MERCOSUR/GMC EXT./RES. Nº 34/06

DIRECTRICES PARA LA CELEBRACIÓN DE ACUERDOS DE RECONOCIMIENTO MUTUO DE FIRMAS ELECTRÓNICAS AVANZADAS EN EL ÁMBITO DEL MERCOSUR

VISTO: El Tratado de Asunción, el Protocolo de Ouro Preto, la Decisión Nº 59/00 del Consejo del Mercado Común y las Resoluciones Nº 24/03 y 22/04 del Grupo Mercado Común.

CONSIDERANDO:

Que en la necesidad de fortalecer la confianza mutua y alcanzar el reconocimiento de firmas electrónicas avanzadas, los Estados Partes podrán celebrar Acuerdos de Reconocimiento Mutuo a través de sus respectivos órganos competentes.

Que es preciso establecer criterios comunes y procedimientos transparentes para la implementación de Acuerdos de Reconocimiento Mutuo entre los Estados Partes.

EL GRUPO MERCADO COMÚN
RESUELVE:

Art. 1 - Aprobar las Directrices para la Celebración de Acuerdos de Reconocimiento Mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR, en los términos de la presente Resolución.

Art. 2 - Definiciones

A efectos de la presente Resolución, se entenderá por:

1) "**Datos de creación de firma"**: los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica;
2) "**Dispositivo de creación de firma**": un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma electrónica;
3) "**Datos de verificación de firma**": los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica;

Art. 3 - El seguimiento de las Directrices será realizado por el SGT Nº 13, cuyas funciones incluirán las siguientes: intercambiar información, proponer pautas, estándares y procedimientos operativos, analizar los avances nacionales en la materia, estudiar la adecuación de las normas nacionales a los lineamientos establecidos en la presente Resolución, analizar la aplicabilidad de criterios de homologación y los supuestos aplicables a la certificación digital.

El SGT Nº 13 promoverá el desarrollo de estudios para la implementación de un sistema de control común entre los Estados Partes con vistas a la aproximación de sus respectivas infraestructuras y armonización de procedimientos.

Art. 4 - Los Estados Partes, en la elaboración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas que celebren entre sí, deberán observar las siguientes Directrices:

I. Estándares generales de interoperabilidad

Se adoptarán los siguientes estándares internacionales de interoperabilidad:

a) el estándar ITU X.509 v3 o ISO/IEC 9594 para los certificados digitales;
b) el estándar ITU X.509 v2 para la lista de certificados digitales revocados;
c) las recomendaciones de IETF RFC 2560 para la verificación en línea del estado del certificado digital;
d) las recomendaciones de IETF RFC 2527 o RFC 3647 para los contenidos de las políticas de certificación y las prácticas de certificación.

El SGT Nº 13 propondrá al GMC la actualización de los estándares técnicos y operativos que consideren convenientes teniendo en cuenta el estado del arte en la materia.

II. Criterios de seguridad física y lógica de los prestadores de servicios de certificación.

Se deberá prever la evaluación y armonización de los aspectos relacionados con el ambiente operativo, en especial aquellos relacionados con:

a) el control de los accesos a servicios y perfiles;
b) la separación de las tareas y atribuciones relacionadas con cada perfil;
c) los mecanismos de seguridad aplicados a los datos e informaciones sensibles;
d) los mecanismos de generación y almacenamiento de los registros de auditoría;
e) los mecanismos internos de seguridad que garanticen la integridad de los datos y los procesos críticos;
f) los aspectos referidos a la seguridad física y lógica de las instalaciones;
g) los mecanismos tendientes a garantizar la continuidad del funcionamiento de los sistemas críticos.
h) el módulo criptográfico utilizado para el almacenamiento de la clave privada de conformidad con el estándar FIPS 140-1 nivel 3, o equivalente según la evaluación que se realizará en el SGT Nº 13

III. Criterios de auditoría y control de los prestadores de servicios de certificación

Se requerirá la existencia de un sistema de acreditación y control de prestadores de servicios de certificación que contemple:

a) la realización de auditorías sobre los prestadores de servicios de certificación que verifiquen todos los aspectos relacionados con el ciclo de vida de los certificados reconocidos y de sus claves criptográficas.
b) los mecanismos de sanción para aquellos prestadores de servicios de certificación que no cumplan con los criterios acordados.

Se dispondrá la evaluación y armonización de los aspectos relacionados con el sistema de control de prestadores de servicios de certificación acreditados, en especial aquellos relacionados con:

a) el alcance y la periodicidad de las auditorías, las cuales deben contemplar como mínimo la revisión de las políticas y prácticas de certificación, de seguridad, del ambiente de seguridad física y lógica, la evaluación de tecnología utilizada, los controles sobre la administración de los servicios, la selección y administración del personal y los contratos de tercerización.
b) la identificación de los eventos a ser registrados, la información mínima de cada uno de ellos y los procedimientos para garantizar la integridad y veracidad de los mismos.
c) la documentación respaldatoria del ciclo de vida de los certificados reconocidos.

IV. Criterios para la emisión de certificados reconocidos

Se contemplará la evaluación y armonización del contenido de los certificados reconocidos, con los siguientes requisitos mínimos:

a) la identificación del proveedor de servicios de certificación que lo expide y del Estado del MERCOSUR donde está establecido
b) los datos de identificación del titular del certificado reconocido: nombre y apellido en caso de ser persona física, o la denominación en caso de ser persona jurídica
c) los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del titular del certificado reconocido
d) el periodo de validez del certificado reconocido
e) el número de serie del certificado reconocido
f) la firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado reconocido
g) la indicación del sitio de Internet en el que se encuentra la política de certificación bajo la cual se emitió el certificado reconocido.
h) la indicación del sitio de Internet que permita acceder a la lista de certificados revocados o al servicio de verificación en linea de su estado.

La evaluación y armonización comprenderán también los mecanismos de seguridad utilizados para la protección de los dispositivos de creación de firma.

V. Recomendación para la verificación segura de firma electrónica avanzada

Durante el proceso de verificación de firma deberá garantizarse con suficiente certeza que:

a) los datos utilizados para verificar la firma corresponden a los datos mostrados al verificador;
b) la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente;
c) se puede identificar de forma fiable el documento electrónico firmado;
d) se verifican de forma fiable la autenticidad y la validez de los certificados digitales al momento de la firma del documento electrónico;
e) figuran correctamente el resultado de la verificación y la identidad del firmante;
f) puede detectarse cualquier cambio pertinente relativo a la integridad del documento electrónico firmado.

VI. Otras características de los prestadores de servicios de certificación

Se deberá incluir la evaluación y armonización de otros aspectos relacionados con la prestación del servicio de certificación, como:

a) los procedimientos de verificación de identidad de quien solicite un certificado reconocido.
b) los criterios de confidencialidad de la información suministrada a los prestadores de servicios de certificación
c) la información mínima a ser publicada por el prestador de servicios de certificación
d) las fuentes de hora confiables utilizadas por los prestadores de servicios de certificación en su operatoria, en sus sistemas y registros de auditoría.

Art. 4 - Esta Resolución no necesita ser incorporada al ordenamiento jurídico de los Estados Partes, por reglamentar aspectos de la organización o del funcionamiento del MERCOSUR.

XXXI GMC EXT. – Córdoba, 18/VII/06