TAG-MRTD/15
WP/4
28/4/04

GRUPO TÉCNICO ASESOR SOBRE LOS DOCUMENTOS DE VIAJE DE LECTURA MECÁNICA

Decimoquinta reunión

(Montreal, 17 - 21 de mayo de 2004)

Cuestión 3 del orden del día: **Informe del Grupo de trabajo sobre nuevas tecnologías (NTWG)**
3.1: Información actualizada sobre la elaboración de especificaciones para la utilización de firmas digitales ICP para los DVLM

NUEVO INFORME TÉCNICO — ICP PARA LOS DVLM

[Nota presentada por el Grupo de trabajo sobre nuevas tecnologías (NTWG) y el equipo de trabajo sobre la infraestructura de clave pública (ICP)]

1. En su 14 reunión el TAG respaldó una nota en la que se proponía la utilización de un mecanismo ICP para proteger la seguridad de los datos electrónicos contenidos en los DVLM. El TAG reconoció el hecho de que la nota se limitaba a describir los conceptos relacionados con la utilización de una guía de claves públicas regida por la OACI y las funciones de los Estados expedidores y receptores. Se convino en que era preciso llevar a cabo más labores para especificar el mecanismo con suficiente nivel de detalle para permitir su implantación. Esta labor suplementaria fue realizada por el equipo de trabajo sobre la ICP instituido por el NTWG.

2. Un nuevo informe técnico fue preparado, en el que se presentaba, con detenido nivel de detalle técnico, las especificaciones que pueden ser utilizadas por los Estados expedidores para llevar a la práctica las ICP para proteger la seguridad de los datos electrónicos contenidos en sus documentos de viaje gracias a la firma electrónica del Estado expedidor, el objeto de seguridad especificado en el documento de viaje permite que el Estado receptor verifique la autenticidad e integridad de los datos electrónicos almacenados en la microplaqueta del documento.

3. En el informe técnico también se especifican los requisitos relativos a los Estados y las organizaciones que desean leer los datos electrónicos y describe una guía de claves públicas que la OACI podría crear. El informe recomienda que las claves públicas de las entidades que firman los documentos se almacenen en el microprocesador mismo de los DVLM, pero esta medida es optativa. La guía de claves públicas será de gran utilidad para los expedidores de DVLM, aun cuando la clave pública esté comprendida en el microprocesador del documento.

4. Además, en el informe técnico se proporcionan especificaciones relativas a otras características de seguridad facultativas que pueden ser adoptadas para contrarrestar las amenazas tales como la escucha clandestina y el “despumar” de datos a partir de las microplaquetas sin contacto.

Además, el Estado expedidor puede, a su discreción, adoptar el elemento de seguridad suplementario que en el informe técnico se denomina “control de acceso de base”.

5. En el informe se describe otra característica de seguridad facultativa, “la autentificación activa”. Este dispositivo, tendiente a prevenir la sustitución de microprocesadores, puede llevarse a la práctica en puestos de control sin personal, en los que el DVLM es utilizado como ficha electrónica para permitir el acceso.

6. La redacción y revisión del informe están los suficientemente avanzadas como para que el NTWG considere que ofrece suficiente información detallada para permitir que los Estados comiencen a expedir pasaportes electrónicos. Sin embargo, al llevarse a cabo la implantación, surgirán cuestiones que exigirán que se continúe revisando el informe.

7. El mecanismo ICP está concebido para proteger los datos inscritos en el momento de la expedición del documento, sin actualización. El nuevo reto a que se enfrenta el NTWG es el de concebir un mecanismo ICP interoperable a escala mundial que aceptaría el agregado de datos electrónicos durante todo el periodo de validez del documento. Tal labor sobrepasa el marco del mandato del actual equipo de trabajo.

8. Una serie de “preguntas frecuentes” se proporcionan en TAG-MRTD-WP/10 a título de complemento del informe. Este documento se preparó a raíz de la naturaleza técnica del informe ICP propiamente dicho. Las preguntas fueron inventadas mayormente por los miembros del equipo de trabajo, pero se tiene la intención de actualizar el documento integrando en él las preguntas verdaderas planteadas por los servicios expedidores del DVLM, a medida que surjan.

9. MEDIDAS PROPUESTAS AL TAG/MRTD

9.1 Se invita al TAG/MRTD a respaldar el informe técnico “PKI for Machine Readable Travel Documents Offering ICC Read-only Access” (aplicación de la ICP para los documentos de viaje de lectura mecánica que permiten únicamente la lectura de microprocesadores), versión 1.0.

— FIN —