

PKI, FIRMA DIGITAL

¿Para todos y para todo?

Carlos Müller - Gerente Comercial - Sitepro

Dada la reciente publicación en el Boletín Oficial del decreto que establece el marco normativo sobre la Ley de Firma Digital en Argentina, han de resurgir sin duda muchos proyectos archivados y con ellos la necesidad de llevar a la práctica implementaciones de esquemas donde se utilicen Certificados Digitales para dar seguridad a distintas transacciones críticas, y para identificar a los actores que participen de las mismas.

La Ley de Firma Digital y su marco normativo son, sin duda, el puntapié inicial a tener en cuenta en todo proyecto de PKI (Public Key Infrastructure), pero hay que tener presente que el simple hecho de utilizar Certificados Digitales no es una “solución en sí misma”, pues hay que contar con tecnologías adecuadas para proteger los Certificados Digitales contra ataques que puedan provocar el robo estas “identidades virtuales”.

Está probado matemáticamente que los esquemas de PKI son seguros, siempre y cuando se mantengan protegidos los Certificados Digitales, la Clave Pública y la Clave Privada (esta última principalmente) de todas las partes que intervengan en dichos esquemas. De nada sirve utilizar claves de 1024 o 2048 bits si luego se terminan almacenando en la PC protegiéndolas con una simple password. La Ley de Firma Digital en Argentina no “exige” ningún dispositivo especial para garantizar la seguridad de los Certificados



Digitales, las Claves Públicas y Privadas de los usuarios, tal como lo hace la legislación chilena por ejemplo, que para lo que ellos denominan “Firma Digital Avanzada” (que se utiliza para operaciones bancarias, entre otras aplicaciones críticas) exigen el uso de dispositivos criptográficos que garanticen la generación y almacenamiento seguro del par de claves, sin posibilidades de que sea extraída de estos dispositivos la Clave Privada, es decir piden que se cumpla con la Norma FIPs 140-2 Nivel 2. En la Argentina, en cambio, sólo se plantea que “los certificadores licenciados deberán informar a todo solicitante, previo a la emisión de

los correspondientes certificados, la política de certificación bajo la cual serán emitidos, sus condiciones y límites de utilización, condiciones de la licencia obtenida y todo aquello que fuere relevante con relación a un uso correcto y seguro de dichos certificados”.

Lo que sí queda claro en la Ley Argentina es la “exigencia” de la protección de las “claves raíces” de las “Autoridades de Registro o Certificantes”, donde se requiere el uso de dispositivos criptográficos para su “generación y almacenamiento”, que cumplan con la Norma FIPs 140-2 Nivel 3, siendo para ello necesaria la implementación de dispositivos

HSM (Hardware Security Module) como los LUNA SA de Safenet. Lo que sin duda implica importantes inversiones para cumplir con este requisito y otros que tienen que ver con el "acceso físico" a los lugares donde se encuentran estos dispositivos y los servidores principales involucrados en los esquemas de PKI.

Es importante entender que para poder "ampararse" en la Ley de Firma Digital se deben cumplir todos sus requisitos, y sin duda esto difícilmente se logre en un cien por ciento, aún luego de pasado el tiempo suficiente para que se logre ir depurando los detalles poco claros que existen en toda nueva tecnología.

También hay que tener en cuenta que en toda implementación de seguridad existen distintos niveles de requerimientos, y por lo general para la mayoría de los usuarios es suficiente implementar soluciones alternativas mucho más simples y menos costosas, y sólo para un grupo reducido, que realiza las operaciones más críticas, sería necesario utilizar mayores niveles de seguridad. Y tal como ha dicho Carlos Achiary, Director de la ONTI (el organismo responsable de PKI en la Argentina), en una nota periodística, "la firma digital hay que usarla donde es necesaria porque agrega complejidad" y "como toda medida de seguridad es cara e incómoda".

Adicionalmente a todo lo expuesto hay que ser conscientes que nada ha cambiado la realidad de Argentina, y Latinoamérica en general, sobre la falta de presupuesto para implementar esquemas costosos como los de PKI, y por lo general los proyectos que utilizan estas tecnologías al ser elevados por la gente de seguridad informática a los directivos de las empresas, o a la gente que manejan las finanzas, terminan en un "mejor dejemos este gasto para el siguiente presupuesto", pues nadie lo ve como lo que es realmente, una inversión.

Por ello para ciertas soluciones donde la escala del proyecto no permita amortizar la inversión necesaria para montar un esquema de PKI, no se debe olvidar analizar otras alternativas más "viables" para nuestra realidad regional, y entender que es preferible no seguir usando "usuario y password" mientras nos aprueban el presupuesto de inversión para estas tecnologías, y avanzar lo antes posible con otras alternativas que nos permitan estar mejor posicionados y no dejar siempre para el mañana todos los proyectos de seguridad que existen en nuestras empresas.

En la gran mayoría de las instalaciones o aplicaciones donde se necesita una "validación fuerte de acceso de usuarios", se puede implementar un "acuerdo entre partes" respecto a los elementos que se utilizarán para esta validación, con lo cual se podría optar por las opciones más simples de implementar y de menor costo, pues lo más importante, en definitiva, es este "acuerdo entre partes" que se va a firmar. ●

Links Relacionados

Link sobre la Normativa:

<http://infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=125115>

Link con Texto Completo:

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/125115/norma.htm>

Link a los ANEXOS:

<http://infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/125115/decadm6-2007-anexo.pdf>



La tranquilidad de saber que alguien lo hace para usted...

▼ Servicios Transistemas, la solución concreta para todas las necesidades de servicios tecnológicos que su empresa pueda requerir.

Soluciones en Servicios de Networking + IT

Servicios Básicos:

- Instalaciones
- Servicio Técnico de Mantenimiento (telefónicos & en sitio)

Otros Servicios:

- Cableado Estructurado
- Capacitación

Servicios Avanzados:

- Consultoría
- Maqueta de Prueba
- Diagnóstico de Redes
- Health Check
- Fine Tuning
- Arquitecturas de Almacenamiento
- Ayuda a la explotación
- Servicios Gestionados

Guiamos el futuro de las soluciones tecnológicas.

Av. Leandro N. Alem 855 - Piso 25 / C1001AAD - Buenos Aires - Argentina

Teléfono: 54 11 4590 3600 / Fax: 54 11 4590 3601

info@transistemas.com.ar