Universidad de Alcalá

Dpto. Ciencias de la Computación

Sistemas Empresariales

Administración Electrónica – III
DNIe y Firma Electrónica

Índice

1. DNI
2. Firma electrónica
3. Seguridad de la información en la eAdmin
4. Interoperabilidad

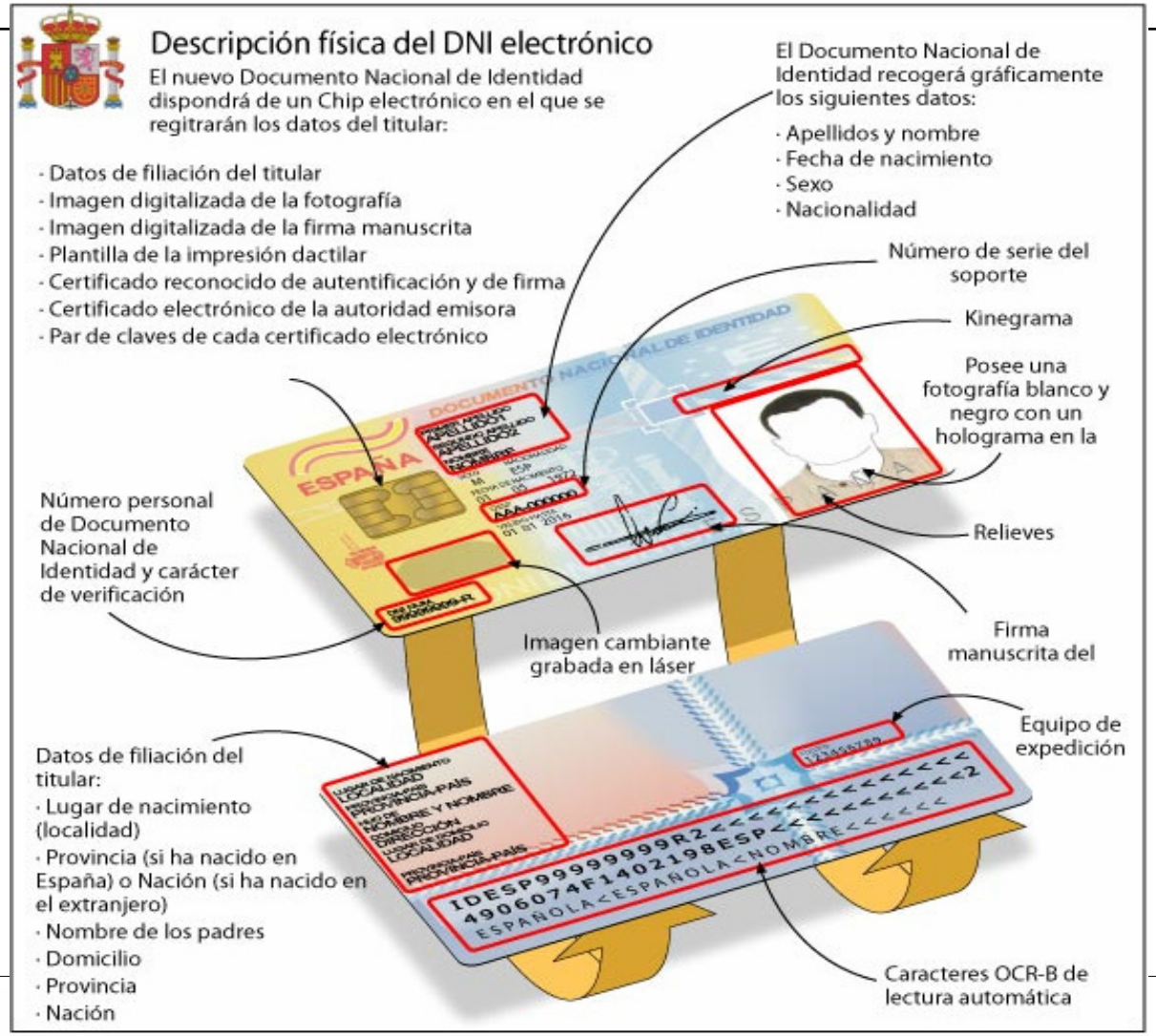
DNI electrónico

- El documento nacional de identidad electrónico **acredita física y electrónicamente** la identidad personal de su titular y permite la firma electrónica de documentos.
- Contiene **dos certificados** cualificados según la ley de firma electrónica, uno para **autenticación** y otro para **firma** (con uno hubiera bastado pero se persigue que el ciudadano distinga los procesos de autenticación y firma)

DNI-e: frenos

- **Usabilidad**: pide muchas veces el PIN, a veces incluso cuando no vas a trabajar con él.
- **Lectores**: precisa de un lector y no todo el mundo lo tiene.
- **Caducidad**: la caducidad del certificado no coincide con la del soporte físico lo que produce confusiones.
- **Renovación**: la renovación sólo puede realizarse en los quioscos de comisarías.
- **Formación, formación** y **formación**

DNI electrónico

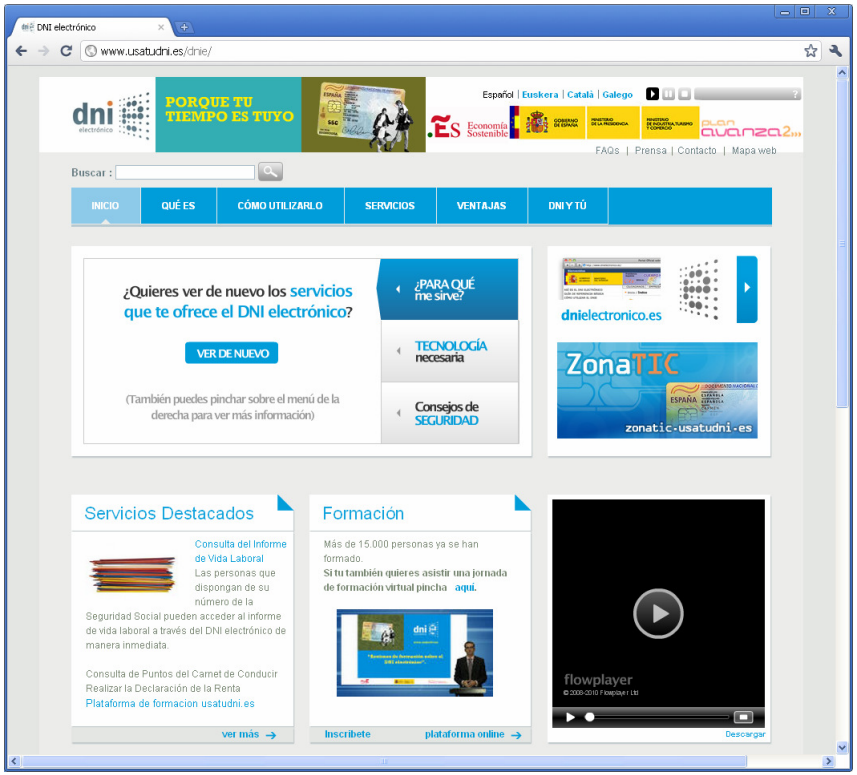


DNI-e:¿qué necesito para usarlo?

- Un lector de tarjetas chip
- El software necesario
  - www.dnielectronico.es sección descargas
- ¿Lo tenemos instalado?
  - Ver si tenemos una carpeta c:\dnie

Práctica: www.usatudni.es

Usemos el dni-e



Práctica: www.usatudni.es

Usemos el dni-e

-Cambio de domicilio a través del portal 060

-Cambio de domicilio en www.seg-social.es

-Consulta vida laboral

-Consulta registro seguros de vida

-Consulta puntos carnet de conducir

Índice

1. DNI
2. Firma electrónica
3. Seguridad de la información en la eAdmin
4. Interoperabilidad

Firma electrónica

- ¿Qué es?
- En qué se sustenta: principios básicos de criptografía
- Ejemplos

Firma electrónica vs firma digitalizada

- **Firma digitalizada:** digitalizar una firma manuscrita

Firma electrónica vs firma digitalizada

- **Firma electrónica:** es un conjunto de datos criptográficos que asocian una identidad (de una persona o un equipo informático) con unos datos (documento, mensaje, etc.).

No tiene una representación inteligible.

Hay una pequeña diferencia entre firma electrónica y firma digital, aunque para nosotros:
Firma digital = Firma electrónica ≠ Firma digitalizada

Firma electrónica

Según art. 3 Ley 59/2003:

1.La **firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden** ser utilizados como medio de identificación del firmante.
2.La **firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de** los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
3.Se considera **firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada** mediante un **dispositivo seguro de creación de firma.**
4.La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el **mismo valor que la firma manuscrita en relación con los consignados en papel.**

Firma electrónica

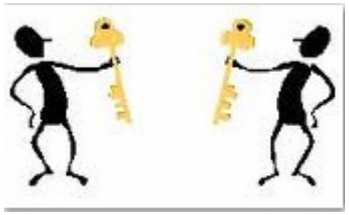
La ***diferencia entre Firma Electrónica y Firma digital*** *estribaría en que esta última denominación se utiliza para las firmas electrónicas basadas en criptografía de clave pública mientras que la otra se utiliza para cualquier tipo de firma electrónica.*

Por tanto tendríamos un concepto amplio de firma electrónica y otro restringido o para una determinada técnica como es la infraestructura de clave pública.

Firma electrónica: fundamentos

- Principios básicos
  - Criptografía simétrica
  - Criptografía asimétrica
  - Funciones hash (resumen)
- ¿Qué es la firma electrónica?
- Práctica

Criptografía simétrica



- Método criptográfico que usa una **misma clave** para cifrar y descifrar mensajes.
- Las dos partes que se comunican han de ponerse de acuerdo **de antemano** sobre la clave a usar.
- El remitente cifra un mensaje usando la clave y el destinatario lo descifra con esta misma clave.
- El principal problema no está ligado a la seguridad, sino al intercambio de claves.

Criptografía asimétrica

- Método criptográfico que usa **un par de claves** para el envío de mensajes. Las dos claves están **relacionadas** y pertenecen a la misma persona.
  - Una clave **pública** que se puede entregar a cualquiera (certificado) o publicarla en algún sitio.
  - Una clave **privada** que el propietario debe guardar de modo que nadie tenga acceso a ella.

Criptografía asimétrica: idea clave

- **Lo que se cifra con una clave se puede descifrar con la otra, pero nunca con la misma.**

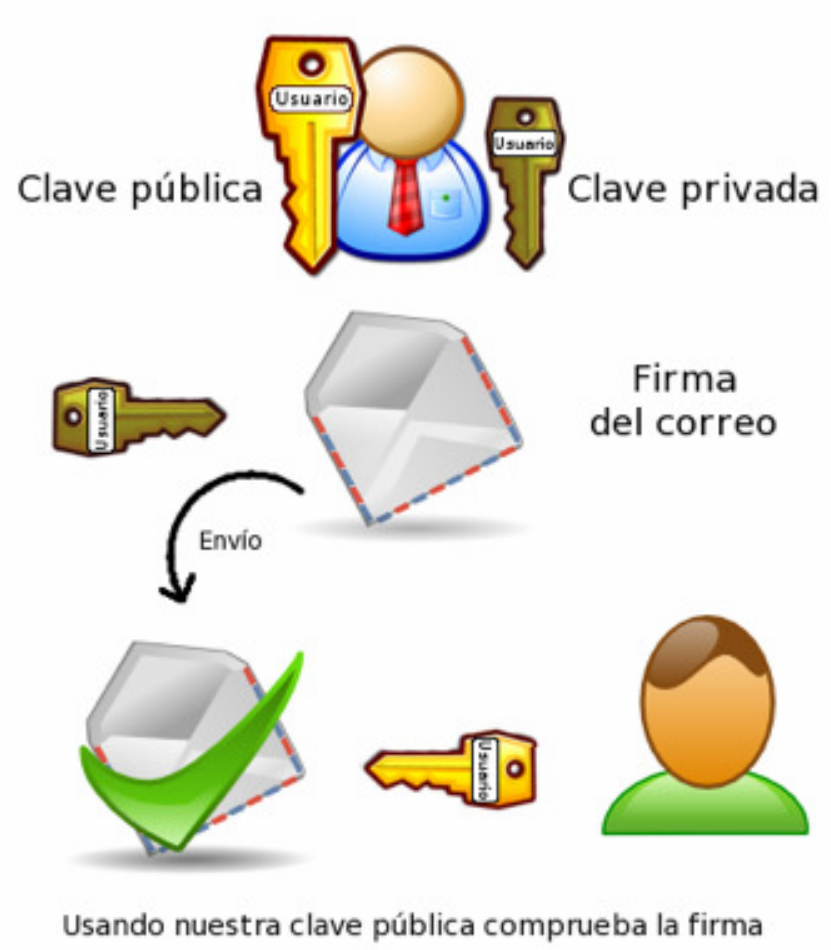
- Si se cifra un mensaje o documento con la clave privada, se podrá descifrar con la clave pública, sin embargo no se puede descifrar utilizando de nuevo la clave privada.
- Si se cifra con la clave pública se puede descifrar con la clave privada.

Criptografía asimétrica

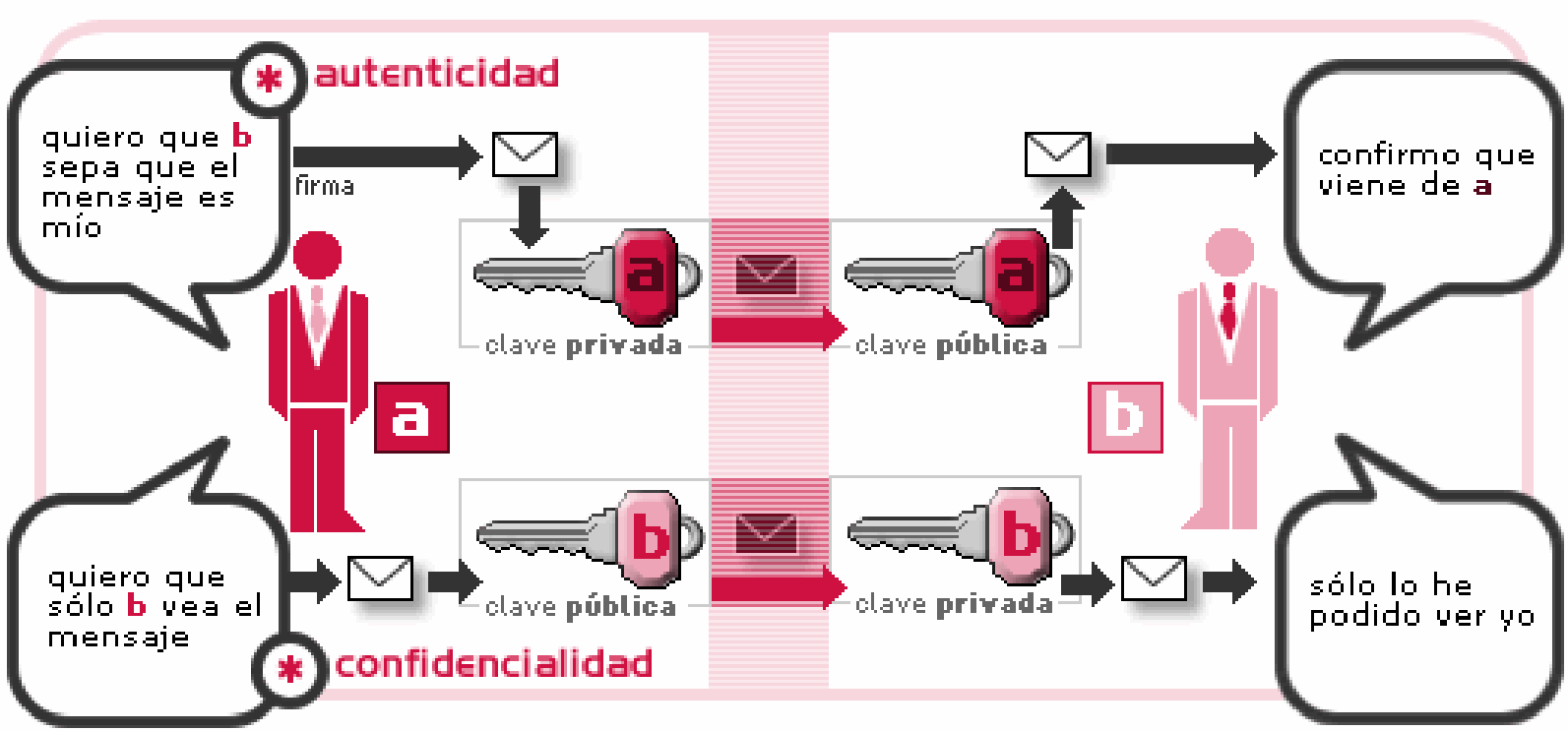
- Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.
- **No es necesario que remitente y destinatario se pongan de acuerdo en la clave a emplear**.
- Antes de iniciar una comunicación secreta tan sólo es necesario que el remitente consiga una copia de la clave pública del destinatario. Sólo el destinatario podrá descifrarlo con su clave privada.

Criptografía asimétrica: cifrado

Criptografía asimétrica: firma



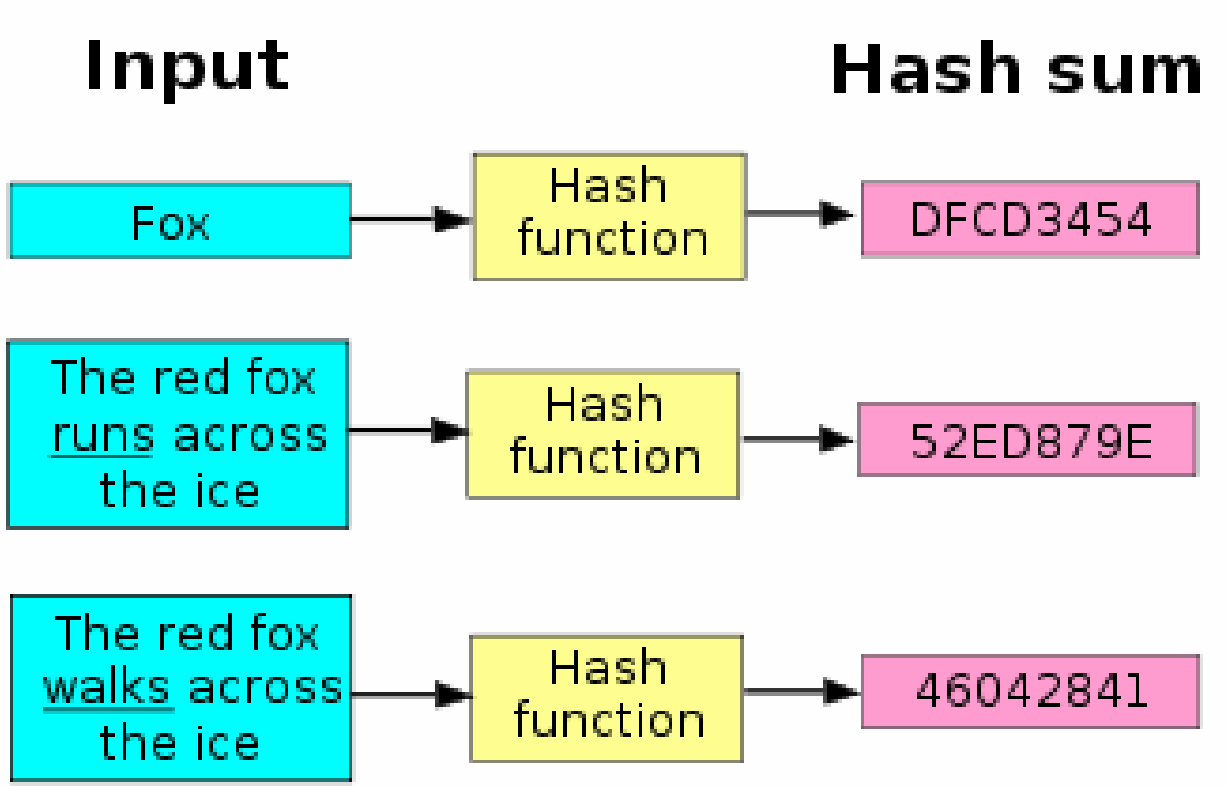
Criptografía asimétrica



Funciones hash o resumen

- Se refiere a una función o método para generar claves que representen de manera **unívoca** un documento, registro, archivo, mensaje, etc.
- Se trata de resumir *algo* (documento, mensaje…) en un código *hash* resultado que tiene la ventaja de ser **único** y de **longitud fija.**

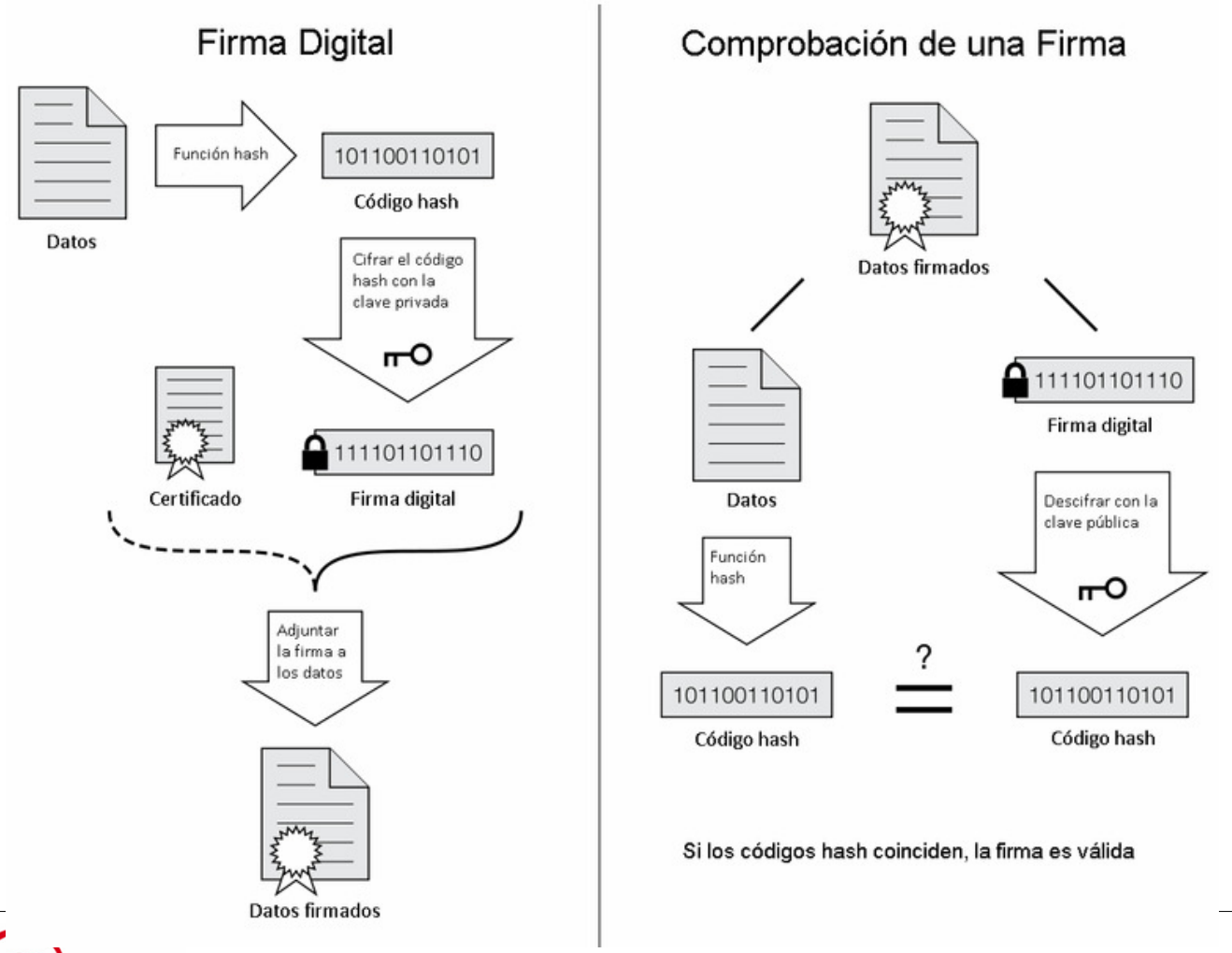
Funciones hash o resumen



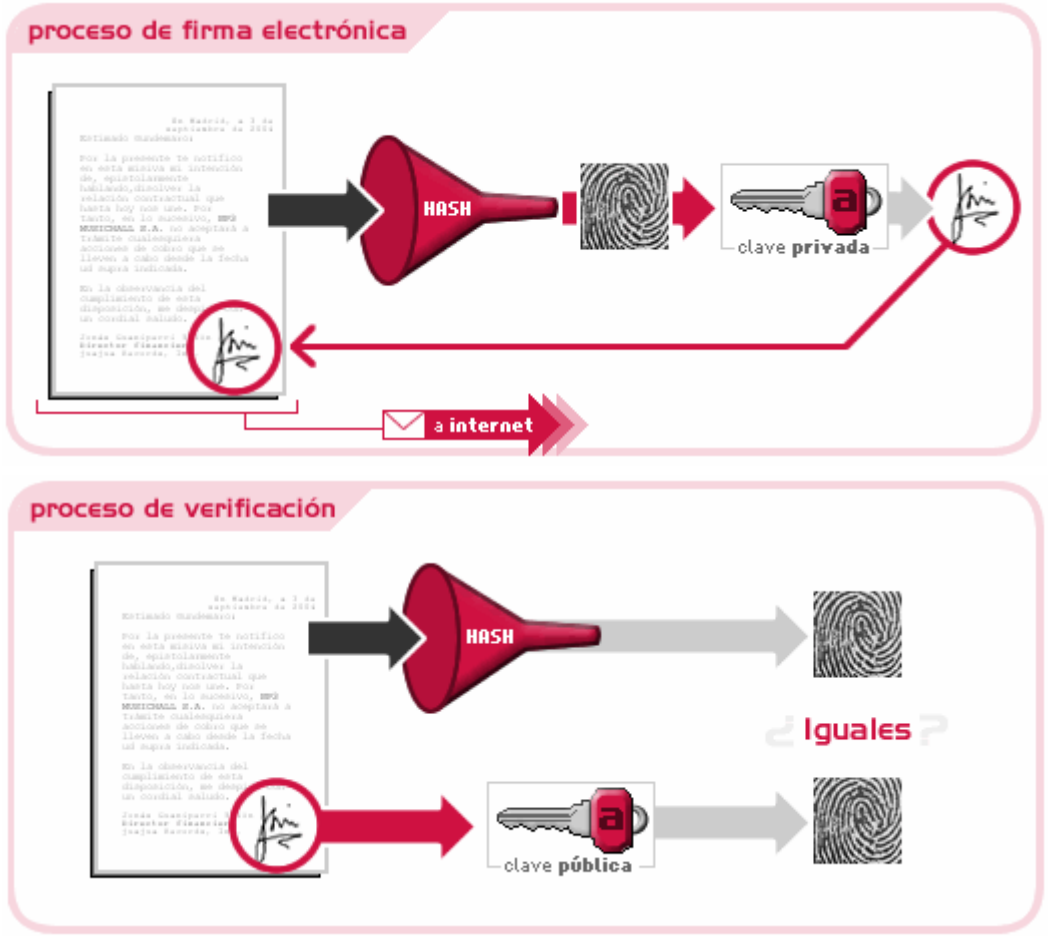
Con todo esto ya tenemos la firma electrónica

- Técnicamente **al firmar se genera primero un hash** o resumen a partir del documento, fichero, mensaje firmado, que **posteriormente es cifrado**. Este cifrado se adjunta al documento junto con el certificado (clave pública) del firmante.
- Para comprobar la firma se genera de nuevo este código hash. Se usa la clave pública para descifrar el código hash enviado y se comprueba si coinciden ambos. Si es así, no hay duda que el documento ha sido firmado por el firmante.

Firma electrónica



Firma electrónica



¿Qué necesito para hacer una firma electrónica?

- Un certificado electrónico (FNMT, CatCert, DNIe, …)
- Una aplicación que me permita firmar:
  - Microsoft Office (word, excel, outlook)
  - Adobe Acrobat, PDFCreator (alternativa libre al Adobe Acrobat)
  - ecoFirma, intecofirma, valide.redsara.es, …

Validación de firmas

- Ya hemos visto implícitamente como se comprueba la firma.
- El receptor deberá hacer una **validación de firma**, pero ¿cómo lo hace el usuario?
  - La propia aplicación lo puede hacer:
    - Outlook comprueba automáticamente la firma de un correo electrónico
    - Adobe Acrobat
    - Word

Validación de firmas

- A veces recibiremos directamente un fichero *de firma,* son ficheros con extensión de archivo
  - .Xsig, .p7b, .p7c, .p7m, .p7s
  - Tendremos que recurrir a una utilidad que permita verificar, p.ej:
    - Online: valide.redsara.es
    - Instaladas en el PC: intecofirma, ecofirma (son libres y están hechas por la administración pública a disposición de los ciudadanos).

Código de verificación

- La mayoría de las veces el resultado de un trámite firmado electrónicamente es un resguardo donde no es operativo incluir el documento con la firma electrónica.
- El documento firmado queda custodiado por la administración que ha realizado el trámite.
- En este caso se emite un **código de verificación**, que no es más que un código (numérico o alfanumérico) que nos permite acceder al documento(s) que representa.

Código de verificación

- Ej. entregando la declaración de la renta por Internet, al final se obtiene un resguardo de entrega donde se incluye una coletilla del tipo: *"La autenticidad de esta declaración puede ser comprobada mediante el Código Seguro de Verificación DA9F4014B2D867E9 en https://www.agenciatributaria.gob.es"*
- Accediendo al servicio y completando los datos se obtendría una copia de la declaración de la renta entregada en dicho trámite:

Sello de tiempo

- Es una firma electrónica donde el mensaje es una fecha y hora.
- Lo normal es que la hora esté servida por un servidor de tiempo que está sincronizado con la hora oficial.
- Sirve para demostrar de forma fehaciente que un hecho electrónico se ha producido en un determinado momento.
- Ej. Publicación fehaciente en el Perfil del Contratante, art. 42.3 de la LCSP *(El sistema informático que soporte el perfil de contratante deberá contar con un dispositivo que permita acreditar fehacientemente el momento de inicio de la difusión pública de la información que se incluya en el mismo).*

Firma electrónica: práctica

- Firmar un documento y enviárselo a un compañero.
- Con Word 2007
  - Botón de Office -> Preparar -> Agregar una firma digital
- Con Word 2003:
  - Menú Herramientas/Opciones/Pestaña Seguridad
- Enviar el documento a un compañero para que compruebe la firma
- Intentar modificar el documento firmado, ¿qué ocurre?

Firma electrónica: práctica

- Con ecoFirma o IntecoFirma
  - Descargar ecoFirma o IntecoFirma e instalarlo en el PC
  - Firmar un documento
  - Enviar a un compañero, validar el documento y agregar una segunda firma
- **De forma online:** http://valide.redsara.es

Índice

1. DNI
2. Firma electrónica
3. Seguridad de la información en la eAdmin
4. Interoperabilidad

Seguridad en eadmin

- Si se compara la eAdmin con la problemática general de las TIC en el sector privado, la diferencia más característica es la **necesidad de mantener en todo momento las mismas garantías de seguridad jurídica de las actuaciones administrativas en papel** en el plano de la tecnología.
- El marco legal de la eAdmin concentra su mayor peso en las problemáticas en torno a la seguridad jurídica.
- La seguridad jurídica está apoyada por la tecnología empleada.

Seguridad en eadmin

- Conceptos principales en torno a los cuales gira esta problemática:
  - Identificación
  - Autenticación
  - Integridad de la información
  - Confidencialidad de la información
  - Disponibilidad de la información y los servicios
  - Trazabilidad
  - Conservación de la información

Seguridad en eadmin: Identificación

- **Identificación: la correcta identificación de remitente y destinatario.**
- **Se refiere principalmente a que los** datos de identidad estén completos de modo que no pueda haber ambigüedad a la hora de establecer la identidad de una persona física o jurídica.

Seguridad en eadmin: Autenticación

- La **garantía de conocer fehacientemente la identidad** de una persona física o jurídica.
- Este concepto guarda una estrecha relación con el **no repudio** (imposibilidad de rechazar la autoría de una determinada acción o documento).
- La **principal herramienta** para la autenticación son sistemas de usuario/clave y la **firma electrónica**. Ambos mecanismos permiten asimismo el no repudio.

Seguridad en eadmin: Integridad de la información

- Se refiere a que se puede **confiar** en que una determinada **información**, por ejemplo, de un documento electrónico, **no fue manipulada** y corresponde a su estado original.

Seguridad en eadmin: Confindencialidad

- Guardar el secreto frente a terceros sobre una determinada información, ya sea un documento, comunicación, etc.
- La principal herramienta para lograr este objetivo es la criptografía.
- Un acceso web **https** nos indica que la información se está transmitiendo de forma cifrada, nadie entre nuestro ordenador y el servidor podrá entender la información si la intercepta.

Seguridad en eadmin: Disponibilidad inf. y servicios

- Se refiere a que la información y/o servicios estén disponibles en todo momento. Esto implica normalmente servicios de alta disponibilidad 24x7, servidores redundantes, centros de respaldo, etc.

Seguridad en eadmin: Trazabilidad

- Se refiere a la información histórica que es importante conocer y conservar, ¿qué cambios ha sufrido la información?, ¿quién ha accedido a ella?, etc.

Seguridad en eadmin: Conservación de la información

- La **correcta conservación y archivo** de la información de modo que se encuentre disponible e íntegra, aún después de que hayan pasado **largos periodos de tiempo**.

Seguridad en eadmin: tecnologías

- Certificados, sellado de tiempo y firma electrónica:
  - Nos dan garantías de identificación, autenticación, integridad, confidencialidad
- Protocolo https:
  - Es un cifrado de datos mediante un certificado de servidor .
  - Garantiza la confidencialidad en la transmisión de información entre el servidor y nuestro navegador

Seguridad en eadmin: tecnologías

- Gestores documentales:
  - Permiten el versionado y control de acceso a la información, garantizando la **conservación y trazabilidad**.
- Firma longeva:
  - La firma electrónica puede llegar a *caducar* con el tiempo, bien porque la tecnología ha avanzado tanto que puede comprometer la criptografía de la firma o por problemas con la validación de certificados caducados.
  - Para evitar esto se **re-firma** cada cierto tiempo de forma automática, creando una cadena de firmas que permiten validar a futuro.
  - Ej. Actas electrónicas han de custodiarse al menos por 30 años. Los certificados con que se firman caducan a los 5 años de haberse emitido.
  - Esto asegura la **conservación a largo plazo.**
- **…**

Esquema Nacional de Seguridad

- **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica**, tiene como objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por **principios básicos** y **requisitos mínimos** que permitan una protección adecuada de la información.

Esquema Nacional de Seguridad

- **Principios básicos:** la **seguridad integral**, la **gestión de riesgos**, la **prevención**, **reacción y recuperación**, las **líneas de defensa**, la **reevaluación periódica**, y la **función diferenciada** por la cual se entiende que en los sistemas de información se diferenciará el **responsable de la información**, el **responsable del servicio** y el **responsable de la seguridad**.
- Además incluye en las **dimensiones de seguridad** a tener en cuenta a la **trazabilidad** de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Esquema Nacional de Seguridad: política de seguridad (1/2)

- **Requisitos mínimos**, se establece que **todos los órganos superiores de las Administraciones públicas** deberán disponer **formalmente** de su **política de seguridad**, que incluirá:
  - **Organización** e **implantación** del **proceso de seguridad**, que deberá comprometer a todos los miembros de la organización.
  - **Análisis y gestión de los riesgos**.
  - **Gestión de personal**, donde destaca el hecho que **todo** el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.
  - **Profesionalidad**.
  - **Autorización y control de los accesos**.
  - **Protección** de las **instalaciones.**

Esquema Nacional de Seguridad, política de seguridad (2/2)

•**Adquisición de productos** en la que se valorarán positivamente los productos certificados.
•**Seguridad por defecto**, es decir, los sistemas deben diseñarse y configurarse de forma que garanticen, al menos, unos mínimos de seguridad por defecto.
•**Integridad** y **actualización** del sistema.
•**Protección** de la **información almacenada y en tránsito** donde se presta especial atención a los así considerados **entornos inseguros** que son los **equipos portátiles**,**PDAs**, **dispositivos periféricos**, **soportes** de información y **comunicaciones sobre redes abiertas** o con **cifrado débil**.
•**Prevención ante otros sistemas** de información interconectados, se ha de proteger el perímetro, en particular, si se conecta a redes públicas como Internet.
•**Registro de actividad**. Este requisito está orientado sobre todo a garantizar la protección de los derechos relacionados con la protección de datos personales.
•**Incidentes** de seguridad.
•**Continuidad** de la actividad, que se logra fundamentalmente mediante unas políticas adecuadas de copias de seguridad y de respaldo.
•**Mejora continua** del proceso de seguridad.

Esquema Nacional de Seguridad

•Se abordan también cuestiones muy concretas, cuestiones como las condiciones técnicas de seguridad en las **comunicaciones electrónicas**, requerimientos de seguridad en las **notificaciones**, **publicaciones electrónicas** y **firma electrónica**, detalles relativos a la realización de **auditorias de seguridad** o los **informes del estado de seguridad** y se explicita que los **registros electrónicos** y las **sedes electrónicos** se encuentran sujetas a las previsiones de este Real Decreto.

Índice

1. DNI
2. Firma electrónica
3. Seguridad de la información en la eAdmin
4. Interoperabilidad

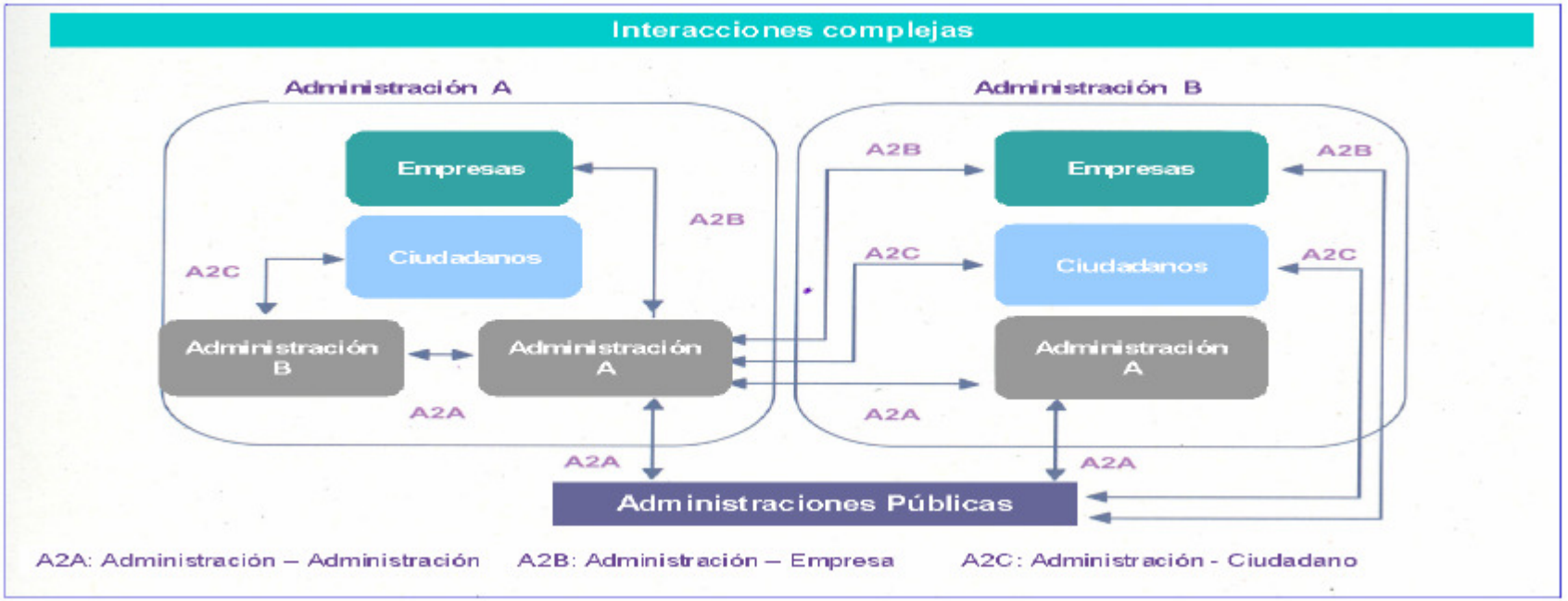
Interoperabilidad

Se entiende por **interoperabilidad** la **capacidad** de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de **compartir** datos y posibilitar el **intercambio** de información y conocimiento entre ellos.

Ley de acceso electrónico de los ciudadanos a los servicios públicos, Anexo, Definiciones.

Interoperabilidad: complejidad

Distintos actores en distintas administraciones, con distintas organizaciones, con distinta organización y procesos, con distintas estructuras de datos y con distintas soluciones tecnológicas arquitecturas e implementaciones



Esquema Nacional de Interoperabilidad

▪Artículo 42 Ley 11/2007. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

1.El Esquema Nacional de Interoperabilidad **comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad**.

2.El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

3.Ambos Esquemas se elaborarán con la participación de todas las Administraciones y se aprobarán por Real Decreto del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local, debiendo mantenerse actualizados de manera permanente.

4.En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos efectos considerarán la **utilización de estándares abiertos** así como, en su caso y de forma complementaria, **estándares que sean de uso generalizado por los ciudadanos**.

Esquema Nacional de Interoperabilidad

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.
- Persigue la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad **técnica, semántica y organizativa** de los sistemas y aplicaciones empleados por las Administraciones Públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

Esquema Nacional de Interoperabilidad: nivel técnico

- **Principio de neutralidad tecnológica** de la **Ley 11/2007** en aspectos concretos como los **documentos electrónicos** emitidos por las Administraciones Públicas y se reitera su importancia haciendo hincapié en el uso de estándares abiertos a todos los niveles considerando su aplicación particularmente **inexcusable** en la relación con los ciudadanos. Se introduce además el criterio de ***coste que no suponga una dificultad de acceso*** para la selección de estos estándares y se provee una definición de ***uso generalizado por los ciudadanos***.

Esquema Nacional de Interoperabilidad: nivel semántico

- Se centra fundamentalmente en la creación y publicación, en su momento, a través del **Centro de Interoperabilidad Semántica de la Administración** de unos **modelos de datos de intercambio** que serán de preferente aplicación para el intercambio de información entre las Administraciones públicas.

Esquema Nacional de Interoperabilidad: nivel organizativo

- Se centra, por una parte, en la **obligación** de las administraciones de la **especificación y publicación de los requisitos técnicos** de los **servicios, datos y documentos electrónicos puestos a disposición de otras administraciones** y, por otra parte, prevé la creación de **inventarios de información administrativa** a través de los cuales las administraciones han de publicar sus procedimiento administrativos y servicios.

ENI: medios de la AGE para facilitar la interoperabilidad

- **Red Sara** y el uso de **servicios horizontales** prestados por la Administración General del Estado (como lo puede ser **@Firma**) como medio para facilitar la interoperabilidad. Además se establece que la sincronización de la fecha y la hora se realizarán con el **Real Instituto y Observatorio de la Armada.**

ENI: interoperabilidad de firma

- Por definir **política de firma electrónica y de certificados**.
- Se definirán **formatos de firma**, los **algoritmos** a utilizar y **longitudes mínimas de las claves**, las **reglas de creación y validación de la firma electrónica**, la **gestión de las políticas de firma**, el **uso de las referencias temporales** y de **sellos de tiempo**, así como la **normalización de la representación de la firma electrónica en pantalla y en papel** para el ciudadano y en las relaciones entre Administraciones públicas.

ENI: recuperación y conservación del documento electrónico

- Se establecen las **condiciones** para la recuperación y conservación del documento electrónico que prevén, entre otras, cosas como la **definición de una política de gestión de documentos** por parte de las Administraciones públicas, la **identificación única e inequívoca de cada documento** o la **clasificación** de acuerdo con un **plan de clasificación**.

ENI: medidas de seguridad en conservación del documento electrónico

- Se reitera la obligación de la adecuada **protección de los datos personales** y se prevé el uso de formatos de **firma longeva** y otros mecanismos como **metadatos de gestión de documentos** que permitan la **conservación a largo plazo** de los documentos electrónicos.

ENI: formatos del documento electrónico

- Se prevén cosas como el uso preferentemente de formatos basados en **estándares abiertos** y la elección de **formatos de documento electrónico normalizados y perdurables** que aseguren la **independencia de los datos de sus soportes**. Incluso se prevé la posibilidad de **copiado autentico de los documentos** ante un posible riesgo de **obsolescencia del formato**.

ENI: digitalización de documentos en soporte papel

- La digitalización se deberá ajustar a la **norma técnica de interoperabilidad** correspondiente a los aspectos del **formato estándar utilizado**, el **nivel de resolución**, la **garantía de imagen fiel e íntegra** y los **metadatos asociados al proceso de digitalización**.