[1. INTRODUCCION 2](#_Toc325035821)

[1.1 Propósito: 2](#_Toc325035822)

[1.2 Ámbito del sistema 2](#_Toc325035823)

[1.3 Definiciones, Acrónimos y Abreviaturas 2](#_Toc325035824)

[1.4 Referencias 3](#_Toc325035825)

[1.5 Visión general del documento 3](#_Toc325035826)

[2. DESCRIPCION GENERAL 4](#_Toc325035827)

[2.1. Perspectiva del producto 4](#_Toc325035828)

[2.2. Funciones del producto 5](#_Toc325035829)

[2.3. Características de los usuarios 6](#_Toc325035830)

[2.4. Restricciones 6](#_Toc325035831)

[2.5. Suposiciones y dependencias 6](#_Toc325035832)

[2.6. Requisitos futuros 6](#_Toc325035833)

[3. REQUERIMIENTOS ESPECIFICOS 7](#_Toc325035834)

[3.1. REQUERIMIENTOS DE SEGURIDAD FISICO 7](#_Toc325035835)

[3.2. REQUERIMIENTOS DE SEGURIDAD LOGICOS 9](#_Toc325035836)

[3.3. REQUERIMIENTOS DE SEGURIDAD DURANTE LA FABRICACION 10](#_Toc325035837)

[3.4. REQUERIMIENTOS DE SEGURIDAD DEL DISPOSITIVO ENTRE EL FABRICANTE Y LA CARGA INICIAL LA CLAVE 11](#_Toc325035838)

[3.5. Funciones 11](#_Toc325035839)

[3.6. Requisitos de rendimiento 13](#_Toc325035840)

[3.7. Restricciones del Diseño 13](#_Toc325035841)

# INTRODUCCION

El presente documento describirá detalladamente la etapa de elicitación y análisis de requerimientos para el desarrollo de un “Hardware Security Module” (HSM). El cual será desarrollado en el Laboratorio de Arquitectura de Computadoras (LAC) de la facultad de Ciencias Exactas, Físicas y Naturales (FCEFyN) de la Universidad Nacional de Córdoba (UNC).

El HSM permitirá manipular y almacenar datos de forma segura utilizando [criptografía](http://es.wikipedia.org/wiki/Criptograf%C3%ADa) de clave pública o “Public Key Criptography” (PKI) para la emisión de certificados firmados digitalmente.

Estos dispositivos son caracterizados por su poderoso procesamiento criptográfico y administración de claves para aplicaciones donde la seguridad y desempeño son la prioridad máxima.

## Propósito:

Este documento deja evidencia de los requerimientos para la construcción de un dispositivo HSM. El mismo esta dirigido a los Ingenieros en Computación que deseen desarrollar un HSM para su futura utilización en un Laboratorio de Firma Digital (LFD).

## Ámbito del sistema

El sistema permitirá la emisión de certificados firmados digitalmente, donde dicho certificado será almacenado un dispositivo de seguridad llamado “token”. Los token almacenan de forma segura la clave privada asociada a la persona física que obtuvo el certificado digital. Además, el sistema brindara confidencialidad de los datos emitidos/recibidos entre los servidores involucrados en el proceso de la firma.

## Definiciones, Acrónimos y Abreviaturas

|  |  |
| --- | --- |
| Autoridad Certificante (AC) | Entidad de confianza, responsable de emitir y revocar los [certificados digitales](http://es.wikipedia.org/wiki/Certificado_digital) , utilizados en la [firma electrónica](http://es.wikipedia.org/wiki/Firma_electr%C3%B3nica), para lo cual se emplea la [criptografía](http://es.wikipedia.org/wiki/Criptograf%C3%ADa) de [clave pública](http://es.wikipedia.org/wiki/Clave_p%C3%BAblica). |
| Autoridad de Registro (AR) | Entidad de confianza encargada de controlar la generación de certificados para los miembros de una entidad. Previa identificación, la Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes. |
| CRL | Lista de certificados (más concretamente sus números de serie) que han sido revocados, los cuales no son válidos y en los que no debe confiar ningún usuario del sistema. |
| Online Certificate Status Protocol (OCSP) | Método para determinar el estado de revocación de un certificado digital X.509. Este protocolo se describe en el RFC 2560 y está en el registro de estándares de Internet. |
| EJBCA | Aplicación open source para gestión de la autoridad de certificación basado en la tecnología JEE. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Referencias

Para la elaboración de este documento se tuvieron en cuenta los siguientes estándares y recomendaciones:

* FIPS 140-2: requerimientos de seguridad para módulos criptográficos. Se agrega un anexo resumen de dicha norma.
* PCI Security Standards Council: es un foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas. <https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf>
* NIST Special Publication 800-22: conjunto de pruebas estadísticas para los generadores de números aleatorios y pseudo-aleatorio para las aplicaciones criptográficas
* EJBCA: aplicación open source para el servidor que cumple la funcionalidad de Autoridad Certificante (CA).
* <http://www.ejbca.org/>

## Visión general del documento

Este documento describe los requerimientos elicitados para el desarrollado de un dispositivo “Hardware Security Module” (HSM) que será utilizado como módulo de hardware para guardar el Certificado Raíz de la Autoridad de Certificación (AC) del Laboratorio de Firma Digital de la Universidad Nacional de Córdoba.

El formato utilizado en su elaboración es el recomendado como Especificación de Requerimientos Software (ERS) del estándar IEEE 830.

# DESCRIPCION GENERAL

Los HSM son la solución más segura y de mayor rendimiento para la protección de las claves criptográficas y la provisión de servicios de cifrado, descifrado, autenticación y servicios de firma digital. Estos módulos están diseñados para una integración estrecha con un servidor de aplicación y son típicamente ubicados en un entorno seguro y gestionado a través de controles de acceso y procedimientos, externos al dispositivo.

## Perspectiva del producto

Un HSM habitualmente está administrado por una aplicación que corre en el servidor de la Autoridad Certificante (AC). Este servidor puede ejecutar una herramienta para administración de PKI tal como Enterprise Java Bean Certification Authotiry (EJBCA), la cual propone la infraestructura de red que muestra la Figura jj, para la emisión y gestión de certificados digitales.



Figura 1: Zonas componentes de topología de red de AC

En la Figura 1 se puede observar que los dos firewall generan claramente tres zonas:

* Zona externa: Es la zona de acceso público para los miembros de la organización, habitualmente conectada a internet a través de un router. Desde esta zona se tiene acceso a servicios específicos de la zona desmilitarizada, a través del Firewall 1, mientras que está bloqueado totalmente el acceso a la zona interna.
* Zona desmilitarizada: En esta red se encuentran habitualmente el servidor de la Autoridad de Registro (AR) y el Servidor para consulta de certificados, utilizando el protocolo OCSP. El tráfico desde esta zona a la zona interna está habilitado para determinados servicios habilitados en el Firewall 2.
* Zona interna: Esta zona es la más segura. Desde ella se puede acceder a la zona desmilitarizada, pero no se puede acceder a la zona externa. En ella se encuentra el Servidor de la AC, el HSM y el Servidor de Backup. El HSM está directamente conectado al Servidor de la AC.

El Servidor de la AC tiene la aplicación encargada de la gestión de los certificados digitales. Esto incluye las tareas de revocación de certificados. Los certificados revocados conforman la “[Certificate Revocation List](http://es.wikipedia.org/wiki/Certificate_Revocation_List" \o "Certificate Revocation List)” (CRL), y es responsabilidad de la AC publicarla y actualizarla de acuerdo a la Política de Certificación. Por otra parte, otra tarea que debe realizar una AC es la gestión asociada a la renovación de certificados por caducidad o revocación. Por otro lado, si la AC emite gran cantidad de certificados, corre el riesgo de que sus CRL sean también de gran tamaño, lo que hace poco práctica su descarga por parte de terceros. Esto ha motivado el desarrollo de mecanismos alternativos de consulta de certificados revocados, como “Online Certificate Status Protocol” (OCSP).

El Servidor de OCSP habilita el servicio de consulta utilizando el protocolo OCSP. Los mensajes OCSP se codifican utilizando “Abstract Syntax Notation One” ([ASN.1](http://es.wikipedia.org/wiki/ASN.1)) y habitualmente se transmiten sobre el protocolo [HTTP](http://es.wikipedia.org/wiki/HTTP). OCSP está especificado en la [RFC 2560](http://tools.ietf.org/html/rfc2560). En ella se definen las características que debe cumplir un servidor OCSP, así como el formato tanto de la petición como de la respuesta. Ambas estructuras de datos se representan según la sintaxis ASN.1.

La función del servidor de la Autoridad de Registro (AR) es permitirle al oficial de registro de una AR controlar la generación de certificados para los usuarios que lo soliciten. Previo control de la identidad del usuario por parte del oficial, la aplicación de la AR se encarga de realizar la petición de la emisión de un certificado y guardar los datos pertinentes en un dispositivo seguro como un token, el cual es entregado al usuario. Sintéticamente, sus funcionalidades son:

* Registrar las solicitudes de los usuarios de certificados nuevos y renovados.
* Permitir al oficial de registro de la AR dejar constancia de la comprobación de la veracidad y corrección de los datos que aportan los usuarios para su identificación, de acuerdo a la Política de Certificación.
* Enviar las peticiones de emisión de certificados a la AC.

## Funciones del producto

EL HSM almacena información “sensible” de la AC. Concretamente, el Certificado Digital entregado por la AC Raíz a la AC. Con esta información, la AC puede firmar los certificados digitales que emite para sus usuarios.

Por otro lado, el HSM garantiza la seguridad en la comunicación que establece con el Servidor AC, proporcionando servicios de confidencialidad e integridad, mediante la ejecución de algoritmos de cifrado y descifrado.

Las funcionalidades internas y datos almacenados en el HSM se los consideran datos “sensibles”, por lo que son almacenados de manera confiable, garantizando su integridad.

## Características de los usuarios

Se pueden reconocer varios roles de usuarios. Entre ellos se encuentran los analistas técnicos del HSM, encargados de su inicialización. Los administradores, que conjuntamente con otros usuarios definidos en la Política de Seguridad de la AC, podrán llevar adelante tareas de mantenimiento. Estas tareas incluyen la instalación del Certificado de la AC y procedimientos de backup, entre otros. A ellos hay que sumarles la posibilidad de disponer de pares de usuarios que habiliten funciones específicas, conjuntamente con el administrador y los analistas técnicos.

Por ejemplo, es frecuente que en la Política de Seguridad de la AC, se defina más de un rol, como necesarios para llevar adelante funciones en el HSM. Concretamente, para realizar una operación de backup, será necesaria la presencia del administrador y al menos un usuario más que habiliten al operador a realizar la tarea.

## Restricciones

En esta sub-sección se describirá aquellas limitaciones impuestas sobre los desarrolladores del producto. Estas son:

* Limitaciones de hardware: el hardware utilizado para la construcción del prototipo de HSM debe ser alguno de los kit de desarrollo, disponibles en el Laboratorio de Arquitectura de Computadoras de la FCEFyN de la UNC.
* Interfaces con otras aplicaciones: el HSM implementará funcionalidades que serán requeridas por el Servidor de la AC, el cual correrá EJBCA. Por ello, se deberá poder contar con evidencias de que las funcionalidades habilitadas con EJBCA podrán ser satisfechas siempre y cuando se trate de estándares.
* Lenguaje(s) de programación: Se deberá utilizar lenguaje orientado a objetos.
* Protocolos de comunicación: Para garantizar los servicios de seguridad de la comunicación entre HSM y Servidor de la AC se debe utilizar protocolos seguros como SSLv3.0.
* Criticidad de la aplicación: se trata de un elemento de criticidad alta en la estructura de una AC.
* Consideraciones acerca de la seguridad:….

## Suposiciones y dependencias

La construcción de este prototipo de HSM depende fuertemente del kit de desarrollo seleccionado para su construcción. Si se decide cambiar el kit de desarrollo, se recomienda revisar y validar la implementación de cada uno los requerimientos funcionales del HSM.

## Requisitos futuros

En la fase de prototipo, la comunicación entre el HSM y el servidor será mediante puerto USB. Queda como una posible mejora a futuro la comunicación utilizando interface Ethernet.

# REQUERIMIENTOS ESPECIFICOS

En esta sección se definirán el conjunto de requerimientos funcionales y de seguridad para la construcción de un prototipo de HSM. Para ambos, se distinguirán entre requerimientos físicos, requerimientos lógicos y requerimientos que aplican al proceso de fabricación y requerimientos para la carga inicial.

## REQUERIMIENTOS DE SEGURIDAD FISICO

El prototipo de HSM debe cumplir los siguientes requerimientos de seguridad físico:

|  |  |  |
| --- | --- | --- |
| Número | Descripción del requerimiento | |
| A1 | | Una de las siguientes opciones A1.x deben cumplirse |
| A1.1\* | | El HSM debe utilizar mecanismos que detecten intentos de manipulación física. En el caso de producirse, se debe borrar automática e inmediatamente toda la información sensible en él contenida. Luego, será inviable recuperar dicha información. |
| A 1.2 | | La protección contra una amenaza debe estar basada en una combinación de al menos dos mecanismos de seguridad independientes; y el fallo de un solo mecanismo de seguridad no compromete la seguridad del HSM.  El HSM también debe incluir características tales que permitan poner en evidencia, con una alta probabilidad, la manipulación de los resultados del dispositivo. |
| A2 | | No debe ser posible determinar cualquier información sensible monitoreando las emisiones electromagnéticas, el consumo de energía, o cualquier otra característica interna o externa. |
| A3 | | EL diseño del HSM debe tener un mecanismo que lo proteja contra sustitución, de tal forma que no sea posible construir un duplicado a partir de componentes disponibles comercialmente y proceder a su reemplazo. Por ejemplo, el gabinete de un HSM no suele estar disponible comercialmente. |
| A4 | | La información y funciones sensibles sólo deben ser utilizadas en las áreas protegidas del HSM. El manejo de la información y funciones con información sensible deben estar protegidas contra la modificación o sustitución, al igual que las claves secretas y privadas. |
| A5 | | Si el dispositivo permite el acceso a las áreas internas de seguridad que contienen componentes sensibles (p.e. para el servicio o mantenimiento), el acceso inmediato a datos sensibles tales como PINS o datos criptográficos deben estar impedidos por el diseño de las áreas internas (p.e. encapsular los componentes en un gabinete anti-sabotaje o sensible a su manipulación), o tener un mecanismo de modo tal que al acceder a las áreas internas se produzca el inmediato borrado de los datos sensibles. |
| A6 | | Debe existir una política de seguridad, disponible para el proveedor, para el uso correcto del HSM. Debe incluir información sobre responsabilidades en la gestión de claves, responsabilidades administrativas, funcionalidades del dispositivo, identificación y requerimientos de medio ambiente. La política de seguridad debe definir las funciones compatibles con el HSM e indicar los servicios disponibles para cada función de forma tabular y clara.  El HSM debe ser capaz de realizar sólo las funciones planteadas, p.e. no hay funcionalidades ocultas. Las únicas funciones habilitadas a efectuar por el HSM son aquellas permitidas por las políticas de seguridad. |
| A7 | | La seguridad del HSM no se debe ver comprometida por las condiciones del medio ambiente o de funcionamiento (p.e. someter al HSM a temperaturas o voltajes de operación fuera de los rangos de funcionamiento establecidos no debe comprometer su seguridad). |

## REQUERIMIENTOS DE SEGURIDAD LOGICOS

El prototipo de HSM debe cumplir los siguientes requerimientos de seguridad lógicos

|  |  |
| --- | --- |
| Numero | Descripción del requerimiento |
| B1\* | Debe proporcionar interfaces seguras, mantenidas lógicamente separadas, distinguiendo entre datos y control para las entradas, y entre datos y estados para las salidas. |
| B2 | No deben existir mecanismos que permitan:   * La salida de claves privadas o secretas en texto plano. * La encriptación de una clave o PIN, con una clave que pueda ser revelada. * La transferencia de una clave desde una parte de alta seguridad a una parte de baja seguridad.   Las funciones de encriptación implementadas en el “Cryptographic Service Providers” (CPS) no deben entregar texto plano a partes del HSM que afecten negativamente la seguridad. |
| B3 | Las técnicas de administración de claves implementadas en el HSM se deben ajustar normas del tipo **ISO 11568** y/o **ANSI X9.24**. Estas técnicas deben ser compatibles con **ANSI TR-31** o una metodología equivalente para mantener el conjunto de claves del **TDEA.** |
| B4\* | El ingreso de claves privadas y secretas, se debe realizar utilizando técnicas aceptadas de acuerdo a la siguiente tabla:   |  |  |  |  | | --- | --- | --- | --- | | Forma de clave | **Técnicas** | | | | **Manual** | **Directa (\*\*)** | **Red** | | Clave en texto plano | No | Yes | No | | Componentes de  clave en texto plano | Yes | Yes | No | | Claves cifradas | Yes | Yes | Yes |   (\*\*) Por puerto tipo consola. |
| B5 | El HSM debe requerir de al menos dos operadores autenticados por separado para la administración local de los servicios que normalmente no están disponibles, como la carga de texto plano, habilitación/deshabilitación de funciones de seguridad, o modificación de datos de autenticación. Las entradas o salidas manuales no encriptadas de los CSPs requieren al menos un operador autenticado. El HSM debe limitar el número llamadas a funciones (servicios) y el tiempo límite para estos servicios. Si el límite es excedido, se requiere una re-autenticación. |
| B6\* | El HSM asegura que cada clave cifrada sea usada solo para una única función criptográfica y solo para su finalidad prevista. Ej.: No debe ser posible cifrar o descifrar arbitrariamente cualquier información utilizando cualquier clave de encriptación contenida en el HSM. |
| B7 | El HSM debe asegurar que si las claves cifradas dentro de los límites de seguridad del HSM son inválidas por cualquier razón (p.e., la manipulación o ausencia a largo plazo de la energía eléctrica), el HSM producirá un error de manera segura. |
| B8\* | Se debe evaluar el generador de números aleatorios para garantizar que sus números aleatorios sean lo suficientemente impredecibles. |
| B9 | Las funciones del HSM no deben estar influidas por las anomalías lógicas, tales como (pero no se limitan a estas) secuencias inesperadas de comandos, comandos desconocidos, comandos en un modo incorrecto a un dispositivo y el suministro de parámetros erróneos. |
| B10 | EL firmware y cualquier actualización posterior del mismo, debe garantizarse que ha sido inspeccionado y revisado mediante un proceso documentado y verificado, y certificado como libre de funciones ocultas no autorizadas o no documentadas. |
| B11 | El HSM debe limpiar o reinicializar automáticamente los buffer internos con información sensible cuando:   * La transacción se ha completado, o * El HSM tenga agotado el tiempo o * El HSM se recupera de un estado de error. |
| B12\* | EL HSM utiliza algoritmos criptográficos, modos y tamaños de claves aceptados. |
| B13 | SI el HSM es diseñado para ser usado para la gestión de PIN, este debe cumplir con los requerimientos de administración de PIN de la norma ISO 9564. La técnica de encriptación de PIN implementad en el HSM están contenidas en la ISO 9564. |
| B14\* | Para asegurar que el HSM está operando de acuerdo a su diseño, el dispositivo debe ejecutar “self-test” comprobando el firmware al menos una vez al día y cuando se encienda. Para ello debe disponer de mecanismos de seguridad en busca de signos de manipulación, y comprobar si el HSM esta en un estado comprometido. Cuando se realizan determinadas operaciones definidas como críticas, el HSM realiza pruebas restringidas. Las técnicas y acciones del HSM ante fallos de un “self-test” son consistentes con aquellas definidas en **FIPS PUB 140-2.** |
| B15 | El HSM debe incluir mecanismos criptográficos para soportar la conexión segura de transacciones, intercambio de datos y eventos generados para su auditoría. |
| B16 | El HSM debe tener la capacidad de devolver su ID. |
| B17\* | El acceso a servicios sensibles debe requerir autenticación. Los servicios sensibles proporcionan acceso a las funciones sensibles subyacentes.  Las funciones sensibles son aquellas que procesan información sensible, tales como las claves de cifrado y contraseñas. La entrada o salida de funciones sensibles no deben revelar o afectar la información sensible. |
| B18 | Si el HSM permite actualizar el firmware, el dispositivo criptográfico debe autenticar la integridad del firmware, en caso que la autentificación no sea confirmada, la actualización del firmware se debe rechazar y eliminar. |

## REQUERIMIENTOS DE SEGURIDAD DURANTE LA FABRICACION

|  |  |
| --- | --- |
| Número | Descripción del requerimiento |
| C1 | Se debe habilitar un procedimiento de control de cambios. |
| C2 | Se debe proteger el firmware almacenado, de manera que no haya modificaciones no autorizadas del mismo, p.e., utilizando procedimientos de autenticación criptográficos de control dual o estandarizados. |
| C3 | El HSM debe estar ensamblado de forma tal que los componentes utilizados en el proceso de fabricación sean aquellos componentes que fueron certificados por la evaluación de Requerimientos de Seguridad Física. Además se debe garantizar que no hayan ocurrido sustituciones no autorizadas. |
| C4 | El software de producción que se carga en el dispositivo en el momento de la fabricación debe ser transportado, almacenado, y utilizado bajo los principios de control dual, previniendo las modificaciones y/o sustituciones no autorizadas. |
| C5 | Posterior a la producción, y antes del despacho desde las instalaciones del fabricante, el HSM y cualquiera de sus componentes deben ser almacenados en un área protegida con control de acceso, embalados y sellados con precinto de seguridad de manera que sea posible detectar el acceso no autorizado al dispositivo o a sus componentes. |
| C6 | Si el HSM se autenticara con la “Key Loading Facility” utilizando información secreta colocada durante la fabricación del dispositivo, esta información secreta deber ser única para cada HSM, desconocida e impredecible para cualquier persona, e instalada en el HSM bajo control dual para asegurar que no se revelen durante la instalación. |

## REQUERIMIENTOS DE SEGURIDAD DEL DISPOSITIVO ENTRE EL FABRICANTE Y LA CARGA INICIAL LA CLAVE

|  |  |
| --- | --- |
| Número | Descripción del requerimiento |
| D1 | Los HSM deben ser enviados desde la fábrica hasta el sitio de carga inicial de claves, bajo controles de verificación que pueden reportar la ubicación de todos los HSM en cualquier momento. |
| D2 | Deben existir procedimientos que permitan auditar el dispositivo, desde su fabricación hasta la carga inicial de claves. |
| D3 | Mientras se envía desde la fabrica hasta el sitio de carga inicial de claves, el dispositivo esta:   * Transportado y almacenado en un paquete embalado con precinto de seguridad; y/o * Transportado y almacenado conteniendo un secreto, el cual será borrado inmediatamente y automáticamente si se intenta cualquier alteración física o funcional del dispositivo, el cual puede ser verificado en la instalación de carga inicial de la claves, pero que no puede ser comprobada por personal no autorizado. |

## Funciones

Los servicios que debe brindar el HSM son los siguientes:

Establecer un canal seguro de comunicación con el Servidor AC

El HSM negociará el establecimiento de un canal seguro con el Servidor de la AC para brindar servicios de seguridad a toda información que se intercambie entre ellos, de manera de cumplir con el Requerimiento Lógico B15.

Firmar certificados

El HSM firmará los certificados digitales que emita la AC. La AC le enviará el CD con información del usuario solicitante. El HSM lo recibirá y lo firmará utilizando la información del certificado raíz de la AC, en él almacenado. Luego le entregará a la AC el CD firmado.

Realizar pruebas automáticas

El HSM efectuara periódicamente pruebas automáticas de integridad sobre su información sensible, de modo que pueda detectar cambios en su funcionalidad y eventualmente producir el borrado de los datos si la seguridad del sistema se ve comprometida. El objetivo de estas pruebas es dar cumplimiento al requerimiento lógico B14.

Realizar “Power On Self Test” ( POST )

El HSM efectuará un test automático, cada vez que sea encendido. Deberá controlar el correcto funcionamiento de sus partes, la integridad de su firmware y avisar mediante alarma en caso de falla de funcionamiento o errores de integridad.

Carga inicial de claves

El HSM recibirá de manera segura la información sensible que en él se vaya a guardar, por ejemplo el Certificado Raíz de la AC.

## Requisitos de rendimiento

Las operaciones criptográficas son tareas que requieren gran capacidad de cálculo por parte de la CPU. Es recomendable la utilización de una arquitectura de procesamiento con un procesador especializado en estas funciones.

## Restricciones del Diseño

Limitaciones de hardware

El hardware utilizado para la construcción del prototipo de HSM debe ser un kit de desarrollo disponible en el Laboratorio de Arquitectura de Computadoras de la FCEFyN de la UNC. En lo posible debe utilizarse un kit que provea de interface Ethernet para su comunicación con el Servidor de la AC y un hardware específico para funciones criptográficas.

Interfaces con otras aplicaciones

Las funcionalidades implementadas en el HSM serán requeridas por una aplicación construida en el Servidor de la AC, utilizando EJBCA.

Lenguaje(s) de programación

El HSM será modelado en las etapas de elicitación, análisis de requerimientos y diseño como un objeto con comportamiento y conocimiento, siguiendo las directivas de un diseño orientado a objetos.

Protocolos de comunicación

Para garantizar los servicios de seguridad en la comunicación entre HSM y Servidor de la AC se debe utilizar protocolos seguros como SSLv3.0.

Criticidad de la aplicación

El HSM es un elemento de criticidad alta en la estructura de una AC.

Consideraciones acerca de la seguridad:….