Crisis de Identidad (Gestión) (Parte 5): El Futuro de la Gestión de la Identidad - La identidad en la nube

|  |  |
| --- | --- |
| Enrique Dutra  MVP | Julio 2012 |
| Posee más de 20 años de experiencia en organizaciones de soporte de IT. Especializándose en seguridad y normalización en estándares COBIT, ISO 17799/27001, ISO 20000:2005, MOF e ITIL. Es Profesional 5 estrellas de Technet Ms., Miembro de Criptored y Culminis. Posee las Certificaciones MCSE - MCDBA - MCP - MCT 2011. Ha sido distinguido como MVP en Seguridad Windows por Microsoft desde el 2006 al 2011. Ha certificado como auditor ISO/IEC 27001:2005.  [Blog](http://seguridadit.blogspot.com.ar/) | |

## Introducción

De la 1ra a la 4ta parte de esta serie, echamos un vistazo a la evolución del concepto de "identidad", conceptos erróneos acerca de la identidad en el mundo de las TI, y algunas soluciones de identidad actuales, con un enfoque sobre la firma digital. También nos fijamos en los criterios para la elección de una solución integral de gestión de la identidad de una organización o una solución de gestión de identidad federada. En este sentido, en esta 5 parte, vamos a discutir el futuro de la gestión de identidades con un enfoque especial sobre el efecto de la nube en el IDM.  
 **Identificadores ID en línea**  
Allá en la primera parte, se discutió el problema de credibilidad a la hora de credenciales de identificación. A menos que la parte que emite las credenciales sea digno de confianza, esas credenciales no tienen sentido. Hoy en día la identidad en línea se verifica principalmente por certificados emitidos por las organizaciones del sector privado comercial, tales como VeriSign, Comodo, y muchos otros. Pero, ¿quién vigila a los vigilantes? Los nuevos proveedores de certificados SSL para sitios web deben someterse a auditorías de seguridad anual, como las que se realizan de acuerdo con el programa WebTrust para Autoridades de Certificación. El mercado de los certificados digitales personales es mucho más fragmentado.  
  
La mera existencia de un certificado digital no garantiza que las credenciales de identidad sean válidas. Algunos certificados son auto-firmado o auto-gestionados, lo que significa que la persona que emitió el certificado también garantiza su legitimidad - obviamente allí no hay controles y equilibrios en el sistema. Por otro lado, la auto-firma de certificados no disminuye la superficie de ataque, ya que no confían en su clave privada a un tercero (autoridad de certificación). Los certificados autofirmados se pueden crear con las herramientas de software, incluidas makecert.exe de Microsoft, Adobe Reader, Llavero de Apple y otros.  
En el mundo real, la mayor parte del crédito se da generalmente a los identificadores que son emitidos por el gobierno. Así, algunos ven un documento oficial de identidad en línea, como los medios más confiables de verificación de la identidad en línea, y el año pasado la Casa Blanca emitió un informe en su estrategia para lograr un sistema de identidades de confianza en el ciberespacio. Hay muchas cuestiones prácticas y políticas relativas a la creación de lo que efectivamente sería un documento nacional de identidad digital. Sin embargo, parece que el gobierno se mueve inexorablemente en esa dirección.  
  
Es probable que tal sistema sería voluntario - en un primer momento. La historia indica que esto eventualmente iba a cambiar. En la década de 1800, los conductores no estaban obligados a tener licencia. En la década de 1970, los niños no estaban obligados a tener número de seguro social. Hoy ambos están dispuestos por el gobierno.  
  
Pero hay algunas dudas en cuanto a exactamente un sistema de identificación del gobierno en línea iba a funcionar. ¿Estaría vinculada a su licencia de conducir o tarjeta de identificación del estado? Sin embargo, el gobierno federal no emitirá esos documentos (aunque con la Ley de Identificación Real, que ha tomado más autoridad sobre los estándares de procesos, con el fin de establecer que los estados lo requieran para su cumplimiento en el 2013). ¿Estaría ligado a su pasaporte, entonces? Pero ¿qué pasa con esas personas que no tienen pasaporte? Según las estadísticas a partir de enero del año pasado, menos del 40% de los estadounidenses tienen pasaporte. ¿Sería estar atado a su número de seguro social? Este es probablemente el número de identificación de mayor número de estadounidenses.  
  
Aunque el número de seguro social fue originalmente diseñado sólo para el propósito de seguir las cuentas de los individuos dentro del programa de Seguridad Social las cartas estaban marcadas, incluso "Por motivos de seguridad social - no para la identificación," las fuerzas armadas lo han utilizado en el lugar de números de servicio desde los años 60 (del Ejército y Fuerza Aérea) y 70 (Armada y los Marines). El número ahora es utilizado por algunos estados en lugar de número de la licencia de conducir. Los bancos, acreedores y empresas de servicios (tales como compañías de cable, teléfono y electricidad) requieren que los clientes proporcionen sus números de seguro social. El número de seguro social es utilizado por las agencias de crédito, compañías de seguros, agencias de aplicación de la ley y casi cualquier otra entidad que requiera la identidad de la persona.  
  
Estas preguntas son importantes porque, si el identificador de línea es un "independiente" forma de identificación, será mucho más difícil asegurar que un individuo no obtenga múltiples identificaciones en línea, o una identificación fraudulenta en línea que se asocia con otra persona o con un seudónimo. Eso sería negar el propósito para el cual están diseñadas las identificaciones oficiales.  
  
Si y cuando la multitud de cuestiones relacionadas con la forma de emitir identificaciones oficiales en línea se han resuelto, la siguiente pregunta es cómo, tecnológicamente, se llevará a cabo. ¿Una entidad de certificación administrado por el gobierno para validar la identidad de cada persona y emitir certificados digitales basados ​​en claves de pares público / privados? ¿Sería ilegal utilizar cualquier certificado, si no es el emitido oficialmente por el gobierno-para firmar los documentos, enviar correo electrónico o hacer negocios en línea? ¿Se convierten en ilegales para enviar mensajes, acceder a sitios web o de ejercer el comercio en línea sin un certificado? La naturaleza del gobierno es mantener la expansión de su autoridad, por lo que a pesar de que estos escenarios, podría parecer descabellada ahora, no es razonable suponer que un día todos puedan reflejar la realidad.

**La batalla por el espacio de la identidad**  
A pesar de inclinación del gobierno por el poder, debido a los engranajes de una enorme y lenta burocracia, probablemente no veremos un omnipresente obligatoria identificación oficial en línea (o tal vez cualquier tipo de documento oficial de identidad en línea), por un largo tiempo. Mientras tanto, las empresas de tecnología que han luchando durante años para convertirse en los principales proveedores de identidad, y están aumentando constantemente el alcance de sus sistemas de identidad propios mediante la aplicación de inicio de sesión único a través de diversos sitios y servicios.z  
  
Microsoft reinventa periódicamente su servicio, que originalmente fue llamado Microsoft Wallet, luego se convirtió en pasaporte y ahora va por el nombre de Windows Live ID. La compañía prevé Passport como un servicio que con el tiempo abarcaría todos los sitios de comercio electrónico, así como lugares propios Web de Microsoft, pero fue criticado por quienes temían su acceso a la información del cliente, y crearía problemas de privacidad. Hubo un tiempo una serie de sitios No-Microsoft, tales como eBay, utilizaba el servicio de Microsoft Passport para iniciar la sesión, pero ahora se utiliza para iniciar sesión en sitios de servicios de Microsoft como MSDN / TechNet, Hotmail, Xbox Live, Zune Marketplace, Messenger y otros servicios de Windows Live.  
  
Mientras tanto, Google se ha metido en el juego de la identidad hasta cierto punto, la vinculación de inicio de sesión a través de sus muchos servicios web. Su cuenta de Google se utiliza para conectarse a Gmail, Google Voice, YouTube, Picasa, Google Docs, Google Wallet sistema de pago móvil, la red social de Google + y otros. La compañía ha estado bajo fuego por sus recientes cambios de [política que ahora le permiten rastrear a los usuarios a través de sus múltiples productos y servicios](http://www.voanews.com/content/google-to-track-users-across-services-138064023/169431.html) y combinar la información del usuario de los diferentes servicios. La Comisión Europea ha propuesto nuevas normas destinadas a dar a los usuarios la posibilidad de optar por este tipo de rastreo.  
  
[Facebook, con su característica "Conectar",](http://techliberation.com/2011/01/09/facebook-as-identity-provider/) también se ha convertido en un proveedor de identidad. Esta característica permite a los usuarios iniciar sesión en otros sitios web fuera de Facebook, usando sus cuentas de Facebook.  
  
Un problema con todo esto está, que muchas personas mantienen más de una cuenta de Windows Live o Gmail porque necesitan varias direcciones correo electrónico para fines diferentes (tales como el hogar, el trabajo y "usar y tirar" - una dirección para entrar en los sitios web que requieren una pero que puede vender las direcciones a los spammers). En el caso de Windows Live, puedo configurar varias cuentas porque quería dos blogs independientes en el sitio del blog de ​​Windows Live (aunque Microsoft ha abandonado el esfuerzo y los usuarios se han trasladado a nuestros blogs de Wordpress). Incluso con Facebook, cuyos términos de servicio requieren que los usuarios sólo tengan una cuenta y para usar sus nombres reales, muchas personas violan esta norma y tienen cuentas separadas para trabajar y jugar.  
  
El otro problema es que cada empresa de alta tecnología tiene un servicio de identidad separado propio (y algunos otros selectos sitios y servicios), y nadie tiene "una identidad en línea para gobernarlos a todos." Si bien esto puede ser bueno desde un punto de vista de la privacidad punto, esto resulta en un tiempo más fácil para los terroristas, run-of-the-mill delincuentes cibernéticos, los spammers o estafadores, acechadores y otros que quieran ocultar sus identidades y/o hacerse pasar por otra persona en línea.   
 **La revolución móvil y la identidad**   
El uso de dispositivos móviles en teléfonos inteligentes generales y, en particular, se ha disparado en los últimos años. [De acuerdo con la firma de investigación Canalys, 488 millones de smartphones se han vendidos en 2011, más de la cantidad de computadoras y las tablets (alrededor de 415 millones](http://www.pcmag.com/article2/0,2817,2399846,00.asp)). Sus cifras muestran como esto aumentó del 62,7 por ciento respecto al año anterior. Las ventas de teléfonos inteligentes en base a las ventas del 2011, se espera que crezca otro 32% en 2012, según los analistas. Incluso Intel se está metiendo en el acto, haciendo equipos con Lenovo y Motorola para crear un teléfono basado en el procesador Atom.   
  
[Según un estudio de Kantar Worldpanel ComTech](http://www.guardian.co.uk/technology/2011/oct/31/half-uk-population-owns-smartphone), casi la mitad de la población del Reino Unido ahora es dueño de los teléfonos inteligentes. El verano pasado, investigadores de Pew estima que el 35 por ciento de los adultos estadounidenses tenían smartphones propios. Esto es cerca de 42 por ciento de todos los propietarios de teléfonos celulares.  
  
Con los teléfonos inteligentes en las manos de tanta gente, y ese número creciendo tan rápido, es lógico considerar la posibilidad de vincular las identidades de los usuarios de sus dispositivos móviles. Considerando que los números de línea fija fueron compartidos generalmente por familias enteras, los teléfonos móviles tienden a ser más personales, con cada miembro de la familia que tiene a su propio número de teléfono. Y con la portabilidad de números entre los transportistas, los usuarios de teléfonos móviles tienden a mantener el mismo número aunque cambien los equipos y los proveedores.  
  
Además, el teléfono móvil se ha convertido en un elemento que la mayoría de los propietarios llevan con ellos dondequiera que vayan, al igual que sus llaves o billeteras. De hecho, se predice que con el tiempo el teléfono móvil sustituirá a las dos cosas. Con Near Field Communications (NFC), que ya está siendo incorporado en los nuevos teléfonos inteligentes, se puede hacer un pago simplemente sosteniendo el teléfono cerca de un dispositivo de terminal para realizar la transacción de tarjeta de crédito. No hay tarjeta física, no es necesaria. NFC también podría ser utilizado como documento de identidad electrónico (en lugar de licencias de conducir o tarjetas de identificación) y se puede utilizar como tarjetas magnéticas electrónicas para abrir puertas o incluso, con la tecnología adecuada incorporado en vehículos, para iniciar los coches.  
  
El uso de los teléfonos inteligentes para proporcionar pruebas de identidad presenta algunos problemas que tendrían que ser resueltos. Obviamente, debe haber mecanismos de seguridad en el lugar para evitar que los delincuentes utilicen teléfonos robados para robar identidades y hacerse pasar por dueños de los teléfonos. Credenciales de necesitarían una fuerte encriptación y de inicio de sesión de teléfono, que tendrían que ser protegidos por contraseñas o números PIN o (preferiblemente) autenticación de dos factores (tales como escáneres de huellas dactilares).  
 **La identidad en la nube**  
El movimiento "en la nube" - para todos, desde los usuarios domésticos a las empresas - traen nuevos desafíos para la gestión de identidades. También trae una nueva necesidad y se centran en las mejores soluciones de identificación en línea. En el pasado, la seguridad de red se basaba en los límites de la seguridad, con todo lo que está dentro del perímetro de la red local se define como de confianza y todo lo que está fuera del perímetro considerado sin confianza. Los cortafuegos (firewall) en la red de "borde", fueron designados los centinelas que protegían a los usuarios y los recursos en el interior de aquellos que estaban en el exterior. Con el Cloud Computing, el borde está desapareciendo - o por lo menos se está haciendo extensible y elástico. Los problemas asociados con la identidad en la nube son complejos, tanto es así que hay grupos de trabajo y conferencias dedicados sólo a este tema.  
  
Las dos tecnologías que se establecen para dar forma al futuro de la informática son la nube y la computación móvil, y estos dos confluyen naturalmente ya que los usuarios cada vez tienen más acceso a servicios en la nube a través de dispositivos móviles. Las compañías que utilizan servicios en la nube tendrán que establecer las credenciales de raíz de confianza con el servicio de nube. Las organizaciones todavía quieren tener el control sobre sus políticas de seguridad, y deben ser capaces de asociarlos a los procesos de la nube habilitado para que las identidades y las autenticaciones se conserven cuando se correlacionan las transacciones de las nubes a través de límites de infraestructura. Exigen seguridad de punto final para la autenticación de usuario, así como seguridad en las transacciones de punto final de los servicios móviles.  
  
Soluciones en la nube de identidad se está trabajando por el hardware y las compañías de software, un ejemplo es la autopista de Intel Nube de acceso 360. Cualquier solución de este tipo tiene que ser compatible con las normas existentes Federados (SAML, OAuth, Open ID) y permitir que el cliente-a-nube de inicio de sesión único de los dispositivos móviles y ordenadores conectados a dos redes domésticas y corporativas. Supervisión, auditoría y aplicación de políticas son consideraciones importantes.  
  
Microsoft Windows Identity Foundation (WIF) es un SDK que los desarrolladores pueden utilizar en la construcción de la identidad de las aplicaciones conscientes de que se despliegue en la nube (así como las aplicaciones on-premise). Está construida sobre Active Directory Federation Services y Windows Azure servicios de acceso de control, que apoya OAuth 2.0. No es una extensión de WIF para SAML 2.0, también. WIF se basa en reclamos basados ​​en la identidad - es decir, los tokens de seguridad emitidos por un servicio de token de seguridad (STS), que contiene un conjunto de información sobre el usuario, junto con una firma digital. Basado en notificaciones de identidad se basa en el STS para autenticar al usuario, en lugar de tener que hacerlo la aplicación.  
  
Independientemente de la aplicación particular, autenticación de múltiples factores hacen que el manejo de la identidad en la nube mucho más segura, si la nube se accede desde los teléfonos inteligentes (como se mencionó anteriormente), de los ordenadores portátiles, tabletas, kioscos y computadoras públicas, televisores inteligentes, consolas de entretenimiento, o medios más exóticos (ordenadores portátiles, Internet habilitados para aparatos de cocina, etc). Es probable que conduzca finalmente a la biometría como una forma común de identificación.   
 **Resumiendo**   
En esta serie de cinco partes, hemos examinado las cuestiones relacionadas con el concepto de identidad, tanto históricamente como en su aplicación a la tecnología moderna y un mundo conectado a Internet. La identidad es un tema complejo, y las soluciones tecnológicas para la gestión de identidades pueden ser aún más. El propósito de este trabajo es señalar las complejidades de tratar con la identidad y para darle al lector una visión general de las soluciones disponibles en la actualidad, y lo que puede venir pronto al mercado en el futuro.   
  
  
Este artículo es de Deb Shinder, y fue traducido al español previa autorización de TechGenix Ltd. La versión original está en Windows Security y puede accederlo desde [aquí.](http://www.windowsecurity.com/articles/Identity-Management-Crisis-Part5.html)