Control de acceso extendido para pasaportes electrónicos

Alina Surós Vicente
Universidad de las Ciencias Informáticas, Habana, Cuba, asuros@uci.cu

Reynier Lester Claro Escalona
Universidad de las Ciencias Informáticas, Habana, Cuba, rlclaro@uci.cu

Adonis Cesar Legon Campos
Universidad de las Ciencias Informáticas, Habana, Cuba, alegon@uci.cu

RESUMEN

La presente investigación, está referida al análisis de las implementaciones de control de acceso extendido para documentos de viaje de lectura mecánica. Esta medida de seguridad es de caracter opcional, para proteger el acceso a los datos biométricos adicionales incluidos en los pasaportes electrónicos. Actualmente se han realizado dos implementaciones, de la cual la más extendida es la correspondiente a la Unión Europea. Se realiza un análisis de las dificultades que todavía persisten en estas propuestas.

Palabras claves: control de acceso extendido, pasaporte electrónico, medidas de seguridad.

ABSTRACT

This paper is about an analysis of the current Extended Access Control (EAC) implementation, for the machine readeable travel document. The EAC is an optional security feature, intended to protect the access to the biometric information included on the ePassports. At present time there are two main implamntations, and the must widely used is that from the European Union. There is also an analysis of the main difficulties that still remains on this implementations.

Keywords: extented acces control, ePassport, security features

1. INTRODUCIÓN

Los documentos de viaje electrónicos, son los documentos de lectura mecánica (DVLM), que cumplen con las normativas de la Organización de Aviación Civil Internacional (OACI), e incorpora un circuito integrado sin contacto (ICC) como tecnología de almacenamiento de datos, ejemplo de estos documentos son el pasaporte electrónico (pasaporte-e) y las tarjetas de identificación electrónicas que cumplen con estas normativas. La información guardada por el emisor del documento en el ICC del pasaporte-e, debe ser leída e interpretada por cualquier nación, con este objetivo, la OACI establece una serie de normas que deben cumplirse durante el proceso de escritura de la información del portador del documento en el ICC del pasaporte-e.

La forma de organización normalizada de los datos en el ICC se denomina Estructura lógica de datos (LDS), que está conformada por un conjunto de datos, que serán estructurados lógicamente en grupos de datos (DG) opcionales y obligatorios. Estos grupos de datos se identifican por un número de referencia (DG1-DG19). Adicionalmente el ICC contiene, uno denominado común y un objeto de seguridad del documento (OACI/ICAO, 2007).

El acceso a los grupos de datos de la LDS es regido por una serie de medidas de seguridad, de gran importancia para el documento, a continuación se explican brevemente, significando su importancia:

- La **autenticación pasiva**, consiste en la firma de los grupos de datos del documento de viaje y su almacenamiento en el objeto de seguridad, con el objetivo de garantizar la autenticidad e integridad de los datos, es la única medida de obligatoria implementación.
- El **control de acceso básico**, donde la información leída óptica o visualmente es utilizada para generar llaves para autenticarse y luego establecer un canal de comunicación seguro, posee la ventaja de proteger contra lecturas no autorizadas.
- La **autenticación activa**, prueba que el chip es auténtico fundamentalmente a partir de la ejecución de un protocolo reto-respuesta a partir de un par de llaves pública (almacenada en el DG15) y privada (almacenada en la zona segura del ICC), previene contra la sustitución del ICC.
- El **control de acceso extendido** y **cifrado de datos**, asociadas a la seguridad de las características biométricas adicionales que contiene el documento, y su implementación está determinada por la decisión de la nación emisora del documento de viaje electrónico (OACI/ICAO, 2006).

El control de acceso extendido (EAC), se encarga de la protección de acceso a los datos biométricos adicionales (diferentes a la imagen facial, elemento obligatorio), llamados datos sensibles. En este proceso interviene el emisor del documento, encargado de autorizar a la lectura de los datos, el sistema de inspección que intentará leer los datos y podrá hacerlo si se encuentra previamente autorizado y el ICC responsable de verificar que el sistema de inspección que intenta tener acceso a los datos sensibles está autorizado.

2. DESARROLLO

La Organización Internacional de Aviación Civil (OACI/ICAO), entidad encargada de estudiar los problemas de la aviación civil internacional y promover los reglamentos y normas únicos en la aeronáutica mundial, ha puesto a la disposición internacional el pasaporte electrónico (pasaporte-e). El pasaporte-e es la última tecnología en este tipo de documento y su característica fundamental es que almacena elementos biométricos para comprobar la identidad del portador. El pasaporte-e incorpora como tecnología de almacenamiento un circuito integrado sin contacto conforme ISO/IEC 14443.

2.1 PASAPORTE ELECTRÓNICO

Para que un pasaporte pueda ser internacionalmente leído e interpretado es necesario el cumplimiento de una serie de normativas al almacenar los datos en el ICC importantes no solo durante el proceso de emisión sino luego en el proceso de recepción de este pasaporte en el punto de inspección. Esta normalización se encuentra establecida en la estructura lógica de datos (LDS), asegurando los datos almacenados, utilizar las normas internacionales en la mayor medida posible, sobre todo la referida al interfuncionamiento mundial en el área biométrica.

La estructura de lógica de datos del ICC, está conformada por un conjunto de datos, que son agrupados lógicamente en grupos de datos opcionales y obligatorios. Estos grupos de datos se identifican por un número de referencia (DG1-DG19). Adicionalmente a estos grupos de datos el ICC contiene uno denominado común y un objeto de seguridad del documento.

En la *Figura 1*, se muestran los grupos de datos en que se ha organizado la LDS, señalando en rojo los que deben ser incluidos de manera obligatoria.

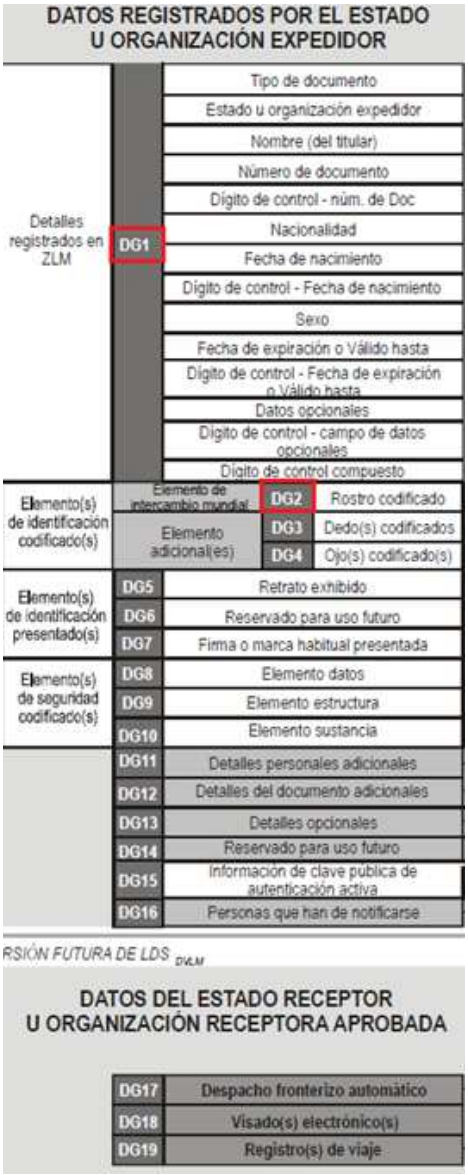

Figura 1. Datos definidos por la OACI para la LDS del ICC (OACI/ICAO, 2006)

2.2 IMPLEMENTACIONES DE EAC

Una de las medidas de seguridad de caracter opcional es el control de acceso extendido, protegiendo a los datos biométricos adicionales (huella e iris) almacenados en los DG3 y DG4. Partiendo del estudio realizado se identifican dos materializaciones de control de acceso extendido EAC, en Singapur (EAC Singapur) y en la Unión Europea (EAC UE). El EAC Singapur, estandarizado a partir de abril de 2006, consiste básicamente en almacenar en el DG14, la llave simétrica necesaria para la comunicación, encriptada con la llave pública del sistema de inspección autorizado para su lectura. (TAG-MRTD, 2006)

El EAC UE, está compuesto por dos mecanismos de seguridad, la autenticación del ICC, que provee una fuerte encriptación de sesión y permite al sistema de inspección verificar que el ICC es genuino. La autenticación del terminal es el segundo mecanismo y permite al ICC verificar que el sistema de inspección está autorizado a tener acceso a los datos sensibles. Está basado en una infraestructura de clave pública (ICP), contando con la presencia en el sistema de inspección de una cadena de certificados, que es enviada al ICC y luego de ser verificada permite el acceso a los datos. La cadena de confianza está formada por los certificados de Autoridad de certificación para la verificación a nivel de país, Verificadores de documentos y Sistemas de inspección. (BSI, 2004)

Teniendo en cuenta los aspectos señalados anteriormente, el EAC Singapur, es estático, pues no existe la posibilidad de adicionar nuevos sistemas de inspección autorizados a los DVLM que han sido personalizados previo a esta nueva autorización. El EAC UE se puede considerar más flexible, pues el proceso de autorización es realizado en la ICP y no tiene influencia en datos almacenados en el ICC. Sin embargo el uso de la ICP acarrea los problemas fundamentales de la ICP están asociados a la administración de los certificados, incluyendo revocación, almacenamiento y distribución de los certificados. Estos problemas son particularmente severos en ambientes con procesamiento y ancho de banda limitados. (Cocks, 2001)

EAC Singapur

El control de acceso extendido implementado en Singapur, ha sido el primero y está basado en ejecutar un comando EXTERNAL AUTENTICATE, comando especificado en la ISO/IEC 7816-4 antes de la operación de lectura. La llave utilizada durante su ejecución es 16-bytes triple-DES, denominada EAC key. Para cada documento es generada una llave diferente, almacenada en el DG13 del ICC encriptada con la llave pública de cada Sistema de Inspección autorizado, como se muestra en la *Figura 2*. El SI debe enviar previamente su llave pública, Kpub para de este modo almacenar la EAC key simétrica correspondiente.

EAC key encrypted using Asymmetric public Key 1 (for IS 1)	EAC key encrypted using Asymmetric public Key 2 (for IS 2)	. . .	EAC key encrypted using Asymmetric public Key n-1 (for IS n-1)	EAC key encrypted using Asymmetric public Key n (for IS n)

Figura 2. Vista conceptual del DG13 (TAG-MRTD, 2006)

El EAC de Singapur, es un esquema poco complejo. Su uso permite adicionar un nivel de protección a los datos sensibles, sin embargo no contempla la posibilidad de adicionar nuevos sistemas de inspección autorizados, en función de nuevos acuerdos bilaterales mediante naciones y ni elementos como revocación de llaves comprometidas.

EAC de la Unión Europea

El control de acceso extendido para los países de la Unión Europea y que debe ser implementado por sus miembros que posean pasaporte electrónico.

EAC UE versión 1

Consiste en dos mecanismos fundamentalmente:

Autenticación del Chip v1: este mecanismo está basado en el protocolo de acuerdo de llaves ephemeral (efímera, temporal)-estática Diffie-Hellmann. La implementación de este protocolo requiere de un par de llaves, la pública se encuentra almacenada en el DG14 y la privada en la zona segura del chip.

Autenticación del Terminal v1: se basa en la presencia en el sistema de inspección de la cadena de certificados, la cual comienza por el certificado emitido por el emisor del MRTD. La llave pública para verificar este certificado está almacenada en el ICC. La ICP definida para este mecanismo de seguridad está conformada por los elementos que se mencionan a continuación y se ilustran en la *Figura 3*.

- Country Verifying CAs (CVCA), emisor de los certificados de los verificadores de documentos. Representa el único punto de confianza del estado emisor. La llave pública para verificar el certificado del DV es almacenada en la zona segura del ICC. Es una autoridad de certificación autorizada por la CVCA.
- Document Verifiers (DV), emisor de los certificados de los sistemas de inspección.
- Inspection Systems (IS), los sistemas de inspección que acceden al ICC.

Los certificados deben ser CVC (Card Verifiable Certificates) o sea certificados verificables en la tarjeta, en este caso en el pasaporte electrónico. Por tanto la cadena de confianza será verificada dentro del ICC. (TAG-MRTD, 2006)

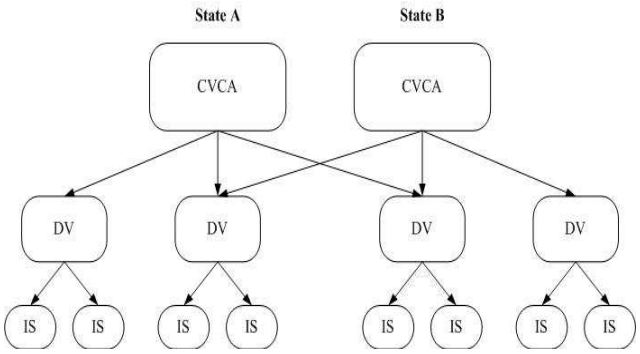

Figura 3. ICP en el EAC de la Unión Europea (TAG-MRTD, 2006)

Este mecanismo está supeditado a la existencia de una ICP, acarreando la administración y distribución de certificados en todos los niveles, ocasionando que este proceso requiera una infraestructura fuerte. Es un punto importante la inexistencia de posibilidad de revocar certificados y de chequear su validez.

Además, debido a que la autenticación del terminal es efectuada luego de la autenticación del chip, pudiera realizarse ataques de denegación de servicio en el caso de un lector malicioso con el envío de certificados inválidos, como el chip tiene memoria limitada, pudiera causar en mal funcionamiento. (Nithyanand, 2009)

EAC UE versión 2

El protocolo en su versión 2 es muy similar, los cambios fundamentales están asociados a la inclusión del mecanismo PACE y la inversión del orden de los pasos, pues se realiza primero la autenticación del terminal. Consiste en la ejecución de forma general de los siguientes pasos:

PACE*:* por las siglas en inglés Password Authenticated Connection Establishment. Consiste, como su nombre lo indica en el establecimiento de la conexión a partir de una contraseña. Se basa en una contraseña autenticada a

partir del protocolo de intercambio de llaves de Diffie-Hellman, que provee una comunicación segura y una autenticación explícita entre el chip y el terminal basada en una contraseña. PACE, permite realizar la autenticación basada en una contraseña o en información impresa en el documento, esta última opción es una variante del BAC, y provee dos ventajas: las llaves de sesión fuertes son proveídas independientemente de la fuerza de la contraseña y que la entropía de la contraseña usada para autenticar puede ser baja. (BSI, 2012)

Autenticación del Terminal v2: este protocolo radica en la ejecución doble del protocolo reto-respuesta que provee una explícita autenticación exclusiva del terminal. En el proceso se autentica una llave pública temporal generada por el terminal que será usada para la mensajería segura durante el siguiente paso que es la autenticación del chip. Se verifica en el chip la cadena de certificados que es enviada por el terminal. La ICP propuesta mantiene la de la versión 1 expresada en *Figura 4*Figura 3. ICP en el EAC de la Unión Europea. (BSI, 2012)

Autenticación del chip v2: este mecanismo está basado en el protocolo de acuerdo de llaves estática-temporal Diffie-Hellmann que provee una comunicación segura y una autenticación exclusiva del chip. En su versión 2 este protocolo provee la autenticación explícita del chip mediante la verificación de un token de autenticación y una autenticación implícita de los datos almacenados ejecutando mensajería segura a partir de nuevas llaves de sesión. (BSI, 2012)

Consideraciones de la ICP

En diciembre de 2012, el BSI (Oficina Federal para la Seguridad en Tecnologías de la Información de Alemania), establece una política de certificación común (CP) para los pasaportes y documentos de viaje emitidos por estados de la Unión Europea. El objetivo es la confianza e interoperabilidad entre los CVCA y DV de los diferentes estados para la ICP-EAC.

A partir de este CP se proveerá un conjunto mínimo de requerimientos con cada SPOC (Single Point of Contact) único punto de contacto, CVCA y DV de los estados miembros deben cumplir, cuando actúan como subscritor bajo una CVCA externa. Los estados miembros deben escribir su CP nacional, como se muestra en la *Figura 4*. (BSI, 2004)

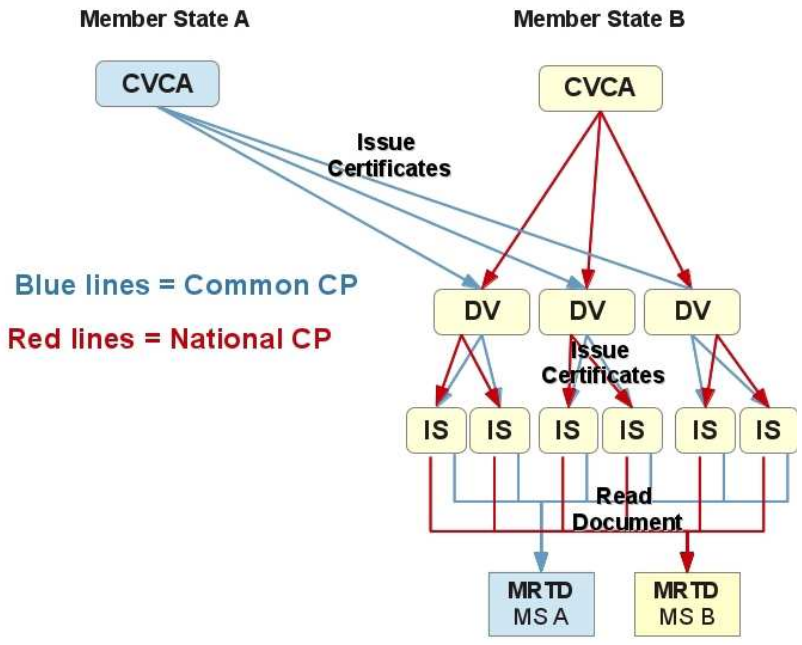

Figura 4. Ámbito del CP común y el CP nacional (BSI, 2004)

Los períodos de validez de los certificados definidos son: (BSI, 2004)

- CVCA (min 6 meses – max 1 año)
- DV (min 2 semanas – max 3 meses)
- IS (min 1 día – max 1 mes)

El SPOC actúa como una interface de comunicación entre los estados miembros. Permite una comunicación online. Cada estado debe operar exactamente un único SPOC, que es la interfaz de comunicación técnica entre los estados concernientes a pasaportes electrónicos y permiso de residencia dentro del ICP-EAC (*Figura 5*).

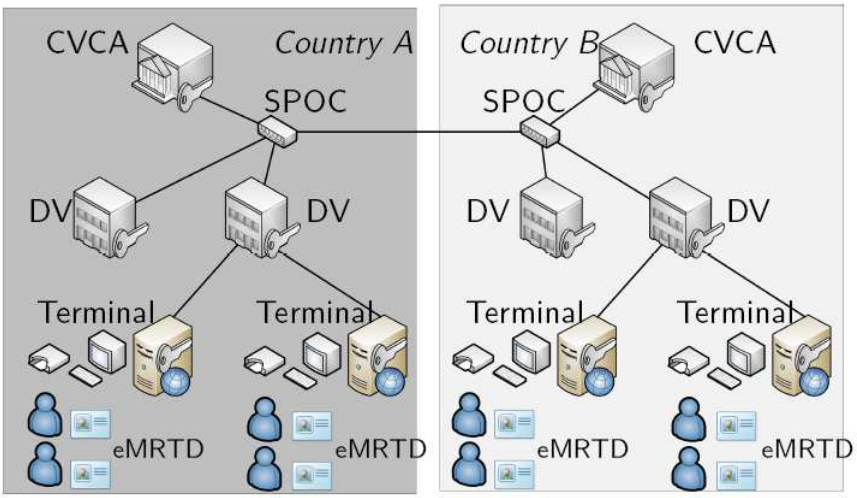

Figura 5. SPOC en la ICP EAC-UE (Harald Baier, 2012)

El SPOC especifica el protocolo de administración de llaves en operación a través de las fronteras internacionales, entre los CVCA componentes de la arquitectura EAC para pasaportes electrónicos y las autoridades de certificación DV. Es usado para el intercambio de llaves y certificados, con el objetivo de: (BSI, 2009)

- El DV pueda enviar una solicitud de certificado a una CVCA exterior.
- La CVCA pueda enviar el certificado al DV solicitante.
- El DV y la CVCA puedan solicitar la lista de certificados válidos necesarios para tener acceso a un pasaporte externo.
- Mensajes de forma general que puedan ser intercambiados entre las entidades del ICP-EAC.

Esta especificación cubre dos canales principales: (BSI, 2009)

- Intercambio manual de datos almacenados en (CD-R,DVD+/-R, memorias USB) o publicada en internet.
- *Web services.*

La comunicación con el *Web Service*, debe realizarse usando *HTTPS* con *TLS* autenticando cliente y servidor. Toda la comunicación debe ser realizada vía internet. Los principales métodos contenidos en el *WSDL* especificado en (BSI, 2009) son:

GeneralMessage (callerID As string , messageID As string , subject As string , body As string)

GetCACertificates (callerID As string , messageID As string)

RequestCertificate (callerID As string , messageID As string , certificateRequest As base64Binary)

SendCertificates (callerID As string , messageID As string , As , statusInfo As)

Aunque mejora algunos elementos de seguridad, como los ataques de denegación de servicio y el SPOC, en esta versión persisten como brechas la verificación de la validez de la cadena de certificados.

3. CONCLUSIONES Y RECOMENDACIONES

Concluyendo los elementos presentados en el trabajo, se puede expresar que todavía persisten dificultades en los esquemas de control de acceso extendidos implementados, los cuáles radican en que:

En el caso de Singapur, no puede ser adicionado un sistema de inspección autorizado luego de personalizado el documento, lo cual hace que la solución sea muy rígida y con gran impacto en el servicio a los viajeros en los puntos de control migratorio. Este esquema no tiene en cuenta el caso de que una llave sea comprometida, con un mecanismo para su revocación Además de que se comprometerían las llaves de los demás pasaportes, debido a que la llave es la misma por cada terminal de verificación y se incluye en cada documento. Un sistema de inspección corrupto, puede compartir la llave simétrica luego de obtenerla.

En el EAC de la Unión Europea en sus dos versiones, una solución más sólida que la propuesta por Singapur, persisten que el ICC no posee reloj interno, por lo tanto la fecha depende de la última actualización realizada según el último certificado leído. Si una llave ha sido comprometida, no puede ser revocado el certificado pues el ICC no verifica contra listas de revocación.

4. REFERENCIAS

BSI. (2004). Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC). TR-03110.

BSI. (2009). ČSN 36 9791. Information technology – Country Verifying Certification Authority Key Management Protocol for SPOC.

BSI. (2012). Technical Guideline TR-03110-1. Advanced Security Mechanisms forMachine Readable Travel Documents –.

BSI. (2012). Technical Guideline TR-03110-2. Advanced Security Mechanisms forMachine Readable Travel Documents. Part 2 – Extended Access Control Version 2 (EACv2),Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI).

BSI. (2012). TR-03139. COMMON CERTIFICATE POLICY FOR THE EXTENDED ACCESS CONTROL INFRASTRUCTURE FOR PASSPORTS AND TRAVEL DOCUMENTS ISSUED BY EU MEMBER STATES.

Cocks, C. (2001). An Identity Based Encryption Scheme based on Quadratic Residues.

Harald Baier, N. B. (2012). Security Protocols and Infrastructures. Chapter 7: Security Protocols for Electronic ID Cards.

ISO/IEC. (2005). ISO/IEC 7816-4. Identification cards — Integrated circuit cards —Part 4: Organization, security and commands for interchange.

Nithyanand, R. (2009). A Survey on the Evolution of Cryptographic Protocols in ePassports.

OACI/ICAO. (2006). Documento 9303. Parte 1 Pasaportes de lectura mecánica. Volumen 2 Especificaciones para pasaportes electrónicos con capacidad de identificación biométrica.

OACI/ICAO. (2007). Documento 9303. Parte 1 Pasaportes de lectura mecánica. Volumen 1 Pasaportes con datos de lectura mecánica almacenados en formato óptico de reconocimiento de caracteres. OACI/ICAO.

TAG-MRTD. (2006). EXTENDED ACCESS CONTROL. Montreal: ICAO/OACI.

Authorization and Disclaimer