred to as the Cooperation Council for the Arab States of the Gulf (CCASG). It includes six countries namely, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. The number of GCC population is estimated to be around 40 million people (GCC Portal, 2011). GCC citizens can usually travel freely between member states without the need for visas, and can use either their passports or national identity cards for border crossings.

Bibliography

- Al-Khouri & Bal, J. (2007), "Electronic Government in GCC countries." in International Journal Of Social Sciences, 1(2), pp.83-98.
- Al-Khouri, A.M. (2011), "PKI in Governemt Identity management Systems." in International Journal of Network Security & Its Applications, 3(3), pp. 69-96.
- Al-Khouri, A.M. and Bechlaghem, M. (2011), "Towards federated e-Identity Management across GCC: A solution's Framework." in Global Journal of Strategies and Governance 4(1). pp. 1-20.
- Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002), "Biometric perils and patches." Pattern Recognition 35(12), pp. 2727-2738.
- Brüderlin, R. (2001)."What is Biometrics?" [Online]. Available from: <http://www.teleconseil.ch/english/introduction.html>. Accessed: August 12, 2011.
- Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005), "PalmHashing: a novel approach for cancelable biometrics." in Information Processing Letters, 93(1), pp. 1-5.
- De Meyer, A. and Loh, C. (2004), "Impact of ICT on government innovation policy: an international comparison", in International Journal of Internet and Enterprise Management 2(1).
- "Dermatoglyphics," Hand Analysis, International Institute of Hand Analysis, 24 January 2005.
- Dutta, S. and Mia, I. (ed.) (2011), "The Global Information Technology Report 2010-2011". [Online] Available from: http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf Accessed: August 15, 2011.
- GCC Portal: <http://www.gcc-sg.org/eng/index.html>. Accessed: August 12 2011.
- Guthrie, I. (2003), "Electronic Government in the Digital Society." Lomonosov Moscow State University, Russia. [Online] available from: egov._digital._society. Accessed: August 12, 2011.
- IMA (2011), "Building the Digital Society," The insitute of mathamtics and its application, UK. [Online]. Available from: building_the_digital_society_20101213122904. Accessed: August 12, 2011.
- Jueneman, R.R. and Robertson Jr., R.J. (1998), "Biometrics and Digital Signatures in Electronic Commerce", in 38 Jurimetrics J. [Online] Available from: <http://nma.com/mcg-mirror/mirrors/digsig.pdf>. Accessed: August 1, 2011.
- Ke, W. and Wang, X. (2008), "How do governments matter to the creation of digital economy?" in Fensel, Dieter and Werthner, Hannes (editors) Proceedings of the 10th international conference on Electronic commerce (ICEC), Innsbruck, Austria, August 19-22, 2008.
- McMahon, Z. (2005), "Biometrics: History," Indiana University, Indiana University Computer Science Department [Online]. Available from: <http://www.cs.indiana.edu/~zmc mahon/biometrics-history.htm>. Accessed: August 12 2011.
- Renaghan, J. (2005), "Etched in Stone," Zoogoer, August 1997, (Smithsonian National Zoological Park, 26 January 2005).
- Richardson, A. (2009), "Why Identification Cards are Important in Today's Economy", Articles Factory [Online]. Available from: <http://www.articlesfactory.com/articles/business/why-identification-cards-are-important-in-todays-economy.html>. Accessed August 21, 2011.
- RNCOS (2011), "Global Biometric Forecast to 2012" [Online]. Available from: http://pdf.marketpublishers.com/463/global_biometric_forecast_to_2012.pdf. Accessed August 30, 2011.
- Ross, A. & Jain, A. (2003), "Information fusion in biometrics." in Pattern Recognition Letter 24(13), pp. 2115-2125.
- Rukhin, A. L. & Malioutov, I. (2005). Fusion of biometric algorithms in the recognition problem. Pattern Recognition Letters, 26(5), 679-684.

Sarkar, I., Alisherov, F., Kim, T., and Bhattacharyya, D. (2010), "Palm Vein Authentication System: A Review". International Journal of Control and Automation, Vol. 3, No. 1, pp. 27-34.

Shoniregun, C.A., and Crosier, S. (2008), Securing Biometrics Applications. Springer-Verlag.

Tilton, C. (2006), "Biometric Standards – An Overview." Daon. [Online]. Available from: http://www.securitydocumentworld.com/client_files/biometric_standards_white_paper_jan_06.pdf. Accessed: August 12, 2011.

Uhlfelder, D. (2000), "Electronic Signatures and The New Economy" [Online]. Available from: <http://ubiquity.acm.org/article.cfm?id=354571>. Accessed: August 1, 2011.

Vamosi, R., Monahan, M., Kim, R., Miceli, D., Van Dyke, A. and Kenderski, J. (2011) 2011 Identity Fraud Survey Report. Javelin Strategy and Research.

Westland, D. and Al-Khoury, A.M. (2010), "Supporting gobierno electrónico progress in the United Arab Emirates," in Journal of Gobierno electrónicoStudies and Best Practices, pp.1-9.

Woodward, J.D. (1997), "Biometrics: Privacy's foe or privacy's friend?", in Proceedings of the IEEE (Special Issue on Automated Biometrics), 85, pp. 1480-1492.

The RIC Project as a new paradigm in Brazilian civil identification

Marcos Elías Claudio Araujo



Marcos Elias Cláudio Araújo

Director of the National Identification Institute – INI Department of the Brazilian Federal Police



Mr. Marcos Elías Cláudio de Araújo was born in Brasilia in 1963. He graduated in Economics in the Catholic University of Brasilia and in Systems Analysis in the University of Brasilia. He is a co-writer of the “The index finger as a reference for civil and criminal identification: An alternative to the thumb finger” paper. At present he is the Director of the National Identification Institute - INI

Abstract

Based on the latest technology, the new system of civil identification adopted by Brazil involves a smart card containing the most up-to-date security features, making it a modern, practical and secure identity document that puts Brazil at the forefront globally in respect of civil identification.

Key words: civil identification, security

The RIC Project as a new paradigm in Brazilian civil identification

According to a report on global best practices by Portugal's Knowledge Society Agency (1), issued just after the turn of the century, various countries had launched studies into the improvement and modernisation of services provided to the public.

The majority of these projects were focused on using technology to modernise public services. Many of them are now in their second phase, involving the creation of “smart” services focused on the citizen.

The implementation of a new form of identification was the starting-point for the modernisation of interacting with those using public services, and in this context several countries have been improving their systems of civil identification.

Along with this international trend for modernising documentation, Brazil supported the United Nations Convention against Transnational Organized Crime, known as the Palermo Convention. It was passed into law by Decree No. 5015 on 12 March 2004. Additional protocols relating to the prevention of the smuggling of migrants by land, sea and air (passed into law by Decree No. 5016 dated 12 March 2004) and the prevention, suppression and punishment of people trafficking (especially of women and children) (passed into law by Decree No. 5017 dated 12 March 2004) anticipate the creation of mechanisms for the security, control and validation of identity cards.

Article 12: Security and control of documents

Each State Party shall take such measures as may be necessary, within available means:

- a) To ensure that travel or identity documents issued by it are of such quality that they cannot easily be misused and cannot readily be falsified or unlawfully altered, replicated or issued; and
- b) To ensure the integrity and security of travel or identity documents issued by or on behalf of the State Party and to prevent their unlawful creation, issuance and use.

Article 13 – Legitimacy and validity of documents

At the request of another State Party, a State Party shall, in accordance with its domestic law, verify within a reasonable time the legitimacy and validity of travel or identity documents issued or purported to have been issued in its name and suspected of being used for trafficking in persons.

The purpose of civil identification is the identification of the population in a way that guarantees their individuality in the range of acts involved in living within a society.

Currently, civil identification of Brazilians is done by identity card (Carteira de Identidade), issued by the identification bureau of one of the federal states or the Federal District, conform to Law No. 7.116 dated 29 August 1983, with regulations in terms of Decree No. 89.250 dated 27 December 1983. This law was responsible for the standardisation of a national model of civil identity. Since then, there has been no investment in or projects related to civil identification in most of the federal states of Brazil, and in particular nothing related to advances in technology and the needs of contemporary society. As a result, the identity card became an obsolete document.

The current system of personal identification legally permits a citizen to obtain up to 27 identity cards, each with a different number, in different states. Add to that the fact that several identification bureaus have problems searching their fingerprint records before issuing an identity card, meaning that a person is able to cheat the system and obtain a number of identity numbers with different personal details in the same state or federal unit.

Another factor contributing to the weakness of this system is the complete absence of integration, at both state and national level, which prevents the investigation of details among the bodies responsible for identification. The State and society are harmed by this fragmentation and institutional dislocation, which compromises the degree of trust placed in the documents issued.

The ongoing project is based on the particular requirement to guarantee the fundamental rights of the citizen. Article 5 of the Constitution states that: "*All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property*". Subsection X provides that: "*the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured*".

Despite this, these constitutional guarantees are disregarded daily, and the private life, honour and image of citizens are violated when their names are used improperly to set up phantom companies, to take out loans and for other purposes based on their social relationships, creating debts and requiring them to prove their own identity. Many people answer for crimes they didn't commit as a result of the deficiencies of the current identity card, while others are buried like paupers because of the lack of integration between civil identification records.

In terms of Law No. 9.454 dated 7 April 1997, a unique RIC (Civil Identity Register) number, contained within the identity card, will be generated and supplied by the central agency once the uniqueness of the citizen's identity, based on fingerprint records, has been confirmed. In terms of Decree No. 7.166 dated 5 May 2010, the new document will give an individual a record in CANRIC - the National Register of Civil Identification - which will be created using the RIC register to catalogue the details needed for the unequivocal identification of citizens.

In terms of Decree No. 7.166/2010, the system's central agency will be responsible for the coordination, archiving and control of CANRIC. The appropriate federal entities, in conjunction

with the central agency, will be responsible for implementing and updating CANRIC, controlling the allocation of RIC numbers, transmitting the identification details gathered in order to allocate the RIC number to the central agency, and issuing the identity card containing the RIC number.

Under the coordination of the Ministry of Justice, the Civil Identification Registry was created with the aim of becoming an important tool for the guaranteeing of social rights and the protection of property. Its introduction will make rapid and secure identification of any Brazilian citizen possible, which will help to prevent fraud and resolve civil disputes. The new identity card is also designed to modernise the country's Civil Identification System, guarantee the uniqueness of each citizen in a national database, strengthen relations between society and government and non-governmental organisations, contribute to the promotion of social and digital inclusion, and widen preventive public security measures.

The proposed project envisages the issue of 150 million RIC numbers (generated after certification of the biometric uniqueness of fingerprints in a nationwide automated, centralised and integrated system) inserted in new identity cards using modern features of identification technology such as microprocessor chips and digital signatures. Funding of the new process of civil identification will be possible through public financing, an issuing fee, the aid of state identification bodies, and the use of digital certification services. Public/private cooperation agreements may also be signed.

With the new system of civil identification, the registers will cease to be regionalised, as is currently the case with the Register General (RG), and will form a centralised databank containing fingerprint details of every citizen. This system will be administered by the Ministry of Justice, through the National Identification Institute of the Federal Police, and will contain additional information such as a photograph, a digital signature, the numbers of other documents and personal details such as height and eye colour.

The implementation of the new identity card is a nationwide project which will affect every Brazilian citizen.

Following implementation of the Civil Identity Register, the project will become an ongoing process. The participating agencies of the National System of Civil Identification Registration (SINRIC) will have uniform physical and technological structures, and appropriate human resources, throughout the country, guaranteeing the same quality of service to the public irrespective of location.

The adoption of the Civil Identity Register will deliver innumerable benefits to society by guaranteeing uniqueness between the citizen and his document, using automated fingerprint identification. This measure will strengthen those public and private services that require identification of the citizen, contributing effectively to the reduction of fraud against individuals, companies and government bodies.

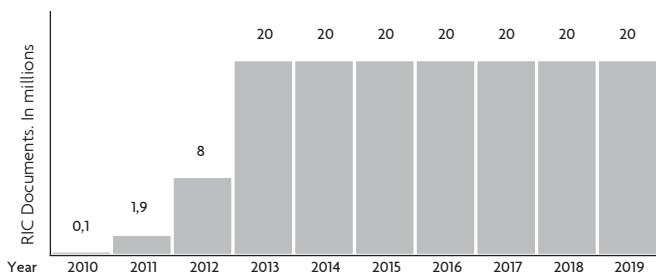
In addition to the introduction of the Civil Identity Register, the RIC Project proposes the adoption of a new identity document with hi-tech specifications, putting Brazil in the vanguard

photo, signature and fingerprint image) are etched by laser, perforating the layers of polycarbonate. The creation of words and images without the use of ink prevents the removal or adulteration of these details;

- **MRZ field with OCR code to ICAO standard:** a mix of numbers and letters that can be read by equipment used in airports, for example. This uses the international standard for travel documents.

As a result of the introduction of the RIC a major agreement is being signed with the state identification bodies who will need the investment necessary to promote technological synergy among the participating institutions of SINRIC, in the form of the secure integration of databases, which will enable the implementation of the project throughout the whole of Brazil, involving the registration of approximately 150 million Brazilians, over a period of nine years (diagram 2).

Projections for RIC Documents and the accumulated value 2010 - 2019



A number of institutions were invited to participate in the development of this project and will soon present integrated proposals for application models relevant to their respective areas of action, strengthening inter-institutional cooperation and integration around the objective of reformulating the concept of civil identification in the country.

The RIC project will help in various areas, such as the welfare system for example, which stores the personal details of approximately 36.5 million taxpayers and 25 million claimants throughout the country who are processed and receive payments every month. The National Social Information Register (CNIS) contains information which guarantees labour and social security benefits. The RIC will allow the public to be dealt with more quickly and in a more convenient, secure and transparent fashion.

Electoral authorities in Brazil currently have a database of approximately 130 million people. The Brazilian electoral process, which is noted internationally, is seeking to increase its reliability by adding biometric authentication to electronic polling stations. With the aim of guaranteeing full exercise of the citizenship rights of each Brazilian voter by preventing people voting more than once in the same election, the Superior Electoral Court launched pilot projects in 2008 for the biometric registration of electors with the collaboration of the National Identification Institute of the Federal Police.

Information supplied by the Brazilian Banking Federation (FEBRABAN) indicates that banks and financial institutions invest approximately 1.2 billion reals annually to guarantee the security of banking transactions, the protection of electronically recorded information, and the availability of banking services to people on low incomes.

The widening of income distribution through the Federal Government's social programmes has contributed to this growth of banking. Progress in this area is inevitable, bearing in mind that various routine transactions can be carried out by citizens in any bank or similar financial institution in the country. The RIC project is becoming a fundamentally important mechanism for this policy of social inclusion and security in relation to the opening of accounts, the granting of credit and the reduction of fraud and losses.

In 2008 the banking sector invested 6.4 billion reals in information technology, and the number of internet banking accounts has grown almost 300% in the last decade, reaching a figure of 23.5 million accounts in 2008.

The number of banking institutions grew by 3.1%, from 18,600 to 19,100, between 2007 and 2008. Total bank spending and investment in information technology increased from 14.9 billion reals in 2007 to 16.2 billion in 2008. These figures, released by FEBRABAN, reveal the scale of the challenge facing the banks.

The fact is that the process of increased access to banking services means that the rate of online transactions will grow much faster than the rate of issue of digital certifications. Industry experts estimate that if everyone had digital certification, the number of internet frauds would fall by up to 80%.

In Brazil, the National Information Technology Institute has been the main driver of the implementation of digital certification, offering citizens increasing numbers of applications and services in the virtual world. The best examples of these are the use of electronic invoicing of imports, the introduction of virtual judicial processes and the Federal Treasury's e-register of individuals.

The combination of this and the RIC project will allow digital certification to become more widespread, and the new identity document will also be an instrument for supporting civic rights and digital inclusion in Brazil. In other words, every Brazilian citizen will have access to the technological means necessary to be recognised in communication networks and the internet, and will be able to use electronic government services.

Digital certification has become the safe way of solving one of the internet's oldest dilemmas: checking the identity of someone buying goods online with a credit card or via a bank account. Certainty of identity is not guaranteed in current transactions. The combination of biometric fingerprinting and digital certification will result in a more secure process of personal identification that will guarantee the improvement of online banking services, the security of communication networks and the reduction of fraud and internet crime.

The commercial sector will also benefit. Commercial establishments will be able to verify

customers' identities using the new identity card and biometric card readers, thereby reducing the risk of loss due to criminal acts.

Along with the use of the latest technology, the RIC will allow Brazilian citizens to be registered following a fingerprint check in a unique nationwide database, ensuring that each individual gets a unique number in the Civil Identity Register by which every Brazilian citizen, whether born or naturalised, will be identified in their interactions with society and with governmental and private organisations, thereby strengthening all of the services that require a citizen's identification. The tool adopted by Brazil for investigating fingerprints, and which will be used for large-scale investigation in the RIC project, is AFIS, the Automated Fingerprint Identification System, which is capable of rapid and accurate extraction of individual morphological characteristics, called minutiae, which allow fingerprint impressions to be distinguished from each other, giving each citizen an unmistakable separate identity. This is therefore the principal tool in the implementation of the Civil Identity Register.

The Federal Police Department already has an operational AFIS installed in the National Identification Institute and its twenty seven regional offices. The Institute's AFIS has an interface, entitled Inter-AFIS, which permits the exchange of information with other automated fingerprint identification systems that have adopted INTERPOL's ANSI/NIST-ITLI-2000 standard.

Another aspect of the Federal Police is its modern technological structure, which is capable of implementing a system of communication and interoperability between the organisations involved.

The Civil Identity Register was officially launched on 30 December 2010 by then President of the Republic Luiz Inácio Lula da Silva, and the State Minister of Justice, Luiz Paulo Teles Ferreira Barreto, with investment of almost 90 million reals provided by the Ministry of Justice, and with the particular purpose of guaranteeing the fundamental rights of citizens.

During the launch ceremony, the Justice Minister, Luiz Paulo Teles Ferreira Barreto, pointed out that the RIC card is one of the most modern identity cards in the world: "The RIC card is more secure and more practical, since it incorporates various security features in a single document". Its adoption will deliver innumerable benefits for society by guaranteeing the uniqueness of each citizen and their document using automated fingerprint identification. This measure will strengthen public and private services that require the identification of the citizen, making an effective contribution to the reduction of fraud against individuals, companies and government bodies.

Every transition is a big challenge, and starting the RIC project demanded strong articulation and a concentrated effort. In parallel with this, it was necessary to establish solid guidelines for its development and credibility.

It should be recognised that in this process the choice of organisational and technological standards was decisive in dictating the direction of the market and indeed the very evolution of governmental applications of the technology. The implementation of a policy of modernisation in the civil identification system, involving the adoption of modern methods, technology,

infrastructure and management models, will facilitate the introduction of a smart and secure identity card into the daily lives of the country's citizens, leading to more trust in their relations with the State and the private sector and protecting their privacy and the integrity of the institutions.

In this sense, the RIC project is seen as the result of the technical and managerial maturity acquired in the years leading up to its inclusion in the government's public policy. The project's objective and management systems were conceived against the background of a global trend and the requirements of a Brazilian government seeking to safeguard democracy and the rule of law, security and social equilibrium.

Brazil, a country of continental proportions which encompasses very diverse economic and cultural realities, has made itself more relevant on the world stage, not just through its economic potential but also by the adoption of responsible public policies that offer social inclusion to millions of citizens living below the poverty line. This creates huge opportunities and challenges that require the adoption of coordinated action to prepare the country for a changing world. The RIC project slots perfectly into this strategy by strengthening Brazil's image in the international arena, and will bring about a paradigm shift in relations between the Brazilian state and its citizens.

Bibliography

1. Palermo Convention, adopted in New York on 15 November 2000
2. Decree No. 5.015, dated 12 March 2004
3. Decree No. 5.016, dated 12 March 2004
4. Decree No. 5.017, dated 12 March 2004
5. Decree No. 7.166, dated 5 May 2010
6. Decree N. 89.250, dated 27 December 1983
7. Law No. 7.116, dated 29 August 1983
8. Law No. 9.454, dated 7 April 1997
9. Report on Global Best Practices by the Knowledge Society Agency of Portugal
10. End of phase 1 of Civil Identification project

Comprehensive project for technological upgrade in the General Register Office of Honduras

Jorge Arturo Reina García



Jorge Arturo Reina García

Director of the National Registry of People (RNP) and President of the RNP's Board of Directors.



Born in 1960, he is a civil engineer and holds a master's degree in Project Management. He has worked as manager of companies producers of concrete and its by-products, he was President of "Ingeniería Gerencial", pioneer and leader company of Honduras and Central America in Project Management and Geographical Information Systems (GIS). Trained as user of GIS, he was Organizational Secretary of the Central Executive Board of the liberal Party (that in 2009 was the government party). Actually he is the Director of the National Registry of People, where he is developing a process of re-engineering and institutional strengthening.

Contact: 6to piso, Edf. Villatoro, Blvd Morazán,

Tegucigalpa MDC, Honduras;

Tel.: (504)22214425, (504)22215520

email: direcciónejecutiva@rnp.hn

jorgearreina@hotmail.com

website: www.rnp.hn

Abstract

The General Register Office is an autonomous and independent special organization with national authority, with functions and processes for which it was declared a National Security Institution. It is responsible for planning, organizing, leading and managing the integrated system of civil registration and identification of natural individuals with the highest quality to attain a safe, comprehensive, efficient and effective management of information and documents. Its MISION is: to ensure the veracity of registration for the perpetuity of facts and acts relative to natural individuals' civil status, the universal right to identity focused on human rights, developing and strengthening the democratic system of Honduras, committed to render services of excellence to attain citizen trust.

The Comprehensive Project for Technological Update of the Honduran General Register Office consists of the solution of structural problems related to the Institution in line with its Nature and Human Rights Goal (Social Inclusion), Public Security, as well as basic support as relevant institution of the National Information sector for the recently launched government Programs: E-Government and E-Signature.

The Comprehensive Project is broken down as follows:

- Modernization Process
- Processes Reengineering and Institutional Strengthening
 - Adoption of a Strategic Plan, Policies, Standards and Procedures,
 - Reorganization of the Administrative Structure;
 - Training
- Identity Card Renewal Project
- Update and Homologation of Databases of Civil Register and Identification;
- Improvement of the Capacity Installed at the Municipal Civil Registers;
- Upgrade of Central Hardware;
- Update and capacity increase of the Civil Register Systems and AFIS software;
- Print line change
- Interaction with other Public and Private Institutions
- External Browsing
- E-Government

Key Words: Afis, databases, general register office of honduras, municipal civil register, reengineering, technological update, identity card

Comprehensive project for technological upgrade in the General Register Office of Honduras

Background

In Honduras the Civil Register was created ascribed to the catholic parishes of the country in the 1890's, which activity was afterwards transferred to the Office of the Municipal Mayor, where it kept on as a decentralized body until 1982 when by a Decree of the National Congress the General Register Office was created and which took over all functions, depending from the National Electoral Court, with the responsibilities of the Civil Register, National Individuals' Identification and elaboration of the National Electoral Census. Some years later, in 2004 through a decree of the National Congress the General Register Office (RNP) was created as an autonomous and independent special organization with national authority, with functions and procedures of civil status registration and of management and issuance of registration documents for which it was declared a National Security Institution as it was closely related to social security, and with the goals of planning, organizing, conducting and managing the integrated system of civil registration and identification of natural individuals with the highest security. To this effect it developed methods, techniques, modern procedures, technological, scientific and specialized controls, for a secure, comprehensive, efficient and effective management of registry information and documents. Therefore, the main activity of the General Register Office is the efficient and permanent management of the Civil Register System, the registration of all citizens' acts and facts from which the National Identification System is derived, what generates the Identity Card and is the basis for the Supreme Electoral Court to elaborate the National Electoral Census as a registry of citizen(s) legally capable to vote in internal, primary and general elections of the country.

In 1984 an inventory of registrations at national level was performed and the unique numerical code of thirteen (13) digits for every individual was established; page numbers were assigned to the pages of the registration books to prevent modifications and to facilitate the capture of Department codes, Municipality, year of registration and correlative number of registration within each municipality; it is restarted every year. The structure of such Code is the following.

- o The first four (4) digits designate the department code and the registration municipality;
- o The following four (4) digits designate the year of registration and,
- o The remaining five (5) digits correspond to the number of the registration act in every municipality, assigned in a chronological order of presentation and it is restarted every year.

The Department code has two digits (01 through 18 and 20 for the Hondurans born in USA); the number variance is established by the alphabetic order of the Department name. If a new department is created, or existing ones are merged, the code assigned will be the one following the last one.

The Municipality code was established with similar criteria: the department head municipality

was assigned the code 01, and the others a correlative numerical code in alphabetic order within each Department. The new municipalities received a code number following the last one, and the same rule will apply for merging municipalities.

There are special codes for Naturalized Hondurans, who were assigned the Department and Municipal code 0890. Code 0880 was created for the case of individuals who apply for a double nationality and code 1292 for the individuals who live in zones recuperated through the resolution of the Supreme Court of La Haye, Holland. The Hondurans reregistered with no court decision and based on the certification they obtained from birth registration issued by the Civil Register, but that were not recorded in the registries of the General Registry Office were assigned a Department code adding 20 digits more to the code of the registration department.

Through the National Registry Office Honduras has permanently worked on fixing the inconsistencies, for data integrity, and to update the Civil Registry for which various projects to adjust information were carried out:

1. In 1983 the Project financed by AID and the Government of Honduras to move the Civil Registry of the Offices of the Municipal Mayor to the General Register Office and to create the first Identity Card with fingerprint records,
2. 1987 Project to Update the Civil Registry, financed by AID,
3. 1991 DEPUR Project, financed by the TNE / GRO.
4. 1996 OEA Project to Strengthen the Civil Registry,
5. 2005 OEA Project to Strengthen Democratic Institutions, and
6. 2011 PNUD project to reduce the Under-Registration, and digitize pending registration information.

Remark: The update Projects have not been completed and have generated information and incomplete Databases that have to be homologated.

As regards individuals' National Identification three (3) projects were completed:

1. In 1984 the first Identity Card with biometric control was created,
2. In 1996 the first Identity Card in the world with combined Biometric control and AFIS was created, and
3. In 2005 a Project to update and modernize the Identification Document (10-fingerpirnt) and the General Register Office.

The 1996 project started the identification of citizens using a fingerprint biometric system with two databases: the first one contains the registrations of the Civil Register (births, deaths, marriages, adoptions, etc.) with a total of approximately 12 million records and a second one with information of the issuance of approximately 3,700,000 unique Identity Cards for the same amount of Honduran citizens, with their demographic data and images (photo and index fingers prints). Since that time over 5 million issues were incorporated for the same amount of citizens of whom there are demographic data and images (photo and fingerprints of 3,234,927 records with fingerprints of the two index fingers) and minutiae vectors. The 2005 project implemented a 10-fingerprint biometric system through which there are demographic data and available

images (photo and fingerprints of 1,802,730 individuals with the 10 fingerprints of the hand), minutiae vectors and is kept in databases of registrations in the Civil Registry (births, deaths, marriages, adoptions etc.) consisting of approximately 16,000,000 records.

Current Identity Card includes information in the bidimensional bar codes (general data on the citizen, department and municipality of application, name of parents).

Operation of the general register office (gro) systems

The GRO serves 8,215,000 people and operates with 333 offices and 1430 employees at national level. It has 76 computerized Municipal Civil Registries (MCR), of which 22 are online covering 70% of the country population, and 222 MCR that operate manually. There are also 20 Departmental Civil Offices, 15 Auxiliary Civil Registries and some activities in the Honduran Consulates worldwide. The centralized operation is developed in 3 buildings and 1 warehouse in Tegucigalpa capital.

The Civil Registry system is centrally managed though it captures information in a decentralized manner, based on a unique registration number of birth or naturalization that afterwards turns to be the identity card number, supplemented by a biometric identification method of every citizen. The system relates the registration of births or naturalizations with the data of the other registrations referred to individuals' civil status and the issue of their identification documents.

The Identity Cards are issued using the information of the application, birth registration, current domicile, citizen photo, ten-fingerprints (that can be replaced at the applicant's request) and are sent to the municipality of application.

The Civil Registry operates in 312 premises, with at least one per Municipality.

The MCR has 23 cities connected online to the Central Headquarters, with digital image capture, (photo, fingerprints and signature) of the identity card applicants. There are also 53 cities with data capture devices for procedures in the Civil Registry and with capability for digital image (photo, fingerprints and signature) of the identity card applicants, but these store the information that is afterwards sent in CD format to the Central Headquarter for processing.

Moreover, the GRO has 75 mobile units for digital data and image capture (photo, fingerprints and signature) which are moved to the required sites, not requiring any special facility as they have their own infrastructure and are enabled to process requests for citizen identification; data are stored and sent to the Central Headquarter in CD format or by the Internet.

In the rest of the offices the registration of natural individuals is processed in the corresponding books, and fingerprints are captured manually. This information is forwarded to the Central Headquarters by traditional mechanisms to be digitized and processed. Registration Books are forwarded when they are full. Registrations are related to birth registries through the communication of margin annotations that are sent to the municipalities with a copy to the central archive.

The system is complemented with the replacements for omission and rectifications or additions

to the original registrations by special resolutions, issued by the Regional Civil Registers or the Office of the Municipal Mayor, which instruct the registration in the respective register. At present there is no computerized communication between the Registers and the Office of the Municipal Mayor.

Informatics applications implemented

The GRO serves citizens nationwide through the following informatics applications:

- o CIVIL REGISTER

1. Capture and Certification of registrations online in the computerized MCR's and digital books.
2. Capture of Registrations from the non-computerized Registers (handwritten books).
3. Procedure for cross-checking information coming from the birth, marriage, death, etc., registrations, automatically generating the margin annotation of the birth registration into the database.
4. Homologation of databases in the Civil Registers.5. Generation of vital statistics
6. Building of every individual's family tree
7. Generation of a file or life page for every individual
8. Issuance of registration certificates contained in the database
9. Mechanisms to browse the Civil Register database
10. Audit procedures to follow-up changes, input and modifications to registrations
11. Production control
12. Multimedia (digitizing of the images contained in the registration books)

- o NATIONAL IDENTIFICATION PROGRAM

1. Digital capture of citizen data, fingerprints, photos and signature and forwarding by the Internet.
2. Transcription of the of non-computerized Civil Registers
3. Digitizing of fingerprints and photo captured by non-computerized Civil Registers
4. Integration of biographical and demographic data, and images to be sent to AFIS, by the Internet.
5. Comparison of fingerprints of those who request the issuance of the first Identity Card against those in the (AFIS) Advanced Finger Identification System database .
6. Printing of the identity cards of new citizens and requests for replacement or renewal.
7. Control of current users
8. Control of applications for the issue of identity cards
9. Control of identity cards issuance and rejection
10. Control of requests for identity cards replacement
11. Back-up of the database of identification cards issued for the first time

o EXTERNAL BROWSE INTO THE NATIONAL IDENTIFICATION SYSTEM AND CIVIL REGISTRY

1. Identification has 3 search components

o Authentication

o Identification

o Browse

2. The Civil Register has 4 Modules:

o Browse by identity number

o Browse by name

o Browse of the Family Tree

o Printing of birth registrations

The GENERAL REGISTER OFFICE renders the service of external browsing to Government agencies with which it has signed agreements:

1. Ministry of Foreign Affairs with its foreign consulates;

2. Ministry of Security

3. Ministry of Economy

4. The Public Prosecutor

5. The Office of Immigration Affairs

6. The Family Allowance Program PRAF

7. The Attorney General's Office

8. The National Commission of Banks and Insurances:

9. The Supreme Court of Justice, etc.

Current situation

The GRO is facing the need of renewing the current identity document what implies a massive registration process, the processing and printing of Identification Documents for over 5 millions citizens, added to the need of an update and the implicit modernization of its information Systems, the infrastructure and administrative structure to improve operative efficiency, to keep an ongoing improvement process and to lead the e-Government implementation process. This considering the relevant role it has to play, the eventual implementation of e-signature, combined with a distorting element of the political type due to the internal and primary elections in November 2012 and the General Elections in November 2013, that overlaps with the probable implementation process of renewing the National Identity Document as it has the function of Electoral Document to vote in both processes.

This brought about the need to start an Institutional Reengineering and Strengthening process that should involve the GRO structure, which has already been started with a diagnosis made in 2010 that showed the following situation:

1. Social Exclusion of the individuals that in Honduras integrate the Under-registration and Under-identification (it ranges between 6% and 8% of the population);
2. Lack or scarce equipment, logistic support, supervision and quality and training of human resources due to Budget Restrictions;
3. Problems with the Technical and Administrative Procedures derived from the non existence of official Policies, Standards and Procedures;

4. Problems of document fraud (Registration, Identity Theft, etc.)
5. The administrative structure is not the appropriate for geographical coverage, services, operative efficiency and an ongoing improvement process;
6. Weakness of the capacities to allow the modernization of information systems, in its Civil Register System, identification and administrative area;
7. Outdated information, dispersion and inconsistency of Databases both of the Civil Registry and Identification, as the automated MCR's still have equipment with a limited capacity and in an amount not enough for the demand;
8. Weakness of the automated process capacity for obsolescence, for not being up-to-date or lack of informatics and communications structure in their Civil Registers at national level,
9. Weakness of the communications infrastructure in all the Civil Registers at national level, what generates deficiencies in process security and in process quickness and;
10. The need to incorporate e-Government and e-Signature as a relevant Institution in the incipient medium-term implementation process as both are strongly supported on citizen identification, users certification and the interchange of information; all processes that should be executed on robust Communications platforms;
11. Renewal of the Identification Document (Identity Card), what implies renewal or replacement to update its informatics capacity in the Identification System, in document personalization, in registration and fingerprints process;
12. Outdated informatics resources in the Central Headquarter to improve and strengthen the Identification System security;
13. Weakness in External Browsing and interchange of information capacities to support the Management of government institutions in the Security area, Justice, Public Prosecution and service private companies as cellular phones, banks, etc.,
14. Weakness in employees capacities to produce a replacement generation;
15. Need of new Hires to render services to the Private Sector as a sustainability element of the Project and the GRO.

Comprehensive Solution Plan

The Plan for a Comprehensive Solution of the structural problems of the GRO derived from the diagnosis of mandatory activities that are not correctly performed, or are incomplete or are simply not done, is supported on the following Pillars:

- Fight against Document Fraud
- Creation of an Anti-Fraud Committee (Secretaries of Security, Interior, Immigration, Public Prosecution and GRO)
- Setting up of internal Controls and Coercion
- Modernization Process
- Process Reengineering and Institutional Strengthening
- Adoption of a Strategic Plan, Policies, Standards, Technical and Adminstrative Procedures (Regulations, Manuals, etc.);
- Reorganization of the administrative Structure (Organization Chart and Reclassification of job positions and wages)

- Identity Card Renewal Project
 - Update and Homologation of the Civil Register and Identification Databases;
 - Equipment and improvement in communications of the MCR's;
 - Renewal of the Central Hardware;
 - Upgrade and extension of the software used for the Civil Register and Biometric Identification Systems (facial features matrix);
 - Replacement of Print Line
- Minors Identification Project
- Interaction with other Public and Private Institutions
 - External Browsing
 - E-Government

Action being taken to accomplish the comprehensive plan

In spite of the strong budget restrictions, the GRO has been working on a new and wide Participation of the most trained and experienced personnel of the institution, with the Labor Union of the GRO and also working closely with the support and trust of International Organizations such as PNUD (United Nations Program for Development), the Spanish and Sweden Cooperation for development, UNICEF, the USA Embassy, the NGO Plan in Honduras, World Vision, etc.

It is relevant to highlight that in the execution of the "Institutional Strengthening of the GRO and the decrease in Under-Registration and Under-Identification in the Excluded Zones of Honduras" Project (PNUD, AGDI, AECID, RNP) we have the honor to be qualified as the Best Project in Honduras (PNUD), in relation to the innovation of images and records to solve the problem of the individuals who have not yet had the universal right to "a Name and a Nationality" due to economic, social or geographical exclusion, among which the following can be mentioned:

- Creation of the Registry Promoter
- Creation of the Under-registration Book
- Decrease or speeding up of the registration requirements for excluded individuals (including a preliminary draft law jointly with the Secretariat of the Presidency)
- Procurement of resources (Vehicles for Citizen Registration, Automated Mobile Equipment, etc.) for Registration and Identification Mobile Brigades
- Coordination with related Institutions (Social State Programs, PRAF, NGO's, Local Social Organizations, Offices of the Mayor, etc.)

Likewise, in the way to accomplish the GRO Comprehensive Plan, a vast series of actions were taken that are summarized below:

- Fight against Document Fraud
- Reactivation of the Antifraud Committee (Secretariats of Security, Interior, Immigration, Public Prosecution and GRO)
- The purge of personnel involved in corruption activities is being carried out with preliminary

results product of the "Document Confiscation", over 100 thousand proceedings and identification requests in offices in the whole country with rational hints of fraud. Such operation has resulted so far in corrective actions applied to human resources as follows: 20 dismissed, 65 suspensions, 225 warnings and starting of judicial procedures. Also, there is an antifraud culture already felt in the GRO.

- Institutional Reengineering and Strengthening

- Reengineering Process,

Starting at the GRO reviewing the Organization Structure and elaborating the controls, administrative and technical procedures through the following Products:

- Draft of Amendments to the GRO law

- Regulations (Law, Registration Career Regime)

- 19 Safety Manuals, Procedures (Administrative and Technical), Functions, Positions and Wages, etc.

- New Adminnistrative Structure (Organization Chart)

- Creation of the Superior Institute of Registration Studies (PNUD and AECID),

At the same time we have started a Personnel Training Process never implemented before.

- Issuance of an Identification Document for minors under 18, which range starts when turning 12, what will avoid theft of identity numbers, for obtaining an early ten-fingerprint record;

- Identity Card Renewal Project

- Update of the Civil Register Databases incorporating the Books of 2004 until uptodate;

- To start the reweing process of the Audit Logs for the update of the Civil Register Databases;

- To identify the inconsistencies between Databases of the Civil Register, and Identification for a joint correction with the MCR's

- Preliminary analysis of alternatives to homologate the Civil Register Databases first and aftwerwads the Civil Register and Identification Databases, combined with the Central Archive Images Databases;

- To start the development of a new Civil Register System (PNUD and IT Department and Civil Register)

- Improvement of the Communications System using cutting-edge technology through Internet and VoIP infrastructure

- The GRO Technological Renewal Plan has been defined and comprises the following areas:

- To elaborate plans;

- To standardize the types of premises, furniture and equipment configuration,

- To determine Software needs;

- To design the Comprehensive Communications System requiered for every MCR, Administrative, IT Technical, Registration and Identification areas,

- To elaborate and Implement the Web Page with Browsing Systems into the Civil Register and Identification, institutional procedures at informatics level within the framework of E-government strategy (jointly with the PNUD);

- To define the Identity Card Renewal Project, establishing the process strategy and plans:

-To select the Material and Security Size of the Identity Document.

-To define Registration Strategies and Printing

- To elaborate thel Mechanization Plan of the Civil Registers in stages
- To create a Temporal Administrative Structure (Committee) of the Project.
- To elaborate the Terms of Reference for the Procument of the Project's resources
- To elaborate Transparent Methodology for the Evaluation of Quotations and Awarding of Contract (s) with a high amount of Proposals; International Bid process with intermediaction (contracting) of an expert External Insititution (PNUD, OEA, etc.) and National and International Supervision (Superior Court of Accounts, National Anticorruption Commission, Churches, Supreme Electoral Court, OEA, ONU, etc.)
- To report the Identity Card Renewal Project to 15 interested international companies
- Presentation of the Comprehensive Project for the Technological Upgrade of the GRO to the National Congress,
To be discussed and to have the financial resources approved. The Relevant Components for the execution in steps are:
 - Update, Depuration, Unification and Homologation of the Civil Register and Identification Databases;
 - Transcription of Books;
 - Depuration of the Central Archive, Civil Register and Identification Databases;
 - Homologation of the GRO Databases
 - Modernization and Strengthening of the MCR's
 - Appropriate premises;
 - Equipment;
 - Communications;
 - Information Registration or Capture
 - Photo;
 - Fingerprints;
 - Update of domicile, personal details, etc.
 - Automated Fingerprint Identification System (AFIS)
 - Software upgrade;
 - Hardware replacement;
 - Print line
 - Printers for the Identity Cards
 - Identity Cards Material
- Benefits of the Project
 - Social Inclusion
 - Documents and Databases Security;
 - Quality Services to the Population, Public and Private Institutions;
 - Depurated Electoral Census;
 - Timely and reliable Vital Statistics (since 1989 there has not been any in Honduras);
 - GRO turned into a true Institution of National Security
 - Reliability;
 - Additional Savings in the State;
 - New Hires;
 - Immediate answer capability of the GRO for the implementation of e-Government.

Cities with its structure, not on-line

Cod. Depto	Cod. Mun.	Departamento	Municipio
01	04	Atlántida	Jutiapa
01	06	Atlántida	San Francisco
01	08	Atlántida	Arizona
02	01	Colón	Trujillo
02	02	Colón	Balfate
02	05	Colón	Saba
02	08	Colón	Sonaguera
04	04	Copan	Copan Ruinas
04	09	Copan	El Paraiso
05	02	Cortés	Omoa
06	04	Choluteca	Duyure
06	06	Choluteca	El Triunfo
06	15	Choluteca	San Marcos de Colón
07	01	El Paraiso	Yuscaran
07	04	El Paraiso	El Paraiso
07	19	El Paraiso	Trojes
08	06	Fco. Morazán	Guaimaca
08	16	Fco. Morazán	Sabanagrande
08	24	Fco. Morazán	Talanga
09	01	Gracias a Dios	Puerto Lempira
10	01	Intibuca	La Esperanza
10	04	Intibuca	Concepción
10	06	Intibuca	Intibuca
10	09	Intibuca	Masaguara
11	01	Isla de la Bahía	Roatan
12	08	La Paz	Marcala
13	01	Lempira	Gracias
13	07	Lempira	Guarita
13	09	Lempira	La Iguala
13	10	Lempira	Las Flores
13	11	Lempira	La Unión
13	12	Lempira	La Virtud
13	13	Lempira	Lepaera
13	16	Lempira	San Andres
13	18	Lempira	Sn Juan Guarita
13	20	Lempira	San Rafael
13	26	Lempira	Valladolid
14	01	Ocotepeque	Ocotepeque
14	07	Ocotepeque	La Labor
14	13	Ocotepeque	San Marcos
14	06	Ocotepeque	La Encarnacion
14	08	Ocotepeque	Lucerna
14	16	Ocotepeque	Sinuapa
15	02	Olancho	Campamento
15	05	Olancho	Dulce Nombre de Culmi
15	23	Olancho	Froylan Turcios (Patuca)
16	13	Santa Barbara	Macuelizo

16	16	Santa Barbara	Petoa
16	17	Santa Barbara	Protección
16	25	Santa Barbara	San Vicente Centenario
17	07	Valle	Langue
18	01	Yoro	Yoro

Cities on-line

Cod. Depto	Cod. Mun.	Departamento	Municipio
01	01	Atlántida	La Ceiba
01	07	Atlántida	Tela
02	09	Colón	Tocoa
03	01	Comayagua	Comayagua
03	18	Comayagua	Siguatepeque
04	01	Copan	Sta. Rosa de Copan
04	13	Copan	Nueva Arcadia
05	01	Cortés	San Pedro Sula
05	02	Cortés	Choloma
05	06	Cortés	Puerto Cortes
05	11	Cortés	Villa Nueva
05	12	Cortés	La Lima
06	01	Choluteca	Choluteca
07	01	El Paraizo	Danli
08	01	Fco. Morazan	Distrito Central
12	01	La Paz	La Paz (sólo Registro Civil)
15	01	Olancho	Juticalpa
15	03	Olancho	Catacamas
16	01	Santa Barbara	Santa Barbara (sólo Registro Civil)
17	01	Valle	Nacaome (sólo Registro Civil)
17	09	Valle	San Lorenzo
18	04	Yoro	El Progreso
18	07	Yoro	Olanchito



Exhibit 3: Automated and online RCM map.

Bibliography

- Terms of Reference of the Technological Update of the General Register Office Project.
- “General Register Office Law”.

The Role of Identification in Social and Digital Inclusion

Dra. Mónica Litza



Dra. Mónica Litza

National Director. National Recidivism Registry. Ministry of Justice and Human Rights



Mónica Litza, graduated as a Lawyer, was appointed Senator of the Province of Buenos Aires for the 2003-2007 period. At present she is the Director of the National Recidivism Registry depending from the Ministry of Justice and Human Rights. She is the author of Law 13.666 “*Digital Signature, Digitizing of the Provincial Public Administration Procedures*”, among others laws.

She was speaker in diverse Seminars and Congresses, having special relevance at the III, IV and V International Biometrics Congress of the Argentine Republic; the III Regional Meeting of AFIS Users of Latin America and the Caribbean “*New Biometric Identification Parameters*”, Perú, 2010; the Biometric Consortium Conference, Tampa, E.E.U.U, 2010; and Biometrics 2010, London, Great Britain, “*Argentinean Biometrics: One Step Forward*”.

Contact Details: Tucumán N° 1353. C.P.: 1050
 Ciudad Autónoma de Buenos Aires
 email: mlitza@dnrec.jus.gov.ar
 web (personal): <http://www.monicalitza.com.ar>

Abstract

This further contribution enables us to expand on developments in biometrics within the Argentine public administration system.

Having described the functions of the National Register of Repeat Offenders in the previous paper, there is no need to analyse those functions again in any great detail, allowing us to concentrate on related aspects of biometrics in present-day Argentina.

We will therefore conduct a comprehensive analysis of the economic, political and social factors that shaped the biometric model, and the relationship between that model and current government policy.

We also considered it appropriate to highlight the role of information and communications technology in choosing the right paradigm as an empirical base for an analysis of the current state of biometrics, and its importance as a policy tool for social inclusion rather than simply for identification purposes.

The development of IT infrastructures, and advances in digital storage methods, have provided an opportunity to rethink administrative models and assign new functions to existing biometric identification systems.

In line with this, we have outlined two developments which will allow the interoperability of public biometric databases to be coordinated so as to design security policies that achieve maximum performance of government functions.

The Role of Identification in Social and Digital Inclusion

Introduction

"I am me and my circumstance..."

This phrase, from “Meditaciones del Quijote” (“Meditations on Quixote”) by Ortega y Gasset (1883-1955), has to be the starting point for understanding the importance of biometry, its trends and its significance as a policy tool for social and digital inclusion within the framework of the National Digital Agenda.

The idea is that the “*contextual reality*” created by man comprises the other half of a person and is represented by technology; in other words, Man’s adaptation of Nature in order to satisfy his needs. Only thus is Man a combination of circumstantial realities created as a source of inspiration by cultures that embrace new thinking.

So this “*reality*” is nothing more than a projection of human creation, and as such transcends it without ceasing to be part of it.

Thus any discussion of biometry involves talking about this technological reality and carrying out a comprehensive analysis in order to get a better understanding of its role in present-day society, in the context of the design of inclusive government policies, without ignoring the role of information and communications technology.

One can say that biometry has overtaken scientific methods of personal identification and become a tool of social inclusion, since it enables greater integration between the daily activity of the state and its citizens.

It would not be possible to offer an analysis of the “*biometric reality*” without first defining its “*contextual reality*”.

As a means of personal identification, biometry assesses facial and behavioural features. It gives form to the Right to Identity, a fundamental right which must be guaranteed by the State, and, by virtue of that right, a new system of further rights has been formulated which are indispensable for the existence of individuals and their integration into society.

In the present day, every process conducted within a biometric system needs sufficiently developed technology in which most instances of data capture and comparison, and their results, are achieved in entirely digital environments.

We should say that we prefer to see biometry as a means of inclusion, whether social or digital, forming part of a combination of resources, established within the framework of government policy, in which the idea of reform and redress are directed at satisfying social needs and guaranteeing the rights of citizens.

To appreciate the importance of biometry as a tool, it is essential to set out its importance

within the government policies underlying the National Digital Agenda. This planning involves critical review, the selection of a universally applicable model, regional integration, and the overarching concept of identity.

The Digital Agenda involves: the guiding principles of electronic government, the standards that guarantee network cyber-security, programs designed to reduce the digital divide, others to promote digital literacy, and yet more to develop new IT platforms, software protection programs, and hardware development.

The use of technology is coordinated by the Under-Secretariat of Management Technologies, which observes the standards of interoperability and compatibility which are the common denominators in the process of integration which allows the information in the government's custody to become more important and more valuable. This coordination is fundamental when designing and planning medium- and long-term policies.

Incorporating technology into state organisations

"Technology only makes sense to the extent that it is provided with content"

As has already been mentioned, the use of biometry as a method of identification involves the authentication of data in a digital environment. It will therefore be useful to take a look back at the technological advances that have taken place over the last few decades both in society in general and specifically within public administration.

The need for interoperability is symptomatic of our "contextual reality", and we must therefore consider its causes.

The neo-liberal policies of the 90s produced one of the biggest reductions in income distribution and, as an immediate consequence; social inequality grew against a background of the opening-up of commercial and financial markets as a result of economic deregulation.

Against this background there was a mass influx of imported capital goods, including hardware and software. At the same time, the demand for more complex software and IT services was fed from abroad, leading to what might be considered a clear technological dependence, further accentuating the existing gap, particularly within public bodies.

Towards the end of the 90s, a survey conducted by Microsoft found that of the 74% of Argentineans who had television, only 7.4% owned a computer, an alarming statistic even without adding the fact that 67% of all computers were in the federal capital, Buenos Aires.

The current situation is that "in 2001, 30% of homes had internet access, and in 2010 that figure had increased to 47%, or 5 million people", in the words of President Cristina Fernández de Kirchner as she helped launch Infojus, the website of the Argentine Legal Information Service of the Ministry of Justice, which allows all citizens to have free and unrestricted access to all relevant information from the judicial system.

If we stop there for a moment, we can clearly see that the challenge has been extending inclusion to the majority of citizens and state organisations in the national digital agenda, which has involved establishing strategies that view digital inclusion as a fundamental tool for social inclusion.

The change in culture that has taken place to make technological resources more available to people has gone hand in hand with computer literacy programs designed to ensure those people can access and make best use of those resources.

In order to analyse the impact of digital growth within public administration organisations, we must consider the different levels of technological development and the usefulness of specific digital services in relation to the ability of users to access them.

Digital inclusion, in the context of a state organisation, means narrowing the existing gap in the access of individuals to its services and creating genuine digital bridges between the various organisations within the national public administration in order to connect the information society.

The process of computerisation and digitalisation in the National Register of Repeat Offenders started more than a decade ago. Through its *"Justice System Reform Program"* it acquired the hardware and software needed to digitalise its criminal records in accordance with the international standards governing the biometric data contained within them, thereby ensuring that the future interoperability of its database with other similar databases.

In addition, the implementation of the Digital Signature Law No. 25.506 has allowed details of criminal records to be certified more securely and, along with new data capture systems, has enabled the widening of identification parameters, ultimately resulting in a better use of the information held by the organisation.

We are working towards a 2.0 culture based on openness, cooperation and interoperability; in other words, we are creating an open and intelligent register as part of the concept of open government.

It is important to point out that the incorporation of technology only makes sense to the extent that it is given content, which is why it must be based on a clearly constructed policy given that it represents an essential tool in the transformation process.

Applied in a context of constant innovation, information and communications technology has eliminated a wide range of bureaucratic tasks.

Promoting digital development such as an operating platform for the state's biometric systems requires the creation of an environment which supports the setting up of new software and hardware companies, which means determining growth strategies that promote science and education.

These new businesses came about in a variety of ways, either through protective measures that promoted domestic industry or through regulations such as the recently enacted Digital

Records Law No. 26.685, which authorises the use of digital files, documents, signatures, communications and e-mail addresses in judicial and administrative proceedings throughout the country's judicial system, and gives the digital versions equal legal effect and probative value as the conventional equivalents.

Public administration involves constantly designing new tools to meet this constantly evolving "contextual reality". That is why, when proposing reform of the National Register of Repeat Offenders Law 22.117, we highlighted the value of biometry as a fundamental element in the fight against crime and reaffirmed its singular importance in the design of security policies.

We believe that the key to defining successful strategies for the simplification of public administrative processes lies in the capacity to establish a management model appropriate to their specific functions, which means abandoning out-dated policies in favour of the concept of the open and proactive organisation.

The guiding principles of cooperation, interconnection and interoperability on which current public policy is based, and constant technological innovation in digital environments, have enabled the construction of new platforms designed to broaden the service traditionally provided by the National Register of Repeat Offenders with the aim of increasing its interaction with the security forces through the National Default and Detention Order Enquiry System (CoNaRC), with the National Road Safety Agency through the National Disqualified Driver Enquiry System (CoNIC), and with the National Register of Persons for the issue of new passports (CoNAAP).

Integration and interaction through new tools

"Someone else already has the information I need"

Linked public database platform

Digital inclusion is the strategy at the heart of the current government's promotion, through its National Telecommunications Plan "Argentina Conectada" (Argentina Connected), of the new social structures created by the advent of the Internet. This makes it possible to consider strategic mergers within public administration in order to centralise information and thus help each government body perform their specific functions.

The coordination and integration of biometric databases through technological platforms presents the state with new scenarios in which accurate and rapid identification of individuals is vital. For those organisations which, like ours, are linked to the identification of individuals, that integration is strategic, since it allows the exchange of biometric information which is currently contained in strictly compartmentalised.

The implementation of a platform will advance the treatment of biometric data through the use of digital environments that highlight the improved running of the state.

In some way these developments are the catalyst for continued construction of a networked

country run on flexible organisational models.

The parties comprising that platform are the National Register of Persons, the National Immigration Directorate, the National Register of Repeat Offenders and the Federal Police, which each have digitalised biometric databases that, despite being fully interoperable, do not currently interact.

Separately, the Linked Public Database Platform is the foundation stone for the implementation of various systems such as the one we are about to discuss.

National system of search and identification of persons (SINABIP)

This system represents the first national development of a search and identification service, allowing the state to address the needs of society, while safeguarding due identification and guaranteeing the Right to Identity.

The aim is to interconnect the different organisations which handle biometric information, such as the National Register of Repeat Offenders, the National Missing Children Register, the National Register of Persons, the National Immigration Directorate and the Federal Police.

A networked register



The National Register of Repeat Offenders
Interacts with the Interior Ministry and the
Ministry of Security



Enquiries from mobile police units:
The National Register of Repeat Offenders (RNR) participates along with other organisations such as the National Register of Persons (RENAPER), the National Register of Firearms (RENAR) and the Register of Motor Vehicles. Specifically, police officers can search the national inquiry system of defaults and detention orders (CONARC) directly from their mobile units



National Criminal Records Search for Passports (CONAPP): the National Register of Repeat Offenders works in conjunction with the National Register of Persons. The Interior Ministry searches criminal records and the list of outstanding default and detention orders in respect of everyone who applies for a passport.

NATIONAL REGISTER OF REPEAT OFFENDERS

A new State paradigm

CONIC
National Register
of Disqualified
Drivers

CONARC
National Inquiry
System for Default &
Detention Orders

CONAPP
National Criminal
Records Search for
Passports

SINABIP
National System
for the Search and
Identification of Persons

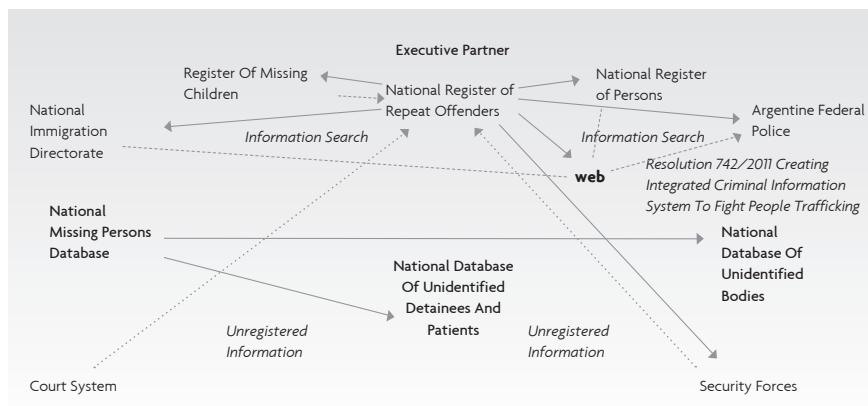
LINKED PUBLIC DATABASE PLATFORM

When added to the system, personal biometric details will be stored in three independent databases which, in addition to being permanently cross-referenced, will be compared with information from the other databases forming part of the system. This methodology, added to the dissemination of useful information, ensures likely success through persistent searching.

In this specific example, judicial authorities and the armed and security forces represent the system's channels of communication, since information is received and transmitted by those parties, which is vitally important to ensure appropriate measures are taken as quickly as possible.

This tool will aid potential victims of complex crime, such as people trafficking, unlawful detention and kidnapping and extortion. It therefore constitutes a significant contribution to policies of public security.

Working diagram of the National System for the Search and Identification of Persons



Conclusion

The last few years have seen the implementation of administration policies designed to standardise the handling of biometric data stored in digital public databases, with the aim of ensuring interoperability.

Those of us involved in public administration understand that seeing through the process of change requires strong political leadership.

The use of biometry as a non-invasive means of identification requires a series of coordinated actions in order to promote the development of technology as well as training in the use of that technology.

In addition, as we have maintained throughout this paper, we can confirm that biometry is more than just part of the science of identification of individuals: it has become a means of social inclusion, because it facilitates better integration of citizens into the day-to-day activities of the state, such as their identification for the purpose of obtaining social security benefits, a copy of their criminal record, a driving licence, an identity card or a passport.

In conclusion we might attempt an analogy based on the expression “we are what we share”, which when applied to the question of biometrics enables us to realise that “in today’s biometric world, to share is to protect”.

Bibliography

Criado, J.I. y Ramilo, M.C.: “E-Administración: ¿Un reto o una nueva moda? Problemas y perspectivas de futuro en torno a internet y las tecnologías de la información y la comunicación en las administraciones públicas del siglo XXI”. Instituto Vasco de la Administración Pública.

Achiary, Carlos (2005): “Interoperabilidad para el gobierno electrónico”, X Congreso Internacional del CLAD sobre Reforma del Estado y la Administración Pública, Santiago, Chile, 18-21 de octubre de 2005

Calderón, Cesar ; Lorenzo, Sebastián (2010): “Open Government - Gobierno Abierto” 1 ed. Buenos Aires, Capital Intelectual.

Cabello, Roxana (2003): “Argentina Digital” Ed. Universidad Nacional de General Sarmiento. Biblioteca Nacional.

Advances in the Federal Penitentiary Service's Biometrics Projects

Néstor Matosian



Néstor Matosian

Director of the Board of Planning and Coordination (COPIC) of the Federal Penitentiary Service



Born on February 10, 1954. He enrolled in the National Penitentiary School in September 1975 and graduated as a Fingerprint Expert in 1978. (School of Fingerprint Experts of the City of Buenos Aires)

Relevant positions:

Year 1995/97: Chief of the Recuperation Centre for people affected by AIDS – Detention Unit (U.2) Devoto.

1998/99: Area Chief – Internal Security Division of the above Unit.

2000: Secretary and Chief of the Young Adults Division at the former Imprisonment Unit (U:16) City of Buenos Aires;

2001: Chief of the External Security Division of the Women Imprisonment Unit “Nuestra Señora del Rosario de San Nicolás” (U.31); Secretary at the Federal Penitentiary Complex I-Ezeiza.

2002: Deputy Director of the Women Detention Centre (U.3)-Ezeiza.

2003: Training Course for Chief Officers.

2004: Deputy Director of the Criminal Unit of Viedma (U.12).

2005: Director at the Judicial Direction.

2006: Director at the Detention Unit (U.2) Devoto – at present belonging to the City of Buenos Aires.

2007: General Director of the Detention Regime.

2008/2009: General Director of the Penitentiary Body.

Year 2010: Deputy Director of the Federal Penitentiary Service.

Since August 2010: member of the Planning and Coordination Council of the Federal Penitentiary Service.

Abstract

Nowadays, the Federal Penitentiary System uses biometry with the aim of obtaining larger social inclusion, in pursuit of the social rehabilitation that the Nation needs.

The access control for visits, the enroll of inmates, the public multi-biometric telephone system, the biometric virtual visit, the use of internet with PIV, are some of the projects that the Federal Penitentiary system is developing together with the Ministry of Justice and the ONTI (National Office of Information Technology), in order to work with more commitment and efficiency on the social rehabilitation, facilitating the access to new technologies and simplifying family visits.

Advances in the Federal Penitentiary Service's Biometrics Projects

In 2005, then president Dr. Néstor Kirchner gave the name “ROBERTO PETTINATO” to the Academy of Advanced Penal Studies. In doing so, he recalled that it was Inspector General Roberto Pettinato who, at the beginning of the 1950s, promoted the reforms that, among other things, introduced the principle of socialisation as a mainstay of the treatment of prisoners within the penal system.

Since Inspector General Pettinato was appointed to head the institution, the Federal Penitentiary Service (SPF) has been symbolic of efforts to education and socialize prisoners, with the aim of making incarceration about reintegration into society rather than punishment.

Since then, the work of the SPF has been to achieve ever better results in this difficult but, in terms of every citizen's safety, hugely important task.

In 1947 the SPF entered what is known as the Period of Progressive Regulation of Law No. 11.833. That law included the creation of the Penitentiary School, with the idea of forming teams to work towards the socialization of prisoners.

With Inspector General Pettinato's arrival the SPF was able not only to turn the advances already introduced by the law 11.833 into reality, but also to emphasize even further the correctional and humanistic principles that have always guided Argentina's approach to punishment.

However the consolidation of the institution took place at the beginning of 1958 with the passing of the National Penitentiary Law as a complement to the Penal Code (Decree Law No. 412 dated 14 January 1958, ratified on 23 October in the same year by the National Congress through Law 14.467). Within the prison system we identify this period as the legal unification of the penal regime.

This old law lasted and went on to serve as the basis for the development and modernization of our prisons and the creation of what is today known as the Federal Penitentiary Service.

With democracy already well re-established, the spirit of constitutional renewal saw the passing into law in 1996 of the Sentencing to Imprisonment Law No. 24.660, which is the country's most advanced set of rules ever in the field of penal legislation. Without a shadow of a doubt, these provisions and related regulations marked the start of a more modern, more open and more inclusive era.

But there is no doubt that it is in the last few years that the changes have become deeper, more far-reaching and above all more controversial. Roberto Pettinato was undoubtedly a revolutionary in the field of punishment, and naming our Academy in his honour is a way of indicating our future direction.

No doubt this was the ex-president's intention, and certainly there is no doubt that this is the road the SPF took. He made us think from that moment on about the future, and anticipate it.

It was during his presidency, and obviously now during the presidency of Cristina Kirchner, that the possibility of incorporating new technology into our work forced us to think differently, since this technology was changing our operating environment dramatically, and producing a revolution in prison life as much as in daily life generally.

With the arrival of Pettinato at the helm of the Penitentiary Service, its work was focused solely on facilitating the rehabilitation and reintegration of prisoners into society. Today that mission is expanding: in recent years, thinking on punishment issues has been extended to social inclusion and equal opportunities. These are the challenges of the times, and the SPF has embraced the government's mandate to address them.

However this reintegration into society cannot be successfully achieved by the Federal Penitentiary Service without adapting to the technological and cultural changes taking place in a rapidly-changing world.

Today, biometrics is a tool that helps our work in relation to the social inclusion and social reintegration that our country needs. In this context the first stage of the Biometric Access Control System that the SPF is putting in place is now operating in the Ezeiza Prison Complex. Implementing this initiative was not straightforward: first we had to overcome resistance from our own staff, then certain concerns within the judicial system, and finally the concerns of prisoners' families.

Everyone worked very hard in this regard, not just in the SPF but within the Ministry of Justice itself, through the Directorate of Information Management (the DGGI) and the National Office of Information Technology (the ONTI), which reports to the Office of the Cabinet Chief of Staff.

This initiative, involving prisoners' families, the judiciary, SPF staff, and even the prisoners themselves, was ultimately a success and today is part of the daily routine, in which the processing of prison visitors is faster, simpler and safer.

This has led us to plan and develop the second stage of this ambitious plan, which sees it being implemented in a further eight penitentiary systems.

However those are not the only biometric projects the SPF is implementing, there are many more. We are very proud of them because they will allow us to educate and train prisoners in new technology so that they can rejoin and participate in a society which is moving forward, and which demands people to be trained in modern technology and to be capable of working in an increasingly technological world.

But in order to achieve this we must work very hard and distinguish between those prisoners who are not seeking to be reintegrated into society from those who have made mistakes and accept the period of their incarceration in our facilities as an opportunity to better themselves, acquire an education and thus make reintegration into society, back with their family, a possibility.

This is no easy task, because our country has been experiencing great change for many years. Take, for example, the technological changes in telephonic communication.

To understand our zeal and dedication to this issue, we first need to be aware that by virtue of article 75 paragraph 22 of the National Constitution the country has added international agreements to the SPF's charter, and has recognised new rights that now have constitutional status.

Thus when an individual is convicted, he may be deprived of his freedom but may not suffer any restriction of his communications or in his right to information.

In SPF facilities, a prisoner can call whoever he wants, without restriction, and just like anyone in the outside world can make as many calls as he wants. In some countries, a convict can choose only five numbers, in others calls are restricted to direct family and a pre-appointed lawyer, but in this country there are no restrictions, and we agree that there should be none, despite the significant inconvenience that results.

In principle, calls from cellphones are prohibited, as they are in all of the world's penitentiary systems, but the smuggling of cellphones into prisons has become widespread, and many prisoners who have no interest in rehabilitation are committing crimes such as frauds and virtual kidnappings by phone. While most of these crimes are committed using cellphones, some are carried out using the public telephones provided for prisoners' use.

This harsh reality is the reason why we are implementing a system of control, location and blocking of high-technology cellphones, and very shortly it will be impossible to make a call from any cellphone without it being detected, located and immediately interrupted.

The SPF is aware that this will lead to an increase in the use of the public telephones to commit crime. The public telephones installed in prisons contain a system designed by the phone company which should always provide a warning to the recipient that the call is being made from a prison; but by using certain phone cards that are available on the market, many prisoners have been able to circumvent this warning and carry out virtual kidnappings and other crimes from these public phones.

To date, service providers have been unable to resolve this problem, and we have instead found a solution to this serious nuisance using biometrics. We have therefore decided to introduce biometric and anti-vandal public telephones in all of our prisons, amounting to more than one thousand phones.

We are making progress in the introduction of this new system of public telephones, which will feature fingerprint and voice recognition, photographic recording of the caller at regular intervals, and a record of the time and duration of the call and the number to which it was made; but in order to guarantee the prisoner's privacy, all of this data is accessible only with a court order following a judicial investigation.

So biometrics is helping to guarantee the rights of those who wish to live correctly, and target only those who seek to offend further. Exercise of the right to communicate is neither removed

or restricted, but we know that an offender can easily be identified and punished.

We are well advanced towards the implementation of this system, which we consider extremely important, and we are sure that in the next CIBRA we will be in a position to describe that implementation.

We are also working hard on the introduction of biometric stations for prisoner registration. As in all of these developments, we are moving forward in stages, but there is no doubt that this initiative will be extremely useful, not just for the permanent verification of a prisoner's identity and the ability to locate him, but also in relation to a very ambitious project being tackled by all national authorities, namely the national biometric network, which the SPF, along with the National Reoffenders Register, will be among the first to join.

Another of the things we are addressing, and which is in an advanced stage of design, is the system of virtual visiting. For a number of years, and especially with the arrival of the phenomenon known as globalisation, the number of foreign nationals in our prisons has grown significantly.

A moment ago I was talking about the difficulties of achieving a prisoner's reintegration into society. That reintegration is much more difficult when a prisoner loses the link with his or her family.

That is why the SPF is working tirelessly to help prisoners maintain and even strengthen their family ties. Without those ties, reintegration is almost impossible.

We are therefore designing a system to help both foreign prisoners and those from this country whose families live at a distance. In all SPF facilities, we will have a biometric virtual visiting room in which, once enrolled, the prisoner and the visitor can have a virtual visit in high quality audio and video and thereby share time together in a way which distance and cost would otherwise prevent, or at least allow only infrequently. In the case of foreign prisoners, responsibility for verifying the identity of the virtual visitor will rest with the local consulate or embassy.

Our institution is, with a lot of government support, introducing revolutionary changes. We are without doubt the most advanced institution, in terms of biometrics, in the country, if not in the region.

I should therefore make reference to the most ambitious and revolutionary project undertaken in relation to the prison system in recent years.

Information technology cannot be ignored and is something we must live with and learn to take advantage of to ensure improved management of governmental processes. Its progress in every aspect of society - work, security, government, higher education and business - is undeniable. It increases our physical and mental capacity, as well as the possibilities for social and digital inclusion and development. Not to include technology in the changes we are proposing would be to exclude the potential benefits to the state and to society as a whole.

Today consideration of penal issues includes thinking about social inclusion and equal opportunities. This is genuine reintegration. We cannot rehabilitate and reintegrate prisoners unless we work on social inclusion. There will be no successful reintegration policy for the Federal Penitentiary Service if we fail to adapt to the technological and cultural changes occurring in the world in which we operate.

Independently of socio-cultural considerations, the question of access to new technology has lodged itself in the public consciousness as an incontrovertible necessity, and increasingly this widens the gap between those who have access to it and those who don't.

In the present day there is a deep conviction that without the knowledge to use and live with a computer, one will in the future be excluded from all of its benefits, which again will create a deep division in society between those with access and those without.

Against this background the federal government has spent a number of years promoting and developing a nationwide plan known as Digital Agenda Argentina with the aim of mapping out a strategy for the use and application of information technology to generate greater inclusion and promote its development.

More recently, the General Assembly of the United Nations declared access to the Internet to be a highly protected human right. In an unprecedented declaration, the UN established that every world government will have an obligation to facilitate a service that is "accessible and affordable for all", and guaranteeing an Internet connection will be a priority.

Among other things, the UN has stipulated that preventing Internet access is a violation of article 19, paragraph 3 of the International Covenant on Civil and Political Rights, and requires that states guarantee Internet access to the whole of society. This Covenant is enshrined in our Constitution.

Nevertheless it is no less certain that our task is to contribute to the maintenance of the nation's security and prevent the commission of crimes using this new technology, so that we need to study ways of preventing such crimes whilst satisfying the constitutional requirement to apply the minimum restrictions possible to the flow of information over the Internet.

We have spent a long time evaluating the problem and, in line with official thinking, there is now a growing fear within the SPF that the lack of contact with computers is becoming a new form of social exclusion which makes our work to rehabilitate and reintegrate prisoners even more difficult.

In view of this, and looking to the future, the Federal Penitentiary Service is working hard to include itself in a national project whose aim is to create an equal, inclusive, progressive and developed Argentina. To this end the SPF is working along with the DGII and the ONTI on the implementation of a complete computerised system, including Internet access, for all prisoners within the prison system.

This new system, which is still under development, will feature a biometric system of personal

identification verification, with face recognition, and as already stated it will provide a means of training and preparing prisoners to re-enter society and return to work.

These are the biometric projects which we are currently developing. There are many of them, they are ambitious, and they are all very important for both the SPF and for the country.

Only a few years ago, when we initiated these projects in the SPF, talk of biometrics was something fanciful or fantastic. Today, the efforts of the SPF and the government have already made them a reality, and they are undoubtedly becoming an effective tool for better management and therefore greater success in social inclusion and reintegration, as a result of which we are able to move a step closer to our constitutional mandate, and especially what is required of us by article 75, paragraph 23: *"to promote positive measures to guarantee real equality of opportunity and treatment, and the full enjoyment and exercise of the rights recognised by this Constitution and by applicable international treaties regarding human rights"*.

Biometric tools in the province of Buenos Aires: Successful cases

Gustavo Donato



Gustavo Donato

Director of the Biometrics Provincial Office



Gustavo Fabián Donato was born on October 8, 1970. He attended Secondary School at the General San Martín Military School and the Military School of the Nation. Since 1993 he has been working at the Ministry of Security of the Province of Buenos Aires as Officer of the Police of the Province of Buenos Aires reaching the rank of Deputy Commissioner. He also attended a graduate course at the National University of Lanús, being the first graduate in the course of Citizen Security. He took post graduate courses on Specialization in Public Security Law and Management at the University Carlos III of Madrid and the Universidad del Salvador (Argentina); a Master degree in National Defense in the School of National Defense and a Postgraduate course in Political Science in the University of Universidad del Salvador, among other courses. He is also a founder member of the civil association Argentine Security Association (legal registration 1059 of the Commercial Registry). Since 2008 he has been working at the Ministry of the Chief of the Cabinet Office and was afterwards appointed in the Biometrics Provincial Office.

Contact: gfdonato@gmail.com | gdonato@gob.gba.gov.ar

Abstract

Without doubt, during the 20th century and the beginnings of the 21st century, humanity has witnessed the biggest advances in all fields, specially in the field of technology. Every day, more and better technologies appear that change fundamentally people's life. States didn't remain outside these changes, and decided to incorporate new technological tools to improve their administration. The emergence of biometry and systems of biometric recognition didn't go unnoticed, and States started to use them in order to improve the security in the handling of information, particularly in what concerns the identification of their inhabitants. The Argentinian Republic has implemented satisfactorily the use of biometric tools and the Province of Buenos Aires has joined up this project, initiating a process of continuous growth in the development of biometric bases in several government fields, fed through the biometric enrolling of individuals. In this paper I will describe concisely the advance of biometry in the country's most populated province, including the creation of the Provincial Office of Biometry, the only of its kind at the national level, as well as some of the projects in which we are daily working to improve people's quality of life in Buenos Aires.

Key Words: Biometrics. Databases. Technology. Information. Objectives. Data. Fingerprints. Enrolment. AFIS. Security. Interoperability.

Biometric tools in the province of Buenos Aires: Successful cases

*"God stamped the hand of every man, that he might know his own works". Commissioner Alberto Pérez.
Papiloscopy Practice Manual*

During the governorship of Daniel Scioli, the government of the Province of Buenos Aires created through the Chief of the Ministerial Cabinet in charge of Mr. Alberto Perez (whose dead father, Commissioner Alberto Perez made a valuable contribution to Biometrics with his book Papiloscopy Practice Manual) the National Biometrics Office in order to implement and promote new techniques and apply international standards in the field of biometrics across all provincial agencies, permitting the dissemination of good practice in the recording of biometric data, and with a view to creating and integrating the resultant biometric databases.

Biometrics being the study of methods and techniques for the unique recognition of each human based on one or more intrinsic behavioural or physical characteristic, we considered the use of biometric tools, and the resultant setting of province-wide standards for improving the security of the information gathered, to be of the utmost importance.

In information technology (IT), biometric authentication refers to technology for measuring and analyzing human physiological and behavioural characteristics for the purpose of authenticating identity. Fingerprints, the iris, facial features, DNA, blood vessel patterns, and the geometry of the palm of the hand are examples of physiological (or static) characteristics, while behavioural (or dynamic) characteristics include one's signature, gait and typing rhythm. The voice is considered a mixture of physiological and behavioural characteristics, although all biometric features share physical and behavioural aspects.

For example the technology used for fingerprint recognition has as its purpose the rapid and precise identification of a single person using their fingerprint, certifying a person's identity in a unique and incontrovertible manner by means of an electronic device (which may be static or portable) that captures the fingerprints, and a program that verifies the identity, whether on a one to one or a one to many basis.

The primary objectives of the Provincial Biometrics Office are:

- 1 To put the Province of Buenos Aires at the forefront in the security, handling and safeguarding of personal information.
- 2 To combine the personal details obtained from individuals in each of the province's various government departments.
- 3 To set standards for the application of biometric techniques to ensure information is secure.
- 4 To generate a biometric database as a central tool for the safeguarding of the identity of each inhabitant of the province.
- 5 Together with the standardization of the recording of biometric details, to work towards the unification of platforms among the databases of the different provincial jurisdictions.

- 6 To design training and regular seminars to promote, instill and communicate the benefits of biometric tools, and to teach good and best practices in the recording of biometric details.

Actions designed to strengthen the Provincial Biometrics Office.

- * Design an integrated information technology development plan for the organization.
- * Coordinate and manage the operational steps necessary for widening the information network (biometric standards) among the different departments involved in the integration of data.
- * Map out the development and installation of database systems, operational programs and applications for the recording, storing and handling of information related to the work of the different departments.
- * Organise training for staff in the use of new biometric tools, systems and applications.
- * Evaluate quality systems in departments considered key to local management.
- * Coordinate and administer the establishment of biometric standards within the framework of relevant international norms (ANSI - NIST).
- * Control and verify the design and planning of additional projects which it will eventually be necessary to introduce for the implementation of the systems already referred to (in accordance with Inquiry No. 2208-358/10 which governed the creation of the Provincial Biometrics Office).

In general terms the strengthening of the Provincial Biometrics Office will allow a root and branch modernization of the organization's operations. This will occur as part of the process of creating technical and managerial capability as regards its organizational development, management and technical processes, the incorporation of technology, and its normative, methodological and instrumental framework aimed at providing support, training and oversight to its activities.

Successful cases of implementation

Provincial Directorate of Road Policy and Safety

The Provincial Directorate of Road Policy and Safety has developed a program to modernize their security processes in relation to the issue of driving licenses in the 135 municipalities situated throughout the province.

The Centralized Driving License Issuing System is designed to highlight the speed, transparency and security which national and international best practice enjoys through the use of technology. To achieve this, procedures for processing licenses are being redesigned and modernized. The province has made a significant investment in testing the validation and security of the new documentation, which contains 32 security measures that give it the same total protection against adulteration or falsification as an international passport.

The security of an identity document such as a driving license is determined by a series of

features designed to make it immune from falsification, adulteration, duplication and forgery. These documents incorporate both visible and non-visible features.

Firstly, the information is printed using special techniques that enable it to be recorded or printed deep into the material from which the license is made. On the front there is a special unique serial number and a two-dimensional code for automatic identification checks, which public and private institutions can use to carry out instant identity checks.

Under normal conditions of use this new driving license will still be in good condition when it expires after five years.

The license is made from a single piece of an innovative material which it is impossible to tear apart.

The so-called first line security features are plain to the eye, whereas additional equipment is needed to detect the second line features, and the third line features are a matter for the forensic laboratory.

First line or Level I Security Measures

1. Single piece of thermoplastic amalgam
2. Surface will be irreparably damaged, in a clearly visible manner, by any attempt to alter the printed details
3. Genuine and exclusive Guilloche patterned background
4. Genuine and exclusive line-based numismatic background
5. Genuine and exclusive sinusoidal-shaped numismatic background
6. Exclusive background printed using the IRIS system
7. Map of the province which changes colour depending on angle of view, printed in OVI/OVP ink
8. Laser-imaged micro photo and DNI number on the reverse
9. Latent image with the dual legend Valid/BsAs on the reverse
10. Embossed Guilloche rosettes perfectly matching the pre-printed image
11. Raised numbers and letters
12. OVD stripe that changes colour depending on angle of view
13. Digital photo of license holder
14. Web of curved lines superimposed on license holder's photo
15. Photo and variable data in the very body of the plastic substratum
16. License holder's digital signature
17. Digital signature of the issuing official

Second line or Level II Security Measures

18. Lines of positive and negative nanotext in the security background
19. Nanotext around the box containing the digital photograph
20. Latent image on the reverse, visible using a decoding lens
21. UV-reactive synthetic substratum
22. UV-reactive laser-imaged detail

Third line or Level III Security Measures

23. Encrypted features only detectable in the laboratory
24. Biometric features only detectable in the laboratory
25. Security background that reacts partially to infrared light, leaving the rest blank
26. Fragmentary text which is left partially invisible by infrared light
27. Unique code linking the printed details with alphanumeric information and images stored in the central database
28. PDF-417 2D barcode containing details of the license holder and the issuing official
29. PDF-247 2D barcode containing details of the issuing official (internal code)
30. PDF-247 2D barcode containing coded AFIS details of the license holder's fingerprints
31. PDF-247 2D barcode containing HCS (Hash Code Security) coded details calculated using the information relating to the license for checking variable details
32. PDF-247 2D barcode containing coded details of the version of the program that produced the license

Thus you can see how biometric technology has been incorporated into the driving license issuing process. The systems of biometric identification undoubtedly revolutionize the system of provincial security since they involve methods of identification and authentication of individuals through physical or behavioral characteristics.

In the case of driving licenses, the unique physical characteristic that identifies a person is his fingerprints.

Fingerprint identification is one of the most commonly used forms of biometry. A fingerprint is formed by a series of ridges. Where these ridges end or divide are called "minutiae". Each one of these points has a unique position and form, which can be measured. By comparing their distribution, it is possible to identify the person to whom the fingerprint belongs.

Biometric systems include a scanning device and software that interprets the physical details and transforms them into a numeric sequence. In the case of fingerprint identification, it should be borne in mind that only the minutiae are recorded, not an image of the whole fingerprint, and the former are represented in a numeric sequence that is stored in PDF-417 and/or BIDI format. Currently the Province has more than three hundred biometric enrolment stations distributed throughout the 135 municipalities of the province.

In addition, an AFIS (Automated Fingerprint Identification System) computer was bought and installed to enable the storing of the biometric details of more than five million driving



license holders within the province, and to enable 1:N verifications and authentications (comparing a unique fingerprint image with a fingerprint database). The province has also acquired PDA-style handheld multibiometric devices to provide the police and municipalities with the ability to carry out 1:1 identifications in the street.

The use of biometrics to identify an individual's unique characteristics offers a series of benefits that have not gone unnoticed by many governments. In the last few years, governmental authorities have instigated the research and implementation of pilot programs and biometric registers for the identification of their citizens, including in passports, identity cards and driving licenses.

Registry of Event Admission Staff (ReCAP)

In 2008 National Law No. 26.370 was passed, which set out rules for the authorization of personnel who deal with the admission and control of the general public at events, and for employers involved in organizing and running public events and shows.

In the Province of Buenos Aires Law No. 13.964 was passed, which adopted the same regime as already established nationally, and in terms of the subsequent Regulatory Decree 1096/09 the Provincial Public Registry of Event Admission Staff was created. This registry, maintained within the purview of the Subsecretariat of Planning in the Ministry of Justice and Security, and whose head is appointed by the Executive, is responsible for the authorization of those who carry out work related to the admission and control of the general public.

Structurally the Registry is organized into two departments:

Registration Department: This takes care of all procedures for the authorization of admission staff and the production of work permits and ID cards. All authorized personnel must display their ID cards at all times when working and the work permit represents their authority to carry out this type of work.

Authorisation Department: This department receives all of the documentation from businesses and venues, as well as granting authorizations to event staff companies and registering venues.

The Provincial Office of Biometrics has set down a protocol for the recording of personal data in the Registration Department. This provides for the biometric registration of all authorised staff by recording fingerprints, a photograph and a digital signature.

Direktorate General of Private Security Agencies

The Directorate General of Private Security Agencies is an organization, under the umbrella of the Ministry of Security of the Province of Buenos Aires, whose function is the exercise of control over companies that provide security services within the province. It has jurisdiction over administrative issues related to the authorization of those companies and their staff. It should be pointed out that there are more than one hundred and twenty thousand private security staff in the province, as many as the total number of officers in the province's police force. Like event admission and crowd control staff, private security firm employees have to satisfy appropriate legal requirements.

The Provincial Office of Biometry has accordingly created a protocol for the recording of those employees' biometric details in order that they can be identified and their authority to carry out security work verified. An AFIS computer has recently been acquired to store the databases

created by ReCAP and by the Directorate General of Private Security Agencies, and to enable 1:N comparisons to be carried out.

Buenos Aires Penitentiary Service

At the beginning of 2011 the Provincial Office of Biometry started working with the Buenos Aires Penitentiary Service to try to resolve fundamental issues related to the development of prison services: one the one hand, the issue of inter-prison transfers and transfers to and from court of inmates at the more than sixty provincial prisons and detention centres, and secondly prison access for prisoners' relatives.

To begin to address the foregoing issues, thirty biometric units for the processing of more than four thousand prisoners and thirty thousand visitors were installed in the Florencia Varela complex (comprising a total of ten separate facilities).

To do this, the Provincial Office of Biometry delivered three biometric units to each facility, one for recording prisoners' biometric details and the other two for the details of the visiting relatives (divided into men and women). The records comprise fingerprints, photograph and digital signature, and will be stored in the AFIS server acquired for use by the Provincial Penitentiary Service.

All of the databases created to date (in other words those set up by the Provincial Directorate of Road Policy and Safety, the Registry of Event Admission Staff, the Directorate General of Private Security Agencies and the Provincial Penitentiary Service) are completely cross-referable, having been set up under protocols and standards certified by the NIST (National Institute of Standards and Technology), the ANSI (American National Standards Institute) and the FBI (Federal Bureau of Investigation), and can be integrated with the databases fed by the five hundred local offices of the Provincial Civil Registry and the Rapid Documentation Centres (CDRs) in which the new DNI and passport are processed.

There is no doubt that with advances in new technology it has today become possible to carry out large-scale biometric projects in respect of the general population to complement the work done in respect of prisoners. Even cost does not present a significant barrier. In fact the main problem lies in finding specialized staff in this field, not only programmers but also people who are familiar with the operational rules, standards and practices in other countries.

Nevertheless, we believe that we are on the right track. We must continue working to improve good and best practices and ensure that all of the biometric databases can be used in cross-reference regardless of where they are or which organization administers them. We are convinced that the application of biometric tools will provide a noticeable improvement in the ability of the Province to protect personal identity.

**Identity, biometrics and digital signature in the region.
Framework for the Ibero-American Social Electronic Identification**

Gabriel Casal / Mercedes Rivolta



Gabriel Casal

Chief of Advisors of the Undersecretariat of Information Technologies



A Lawyer and Professor at the National University of La Plata. He worked as a Consultant at the National Direction of Culture and Education in the Province of Buenos Aires between 1994 and 1999. Chief of the Committee of Legal Affairs of the General Council of Culture and Education of the Province of Buenos Aires. Undersecretariat of the National Council for the Coordination of Social Policies of the Presidency. National Director of the National Identification, Tax and Social System - SINTYS. National Director of SIEMPRO-System for Information, Evaluation and Monitoring of Social Programs. Consultant at the Ministry of the Interior for the General Direction of IT Management. Consultant at the Ministry of Justice, Security and Human Rights of Argentina, in the General Direction of IT Management. Member of the Technical Committee in charge of writing the Code of Criminal Procedures of the Argentine Republic. Expert appointed by CLAD President in the Committee in charge of writing the new CLAD doctrinal document. Argentine Coordinator in the Digital MERCOSUR Project. Substitute Representative in the Subgroup 13 of E-Commerce in the MERCOSUR. Member of the Organizing Committee of the International Biometrics Congress of the Argentine Republic since 2006.

Contact: gabrielcasal@sgp.gov.ar, gcasal@jefatura.gob.ar, <http://ar.linkedin.com/pub/gabriel-casal/4/264/756>



Mercedes Rivolta

Advisor to the Undersecretariat of Management Technologies of the Chief of the Cabinet Office.



Lawyer. She has earned a degree of Magister in Public Administration (FCE UBA) and is member of the Staff of Government Administrators of the Cabinet Chief's Office. At present she is an advisor to the Undersecretariat of Management Technologies of the Chief of the Cabinet Office of Argentina. She was a member of the technical commissions in charge of writing Law No. 25.506 of digital signature, the Decree No. 1023/01 that sets up the public procurement regime of the National Administration, and a coordinator of the Technical Committee that wrote the Regularity Decree No. 2628/02 of the Argentine digital signature law. As an international consultant she has provided assistance to the governments of Panama, Dominican Republic, Peru, Paraguay, Colombia, Inter-American Development Bank and World Bank on subjects related to the regulation of electronic systems in public procurement and digital signature infrastructure.

Contact: mrivolta@jefatura.gob.ar, mercedesrivolta@yahoo.com.ar, <http://ar.linkedin.com/in/mercedesrivolta>

Abstract

The Framework for the Ibero-American Social Identification, a complement to the 2007 Ibero American Charter on E-Government, is an initiative that was presented by Argentina, at the XIII Meeting of the Ibero American Network of Ministers of the Presidency and Equivalent (RIMPE), in which subjects related to Citizen Participation in the E-government era: Education for Citizens and Digital Inclusion, were dealt with.

We consider that the Framework for the Ibero-American Social Identification is relevant for various reasons:

- a. It is the first expression of understanding among the Ibero-American countries that addresses the identification and the use of technology issues.
- b. It introduces the electronic authentication concept, as a link between the concepts of individuals identification in physical environments and the electronic/digital signature.
- c. It is the first time that a document deals in a jointly fashion with both issues, individuals identification in physical environments and individuals identification in electronic environments.
- d. It is the first expression of understanding among the Ibero-American countries that agree on a common glossary on the issues related to e-commerce, digital government and authentication in electronic environments.
- e. It constitutes a valuable antecedent to attain future agreements for mutual acknowledgement of digital signatures.

Therefore, we then understand that the Framework for the Ibero-American Social Identification turns to be a big leap forward. In this paper we analyze the mentioned framework from the legal point of view, identifying those aspects that are relevant from our legal system.

We are pursuing to start an interchange of opinions on these aspects, with the aim of contributing, in the middle term, to the attainment of agreements to facilitate individuals access to e-commerce and e-government.

Keywords: Argentina, Latin American Social Framework Electronic Identification, biometrics, digital signature, electronic signature, digital document, public administration, identity document, Information and Communication Technologies, Electronic Government Electronic Government Ibero-American

Identity, biometrics and digital signature in the region.

Framework for the Ibero-American Social Electronic Identification

Introduction

"Today, no scene nor mirror, but a screen and the network"
Jean Baudrillard

Since the 1st. edition of the book Biometrics, that was launched for the 5th. International Biometrics Conference of the Argentina Republic - CIBRA 2010, it has only passed one year. Nevertheless, an event that we consider a big progress on this subject has taken place.

We are referring to the Framework for the Ibero-American Social Electronic Identification to which we are going to refer as the Social e-ID Framework, complementary to the 2007 Ibero American Charter on E-Government.

The Social e-ID Framework is an initiative that was presented by Argentina at the XIII Meeting of the Ibero American Network of Ministers of the Presidency and Equivalent (RIMPE), in which subjects related to Citizen Participation in the E-government era: Education for Citizens and Digital Inclusion, were dealt with.

As a result of the meeting, the Lisbon Declaration was approved, which recommends "*the development of safe identification and electronic authentication is another condition for the pretended change, stressing its role in promoting procedure simplification and fostering the use of electronic services.*"

Such Lisbon Declaration acknowledges that "*e-government objectives shall go further than mere efficacy and efficiency of administration processes towards ways to enable social, political, and economical changes focused on human development, equal opportunities and social justice.*"

In turn, as a result, on July 1st, 2011 the Social e-ID Framework was approved in Asunción, Paraguay, during the *XII Ibero American Conference of Ministers of Public Administration and State Reform*, with the participation of 18 countries with over 40 delegates, within the framework of the "*XXI Ibero American Summit of Heads of State and Government*". In that opportunity, the participating nations committed to "*Continue the adoption of the Ibero American Charter on E-Government, which fosters the acknowledgement of the right to electronic access to the administration. For this purpose, it is necessary to encourage digital inclusion of all the inhabitants of the region, to foster social electronic identification and turn the Knowledge and Information Society into an opportunity for all, particularly by the inclusion of those at risk of being left behind*".

The signatory nations of the Asunción Declaration agreed on "Approving the Framework for the Ibero American Social Electronic Identification" as an addendum to the Ibero American Charter on E-Government.

The Social e-ID Framework is not a positive standard, as it has not been internalized for each of the nations. Nevertheless, it is a big progress as it represents the will of the Ibero American nations to attain a common criteria to deal with the issue of individuals' identification in physical and digital environments, expressed for the first time.

We consider that the Social e-ID Framework is relevant for various reasons:

- a. It is the first expression of understanding among the Ibero-American countries that addresses the identification and the use of technology issues.
- b. It introduces the electronic authentication concept, as a link between the concepts of individuals identification in physical environments and the electronic/digital signature.
- c. It is the first time that a document deals in a jointly fashion with both issues, individuals' identification in physical environments and individuals identification in electronic environments.
- d. It is the first expression of understanding among the Ibero-American countries that agree on a common glossary on the issues related to e-commerce, digital government and authentication in electronic environments.
- e. It constitutes a valuable antecedent to attain future agreements for mutual acknowledgement of digital signatures.

Therefore, we then understand that the Social e-ID Framework turns to be a big leap forward. In this paper we analyze the mentioned framework from the legal point of view, identifying those aspects that are relevant for our legal system.

We are pursuing to start an interchange of opinions on these aspects, with the aim of contributing, in the middle term, to the attainment of agreements to facilitate individuals access to e-commerce and e-government.

We are confident that progress in e-commerce is highly positive for the development of the economy, specially for the small and medium sized enterprises, with the consequent increase in decent jobs and the development of regional economies. And we understand that as there is progress in e-government, the access of individuals into their government, its administration, the State, means more democracy, more participation, more transparency, better government. But fundamentally, we are convinced that social inclusion policies deployed by our governments need individuals' identification to be effective. And that the effective exercise of rights starts when an individual has been identified, that individual possesses an identity and such identity is acknowledged.

Chapter II briefly describes the Argentine legal framework for individuals identification and digital signature. The main concepts are dealt with, their relationship with biometrics and digital signature and their legal nature.

Chapter III presents the Social e-ID Framework, and particularly, its principles and contents from the legal perspective.

In both Chapters, the Argentine legal concepts and those of the Social e-ID Framework are related, attempting to identify consistencies, coincidences and discrepancies, if there were any.

Chapter IV contains the conclusions and new opportunities that emerge from the Social e-ID Framework.

II. Argentine legal framework

The Social e-ID Framework focuses identification from different perspectives. It deals with the process of individuals' identification and the documents that are proof of such identity in the physical world. Also, it considers the issue of individuals' identification in virtual environments, for which it refers to the electronic signature and digital signature concepts, and introduces the electronic authentication concept. In both cases, i.e., applicable to both situations (identification in physical environments through identity documents and identification in digital environments), the Social e-ID Framework provides for the use of biometrics.

In the present paper we are going to deal with Argentine regulations referred to these issues.

a.I ndividuals' identification in physical environments

As the Social e-ID Framework has stated, individuals' identification is, simultaneously, an obligation and a right that enables the exercise of other rights: voting, social, educational, health, taxes, etc. It is a right for individuals and an obligation for the State in its double role: to establish the mechanisms to prove identity and to ensure its full exercise. With no identification there is no possibility of enforcing individuals' rights.

The acknowledgment of a human being's full legal capacity is a necessary condition for the effective exercise of his or her economic, cultural, social, and political rights, among others. The Argentine Republic considers that the identification and documentation of all physical persons is strategic. To that effect, our country has passed a law that regulates individuals identification, Law No. 17.671. This regulation assigns an institution of the national public administration, with a federal scope, the function of identifying, enrolling and issuing the national identity document to all the inhabitants of our country and the Argentineans who live abroad. (CASAL; 2010)

Such function is assigned to the Citizen National Register, an institution that depends from the National Ministry of the Interior. Identification of all the visible existence individuals who are domiciled in the country, or in an Argentine jurisdiction and of all the Argentineans wherever they are domiciled (art. 1st. Law 17.671), are part of its functions. In its articles, the Law regulates the competences of the Register, previous created by Law No. 13.482.

This Law No. 17.671, passed in 1968 and called the Identification, Enrolment and Classification of the National Human Potential Law, also creates the National Identity Document, only valid document for individuals' identification in all the extension of the national territory. It assigns the Register the "exclusive" authority of issuing the National Identity Document (article 11).

This National Identity Document is the only document proof of individuals' identity in

Argentina, and it is also legal to travel to border countries. We can thus see that in Argentina there is a law that regulates the individuals' identification procedure, assigns that competence to an institution of the federal administration, creates the national identity document, provides for the use of biometric technologies in that process and rules that such document will be the only valid means to prove physical individuals' identity. In effect, the Law rules:

"Article 13: The submission of the national identity document issued by the Citizen National Register shall be mandatory in all circumstances where it is necessary to prove the identity of the individuals comprised in this law, and which cannot be replaced by any other identity document whatever its nature and origin."

The above-mentioned law regulates the procedure by which the Register will perform the individuals' identification function, providing for the following actions that are its responsibility:

"Article 2º... a) enrolment and identification of the individuals comprised in article 1, through the registration of their most relevant antecedents from birth, and along the different stages of their life, what shall be kept permanently updated;

b) classification and processing of all information related to that human potential, in order to satisfy the following requirements:

To provide the Federal Government with the necessary databases so that it can establish, with the intervention of specially technical services, the most appropriate demographic policy for the National interest.

To make available the necessary judging elements for the State organizations and private entities requesting them to carry out an appropriate administration of the human potential, facilitating the active participation en the National defence and development plans.

c) the issuance of national identity documents, on an exclusive basis, as well as all the other reports, certificates or testimonies provided for in this law, based on finger-print identification "

This law also established the creation of an "Identification File", which on its article 7 provides for the use of biometric technologies applied to the process of individuals identification, what has been considered a highly innovative issue since the law was sanctioned, and it has been kept updated until the present. (CASAL; 2010) In effect, this article reads:

“The individuals comprised in the article 1 shall be enrolled in the Citizen National Register, who shall be assigned an identification file containing a fixed, exclusive and unchangeable number, that shall be modified only if there is a duly checked mistake. That file shall be constituted at the moment of birth and all the personal antecedents of greater relevance related to that individual's activity in the different stages of life shall be added. Every identified individual has the right to demand that the file shall contain antecedents, merits and tittles considered favourable for him or her.

The information on the identification file shall precisely prove its content. In the headquarters of the Citizen National Register there shall be at least patronymic files in line with the Argentine

Vucetich system or any other that technical evolution may recommend in the future.”.

As in almost all the legislation that provides for the enrolment and issuance of a document to physical persons, the Argentine law established the constitution of a personal file containing individuals' patronymic data – their transcendental biographical data -, the individual's physical identification by means of the 10-fingerprint registration and the assignment of a “fixed, exclusive and immutable” number according to the wording of the Law. (CASAL; 2010)

The use of digital technologies for the identification of Argentine citizens and foreigners, as well as the issue of the National Identity Document is authorized by Decree No. 1501/2009, regulating Law No. 17.671. This Decree rules that the New National Identity Document will be issued in two formats: booklet and card. It gives the Citizen National Register, depending from the Ministry of the Interior, the function of establishing the design, characteristics and details of the new ID, both in its booklet and card format, with its nomenclature, description and security and inviolability features.

On the other hand, Resolution No. 1800/2009, regulating the Decree mentioned ut supra, established the confidential nature of the contents referred to the security aspects and features of the ID, which are exclusively reserved to the authorities with the power of conducting an expert's audit, in order to keep verification and validation of them by the competent authorities under maximum security conditions.

Consequently, the new ID contains patronymic data, fingerprints and photos, and a 2D barcode that incorporates the biographical and biometric data of the document's owner. This new regulation gives the Citizen National Register the authority to digitize the procedure and to modernize documentation, as the substantial stage previous to the issue of the electronic ID.

The 1968 Law, as set at the end of its article 7, has provided for the technical evolution for the treatment of fingerprint data in individuals' identification, more precisely in the processes conducted by the Citizen National Register (ReNaPer).

Therefore, the enrolment process and further comparison of fingerprints, as established in the law, can be validly performed manually by a fingerprint expert, or through the use of an automated system known as AFIS (Automatic Fingerprint Identification System). (CASAL; 2010)

In Argentina, then, we have a specific legal framework that regulates the individuals' identification process, and assigns this function to an institution with federal scope - Citizen National Register, and provides for the use of biometric technologies. The identification of visible existence individuals in the Argentine Republic is legally supported on the use of biometrics technologies.

Protection of the right to identity

The Argentine Legal System recognizes the right to identity and, consequently, it is the State's obligation to identify individuals. This issue is ruled by Law No. 24.540, that establishes the newborn identification regime, its amendment, No. 24.884 and Law No. 26.061 referred to the

total protection of children and adolescents, set in force by Decree No. 415/06.

The right to identity is expressly recognized by Law No. 26.061. In its article 11, the law covers the concept of identity, the right to have a name, to the language of origin, to know who the biological parents are (except for the cases of full adoption in the terms of articles 327 and 328 of the Civil Code), to the culture of the place of origin and to preserve individuals' identity and idiosyncrasy.

ARTICLE 11. — THE RIGHT TO IDENTITY. Children and adolescents have the right to have a name, a nationality, their language of origin, to know who their biological parents are, to the preservation of their parental relationships in compliance with the law, to the culture of their place of origin and to preserve their identity and idiosyncrasy, except for the cases foreseen in the articles 327 and 328 of the Civil Code.

This right to identity has a close relationship with the obligation that the same law puts under the State responsibility in the following article, which establishes the guarantee of identification and enrolment in the Register of Marital Status and Capacity of Individuals. This law incorporates the guarantee of newborns identification by the State. The law states that identification procedures shall be:

- Simple
- Quick
- Free
- Mandatory
- In time
- Immediate

Likewise, the law defines that such newborn identification process shall necessarily establish the parental relationship with his or her mother, as set forth by Law No. 24.540. In this sense, the Law foresees that if the parents do not have the documents proof of their own identity, the state agencies shall take the necessary measures to obtain the mandatory identification. The Law establishes free registration for those adolescents and mothers who have not been timely registered, by the Register of Marital Status and Capacity of Individuals (article 12).

ARTICLE 12. — STATE GUARANTEE OF IDENTIFICATION. REGISTRATION IN THE REGISTER OF MARITAL STATUS AND CAPACITY OF INDIVIDUALS. State agencies shall guarantee simple and quick procedures so that newborns are identified freely, obligatorily and immediately after they are born, establishing the parental relationship with their mother, as provided for in Law No. 24.540.

Should there be no document proving the father's or mother's identity, the State agencies shall take the necessary measures to obtain the mandatory identification referred to in the above paragraph, what shall be specially considered by the regulations of this law.

The adoption of the specific measures for the free registration of all those adolescents and

mothers who have not been timely registered in the Register of Marital Status and Capacity of Individuals shall be facilitated.

This article is regulated by Decree No. 415/06, that provides for the situation where the father is unknown. In this case, the Law foresees the intervention of the Civil Register officers to orient the mother in this situation, as per the following procedure:

ARTICLE 12: In all cases where a child is registered with an unknown father, the officer of the Civil Register shall hold a private interview with the mother where she will be informed that it is a human right that a minor knows his or her identity; that, declaring who the father is, will allow the child to exercise the right to receive an alimony, and that this declaration shall not hinder the mother to exercise the right to keep the custody and control and to provide protection. To these effects, the documentation in which the child's human rights are stated shall be delivered to his or her mother, and the intervening officer, in turn, shall be able to require the collaboration by the corresponding local administrative authority so that specialized personnel complete information and give advise. Likewise, that party shall be informed, that in case she keeps the registration with an unknown father, the procedure will be as provided for in the article 255 of the Civil Code.

The Civil Code in its article 255 instructs the Civil Register to report the Office Responsible for Defending Minors about all the cases of minors registered as children with an unknown father, so that this instance can foster the necessary actions to determine paternity and further recognition of the child by the alleged father, being able to start the corresponding legal action if there were an expressed authorization by the mother.

Civil Code, Art. 255. In all cases where a minor is registered as a son or daughter of an unknown father, the Civil Register shall report this to the Office Responsible for Defending Minors, which shall try to determine the paternity and the recognition of the child by the alleged father. Failing this, it shall be able to promote the corresponding legal action if there is an expressed conformity by the mother to do so.

Following the procedures established by the regulatory Decree No. 415/06 of Law No. 26.061, the situation where any of the parents of the baby to be born has no identity document is foreseen. In this situation, the rules foresees that on the occasion of the prenatal medical checks or when the mother is hospitalized to deliver the baby, the authorities of such medical centre shall report the competent agencies about the referred situation of lack of identity documents so that the document can be issued. If this is impossible, the rule foresees that in the situation in which at the moment of delivery the parents have not obtained their identity document, the authorities of the medical centre shall state in the Birth Certificate the first name, last name, date of birth, domicile, age, fingerprints and nationality of the father or mother lacking the identity document.

The rule foresees the application of Law No. 24.540 in relation to the identification of newborns. Moreover, the Law favours the setting up of Civil Register offices in all maternity hospitals in order to facilitate the identification of newborns and of their parents lacking identity

documents.

On the other hand, Law No. 26.061 establishes the right to have identity papers in its article 13. It expressly recognizes the right to obtain public documents to prove the identity of all children, adolescents and mothers lacking identity documents, in line with provisions of Law No. 24.540.

ARTICLE 13. — RIGTH TO OBTAIN AN IDENTITY DOCUMENT. Children, adolescents and mothers lacking identity documents, have the right to obtain public documents to prove their identity, in line with current regulation in the terms set forth in the procedures foreseen in Law No. 24.540.

Decree No. 415/06 regulating the above mentioned Law, establishes that the national identity documents shall be free for every child and adolescent born in the national territory, i.e., until they are 18 years old.

ARTICLE 13: It is declared that the issuance of the first National Identity Document shall be free for every child and adolescent born in the national territory.

Newborns identification procedure

The procedures for newborns identification are established by Law No. 24.540, applied to all babies born in the national territory, alive or dead, and their mother. In the cases when the delivery is in a medical centre, the article 2 establishes that during labour the mother shall be identified, and after delivery and before cutting the umbilical cord the newborn has to be identified, in line with the procedures foreseen in article 6.

The Law provides for anomalous situations such as a premature or malformed baby which make the capture of foot and finger prints not possible. It establishes that the Citizen National Register, responsible agency in the issue of individuals' identification in our country, shall be the application authority. (CASAL; 2010)

In its article 6, Law No. 26.061 establishes the procedure to follow for the identification of the newborn and the relationship with his or her mother.

ARTICLE 6 — Identification shall be performed on a unique file, numbered by the Citizen National Register, in three copies, containing the following data:

- About the Mother: first and last name, national identity document type and number and 10-fingerprint.
- About the Child: name under which the newborn shall be registered, sex, right palm and foot prints and classification of both.
- If the baby was born alive.
- First and last name and signature of the intervening identifier.
- First and last name and signature of the intervening doctor or professional who assisted in

delivery.

- Date, time and place of birth and the filling out of the card.
- Fingerprints taken at the moment of being discharged from hospital.
- Information about the hospital or medical care institution: name and domicile.
- Remarks

The Law establishes an identification procedure for the mother-baby binomial, which is supported on the collection of biometric data at the moment of delivery, both of the mother and the baby. These biometrical data shall afterwards guarantee the identity of the newborn and later of the individual in adulthood.

In the Autonomous City of Buenos Aires, in 2003 Law No. 1226 was promulgated, which creates the Identification System of the Newborn and His or Her Mother, of mandatory characteristic, that has the goal of guaranteeing individuals their legitimate right to identity as well as the indemnity of the mother parental relationship.

The identification system provided for in Law No. 1226 has the goal of guaranteeing the indemnity and integrity of the mother-baby binomial, for which it establishes the identification of any baby born alive or dead and his or her mother. Moreover, the Law establishes the capturing and filing of the blood genetic prints corresponding to both, mother and baby, with the goal of guaranteeing newborns' right to identity.

The above-mentioned Law foresees the identification process of both, mother and baby, considering for this purpose the capturing of genetic blood prints corresponding to the newborn and his or her mother so as to guarantee the newborn's right to identity.

The Law of the City of Buenos Aires does not include the capturing of the mother and baby fingerprints, reason why there emerges the question of which the correct procedure is, as Law No. 26.061 is of national scope. A possible answer is that the City of Buenos Aires law is complementary to the national law, thus, the mother-baby binomial identification process in the City of Buenos Aires shall necessarily provide for the capturing of the genetic blood prints foreseen in Law No. 1226, and additionally, the data required in Law No. 26.061, that is, biographical data, name, domicile and 10-fingerprints of mother and footprint of newborn. (CASAL; 2010)

This interpretation is strengthened by the article 16 of above Law of the City of Buenos Aires, which expressly foresees that this Law is complementary to the National Law No. 24.540, predecessor of Law No. 26.061.

In the province of Formosa rules Law No. 1129 that foresees the newborn's identification system, within the framework of children rights, one of which is the preservation of their identity. The Ministry of Human Development has implemented a system that consists of the identification of the newborn through fingerprints – also those of the mother – and foot print of the baby

apart from a unique code, with the purpose of assuring the mother-baby binomial to avoid changes or confusions.

The system foresees two identification instances: One is before cutting the baby's umbilical cord, when the paediatrician requires it, and the second moment is before the mother is discharged from hospital together with her baby. The system is to use a card, on which back the identifier will write the mother's personal data and the thumb fingerprint of the mother, the right palm print and the right foot print of the baby will be taken. Two identical copies of the card are filled out with all the information required; one is kept at the hospital and the other is forwarded to the Civil Register.

Use of biometrics technologies in the identification process

Although this book has dealt with biometrics, explaining its definition and scope, we recall a definition given in previous papers, understanding by biometrics all those human beings' identification and authentication methods through their physiological and behavioural traits. Individuality is what makes one element different from all the similar elements of the same specie; and to determine individuality it is necessary to compare, placing one element by the other to be able to observe similitude and differences between both. (CASAL; 2010).

El Social e-ID Framework provides a definition of biometrics technology, understanding as such *"the biometric acknowledgement of the automated methods that ensure individuals recognition based on distinguishable physical or behavioural traits. Technologies used in biometrics include recognition of fingerprints, face, veins patterns, iris, voice and typing rhythm, among others."*

The above-mentioned Ibero American Framework includes in its glossary the definition of a biometrics system as *"the computerized recognition system based on one or various patterns that operates requiring biometric data to an individual, collecting a pattern of the data acquired and comparing the sample against a previously registered template. Depending on the application, this template can be stored in a centralized database or in an individual device as a token or smart card."*

There are two types of identities, the absolute identity and the practical identity; the latter is the one that is determined demonstrating sufficient similitude and is in fact the relevant one at the time of dealing with biometric systems.

Therefore, identity is the set of characteristics that individualize a person: name, age, nationality, civil status, profession, personal marks, fingerprints, etc. (SILVEYRA; 2006)

Recently, the word biometrics has been identified with the automated methods that analyze determined human characteristics in order to identify and authenticate individuals (SIGÜENZA PIZARRO Y TAPIADOR MATEOS; 2005)

Biometrics allows recognizing an individual's physical or behavioural traits. At present, there are different types of possible recognition through: fingerprints, iris, palm, DNA, veins, handwriting, and typing rhythm, among others. In the last five years, biometrics technologies have shown

considerable progress, providing a multiplicity of solutions today, that governments can use for individuals' identification. These biometric data are the basis for the development and implementation of different public policies related to: security, e-government, border traffic and also to set up social policies.

Every social policy requires the individual's identification as a basic element. It is the individual's right and the State's obligation. For this reason the decision made by governments on this issue will have a direct impact on other public policies to be implemented. This consideration should be present at the time of elaborating biometric databases projects, as these will be the basis on which other policies will be efficiently built: social inclusion, the fight against crime and e-government, among others.

Another core element is the interoperability among biometric databases. It has little value to have these data available if they cannot be shared. In this sense, the Social e-ID Framework is an important progress for the future development of interoperability standards referred to biometrics technologies, as to facilitate the interchange of information among the administrations or agencies of the nations in our region.

b. Individuals' identification in virtual environments

Argentina has a complete legal framework with relation to the validity of electronic transactions. Law No. 25.506 of digital signature acknowledges "the use of electronic signature and digital signature and its legal efficacy under de conditions established" by such law. (Article 19)

The digital signature Law No. 25.506, which has as an antecedent the already mentioned Decree 427 of April 1998, is the legal framework that grants legal validity to a digital document, an electronic signature and a digital signature. In its first chapter it contains a series of provisions aimed at eliminating present obstacles in the traditional civil and commercial law to recognize the validity of legal acts. In line with the UNCITRAL model laws on e-commerce and e-signature, the Argentine law contains a series of provisions that, based on the concept of functional equivalent, grant legal value to the transactions performed on a support different from paper. (BUGONI, FERNANDEZ, RIVOLTA; 2010).

The main obstacles were represented by: a) the document had to be paper-based, b) the document had to be signed, and c) the document had to be an original and there were restrictions on the way the document had to be kept. (RIVOLTA; 2008)

Argentina has a full legal framework supporting electronic transactions: Law No. 25.506 (Official Bulletin 14/12/2001), el Decree No. 2628/02 (Official Bulletin. 20/12/2002), el Decree No. 724/06 amending Decree N° 2628/02 (Official Bulletin. 13/06/06) y the Administrative Decision of the Chief of the Cabinet's Office No. 6/07 (Official Bulletin 12-02-07).

The Digital Signature Law No. 25.506 acknowledges the legal value of the electronic document, the electronic signature and the digital signature in all the national territory. It is a law that complements the provisions of the Civil Code in order to facilitate the use of digital means to perform transactions, both between particular individuals and by the National Administration/

Agencies. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Law N° 25.506 incorporates the concept of digital document, giving it the same status as a traditional paper-based document, making clear that the electronic document complies with the requirement that it has to be written, included in the traditional codes. The Law reads:

ARTICLE 6 — Digital document. A digital document is the digital representation of acts or facts, independently from the support used to fix it, keeping or filing. A digital document also complies with the writing requirements.

With respect to the signature, Law No. 25.506 incorporates two concepts: electronic signature and digital signature. (MASON, 2006:148). Both types of signatures are valid, in compliance with the article 1 of the Law. More precisely, there is a wide range of alternatives for an e-signature, from a simple e-mail, the use of shared public key technologies (PGP), or the use of key words based on symmetric cryptography, to the use of a public key technology based on digital certificates issued by a certification entity that is not licensed by a public authority. A digital signature that uses asymmetric cryptography and public key technology can be considered as an e-signature, the same as a mere inclusion of the name as part of the text in an e-mail, as long as the signer has executed or adopted the symbol with the intention of signing. This means a declaration of the signer's will with respect to the content of the message. (SCHAPPER, 2004)

The difference between an electronic signature and a digital signature from the legal point of view is the burden of proof of its validity. In its Article 5, the Law defines an electronic signature as "*the set of electronic data integrated, connected or associated in a logic manner to other electronic data, used by the signatory as a means of identification that lacks any of the legal requisites to be considered a digital signature. If the electronic signature is not acknowledged, the individual invoking it has to prove its validity.*"

A digital signature is the signature based on digital certificates issued by a certification authority licensed by the Authority of Application of the law. The article 2 defines a digital signature as the "*result of applying a mathematical procedure to a digital document that requires information of exclusive knowledge of the signer, and that has to be under the signer's absolute control. The digital signature has to enable verification by third parties, under the condition that such verification-audit allows identification of the signer and detection whether there was any alteration of the digital document after signed. The signature and verification procedures to be used to that effect shall be determined by the application authority in line with current international technological standards.*"

The Law gives the digital signature a higher value of evidence compared to the electronic signature. It assigns two *juris tantum* presumptions (rebuttable presumption), i.e., they admit rebutting proof. In effect, the article 7 states that a digitally signed document bears the presumption of authorship with respect to the individual who owns the digital certificate. In turn, article 8 establishes the presumption of integrity of the digitally signed electronic document, i.e., that presumes that such document has not been altered. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Nevertheless, it has to be highlighted that the digital signature on a document does not hinder its modification. It simply assures that, if the digitally signed electronic document suffers any alteration, this fact remains evident. For this reason legislators assign it a presumption of integrity. (RIVOLTA; 2008)

Apart from that, an electronic document has to comply with the provisions of the Law about the quality of being an “original” - article 11 - and about the conservation of digital documents - article 12. It contains provisions relative to the consideration of original and to the written aspect stressing that an electronic document complies with those requirements as long as it is accessible for a latter check. (RIVOLTA; 2010)

The system established by Law No. N° 25.506 is based on a Digital Signature Infrastructure scheme which considers a digital signature only the one that has been produced through the use of public key certificates issued by certifiers previously licensed by the Application Authority, the Chief of the Cabinet's Office.

Nevertheless, the Law provides for the case where the certificates have been issued by foreign certification authorities. Such situation is established in the article 16, admitting its validity under certain conditions. In effect, with respect to the validity of certificates issued by foreign certification authorities, the Law reads:

Article 16: Acknowledgment of foreign certificates. Digital certificates issued by foreign certification authorities shall be acknowledged under the same terms and conditions demanded by the law and its regulations when:

- a) They comply with the conditions established in the present law and its corresponding regulations for certificates issued by national certification authorities and there is a valid reciprocity agreement signed by the Argentine Republic and the certification authority of the country of origin, or
- b) Such certificates are acknowledged by a licensed certification authority in the country, which shall ensure its validity and effect in compliance with the present Law. In order to have effects, this acknowledgement shall be validated by the application authority.

The Law No. 25.506 establishes a Public Key Infrastructure scheme, constituting a system based on asymmetric cryptography, with a public entity that grants the license and authorises the operation of the certification authorities that issue the digital signature certificates and which elements are described in the following chapters, specifically referred to the components of the Digital Signature Infrastructure: digital certificates, licensed certification authorities, holders of certificates, institutional organization, authorities, audit system, responsibility, sanctions regimes,

Given the limitations in the extension of this article, only the main concepts established in the law will be dealt with.

Digital Signature Infrastructure

A Digital Signature Infrastructure, or PKI (Public Key Infrastructure) is a “combination of technology (hardware and software), processes (policies, practices and procedures) and legal components (agreements) that associate the identity of the holder of a private key with its corresponding public key, using asymmetric cryptography technology” The use of a PKI in digital environments can be varied: to protect confidentiality (through the encryption of communications or stored data), to authenticate the identity of an individual or an organization, to report on the integrity of an electronic message or document, and to guarantee the non repudiation of electronic messages or transactions . (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Components of the Digital signature Infrastructure

Public key Technologies cannot guarantee by themselves the identification of individuals in the real world, either the identification of physical individuals, public and private organizations or attributes of entities of any type, such as servers.

For this purpose, other additional actions have to be adopted, besides the public key technology. When speaking of Public Key Infrastructures (synonym of Digital Signature Infrastructure), reference is made to this set of elements that comprise the pairs of keys associated to an identification in the real world. It also comprises the mechanisms to generate the pairs of keys, the security measures to store the private key, and in this sense it is worth mentioning the devices for generating and storing the private key, as well as the mechanisms to secure the private key, that can be from a simple password, a passphrase, or based on biometrics (for example, fingerprints). (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010).

A distinctive characteristic of a PKI is that the receiver of the message has to have access to the public key of the individual who sends it. Thus it is how the digital certificate concept appears, as well as the need to have directories where such digital certificates are published, and that have to be accessible for public consultation.

In order to satisfy the requirements stated in the above paragraph, a PKI involves the following elements:

- Standards and protocols;
- Software to implement a large number of functions and protocols;
- Private keys protection;
- A public keys repository, its creation, maintenance and use;
- The elements to allow certification entities to digitally sign certificates;
- A legal framework to regulate and support the infrastructure and its operation and
- Services to support the operation of applications that use digital signature.

Summarizing, a public key infrastructure includes:

- A Certification Authority (CA – English acronym), also known as Certification Organization or

Certifier, according to different legislation. The CA issues and guarantees the authenticity of Digital Certificates. A Digital Certificate includes the public key or other information related to the public key.

- A Registration Authority (RA – English acronym) – validates Digital Certificates requirements. The RA authorizes the issue of the public key certificate to the requiring individual by the Certification Authority.
- A certificate management system – a software application provided the PKI vendor.
- A directory where certificates and their public key are stored.
- A Digital Certificate includes the name of the signer and his/her public key, the digital signature of the Certification Authority that issues the certificate, a series number and the expiration date.
- Subscribers: the individuals or entities mentioned or identified on the public key certificates, the holders of private keys corresponding to the public keys of the digital certificates.
- Users: the individuals who validate the integrity and authenticity of a digital document or data message, based on the signatory digital certificate. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Definition of a digital signature

We are now going to analyze the process of digitally signing an electronic document. In line with Argentine Law, the process to digitally sign an electronic document has two stages:

- A first step when the subscriber/holder of a digital certificate digitally signs an electronic document
- A second step when a third party, the receiver of that digitally signed electronic document checks for the message authorship and integrity.

Digital signatures are an important application of this public key technology. In effect, the individual who sends a message uses his/her private key to encrypt the secure message digest (obtained through the calculation of the message hash function). That individual sends the encrypted digest and its digital certificate which has the public key. El receiver decrypts the digest using the sender's public key, which matches the private key of it. The receiver of the message checks the digital signature of that message, for which recalculates its hash function, and if both match checks that the message has not been tampered with, process through which the receiver has certainty of its integrity. If the receiver could decrypt the digest by means of the public key corresponding to the sender of the message, the receiver checks the authorship of the digitally signed electronic document. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Technological Standards

The same as in other environments, public key technologies are supported on standards. As public key initiatives and infrastructures increase in number, modifications to the standards initially used have to be implemented to enlarge their functionality or to make them more

specific and with a clearer semantic content. (BUGONI, RIVOLTA; 2007), (RIVOLTA; 2008), (RIVOLTA; 2010)

Standards are referred to the following components, among many other:

- Standards for encryption algorithms and hash algorithms.
- Protocols for parameters associated to the encryption algorithms and hash algorithms.
- Protocols to facilitate the access of users to public keys.
- Protocols to facilitate the access of users to revocation reports
- Standards for secure generation of pairs of keys
- Standards and protocols to support synchronization and time stamping mechanism with probative value
- Standards for the following software and applications:
 - Generation of pairs of keys
 - Storage of private keys
 - Storage of public keys
 - Users' access to public keys
 - Generation of secure message digest
 - Message encryption
 - Message creation
 - Request of public keys
 - Verification of public keys: their validity, their expiring term, if not having been revoked
 - Message decryption
 - Secure digest decryption
 - Comparison of decrypted digests
 - Time
 - Private keys protection
 - Against intrusions when they are stored
 - Against intrusions when they are in the main memory
 - Against non-authorized invocations
- Of Directory if it is used as a public keys Repository:
 - Protocols to insert data and keep data in the repository
 - Protocols to access to repository data
- Of the Certification Authority certificates:
 - Standards for certificate formats
 - Profiles for the application of Standards in particular contexts
- Protocols for the communication of certificates to the parties that may need them
- Means through which message receivers are able to evaluate whether they check the certificate digital signature
- Means through which message receivers can check the certificate digital signature
- Means through which message receivers can evaluate the extension of the statements contained in the certificate
- If certificates are signed by Certification Authorities

- Standards for Certification Authorities
- Standards and procedures for registration and audit of Certification Authorities
- Procedures to appeal against the Certification Authority
- Insurances to be underwritten by the Certification Authorities

If the legal framework links a pair of keys with something from the real world as part of a PKI, further than the computer-based application level (as it is the case in Argentina and most of the Latin-American legislation), the PKI shall contain the means to establish the association of the pair of keys with a device, physical person, juridical person, attribute, public agency or location. (RIVOLTA, SCHAPPER; 2004)

III. Framework For The Ibero American Social Electronic Identification

Since the explosive development of ICT, the main objective of legislation on electronic commerce or electronic signature has been to remove the obstacles to use the domestic traditional legislation in every country for the new applications based on electronic transactions. To this effect, countries have developed specific legislation that provides new alternatives to handwritten signatures, based on the Model Law of Uncitral on E-Commerce (1996) and on Electronic Signature (2001), on the Directive 99/93 of the European Union, on the Law of Electronic Signature, of the U.S.A. known as E-Sign, or on a combination of them. (RIVOLTA, SCHAPPER; 2004), (UNCITRAL; 2009).

The countries of the region have developed specific legislation on electronic commerce or electronic signatures. The approaches adopted are based on the particular legal system of each country involved. In those countries which legal systems belong to the common law, in which legislation is more open, it has often been necessary to acknowledge the non repudiation of an electronic document (electronic record) or of an electronic signature (as ruled by the Electronic Signature Law of the United States of America - E-Sign). In those countries with codified civil law regimes, the legislation developed for electronic signatures or electronic commerce is very prescriptive, with emphasis on technical and operational rules and on the acts formalities, specifically those based on digital signatures. (RIVOLTA, SCHAPPER; 2004).

Nevertheless, in spite of the big progress attained on this issue, national legislations do not cross borders, for which thinking of a scenario of international and regional transactions generated the need to build minimum consensus to facilitate agreements focused on establishing standards of transnational scope.

The goal of the Social e-ID Framework is to establish a set of concepts, fundaments, principles, orientations for the design, implementation and development of a Social Ibero American Electronic Identification to consolidate the acknowledgement and effective full possession of the social rights of Ibero American citizens in the region.

a.- Social electronic identification and electronic authentication

The Social e-ID Framework makes a distinction between the following concepts which are defined as:

1. “Social Electronic Identification”: understanding as such the *“procedure by means of which external elements enable assigning an identity with determined attributes to a concrete individual, i.e., it is the verification of the data that prove that an individual is effectively the person he/she claims to be, an individual subject of law, with determined attributes.”*
2. “Electronic Authentication”: understanding as such the *“process to verify the authenticity of the identifications performed or required by an individual, either a physical person or a legal entity, or about information such as a message or other means of electronic transmission. The authentication process is the second of two steps that involve: 1) The submission of a means to prove the identification before a system and, 2) The presentation or generation of information that corroborates the binding between the means submitted and the individual or entity identified.”*

In this sense, the Social e-ID Framework in its text defines two concepts that usually appear dissociated. In effect, *“social electronic identification”* refers to the procedure of binding the attributes of an individual and the individual him/herself, and also the process of verifying that information with the concrete individual. It mentions two moments, that would be comprised in the social electronic identification concept. A first moment in which the authority certifies the identity of an individual, after being bound to determined attributes (name, place of birth, family information, biometric data) with the physical individual him/herself, through an established procedure. And a second moment in which somebody verifies the correlation of such data with that individual.

This procedure shall be based on elements that are external to the individual, which shall appear on an official document that will prove such identity thereafter. This document shall contain these data in a manner that allows the identification process by third parties.

The *“electronic authentication”* concept is innovative. It is the first time it appears on documents related to identification. This concept makes reference to a third moment: verification of the authenticity of the identifications made or requested by a physical person or legal entity, about information such as a data message or other means of electronic identification. This concept introduces some innovative elements that we would like to highlight.

On the one hand, it is applied to physical individuals as well as legal identities, i.e., to automated electronic devices as servers, computer systems, etc. that interact between each other or with particular individuals. Thus, the value of the action performed by a computer system is included, even with no direct human activity. This element is already in the Argentine digital signature Law, which in its article 10 acknowledges the presumption of the sender. This law established that it is presumed, except if it is otherwise proved, and that the document digitally signed comes from the sender, in those cases where this digital document has been automatically sent by a programmed device and bears the digital signature of the sender.

On the other hand, the “electronic authentication” concept that refers to the authenticity verification process of the identifications performed by means of data messages or other electronic transmission means; it is a concept that fully respects the principle of technological neutrality that has to prevail in every rule. In effect, considering that technology evolution time is extremely fast, while the normative elaboration processes are long by definition, as they require complex consensus, an appropriate normative technique indicates the benefit of having neutral technological regulations, i.e., that are not defined by one technology or another, as they will surely turn obsolete in the short term. In the cases where the laws adopt a technological solution, they are no longer part of the solution but become part of the problem. (SCHAPPER, RIVOLTA, VEIGA MALTA; 2006)

The electronic authentication concept contained in the Social e-ID Framework is technologically neutral. When it refers to “other means of electronic transmission” it provides for the possibility of including any other means different from paper-based physical support, without establishing a particular technology.

In this sense, the Social e-ID Framework accepts as forms of electronic authentication what is known as e-signatures, digital signatures, biometrics technology and any other electronic mechanism to prove an identity. This initiative is innovative in that it correctly defines the functions: on the one hand, identification that includes technological elements such as biometrics; and on the other hand, the electronic authentication process that accepts any type of electronic procedures.

This vision is better than the current one. In effect, the current legal Framework, derived from the e-commerce, e-signature and digital signature laws, has stressed the function of signing the documents. Not disregarding that they are a very important progress for e-commerce and e-government development, the e-signature and digital signature laws are referred to two different situations. On the one hand, the electronic substitute of the handwritten signature, as an expression of consent by the individual when executing a legal act; and in the other hand, the process of being identified by a computer system.

We can see an example in the case of e-invoices. A paper-based invoice does not require the signature of the vendor who issues it. Nevertheless, some initiatives of e-invoice included digital signature. This means that more formalities were required to the digital solution than the traditional method.

El Social e-ID Framework, in a correct manner from our judgement, defines de instance of electronic authentication independently from the concepts of e-signature and digital signature defined in the glossary, as it is about different institutes. As an example, when I go into a Civil Register to get married, I do not need to submit any credentials, but at the moment of signing the marriage act, my handwritten signature expresses my consent.

The Social e-ID Framework is inspired in the UNCITRAL Convention on Electronic Communications in International agreements, that provides for the functional equivalent concept, accepting the use of varied electronic authentication techniques. As regards the legal

reasons, it is possible to assert that the evolution of law has exceeded the initial vision tending to accept only digital signatures. (UNCITRAL; 2007)

In this sense, the legal scenario is sufficiently wide as to validate any electronic authentication method that is agreed upon between the parties or which procedures has any type of procedural framework. Therefore, symmetric keys, biometrics technologies, digital signatures issued by not licensed certification authorities are accepted, all them with the same legal value as an electronic signature susceptible to satisfy the legal requirement of a “signature” as an expression of the individual’s consent.

b.-Authentication factors

The Social e-ID Framework contains a glossary of terms that are the starting point for establishing agreements among our countries.

It defines the authentication factors as those “*elements that comprise the identification process*”, namely:

- Something that I know: the individual is authenticated by means of something that he or she knows: a key, an identification number– PIN, a phrase or an answer to a security question.
- Something that I have: the person is authenticated using something that he or she has: a token, a smart card, a digital certificate.
- Something that I am: the individual is authenticated based on an own characteristic, i.e., biometric data.

The glossary also defines the biometrics technology, concept as those “*methods that ensure individuals recognition based on distinguishable physical or behavioural traits. Technologies used in biometrics include recognition of fingerprints, face, veins patterns, iris, voice and typing rhythm, among others.*” (MARCO; 2011)

As regards biometrics systems, the Social e-ID Framework, defines them as “*a computerized recognition system based on one or various patterns that operates requiring biometric data to an individual, collecting a pattern of the data acquired and comparing the sample against a previously registered template. Depending on the application, this template can be stored in a centralized database or in an individual device as a token or smart card.*” (MARCO; 2011)

Following these definitions the Social e-ID Framework defines the Public Key Infrastructures, also known as Digital Signature Infrastructures or PKI. They can be defined as “*the set of hardware, software, persons, policies and procedures necessary to create, manage, store, distribute and revoke public key certificates based on asymmetric cryptography, that facilitate the creation of a verifiable association between a public key and the identity of the possessor of the corresponding private key.*” (MARCO; 2011)

It follows making reference to digital signature, also called safe electronic signature, advanced electronic signature or acknowledged electronic signature. The Social e-ID Framework recognizes two aspects for a digital signature: the technological and the legal ones. The technological meaning is related to public key technologies. The legal one is related to the

definition that national laws have included as an equivalent of the handwritten signature. The Social e-ID Framework introduces this double aspect in order to overcome the issues that may arise due to different interpretations.

It expressly provides for two meanings of the digital signature concept:

From the technological point of view, a digital signature is the authentication mechanism that -supported on asymmetric cryptography, i.e. that it uses two keys, a private and a public one- allows identification of the signer and ensures the integrity of the content of the electronic document signed.

From the legal point of view, the laws require an administrative procedure. This means that to be considered a legal digital signature this mechanism needs to be applied through the use of a digital certificate issued by a certification entity approved by the governing body of the State in this subject matter.

But this concept of digital signature, what allows ensuring the authorship of an electronic document, should not be confused with identity verification in digital environments. The same as in the civil law, a signature is the expression of an individual's consent in a determined transaction, different from that individual's identification, which is performed through the inspection of that individual's identity document. In a digital environment, there is often confusion between the digital signature and the identification function of individuals in electronic environments. The identification function is assigned to the Citizen National Register as per national legislation.

In this sense, the possibility of developing national identity documents containing an electronic device with the owner's biometric data shall be a big progress for individuals' identification in digital environments. Until this can be implemented, we shall have to keep with the traditional electronic authentication systems.

Finally, the Glossary provides for the definition of "electronic signature". The Social e-ID Framework defines an electronic signature as "any sound, symbol or process, attached or logically bound to an electronic document that expresses an individual's consent, issued in digital format, and executed or adopted by such person with the purpose of signing the electronic document. In general, the laws give the name of "electronic signature" to any authentication mechanism that does not comply with any of the requirements demanded for a digital signature, that are going to be dealt with later. "Electronic signature" is the generic or neutral term to refer to the universe of technologies that any individual may use to express his or her consent about the content of a document." (MARCO; 2011)

c. Mutual acknowledgement agreements

The Social e-ID Framework, in its 3rd. Chapter, provides for the mutual acknowledgement agreements between signatory nations of the Declaration of Asunción. The Social e-ID Framework has set the objective of dealing with the aspects related to individuals' electronic identification in physical or virtual environments in order to set up the basis to develop future mutual acknowledgement agreements, which shall ensure a common environment for an Ibero

American Social Electronic Identification. (MARCO; 2011)

The Social e-ID Framework attempts to be a starting point to orient the discussions on legal and technical aspects necessary to sign agreements on data interchange, systems interoperability and development of common technological standards in the field of electronic identification, including biometrics technologies and digital signature certificates.

Conclusions

As we already said in a previous paper (CASAL; 2010), the issue of identification in digital environments has not been solved yet. On the contrary, due to the development of e-government transactional platforms, it is an aspect that has been started to be analyzed.

On the one hand, nations have traditional citizen identification systems that consist of identity documents and travel documents for border transit. On the other hand, electronic-information systems use different technological elements to authenticate individuals in such applications.

At present, as regards the e-government aspect, the trend is to use authentication mechanisms based on shared keys, and an incipient movement tends to use digital certificates, basically to identify safe web sites.

Moreover, since a few years ago, biometric identification systems emerged. Powerful technologies have been developed to recognize individuals through biometric data: iris, fingerprints, face, hand, veins, DNA, among others.

These biometrics technologies have been applied in various countries to issue identity documents, by including in such documents devices to store an individual's biometric information, i.e. data that would later enable the identity verification of that individual.

The use of biometrics is beneficial for governments as it facilitates the indubitable identification of individuals, and, if technological devices are included, it would allow enlarging the scope of e-government policies. But mostly, it is a necessary instrument to protect the identity of each of us. Being identity theft one of the commonest crimes of our times, nothing better than biometric identification to protect our right to identity. (CASAL; 2010)

The right to identity is an extremely personal right. We share with Bustamante Donas the concept that "There is no social justice without social inclusion, and on these days social inclusion cannot be understood without digital inclusion". The identity concept is intimately related to citizenship, understood as the capacity to interact with administrations through information networks and to access to the most complete and simplest to use services". (BUSTAMANTE DONAS; 2007)

The e-ID Framework for the first time introduces a distinction and a relationship. The distinction is connected with the clear definition of signature, identification and authentication. We say that for the first time it sets up a relationship as when introducing the electronic authentication concept, it establishes a connection between identification and electronic/digital signature.

The e-ID Framework for the first time allows a distinction between the concepts of signature, an element that represents an individual's consent by means of a legal act, and the idea of identification in electronic environments, contained in the electronic identification concept.

A signature is a means that the law acknowledges to bind a document to its author. In a wide sense, a signature is any method or symbol used by an individual with the purpose of binding him/herself or authenticating a document. (LORENZETTI; 2001). The techniques used to sign may be varied: from a handmade drawing on a piece of paper (handwritten signature), a manual signature contained in a stamp, the digitised handwritten signature, a shared key (for example in ATM's), a biometric identification or an asymmetric key recognized or not in a PKI scheme. But any of these techniques will be legally recognized as the individual's "signature" (RIVOLTA; 2010)

Our Civil Code, the foundation of the system of civil law in Argentina, established that the signature has to be a requisite to validate private and public instruments, as the expression of the individual's consent with the object of the legal act. The Code written by Vélez, dated in 1869, in its articles does not require that the signature be handwritten, except for the holographic testament. In effect, article 3639 establishes that:

Art. 3.639. The holographic testament to be valid as regards its forms has to be entirely written, dated and signed by the testator's own hand. The lack of any of these formalities annuls its entire content.

On the other hand, our Civil Code establishes that the forms and solemnities of legal acts shall be those established by law in the place of enforcement.

Art. 950. Respect to the forms and solemnity of the legal acts, their validity or nullity will be ruled by the laws and customs of the place where they are celebrated (article 12).

At the same time, the Code foresees the existence of public and private instruments. In every case, the signature constitutes an essential requisite. The absence of a signature turns the act null.

Art. 988. For a public instrument to be valid, it essentially requires that it be signed by all the interested parties that appear as part of it. If any or some of the solidary or merely joint co-interested parties shall not sign it, the act would have no value for all those who had signed it.

Art. 989. Public instruments are annulable when any of the parties that appeared to have signed on them, shall claim that they are completely, or in their principal part false, or if those instruments have amendments, words inserted between lines, erasures or alterations in their essential parts, such as date, names, quantities, amounts, objects, etc., not amended to that effect.

Art. 1.012. The signature of the parties is an essential condition for the existence of any act being private. The signature cannot be replaced by signs or by the initials of first and last names.

The Civil Code provides for the principle of freedom of forms for the legal acts celebrated by private instruments.

Art. 1.020. For the acts under private signature there is no special formality. The parties can write them in the language and solemnity they consider most convenient.

The Civil Code provides for the repudiation of the act, enabling the signer to repudiate the content of such, through the probation elements considered convenient, except for that from the witnesses.

Art. 1.017. El signatory nevertheless can object to the content of the act, proving that the declarations and obligations contained in it are not those that he/she intended to do or contract. This proof can be done with witnesses.

Summarizing, the introduction of the electronic authentication concept promoted by the el Social e-ID Framework enables to clear differentiate between an individual's identification process in a digital environment, and the act of signing a document. Signing a document, both on a paper-based or a digital document is the act of expressing an individual's consent with respect to granting a determined legal act.

Electronic authentication, on the other hand, is a previous stage, in which individuals appear themselves before a system and prove their identity. They do not express will, or consent with any legal act.

The Social e-ID Framework is a huge progress. It establishes a common matrix to start a dialogue to facilitate the mutual acknowledgement of electronic identifiers, and the route of a coherent path as regards individuals identification. Our countries are reporting progress in narrowing the digital divide through effective actions in the field of social inclusion.

Therefore there is a new scenario in which individuals' identification is a requisite that cannot be deferred to attain an effective execution of public policies related to inclusion. At the same time, the increase in ICT users is being accomplished thanks to digital inclusion educational programs and the extension of the access to electronic means faces us with the challenge of being prepared for an increase in digital services demand. This implies the deployment of quick and safe electronic authentication mechanisms.

It would be desirable that national standards and rules be inspired in this Ibero American Framework, as well as the agreements attained be in line with international schemes, i.e., be based on community sources or international treaties that set up minimum common criteria with a technologically neutral approach to endow them with the capacity of being current in spite of the ongoing technological progress (LORENZETTI, 2001), (RIVOLTA; 2008).

The Social e-ID Framework is a first step.

Bibliography

- BUSTAMANTE DONAS, J. (2007): "Los nuevos derechos humanos: gobierno electrónico e informática comunitaria", Link: Revista Venezolana de Información, Tecnología y Conocimiento – Mayo Agosto, 2007, volumen 4, número 002, Universidad de Zulia, Venezuela. Available on the internet at: <http://redalyc.uaemex.mx/redalyc/pdf/823/82340202.pdf>.
- BUGONI, M. y RIVOLTA, M. (2007): "e-autenticación. Firma Digital y Firma Electrónica. Panorama en la República Argentina", Observatorio de Políticas Públicas de la Jefatura de Gabinete de Ministros, Buenos Aires, September 2007.
- BUGONI, M.; RIVOLTA, M. y FERNANDEZ, J. (2010): "Políticas de Tecnologías de la Información y las Comunicaciones en la Gestión Pública", en "Políticas Públicas en Democracia", Secretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros de Argentina, Buenos Aires, 2010.
- CASAL, G. (2010): "Derecho a la identidad y biometría en la Argentina", Paper presented at the XV CLAD International Congress on the Reform of the State and the Public Administration, Santo Domingo, November 2010.
- CASAL, G. (2010): "Derecho a la identidad y biometría en la Argentina", en Biometrías. Herramientas para la Identidad y la Seguridad Pública, Jefatura de Gabinete de Ministros, Buenos Aires, 2010.
- CARTA IBEROAMERICANA DE GOBIERNO ELECTRONICO, CLAD, 2007. Available in Internet at: <http://www.clad.org/documentos/declaraciones/cartagobelec.pdf>.
- MARCO PARA LA IDENTIFICACION ELECTRONICA SOCIAL IBEROAMERICANA (2011), Available on the Internet at: <http://www.clad.org/documentos/otros-documentos/marco-para-la-identificacion-electronica-social-iberoamericana>
- MASON, S. (2006): "Electronic Signatures in Practice" Journal of High Technology Law, Volume 6, Number 2, 148 – 164. J. High Tech L. 148 Available on the Internet at: <http://www.jhtl.org/docs/pdf/Mason.pdf>.
- RIVOLTA, Mercedes y SCHAPPER, Paul (2004): "Autenticación & Firmas Digitales en E-Legislación y Seguridad. Guía para la regulación y el gerenciamiento de aplicaciones de comercio electrónico y de compras públicas electrónicas", Inter American Development Bank, 2004. Available on the Internet at <http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=645510>
- RIVOLTA, M., SCHAPPER, P. y VEIGA MALTA, J. (2006): "Risk and Law in Authentication", Digital Evidence Journal, Vol 3 number 1, London, UK, 2006.
- RIVOLTA, M. (2008): "Leyes de 3^a generación: hacia el pleno reconocimiento del derecho a la administración electrónica". Paper presented at the XIII CLAD Congreso for the Reform of the State and the Administration, Buenos Aires, November 2008.
- RIVOLTA, M. (2010): "Biometría y autenticación digital: firma electrónica segura o firma digital", en "Biometrías. Herramientas para la Identidad y la Seguridad Pública", Jefatura de Gabinete de Ministros, Buenos Aires, 2010.
- SILVEYRA, J. (2006): "Sistemas de Identificación Humana", Ediciones La Rocca, Buenos Aires 2006.
- SIGÜENZA PIZARRO Y TAPIADOR MATEOS (2005): "Tecnologías Biométricas aplicadas a la Seguridad", Alfaomega – Ra-Ma, México 2005.
- UNCITRAL (2001): "Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001", United Nations, Nueva York, 2002. Available on the Internet at: <http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf>.
- UNCITRAL (2007): "Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en Contratos Internacionales", Naciones Unidas, Nueva York, 2007. Available in Internet at

http://www.uncitral.org/pdf/spanish/texts/electcom/06-57455_Ebook.pdf

UNCITRAL (2009): "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firma electrónica", Naciones Unidas, Viena, 2009. Available in Internet at http://www.uncitral.org/pdf/spanish/publications/sales_publications/Promoting_confidenceS.pdf.

Annex

Framework for the ibero-american social electronic identification

Approved by the XIII Ibero American Conference
of Ministers of the Federal Administration
and Reform of the State

Asunción, Paraguay, June 30 - July 1, 2011

Content

I.	Executive Summary	497
II.	Antecedents	498
	Lisbon Declaration	498
	Sectorial Conferences Ministers	499
	Declaration of Mar del Plata	501
	Ibero-American charter on E- Government	502
III.	Elements for Electronic Identification	504
	Relevance of Electronic Identification for the Full Exercise of Rights	504
	Elements that Allow Identification	505
	Electronic Identity Document	506
	Towards and Interchange of Biometric Data	507
	Digital Signature Infrastructures	507
	UNCITRAL Regulations	507
	MERCOSUR Regulations	508
IV.	Challenges and Conclusions	509
V.	Framework for the Ibero-American Social Electronic Identification	510

I. Executive Summary

The present document has the goal of presenting the “FRAMEWORK FOR THE IBEROAMERICAN SOCIAL ELECTRONIC IDENTIFICATION”, as a necessary tool for the effective exercise of individuals’ rights in our region. It is in line with the recommendations made in 2010 Lisbon Declaration. Its initial presentation took place in the first meeting of the inter-governmental Work Team on e-government promoted by the past Ibero American Network of Ministers of the Presidency and Equivalent, held in Lisbon, Portugal, on September 9 and 10, 2010. This first Inter-governmental Work Team meeting took place on April 12 of this year, in Cartagena de Indias, Colombia.

Without identification there are no rights. The exercise of rights necessarily requires the full identification of individuals, a function that corresponds to the State. The State is responsible for individuals’ identification and for ensuring every individual’s identity. In an increasingly IT-based world, governments make use of ICTs for the implementation of substantive public policies. How to attain a full identification of individuals, how to recognize such identifications between countries,

how to facilitate remote access to the services rendered by the Public Administration, are issues related to a proper electronic identification of individuals.

This electronic identification is necessary for the access to IT-based systems, e-government and e-commerce applications, but also for the execution of social policies. In addition to this use, modern identity documents, basically passports and national documents, are using electronic identification means, what demands considering that even in the instances of in person identification, information and communications technologies attain a relevant role.

Consequently, it is mandatory to have a conceptual framework in the region referred to social electronic identification, which can be taken as a guideline by our countries for individuals' identification and electronic authentication, a basic element for the full exercise of rights and an effective implementation of public policies for social inclusion.

In Section II of this presentation, the antecedents on which this Framework is supported, basically the recommendations resulting from the ministers meetings in 2010 and the Ibero American Charter on E-Government approved 2007 are shown.

In Section III there is a list of the considerations that motivate the current Framework. The main juridical and technological concepts involved in individuals' identification and electronic authentication are described.

In Section IV the conclusions, mentioning the challenges that our countries are facing as regards individuals' identification and possible roads to follow, are presented..

Finally, the "Framework for the Ibero American Social Electronic Identification", which was considered and discussed by the representatives of the States of this region is included.

II. Antecedents

Along 2010, an extensive agenda of meetings of the Ibero American Summit of Heads of State and of Governments was developed. Sectorial ministers meetings, that involved the participation of representatives of the Agricultural, Health, Labour, Public Administration and Reform of the State, Tourism, Education, Childhood and Adolescence, Justice, Presidency, Housing and Urban Planning fields were held. Such activities concluded in the XX Ibero American Summit, which issued the Declaration of Mar del Plata "Education for Social Inclusion".

In all the sectorial ministerial meetings, in different ways, the issue of social inclusion was dealt with as the axis of the region public policies. Specially in the XIII Meeting of the Ibero American Network of Ministers of the Presidency and Equivalent (RIMPE), held in Lisbon, Portugal, the issue of Citizen Participation in the era of e-government was discussed. In that meeting the countries agreed that the "*goals of e-government have to go further than mere ethics and efficiency of the administration processes, towards forms that allow social, political and economical changes, focused on human development, equal opportunities and social justice.*"

Lisbon Declaration

The XIII Meeting of the Ibero American Network of Ministers of the Presidency and Equivalent (RIMPE), dealt with Citizen Participation in the area of E-government: Education for Citizens and Digital Inclusion. The ministers agreed on the cooperation, information and coordination in the E-government area within the Ibero American context. Likewise, the gathering of information on programs, actions and good practices in the area of simplification, administrative modernization

and digital inclusion carried out in different Ibero American countries with the goal of developing cooperation projects of common interest was agreed.

Among others, the Lisbon Declaration, contains recommendations to Governments related to “*a more open, transparent and collaborative Administration model, that allows effectively responding to economic, social, cultural and environmental challenges posed at worldwide level*”. For this purpose, the Declaration considers the use of ICTs to transform the Administration. In this sense, the signatory countries consider that “*the electronic administration and administrative simplification policies shall contribute, in an articulated manner, to the development public services of higher quality*”.

To this effect, the Lisbon Declaration acknowledges that “*the development of safe identification and electronic authentication is another condition for the pretended change, stressing its role in promoting procedures simplification and fostering the use of electronic services*.” Finally, the Lisbon Declaration acknowledges that “*e-government objectives shall go further than mere efficacy and efficiency of administration processes towards ways that allow social, political, economical changes focused on human development, equal opportunities and social justice*.”

Consequently, the signatory countries of the Lisbon Declaration agreed:

- To foster programs that relate electronic administration to administrative simplification, with the goal of turning interactions of citizens and business with the Government Administration simpler, faster and more efficient, reducing operation costs and time, for the exercise of economical activities, and increasing the efficiency of the Public Administration,
- To interchange experiences between the Ibero American community, in relation to the creation of unique, physical or virtual integrated systems that should be organized in line with citizens and businesses demand.
- To interchange experiences relative to the implementation of forms of safe electronic and biometric identification and of articulation mechanisms for the development of trans-border electronic services, in the Ibero American context,
- To articulate the interchange of experiences in the use of ICTs to ensure transparency in the processes of public decision making and to provide with new ways of democratic participation.
- To promote digital inclusion policies and practices and other mechanisms to facilitate the access to electronic services so that citizens can benefit from ICTs potentialities, in an egalitarian and universality manner, so that social and territorial cohesion are ensured.

Sectorial Ministers Conferences

In all the sectorial ministers conferences, the issue of social inclusion was dealt with as the axis of the region public policies, and the use of communications and information technologies for the deployment of substantive public policies.

In effect, in the X Ibero American Conference of Agricultural Ministers in Mar del Plata, held under the “*Education and Agriculture for the Inclusive Development*” theme, the issues dealt with were the settlement of wide ranging agreements to improve life conditions of rural inhabitants, to promote family agriculture, to ensure food security and to favour the access to educational systems and a respectable and paid job.

Additionally, the XII Ibero American Conference of Ministers and High Rank Responsible for Infancy and Adolescence held in Buenos Aires, stated its commitment to adopt legislation, policies and institutional practices to facilitate the construction of integral systems for the protection of infancy and adolescence.

Likewise, the Ministries agreed to set up a virtual platform, on the SEGIB institutional web, to facilitate

the access and availability of material and experiences.

In the XII Ibero American Conference of Health Ministers, held in Buenos Aires, it was decided to foster an integrated Health and Education agenda for social inclusion and it was agreed to carry out joint actions to foster human resources training and education.

In the same sense, the XII Ibero American Conference of Ministers of Public Administration and State Reform, held in Buenos Aires, fostered the promotion and implantation of the Ibero American Charter for the Public Service and the Ibero American Charter on Public Management. The 18 participating countries agreed to decidedly promote the Ibero American Charter on E-Government.

Due to the impact that communication and information technologies currently have on the development of societies, and that their use by governments can lead to a positive result in public management, the Ibero American Charter on E-Government acknowledges citizens' right to interact electronically with public administrations to facilitate their participation and turn the latter more transparent, effective and efficient.

The Charter also promotes, with the same goals, the construction of an information and knowledge society that shall be inclusive, focused on individuals and oriented to development, considering the irreplaceable role of the States to ensure the universalization of all the population and the continuity of electronic services and strengthening of democracy. Consequently, the participants of this meeting agreed to adopt the principles and orientations of the Ibero American Chart by the States of this region, for which they decided to develop policies and tools to facilitate communications and services interoperability, as well the promotion of the use of public software in public administrations.

On the other hand, the XIV Ibero American Forum of Ministers and High Rank Officers of the Housing and Urban Planning Sector, held in Buenos Aires, the 15 participating Ibero American countries agreed to give maximum priority to the actions related to housing in urban areas that are part of integral programs to ensure public facilities, specially educational buildings.

Similarly, the X Ibero American Conference of Ministers of Tourism, held in Córdoba, Argentina, under the "Tourism, Education and Social Inclusion" theme, agreed to go on working in the sensitization and building of awareness in regard to the relevance of tourism as an economy reactivation tool and stimulus of national and local economies of Ibero America. They also decided to keep on with the efforts to create the Ibero American Network on Training on Tourism and a group integrated by Argentina, Brazil, Costa Rica, Spain and Paraguay, was formed, with the goal of elaborating a project to turn this Network feasible.

It was also decided to foster the sustainability concept in tourism, education, training and practice, in order to favour the harmony between human beings and nature, and at the same time encouraging the promotion of new technologies and innovative practices leading to improve current competitive levels in this sector.

On the other hand, and inspired in the social inclusion axis present in all sectorial ministerial meetings, in the XIII Ibero American Conference of Culture, held in Buenos Aires, the ministers analyzed the constitution of an Ibero American Common Market for Music, the creation of an Ibero American Cooperation Fund for Music and the constitution of an Ibero American Music Portal. The participating countries also dealt with the Ibero American Cultural Charter, the Cumbres Project, an artistic and cultural education program, for the region, and culture as a tool for social inclusion.

With respect to education, the XX Ibero American Conference on Education, held in Buenos

Aires, dealt with the 2021 Educational Goals Project: the education we want for the generation of the bicentennials. In the Declaration of Buenos Aires, the ministers of Education agreed that “*our commitment to support education and inclusion, as well as the public policies related to them, require the contribution of all our societies to make its universalization possible under conditions of quality and equity.*”

It was highlighted that the “*2021 Educational Goals Program: the education we want for the generation of the bicentennials ... will strategically contribute to face the pending challenges from the XX century, specially in the field of literacy and basic education of youths and adults, the access to education and the quality of teaching, and the challenges of the XXI century, specially as referred to innovation, scientific development and the incorporation to the information and knowledge society*”.

Finally, the Declaration considers requesting SEGIB and OEI, that under the framework of the objectives of the 2021 Goals, and specifically of the fifth general goal, to continue elaborating an Ibero American cooperation program in the introduction of ICTs into the educational system, with the goal of spreading the different national experiences, evaluating the different educational methodologies, promoting horizontal cooperation among Ibero American countries and to support training of teachers in the use of ICTs.

In a similar sense, the II Ibero American Forum of Ministers of Labour, held in Buenos Aires, Argentina under the “*A Respectable and Paid Job and Education for Social Inclusion*” theme, dealt with the following subjects: development with respectable and paid job and social inclusion (the role of education in professional training); the productive models; innovation and technology (education and learning along life); the actors of the labour world in face of a respectable and paid job; education for social inclusion; Ibero American cooperation and networks (progress in the construction of the Ibero American Network of Work Inspection).

In this meeting, the ministers analyzed the challenges of the crisis and the need to set up innovative policies for social inclusion. On the other hand, the need of policies capable of articulating various productive models and innovation and technology as challenges for education and learning along life were discussed. Finally, the issue of the actors in the labour World in face of education, the Ibero American cooperation and the strategic view in the construction of the regional environment were dealt with.

With respect to the XVII Conference of Ministers of Justice in Ibero-America, held in the City of México, the Ibero American Agreement on the use of Videoconference in the juridical cooperation among justice systems, as well as the Ibero American Program for the Access to Justice was approved. The Ministers approved a series of Recommendations relative to the fight against organized crime, the promotion of human rights of vulnerable groups and processes modernization. The following are the central axes for the COMIIB work for the following two-year period: the access to justice, the reforms of the penitentiary system, the modernization of justice and the fight against organized crime. Likewise, the launch of the Ibero American Portal of Electronic Justice was supported, as well as the development of the Observatory of Ibero American Justice and the work developed by IberRed.

Declaration of Mar del Plata

In the XX Ibero-American Summit, under the “*Education for Social Inclusion*” theme, the Heads of State and Government emphasized the common goal of progressing in the construction of fair, democratic, participative and supportive societies, under the framework of Ibero-American cultural, historical and educational cooperation and integration, to attain intra and intercultural education and social inclusion in the Ibero American region for the quality of all individuals, to promote a more just

Ibero America, with economic, social and cultural development within the framework of democratic, supportive and participative societies that promote the welfare of all the inhabitants of our region.

Likewise, the document emphasizes the role of governments, that “*have to facilitate citizen access and comprehension of laws and to walk towards a more open and collaborative Administration model, that allows an effectively responding to economic, social, cultural and environmental challenges posed at worldwide level.*”

Among other documents, the Declaration of Mar del Plata reflects the commitment of the countries of this region to attain the following objectives:

- *To introduce the principle of inclusion into the educational systems so that no person is neglected an education proposal, related and timely with respect to that person's needs, expectations, interests and identity, either under the modality of formal education or no formal and informal education. (Objective 7).*
- *To attain full literacy in all the countries of the region before 2015. (Objective 11)*
- *To promote the universal access of pupils and teachers to the information and communication technologies and to a quality IT-based education taking into account its fundamental role in education, culture, health, social inclusion, economic growth and sustainable development. (Objective 23)*
- *To foster research and development of innovative strategies for the incorporation of information technologies in the teaching-learning process and in initial and on-going teacher training through the development of contents for the digital and technological literacy programs. (Objective 24)*
- *To encourage the interchange of experiences and to strengthen Ibero-American cooperation in science, technology and innovation and training of qualified human resources, developing national and international actions to promote social inclusion and sustainable development. (Objective 25).*

Ibero-American Charter on E-Government

The Ministers of Public Administration and State Reform and the Heads of the Delegations of the Ibero- American Governments, who met in May 31-June 1, 2007 in Chile, on the occasion of the IX Ibero- American Conference of Ministers of Public Administration and Reform of the State, acknowledged the digital gap among developed and under development countries, and expressed their commitment to narrow the digital gap and turn the Knowledge and Information Society into an opportunity for all, particularly by the inclusion of those at risk of being left behind.

From this perspective, the Ibero- American authorities dealt with the use of new Technologies by governments and public administrations, issuing an Ibero-American Charter on E-Government as a tool to improve public management. In that document they stated: “*We are firmly committed to narrow the digital gap and turn the knowledge and information society into an opportunity for all, particularly by the inclusion of those at risk of being left behind.*”

The Charter underscores that the approach to ICTs use in public management must be that of citizens and their rights, To the effect of this charter, “citizen” is defined as “any natural or legal person who has to interact with a Public Administration and is domiciled in the relevant country or is rightfully entitled for interacting from abroad.”

The Ibero-American Charter on E-Government emphasizes the central role of individuals, not of technology. In that sense, the Chart fosters the acknowledgment of citizens right to interact electronically with a Public Administration . This implies the opening of multiple possibilities to access more easily to Public Administrations, with the following benefits:

- To know what the Administrations are doing.
- To set up the basis for a more open government.
- To overcome physical and space barriers, that for being in remote places or for other reasons many times turn the access of individuals to their administrations difficult.
- To promote inclusion and equal opportunities so that all citizens may have access, whichever their territorial or social status, to the benefits offered by the society of knowledge.
- To actively participate in public affairs.

The Pucón Charter contemplates two objectives: a final and direct objective that is to accept the right of citizens to procedures that facilitate their participation in public management and their relationship with public Administrations. This right, in turn, shall be a contributing material to increase transparency in the Administrations, ensure the respect for the principle of equality and generate a more efficient and effective management.

On the other hand, the Charter pursues an indirect strategic objective: to promote the generation of a knowledge and information society that must be all-inclusive, citizen-centric and development-oriented

In this sense, and what constitutes an extraordinary progress as regards the acknowledgement of social rights, the Ibero-American Charter on E-Government expressly states as an objective: *"To define the content in citizens' right to interact electronically with their Governments and Public Administrations."* (paragraph b) of Article 1º)

In this sense, the Ibero American Charter on E-Government highlights *"the irreplaceable role of the State in these issues to ensure universalization of all the population, and the continuity of e-services and strengthening of democracy."*

It defines the “e-government” concept as a synonym of “e-administration”, understanding as such as the “use of ICTs by Government and Public Administration to improve the information and state-supplied services to citizens, to focus public management efficacy and efficiency and to substantially improve transparency of the public sector and citizens’ participation.”

As part of e-government instruments, the Charter contemplates the issue of individuals identification. In this sense, it emphasizes the Government obligation to have the essential instruments to provide citizens (in a wide sense) the electronic access to the Administration. Within these instruments, it considers as a fundamental factor *"identifying citizens, Public Administration, public officials and agents of these Public Administrations that use electronic media, as well as the authenticity of the electronic documents where they state their will or declarations."*

Likewise, the issue of e-identification is dealt with in relation to the principle of security guiding every e-government activity. In effect, the Charter recommends the States to enact legal and technical standards to ensure all citizens and Public Administrations the necessary conditions so that *"their electronic relations can be secure and safe, both referred to the identity of individuals, department or agency, as well as the authenticity and integrity of the information conveyed, and consequently, the impossibility of being repudiated by the emitter".*

The charter further defines the concept of authenticity and integrity of the information conveyed as the one that represents the content of the original emission and that has not been tampered with or in any other way altered. In this sense, it recommends the States to consider “physical systems, electronic signature systems, even de advanced ones, as well as other alternative systems that may replace electronic signatures, when the nature of the formalities and procedures so require in order to

identify the communicating party and ensure the authenticity of the contents of the communication" in the norms regarding E-Government security.

As it is shown, for the Ibero-American Charter on E-Government, individuals identification is the core element for the implementation of e-government policies, as an essential and basic instrument for the execution of public policies as well as their role related to identification in electronic environments. In this sense, the digital signature gains special relevance as an instrument that allows, on the one hand, to identify the authorship of electronic documents, and simultaneously, to confirm the integrity of such digital documents.

III. Elements for Electronic Identification

This sections deals with the aspects that explain the reasons why electronic identification is a key element for the implementation of public policies for social inclusion. It also contains a succinct description of the technologies involved.

Relevance of Electronic Identification for the Full Exercise of Citizens Rights

Our countries are daily progressing in explicitly acknowledging their inhabitants social rights. The search for social inclusion not only implies acknowledgement of these rights, but also to provide the necessary conditions to ensure their effective exercise.

From the juridical perspective, an individual's identity is the base on which the framework of rights and obligations is built. Although rights are established *erga omnes*, i.e, for everybody in general, the appropriation of a particular situation supported by the regulations framework with its respective rights and obligations, emerge from the specific identity of every individual.

In another sense, the concept of an individual's identity makes reference to the confirmation that the data that prove that an individual is effectively the person that he or she claims to be, rights-bearing subject, with determined attributes. This confirmation of data that prove the identity is known as "identification", i.e. the procedure that by means of external elements allow assigning an identity with determined attributes to a concrete individual.

In any relationship between two persons or more, with legal effects, it is necessary to prove these parties' identity. An agreement, a lawsuit, a marriage, a purchase, a sale, in fact, every transaction with legal effects requires the identification of the parties participating in it as a previous step for its execution. In the public administration the situation is similar. The procedures and formalities performed before the Administration require the identification of the individual starting it and the officials that participate. A purchase requires the identification of those who participate in the bid, the notification of an administrative procedure is performed for a determined individual and is executed by a competent official, in fact, every activity in the Public Administration involves a party that performs it and that party has to be identified.

The implementation of public policies of social scope also requires the identification of its beneficiaries. Educational, health, digital inclusion policies, all of them are supported on a correct identification of the beneficiaries. To have access to these social policies, individuals have to prove their identity by means of a document in order to have access to benefits and to fully exercise their rights. Consequently, if an individual does not have any identification document he or she cannot have access to his or her rights, cannot claim for them, summarizing, that individual does not exist for the State.

Individual's identification is an essential element of legal acts as an error on the individual's identification brings about the nullity of the legal act, for being a vice of consent that invalidates the legal relation.

individual's identity and identification are subject of the substantive law and the procedural law. Identification is referred both to the individual's identity information (first name, last name, age, sex, address and nationality), and the action and procedure of checking and proving that identity. An individual's identification is assumed as the individualization within a social context. That individual is identified by other data, as it will be seen later, that are the data object of biometrics. Unique personal features that have the purpose of indubitably identifying that individual.

Now then, the law is what defines what instruments and procedures will be considered valid for any individual's identification. It is the State the responsible for individuals' identification, from different procedures in line with the legislation of the country involved. In Argentina, individuals' identification is ruled by Law No. 17.671 (Law for the Identification, Recording and Classification of the National Human Potential), and is performed by means of a National Identity Document. Moreover, there are documents for identification when crossing borders, passports. Not every country has the regulations to establish the unique identification documents. Nevertheless, there are standards for passports due to the need to be acknowledged further than the border of the issuing country.

An individual who has not been identified by the State, is a "non-existent" individual. That person does not have a birth certificate, and consequently a document proof of identity. That individual is an easy target for human trafficking, sexual exploitation and abuse of minors, pornography, organ trafficking, among other crimes. One of the basic functions of the State is to ensure individuals' identification. An individual without a birth certificate, cannot exercise his or her rights, or be granted social assistance and enter the labour market: summarizing, that individual does not exist for the law. Not having a birth certificate, i.e., not being registered in the citizens national registry, is one of the causes for social exclusion, because a child who is not registered, is a child with no name, face or identity.

Elements that Allow Identification

Historically, an individual's identification process was based on the comparison of a feature with a data, but as applications grew, the non personal recognition mechanisms turned to be mandatory. For example, not long ago, in Argentina the National Identity Document was issued after a fingerprint expert checked the fingerprint taken to the applicant against the fingerprint recorded on the first file. This process took a long time. Today, in the new system implemented by the Ministry of the Interior, this checking process is automated, speeding up the time necessary to issue a new National Identity Document

With the progress in the technology field, the authentication and identification process started to be supported on new tools. Today in order to pay with a credit card, it is necessary to submit the credit card and the ID with the individuals' photo, which is checked at the sales point (by the sales person). Nevertheless, as there is not an automated and technology-supported identity verification process it may happen that a person who had stolen an individual's credit card and ID, has changed the photo and be able to purchase without being detected.

Biometric technologies were originally used for legal purposes, basically for crime investigation. But the overall development of ICTs has widely extended their use with other goals. Biometrics provides those identification techniques that are based on an individual's physical characteristics: DNA, fingerprints, facial patterns or iris characteristics. In fact, characteristics that makes a person unique.

Governments rely on biometrics to identify people, authenticate their identity in information systems, to strengthen public security in airports and cities, and to restrict the access to secure places, both physical (buildings) and virtual (information systems and applications).

Recognition systems that use biometric technologies recognize a person based on physical characteristics (fingerprints, facial and hand characteristics, iris patterns) or behavioural characteristics learned or acquired (voice, holographic signature and keyboard typing patterns)

The use of biometric techniques for individuals' identification is supported on the use of devices that contain their information and scanners-readers of it. These devices can be intelligent cards that store biometric data in a Integrated Circuit Chip (ICC), in turn protected by public key technologies (used by the authority that delivers the personal identification device to sign the ICC) and by asymmetric key technologies (a PIN – Personal Identification Number), e.g., the access to information systems or computing centres.

This device is a physical artefact (for example an identity card, an intelligent card) issued to an individual by a competent authority that contains data stored that prove that individual's identity (for example a portrait photo, fingerprints, etc.) so that the identity of the holder of that document can be compared against the information stored by other person (i.e., they have to be accessible for a person to be read) or by an automated system (i.e., that can be accessed or compared electronically).

Authentication factors currently used are three, based on:

- Something that I know: *the individual is authenticated by means of something that he or she knows: a key, an identification number – PIN, a phrase or an answer to a security question.*
- *Something that I have: the person is authenticated using something that he or she has: a token, a smart card, a digital certificate.*
- *Something that I am: the individual is authenticated based on an own characteristic, i.e., biometric data.*

The factors based on knowledge and ownership require that the individual that is going to be identified by a system has to remember to carry the device. Instead, when biometric technologies are applied, that data is in that individual and it is almost impossible to be falsified, i.e., be used by other individual for identity impersonation. It is said that in the first two factors, the relationship between the data and its verification is weak, what makes identity impersonation easier, as the system cannot distinguish between the legitimate possessor of the device and someone who had stolen it; the same applies for a key.

The main function of applied biometrics is referred to the identification of individuals, both in the real and the virtual environment.

Electronic Identity Document

The identification of persons who are born in their territory is one of the State's basic functions in some countries, what in general is responsibility of the Civil Registry. In our region, governments have introduced a state modernization process which considers the possibility of incorporating ICTs to accomplish such identification function.

But apart from fulfilling this individuals' identification function, the use of biometrics in national electronic documents brings about the deployment of additional functionalities. In this context, the use of biometrics for this purpose will enable the creation of a unified database with individuals' identification information. The availability of this information will make the accomplishment of other

governmental functions easier and more effective, such as education, social security, and in general, any other public policy that may demand beneficiaries' identification.

Towards an Interchange of Biometric Data

Governments need to have secure identification mechanism to implement public policies. Identification allows people to have access to social benefits, social security benefits, to enrol their children at school, to receive hospital care, to vote, etc. The State shall ensure the full exercise of social, voting and civil rights, public security and cross-border traffic. For all these public policies, biometric data associated to biographical data is one of the keys for success. To have this biometric database associated to biographical data allows and facilitates the implementation of the major public policies.

From the point of view of the user, it is simply "*one finger for a couple of seconds: this is what an individual will be required*". It can be a hospital, a bank, a government agency or a polling station. An individual will be requested to place his/her finger on a finger scanner device that will immediately confirm if that finger effectively is that individual's finger. From the governments' point of view, it is an essential tool to facilitate the execution of relevant public policies. It is not enough to have biometric data in different databases managed by different agencies or organizations, but to cooperate and share that information for a rational use, supported on ICTs, of easy access by non-experts and in line with current times.

Therefore the issue is to set up collaboration mechanisms to be able to have quick information from the integration of a database of biographical and biometric data of an individual in a digitized format, susceptible to be shared in real time by different government agencies. At present, the only information the government has stored in digital format are the biographical data of an individual: first, middle and last name, sex, date of birth, etc.

In turn, biometric data (fingerprints) have historically been kept in paper-based documents in a file. They cannot be used by an automatic identity verification system. For not having these tools available, a physical person may have more than one identity because there is no way to make a 'one to n' control', i.e. against the total.

In addition to the uses in banking, health and social services, an evident use of this system would be for voting. This would be basic to create voting rolls with biometric patterns to verify the voter's identity before casting his/her vote. This will ensure that no person will be able to vote under another individual's name.

Signature Infrastructures

The countries of this region have made progress in the legal recognition of the document and the electronic signature.¹

In some countries legislation has considered digital signature schemes, i.e., electronic authentication systems based on public key technologies. This means the existence of Digital Signature Infrastructures, of national scope. Nevertheless, in an environment where commercial and government transactions cross borders, this legislation does not cover such interchanges, there being a legal vacuum.

UNCITRAL Regulations

Thus, it turns necessary to promote agreements among the countries of the region, that taking into

consideration the own national regulations, establish the basis for the mutual acknowledgement of digital signatures.

In this sense, there are antecedents as the UNCITRAL Convention on the Use of Electronic Communications in International Contracts. Since the Model Law on Electronic Commerce was passed in 1996, the countries have been adopting laws on this issue. Nevertheless, such laws have a limited scope as they are applied to domestic transactions in each country, there not being any regulation on the wide range of cross-border transactions that are done on the Internet. To overcome this situation, UNCITRAL elaborated the Convention on International Electronic Communications that has been signed by 18 nations among which are China, Russia and Korea, and from this region Paraguay, Colombia, Honduras and Panama.

Such Convention, adopted by the General Assembly of November 23, 2005, has the goal of promoting legal certainty and trading predictability when electronic communications are used in international contracts. It applies to the determination of the location of the parties involved in an electronic environment; the time and place the electronic communications are sent and received; the use of automated message systems to generate agreements; and the criteria applied to determine the functional equivalence between the electronic communications and the paper documents, including the "original" paper-based documents, as well as the methods for electronic authentication and handwritten signature.

The UNCITRAL Convention is supported on the technological neutrality principle, admitting any authentication method that allows on the one hand to establish the identity of a person and on the other hand to establish the personal involvement of that person. Also support the agreements of the parties, backgrounds, proportionality between means and ends, including the post-test. Such methods been considered as the functional equivalent of the firm applying traditional laws.

MERCOSUR Regulations

In the MERCOSUR environment, with its original integration by four member countries (Argentina, Brazil, Paraguay and Uruguay), the digital signature issue started to be dealt with in the Work Sub-Team No. 13 on Electronic Commerce, on which framework the two resolutions on digital signature were passed.

Resolutions on Electronic Commerce

In 2006, the MERCOSUR Work Sub-Team No. 13 on Electronic Commerce passed two Resolutions on Digital Signature. The first one, Resolution No. 34/06, establishes the Guidelines for mutual agreement contracts on electronic signatures in the environment of the MERCOSUR.² The second Resolution No. 37/06, considers the legal efficacy of the electronic document, the electronic signature and the advanced electronic signature in the environment of the MERCOSUR.³

None of these Resolutions have a practical effect as the first one, although it does not require the incorporation into the internal law, it does not establish a recognition agreement in itself but it establishes guidelines to that effect. The second one requires its incorporation into the internal law to have legal efficacy, for which it only represents a general declaration with no legal effects.

¹ See Argentina Law on Digital Signature N° 25.506; the Dominican Republic Law on E-Commerce, E-Documents and Digital Signature N° 126-02; Peruvian Law on Digital Signature N° 27.269; Brasil N° 2200-2; Chile on Digital Signature N° 19.979; Colombian Law on E-Commerce and Digital Signature N° 527-1999; Ecuador Law on E-Commerce, Digital Signatures and Data messages; Venezuelan law of Data messages and Digital Signatures; México: Decree that reforms several statements of the Civil Code for the Federal District and Federal Code, Civil Procedures, Commerce Code and Federal Code of consumer protection (2000); Panamá, Digital Signature Law (2001); and Uruguay, Law N° 18.600 (2009) on Electronic Documents and Digital Signature.

² Available at http://www.mercosur.int/msweb/Normas/normas_web/Resoluciones/ES/RES%20034-2006.pdf

IV. Challenges and Conclusions

At present the countries of the region are working on digital inclusion projects that will shortly allow to narrow the existing digital divide. Educational projects supported on computers for students, spots to access to broad band, accessibility policies, impact of social networks present in the digital agendas of our countries, are showing a real fact: more people connected, more services provided on the Internet, increased need to ensure individuals identification in electronic means.

To comply with these recommendations of Lisbon Declaration, tending to attain "*a more open, transparent and collaborative Administration model, that allow effectively responding to the economic, social, cultural and environmental challenges posed at worldwide level*", the signatory countries consider that "*the development of accurate identification and authentication mechanisms, is another condition for the intended change, highlighting its role in promoting the simplification of procedures and fostering the use of electronic services.*"

In this sense, the present document contains a description of the issues involved in electronic identification processes and its relevance for citizens' full exercise of their rights. The biometric technologies involved have been briefly described, specially those related to the electronic identity document.

The difficulties for its implementation are not related to the technology itself, as they have a high degree of development. They are neither related to the existence of international standards, which have been developed and accepted. As any project that implies implementing ICT technologies in the State administrative management, these projects are focused on the building of a biometric database or replacing current identity documents by the electronic ones, facing the same risk factors as any other cross-cutting technological project.

The challenges faced by our countries at the moment of implementing technological projects in the public sector in order to develop E-Government⁴, are not related so much to the scarce of resources, or an insufficient infrastructure, or a lack of professionals, but to the lack of coordination between public agencies. In effect, the efforts performed by governments not many times attain the expected results, not for the lack of resources but because different agencies carry out projects in a non coordinated manner, what generates water-tight compartments.

It is clear that the attainment of successful results in the implementation of technological projects in public management requires an adequate planning, and monitoring and evaluation shall go in hand with their development. But this is not enough to ensure the project's success, moreover those where various agencies are involved, i.e. cross-cutting projects in the Administration. A key element is the role of policy makers, especially those that participate in the processes of definition of public policies related to the use of technologies in the Administration or to State Modernization.

"Leadership" is the most important success factor in the design and implementation of electronic strategies. If there is no decisive leadership it will not be possible to overcome the resistances to change that naturally implies the modification of the work modes derived from the incorporation of ICTs in public management.

³ Available at http://www.mercosur.int/msweb/Normas/normas_web/Resoluciones/ES/GMC_2006_RES-037_ES_EficaciaFirmaDigital.pdf

⁴ Este documento adopta la definición de "gobierno electrónico", como sinónimo de "administración electrónica", contenida en la Carta Iberoamericana de Gobierno Electrónico, 2007. La Carta de Pucón entiende por tal al "uso de las TIC en los órganos de la Administración para mejorar la información y los servicios ofrecidos a los ciudadanos, orientar la eficacia y eficiencia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos."

In this sense, we propose this document on Ibero American Social Electronic Identification that shall contain the general framework, basic guidelines, to be followed by our countries in order to implement fast and effective authentication and identification systems as a basic input for the implementation of public policies for social inclusion, and to ensure every inhabitant of our region the right to identity.

Based on previous consideration, the Framework for the Ibero American Social Electronic Identification is enclosed, considered by the States of the region in Asunción, Paraguay.

V. Framework for the Ibero-American Social Electronic Identification

Preamble

The countries of the region have reported progress in setting public policies for social inclusion that require the use of information and communications technologies (ICTs) for their implementation.

The IX Ibero-American Conference of Ministers of the Public Administration and Reform of the State held in Pucón, Chile, on June 1, 2007 approved the 2007 Ibero American Charter on Electronic Government that establishes a set of concepts, values and useful guidelines for its design, implementation, development and consolidation as a tool contributing to the improvement of Ibero American public management, while in many current legislations, the legal value of electronic documents, electronic signatures and digital signatures are recognized.

Individual's identification constitutes an essential requisite for the full exercise of their rights. As an unavoidable duty of the Ibero American States, the correct identification of individuals has to be ensured, as well as safeguarding and protecting the right to identity of every inhabitant on the territory.

The XIII Meeting of the Ibero American Network of Ministers of the Presidency and Equivalent (RIMPE), held in Lisbon, Portugal dealt with Citizen Participation in the area of E-government: Education for Citizens and Digital Inclusion and in the Lisbon Declaration it is acknowledged that *"goals of e-government have to go further than mere ethics and efficiency of the administration processes, towards forms that allow social, political and economical changes, focused on human development, equal opportunities and social justice"*.

The Lisbon Declaration also recognized that the development of safe identification and electronic authentication, is another condition for the pretended change, stressing its role in promoting procedure simplification and fostering the use of electronic services.

Consequently, the present Framework has the goal of establishing a set of concepts, fundaments, principles and useful guidelines for the design, implementation and development of an Ibero American Social Electronic Identification to consolidate the exercise and effective enjoyment of Ibero American citizen's social rights.

First Chapter. Purpose and scope of Ibero-American Social Electronic Identification

Objectives	1	<p>The present Framework for the Ibero American Social Electronic Identification has the following objectives:</p> <ul style="list-style-type: none">a. To provide a concept framework and the components involved in individuals' identification processes, that by means of technological elements, facilitate E-Government development and the implementation of public policies for social inclusion in Ibero America.b. To promote the use of electronic identification documents in the countries of the region, including electronic passports and national identity documents.c. To provide technical recommendations to public administrations for the electronic authentication processes, covering remote authentication of users on open networks.d. To constitute a generic framework of leading principles, policies and management procedures, to set up the basis to establish a future scheme of mutual recognition of social identification devices in the countries of the Ibero American community.e. To serve as a guide for the design, regulation, implementation, development, improvement and consolidation of national models for individuals' electronic identification by the regional public administrations.
Purpose	2	<p>The objectives set forth in the previous paragraph have multiple purposes:</p> <ul style="list-style-type: none">a. To promote citizen participation in public management, through the implementation of quality electronic services and guidelines for interaction between inhabitants and their public administration by electronic means.b. To seek the acknowledgement of the right to interact electronically with the Administration as considered in the Ibero American Charter on E-Government.c. To facilitate communication and relationship between individuals and public administrations by electronic means.d. To establish a cross-border acknowledgement framework for electronic identification and authentication devices.e. To promote the use and mutual acknowledgement of electronic identity documents.f. To ensure the protection of individuals' right to identity.g. To facilitate data interchange among the countries of the region, in line with the national regulations on personal data protection.

- Social Electronic Identification Concept
- 3 Without prejudice of the denominations adopted in national legislation, "*Electronic Social Identification*" is understood as the process that through external elements allows assigning a concrete person an identity with determined attributes, i.e., the verification that the data that prove that an individual is effectively the person he or she claims to be, subject of rights, with determined attributes.
- Within the present framework, "*Electronic Authentication*" is understood as the verification process of the authenticity of the identifications made or requested by a physical person or entity, on data such as a message or other means of electronic transmission. The authentication process is the second of two steps that comprise:
- 1) The submission of a means that proves identification before the system and,
 - 2) The presentation or generation of information that corroborates the relationship between the means submitted and the identified person or entity.
- Fundaments of Social Electronic Identification
- 4 The Ibero American Social Electronic Identification is supported on the following fundaments:
- a. Individuals identification is a State unavoidable obligation, as well as the protection against its inviolability.
 - b. The acknowledgement of the right to identity for all individuals, as well as the protection of its integrity and guarantee of its full exercise.
 - c. The egalitarian access to the society of information as a relevant public asset, that has to be fostered by all the governments of the region.
 - d. The acknowledgement of the principles defined in the Ibero American Charter on E-Government.

Principles for Social Electronic Identification Framework	5	<p>Based on previous fundaments, the Ibero American Social Electronic Identification is guided by the following principles:</p> <ul style="list-style-type: none"> a. Equality and non discrimination principle: in no case the use of electronic means can imply the existence of restrictions or discriminations for the inhabitants that interact with their public administrations. b. Legality principle: to keep guarantees provided for in the traditional modes of relations between people and the Government and the Administration when performed by electronic means. c. Conservation principle: it ensures that electronic communications and documents are kept in an accessible manner for its further use or reference, in similar conditions as in traditional means. d. Transparency and accessibility principle: it ensures that the information of public administrations and their services by electronic means is made in an understandable language in line with the recipient's profile. e. Proportionality principle: so that security methods are the adequate ones for the nature of the relation established with the Administration. f. Responsibility principle: so that the Administration and the Government be accountable for the actions performed by electronic means in the same manner as those made by the traditional means. g. Technological adequacy principle: Administrations shall choose the most adequate technologies to satisfy their needs.
---	---	---

Second Chapter. Elements involved in the Identification process

Guarantee of the right to interact electronically with the Administration	6	The Ibero American States must take care of the effective exercise of the individuals' right to interact electronically with the Administration, what requires ensuring social electronic identification of their inhabitants.
---	---	--

For the purpose of social electronic identification, of the inhabitants of the Ibero American Community, the Ibero American States will understand by:

- a. **Authentication factors:** are those elements that integrate the identification process.
Authentication factors currently used are three, and are based on:
 - Something that I know: I the individual is authenticated by means of something that he or she knows: a key, an identification number— PIN, a phrase or an answer to a security question.
 - Something that I have: the person is authenticated using something that he or she has: a token, a smart card, a digital certificate.
 - Something that I am: the individual is authenticated based on an own characteristic, i.e., biometric data

The factors based on knowledge and possession require that the person who is to be authenticated before a system remember or carry the device. Instead, when biometric technologies are applied, the data is carried by that person him/herself, and it is almost impossible to be tampered with, or in any other way altered for impersonation purposes. It is said that in the first two factors the connection between data and their verification is weak, what facilitates impersonation, as the system cannot distinguish between the actual possessor of the device and someone who has stolen it; the same applies to the key.

- b. **Biometric technologies:** Biometric recognition is understood as the automated methods that ensure individuals recognition based on distinguishable physical or behavioural traits. Technologies used in biometrics include recognition of fingerprints, face, veins patterns, iris, voice and typing rhythm, among other.
- c. **Biometric System:** It is an IT recognition system based on one or various patterns that operates requiring biometric data to an individual, collecting a pattern of the data acquired and comparing the example against a previously registered template. Depending on the application, this template can be stored in a centralized database or in an individual device as a token or smart card.
- d. **Public Key Infrastructures:** (also known as Digital Signature Infrastructures or PKI). They can be defined as the set of hardware, software, persons, policies and procedures necessary to create, manage, store, distribute and revoke public key certificates based on asymmetric cryptography, that facilitate the creation of a verifiable association between a public key and the identity of the possessor of the corresponding private key.

- e. **Digital Signature:** –also called safe electronic signature, advanced electronic signature or acknowledged electronic signature -. The digital signature concept has at least two meanings: a technological one, related to public key technologies; and a legal one, that is related to the definition that national laws have included as an equivalent of the handwritten signature. From the technological point of view, a digital signature is the authentication mechanism that, supported on asymmetric cryptography, i.e. that it uses two keys, a private and a public one, allows identification of the signer and ensures the integrity of the content of the electronic document signed. From the legal point of view, the laws require an administrative procedure. This means that to be considered a legal digital signature, this mechanism needs to be applied through the use of a digital certificate issued by a certification entity approved by the governing body of the State in this subject matter.

- f. **Electronic signature:** the concept is applied to any sound, symbol or process, attached or logically associated to an electronic document that express a person's consent issued electronically. In general, the laws call "electronic signature" any authentication mechanism that does not comply with any of the requirements for a digital signature. "Electronic signature" is the generic and neutral term to refer to the universe of technologies that a person can use to express his or her consent about the content of a document.

Third Chapter. Mutual Consent Agreements

- | | |
|--|---|
| Adoption of regional commitments | <ul style="list-style-type: none"> 8 The present Framework promotes all those issues, that related to electronic identification processes of individuals in physical or virtual environments, constitute the basis for future agreements of mutual acknowledgement, between the Ibero American States, that are mandatory to attain a common effective means for Ibero American Social Electronic Identification.
 9 Through this Framework, the Ibero American States will focus the discussion of the legal and technical aspects necessary for the execution of data interchange agreements, the interoperability of the systems and the establishment of common technological standards.
 10 The Ibero American States are committed to the interchange of national experiences as regards the implementation of the electronic identity document and the electronic passport, and any other mechanism for digital authentication.
 11 At last, this Framework includes the contents of understanding so that the Ibero American States can execute agreements of mutual acknowledgement of digital certificates.
 12 To constitute a generic framework of leading principles, policies and management procedures, to set up the basis to establish a future scheme of mutual recognition of social identification devices in the countries of the Ibero American community. |
| Addendum to the Ibero-American Charter on E-Government | |

