NACIONAL

RESOLUCION 194/1998
SECRETARIA GENERAL DE LA FUNCION PUBLICA (S.G.F.P.)

Firma digital. "Estándares sobre tecnología de firma digital para la Administración Pública Nacional". Aprobación de los aludidos por el art. 6° del dec. 427/98.
del 27/11/1998; Boletín Oficial 04/12/1998

Artículo 1° - Apruébanse los estándares aplicables a la "Infraestructura de Firma Digital para el Sector Público Nacional" a que alude el Artículo 6° del Decreto N° 427/98 y Anexo I, los cuales se enuncian en el Anexo de la presente bajo la denominación "ESTANDARES SOBRE TECNOLOGIA DE FIRMA DIGITAL PARA LA ADMINISTRACION PUBLICA NACIONAL".
Art. 2° - Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.
Claudia E. Bello.

ANEXO
ESTANDARES SOBRE
TECNOLOGIA DE FIRMA DIGITAL PARA LA
ADMINISTRACION PUBLICA NACIONAL
Organismo Licenciante
Secretaría de la Función Pública
Noviembre, 1998
Versión 1.00
INDICE

3.2.5 - Revocación de un certificado de usuario
3.2.6 - Renovación de un Certificado
3.3 - Titulares de Certificados
4 - ESTANDARES TECNOLOGICOS
4.1 - Seguridad
4.1.1 - Algoritmos Criptográfico
4.1.2 - Almacenamiento de claves y certificados
4.1.3 - Generación del par de claves
4.1.4 - Usuarios
4.1.4.1 - Responsabilidades
4.1.5 - Autoridades Certificantes Licenciadas
4.1.5.1 - Auditorías
4.1.6 - Servicio de Directorio
4.1.7 - Seguridad Informática
4.1.8 - Seguridad física de los equipos
4.2 - Firma Digital
4.2.1 - Tecnología de Clave Pública
4.2.1.1 - Par de claves
4.2.1.2 - Firmas Digitales
4.2.1.3 - Algoritmos de Encriptado
4.2.2 - Certificados
4.2.2.1 - Tipos
4.2.2.2 - Datos Básicos
4.2.2.3 - Extensiones
4.2.2.4 - Formatos
4.2.2.5 - Identificación única
4.2.2.6 - Número de Serie
4.2.2.7 - Periodo de Validez
4.2.2.8 - Titular
4.2.2.9 - Emisor
4.2.3 - Solicitudes de Certificados
4.2.3.1 - Solicitud de una AC al OL
4.2.3.2 - Solicitud de un Titular a una ACL
4.2.3.3. - Certificados para Servidores
4.2.4 - Lista de Certificados Revocados (CRL)
4.2.5 - Tipos de dispositivos utilizados para almacenar las claves privadas
4.2.6 - Comunicación
4.2.6.1 - Comunicación segura en línea
4.2.6.2 - Formato de transferencia de Correo Electrónico (Email).
4.2.7 - Servicios de Directorio
4.2.8 - Otros servicios
4.2.8.1 - TimeStamp
4.2.8.2 - Key Recovery
4.2.8.3 - Servicios de notariado
A - INFORMACION
A.1 - Organizaciones Internacionales
A.1.1 - International Telecommunications Union
A.1.2 - Internet Engeneering Task Force (IETF) Working Group
A.1.3 - National Institute of Standards and Technology (NIST)
A.2 - Consideraciones generales
A.2.1 - Key Recovery
A.2.2 - Data Recovery
A.3 - Importancia de la Clave Privada en función de la jerarquía
A.4 - Medios de Almacenamiento
A.4.1 - Sobre Smart Cards - interoperabilidad

1 - INTRODUCCION

El presente documento describe las especificaciones técnicas, obligaciones y recomendaciones que deben seguir tanto el Organismo Licenciante (OL) como las Autoridades Certificantes Licenciadas (ACLs) para integrar la Infraestructura de Firma Digital de la Administración Pública Nacional (IFDAPN), tal como lo detalla el Decreto Nº 427/98 (en adelante "Decreto").

Este documento se encuentra complementado por la Política de Certificación (Serie B) y por los Procedimientos de Certificación (Serie C) que deben seguir todas las Autoridades Certificantes (ACs) para obtener una licencia por parte del OL, y que deben ser obedecidos para que dicha licencia no sea revocada.

Para la redacción del mismo se han tenido en cuenta lo determinado por el Decreto antes mencionado así como los estándares sobre la Tecnología de Firma Digital que han sido desarrollados por grupos internacionales de trabajo y organismos internacionales de estandarización.

Las recomendaciones presentes deben ser seguidas para la selección o implementación de los componentes de la IFDAPN frente a otras alternativas, salvo circunstancias particulares, las cuales deben ser sometidas a la aprobación de la Autoridad de Aplicación.

En el presente documento se enuncian obligaciones y recomendaciones que deben ser tenidas en cuenta por las ACLs con respecto a la seguridad informática de los equipos involucrados en la Infraestructura de Firma Digital. El Organismo Auditante (OA) evaluará el ambiente de control antes de producir un informe positivo que permita emitir el certificado correspondiente. La seguridad física, lógica y de operación y la selección del personal que participe en tareas relacionadas a las ACLs es tema de crucial importancia para la confiabilidad del sistema.

Los estándares tecnológicos, obligaciones y recomendaciones enunciados en el presente documento serán actualizados periódicamente para adecuarlos a los cambios emergentes de la tecnología y para su adaptación a los procedimientos involucrados en la Administración Pública Nacional, respetando el espíritu del decreto de formar un programa piloto para incorporar esta tecnología en la gestión pública.

Este documento forma parte de la Serie A de documentos emitidos por el Organismo Licenciante.

2 - CONSIDERACIONES

Los temas que se enuncian a continuación son considerados críticos para la redacción de los estándares y deben ser tenidos en cuenta como parámetro de evaluación de futuras modificaciones o agregados que sean necesarios.

2.1 - Ambito

El Decreto Nº 427/98 marca las obligaciones, necesidades y estructura general que deben cumplir las Autoridades Certificantes Licenciadas (ACLs), el Organismo Licenciante (OL) y los suscriptores o titulares de certificados (1). Dicha estructura es estática, sólo variable en la cantidad de ACLs y certificados emitidos por éstas. No existe interacción entre ninguna de estas Autoridades o el Organismo Licenciante con organizaciones del ámbito privado.

2.2 - Tecnología

Es importante que los estándares especificados en el presente documento sean apropiados, efectivos, maduros, de ágil disponibilidad y confiables y consistentes con aquellos que se encuentran ampliamente difundidos y que cuentan con aceptación internacional.

Por las características de esta tecnología, en ocasiones no es posible indicar estándares

emitidos por organismos de estandarización. Sin embargo, es posible encontrar grupos internacionales de trabajo que son los generadores de estudios previos a dichas normas. Parte de la documentación enunciada ha sido generada y es mantenida por dichos grupos.

2.3 - Seguridad

Para proveer a los usuarios de esta tecnología de un nivel apropiado de seguridad y confianza, es necesario que todos los elementos involucrados en el desarrollo y mantenimiento de la Infraestructura de Firma Digital de la Administración Pública Nacional (IFDAPN) exhiban un nivel verificado de seguridad acorde con estándares internacionales vigentes.

2.4 - Interoperabilidad

La interoperabilidad es uno de los aspectos cruciales que deben formar parte del objetivo de los estándares adoptados. Por tal motivo se enuncian los estándares tecnológicos que deben ser seguidos por todas las ACLs. Sin embargo, aquellos aspectos que no se encuentren contemplados deben ser consistentes con los conceptos presentes en 2.2 - Tecnología.

3 - INFRAESTRUCTURA DE FIRMA DIGITAL DE LA ADMINISTRACION PUBLICA NACIONAL (IFDAPN)

La IFDAPN se encuentra conformada por:

Organismo Licenciante (OL)

Organismo Auditante (OA)

Autoridades Certificantes Licenciadas (ACLs)

Suscriptores. Son agentes o funcionarios de los organismos de la Administración Pública Nacional. Es posible incorporar a ciudadanos que, mediante un acuerdo entre partes con el organismo emisor del certificado, acuerden utilizar esta tecnología para la firma de documentos digitales.

Otros componentes, tales como Autoridades Certificantes del ámbito privado o ciudadanos que no prestan funciones dentro de la Administración Pública Nacional, son tratados como externos a la IFDAPN, y no se encuentran alcanzados ni regulados por este estándar. Sin embargo, no se excluye la posibilidad de interactuar con ellos, siempre y cuando se tengan en consideración los aspectos enunciados en el presente documento.

Las ACLs pueden modularizar su operatoria creando Autoridades de Registración que realicen las tareas de recepción y verificación de las solicitudes. Estas entidades serán consideradas como parte de la ACL con la que operan y deben respetar los estándares y requisitos de seguridad exigidos para ella.

3.0.1 - Oficial certificador

El OL y cada ACL deben contar con uno o varios responsables que cumplen la función de Oficial Certificador, encargado de la clave privada. Su tarea es firmar los certificados emitidos por la ACL o por el OL, según el caso. También puede utilizar dicho par de claves para firmar las Listas de Certificados Revocados (Certificate Revocation Lists - CRLs) salvo que se haya dispuesto utilizar un par de claves distintas para esta tarea.

Esta responsabilidad puede ser dividida entre varias personas si los procedimientos utilizados por la ACL así lo requieren. De ser así, la clave privada puede ser dividida entre los responsables y requerir una cantidad mínima de ellos para realizar cualquier operación. Esta división puede ser llevada a cabo físicamente (división de la clave privada en tramos disjuntos) u operacionalmente (si el sistema utilizado requiere de todos los componentes para poder operar). En ambos casos debe indicarse en el Manual de Procedimientos de la ACL qué mecanismos son utilizados para llevar a cabo las tareas del Oficial Certificador.

3.1 - Organismo Licenciante

El OL es el encargado de emitir los certificados para las ACLs a fin de que éstas puedan operar dentro de la IFDAPN. Los procedimientos necesarios para obtener un certificado emitido por este organismo se encuentran detallados en el Manual de Procedimientos correspondiente y el tipo de certificado, datos relativos al mismo, y demás aspectos se encuentran en su Política de Certificación.

Es obligación del OL mantener el más alto grado de seguridad en sus procedimientos de acceso y acreditación de certificados, ya que de encontrarse comprometida su clave privada, se vería afectada toda la IFDAPN.

El Organismo Licenciante, en su rol de Autoridad Certificante de las ACLs de la Administración Pública Nacional, debe cumplir las mismas obligaciones que éstas en lo que respecta a la verificación de los datos de los certificados que emite, la revocación de los mismos y demás situaciones que tengan lugar en el ciclo de vida de un certificado.
El OL sólo se encuentra habilitado a emitir certificados a ACs, no a personas. Las garantías que el OL ofrece a las ACLs, así como las obligaciones y derechos que éstas tienen se encuentran detalladas en la Política de Certificación del OL.
Tanto los certificados emitidos como las Listas de Certificados Revocados (CRLs) deben encontrarse accesibles públicamente, y se debe ofrecer un servicio de directorio tal como se indica en 4.2.7 - Servicios de Directorio.
Asimismo, el OL está obligado a diseñar un plan de contingencias que permita la continuidad de sus servicios, circunstancia que debe estar prevista en su Manual de Procedimientos. Dicho plan debe ser aprobado por el OA.
3.1.1 - Certificado del OL
El OL posee un par de claves y un certificado autofirmado. Dicho certificado es público y debe encontrarse accesible en todo momento.
La clave privada es entregada al responsable o responsables de cumplir con la función de Oficial Certificador, y sólo será empleada para firmar los certificados emitidos a las ACLs y las CRLs correspondientes. Dichos responsables deben proteger dicha clave de accesos no autorizados utilizando los medios sugeridos en el presente documento (ver 4.1.2 - Almacenamiento de claves y certificados).
El certificado del OL cumple con los estándares enunciados en 4.2 - Firma Digital y cuenta con los siguientes atributos:

Titular	(CN)	Organismo Licenciante de la Administración Pública Nacional
Organización	(O)	Organismo Licenciante de la Administración Pública Nacional
Correo Electrónico	(EA)	certificador@pki.gov.ar
Localidad	(L)	Ciudad de Buenos Aires
Provincia	(P)	Buenos Aires
País	(C)	Argentina

El par de claves del OL es generada por el algoritmo RSA (Rivest Shamir Adleman) con una longitud (modulus) de 2048 bits (2) [PKCS#1].
El período de validez de dicho certificado es de 10 años a partir de su fecha de emisión.
El algoritmo de firma utilizado para firmar el certificado del Organismo Licenciante así como los certificados emitidos por éste es md5WithRSAEncryption.
3.1.2 - Sobre Autoridades Certificantes
Todas las ACs que deseen operar dentro de la IFDAPN deben cumplimentar los pasos indicados en Manual de Procedimientos del Organismo Licenciante, y someterse a los requisitos indicados en dicho manual.
Los certificados que se les emitan se encuentran regulados por la Política de Certificación correspondiente publicada por el Organismo Licenciante.
3.1.3 - Obtención de un certificado para una Autoridad Certificante
Una AC debe obtener un certificado emitido por el OL para poder operar dentro de la Administración Pública Nacional y lograr que los certificados emitidos por ella sean aceptados por cualquier otro titular o usuario dentro de la IFDAPN.
Los pasos que debe cumplimentar se encuentran detallados en el Manual de Procedimientos del OL y la política que rige al certificado emitido se encuentra descripta dentro de la Política de Certificación de dicho organismo. En 4.2.3.1 - Solicitud de una AC al OL se encuentran detallado el estándar tecnológico que deben seguir las solicitudes remitidas al OL.
3.1.4 - Revocación y Listas de Certificados Revocados (CRLs)
El OL debe proveer los medios técnicos necesarios para permitir que los responsables de las ACLs completen una solicitud de revocación. Debe garantizar la verificación de la

identidad del solicitante del requerimiento de revocación para impedir fraudes. Dicho procedimiento debe estar indicado en el Manual de Procedimientos del OL.
Los plazos que median entre la recepción de una solicitud de revocación y su efectivización deben ser lo más breves posibles. Dichos plazos se encuentran expresados en la Política de Certificación según el tipo de certificado. Los pedidos de revocación que vengan firmados digitalmente con la clave privada correspondiente al certificado a revocar deben ser aceptados de inmediato.
La revocación de un certificado debe ser seguida de la emisión de una nueva CRL que incluya el número de certificado revocado. Sin perjuicio de ello, el Manual de Procedimientos del OL indica la periodicidad con que deben emitirse las CRLs.
El OL tiene la obligación de mantener una copia de cada uno de las CRLs emitidas así como de los certificados emitidos.
3.2 - Autoridad Certificante Licenciada
Las Autoridades Certificantes Licenciadas (ACLs) están habilitadas para emitir certificados a agentes o funcionarios que se encuentren dentro de su ámbito de competencia. Para emitir dichos certificados debe obtener un certificado emitido por el OL cumplimentando los pasos descriptos en el Manual de Procedimientos de dicho organismo. Puede emitir certificados a personas que no se encuentran en su ámbito de competencia, indicando tal circunstancia en la Política de Certificación propia del tipo de certificado emitido.
Las ACLs no se encuentran habilitadas para emitir certificados a otras Autoridades Certificantes, sólo a personas. Para lograr que esta jerarquía se mantenga y no permita más niveles de los establecidos es necesario que las aplicaciones de ACLs soporten las extensiones de certificados diseñadas a tal efecto (ver 4.2.2.3 - Extensiones).
Las garantías que las ACLs ofrecen a los titulares de certificados emitidos por ésta, así como las obligaciones y derechos de estos últimos frente a la ACL se encuentran detallados en la Política de Certificación para cada tipo de certificado emitido.
Las ACLs deben mantener apropiados niveles de seguridad en sus redes de computadoras, sus instalaciones físicas y en el manejo de su clave privada (ver 4.1 - Seguridad). Para su operatoria deben mantener un nivel de servicios mínimo frente a sus usuarios tal como se detalla en 3.2.2 - Servicios mínimos.
3.2.1 - Certificado
La longitud del par de claves de una ACL debe ser de 2048 bits (RSA). Puede utilizarse una longitud menor siempre y cuando argumenten alguna necesidad particular, pero siempre debe ser igual o superior a 1024 bits (RSA).
Los certificados emitidos por una ACL deben cumplir los pasos indicados en su Manual de Procedimientos. Una ACL puede emitir diferentes tipos de certificados, cada uno con atributos propios y para ser utilizados en distintos aplicaciones o funciones, pero en todos los casos debe contar con un detalle de los procedimientos y con una Política de Certificación propia para cada tipo de certificado.
3.2.2 - Servicios mínimos
Una ACL puede ofrecer distintos servicios y mecanismos para recibir un requerimiento de certificado y para otorgar el mismo a su titular. Estos mecanismos se encuentran descriptos en detalle en el Manual de Procedimientos de la ACL, el cual ha sido aprobado por el OL y por el OA.
La recepción de solicitudes de revocación y la publicación periódica de la CRL, tal como lo estipula la Política de Certificación de cada tipo de certificado, son servicios obligatorios que debe ofrecer una ACL. Debe garantizar el acceso permanente a dichos servicios, proponiendo una solución para una eventual contingencia.
El plan de contingencias de una ACL debe ser aprobado por el OA a fin de emitir el informe necesario para poder ser certificada por el OL.
3.2.3 - Emisión de un Certificado a un usuario
Una Autoridad Certificante Licenciada debe redactar y publicar un Manual de Procedimientos y una Política de Certificación para cada uno de los tipos de certificados que emita, detallando los pasos que deben ser seguidos para la emisión de un certificado y las responsabilidades, derechos y demás aspectos relativos a la emisión.

Los manuales deben ser puestos a disposición del OL para que sean evaluados y aprobados antes de poder emitir un certificado.
En dichos manuales se deben contemplar:
Características del certificado a emitir, es decir, los atributos a ser incluidos, periodo de validez, longitud mínima de la clave a ser utilizada, algoritmos permitidos, etc.
Procedimiento de verificación de identidad del titular y de los atributos incluidos en el certificado.
Procedimiento para la revocación del certificado, así como personas legalmente autorizadas a solicitar dicha revocación.
Mecanismo de consulta de las CRLs emitidas y directorio de certificados.
3.2.4 - Obtención de un par de claves y de un certificado por parte del titular o suscriptor
A continuación se describen los pasos que un titular debe seguir para obtener un certificado. Dicho certificado debe ser emitido por una ACL para que sea válidamente aceptado en la IFDAPN.
Los pasos que un suscriptor debe seguir son:
1.- Generar un par de claves
El par de claves debe ser generado por un algoritmo aceptable y con una longitud mínima que garantice que no existen riesgos de que sea vulnerable. Estas especificaciones se deben encontrar detalladas en la Política de Certificación del tipo de certificado a ser solicitado.
El par de claves puede ser generado por distintos medios, como se indica más adelante, pero en ningún caso la ACL debe conocer ni tomar contacto con la clave privada.
2.- Remitir la clave pública con sus datos personales a la ACL y cumplimentar los controles necesarios para verificar su identidad.
Es obligación de la ACL cumplimentar los pasos indicados en el Manual de Procedimientos. Una vez aprobada la solicitud, se debe generar un certificado, remitirlo a su titular (o informarle que debe pasar a retirarlo) y publicarlo en un repositorio de certificados emitidos (Ver 4.2.7 - Servicios de Directorio).
3.- Retirar el certificado
Dependiendo de la aplicación y del formato de exportación del certificado, el titular del mismo incorporará dicho certificado en el medio de almacenamiento correspondiente.
3.2.5 - Revocación de un certificado de usuario
En todo momento el titular debe contar con la posibilidad de solicitar la revocación de su certificado. La ACL debe detallar en su Manual de Procedimientos los medios y pasos que debe seguir un usuario para solicitar la revocación, la cual no necesariamente será inmediata, ya que puede ser necesario verificar si el solicitante se encuentra habilitado a tal efecto. Una vez revocado, el certificado debe ser incluido en la CRL que periódicamente debe emitir dicha autoridad.
La revocación de un certificado debe ser seguida de manera inmediata de la emisión de una CRL que incluya el número de certificado revocado. El Manual de Procedimientos de la ACL debe indicar la frecuencia de emisión de las CRLs.
3.2.6 - Renovación de un Certificado
Las ACLs pueden ofrecer el servicio de renovación de certificados (tal como se indica en los estándares X.509 [PKIX1]). Este procedimiento debe encontrarse incluido en el Manual de Procedimientos.
La ACL, antes de renovar un certificado, debe recibir una solicitud de renovación por parte del suscriptor.
3.3 - Titulares de Certificados
Las Autoridades Certificantes Licenciadas (ACLs) emiten certificados para titulares.
Las obligaciones y derechos de dichos titulares de certificados se encuentran detallados en la Política de Certificación del tipo de certificado emitido.
Los titulares de los certificados deben cumplir con las indicaciones de la ACL a fin de proteger su clave privada de posibles compromisos. Tal como lo indica el Decreto Nº 427/98, es responsabilidad del titular "Mantener el control de su propia CLAVE PRIVADA e impedir su divulgación". Si la clave privada se ve comprometida debe iniciar la revocación del certificado correspondiente en forma inmediata. El resguardo de su clave

privada debe mantenerse aunque el certificado se encuentre expirado.
Un titular no debe utilizar su clave privada para firmar documentos si el certificado correspondiente se encuentra expirado.
Para los titulares de certificados se recomienda utilizar una longitud igual o superior a 1024 bits (RSA o DSA) , aunque nunca inferior a 512 bits (RSA o DSA). Una longitud de 512 bits (RSA o DSA) puede ser aceptada por una ACL siempre y cuando garantice un uso limitado de los certificados para aplicaciones no críticas y un periodo de validez corto (no superior a 1 año). Dicha longitud de clave no se encuentra comprometida en la actualidad y es posible su uso tal como se referencia en:
http://www.rsa.com/rsalabs/pubs/techreports/security_estimates.pdf
4 - ESTANDARES TECNOLOGICOS
En la presente sección se enuncian los estándares tecnológicos que deben cumplir los productos, instalaciones y protocolos que sean utilizados dentro de la IFDAPN.
Esta sección se compone de requisitos para obtener y mantener la licencia y de recomendaciones que pueden ser seguidas para lograr un mayor grado de compatibilidad en las aplicaciones de distintos organismos dentro de la Administración Pública Nacional. Las recomendaciones presentes deben ser seguidas para la selección o implementación de los componentes de la IFDAPN frente a otras alternativas, salvo circunstancias particulares, las cuales deben ser sometidas a la aprobación de la Autoridad de Aplicación.
4.1 - Seguridad
El nivel de seguridad requerido para una ACL es función de los tipos de certificados que emita, y se encuentra establecido en la Política de Certificación correspondiente a cada tipo. Dicho es evaluado durante la auditoría que el OA efectúa como requisito para el licenciamiento de la Autoridad Certificante solicitante.
4.1.1 - Algoritmos Criptográfico
Un aspecto crítico relacionado con la tecnología de firma digital y la seguridad es la selección de los algoritmos criptográficos empleados, tanto aquellos utilizados para firmar un documento como para mantener protegida la clave privada. En 4.2.1 - Tecnología de Clave Pública se enuncian los algoritmos estándar a utilizar dentro de la IFDAPN.
4.1.2 - Almacenamiento de claves y certificados
Las claves privadas de cada una de las entidades de la IFDAPN deben ser almacenadas en dispositivos que garanticen su integridad. Es prioritario, por lo tanto, emplear los medios necesarios para asegurar que dichas claves no sean comprometidas en ningún momento, es decir, que se encuentren protegidos frente a accesos indebidos por parte de otros usuarios o aplicaciones.
Los certificados del OL, o de las ACL que sean utilizados para la verificación de una firma deben ser almacenados en dispositivos que garanticen su integridad. Debe prevenirse la posibilidad de sustituir el certificado del OL por un certificado falso.
Es responsabilidad del titular de una clave privada y de una Autoridad Certificante Licenciada "Mantener el control de su propia CLAVE PRIVADA e impedir su divulgación" (Decreto Nº 427/98, Anexo I).
Si la clave de un usuario se ve comprometida, éste debe solicitar la revocación del certificado correspondiente de forma inmediata, siendo él mismo el principal perjudicado de ocurrir un ilícito. Sin embargo, si la clave comprometida corresponde a una ACL todos los certificados emitidos por ésta podrían verse comprometidos. Es natural entonces que se empleen mayores y mejores recursos para mantener segura la clave de una ACL que la de un usuario, dado que una habilita el uso de la otra. (ver A.3 - Importancia de la Clave Privada en función de la jerarquía)
Las claves privadas de las ACLs y de los suscriptores deben encontrarse siempre resguardadas por un mecanismo criptográfico simétrico que las proteja (ver 4.2.1.3 - Algoritmos de Encriptado). El formato de almacenamiento de la clave privada depende del dispositivo utilizado. En caso de ser necesaria su extracción del dispositivo, es necesario que el formato utilizado corresponda a alguno de los estándares enunciados. Sin embargo, es recomendable utilizar dispositivos que no requieran su extracción y que realicen las operaciones criptográficas dentro de los mismos.

Es recomendable emplear el mayor grado de seguridad en la selección del algoritmo, en la longitud de la clave, en el medio de almacenamiento de la clave privada y en la implementación de los algoritmos empleados. Sin embargo no todos los documentos firmados o las aplicaciones que utilicen esta tecnología poseen similar criticidad o importancia. No se encuentra dentro del alcance de este documento la determinación del grado de seguridad aplicable a cada documentos a ser firmado digitalmente, y es tarea de cada uno de los organismos determinar el nivel de seguridad que deberá utilizar en sus aplicaciones en lo que respecta al almacenamiento y la longitud de la clave a emplear, respetando siempre los requisitos mínimos establecidos en este documento.
Deben seguirse las siguientes indicaciones para el uso de esta tecnología dentro de la IFDAPN:
Los agentes o funcionarios deben emplear claves de 1024 bits (RSA o DSA) de longitud o superior para firmar documentos.
Las ACLs deben poseer claves de 1024 bits o superiores para firmar los certificados de los usuarios.
Se permite el uso de claves iguales o superiores a 512 bits (RSA o DSA) de longitud para aplicaciones particulares que no requieran niveles elevados de seguridad tal como se indica en 3.3 - Titulares de Certificados.
Las ACLs deben garantizar un almacenamiento confiable de toda la información relativa a los certificados emitidos y de la información respaldatoria que garantiza que se han seguido los procedimientos de autenticación para la emisión de cada certificado.
El plan de contingencias y de seguridad presentado ante el OL debe contemplar los pasos a seguir para evitar que dicha información sea destruida. (ver A.4 - Medios de Almacenamiento)

4.1.3 - Generación del par de claves

Las etapas de generación del par de claves, almacenamiento de la clave privada en un dispositivo (encriptada por alguno de los algoritmos enunciados en 4.2.1.3 - Algoritmos de Encriptado) y generación del pedido de certificado deben ser llevadas a cabo por el titular de dicho par de claves o por el representante de la ACL.
Dicho par de claves debe corresponder a un algoritmo aceptable dentro de las actuales especificaciones técnicas (ver 4.2.1.2 - Firmas Digitales), y debe ser de una longitud adecuada para el tipo de certificado que se solicite. Esta información se encuentra indicada en la Política de Certificación del certificado solicitado.
Una ACL puede rechazar la solicitud de un certificado si considera que el par de claves no ha sido generado utilizando un mecanismo seguro, o si no cumple con algunos de los requisitos indicados en el Manual de Procedimientos o en la Política de Certificación correspondiente.
Para la generación de números aleatorios empleados en los presentes algoritmos de generación de claves deben ser tenido en cuenta las recomendaciones presentes en [RFC1750].

4.1.4 - Usuarios

El procedimiento y los mecanismos empleados para que un usuario opere con su clave privada, ya sea para firmar o para autenticarse, son elementos fundamentales para la seguridad de la firma digital.
Un usuario debe confiar en las aplicaciones que utiliza, y es responsabilidad de quienes diseñan e implementan tales aplicaciones transmitir dicha confianza a los usuarios.
Es responsabilidad del titular de una clave privada "Mantener el control de su propia CLAVE PRIVADA e impedir su divulgación" (Decreto Nº 427/98, Anexo I).

4.1.4.1 - Responsabilidades

Todas las aplicaciones que utilicen esta tecnología deben garantizar que la clave privada no se encuentra comprometida en ningún momento y sus responsables deben responder por las pérdidas que esto puede ocasionar de no cumplir con los procedimientos correspondientes.
Por otro lado, será responsable el usuario si es éste quien no cumple las recomendaciones y procedimientos indicados a los efectos de proteger dicha clave.

4.1.5 - Autoridades Certificantes Licenciadas

Las ACLs deben ofrecer un alto grado de seguridad en relación a los equipos informáticos y de comunicación empleados, al personal empleado para operar la ACL, a los responsables de operar la clave privada de la ACL y a los procedimientos utilizados para la autenticación de los datos a ser incluidos en los certificados.
Todos estos procedimientos están sujetos a auditorías tal como lo indica el Decreto Nº 427/98.
4.1.5.1 - Auditorías
Una ACL es auditada periódicamente según lo establece el Decreto Nº 427/98. Los informes de auditoría deben ser tenidos en cuenta para permitir el licenciamiento, en caso de tratarse de una AC en proceso de licenciamiento, y para que pueda continuar su operatoria.
Las recomendaciones surgidas de las auditorías sobre problemas de seguridad u operatoria en la ACL deben ser atendidos en el menor plazo posible, consecuente con la complejidad del problema y acordando dicho plazo con el OL.
4.1.6 - Servicio de Directorio
La integridad del directorio de certificados y CRLs debe estar permanentemente asegurada. Es responsabilidad de la ACL garantizar la disponibilidad de este servicio y la calidad de los datos suministrados por éste.
4.1.7 - Seguridad Informática
Las computadoras involucradas en el procesamiento, autenticación, verificación y emisión de los certificados deben cumplir con las especificaciones del "Libro Rojo" (Red Book) del Centro Nacional de Seguridad de Computación de los Estados Unidos (US National Computer Security Center), clase C2.
Los redes de comunicación empleadas para el procesamiento, autenticación, verificación y emisión de los certificados deben ser protegidas de accesos externos por medio de controles físicos y lógicos apropiados, permitiendo solamente la prestación de aquellos servicios relativos a las tareas de la ACL. Debe contarse con una política de seguridad implementada para proteger dicho equipamiento de accesos no autorizados.
4.1.8 - Seguridad física de los equipos
Las equipos de computación empleados en el procesamiento, autenticación, verificación y emisión de los certificados deben encontrarse físicamente protegidos del acceso por parte del personal no autorizado.
Los medios aplicados para restringir dicho acceso pueden ser complementados por otros mecanismos de seguridad que garanticen un nivel apropiado de seguridad acorde a la información crítica de la ACL.
4.2 - Firma Digital
Los presentes especificaciones se basan en estándares tales como ITU-T X.509 [ISO94-8], ANSI [X9.55], [X9.57] y [X9.62] y en los documentos de trabajo sobre PKIX del Internet Engineering Task Force (IETF) [PKIX1] y [PKIX3].
Con respecto a las características criptográficas, debido a la gran cantidad de algoritmos disponibles, es necesario seleccionar un estándar que garantice la interoperabilidad dentro de la IFDAPN. Los algoritmos y protocolos sobre los cuales se requiere un estándar son:
Firma digital.
Manejo de claves.
Funciones de Hash seguro.
Generación de claves.
La seguridad aportada a los usuarios dentro de la IFDAPN está fuertemente relacionada con la selección de dichos algoritmos y con la longitud de sus claves. Por otro lado, la incorporación rápida de esta tecnología a los servicios con los que actualmente se cuentan se verá condicionada por la disponibilidad y soporte técnico apropiados.
Por lo tanto, los siguientes factores deben ser tenidos en cuenta para la selección de los algoritmos incorporados en los estándares de la IFDAPN:
Aceptabilidad internacional del Algoritmo.
Disponibilidad de aplicaciones o bibliotecas (libraries) que faciliten su uso.
Reconocimiento internacional de su aceptación en medios especializados.

4.2.1 - Tecnología de Clave Pública

4.2.1.1 - Par de claves

La generación del par de claves mediante alguno de los algoritmos autorizados es una etapa crucial en el mecanismo de obtención de un certificado. El producto utilizado para esta tarea debe ser altamente confiable, no sólo su origen (es decir, el proveedor de dicho software) sino también de su capacidad técnica. Un usuario no debe confiar en cualquier software para generar su par de claves, y menos aún utilizar intencionalmente un par de claves ya generado por otro usuario.

En todo momento la clave privada del par de claves debe estar permanentemente protegida. Esto se logra utilizando medios físicos que prevengan un acceso indebido y encriptando su contenido por medio de un algoritmo simétrico (ver 4.2.1.3 - Algoritmos de Encriptado). (ver A.5 - Navegadores generadores de Par de Claves)

El par de claves generado debe pertenecer a alguno de los algoritmos enunciados en 4.2.1.2 - Firmas Digitales.

4.2.1.2 - Firmas Digitales

El conjunto de algoritmos preferidos para firma digital es md5WithRSAEncryption [PKCS#1] con una longitud de clave igual a superior a 1024 bits (RSA).

Es igualmente aceptable sha1WithDSAEncryption [FIPS180] [FIPS186] con la misma longitud de clave del algoritmo DSA.

4.2.1.3 - Algoritmos de Encriptado

Es necesario en todo momento mantener encriptada la clave privada del titular, de la ACL y del OL. Es posible utilizar algoritmos tales como Triple DES [X9.52] en sus distintos modos de operación [FIPS 81] CBC, CFB, OFB con longitudes de claves de 112 y 168 bits.

Otro algoritmo aceptado para este fin es IDEA [IDEA] con bloques de 128 bits e idénticos modos.

Se podrán incorporar otros algoritmos al presente estándar siempre y cuando cumplan con las premisas enunciadas en 2.2 - Tecnología.

4.2.2 - Certificados

La IFDAPN utiliza certificados X.509 versión 3 tal como se indica en el estándar ISO/IEC/ITU X.509 [IETF1]. Este estándar pertenece a un grupo de estándares definidos en ITU-T X.500 Directory Service Standards.

4.2.2.1 - Tipos

Una ACL puede emitir distintos tipos de certificados. Estos pueden ser diferenciados por el grado de compromiso empleado en la verificación de cada uno de los datos que contienen, y por los datos contenidos (diferentes atributos en su Nombre Distinguido, "Distinguished Name" en adelante DN, diferentes algoritmos y diferentes extensiones).

A cada tipo de certificado le corresponde una Política de Certificación propia.

El uso de cada tipo de certificado se encuentra descripto en la Política de Certificación correspondiente y las aplicaciones que se desarrollen a tal efecto.

4.2.2.2 - Datos Básicos

Los certificados emitidos poseen los siguientes campos (como mínimo):

<table>
<tr><td rowspan="2">Firma del Emisor</td><td>ID del Algoritmo</td><td>Algoritmo usado para esta firma</td></tr>
<tr><td colspan="2">Encriptado de resultado de la función de Hash sobre el certificado</td></tr>
</table>

Versión	Número de versión del formato X.509	
Número de Serie (Serial Number)	Unico número identificador del certificado generado por el emisor del mismo.	
Firma (Signature)	ID del Algoritmo	Algoritmo usado para firmar el certificado
Emisor (Issuer)		Nombre del emisor del certificado (en formato X.500)
Validez (Validity)	No antes de (Not Before)	Fecha de inicio de validez
	No después de (Not After)	Fecha de finalización
Titular (Subject)		Nombre del titular del certificado (en formato X.500)
Información de la clave pública del Titular	ID del Algoritmo	Algoritmo de firma del titular
	Parámetros	Parámetros aplicables a la clave pública
	Clave Pública	Clave Pública del titular
Extensiones	(Opcional)	Extensiones agregadas a los certificados tal como lo indica el estándar.

4.2.2.3 - Extensiones

Es recomendable que los certificados emitidos por las ACLs incorporen aquellas extensiones que imponen restricciones en el uso de los certificados (key usage, basic constraints) y aquellas que informan sobre la política de certificación correspondiente (certificate policies). (ver A.6 - Extensiones X.509 v3).

4.2.2.4 - Formatos

Los certificados emitidos por las ACLs y por el OL deben ser entregados en formato PEM o DER [ISO25-1] para poder ser incorporados a las aplicaciones que requieran su uso.

4.2.2.5 - Identificación única

Es necesario que cada titular de certificado sea distinguido unívocamente. Cada usuario tiene un simple DN, que debe ser compatible con el estándar X.520 [ISO9594-6].

Se recomienda incluir en cada DN de usuario los siguientes datos como mínimo:

Nombre y apellido completo, según figure en su Documento Nacional de Identidad, libreta de enrolamiento o libreta cívica, o en su caso, Cédula de Indentidad o Pasaporte.

Organismo donde desempeña sus funciones, u organismo emisor del certificado en caso de tratarse de un usuario externo a la Administración Pública Nacional.

Localidad, Provincia y País de residencia habitual.

Un identificador único utilizado por la ACL para evitar conflictos con otros certificados emitidos.

4.2.2.6 - Número de Serie

El número de serie será un número entero único asignado por cada ACL a cada certificado emitido. Estos números son correlativos y se incluirán en las CRLs si el certificado es revocado.

4.2.2.7 - Período de Validez

Los campos que indican el periodo de validez ("no antes de" y "no después de") detallan fecha y hora. Los valores incluidos en estos campos se encuentran expresados en Coordinated Universal Time (UTC).

4.2.2.8 - Titular

Es un identificador del titular del certificado en formato X.520. Debe ser único dentro de la ACL que emita el certificado. Los atributos que lo componen son aquellos indicados en la Política de Certificación correspondiente a este tipo de certificados.

4.2.2.9 - Emisor

Es un identificador, o DN, del emisor del certificado en formato X.520, que se encuentra en el certificado que posee dicho emisor.

4.2.3 - Solicitudes de Certificados(3)

Para emitir un certificado es necesario contar con una solicitud, la cual debe contener la

clave pública de quien solicita dicho certificado (o en su caso de la Autoridad Certificante a licenciar) junto a otros datos del mismo. Dicha solicitud debe encontrarse firmada utilizando la clave privada correspondiente a la clave pública incluida en la solicitud.
Siguiendo los pasos indicados en el Manual de Procedimientos para el tipo de certificado solicitado, la ACL (o en su caso el OL) procede a emitir el certificado correspondiente.
Para verificar la posesión de la clave privada correspondiente se utilizan los mecanismos que se describen en la sección 2.3 (Proof of Possession (POP) of Private Key) en Internet X.509 Public Key Infrastructure Certificate Management Protocols [PKIX-CMP].
4.2.3.1 - Solicitud de una AC al OL
Las Autoridades Certificantes que deseen ser licenciadas por el OL deben remitir una solicitud de certificado en formato PKCS#10 [PKCS#10].
Dicho requerimiento puede ser transmitido en formato DER o PEM [ISO25-1], dependiendo del producto generador del requerimiento.
4.2.3.2 - Solicitud de un Titular a una ACL
Las solicitudes de los usuarios hacia una ACL pueden ser remitidas en formato PKCS#10 [PKCS#10].
Pueden utilizarse otros formatos o mecanismos, principalmente aquellos desarrollados para ser solicitados utilizando los Navegadores de Internet, siempre y cuando se pueda garantizar que el solicitante posee la clave privada correspondiente a la clave pública incluida en la solicitud (ver A.5 - Navegadores generadores de Par de Claves).
4.2.3.3. - Certificados para Servidores
Los certificados para servidores (para ser utilizados en el protocolo HTTPS u otros servicios utilizando protocolo TLS o SSL v3) pueden ser emitidos por las ACLs para aquellos servidores que se encuentren dentro de su ámbito de aplicación. Debe garantizarse el derecho al uso del denominador utilizado (nombre del servidor) por parte del ente que posea la autoridad sobre la zona del Dominio de Nombres correspondiente [RFC1034][RFC1035].
Debe nombrarse un responsable de la clave privada correspondiente al certificado emitido al servidor correspondiente.
4.2.4 - Lista de Certificados Revocados (CRL)
La IFDAPN utiliza Lista de Certificados Revocados X.509 versión 2 tal como se indica en el estándar ISO/IEC/ITU X.509 [IETF1]. Este estándar pertenece a un grupo de estándares definidos en ITU-T X.500 Directory Service Standards.
4.2.5 - Tipos de dispositivos utilizados para almacenar las claves privadas
Es responsabilidad del organismo que incorpore la presente tecnología a sus procedimientos la selección del almacenamiento apropiado para cada aplicación, garantizando siempre el mayor grado de seguridad sobre las claves privadas de los usuarios. En
A.4 - Medios de Almacenamiento se encuentra una lista de dispositivos que pueden ser utilizados con una descripción de sus características más relevantes en lo que respecta al uso de esta tecnología.
Tal como se indica en el Decreto Nº 427/98, es responsabilidad de la ACL dar a conocer a los usuarios las responsabilidades y obligaciones que contrae por el hecho de ser titular de un certificado correspondiente a su clave privada. De la misma manera debe instruir a dichos usuarios sobre la mejor manera de proteger dicha clave de accesos indebidos.
Es recomendable que las claves privadas sean almacenadas en Smart Cards (Tarjetas Inteligentes) u otros dispositivos removibles de manera tal de garantizar su seguridad física. Es posible hacer uso de otro tipo de dispositivos para aplicaciones o funciones, garantizando siempre la integridad y seguridad de la clave privada.
Es recomendable que las Smart Cards que sean incorporadas en la IFDAPN soporten PKCS#11 ya que permite un nivel de seguridad apropiado y asegura interoperabilidad. Sin embargo, es posible utilizar el estándar definido como CryptoAPI si la plataforma operativa es un entorno Windows. En ambos casos el proveedor de Smart Cards debe ofrecer una o ambas interfaces cumpliendo los estándares sobre algoritmos, longitud de clave y encriptado de claves indicados. El estándar ISO7816 debe ser soportado estos dispositivos que sean incorporados a la IFDAPN. Asimismo, deben ofrecer conectividad utilizando la

última versión del estándar PC/SC definido en [PCSC]. (ver A.4.1 - Sobre Smart Cards - interoperabilidad)

4.2.6 - Comunicación

4.2.6.1 - Comunicación segura en línea

Se recomienda utilizar el protocolo Transport Layer Security (TLS) para establecer una comunicación segura entre aplicaciones [PKIX-TLS], o bien SSL versión 3.

TLS es el estándar resultante del protocolo Secure Socket Layer (SSL). Permite autenticar tanto al servidor como al cliente de una aplicación utilizando certificados X.509.

4.2.6.2 - Formato de transferencia de Correo Electrónico (Email).

Es recomendable que las aplicaciones de correo electrónico que utilicen esta tecnología cumplan con el estándar S/MIME para la transmisión de mensajes.

S/MIME es una iniciativa de RSA Data Security Inc. que actualmente es un estándar de internet definido en [SMIME]. Especifica una mensajería electrónica segura.

4.2.7 - Servicios de Directorio

Las ACLs y el OL deben ofrecer un servicio de directorio compatible con el protocolo LDAP y permitir que las aplicaciones accedan a los certificados emitidos y a las CRLs. Este servicio se debe encontrar actualizado con la frecuencia indicada en las Políticas de Certificación de cada tipo de certificado. (ver A.7 - Servicios de Directorios)

La implementación de un servicio de estas características debe soportar la inclusión de certificados de usuario, certificados de ACLs y CRLs.

Junto al Servicio de Directorio se puede disponer del servicio de consulta en línea del estado de un certificado. Dicho servicio se encuentra definido en [PKIX-OSCP].

4.2.8 - Otros servicios

No se encuentran contemplados en el Decreto N° 427/98 como obligaciones de las ACLs otros servicios relacionados a la presente tecnología. Sin embargo, pueden ser incorporados siempre que no se comprometa el nivel de seguridad necesaria o se dejen de cumplir con los estándares de la IFDAPN.

4.2.8.1 - TimeStamp

El servicio de TimeStamp permite adicionar a un documento un sello de fecha y hora seguro. Este sello es emitido por una Autoridad de Sellado de Fecha (Time Stamp Authotiry, TSA), que es una entidad confiable similar a una ACL. Una TSA que ofrezca los servicios dentro de la Administración Pública Nacional debe cumplir con el estándar definido en [PKIX-TS].

4.2.8.2 - Key Recovery

El Decreto Nº 427/98 no contempla las características de encriptado que posibilita esta tecnología. (ver A.2.1 - Key Recovery)

4.2.8.3 - Servicios de notariado

El Servicio de Notariado se encuentra definido en el estándar Internet X.509 Public Key Infrastructure Data Certification Server Protocols [PKIX-DCS].

Al igual que el servicio de TimeStamp, puede ser implementado por una institución u organismo. Sin embargo, no se encuentra contemplado dentro del Decreto Nº 427/98.

A - INFORMACION

A.1 - Organizaciones Internacionales

A.1.1 - International Telecommunications Union

ITU es el responsable de los estándares X.509 para formato y directorio de certificados. http://www.itu.ch

A.1.2 - Internet Engeneering Task Force (IETF) Working Group

El "Internet Engeneering Task Force Working Group" es un grupo de trabajo organizado para producir técnicas y otro tipo de contribuciones a la ingeniería y evolución de Internet y sus tecnologías. Se encuentra abierto a cualquier individuo interesado y su tarea principal es la producción de nuevas especificaciones de estándares para Internet. El IETF no es una organización dedicada a la producción de estándares, aunque muchas de las especificaciones producidas por dicho grupo han sido adoptadas como tales.

El IETF Simple Public Key Infraestructure (SPKI) Working Group se encuentra desarrollando un estándar para un formato de certificado de clave pública, firma asociada y

otros formatos y protocolos de adquisición de claves. Es intención que el SPKI provea mecanismos para soportar seguridad en un amplio rango de aplicaciones sobre Internet, incluyendo Internet Protocol Security Evaluation Criteria (IPSEC), correo electrónico encriptado y documentos en WWW, protocolos de pago y otras aplicaciones que requieren certificados para acceder.

A.1.3 - National Institute of Standards and Technology (NIST)

El NIST fue creado por el Congreso de los EE.UU. para apoyar a la industria en el desarrollo de las tecnologías necesarias para mejorar la calidad de los productos, para modernizar sus procesos de fabricación, para asegurar su confiabilidad y para facilitar su rápida comercialización en base a los últimos avances científicos.

http://www.itl.nist.gov

A.2 - Consideraciones generales

A.2.1 - Key Recovery

El Decreto Nº 427/98 prohíbe expresamente que una ACL tome contacto con una clave privada perteneciente al titular de un certificado emitido por ella misma o por otra ACL. Esto también rige para el OL con respecto a las ACLs.

Por tal motivo este servicio no puede ser ofrecido por el OL ni por las ACLs que operan dentro de la IFDAPN. Los titulares de certificados que pierdan la clave privada correspondiente a la clave pública presente en el certificado deben solicitar la revocación inmediata del mismo a fin de evitar posibles fraudes.

Las ACLs y los titulares de certificados deben utilizar medios alternativos de resguardo para garantizar la recuperación de su clave privada si ésta se viese destruida por algún motivo.

A.2.2 - Data Recovery

Dado que es posible utilizar el mismo mecanismo para mantener comunicaciones encriptadas, y que es necesaria la clave privada del receptor para la lectura de la información encriptada (ya sea para recuperar la clave simétrica de sesión con la que se encriptó la comunicación, o porque se utilizó un mecanismo asimétrico de encriptado), la pérdida de dicha clave, de no tomarse los recaudos necesarios, imposibilitará la recuperación de información.

Es recomendable que se utilice un par de claves diferente para encriptar los documentos a aquel utilizado para firmar. Para dicho par de claves se puede emplear un mecanismo de key recovery de tal manera que, en caso de pérdida, puede ser recuperada la clave privada.

A.3 - Importancia de la Clave Privada en función de la jerarquía

Al comprometer la clave privada de un usuario es posible que otro individuo impersone al titular de dicha clave, utilizándola para firmar documentos digitalmente o altere de manera indetectable uno previamente firmado. De esta manera se está comprometiendo la confiabilidad del sistema ya que es imposible determinar el firmante real del documento, es decir, no es posible distinguir al titular de la clave privada del impostor. Según se indica en el Decreto Nº 427/98, el titular de la clave privada es el responsable de todo acto en el que intervenga la misma, y en caso de verse comprometida debe informar de inmediato a la ACL emisora para que su certificado sea revocado.

Una tarea similar debe seguir una ACL si considera que su clave privada se ha visto comprometida. Pero en este caso los afectados son todos los certificados que han sido emitidos por dicha ACL si no es posible determinar el momento a partir del cual dicha clave se vio comprometida.

Es natural, por lo tanto, emplear mayores y mejores recursos para proteger la clave de una ACL que la de un usuario, lo cual no implica una mayor importancia sino la necesidad de evitar consecuencias operativas más graves.

A.4 - Medios de Almacenamiento

Existen actualmente diversos medios disponibles para el almacenamiento de la clave privada, tanto de las ACLs como de los titulares de certificados. La lista que se transcribe a continuación no es exhaustiva ya que pueden surgir nuevas tecnologías que serán oportunamente incorporados al presente documento.

Diskette

Presenta características que lo hacen, por el momento, el medio más práctico y económico: se puede leer en todas las computadoras, es fácilmente transportable y permite almacenar un gran volumen de información. Sin embargo no es un medio confiable ya que su uso intensivo puede causar pérdida de información. En caso de utilizarse se recomienda realizar copias de resguardo de la clave privada del titular.

Disco Rígido

Al igual que el diskette se encuentra en todos los equipos aunque es más confiable con respecto al mantenimiento de la información. Sin embargo cuenta con varias desventajas:

n no es transportable, lo que implica que el usuario sólo puede utilizar su clave privada desde una sola estación de trabajo,

n la mayoría de los equipos no cuentan actualmente con un Sistema Operativo que impida el acceso de usuarios no habilitados a los archivos donde se almacene la clave privada. Aunque esta clave se encuentra protegida por un sistema criptográfico que restringe su uso al titular de la misma, no puede evitarse su destrucción voluntaria o involuntariamente.

Es recomendable contar con una política de seguridad para los equipos, no sólo a nivel de red, si se desea utilizar este tipo de dispositivos.

Los discos rígidos removibles solucionan el problema de la seguridad, pero igualmente deben ser utilizados personalmente.

Smart Cards

Los Smart Cards (Tarjetas Inteligentes) son los dispositivos mejor considerados para esta tarea. Cuentan con varias características que hacen apropiado su uso para almacenar las claves privadas: son fácilmente transportables y seguros.

Incluso es posible incorporar dentro de estos dispositivos los algoritmos necesarios para la generación del par de claves, la firma y la verificación de manera tal de proteger la clave privada de todo acceso externo.

El inconveniente actual es la poca disponibilidad de lectores instalados sobre el parque actual de computadoras personales. Dichos lectores pueden ser incorporados a las computadoras de manera externa o interna. Es posible el uso de un dispositivo que es incorporado dentro del lector de diskette.

Con respecto a la seguridad de estos dispositivos algunas tarjetas tienen características que deben evitarse:

n Baja entropía utilizada para la generación de los números primos a ser utilizados para la generación del par de claves. Se deben utilizar algoritmos con las carácterísticas que se enuncian en 4.1.3 - Generación del par de claves.

n La protección de la clave privada se realiza utilizando una clave de sólo 4 dígitos, algo que es fácilmente detectable con un ataque de fuerza bruta. Se deben evitar este tipo de mecanismos para la protección de una clave privada.

En A.4.1 - Sobre Smart Cards - interoperabilidad se enuncian los actuales estándares del mercado en lo que respecta a lectores de este tipo de tarjetas.

Tarjetas de memoria

Estas tarjetas permiten solamente almacenar información, sin ninguna capacidad criptográfica. Cuenta con las mismas limitaciones que los Smart Cards en lo que respecta a los lectores y al almacenamiento seguro de la información. Es recomendable, por lo tanto, el uso de Smart Cards en lugar de estos dispositivos.

Módulos Criptográficos en hardware

Estos dispositivos permite almacenar la clave privada y realizar todos los cálculos criptográficos dentro del mismo. Su capacidad, tanto en seguridad como en velocidad de cálculo, es superior a la una implementación y ejecución por software, lo que lo hacen apropiados para aplicaciones críticas, de máxima seguridad donde se requiera dicha capacidad. Sin embargo, no son apropiados para almacenar las claves privadas de los usuarios ya que no son transportables.

A.4.1 - Sobre Smart Cards - interoperabilidad

La interoperabilidad en sus distintos niveles - físico, lógico de acceso y de estructura de datos - entre distintas Smart Cards debe ser considerada al incorporar dicha tecnología en los sistemas o aplicaciones que operen dentro de la IFDAPN

Con el objetivo de permitir la interoperabilidad entre tarjetas y lectores, la International Standard Organization (ISO) definió en 1996 el estándar 7816 [ISO7816] para tarjetas con circuitos integrados con contactos. Este se encuentra focalizado en lograr interoperabilidad en niveles físico, eléctrico y de protocolos de transferencia de datos.
En Mayo de 1996 se formó el grupo de trabajo PC/SC (PC/SC Workgroup) con participación de fabricantes de PC (Personal Computers) y Smart Cards. El objetivo del mismo es definir un estándar para superar el problema del acceso a los datos desde plataformas heterogéneas. En diciembre de 1997, dicho grupo de trabajo publicó la primera versión del estándar [PCSC].
No existe un estándar que defina el formato de la información (de carácter criptográfico) que es almacenada dentro de un Smart Card. Dicha información es dependiente de cada una de las aplicaciones que hagan uso de la misma. Es recomendable, teniendo en cuenta el limitado espacio de almacenamiento disponible, que antes de generar dicha estructura sean considerados todos los sistemas y aplicaciones sobre los cuales la misma tarjeta será utilizada.
PKCS#11 (Cryptographic Token Interface) es un estándar mantenido y publicado por RSA Data Security Inc. y ampliamente aceptado por la industria. Especifica un estándar de bajo nivel para acceder a dispositivos criptográficos desde cualquier plataforma.
Describe una interfaz normalizada para acceder a motores criptográficos, conocidos como Tokens. Cada Token es capaz de almacenar información sensitiva y no sensitiva, manejar permisos de acceso y realizar operaciones criptográficas. Una aplicación puede consultar a un Token sobre las capacidades que soporta, por lo tanto, no todos tienen que ofrecer necesariamente el mismo grado de funcionalidad.
Las aplicaciones pueden utilizar esta interfaz para acceder o almacenar las claves privadas o las funcionalidades criptográficas necesarias sin importar si éstas han sido desarrolladas por software o hardware.
Microsoft Comp. provee una arquitectura de servicio criptográfico sobre sus sistemas operativos Windows 95, Windows 98 y Windows NT utilizando una interfaz llamada CryptoAPI. De esta manera, cualquier aplicación requiriendo un servicio criptográfico lo puede solicitar por medio de esta interfaz. Este servicio permite a las aplicaciones comunicarse con módulos criptográficos llamados Cryptographic Service Providers (CSP). Un CSP preinstalado por el sistema operativo se encuentra presente, con las limitaciones criptográficas impuestas por la legislación de EEUU al respecto de estos módulos.
Los CSPs ofrecen información sobre sus capacidades a las aplicaciones que lo requieran. Pueden desarrollarse CSPs propios para acceder a las capacidades criptográficas que ofrecen las Smart Cards.
Es necesario que dichos CSPs cumplan con los estándares expuestos en el presente documento con respecto a los algoritmos habilitados y sus longitudes de clave. Dichos CSPs deben encontrase firmados digitalmente por Microsoft Comp. para que puedan ser incorporados dentro de la arquitectura del sistema operativo.

A.5 - Navegadores generadores de Par de Claves

En la actualidad las claves son generadas en su mayoría por los Navegadores de Internet (Netscape Communicator e Microsoft Internet Explorer), los cuales cuentan con la limitación de generar sólo claves de longitud igual o inferior a 512 bits (algoritmo RSA).
Esta limitación se encuentran determinada por las restricciones de exportación que actualmente aplica el gobierno de Estados Unidos a los productos que contienen componentes criptográficos.
Se encuentra en la actualidad en estudio un estándar para el acceso e interacción con Autoridades Certificantes utilizando el protocolo HTTP [PKIX-WEB].

A.6 - Extensiones X.509 v3

El estándar X.509 enumera cada una de las extensiones que pueden ser incluidas en los certificados. Algunas de ellas deben ser consideradas "críticas" ya que de no incluirse en los certificados emitidos puede verse afectado el funcionamiento de algunas aplicaciones.
Las extensiones estándar se encuentran definidas en [PKIX1], aunque es posible incorporar nuevas extensiones que hayan sido registradas ante autoridades apropiadas, por ejemplo la

ISO.
Las extensiones estándar incorporadas hasta el momento se pueden dividir en las siguientes grupos:
Información sobre la clave.
Existen cuatro extensiones relacionadas con información relativa al uso del certificado y del par de claves. Esta son: authority key identifier, subject key identifier, key usage y privake key usage period.
Información sobre Política de Certificación.
Estas extensiones proveen a las ACLs un mecanismo para distribuir información relacionada con las políticas de certificación aplicadas a cada tipo de certificado emitido. Estas son: certificates policies y policy mapping.
Atributos de usuarios y Autoridades Certificantes.
Este tipo de extensiones aportan información adicional para la identificación de los titulares de los certificados y de las ACs. Entre ellas se encuentran: subject alternative name, issuer alternative name, subject directory attributes.
Restricciones de certificación.
Estas extensiones ofrecen a las ACs un mecanismo para limitar y controlar a otras ACs certificadas por éstas. Son: basic constraints, name constraints y policy constraint.
A.7 - Servicios de Directorios
El servicio de directorio permite acceder a información relativa al certificado que no se encuentra incluida en el mismo, como por ejemplo si ha sido revocado, a las Listas de Certificados Revocados (CRLs) que debe emitir una ACL de acuerdo a la Política de Certificación de cada tipo de certificado.
Las características relevantes de este servicio son:
Debe permitir el acceso a los certificados en función de la identificación única del titular del certificado o del número de serie del mismo.
Debe permitir un control de acceso a los datos contenidos en él, de tal manera de hacer públicos sólo aquellos datos que se encuentren en el certificado.
Debe utilizar un protocolo estándar internacionalmente aceptado y de disponibilidad local.
A.7.1 - X.500
El estándar X.500 integra un conjunto de protocolos y modelos de información con el objetivo de implementar un servicio de directorio global.
El modelo X.500 es jerárquico y permite mantener una parte de dicho directorio global. La conexión con otros servidores de directorio ofrece al usuario un mecanismo único para la búsqueda de información.
A.7.2 - LDAP
LDAP (Lightweight Directory Access Protocol) es un protocolo de acceso a directorios de información. LDAP fue desarrollado como un subconjunto de operaciones sobre el protocolo definido en el estándar X.500 llamado DAP (Discretionary Access Protocol).
LDAP opera sobre redes TCP/IP y se encuentra publicado (versión 2) como un estándar de internet en [RFC1777].
A.8 Verificación de una firma y refirmado de documentos
En un certificado X.509 v3 se encuentra indicado su periodo de validez. Un titular no debe utilizar su clave privada para firmar documentos si el certificado correspondiente se encuentra expirado.
La verificación de una firma se debe hacer teniendo en cuenta si en el momento de la firma el certificado correspondiente a la clave privada empleada se encontraba vigente. De esta manera se garantiza que el firmante se encuentra habilitado para utilizar su clave privada.
Sin embargo, es posible que la clave privada empleada para firmar se encuentre expuesta con el tiempo a ser descubierta. Por ello, y a los fines de evitar fraudes, es necesario que los documentos que han sido firmados con anterioridad sean refirmados utilizando un par de claves nuevas y un certificado con vigencia actual.
C - GLOSARIO

Firma Digital	*Digital Signature*	Es un dato digital utilizado para verificar simultáneamente la identidad del autor de un documento digital y que éste no ha sido modificado. DEF. ANEXO II: *' Resultado de una transformación de un DOCUMENTO DIGITAL CRIPTOSISTEMA ASIMETRICO y un DIGESTO SEGURO, de forma tal que una persona que posea el DOCUMENTO DIGITAL inicial y la CLAVE PUBLICA del firmante pueda determinar con certeza* *1. Si la transformación se llevó a cabo utilizando la CLAVE PRIVADA que corresponde a la CLAVE PUBLICA del firmante, lo que impide su repudio* *2. Si el DOCUMENTO DIGITAL ha sido modificado desde que se efectuó la transformación, lo que garantiza su integridad.* *La conjunción de los dos requisitos anteriores garantiza su NO REPUDIO y su INTEGRIDAD.'*
HTTP	Hyper Text Transport Protocol	Protocolo de transporte utilizado para acceder a objetos a partir de un identificador referencial universal.
APN	Infraestructura de Firma Digital de la Administración Pública Nacional	Representa todos los elementos parte de la infraestructura: OL, ACLs, OA y titulares de certificados regulados por el Decreto Nº 427/98 y por los presentes estándares.
Oficial Certificador	Oficial Certificador	Responsable o responsables de la clave privada del Organismo Licenciante o de las Autoridades Certificantes Licenciadas.

PEM	Privacy Enhanced Mail	Un conjunto de estándares propuestos en Internet. Indican el formato de información.
PKI	Infraestructura de Clave Pública Public Key Infrastructure	Hardware, software, canales de comunicación y procedimientos necesarios para proveer un servicio de certificación.
OL	Organismo Licenciante	Organismo Licenciante de acuerdo al Decreto Nº 427/98.
Usuario	Titular de un certificado y su correspondiente clave privada	Titular de un par de claves y un certificado emitido a su nombre que interactúa con uno o varios sistemas que utilizan esta tecnología dentro de la IFDAPN.
X.509	Formato de Certificado	X.509 es el formato de certificado más extensamente reconocido. Se encuentra definido en el estándar ISO/IEC/ITU X.509. Actualmente se encuentra definida la versión 3.

D - REFERENCIAS

[FIPS180]	FIPS PUB 180-1, *Secure Hash Standard*, NIST, April 1995. Disponible en: http://www.itl.nist.gov/div897/pubs/fip180-1.htm
[FIPS186]	FIPS PUB 186, *Digital Signature Standard*, NIST, May 1994. Disponible en: http://www.itl.nist.gov/div897/pubs/fip186.htm
[FIPS 46]	FIPS PUB 46-2, *Data Encryption Standard*, December 1993. Disponible en: http://www.itl.nist.gov/div897/pubs/fip46-2.htm
[FIPS 81]	FIPS PUB 81, *DES Modes of Operations*, June 1981. Disponible en: http://www.itl.nist.gov/div897/pubs/fip81.htm
[ISO25-1]	ISO/IEC 8825-1 (1994), *Information Technology - ASN.1 Encoding Rules - Specification of Basic Encoding Rules (VER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*
[ISO7816]	ISO 7816 (parts 1-3). *Asynchronous smartcard information.* International Standard Institute. (1996)
[ISO9594-6]	ISO/IEC 9594-6 (1992), *Selected Attribute Types.*
[PCSC]	*Interoperability Specification for ICCs and Personal Computer Systems*, PC/SC Working Group, Dic 1997. Disponible en: http://www.smartcardsys.com/
[PKCS#1]	PKCS #1: *RSA Encryption Standard, Version 1.4*, RSA Data Security, Inc., 3 June 1991. Disponible en: http://www.rsa.com/pub/pkcs/
[PKCS#9]	PKCS #9: *Selected Attribute Types, Version 1.1*, RSA Data Security, Inc., 1 November, 1993. Disponible en: http://www.rsa.com/pub/pkcs/

[PKCS#10]	PKCS #10: *Certification Request Syntax Standard, Version 1.6*, RSA Data Security, Inc., 1 November, 1993. Disponible en: http://www.rsa.com/pub/pkcs/
[PKIX1]	Internet Draft, *Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile*, R Housley, W. Ford and D. Solo, July 1997. Working draft "in progress" disponible en: http://www.ietf.org /internet-drafts/draft-ietf-pkix-ipki-part1-04.txt
[PKIX3]	Internet Draft, *Internet Public Key Infrastructure Part III: Certificate Management Protocols*, C. Adams and S. Farrell, June 1997. Working draft "in progress" disponible en: http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-02.txt
[PKIX-CMP]	Internet Draft, *Internet X.509 Public Key Infrastructure Certificate Management Protocol*, C. Adams and S. Farrell, May 1998. Disponible en: http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-08.txt
[PKIX-DCS]	Internet Draft, *Internet X.509 Public Key Infrastructure Data Certification Server Protocols*, C. Adams and R. Zuccherato, Sep 1998. Disponible en: http://www.ietf.org/internet-drafts/draft-ietf-pkix-dcs-00.txt
[PKIX-TS]	Internet Draft, *Internet X.509 Public Key Infrastructure Time Stamp Protocols*, C. Adams, P. Cain, D. Pinkas and R. Zuccherato, Sep 1998. Disponible en: http://www.ietf.org/internet-drafts/draft-ietf-pkix-time-stamp-00.txt
[PKIX-OSCP]	Internet Draft, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol*, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin and Carlisle Adams, Sep 1998. Disponible en: http://www.ietf.org/internet-drafts/draft-ietf-pkix-ocsp-06.txt
[PKIX-TLS]	Internet Draft, *The TLS Protocol Version 1.0*, Tim Dierks, Consensus Development and Christopher Allen, Nov 1997. Disponible en: http://www.ietf.org/internet-drafts/draft-ietf-tls-protocol-05.txt
[PKIX-WEB]	Internet Draft, *WEB based Certificate Access Protocol - WebCAP/1.0*, Surendra Reddy, April 1998. Disponible en: http://www.ietf.org/internet-drafts/draft-ietf-pkix-webcap-00.txt
[RFC822]	RFC 822, *Standard for the Format of ARPA Internet Text Messages*, David H. Crocker, August 13, 1982.
[RFC1034]	RFC 1034, *Domain Names - Concepts and Facilities*, P. Mockapetris, Nov 1987.
[RFC1035]	RFC 1035, *Domain Names - Implementation and Specification*, P. Mockapetris, Nov 1987.
[RFC1750]	RFC 1750, *Randomness Recomendations for Security*, D. Eastlake, S. Crocker, J. Schiller. December 1995. Disponible en: ftp://ftp.isi.edu/in-notes/rfc1750.txt
[RFC1777]	RFC 1777, *Lightweight Directory Access Protocol*, Ed Yeoung, Howes, and Killie. March 1995. Disponible en: ftp://ftp.isi.edu/in-notes/rfc1777.txt
[SMIME]	RFC 2311, *S/MIME Version 2 Message Specification*. Network Working Group. Mar 1998. Disponible en: ftp://ftp.isi.edu/in-notes/rfc2311.txt y http://www.imc.org/ietf-smime/
[X9.52]	Draft American National Standard X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation*, Revision 6.0, May, 1996
[X9.55]	Draft American National Standard X9.55-1995, *Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists*, Nov. 11, 1995