Resolución 45/1997, de 17 de marzo, establece pautas técnicas para elaborar una normativa sobre firma digital. Infraestructura de Firma Digital y Documento Electrónico

17 - 3 - 97

VISTO el Decreto Nº 660 del 24 de Junio de 1996, el Decreto Nº 998 del 30 de Agosto de 1996, el Acta de fecha 30 de Diciembre de 1996 del SUBCOMITE DE CRIPTOGRAFIA Y FIRMA DIGITAL, integrante del COMITE DE USUARIOS DE PROCESAMIENTO DE IMAGENES (C.U.P.I.), y

CONSIDERANDO:

Que dentro de las acciones asignadas a la competencia de la SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS, se encuentran las de promover el estudio y el análisis del valor legal de los documentos electrónicos y el de los sistemas tendientes a resguardar la seguridad y la privacidad de la información contenida en medios electrónicos, como así también las de proponer las medidas y dictar las normas que promuevan el perfeccionamiento de la organización y el adecuado funcionamiento de la Administración Pública Nacional.

Que en virtud de la competencia atribuida por el Decreto Nº 660/96, modificado por el Artículo 2º del Decreto Nº 998/96, la Dirección Nacional de Coordinación e Integración Tecnológica de la SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS ha participado en el Subcomité de Criptografía y Firma Digital, creado en Julio de 1996 e integrado por funcionarios de distintos organismos de la Administración Pública Nacional, cuya misión ha sido analizar y proponer medidas relacionadas con la incorporación de la tecnología de firma digital a los procesos de información del sector público, y los aspectos legales vinculados.

Que como resultado de dicho análisis, se elaboró el documento por el cual se aprobaron las conclusiones finales acerca de las pautas técnicas a tener en cuenta en una normativa de firma digital, que figura en el Anexo a la presente, el que debe ser utilizado como base fundamental para una normativa útil y eficiente para la difusión del empleo de la firma digital en el sector público.

Que la Administración Pública Nacional no puede permanecer ajena a los avances tecnológicos y al empleo de los nuevos medios que provee el mercado, especialmente cuando contribuyen a aumentar la productividad de sus organismos, a optimizar el manejo de la información y reducir los costos de almacenamiento y el traslado de papel.

Que la tecnología necesaria para otorgar seguridad a los documentos digitales, así como el intercambio de información digital, se encuentra actualmente disponible, habiendo alcanzado un razonable grado de confiabilidad y seguridad.

Que resulta conveniente brindar el marco normativo que favorezca el empleo y difusión de aquellas tecnologías en el ámbito de la Administración Pública Nacional.

Que es competencia de la SECRETARIA DE LA FUNCION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS, dictar el marco regulatorio para el establecimiento de las políticas sobre tecnologías referidas a informática, teleinformática, tecnologías multimedios, instalaciones y comunicaciones asociadas y otros medios y sistemas electrónicos, conforme a lo establecido en el Anexo II del Decreto Nº 660/96, modificado por el Artículo 2º del Decreto Nº 998/96.

Por ello,

LA SECRETARIA DE LA FUNCION PUBLICA DE LA JEFATURA DE GABINETE DE MINISTROS RESUELVE:

ARTICULO 1 . ➦

Adherir y adoptar como propias las conclusiones aprobadas mediante el acta de fecha 30 de Diciembre de 1996 por el SUBCOMITE DE CRIPTOGRAFIA Y FIRMA DIGITAL DEL COMITE DE USUARIOS DE PROCESAMIENTO DE IMAGENES (C.U.P.I.), y que como Anexo es parte integrante de la presente Resolución.

ARTICULO 2. ➦

Autorizar al empleo en el ámbito de la Administración Pública Nacional de la tecnología enunciada en el Anexo aludido en el artículo precedente, para la promoción y difusión del documento y firma digitales, en los términos y con los alcances allí definidos.

ARTICULO 3. ➦

Comuníquese, publíquese conjuntamente con su Anexo, dese a la Dirección Nacional de Registro Oficial y archívese.

NORMATIVA SOBRE FIRMA DIGITAL. ➦

De las autoridades certificantes de claves públicas y de los certificados de clave pública

La autoridad certificante de claves públicas certifica la correspondencia entre una clave pública y la persona física o jurídica titular de la misma, mediante la emisión de un certificado de clave pública. Este certificado permite identificar inequívocamente al firmante del documento digital, evitando así la posibilidad del repudio.

Consecuencias de la omisión del requerimiento de autoridades certificantes de claves públicas y de certificados de clave pública: Al no poder asociar una clave pública con su titular, no sería posible identificar inequívocamente al firmante de un documento digital, por lo que el documento sería repudiable y el sistema carecería de confiabilidad.

Aspectos a tener en cuenta para elaborar la normativa:

En cuanto a las autoridades certificantes:

- Enunciar los requisitos que debe reunir una entidad para actuar como autoridad certificante.
- Establecer las causales de revocación o suspensión de la licencia de una autoridad certificante.
- Establecer en todos los casos la publicidad de sus procedimientos de modo de permitir su conocimiento por terceros.
- Establecer las bases de control a través de auditorías, a fin de evaluar la gestión de las autoridades certificantes.
- Determinar los alcances de la responsabilidad por la actuación de las partes involucradas (autoridades certificantes, titulares de pares de claves, y organismos de contralor).

En cuanto a los certificados de clave pública:

- Enunciar los requisitos de normalización de acuerdo a estándares internacionales.
- Determinar las condiciones de vigencia de los certificados de clave pública (emisión, aceptación, revocación, suspensión y expiración).
- Establecer los derechos y obligaciones del suscriptor y de la autoridad certificante emisora.
- Establecer los requisitos de publicación de los certificados y las listas de certificados revocados o suspendidos.

Justificación de mencionar en la normativa a un único mecanismo de firma digital:

El objetivo en la redacción de una normativa de esta especie debe ser el contemplar estándares tecnológicos de mínima que aseguren la determinación de la autoría de la firma digital y la inalterabilidad del contenido del documento digital así suscripto.

La propuesta de utilizar criptografía de clave pública no es restrictiva por las siguientes razones:

- Aunque en el futuro se desarrollen otros mecanismos para implementar firmas digitales, las futuras normativas que los implementen no tienen necesariamente que invalidar el de clave pública, de la misma manera que la normativa que se propone no invalidará la utilización de la firma ológrafa.
- Una normativa de este alcance no debe hacer referencia a una tecnología en particular. El mecanismo de clave pública no es una tecnología, sino una familia de métodos matemáticos (algoritmos) que admiten distintas implementaciones tanto en hardware como en software. De la misma manera, la implementación de la firma ológrafa no se relaciona con el tipo de papel utilizado.
- El requerimiento de clave pública no es restrictivo puesto que especifica a una familia de algoritmos criptográficos y no a uno en particular, permitiendo la utilización posterior de nuevos algoritmos mas eficientes a medida que sean descubiertos y probados.
- Los mecanismos criptográficos simétricos por su naturaleza, requieren que la misma clave secreta sea utilizada para encriptar como para desencriptar un documento. Al necesariamente tener que compartir la clave secreta, la misma deja de serlo por lo que cualquier documento digital, "firmado" digitalmente por medio de un mecanismo criptográfico simétrico, sería pasible de repudio. De hecho no existe ninguna posibilidad lógica de implementar la firma digital basada en mecanismos criptográficos simétiricos. Como consecuencia, para evitar el problema del repudio, en 1977 se idearon los mecanismos criptográficos asimétricos (también denominados "de clave pública") que emplean DOS (2) claves distintas pero íntimamente relacionadas: la clave privada, que se mantiene secreta, nunca se divulga y se utiliza para firmar documentos digitales, y la clave pública que se publica y se utiliza para verificar las firmas basadas en la correspondiente clave privada.

- El Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la Asociación de Abogados de los E.E.U.U. ("Information Security Committee, Science and Technology Section, American Bar Association") en su Normativa de Firma Digital recomienda la utilización del mecanismo de clave pública como única alternativa para otorgarle a la firma digital el tratamiento de la firma ológrafa. Dicho Comité está integrado por representantes de los siguientes organismos gubernamentales :

    - Canada Department of Justice (Departamento de Justicia de Canadá) Justice
    - Commonwealth of Massachusetts (Estado de Massachusetts, EE.UU:) Justice
    - Georgia Secretary of State Office (Secretaría de Estado de Georgia, EE.UU.) Justice
    - Government of Quebec (Gobierno de Quebec, Canadá) Justice
    - Los Angeles County (Condado de Los Angeles, California, EE.UU.) Justice
    - NASA North American Space Administration (Administración Norteamericana del Espacio) Justice
    - NSA National Security Agency (Administración Nacional de Seguridad, EE.UU.) Justice
    - State of Utah (Estado de Utah, EE.UU.) Justice
    - U.S. Department of State (Departamento de Estado EE.UU.) Justice
    - U.S. Postal Inspection Service (Servicio de Inspección Postal, EE.UU.) Justice
    - U.S. Social Security Administration (Administración de la Seguridad Social de los EE.UU.) Justice
    - Utah Attorney General´s Office (Fiscalía del Estado de Utah, EE.UU.) Justice y de las siguientes instituciones:

    - American Society of Notaries Public (Sociedad Americana de Notarios Públicos)
    - Chambres des Notaries du Quebec (Cámaras de Comercio de Quebec, Canadá)
    - Fedération Nationale des Chambres de Commerce et d'Industrie de Belgique (Federación Nacional de Cámaras de Comercio y de Industria de Bélgica)
    - International Law Institute (Instituto Internacional de Leyes)
    - International Union of Latin Notaries- Italy (Unión Internacional de Notarios Latinos - Italia)
    - National Notary Association (Asociación Nacional de Notarios, EE.UU.)
    - Notaries Society of England (Asociación de Notarios de Inglaterra)
    - Society of Public Notaries of london (Asociación de Notarios Públicos de Londres, Inglaterra)
    - U.S. Council for International Business (Consejo de Comercio Internacional de los EE.UU.)
    - Université de Montréal (Universidad de Montreal, Canadá).
    - University of Miami Law School (Universidad de Derecho de Miami, Florida, EE.UU.)
    - Múltiples estándares internacionales de firma digital requieren el mecanismo de clave pública.
    - El mecanismo de clave pública tiene amplia difusión y no está relacionado con ningún proveedor o país en particular.

CONCLUSIONES

La normativa sobre firma digital permitirá:

- la digitalización de cualquier circuito de información,
- la generalización de la utilización de firma digital a través de la adopción de pautas uniformes que permitan verificar la autenticidad e integridad de los documentos

digitales que requieran firma para su validez, y
- un menor riesgo de fraude en los documentos digitales suscriptos digitalmente.

Anexo. Firma Digital - Aspectos Técnicos Relevantes ➦

La criptografía de clave pública utiliza un par de claves. Cada clave efectúa una transformación unívoca sobre los datos y es función inversa de la otra clave: sólo una clave puede "deshacer" lo que su par ha "hecho". El poseedor de una clave pública la da a conocer, manteniendo secreta su clave privada. Para enviar un mensaje confidencial, el autor lo codifica (encripta) con la clave pública del receptor. El mensaje encriptado de esa manera sólo puede ser decodificado (desencriptado) con la clave privada del receptor. En sentido inverso, el emisor puede codificar sus datos con su clave privada, o sea que la clave puede ser utilizada en ambas direcciones. Esta es la base de la "firma digital", ya que si un usuario puede desencriptar un mensaje con la clave pública de una persona, sólo esta última pudo haber usado su clave privada inicialmente para encriptarlo. Partiendo de que sólo el poseedor de la clave privada puede utilizarla, el mensaje encriptado se transforma en una firma digital, es decir un documento que ninguna otra persona pudo haber generado.

Una firma digital se crea aplicando un algoritmo de "hash" (proceso que permite obtener un mensaje de longitud menor a partir de un documento, siendo prácticamente imposible encontrar otro mensaje que genere el mismo resumen) sobre un mensaje de texto. El resultado de este proceso es un digesto o resumen. Luego se encripta el digesto con la clave privada del individuo que envía el mensaje, transformándolo en una firma digital. Esta firma sólo puede ser desencriptada con la clave pública del mismo individuo. El receptor del mensaje desencripta la firma digital y luego recalcula el digesto. Luego éste nuevo digesto es comparado con el digesto del mensaje contenido en la firma. Si ambos coinciden, se concluye que el mensaje no ha sido alterado. Al utilizar la clave pública del emisor para verificar la firma, se comprueba que el texto tiene que haber sido firmado con la clave privada conocida únicamente por el emisor. Este proceso de autenticación se incorporará en todas las aplicaciones consideradas seguras.

Los usuarios de estas tecnologías de firma digital generalmente anexan su clave pública al documento enviado, de manera tal que el receptor no necesita localizar dicha clave en un repositorio de claves públicas. Pero ¿cómo puede el receptor asegurarse de que esa clave pública, o inclusive del directorio público, pertenece realmente a la persona que dice poseerla? ¿Puede un tercero ingresar en la red como un usuario legítimo, esperando y observando como otros, sin saberlo, envían documentos sensibles y/o secretos a una cuenta falsa creada por ese impostor?.

La solución es el certificado de clave pública, una especie de "pasaporte" o identificador digital. El certificado (que contiene la clave pública del usuario) ha sido firmado por alguien confiable: una Autoridad Certificante. El notario público da sustento al proceso de claves públicas dando fe de la identidad del poseedor de la clave pública en la solicitud de aprobación del firmante.