BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

ESTÁNDAR FISICO

FIRMA DIGITAL

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

EF-FDI

BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

ESTÁNDAR FISICO

FIRMA DIGITAL

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

EE-FDI

Tabla de contenido

1. Introducción **1**
2. Alcance **1**
3. Términos empleados **1**
4. Documentos aplicables y anexos **2**
5. Controles físicos **2**
5.1. Proceso de verificación y aceptación de lectores de huellas dactilares, cámara fotográfica y lectores de tarjetas inteligentes 3
5.2. Proceso de homologación de dispositivos criptográficos (tarjetas inteligentes) 3
5.3. Instalaciones físicas de las OR 3
5.3.1. Mobiliario y equipo - Recinto de emisión de certificados digitales 4
5.3.2. Mobiliario y equipo - Quiosco de activación de certificados digitales 4
5.3.3. Características y dimensiones físicas 5
5.3.3.1. Recinto de emisión y Quiosco de activación separados *5*
5.3.3.2. Recinto de emisión y Quiosco de activación en un mismo cubículo *6*
5.4. Requisitos de Seguridad 7
6. Anexos **8**
6.1. Especificaciones técnicas 8
6.1.1. Anexo No. 1: Lector de Huellas Dactilares 8
6.1.2. Anexo No. 2: Cámara Fotográfica Digital 9
6.1.3. Anexo No. 3: Especificaciones Fotográficas 10
6.1.4. Anexo No. 4: Cámara para circuito cerrado de T.V. 11
6.1.5. Anexo No. 5: Lector de Tarjetas Inteligentes 11
6.1.6. Anexo No. 6: Dispositivos criptográficos (Tarjetas inteligentes) – PKI 12
6.1.7. Anexo No. 7: Diseño de la tarjeta inteligente - PKI 16
6.1.8. Anexo No. 8: Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV 19
6.1.9. Anexo No. 9: Diseño de la tarjeta inteligente – PKI sobre Tarjetas de Pago certificadas por EMV 23
6.1.10. Anexo No. 10: Proceso de homologación de dispositivos criptográficos para el almacenamiento de certificados de firma digital 24
7. Disposiciones transitorias **61**
7.1. De los requerimientos condicionados 61

Sistema Nacional de Pagos Electrónicos

Sistemas de Pago - BCCR Año 2015

1. Introducción

Este libro establece los requisitos relacionados con la infraestructura física y de seguridad así como otras consideraciones generales que deben cumplir las entidades que funjan como Oficinas de Registro (OR) de la Autoridad Certificadora (CA) del Sistema Nacional de Pagos Electrónicos (SINPE) y así gestionar certificados digitales dentro de la jerarquía nacional de certificadores registrados de Costa Rica.

2. Alcance

Los requisitos y disposiciones contenidas en este documento son de acatamiento obligatorio por parte de las entidades que funjan como OR, las cuales, para poder operar deben cumplir con los estándares aquí establecidos.

3. Términos empleados

Para los fines del presente documento, se entenderá por:

- AR: Agente de Registro, es la persona responsable de la ejecución de las actividades propias de la OR, debe realizar las validaciones y verificaciones definidas en la política del certificado que corresponda, así como firmar digitalmente la evidencia presencial que recolecta durante la emisión de cada certificado digital.
- BCCR: Banco Central de Costa Rica.
- CA: Autoridad Certificadora. Son todas las entidades autorizadas a emitir certificados de llave pública dentro de la jerarquía nacional de certificadores.
- Dispositivo criptográfico: Tarjeta inteligente con microprocesador (chip de circuito integrado) criptográfico, con la capacidad para generar a lo interno un par de llaves y de almacenar los certificados digitales que emite la CA del SINPE.
- OR: Oficina de Registro. Es una entidad que ejecuta labores de identificación y autenticación de los solicitantes que aplican por un certificado. Además, valida la información contenida en las solicitudes de certificado y tramita las solicitudes de revocación para los certificados.
- SINPE: Sistema Nacional de Pagos Electrónicos.
- Solicitante: Persona física que, facultada por las políticas establecidas por el certificador del SINPE, presenta al registrador una solicitud de emisión de un certificado

Para consultar algún otro término que aparezca en este documento, remítase a la “Norma complementaria – Glosario general”.

4. Documentos aplicables y anexos

Siglas	Nombre del documento
RSP	Reglamento del Sistema de Pagos
NC-GGE	Norma complementaria – Glosario general
NC-FID	Norma complementaria – Firma Digital
NC-RPS	Norma complementaria – Requisitos para participar en el SINPE
NC-AES	Norma complementaria – Administración de Esquemas de Seguridad
ISO/IEC 1974-5:2005 (E)	Information technology Biometric data interchange format Part 5 Image data
	Política de Certificados para la Jerarquía Nacional de Certificadores registrados
	Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica (Oficinas de Registro para efectos de esta normativa)
INTE-ISO-21188:2007	Infraestructura de llave pública para servicios financieros — Estructura de prácticas y políticas
	Anexo No. 1: Lector de Huellas Dactilares
	Digital Anexó
	Anexo No. 3: Especificaciones Fotográficas
	Anexo No. 4: Cámara para circuito cerrado de T.V.
	Anexo No. 5: Lector de Tarjetas Inteligentes
	Anexo No. 6: Dispositivos criptográficos (Tarjetas inteligentes) – PKI
	Anexo No. 7: Diseño de la tarjeta inteligente - PKI
	Anexo No. 8: Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV
	Anexo No. 9: Diseño de la tarjeta inteligente – PKI sobre Tarjetas de Pago certificadas por EMV
	Anexo No. 10: Proceso de homologación de dispositivos criptográficos para el almacenamiento de certificados de firma digital

5. Controles físicos

Las OR deben mantener controles físicos para asegurar la ejecución de las funciones de recepción, validación, verificación y de la gestión de las solicitudes de emisión o revocación de los certificados digitales en cumplimiento de lo establecido en los documentos de: “Política de Certificados para la Jerarquía Nacional de Certificadores Registrados” y “Directrices para las Autoridades de Registro, características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica”, (OR para efectos de esta normativa).

5.1. Proceso de verificación y aceptación de lectores de huellas dactilares, cámara fotográfica y lectores de tarjetas inteligentes

Para el funcionamiento adecuado del servicio de Firma Digital en las OR, este tipo de dispositivos deben haber pasado un proceso de verificación por parte de la CA del SINPE.

Si la OR desea utilizar un dispositivo que la CA del SINPE no ha verificado deberá someterlo al proceso de verificación por medio del Centro de Operaciones del SINPE, su incorporación estará sujeta a:

- La verificación de cumplimiento de las especificaciones técnicas por parte del BCCR.
- Que se aporte la documentación pertinente que demuestre que el dispositivo cuenta con soporte y garantía del fabricante.
- Que se aporte al BCCR la documentación y el software correspondiente y la facilidad de establecer comunicación directa con el personal técnico experto del dispositivo.
- La verificación que pueda realizar el BCCR, de que la marca y modelo correspondiente al dispositivo funciona adecuadamente con el servicio de Firma Digital.
- La disponibilidad de recursos del BCCR y a la factibilidad para el desarrollo de los componentes que se podrían requerir para su uso automático en el sistema.
- Cualquier otro detalle que la CA del SINPE considere relevante hacer saber a la OR respecto a su solicitud de verificación de dispositivos.

La OR se dará de alta hasta que la marca y modelo de los dispositivos que desee utilizar hayan sido verificados y aceptados por la CA del SINPE.

5.2. Proceso de homologación de dispositivos criptográficos (tarjetas inteligentes)

Las OR deberán operar el Servicio de Firma Digita únicamente con dispositivos criptográficos homologados por la CA del SINPE.

La CA del SINPE mantiene abierto, en forma permanente, un proceso de homologación. Los interesados en homologar dispositivos criptográficos pueden solicitarlo por escrito ante la División de Sistemas de Pago del BCCR aportando los dispositivos, la documentación y demás requisitos que la CA SINPE solicite. El anexo 11 incluye todos los requisitos de participación y demás detalles del proceso de homologación.

Los requisitos de los dispositivos criptográficos se detallan en los Anexos 6 y 9. Las características descritas en los anexos mencionados son los que se verifican en el proceso de homologación.

Conforme al último proceso de homologación realizado por la CA del SINPE los dispositivos homologados son los que se detallan en el apartado de Firma Digital de la página web del Banco Central de Costa Rica (http://www.bccr.fi.cr/). Adicionalmente se muestra una lista no exhaustiva de lectores de tarjetas inteligentes que funcionan correctamente con las tarjetas de firma digital de la CA SINPE – Persona Física.

5.3. Instalaciones físicas de las OR

Existen dos procesos básicos que deben ejecutarse en una autoridad de registro. El primero de estos procesos se realiza en el **Recinto de emisión de Certificados Digitales**, en el cual el Agente de Registro (AR) realiza la gestión y trámite de la solicitud del certificado. El segundo se realiza en el

Quiosco de activación de certificados digitales en el cual el suscriptor activa el dispositivo criptográfico (Tarjeta Inteligente) que contendrá el certificado digital.

Tanto el recinto de emisión de Certificados Digitales como el Quiosco de activación de certificados digitales deben cumplir con las facilidades de accesibilidad contempladas en la Ley 7600 "Igualdad de Oportunidades para las personas con Discapacidad". Además, las instalaciones físicas de las OR deben cumplir con los siguientes requisitos:

5.3.1. Mobiliario y equipo - Recinto de emisión de certificados digitales

Los recintos destinados para gestionar la emisión de certificados digitales deben contar como mínimo con el siguiente mobiliario y equipo:

- Una computadora que cumplan con los requisitos tecnológicos establecidos en los puntos "6.4 Estaciones de trabajo" y "6.5.3.4 PCs" de la Norma Complementaria – Requisitos para participar en el SINPE.
- Un lector de huellas dactilares: Requerido para recopilar las huellas dactilares del solicitante. (especificaciones en el Anexo 1).
- Una cámara fotográfica digital: La cámara servirá para tomar las fotos al suscriptor. (especificaciones en el Anexo 2).
- Un fondo para la toma de fotografías: (especificaciones en el Anexo 3).
- Una cámara de circuito cerrado de televisión: Necesaria para dejar evidencia del proceso de emisión de certificados digitales. (especificaciones en el Anexo 4).
- Dos lectores de tarjetas inteligentes (Smart card reader): Se requieren dos lectores independientes para diferenciar las operaciones ejecutadas por el AR, de las que corresponden al solicitante dentro del proceso de emisión de certificado digital. (especificaciones en el Anexo 5).
- Un teléfono con salida externa para solicitar y prestar soporte técnico al servicio de Firma Digital cuando se requiera.
- Un mecanismo de anti - coacción: el cual será accionado por el Agente de Registro en caso de que intenten coaccionarlo para la emisión de un certificado digital. Un ejemplo de este mecanismo, sin estar limitado únicamente a éste es un botón o interruptor para activación de una alarma.

  Este mecanismo deberá alertar al personal de seguridad del edificio y activar un plan de atención para el incidente.
- Una silla para el operador del servicio.
- Una silla para el solicitante del certificado: Que el respaldo no obstaculice el fondo para toma de la fotografía.

5.3.2. Mobiliario y equipo - Quiosco de activación de certificados digitales

- Recinto: El recinto debe garantizar la privacidad del solicitante durante el proceso de activación del certificado digital de forma tal que nadie, por ningún medio, observe al suscriptor definiendo su PIN de activación del certificado.
- Una computadora que cumpla con los requisitos tecnológicos establecidos en los puntos "6.4 Estaciones de trabajo" y "6.5.3.4 PCs" de la Norma Complementaria – Requisitos para participar en el SINPE. No obstante, en este caso el teclado no debe ser ergonómico debido a que esta forma de teclado dificulta su uso por parte de personas no videntes.

Esta computadora debe evitar la instalación de programas y debe estar custodiada dentro del perímetro de seguridad de la OR. El CPU debe estar protegido de tal forma que el solicitante solo tenga acceso al monitor, el teclado, el mouse, el lector de huellas y el lector de tarjetas para la activación de los certificados.

- Un lector de tarjetas inteligentes (Smart card reader) en la computadora donde se activará el certificado por parte del Suscriptor. (especificaciones técnicas contenidas en el Anexo No 5).
- Un lector de huellas dactilares: Que le permita al suscriptor activar la tarjeta inteligente utilizando su huella digital (especificaciones en el Anexo 1).
- Una cámara de circuito cerrado de televisión: Es requerida para validar el proceso, de acuerdo a los parámetros de grabación definidos en el anexo 4. En este caso la cámara debe ubicarse de tal forma que sea imposible obtener información relacionada con la activación del certificado digital. Esta cámara puede ser compartida con el Recinto de Trámite de certificados digitales siempre y cuando la cámara pueda filmar simultáneamente la actividad de ambos recintos de modo que quede evidencia de toda la actividad desarrollada durante el trámite y la activación de los certificados.
- Contar con parlantes u otro medio de sonido que permita a los suscriptores no videntes escuchar en forma eficiente las instrucciones para la activación de su certificado.

5.3.3. Características y dimensiones físicas

Las instalaciones físicas de la entidad donde se encuentran ubicados los recintos de atención a clientes, deben contar con un perímetro de seguridad con personal de vigilancia asignado durante el horario de operación de los mismos.

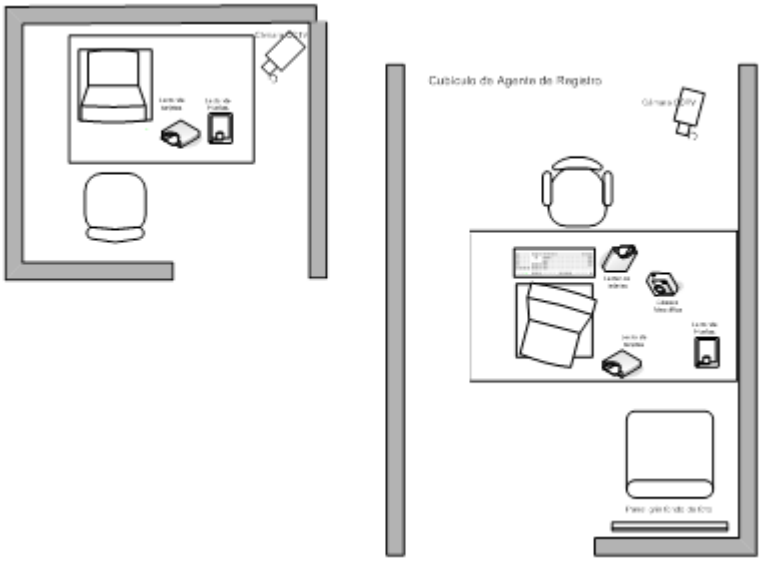
Las instalaciones del Quiosco deben tener las previsiones para los casos excepcionales (personas con discapacidad, sin huellas digitales, etc.).

Los recintos utilizados para la emisión y activación de los certificados digitales pueden ajustarse a uno de los siguientes modelos:

5.3.3.1. Recinto de emisión y Quiosco de activación separados

En esta modalidad el recinto de emisión está separado del Quiosco de activación de los dispositivos para garantizar la privacidad en el proceso de activación y tiene la ventaja de que varios cubículos de Agentes de Registro pueden compartir un mismo Quiosco de activación.

En lo que corresponde a las cámaras de video, debe considerarse que bajo este modelo, se requieren cámaras independientes: las de los recintos de emisión, para monitorear el ambiente de emisión de certificados de cada agente de registro así como para evidenciar que los procesos son ejecutados correctamente y la del quiosco, para evidenciar que la persona realizó su proceso de activación de forma personal y sin ningún tipo de ayuda. Se debe tomar en cuenta que las labores de vigilancia y monitoreo de las cámaras del quiosco no deben atentar contra la privacidad, dada la naturaleza de las labores realizadas.



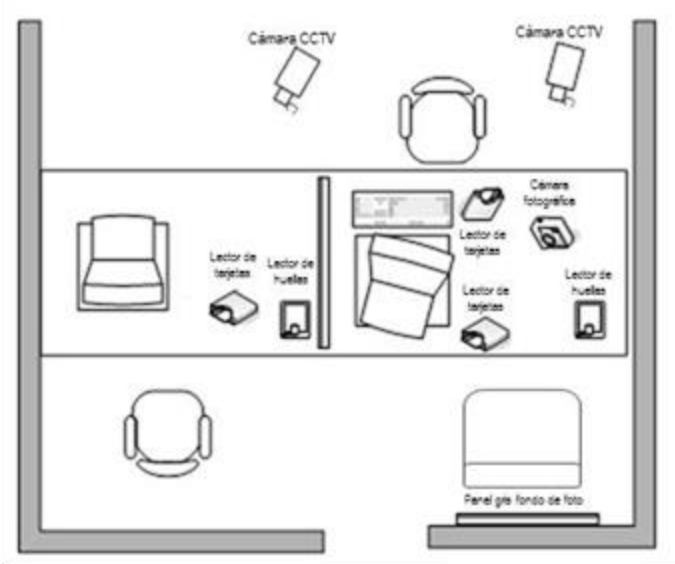
El Recinto de Trámite (Cubículo de Agente de Registro) no necesariamente tiene que estar cerrado por paredes, este puede ser diseñado como un espacio más abierto similar al que se usa en las plataformas de servicio al cliente e incluso puede estar ubicado en cubículos de estas plataformas. De igual forma el diseño del Quiosco de Activación puede ser diferente siempre y cuando se garantice que por ningún medio o dispositivo ninguna persona distinta al suscriptor pueda obtener los datos de activación del dispositivo.

5.3.3.2. Recinto de emisión y Quiosco de activación en un mismo cubículo

Este modelo consiste en separar dentro de un área común el recinto de emisión y el correspondiente al Quiosco. Una división entre las dos áreas debe garantizar la privacidad del proceso de activación del certificado. En este escenario el agente de registro tiene mayor control del proceso de activación por parte del solicitante, sin que tenga que involucrarse en el mismo.

Debido a que en este modelo el Recinto de emisión y el Quiosco de activación de certificados se encuentran en un área común, puede utilizarse una sola cámara de circuito cerrado de televisión, siempre y cuando, se garantice que la evidencia que se recoge por medio del video del proceso de emisión y del proceso de activación del certificado cumpla con las especificaciones contenidas en este estándar.

Como medida de seguridad, un nuevo solicitante no podrá ser atendido mientras el proceso de emisión y el de activación del solicitante anterior no haya terminado (esto obliga a esperar hasta que la activación sea finalizada).



El Recinto de emisión (Cubículo de Agente de Registro) no necesariamente tiene que estar cerrado por paredes, este puede ser diseñado como un espacio más abierto similar al que usualmente se usa en las plataformas de servicio al cliente e incluso puede estar ubicado en cubículos de estas plataformas. De igual forma el diseño del Quiosco de Activación puede ser diferente siempre y cuando se garantice que por ningún medio o dispositivo ninguna persona distinta al suscriptor pueda obtener los datos de activación del dispositivo.

Una misma OR puede utilizar uno o ambos esquemas de operación de acuerdo con las posibilidades que le brinde la infraestructura de las instalaciones físicas en donde se vaya a prestar el servicio de emisión de certificados digitales. Cualquiera que sea el caso, ambos recintos deben ajustarse a los requerimientos establecidos para cumplir con la "Política de Certificados para la Jerarquía Nacional de Certificadores Registrados" y las “Directrices para las Autoridades de Registro, características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica” (OR para efectos de esta normativa) y las disposiciones y requisitos establecidos en las Normas del servicio de Firma Digital.

5.4. Requisitos de Seguridad

Las instalaciones físicas de las OR además de cumplir con las normas establecidas en el Libro Administración de Esquemas de Seguridad de la Serie de Normas y Procedimientos del SINPE, deben cumplir con los siguientes requisitos mínimos de seguridad específicos para este servicio:

- Perímetro de seguridad: las instalaciones del recinto de emisión y del quiosco de activación de certificados digitales deben estar ubicados dentro de un edificio que posea un perímetro de seguridad con personal de vigilancia asignado, al menos durante el período de operación.

- Controles de acceso: Los equipos deben contar con controles de acceso lógico a las aplicaciones del Servicio de Firma Digital. Únicamente el personal autorizado para gestionar los certificados digitales (“Agente de Registro”) debe tener acceso a este servicio. Además, solamente personal autorizado debe contar con acceso al recinto de trámite de certificados.
- Prevención de incendios: contar con dispositivos de detección de humo o incendio con su respectiva alarma.
- Gabinetes o armarios: con llave, de uso exclusivo de la OR, para guardar documentación propia de la OR. Las llaves deben ser sólo manejadas por el personal autorizado.
- Protección contra fallas en el fluido eléctrico: los equipos deben estar protegidos contra fallas en el fluido eléctrico y otras anomalías en la energía.
- Vigilancia y monitoreo: el ambiente de la OR debe mantener monitoreo por Circuito Cerrado de Televisión (CCTV), o cualquier otra tecnología de video-vigilancia de las actividades de la OR:

  Las imágenes deben ser mantenidas en un ambiente seguro por al menos 3 meses.
- Iluminación de emergencia: que permita mantener la iluminación en las instalaciones de la OR en caso de emergencia.
- Custodia de los dispositivos criptográficos (Smart cards) y control del inventario de las mismas.

  Los dispositivos criptográficos (Smart cards) se deben mantener bajo custodia con control de inventario permanente.

  Los dispositivos criptográficos deben resguardarse en una bóveda o caja fuerte de seguridad y el responsable de su resguardo y control de inventario debe ser un custodio quien debe ser una persona distinta al Agente de Registro.

  Deben existir registros que evidencien la recepción y devolución de los dispositivos por parte de los agentes de registro.

  Los procedimientos para la custodia y el control del inventario de los dispositivos criptográficos deberán ser entregados a la CA del SINPE durante el proceso de verificación del cumplimiento de requisitos que ésta realice para autorizar la operación de la OR.

6. Anexos

6.1. Especificaciones técnicas

6.1.1. Anexo No. 1: Lector de Huellas Dactilares

El lector debe capturar las imágenes de la huella dactilar a pesar de manchas en los dedos de tinta, tintura, grasa o suciedad, dedos secos y húmedos. Los requerimientos particulares para el lector de huellas deben cumplir con los siguientes requisitos:

- Lector de tecnología óptica de una sola huella con capacidad de soporte para 8 bits en escala de grises, resolución mínima de 500 dpi.
- Tamaño mínimo de la imagen 416x416 pixeles.
- Conexión por USB versión 2.0 o mayor.
- Alimentación eléctrica a través del puerto USB.
- Capacidad de trabajar a temperaturas entre los 0 y los 40 grados centígrados.

- Área de captura en vidrio, con capacidad de trabajar en humedades del 10% al 90% sin que se presente empañamiento del vidrio del lector.
- Capacidad de trabajar sobre el sistema operativo Windows 7 o superior.
- Componentes certificados por el FBI y verificables a través de la “IAFIS Certified Product List”1.
- Resistencia a descargas electroestáticas, suciedad, polvo y solventes.
- Cumplir con el ANSI INCITS 358-2002, que especifica la interfaz de BioAPI versión 1.1.
- Área de adquisición de al menos 19 mm por 19 mm.
- Verificación de una huella en menos de 1 segundo.
- Identificación biométrica en menos de 2 segundos.
- MTBF de al menos 10.000 horas.
- Capacidad de generar una compresión WSQ y generar una minucia estándar en formato MINEX2.
- Generación de la imagen de la huella en formato WSQ certificado por el FBI.
- Permita hacer match 1 a 1.
- Que cumplan con el estándar "ISO/IEC 19794-2 y "ANSI INCITS 378" para la generación de la minucia tanto en formato record-based como en formato compact for smart card.
- Certificado por MINEX.
- Cumplimiento del ISO 19794-4.

Las funcionalidades de captura y verificación de huellas dactilares que existen actualmente en el servicio de Firma Digital se desarrollaron con el SDK SAGEM Morphokit versión 5.2. Los lectores de huellas deben ser compatibles con este SDK para que funcionen con la plataforma de Firma Digital, previa verificación por parte de la CA del SINPE.

6.1.2. Anexo No. 2: Cámara Fotográfica Digital

La cámara debe cumplir los siguientes requerimientos:

- Debe poseer un ZOOM Óptico de al menos 4x. Debe contar con un sistema de auto-enfoque.
- Debe contar con un método de control de exposición y medición de la luz.
- Debe tener el flash incorporado y permitir toma de fotos con “reducción de ojos rojos”.
- Debe ser capaz de almacenar la foto tomada en un archivo con formato Exif v.2.2 (JPEG).
- Debe permitir tomar fotos con una resolución mínima de 640x480 pixeles o directamente proporcional, que respete la relación 4:3 (Por ejemplo: 1600x1200, 2048x1536, etc.).
- Debe contar con tecnología de detección de rostros.
- Preferiblemente debe incluir el adaptador de corriente.
- Debe incluirse el trípode o brazo que sujete la cámara en una posición fija.

---

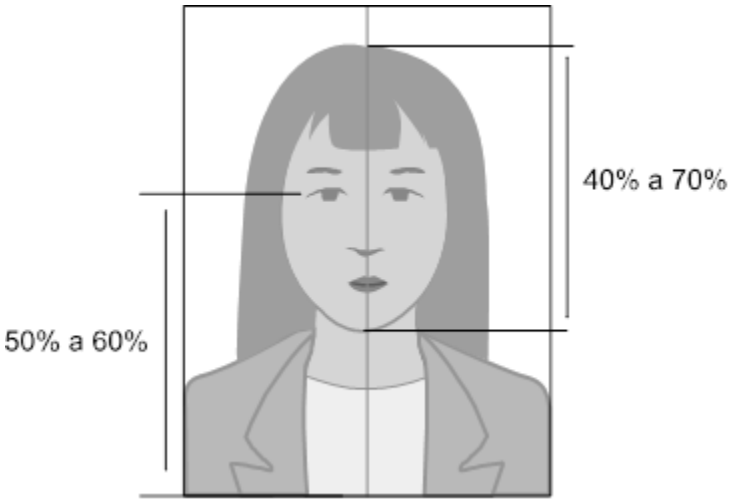
[1] *http://www.fbibiospecs.org/fbibiometric/iafis.html.*

En el mediano plazo el servicio de Firma Digital incluirá la funcionalidad para que la cámara fotográfica pueda ser manipulada desde la misma aplicación. El desarrollo de esta funcionalidad y cualquier otra con respecto a la fotografía se realizará utilizando el SDK de Canon EDSDK. Para sacar provecho de dicha funcionalidad, las cámaras fotográficas que la OR utilice pueden ser opcionalmente CANON, compatibles con dicho SDK.

6.1.3. Anexo No. 3: Especificaciones Fotográficas

La fotografía del solicitante debe tomarse de acuerdo a las siguientes especificaciones:

- La cara de la persona debe abarcar entre un 40% y un 70% de la altura de la fotografía. La cara debe encontrarse centrada en la fotografía de acuerdo a las proporciones indicadas en la siguiente imagen de referencia. Se recomienda colocar la cámara aproximadamente (120 cm) del sujeto y mantenerla al nivel del ojo del sujeto.



- El contraste y la luz en la foto deben ser normales.
- Evite sombras sobre la cara o en el fondo.
- Incluir una cara completa, de frente y con los ojos abiertos. El cabello no puede cubrir los ojos.
- No se permiten fotos con los “ojos rojos”.
- La cara en la foto debe tener una expresión normal (boca cerrada).
- Asegúrese que la foto presente una cabeza completa desde la parte superior de la cabeza (cabello) hasta los hombros.
- Los hombros deben estar de frente en forma horizontal. No se permiten fotos donde el solicitante tenga una posición distinta.
- Las fotos no deben incluir gafas oscuras o sombreros. Solo se permitirá el uso de gafas en el caso en que en el documento de identidad del solicitante aparezca portando gafas pero en ningún caso podrán ser oscuras ni ocasionar reflejos que distorsionen, dificulten o entorpezcan la nitidez de la fotografía de modo que se dificulte la identificación del solicitante.
- No se permiten manos, brazos, u otra parte del cuerpo de alguna persona que esté ayudando al solicitante a tomarse la foto. Tampoco se permite que aparezca otro tipo de objetos en la foto.
- La resolución de la foto debe ser de 640 x 480 pixeles en formato JPG o proporcional.

- El fondo debe ser color gris, liso, sin sombras y no tener patrones, con el fin de minimizar reflejos no deseados. La iluminación del fondo debe ser uniforme para remover cualquier sombra o efectos de luz que puedan interferir con el reconocimiento del contorno facial. (Ref. ISO/IEC 19794-5:2005 (E) “Information technology Biometric data interchange format Part 5 Image data).

6.1.4. Anexo No. 4: Cámara para circuito cerrado de T.V.

a) Especificaciones de las cámaras del CCTV para Autoridades de Registro:

i) La tecnología de la plataforma de CCTV, preferiblemente, debe ser digital; sin embargo, puede utilizarse también tecnología analógica cuando sea una restricción de la plataforma de CCTV que la OR posee.

ii) Resolución mínima de 320 x 240.

iii) Dos cuadros por segundo (2 FPS) o superior.

iv) El tiempo de almacenamiento debe ser al menos de 3 meses.

v) La cámara debe estar ubicada a una distancia no mayor de 3 metros de los objetivos de grabación.

b) Condiciones ambientales:

Garantizar la luminosidad artificial del área y validar que las condiciones externas no la afecten (por ejemplo si es de mañana o tarde, o bien, por las condiciones ambientales según la época del año). Evitar decoraciones del cubículo que afecten la visibilidad de la cámara, lo cual significa que no debe haber obstáculos entre la cámara y los objetivos a grabación.

c) Objetivo de grabación.

Las siguientes áreas o procesos deben ser grabadas para evidenciar el proceso de emisión y entrega de certificados digitales:

i) Proceso de entrega y verificación del documento de identidad.

ii) Proceso de recopilación de evidencia presencial (foto, huellas dactilares, escaneo de cédula).

iii) Entrega del dispositivo con el certificado.

iv) Proceso de activación del certificado guardando la confidencialidad de la activación.

6.1.5. Anexo No. 5: Lector de Tarjetas Inteligentes

Los lectores de tarjetas inteligentes tienen la particularidad que la OR además de usarlos en el servicio de Firma Digital, también puede adquirirlos para entregarlos a sus clientes en conjunto con la tarjeta inteligente.

Los lectores que la OR utilizará en los Recintos de Trámite de Certificados Digitales y en los Quioscos de Activación de Certificados Digitales deben:

- Soportar tarjetas que cumplan con el estándar ISO/IEC 7816, partes de la 1 a la 3, con soporte como mínimo a los protocolos de transmisión T=0 y T=1 y con soporte de tarjetas inteligentes clase A y clase B del ISO 7816.
- Poseer conexión al computador por puerto USB 2.0 o superior.
- Poseer alimentación de energía eléctrica a través del puerto USB.

- Cumplir con la especificación PC/SC.
- De preferencia, el lector debe ser de contacto de aterrizaje (landing contact).
- De preferencia el lector debe tener la capacidad de "flash upgradable" para facilitar la actualización del firmware del mismo.

Adicional a dichos requerimientos, para cumplir con el principio de igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas (artículo 2 de la Ley 8454), los lectores de tarjetas inteligentes que la OR entregue a sus clientes deben cumplir con las siguientes especificaciones:

- Poseer drivers para ser utilizados apropiadamente en plataformas Windows. Mac OS y Linux, en las versiones oficialmente soportadas por cada fabricante. Deben proveerse los drivers para que los lectores sean reconocidos por dichos sistemas operativos.
- Los lectores deben estar en la lista de productos certificados por Microsoft, para los sistemas operativos Windows oficialmente soportados por Microsoft como fabricante. Esta lista es verificable en la página "Windows Logo'd Product List" https://sysdev.microsoft.com/en-us/hardware/lpl, o en la página de Windows Compatibility Center http://www.microsoft.com/en-us/windows/compatibility/CompatCenter/Home,

Los requisitos antes mencionados no descartan que los lectores de tarjetas puedan estar incorporados en cualquier componente de la computadora (CPU, monitor, teclado, etc.).

6.1.6. Anexo No. 6: Dispositivos criptográficos (Tarjetas inteligentes) – PKI

El fin último de los dispositivos criptográficos es el de entregarlos al cliente de la OR como repositorio de los certificados digitales de autenticación y firma digital y de las llaves públicas y privadas correspondientes.

La siguiente lista de requerimientos incluye características que garantizan el funcionamiento de los dispositivos criptográficos en los Recintos de Trámite de Certificados Digitales y en los Quioscos de Activación de Certificados Digitales. Adicionalmente se incluyen características necesarias para que los clientes puedan utilizarlos en diversas plataformas tecnológicas y para que la CA del SINPE cumpla con el principio de igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas (artículo 2 de la Ley 8454).

Adicionalmente, y con el fin de garantizar el adecuado funcionamiento de estos dispositivos, es requisito indispensable que al realizar una compra, la entidad operadora de la OR solicite a sus proveedores que la versión o modelo de los dispositivos que le estén ofertando haya sido homologado previamente por la CA SINPE – Persona Física.

Una vez que un proveedor haya homologado sus dispositivos, se deberá realizar un nuevo proceso de homologación en caso de que se realice algún cambio en las características de los mismos, debiendo demostrar ante la entidad interesada en la adquisición de los mismos que los dispositivos ofertados están debidamente homologados.

1. Requisitos Generales

a) Las características físicas de las tarjetas inteligentes, incluyendo materiales, fabricación y dimensiones, deben cumplir con el estándar ISO/IEC 7810, específicamente para la tarjeta de tamaño ID-1 (nominalmente 85.60 mm de ancho por 53.98 mm de alto por 0.76 mm de grosor, el estándar específica un rango de dimensiones mínimas y máximas).

b) Las pruebas realizadas a las tarjetas para demostrar que cumplen con los parámetros especificados en el estándar ISO/IEC 7810 deben haberse realizado en cumplimiento con los procedimientos de pruebas estipulados en el estándar ISO/IEC 10373-1.

c) Las tarjetas inteligentes deben ser dispositivos con microprocesador criptográfico con un único chip de circuito integrado con contactos y deben cumplir con las características descritas en el estándar ISO/IEC 7816-1. Además, deben cumplir con en la enmienda 1 de este mismo estándar (ISO/IEC 7816-1/Amd.1:2003) en lo que respecta al alto máximo de la superficie del chip.

d) El chip de los dispositivos criptográficos debe poseer ocho contactos según lo indica el estándar ISO/IEC 7816-2, cuya dimensión y ubicación en la tarjeta debe cumplir con lo especificado en dicho estándar.

e) Las pruebas realizadas para demostrar que el chip de los dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 1 y 2 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3 para los chips criptográficos de contactos y los dispositivos de interface relacionados.

2. Requisitos de Seguridad del Chip (hardware, firmware y software)

a) El chip del dispositivo criptográfico debe tener la capacidad de generar pares de llaves criptográficas (pública y privada) a lo interno del chip de al menos 2048 bits.

b) Después de que la tarjeta ha sido inicializada y personalizada, la capacidad de la memoria EEPROM debe permitir el funcionamiento correcto de la aplicación PKI y el almacenamiento simultáneo de al menos cuatro certificados X.509 V3 y sus correspondientes llaves de 2048 bits.

c) De preferencia, la aplicación a lo interno de la tarjeta, que provee la funcionalidad de firma digital (en adelante llamada aplicación PKI), deberá residir en la memoria ROM.

d) A ningún nivel (hardware, firmware, software, middleware) el dispositivo criptográfico debe permitir que la llave privada generada a lo interno del chip abandone o sea extraída del mismo.

e) El dispositivo criptográfico debe soportar como mínimo los algoritmos criptográficos: SHA-1, SHA-256, 3DES, RSA con llaves de 2048 bits.

f) El chip del dispositivo criptográfico debe poseer certificación a nivel 3 o superior del estándar FIPS 140-2 o la certificación Common Criteria EAL 4+ en el perfil de protección SSCD Tipo 3 (Secure Signature-Creation Device). Las tarjetas que sólo posean la certificación FIPS 140-2 nivel 3 o superior, deben operar en modo FIPS de forma natural. La CA del SINPE se reserva el derecho de aceptar las tarjetas cuya certificación del NIST indique la leyenda “cuando es operado en modo FIPS” (When operated in FIPS mode), hasta poder analizar la Política de Seguridad correspondiente y concluir que la operación en modo FIPS, una vez habilitada, es irreversible. La documentación oficial que demuestre las certificaciones debe corresponder en marca y modelo a las tarjetas inteligentes que usará la OR.

Cualquiera de las dos certificaciones debe incluir el circuito integrado de contactos, el sistema operativo y la aplicación PKI en la tarjeta. La CA SINPE se reserva el derecho de aceptar tarjetas que están siendo sometidas a un proceso de certificación completo de los tres elementos, siempre y cuando aporten los resultados de una valoración de un tercero así como certificaciones FIPS o Common Criteria independientes para el chip y el sistema operativo.

g) La aplicación PKI debe implementar controles para evitar ataques de fuerza bruta contra el PIN y para asegurar que la comunicación entre el chip y el middleware sea encriptada.

h) La aplicación PKI a lo interno de la tarjeta debe cumplir con las especificaciones del estándar ISO 7816 parte 4 “Organization, security and commands for interchange” en lo que se refiere a la arquitectura de seguridad, la organización de datos y aplicaciones para el intercambio de información entre el dispositivo y el exterior (APDU).

i) Las funciones criptográficas implementadas en la tarjeta deben cumplir con las especificaciones del estándar ISO 7816 parte 8 “Comandos para las operaciones de seguridad”.

j) Como mínimo, la tarjeta debe implementar los comandos de administración del ciclo de vida estipulados en el estándar ISO 7816 parte 9 “Comandos para la administración de la tarjeta”.

k) Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 4, 8 y 9 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.

l) La tarjeta debe implementar un modelo de “Ciclo de Vida” para controlar diferentes estados de la funcionalidad y seguridad de la tarjeta. La tarjeta debe ser entregada a la Entidad Emisora en un estado que garantice que está lista para el proceso de generación de llaves y para el almacenamiento de los certificados digitales. Adicionalmente, una vez que la tarjeta contenga las llaves necesarias y los elementos de seguridad, debe cambiar a un estado que garantice su seguridad y su funcionalidad total.

m) El fabricante deberá configurar el sistema operativo del dispositivo criptográfico, de forma que sólo la CA del SINPE tenga acceso a los comandos administrativos del chip, estableciendo para ello el conjunto de llaves de administración de los dispositivos (también conocidas como ISD keys) conforme a lo especificado en el estándar Global Platform y de forma confidencial y exclusiva para la CA del SINPE. La distribución de estas llaves deberá hacerse siguiendo los controles apropiados para salvaguardar su confidencialidad y garantizar que sólo son conocidas por la CA del SINPE y el fabricante. La entrega de los valores de las llaves (cuando aplique) deberá realizarse bajo controles que garanticen su confidencialidad.

n) El dispositivo criptográfico debe ser configurado por el fabricante para que al momento de su entrega el “Estado del ciclo de vida de los dispositivos” tenga el valor “SECURED” de acuerdo al estándar Global Platform.

o) Las acciones administrativas sobre la tarjeta solamente deben ser ejecutadas cuando se utiliza la llave de administración (Admin Key) como mecanismo de autenticación. Lo anterior debe incluir la funcionalidad de inicialización del dispositivo, creación y borrado de llaves y certificados, así como el desbloqueo del PIN de usuario. Dichas capacidades administrativas no deben ser accesibles para los usuarios finales.

p) La tarjeta debe proveer un PIN de usuario, para controlar el acceso a la funcionalidad que provee la aplicación PKI. El PIN debe tener un tamaño mínimo de 4 y máximo de 14 dígitos. Después de 7 intentos fallidos del PIN, la aplicación PKI se debe bloquear. Adicionalmente, la aplicación PKI debe implementar, a lo interno del chip, reglas de complejidad del PIN que limiten el uso de dígitos repetidos (máximo 2) y el uso de dígitos consecutivos (máximo 2), de forma que, independientemente de la aplicación o sistema operativo que se utilice para cambiar el PIN, la tarjeta siempre verifique dichas reglas.

3. Requisitos de Compatibilidad con la CA del SINPE

a) La tarjeta inteligente debe tener, a lo interno del chip, la aplicación PKI LASER de NXP Semiconductors[2] y utilizar esta como aplicación PKI.

b) La tarjeta inteligente debe ser compatible con la herramienta Forefront Identity Manager (FIM) de Microsoft versión FIM 2010 R2, para plataforma de 64 bits, que es el sistema administrador de dispositivos (CMS por sus siglas en inglés) utilizado por la CA del SINPE. Esta compatibilidad debe estar dada a través de un minidriver oficialmente certificado por Microsoft. Si las tarjetas requieren de algún proceso de inicialización específico para poder ser utilizados en FIM, ese proceso deberá ser realizado por el fabricante previo a su entrega a la Entidad Emisora. Cuando el fabricante entregue las tarjetas a la entidad, las mismas deben estar totalmente listas para ser utilizadas en FIM.

c) La tarjeta debe implementar una funcionalidad que garantice que viene de fábrica pre-personalizada con una llave de administración (admin key) única y específica para el uso de la CA del SINPE. Esta llave debe permitir su diversificación posterior y debe ser bloqueada después de 10 intentos fallidos; dicha configuración se consignará en el perfil de FIM. El valor de esta llave será establecido por la CA del SINPE quien lo facilitará al fabricante. La entrega deberá hacerse siguiendo los controles apropiados para salvaguardar su confidencialidad.

d) Las tarjetas deben estar configuradas para que el número UID (Unique Permanent Identification) que tienen en su chip (establecido en el momento de su fabricación) sea asignado a la variable CP_CARD_GUID, agregando los ceros a la izquierda necesarios, de forma que se garantice que este número corresponda al desplegado por FIM como número de serie del dispositivo. Por ejemplo si el número de serie del chip es 0653000341246254, la variable CP_CARD_GUID debe ser actualizada con el valor 00000000000000000653000341246254, de forma que en FIM se despliegue el valor {00000000-0000-0000-0653-000341246254}. Este valor deberá garantizar la unicidad del número de serie del chip, por lo que se recomienda que esté formado por fecha de fabricación + número de serie + id del batch. Cada vez que se realice una compra el proveedor debe entregar, en conjunto con los dispositivos criptográficos, un archivo electrónico en formato XML que contenga los números de serie de todos y cada uno de los dispositivos de la compra. El formato del archivo en que se reciba la información deberá realizarse de conformidad con las especificaciones contenidas en el Estándar Electrónico – Firma Digital.

e) La aplicación PKI debe ser capaz de firmar digitalmente solicitudes de certificado construidas con formato PKCS #10 y que se le envían a la CA del SINPE para la emisión de los certificados correspondientes. Lo anterior como señal de posesión de la llave privada por parte del solicitante.

4. Requisitos de Interoperabilidad y Neutralidad Tecnológica

a) El sistema operativo del dispositivo criptográfico debe ser de plataforma abierta Java Card, que permita el funcionamiento de múltiples aplicaciones que se ejecuten a lo interno del chip y que se puedan incluir posteriormente. Las características del Sistema Operativo deben ser tales que permita que haya independencia en quién o quiénes puedan desarrollar dichas aplicaciones.

b) El sistema operativo del dispositivo criptográfico debe cumplir con la especificación de Global Platform 2.1.1 o superior, con el objetivo de permitir cualquier combinación de aplicaciones de diferentes tipos o proveedores en un único dispositivo criptográfico.

---

2 *La aplicación PKI LASER de NXP Semiconductors es la misma que poseen las tarjetas ID Protect Laser Card de Athena (Actualmente NXP Semiconductors) que se encuentran homologadas.*

c) Para lograr la comunicación entre los computadores y la aplicación PKI de la tarjeta, el fabricante debe suministrar el middleware IDProtect, asociado a la aplicación PKI LASER, para acceder la funcionalidad PKI dentro de la tarjeta. El middleware debe proveer las siguientes interfaces:

i) Un CSP con soporte a CryptoAPI.

ii) Un minidriver.

iii) Una librería PKCS#11.

iv) Un driver Tokend para Mac.

d) El CSP debe operar en sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.

e) El minidriver debe estar oficialmente certificado por Microsoft y debe cumplir con el "Windows Smart Card Minidriver Specification" con soporte a Base CSP y KSP para los sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.

f) La librería PKCS#11 debe ser provista para las plataformas Windows, Mac OS y Linux; en las versiones oficialmente soportadas por cada fabricante.

g) El middleware debe permitir que los certificados digitales, las llaves y la funcionalidad de la aplicación PKI puedan ser accedidos en aplicaciones de usuario final que corren, como mínimo, en los navegadores nativos de las plataformas Windows (IE Explorer) y Mac OS (Safari), y en Mozilla Firefox y Google Chrome; en las versiones oficialmente soportadas por cada fabricante.

h) El fabricante debe garantizar que los certificados emitidos a través del minidriver sean utilizables también por medio de los otros drivers solicitados (PKCS#11 y Tokend). Es decir, que las tarjetas con certificados emitidos en un sistema operativo Microsoft a través del minidriver puedan ser utilizadas en otros sistemas operativos distintos a Microsoft.

i) El uso de cada contacto y las interfaces eléctricas en los dispositivos criptográficos debe cumplir las especificaciones de los estándares ISO/IEC 7816-3, ISO/IEC 7816-10 e ISO/IEC 7816-12, según los tipos de interfaces que el dispositivo provea y a la asignación de cada contacto conforme al Anexo A del estándar ISO/IEC 7816-2.

j) Para permitir la interoperabilidad de los dispositivos criptográficos entre diferentes organizaciones, los elementos de datos del dispositivo deben cumplir con las especificaciones del estándar ISO 7816-6.

k) Los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-7 en el uso de los comandos para el lenguaje SCQL.

l) Las funciones criptográficas implementadas en el chip de los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-15, de forma que se garantice la compatibilidad de las aplicaciones criptográficas con varios emisores de dispositivos.

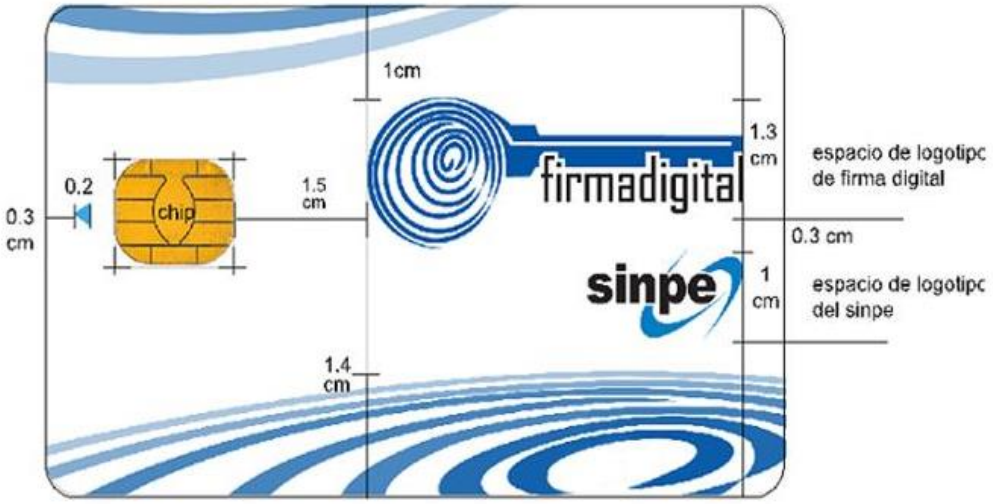
m) Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 3, 10, 12, 6, 7 y 15 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.

n) Las tarjetas deben ser compatibles con lectores de tarjetas estándar, en cumplimiento de las especificaciones PC/SC y del ISO 7816 partes 1 a 3. Además, deben soportar como mínimo los protocolos de transmisión T=0 o T=1.

6.1.7. Anexo No. 7: Diseño de la tarjeta inteligente - PKI

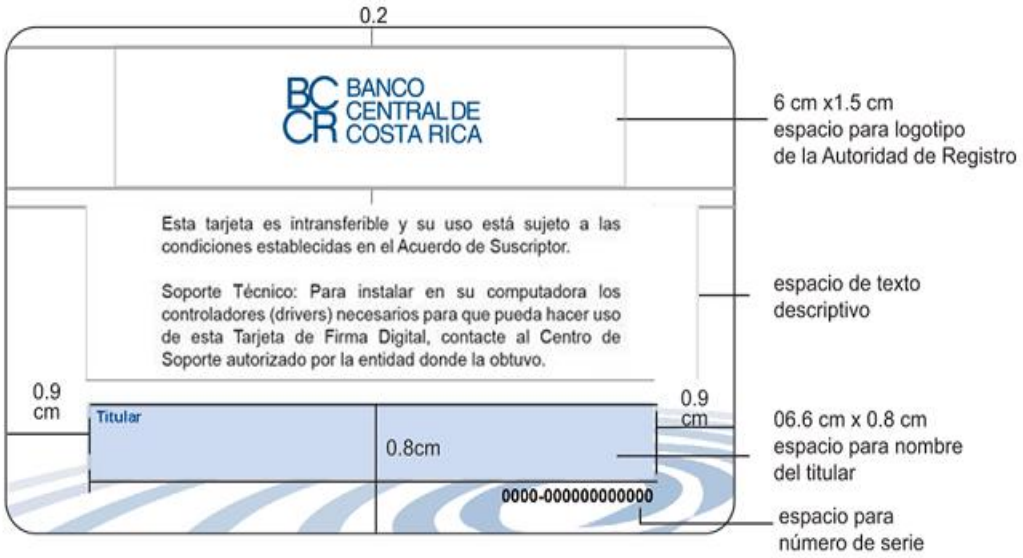
En las imágenes que se muestran a continuación se especifican el arte y los campos de uso obligatorio y las dimensiones que debe contener el diseño de las tarjetas inteligentes de la CA del SINPE:

Anverso



Al dorso, en la parte superior se asigna el espacio para que las autoridades de Registro que así lo deseen, incluyan su logotipo en las dimensiones establecidas en las siguientes imágenes:

Reverso



- El número de serie impreso debe corresponder al número desplegado por FIM como número de serie de la tarjeta, el cual en cumplimiento con los requerimientos del Anexo 6 debe ser equivalente al UID (Unique Permanent Identification) del chip de la tarjeta. El formato de impresión del número de serie debe ser 9999-999999999999.

- La impresión de la tarjeta debe realizarse con una tecnología de impresión tal que el fabricante garantice su calidad por un mínimo de cuatro años, para lo cual las tarjetas deben laminarse tanto en su anverso como en su reverso, tomando en cuenta que debe dejarse libre el espacio del chip. El número de serie deberá ser impreso con tecnología láser.
- El espacio para el nombre del titular deberá quedar libre de la laminación y deberá ser un panel especial para firma manuscrita, al estilo del que se utiliza en las tarjetas de crédito, de forma que la persona a quien se le entregue la tarjeta pueda firmar en este espacio con un bolígrafo de tinta común.
- El archivo en formato digital con el diseño de impresión en digital se podrá entregar en los siguientes formatos: .psd, .eps, .pdf, .tiff, .gif y .jpg, La OR interesada debe solicitarlo por escrito, y será entregado junto con todos los requisitos de diseño.

Adicionalmente, aunque recomendamos que el número y el correo del centro de soporte estén siempre consignados en el reverso de la misma tarjeta para que el cliente lo tenga a mano, en los casos en que las OR no considere conveniente estampar el número del Centro de Soporte en el reverso de la tarjeta por el riesgo de desactualización que esto pudiera representar si llegaren a cambiar de proveedor de soporte, estas OR deberán entregar al cliente una “tarjeta” impresa con la información de dicho centro. Esta tarjeta adicional puede estar confeccionada en cartón resistente o en plástico y su diseño debe ser el siguiente:

Tarjeta Opcional

Para evitar tener que hacer entrega de esta tarjeta adicional, una solución alterna, podría consistir en consignar en el reverso de la tarjeta un número de teléfono centralizado en la entidad que opera la Oficina de Registro que direccione las llamadas a cualquiera que sea el Centro de Soporte que tengan implementado o bien contratado en cualquier momento.

6.1.8. Anexo No. 8: Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV

La siguiente especificación técnica asume que el dispositivo criptográfico (tarjeta inteligente) cumple con lo especificado por EMVC y cuenta con una certificación que lo demuestra.

Estas especificaciones no definen ni sustituyen la funcionalidad EMV, son en cambio un suplemento que permite adicionar funcionalidad de Firma Digital al mismo chip, por lo que cada entidad debe asumir por su cuenta y de forma previa, los procesos de certificación EMV pertinentes.

La funcionalidad de firma digital aquí especificada se administra y opera de forma independiente a EMV, respetando el esquema de seguridad definido por EMV para este fin.

1. Especificaciones Técnicas

El dispositivo debe ser una tarjeta de circuito integrado, con un chip de contacto con microprocesador criptográfico, que contenga una o varias aplicaciones de pago EMV, que cuenten con una certificación verificable del cumplimiento de las Especificaciones de Tarjetas de Circuito Integrado para Sistemas de Pago de EMVCo y una aplicación PKI (funcionalidad de firma digital) que cumpla los siguientes requisitos de seguridad, de compatibilidad con la infraestructura de emisión de la CA SINPE, de interoperabilidad y de neutralidad tecnológica.

2. Requisitos Generales

Los dispositivos criptográficos deben contar con una certificación verificable del cumplimiento de las Especificaciones de Tarjetas de Circuito Integrado para Sistemas de Pago de EMVCo.

3. Requisitos de seguridad del chip (hardware, firmware y software)

a) El chip del dispositivo criptográfico debe tener la capacidad de generar pares de llaves criptográficas (pública y privada) a lo interno del chip de al menos 2048 bits.

b) Después de que la tarjeta ha sido inicializada y personalizada, la capacidad de la memoria EEPROM debe permitir el funcionamiento correcto de la aplicación PKI y el almacenamiento simultáneo de al menos cuatro certificados X.509 V3 y sus correspondientes llaves de 2048 bits.

c) Todas las aplicaciones que contenga la tarjeta deben ser cargadas en el chip desde el momento de fabricación de la tarjeta. La Entidad Emisora de los dispositivos de pago, junto con el fabricante de las tarjetas, deberán acordar los controles para garantizar que no se pueden agregar, modificar o eliminar aplicaciones de la tarjeta y que únicamente el fabricante y la entidad emisora (si ésta lo considera conveniente) tienen acceso a los comandos administrativos del chip. De preferencia la aplicación PKI deberá residir en la memoria ROM.

d) A ningún nivel (hardware, firmware, software, middleware) el dispositivo criptográfico debe permitir que la llave privada generada a lo interno del chip abandone o sea extraída del mismo.

e) El dispositivo criptográfico debe soportar como mínimo los algoritmos criptográficos: SHA-1, SHA-256, 3DES, RSA con llaves de 2048 bits.

f) El chip del dispositivo criptográfico debe poseer certificación a nivel 3 o superior del estándar FIPS 140-2 o la certificación Common Criteria EAL 4+ en el perfil de protección SSCD Tipo 3 (Secure Signature-Creation Device). Las tarjetas que sólo posean la certificación FIPS 140-2 nivel 3 o superior, deben operar en modo FIPS de forma natural. La CA del SINPE se reserva el derecho de aceptar las tarjetas cuya certificación del NIST indique la leyenda

"cuando es operado en modo FIPS" (When operated in FIPS mode), hasta poder analizar la Política de Seguridad correspondiente y concluir que la operación en modo FIPS, una vez habilitada, es irreversible. La documentación oficial que demuestre las certificaciones debe corresponder en marca y modelo a las tarjetas inteligentes que usará la OR.

g) Cualquiera de las dos certificaciones debe incluir el circuito integrado de contactos, el sistema operativo y la aplicación PKI en la tarjeta. La CA SINPE se reserva el derecho de aceptar tarjetas que están siendo sometidas a un proceso de certificación completo de los tres elementos, siempre y cuando aporten los resultados de una valoración de un tercero así como certificaciones FIPS o Common Criteria independientes para el chip y el sistema operativo.

h) La aplicación PKI a lo interno del chip debe implementar controles para evitar ataques de fuerza bruta contra el PIN y para asegurar que la comunicación entre el chip y el middleware sea encriptada.

i) La aplicación PKI debe cumplir con las especificaciones del estándar ISO 7816 parte 4 "Organization, security and commands for interchange" en lo que se refiere a la arquitectura de seguridad, la organización de datos y aplicaciones para el intercambio de información entre el dispositivo y el exterior (APDU).

j) Las funciones criptográficas implementadas en la tarjeta deben cumplir con las especificaciones del estándar ISO 7816 parte 8 "Comandos para las operaciones de seguridad".

k) Como mínimo, la tarjeta debe implementar los comandos de administración del ciclo de vida estipulados en el estándar ISO 7816 parte 9 "Comandos para la administración de la tarjeta".

l) Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 4, 8 y 9 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.

m) La administración sobre las aplicaciones cargadas en el chip debe estar implementada de manera independiente; es decir que la administración sobre las aplicaciones de pago será de la Entidad Emisora y sobre la aplicación PKI será de la CA del SINPE. En caso de que la implementación de este requisito incluyera la definición de llaves de administración, el fabricante debe garantizar la independencia de las mismas, de forma que las diferentes llaves sean establecidas de forma confidencial y exclusiva para la Entidad Emisora y para la CA del SINPE, según corresponda. La entrega de los valores de las llaves (cuando aplique) deberá realizarse bajo controles que garanticen su confidencialidad.

n) La tarjeta debe implementar un modelo de "Ciclo de Vida" para controlar diferentes estados de la funcionalidad y seguridad de la tarjeta. La tarjeta debe ser entregada a la Entidad Emisora en un estado que garantice que está lista para el proceso de generación de llaves y para el almacenamiento de los certificados digitales. Adicionalmente, una vez que la tarjeta contenga las llaves necesarias y los elementos de seguridad, debe cambiar a un estado que garantice su seguridad y su funcionalidad total.

o) Las acciones administrativas sobre la tarjeta solamente deben ser ejecutadas cuando se utiliza la llave de administración (Admin Key) como mecanismo de autenticación. Lo anterior debe incluir la funcionalidad de inicialización del dispositivo, creación y borrado de llaves y certificados, así como el desbloqueo del PIN de usuario. Dichas capacidades administrativas no deben ser accesibles para los usuarios finales.

p) La tarjeta debe proveer un PIN de usuario, para controlar el acceso a la funcionalidad que provee la aplicación PKI. El PIN debe ser numérico con una tener un tamaño mínimo de 4 y máximo de 14 dígitos. Después de 7 intentos fallidos del PIN, la aplicación PKI se debe bloquear. Adicionalmente, la aplicación PKI debe implementar, a lo interno del chip, reglas de complejidad del PIN que limiten el uso de dígitos repetidos (máximo 2) y el uso de dígitos

consecutivos (máximo 2) de forma que, independientemente de la aplicación o sistema operativo que se utilice para cambiar el PIN, la tarjeta siempre verifique dichas reglas.

4. Requisitos de compatibilidad con la CA del SINPE

a) La tarjeta inteligente debe tener, a lo interno del chip, la aplicación PKI LASER de NXP Semiconductors[3] y utilizar esta como aplicación PKI.

b) La tarjeta inteligente debe ser compatible con la herramienta Forefront Identity Manager (FIM) de Microsoft versión FIM 2010 R2, para plataforma de 64 bits, que es el sistema administrador de dispositivos (CMS por sus siglas en inglés) utilizado por la CA del SINPE. Esta compatibilidad debe estar dada a través de un minidriver oficialmente certificado por Microsoft. Si las tarjetas requieren de algún proceso de inicialización específico para poder ser utilizados en FIM, ese proceso deberá ser realizado por el fabricante previo a su entrega a la Entidad Emisora. Cuando el fabricante entregue las tarjetas a la entidad, las mismas deben estar totalmente listas para ser utilizadas en FIM.

c) La tarjeta debe implementar una funcionalidad que garantice que viene de fábrica pre-personalizada con una llave de administración (admin key) única y específica para el uso de la CA del SINPE. Esta llave debe permitir su diversificación posterior y debe ser bloqueada después de 10 intentos fallidos; dicha configuración se consignará en el perfil de FIM. El valor de esta llave será establecido por la CA del SINPE quien lo facilitará al fabricante; la entrega deberá hacerse siguiendo los controles apropiados para salvaguardar su confidencialidad.

d) Las tarjetas deben estar configuradas para que el número UID (Unique Permanent Identification) que tienen en su chip (establecido en el momento de su fabricación) sea asignado a la variable CP_CARD_GUID, agregando los ceros a la izquierda necesarios, de forma que se garantice que este número corresponda al desplegado por FIM como número de serie del dispositivo. Por ejemplo si el número de serie del chip es 0653000341246254, la variable CP_CARD_GUID debe ser actualizada con el valor 00000000000000000653000341246254, de forma que en FIM se despliegue el valor {00000000-0000-0000-0653-000341246254}. Este valor deberá garantizar la unicidad del número de serie del chip, por lo que se recomienda que esté formado por fecha de fabricación + número de serie + id del batch. Cada vez que se realice una compra el proveedor debe entregar, en conjunto con los dispositivos criptográficos, un archivo electrónico en formato XML que contenga los números de serie de todos y cada uno de los dispositivos de la compra. El formato del archivo en que se reciba la información deberá realizarse de conformidad con las especificaciones contenidas en el Estándar Electrónico – Firma Digital.

e) La aplicación PKI debe ser capaz de firmar digitalmente solicitudes de certificado construidas con formato PKCS #10 y que se le envían a la CA del SINPE para la emisión de los certificados correspondientes. Lo anterior como señal de posesión de la llave privada por parte del solicitante.

5. Requisitos de interoperabilidad y neutralidad tecnológica

a) El sistema operativo del dispositivo criptográfico debe ser de plataforma abierta Java Card, que permita el funcionamiento de múltiples aplicaciones que se ejecuten a lo interno del chip. Las características del Sistema Operativo deben ser tales que permita que exista total independencia al desarrollar las diferentes aplicaciones.

---

3 *La aplicación PKI LASER de NXP Semiconductors es la misma que poseen las tarjetas ID Protect Laser Card de Athena (Actualmente NXP Semiconductors) que se encuentran homologadas.*

b) Tanto el sistema operativo como las aplicaciones implementadas en la tarjeta deben cumplir con las especificación de GlobalPlatform Card v 2.1.1 o superior incluida la especificación GlobalPlatform para el API de Java Card.

c) Para lograr la comunicación entre los computadores y la aplicación PKI de la tarjeta, el fabricante debe suministrar el middleware IDProtect, asociado a la aplicación PKI LASER para acceder la funcionalidad PKI dentro de la tarjeta. El middleware debe proveer las siguientes interfaces:

i) Un CSP con soporte a CryptoAPI.

ii) Un minidriver.

iii) Una librería PKCS#11.

iv) Un driver Tokend para Mac.

d) El CSP debe operar en sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.

e) El minidriver debe estar oficialmente certificado por Microsoft y debe cumplir con el "Windows Smart Card Minidriver Specification" con soporte a Base CSP y KSP para los sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.

f) La librería PKCS#11 debe ser provista para las plataformas Windows, Mac OS y Linux, en las versiones oficialmente soportadas por cada fabricante.

g) El middleware debe permitir que los certificados digitales, las llaves y la funcionalidad de la aplicación PKI puedan ser accedidos en aplicaciones de usuario final que corren, como mínimo, en los navegadores nativos de las plataformas Windows (IE Explorer) y Mac OS (Safari) y en Mozilla Firefox y Google Chrome; en las versiones oficialmente soportadas por cada fabricante.

h) El fabricante debe garantizar que los certificados emitidos a través del minidriver sean utilizables también por medio de los otros drivers solicitados (PKCS#11 y Tokend). Es decir, que las tarjetas con certificados emitidos en un sistema operativo Microsoft a través del minidriver puedan ser utilizadas en otros sistemas operativos distintos a Microsoft.

i) El uso de cada contacto y las interfaces eléctricas en los dispositivos criptográficos debe cumplir las especificaciones de los estándares ISO/IEC 7816-3, ISO/IEC 7816-10 e ISO/IEC 7816-12, según los tipos de interfaces que el dispositivo provea y a la asignación de cada contacto conforme al Anexo A del estándar ISO/IEC 7816-2.

j) Para permitir la interoperabilidad de los dispositivos criptográficos entre diferentes organizaciones, los elementos de datos del dispositivo deben cumplir con las especificaciones del estándar ISO 7816-6.

k) Los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-7 en el uso de los comandos para el lenguaje SCQL.

l) Las funciones criptográficas implementadas en el chip de los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-15, de forma que se garantice la compatibilidad de las aplicaciones criptográficas con varios emisores de dispositivos.

m) Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 6 y 15 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.

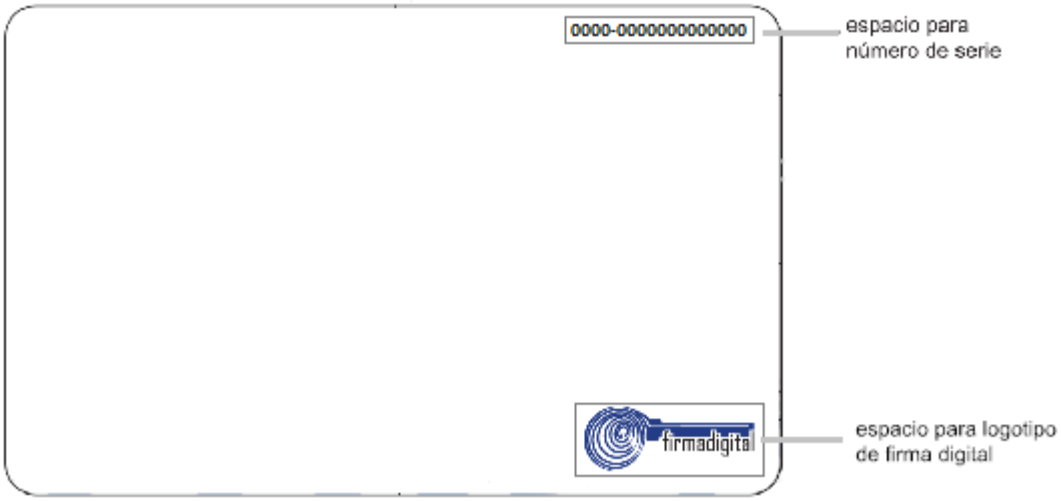
n) Las tarjetas deben ser compatibles con lectores de tarjetas estándar, en cumplimiento de las especificaciones PC/SC y del ISO 7816 partes 1 a 3. Además, deben soportar como mínimo los protocolos de transmisión T=0 o T=1.

6.1.9. Anexo No. 9: Diseño de la tarjeta inteligente – PKI sobre Tarjetas de Pago certificadas por EMV

En las imágenes que se muestran a continuación se especifican los campos de uso obligatorio que debe contener el diseño de las tarjetas inteligentes de que implementen Firma Digital sobre EMV:

Anverso

Reverso



- El número de serie impreso debe corresponder al número desplegado por FIM como número de serie de la tarjeta, el cual en cumplimiento con los requerimientos del Anexo 9 debe ser

equivalente al UID (Unique Permanent Identification) del chip de la tarjeta. El formato de impresión del número de serie debe ser 9999-999999999999.

- La impresión de la tarjeta debe realizarse con una tecnología de impresión tal que el fabricante garantice su calidad por un mínimo de cuatro años, para lo cual las tarjetas deben laminarse tanto en su anverso como en su reverso, tomando en cuenta que debe dejarse libre el espacio del chip. El número de serie deberá ser impreso con tecnología láser.
- El espacio para la firma del titular deberá ajustarse a lo estipulado para las tarjetas EMV.
- El archivo en formato digital con el diseño de impresión en digital se podrá entregar en los siguientes formatos: .psd, .eps, .pdf, .tiff, .gif y .jpg, La OR interesada debe solicitarlo por escrito, y será entregado junto con todos los requisitos de diseño.

6.1.10. Anexo No. 10: Proceso de homologación de dispositivos criptográficos para el almacenamiento de certificados de firma digital

1. Objetivo

Establecer el proceso para la homologación de dispositivos criptográficos de acuerdo a las especificaciones técnicas establecidas en el Estándar Físico – Firma Digital.

2. Requisitos de Participación

Los interesados deberán entregar, para cada dispositivo criptográfico a homologar, un sobre cerrado y rotulado: “Homologación de Dispositivos Criptográficos para la CA de Persona Física del SINPE”, más el nombre del proveedor, el tipo de dispositivo (Tarjeta Inteligente PKI/Tarjeta Inteligente PKI-EMV), marca y modelo del dispositivo, lo siguiente:

a) Una carta dirigida a CA SINPE – Persona Física firmada por el representante legal de la empresa proveedora, especificando lo siguiente:

i) Nombre, número de teléfono y dirección de correo electrónico del contacto oficial por parte del proveedor.

ii) Nombre y dirección de correo electrónico del personal técnico del fabricante a quien se le pueda dirigir directamente las consultas técnicas que la CA SINPE – Persona Física considere necesarias durante el proceso de homologación.

iii) Características de los dispositivos que se están presentado para homologación (cantidad, tipo tarjeta, marca, modelo) y demás características que el proveedor considere relevantes.

iv) Número de certificado FIPS 140-2 nivel 3 otorgado por el NIST o el número de certificado de Common Criteria EAL 4+ en el perfil de protección SSCD Tipo 3 (Secure Signature-Creation Device), que respalde la marca y modelo de los dispositivos que se están entregando.

b) Una copia impresa o digital de la tabla “Requisitos Técnicos” contenida en este anexo. El proveedor deberá anotar el nombre de los documentos electrónicos solicitados, en la columna “Detalle de Cumplimiento”, según corresponda. Esta copia será la base para realizar la verificación de cada uno de los requisitos técnicos. Para estos efectos la CA SINPE – Persona Física enviará por correo electrónico a cada proveedor una copia electrónica del presente anexo previa solicitud del mismo.

c) Documento impreso del Acuerdo de Confidencialidad, el cual debe ser presentado debidamente lleno con firma y sellos del fabricante de los dispositivos criptográficos. El objetivo de esta formalidad es garantizar el adecuado manejo de las llaves de administración

de los dispositivos criptográficos. Para estos efectos la CA SINPE – Persona Física enviará por correo electrónico a cada proveedor una copia electrónica del Acuerdo de Confidencialidad previa solicitud del mismo.

d) Al menos cuatro dispositivos criptográficos de cada tipo que se presente a homologación, para las pruebas respectivas.

e) Un disco compacto que contenga toda la documentación electrónica solicitada para cada tipo de dispositivo en la columna "Evidencia de Cumplimiento" de la tabla "Requisitos Técnicos" y rotulado de la siguiente forma: "Evidencia de Cumplimiento" más el tipo de dispositivo criptográfico (Tarjeta Inteligente PKI/Tarjeta Inteligente PKI-EMV), la marca, modelo de los dispositivos criptográficos y el nombre del proveedor.

f) Un disco compacto con tres carpetas, una para cada plataforma: Windows, Mac y Linux. Cada carpeta debe incluir dos sub carpetas: una para plataforma de 32 bits (con el nombre "32 bits") y otra para 64 bits (con el nombre "64 bits"). Cada sub carpeta debe contener el middleware con las interfaces para acceder los certificados y las llaves del dispositivo criptográfico, de acuerdo a las especificaciones técnicas. La carpeta para plataforma Windows debe contener el minidriver (en formato .msi), el CSP con soporte a Crypto API y la interfaz PKCS#11. La carpeta para plataforma Mac debe contener la interfaz PKCS#11 y la librería tokend. La carpeta para plataforma Linux debe contener la interfaz PKCS#11.

En el disco compacto debe entregarse un manual con los pasos de la instalación del software, las particularidades del proceso de instalación y la configuración necesaria para el funcionamiento de los dispositivos en cada una de las plataformas y navegadores. El manual también deberá especificar detalladamente los pasos para la desinstalación del middleware. Los manuales deberán entregarse en formato digital en el disco compacto.

Este disco compacto debe rotularse con el nombre MIDDLEWARE, el tipo de dispositivo criptográfico (Tarjeta Inteligente PKI/Tarjeta Inteligente PKI-EMV), la marca y modelo del dispositivo criptográfico y el nombre del proveedor.

g) Una aplicación que provea al usuario final la facilidad de administración del dispositivo criptográfico, la cual es únicamente para uso del personal técnico de la CA SINPE – Persona Física.

La aplicación debe permitir ver el contenido del dispositivo, cambiar el PIN y permitir ver el detalle del hardware, firmware y versión de sistema operativo. Adicionalmente, debe ser compatible como mínimo con los sistemas operativos oficialmente soportados por Microsoft.

La aplicación debe incluir un manual de usuario que explique los pasos para la instalación y desinstalación, así como una explicación de cada una de las funcionalidades que la aplicación implementa. El manual debe indicar claramente los sistemas operativos donde corre la aplicación, así como la interface bajo la cual se comunica con el dispositivo (minidriver, CSP con soporte CryptoAPI o librería PKCS#11). El manual debe entregarse en formato digital en el mismo disco compacto que contiene la aplicación descrita en este punto.

El contenido del sobre será parte de la evidencia del proceso de homologación, por lo que será conservado por la CA SINPE – Persona Física una vez finalizado el proceso.

3. Reglas para la homologación

a) La marca y modelo de los dispositivos criptográficos homologados por la CA SINPE – Persona Física serán publicadas en el apartado de Firma Digital de la página web del Banco

Central de Costa Rica (http://www.bccr.fi.cr/). Con base en este proceso, la CA SINPE - Persona Física operará únicamente con los dispositivos criptográficos homologados.

b) Los dispositivos criptográficos que resulten homologados en este proceso deberán someterse a un nuevo proceso de homologación en caso de que varíen las características de los mismos o bien cuando la CA SINPE- Persona Física haya variado las especificaciones técnicas para estos.

c) El proceso de homologación será ejecutado únicamente en aquellos casos en que la totalidad de Requisitos de Participación se cumplan. Las pruebas de funcionamiento se realizarán únicamente sobre los dispositivos para los cuales la CA SINPE - Persona Física haya validado el cumplimiento de los Requisitos Técnicos, verificables por medio de los documentos aportados.

d) Los proveedores tienen la facultad para elegir el tipo de los dispositivos criptográficos que deseen presentar para homologación: tarjetas PKI, tarjetas PKI sobre Tarjetas de Pago certificadas por EMV, o ambas.

e) La CA SINPE – Persona Física se reserva el derecho de solicitar cualquier explicación que considere necesaria para aclarar aspectos técnicos del dispositivo o de la documentación presentada.

f) Al presentar la carta especificada en el punto a) de los Requisitos de Participación, el proveedor acepta la participación sujetándose en todo a las condiciones descritas.

4. Proceso de homologación

El proceso para homologar los dispositivos criptográficos se realizará en etapas que corresponden con las secciones de las especificaciones técnicas. La CA SINPE – Persona Física se reserva el derecho de realizar revisiones documentales, revisión de certificaciones, pruebas de funcionamiento y pruebas de compatibilidad con herramientas de terceros.

Las pruebas incluidas en el proceso de homologación se realizarán con base en el siguiente esquema:

a) Revisión de Requisitos Generales

- **i)** Verificación de certificaciones.
- **ii)** Revisión documental de características técnicas.

b) Revisión de Requisitos de Seguridad del Chip

- **i)** Verificación de certificaciones.
- **ii)** Revisión documental de características técnicas.
- **iii)** Verificación de la presentación del Acuerdo de Confidencialidad.
- **iv)** Creación de llaves en la tarjeta (requiriendo el Admin Key).
- **v)** Bloqueo del dispositivo por intentos fallidos de digitación del PIN.
- **vi)** Prueba de cambio de PIN y de las reglas de complejidad.

c) Revisión de Requisitos de Compatibilidad con la CA del SINPE

- **i)** Revisión documental de características técnicas.
- **ii)** Emisión de certificados de autenticación y firma digital.
- **iii)** Activación del dispositivo criptográfico y definición del PIN.
- **iv)** Eliminación de los certificados de firma y autenticación del dispositivo criptográfico.

v) Re-emisión de nuevos certificados en el mismo dispositivo.

vi) Bloqueo del dispositivo criptográfico al utilizar el “Admin Key” de forma errónea.

d) Revisión de Requisitos de Interoperabilidad y Neutralidad Tecnológica

i) Verificación de certificaciones.

ii) Revisión documental de características técnicas.

iii) Pruebas de autenticación y firma digital utilizando aplicaciones Web.

iv) Pruebas de firma digital utilizando aplicaciones ofimáticas.

v) Pruebas de la aplicación de administración del dispositivo.

5. Requisitos Técnicos

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Requisitos Generales		
Las características físicas de las tarjetas inteligentes, incluyendo materiales, fabricación y dimensiones, deben cumplir con el estándar ISO/IEC 7810, específicamente para la tarjeta de tamaño ID-1 (nominalmente 85.60 mm de ancho por 53.98 mm de alto por 0.76 mm de grosor, el estándar especifica un rango de dimensiones mínimas y máximas).	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento electrónico con la certificación emitida por un laboratorio autorizado, la cual evidencie que las tarjetas fueron sometidas a las pruebas respecto al estándar ISO/IEC 10373-1. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
Las pruebas realizadas a las tarjetas para demostrar que cumplen con los parámetros especificados en el estándar ISO/IEC 7810 deben haberse realizado en cumplimiento con los procedimientos de pruebas estipulados en el estándar ISO/IEC 10373-1.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Las tarjetas inteligentes deben ser dispositivos con microprocesador criptográfico con un único chip de circuito integrado con contactos y deben cumplir con las características descritas en el estándar ISO/IEC 7816-1. Además, deben cumplir con en la enmienda 1 de este mismo estándar (ISO/IEC 7816-1/Amd.1:2003) en lo que respecta al alto máximo de la superficie del chip.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento electrónico con la certificación emitida por un laboratorio autorizado, la cual evidencie que las tarjetas fueron sometidas a las pruebas respecto al estándar ISO/IEC 10373-3. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
El chip de los dispositivos criptográficos debe poseer ocho contactos según lo indica el estándar ISO/IEC 7816-2, cuya dimensión y ubicación en la tarjeta debe cumplir con lo especificado en dicho estándar.		
Las pruebas realizadas para demostrar que el chip de los dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 1 y 2 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3 para los chips criptográficos de contactos y los dispositivos de interface relacionados.		
Requisitos de Seguridad de Chip		
El chip del dispositivo criptográfico debe tener la capacidad de generar pares de llaves criptográficas (pública y privada) a lo interno del chip de al menos 2048 bits.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Después de que la tarjeta ha sido inicializada y personalizada, la capacidad de la memoria EEPROM debe permitir el funcionamiento correcto de la aplicación PKI y el almacenamiento simultáneo de al menos cuatro certificados X.509 V3 y sus correspondientes llaves de 2048 bits.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	
De preferencia, la aplicación a lo interno de la tarjeta, que provee la funcionalidad de firma digital (en adelante llamada aplicación PKI), deberá residir en la memoria ROM.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
A ningún nivel (hardware, firmware, software, middleware) el dispositivo criptográfico debe permitir que la llave privada generada a lo interno del chip abandone o sea extraída del mismo.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
El dispositivo criptográfico debe soportar como mínimo los algoritmos criptográficos: SHA-1, SHA-256, 3DES, RSA con llaves de 2048 bits.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
El chip del dispositivo criptográfico debe poseer certificación a nivel 3 o superior del estándar FIPS 140-2 o la certificación Common Criteria EAL 4+ en el perfil de protección SSCD Tipo 3 (Secure Signature-Creation Device). Las tarjetas que sólo posean la certificación FIPS 140-2 nivel 3 o superior, deben operar en modo FIPS de forma natural. La CA del SINPE se reserva el derecho de aceptar las tarjetas cuya certificación del NIST indique la leyenda "cuando es operado en modo FIPS" (When operated in FIPS mode), hasta poder analizar la Política de Seguridad correspondiente y concluir que la operación en modo FIPS, una vez habilitada, es irreversible. La documentación oficial que demuestre las certificaciones debe corresponder en marca y modelo a las tarjetas inteligentes que usará la OR. Cualquiera de las dos certificaciones debe incluir el circuito integrado de contactos, el sistema operativo y la aplicación PKI en la tarjeta. La CA SINPE se reserva el derecho de aceptar tarjetas que están siendo sometidas a un proceso de certificación completo de los tres elementos, siempre y cuando aporten los resultados de una valoración de un tercero así como certificaciones FIPS o Common Criteria independientes para el chip y el sistema operativo.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. El cumplimiento de este punto se validará en la página http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm si cumple con FIPS 140-2 o en la página http://www.commoncriteriaportal.org/products/ si cumple con Common Criteria. La validación se realizará de acuerdo al número de certificado declarado en la carta solicitada en el punto 1 de los Requisitos de Participación. La CA SINPE – Persona Física se reserva el derecho de analizar las certificaciones y su documentación y pedir todas las aclaraciones que considere pertinentes para decidir si el alcance de la certificación satisface el requerimiento estipulado.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La aplicación PKI debe implementar controles para evitar ataques de fuerza bruta contra el PIN y para asegurar que la comunicación entre el chip y el middleware sea encriptada.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
La aplicación PKI a lo interno de la tarjeta debe cumplir con las especificaciones del estándar ISO 7816 parte 4 "Organization, security and commands for interchange" en lo que se refiere a la arquitectura de seguridad, la organización de datos y aplicaciones para el intercambio de información entre el dispositivo y el exterior (APDU).	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento electrónico con la certificación emitida por un laboratorio autorizado, la cual evidencie que las tarjetas fueron sometidas a las pruebas respecto al estándar ISO/IEC 10373-3. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
Las funciones criptográficas implementadas en la tarjeta deben cumplir con las especificaciones del estándar ISO 7816 parte 8 "Comandos para las operaciones de seguridad".		
Como mínimo, la tarjeta debe implementar los comandos de administración del ciclo de vida estipulados en el estándar ISO 7816 parte 9 "Comandos para la administración de la tarjeta".		
Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 4, 8 y 9 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La tarjeta debe implementar un modelo de "Ciclo de Vida" para controlar diferentes estados de la funcionalidad y seguridad de la tarjeta. La tarjeta debe ser entregada a la Entidad Emisora en un estado que garantice que está lista para el proceso de generación de llaves y para el almacenamiento de los certificados digitales. Adicionalmente, una vez que la tarjeta contenga las llaves necesarias y los elementos de seguridad, debe cambiar a un estado que garantice su seguridad y su funcionalidad total.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
El fabricante deberá configurar el sistema operativo del dispositivo criptográfico, de forma que sólo la CA del SINPE tenga acceso a los comandos administrativos del chip, estableciendo para ello el conjunto de llaves de administración de los dispositivos (también conocidas como ISD keys) conforme a lo especificado en el estándar Global Platform y de forma confidencial y exclusiva para la CA del SINPE. La distribución de estas llaves deberá hacerse siguiendo los controles apropiados para salvaguardar su confidencialidad y garantizar que sólo son conocidas por la CA del SINPE y el fabricante. La entrega de los valores de las llaves (cuando aplique) deberá realizarse bajo controles que garanticen su confidencialidad.	La distribución en forma confidencial de estas llaves aplica únicamente para los procesos de compra de dispositivos. Para efectos de este proceso de homologación, la CA SINPE – Persona Física no requiere conocer el valor de estas llaves; sin embargo se requiere que el fabricante envíe un Acuerdo de Confidencialidad donde se compromete a que las llaves fueron generadas de manera segura, secreta y exclusiva para la CA SINPE – Persona Física. De igual forma se requiere que el fabricante haga constar en este mismo documento que el estado del ciclo de vida de las tarjetas que entrega para homologación tiene el valor "SECURED" de acuerdo al estándar Global Platform.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
El dispositivo criptográfico debe ser configurado por el fabricante para que al momento de su entrega el "Estado del ciclo de vida de los dispositivos" tenga el valor "SECURED" de acuerdo al estándar Global Platform.	De conformidad con el punto 3 de los Requisitos de Participación, se adjunta copia del Acuerdo de Confidencialidad el cual debe entregarse impreso y con la firma y sellos del fabricante de los dispositivos.	
Las acciones administrativas sobre la tarjeta solamente deben ser ejecutadas cuando se utiliza la llave de administración (Admin Key) como mecanismo de autenticación. Lo anterior debe incluir la funcionalidad de inicialización del dispositivo, creación y borrado de llaves y certificados, así como el desbloqueo del PIN de usuario. Dichas capacidades administrativas no deben ser accesibles para los usuarios finales.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La tarjeta debe proveer un PIN de usuario, para controlar el acceso a la funcionalidad que provee la aplicación PKI. El PIN debe tener un tamaño mínimo de 4 y máximo de 14 dígitos. Después de 7 intentos fallidos del PIN, la aplicación PKI se debe bloquear. Adicionalmente, la aplicación PKI debe implementar, a lo interno del chip, reglas de complejidad del PIN que limiten el uso de dígitos repetidos (máximo 2) y el uso de dígitos consecutivos (máximo 2), de forma que, independientemente de la aplicación o sistema operativo que se utilice para cambiar el PIN, la tarjeta siempre verifique dichas reglas.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento, denominado "Reglas de Complejidad del PIN", que contenga una lista de todas las reglas de complejidad del PIN, ya sean las requeridas en este punto o cualquier otra adicional. Para cada regla se debe indicar si la funcionalidad está implementada a lo interno del chip o por medio de software. Adicionalmente, el cumplimiento de estos puntos se verificará con las pruebas de funcionamiento.	
Requisitos de Compatibilidad con la CA SINPE		
La tarjeta inteligente debe tener, a lo interno del chip, la aplicación PKI LASER de NXP Semiconductors y utilizar esta como aplicación PKI.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el complimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La tarjeta inteligente debe ser compatible con la herramienta Forefront Identity Manager (FIM) de Microsoft versión FIM 2010 R2, para plataforma de 64 bits, que es el sistema administrador de dispositivos (CMS por sus siglas en inglés) utilizado por la CA del SINPE. Esta compatibilidad debe estar dada a través de un minidriver oficialmente certificado por Microsoft. Si las tarjetas requieren de algún proceso de inicialización específico para poder ser utilizados en FIM, ese proceso deberá ser realizado por el fabricante previo a su entrega a la Entidad Emisora. Cuando el fabricante entregue las tarjetas a la entidad, las mismas deben estar totalmente listas para ser utilizadas en FIM.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el complimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento, para lo cual los dispositivos criptográficos deben venir configurados para funcionar en FIM de acuerdo al perfil indicado en el anexo “Configuración de la plantilla del perfil del dispositivo criptográfico en FIM”.	
La tarjeta debe implementar una funcionalidad que garantice que viene de fábrica pre-personalizada con una llave de administración (admin key) única y específica para el uso de la CA del SINPE. Esta llave debe permitir su diversificación posterior y debe ser bloqueada después de 10 intentos fallidos; dicha configuración se consignará en el perfil de FIM. El valor de esta llave será establecido por la CA del SINPE quien lo facilitará al fabricante. La entrega deberá hacerse siguiendo los controles apropiados para salvaguardar su confidencialidad.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Las tarjetas deben estar configuradas para que el número UID (Unique Permanent Identification) que tienen en su chip (establecido en el momento de su fabricación) sea asignado a la variable CP_CARD_GUID, agregando los ceros a la izquierda necesarios, de forma que se garantice que este número corresponda al desplegado por FIM como número de serie del dispositivo. Por ejemplo si el número de serie del chip es 0653000341246254, la variable CP_CARD_GUID debe ser actualizada con el valor 0000000000000000006530003412462 54, de forma que en FIM se despliegue el valor {00000000-0000-0000-0653-000341246254}. Este valor deberá garantizar la unicidad del número de serie del chip, por lo que se recomienda que esté formado por fecha de fabricación + número de serie + id del batch. Cada vez que se realice una compra el proveedor debe entregar, en conjunto con los dispositivos criptográficos, un archivo electrónico en formato XML que contenga los números de serie de todos y cada uno de los dispositivos de la compra. El formato del archivo en que se reciba la información deberá realizarse de conformidad con las especificaciones contenidas en el Estándar Electrónico – Firma Digital.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La aplicación PKI debe ser capaz de firmar digitalmente solicitudes de certificado construidas con formato PKCS #10 y que se le envían a la CA del SINPE para la emisión de los certificados correspondientes. Lo anterior como señal de posesión de la llave privada por parte del solicitante.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	
Requisitos de Interoperabilidad y Neutralidad Tecnológica		
El sistema operativo del dispositivo criptográfico debe ser de plataforma abierta Java Card, que permita el funcionamiento de múltiples aplicaciones que se ejecuten a lo interno del chip y que se puedan incluir posteriormente. Las características del Sistema Operativo deben ser tales que permita que haya independencia en quién o quiénes puedan desarrollar dichas aplicaciones.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
El sistema operativo del dispositivo criptográfico debe cumplir con la especificación de Global Platform 2.1.1 o superior, con el objetivo de permitir cualquier combinación de aplicaciones de diferentes tipos o proveedores en un único dispositivo criptográfico.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Para lograr la comunicación entre los computadores y la aplicación PKI de la tarjeta, el fabricante debe suministrar el middleware IDProtect, asociado a la aplicación PKI LASER, para acceder la funcionalidad PKI dentro de la tarjeta. El middleware debe proveer las siguientes interfaces: Un CSP con soporte a CryptoAPI Un minidriver Una librería PKCS#11 Un driver Tokend para Mac	De conformidad con los puntos 6 y 7 de los Requisitos de Participación, se debe entregar el disco compacto que contenga las versiones más recientes del middleware con las interfaces para acceder los certificados y las llaves del dispositivo criptográfico solicitadas. Respecto a la certificación solicitada para el minidriver, en el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento denominado "Certificación Microsoft" cuyo contenido sea la certificación dada por Microsoft. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. El cumplimiento de este punto se verificará en la página "Windows Certified Products List" https://sysdev.microsoft.com/en-us/hardware/lpl/ .	
El CSP debe operar en sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.		
El minidriver debe estar oficialmente certificado por Microsoft y debe cumplir con el "Windows Smart Card Minidriver Specification" con soporte a Base CSP y KSP para los sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.		
La librería PKCS#11 debe ser provista para las plataformas Windows, Mac OS y Linux; en las versiones oficialmente soportadas por cada fabricante.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
El middleware debe permitir que los certificados digitales, las llaves y la funcionalidad de la aplicación PKI puedan ser accedidos en aplicaciones de usuario final que corren, como mínimo, en los navegadores nativos de las plataformas Windows (IE Explorer) y Mac OS (Safari), y en Mozilla Firefox y Google Chrome; en las versiones oficialmente soportadas por cada fabricante.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	
El fabricante debe garantizar que los certificados emitidos a través del minidriver sean utilizables también por medio de los otros drivers solicitados (PKCS#11 y Tokend). Es decir, que las tarjetas con certificados emitidos en un sistema operativo Microsoft a través del minidriver puedan ser utilizadas en otros sistemas operativos distintos a Microsoft.	Su cumplimiento se verificará en las pruebas de funcionamiento.	
El uso de cada contacto y las interfaces eléctricas en los dispositivos criptográficos debe cumplir las especificaciones de los estándares ISO/IEC 7816-3, ISO/IEC 7816-10 e ISO/IEC 7816-12, según los tipos de interfaces que el dispositivo provea y a la asignación de cada contacto conforme al Anexo A del estándar ISO/IEC 7816-2.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento electrónico con la certificación emitida por un laboratorio autorizado, la cual evidencie que las tarjetas fueron sometidas a las pruebas respecto al estándar ISO/IEC 10373-3. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
Para permitir la interoperabilidad de los dispositivos criptográficos entre diferentes organizaciones, los elementos de datos del dispositivo deben cumplir con las especificaciones del estándar ISO 7816-6.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-7 en el uso de los comandos para el lenguaje SCQL.		
Las funciones criptográficas implementadas en el chip de los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-15, de forma que se garantice la compatibilidad de las aplicaciones criptográficas con varios emisores de dispositivos.		
Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 3, 10, 12, 6, 7 y 15 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.		
Las tarjetas deben ser compatibles con lectores de tarjetas estándar, en cumplimiento de las especificaciones PC/SC y del ISO 7816 partes 1 a 3. Además, deben soportar como mínimo los protocolos de transmisión T=0 o T=1.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Requisitos Generales		
Los dispositivos criptográficos deben contar con una certificación verificable del cumplimiento de las Especificaciones de Tarjetas de Circuito Integrado para Sistemas de Pago de EMVCo.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
Requisitos de Seguridad de Chip		
El chip del dispositivo criptográfico debe tener la capacidad de generar pares de llaves criptográficas (pública y privada) a lo interno del chip de al menos 2048 bits.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Después de que la tarjeta ha sido inicializada y personalizada, la capacidad de la memoria EEPROM debe permitir el funcionamiento correcto de la aplicación PKI y el almacenamiento simultáneo de al menos cuatro certificados X.509 V3 y sus correspondientes llaves de 2048 bits.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	
Todas las aplicaciones que contenga la tarjeta deben ser cargadas en el chip desde el momento de fabricación de la tarjeta. La Entidad Emisora de los dispositivos de pago, junto con el fabricante de las tarjetas, deberán acordar los controles para garantizar que no se pueden agregar, modificar o eliminar aplicaciones de la tarjeta y que únicamente el fabricante y la entidad emisora (si ésta lo considera conveniente) tienen acceso a los comandos administrativos del chip. De preferencia la aplicación PKI deberá residir en la memoria ROM.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
A ningún nivel (hardware, firmware, software, middleware) el dispositivo criptográfico debe permitir que la llave privada generada a lo interno del chip abandone o sea extraída del mismo.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
El dispositivo criptográfico debe soportar como mínimo los algoritmos criptográficos: SHA-1, SHA-256, 3DES, RSA con llaves de 2048 bits.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
El chip del dispositivo criptográfico debe poseer certificación a nivel 3 o superior del estándar FIPS 140-2 o la certificación Common Criteria EAL 4+ en el perfil de protección SSCD Tipo 3 (Secure Signature-Creation Device). Las tarjetas que sólo posean la certificación FIPS 140-2 nivel 3 o superior, deben operar en modo FIPS de forma natural. La CA del SINPE se reserva el derecho de aceptar las tarjetas cuya certificación del NIST indique la leyenda "cuando es operado en modo FIPS" (When operated in FIPS mode), hasta poder analizar la Política de Seguridad correspondiente y concluir que la operación en modo FIPS, una vez habilitada, es irreversible. La documentación oficial que demuestre las certificaciones debe corresponder en marca y modelo a las tarjetas inteligentes que usará la OR. Cualquiera de las dos certificaciones debe incluir el circuito integrado de contactos, el sistema operativo y la aplicación PKI en la tarjeta. La CA SINPE se reserva el derecho de aceptar tarjetas que están siendo sometidas a un proceso de certificación completo de los tres elementos, siempre y cuando aporten los resultados de una valoración de un tercero así como certificaciones FIPS o Common Criteria independientes para el chip y el sistema operativo.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. El cumplimiento de este punto se validará en la página http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm si cumple con FIPS 140-2 o en la página http://www.commoncriteriaportal.org/products/ si cumple con Common Criteria. La validación se realizará de acuerdo al número de certificado declarado en la carta solicitada en el punto 1 de los Requisitos de Participación. La CA SINPE – Persona Física se reserva el derecho de analizar las certificaciones y su documentación y pedir todas las aclaraciones que considere pertinentes para decidir si el alcance de la certificación satisface el requerimiento estipulado.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La aplicación PKI a lo interno del chip debe implementar controles para evitar ataques de fuerza bruta contra el PIN y para asegurar que la comunicación entre el chip y el middleware sea encriptada.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
La aplicación PKI debe cumplir con las especificaciones del estándar ISO 7816 parte 4 "Organization, security and commands for interchange" en lo que se refiere a la arquitectura de seguridad, la organización de datos y aplicaciones para el intercambio de información entre el dispositivo y el exterior (APDU).	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento electrónico con la certificación emitida por un laboratorio autorizado, la cual evidencie que las tarjetas fueron sometidas a las pruebas respecto al estándar ISO/IEC 10373-3. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
Las funciones criptográficas implementadas en la tarjeta deben cumplir con las especificaciones del estándar ISO 7816 parte 8 "Comandos para las operaciones de seguridad".		
Como mínimo, la tarjeta debe implementar los comandos de administración del ciclo de vida estipulados en el estándar ISO 7816 parte 9 "Comandos para la administración de la tarjeta".		
Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 4, 8 y 9 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La administración sobre las aplicaciones cargadas en el chip debe estar implementada de manera independiente; es decir que la administración sobre las aplicaciones de pago será de la Entidad Emisora y sobre la aplicación PKI será de la CA del SINPE. En caso de que la implementación de este requisito incluyera la definición de llaves de administración, el fabricante debe garantizar la independencia de las mismas, de forma que las diferentes llaves sean establecidas de forma confidencial y exclusiva para la Entidad Emisora y para la CA del SINPE, según corresponda. La entrega de los valores de las llaves (cuando aplique) deberá realizarse bajo controles que garanticen su confidencialidad.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
La tarjeta debe implementar un modelo de “Ciclo de Vida” para controlar diferentes estados de la funcionalidad y seguridad de la tarjeta. La tarjeta debe ser entregada a la Entidad Emisora en un estado que garantice que está lista para el proceso de generación de llaves y para el almacenamiento de los certificados digitales. Adicionalmente, una vez que la tarjeta contenga las llaves necesarias y los elementos de seguridad, debe cambiar a un estado que garantice su seguridad y su funcionalidad total.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Las acciones administrativas sobre la tarjeta solamente deben ser ejecutadas cuando se utiliza la llave de administración (Admin Key) como mecanismo de autenticación. Lo anterior debe incluir la funcionalidad de inicialización del dispositivo, creación y borrado de llaves y certificados, así como el desbloqueo del PIN de usuario. Dichas capacidades administrativas no deben ser accesibles para los usuarios finales.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La tarjeta debe proveer un PIN de usuario, para controlar el acceso a la funcionalidad que provee la aplicación PKI. El PIN debe ser numérico con una tener un tamaño mínimo de 4 y máximo de 14 dígitos. Después de 7 intentos fallidos del PIN, la aplicación PKI se debe bloquear. Adicionalmente, la aplicación PKI debe implementar, a lo interno del chip, reglas de complejidad del PIN que limiten el uso de dígitos repetidos (máximo 2) y el uso de dígitos consecutivos (máximo 2)., de forma que, independientemente de la aplicación o sistema operativo que se utilice para cambiar el PIN, la tarjeta siempre verifique dichas reglas.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento, denominado "Reglas de Complejidad del PIN", que contenga una lista de todas las reglas de complejidad del PIN, ya sean las requeridas en este punto o cualquier otra adicional. Para cada regla se debe indicar si la funcionalidad está implementada a lo interno del chip o por medio de software. Adicionalmente, el cumplimiento de estos puntos se verificará con las pruebas de funcionamiento.	
Requisitos de Compatibilidad con la CA SINPE		
La tarjeta inteligente debe tener, a lo interno del chip, la aplicación PKI LASER de NXP Semiconductors y utilizar esta como aplicación PKI.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el complimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La tarjeta inteligente debe ser compatible con la herramienta Forefront Identity Manager (FIM) de Microsoft versión FIM 2010 R2, para plataforma de 64 bits, que es el sistema administrador de dispositivos (CMS por sus siglas en inglés) utilizado por la CA del SINPE. Esta compatibilidad debe estar dada a través de un minidriver oficialmente certificado por Microsoft. Si las tarjetas requieren de algún proceso de inicialización específico para poder ser utilizados en FIM, ese proceso deberá ser realizado por el fabricante previo a su entrega a la Entidad Emisora. Cuando el fabricante entregue las tarjetas a la entidad, las mismas deben estar totalmente listas para ser utilizadas en FIM.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el complimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento, para lo cual los dispositivos criptográficos deben venir configurados para funcionar en FIM de acuerdo al perfil indicado en el anexo “Configuración de la plantilla del perfil del dispositivo criptográfico en FIM”.	
La tarjeta debe implementar una funcionalidad que garantice que viene de fábrica pre-personalizada con una llave de administración (admin key) única y específica para el uso de la CA del SINPE. Esta llave debe permitir su diversificación posterior y debe ser bloqueada después de 10 intentos fallidos; dicha configuración se consignará en el perfil de FIM. El valor de esta llave será establecido por la CA del SINPE quien lo facilitará al fabricante; la entrega deberá hacerse siguiendo los controles apropiados para salvaguardar su confidencialidad.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Las tarjetas deben estar configuradas para que el número UID (Unique Permanent Identification) que tienen en su chip (establecido en el momento de su fabricación) sea asignado a la variable CP_CARD_GUID, agregando los ceros a la izquierda necesarios, de forma que se garantice que este número corresponda al desplegado por FIM como número de serie del dispositivo. Por ejemplo si el número de serie del chip es 0653000341246254, la variable CP_CARD_GUID debe ser actualizada con el valor 0000000000000000006530003412462 54, de forma que en FIM se despliegue el valor {00000000-0000-0000-0653-000341246254}. Este valor deberá garantizar la unicidad del número de serie del chip, por lo que se recomienda que esté formado por fecha de fabricación + número de serie + id del batch. Cada vez que se realice una compra el proveedor debe entregar, en conjunto con los dispositivos criptográficos, un archivo electrónico en formato XML que contenga los números de serie de todos y cada uno de los dispositivos de la compra. El formato del archivo en que se reciba la información deberá realizarse de conformidad con las especificaciones contenidas en el Estándar Electrónico – Firma Digital.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
La aplicación PKI debe ser capaz de firmar digitalmente solicitudes de certificado construidas con formato PKCS #10 y que se le envían a la CA del SINPE para la emisión de los certificados correspondientes. Lo anterior como señal de posesión de la llave privada por parte del solicitante.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	
Requisitos de Interoperabilidad y Neutralidad Tecnológica		
El sistema operativo del dispositivo criptográfico debe ser de plataforma abierta Java Card, que permita el funcionamiento de múltiples aplicaciones que se ejecuten a lo interno del chip. Las características del Sistema Operativo deben ser tales que permita que exista total independencia al desarrollar las diferentes aplicaciones.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
Tanto el sistema operativo como las aplicaciones implementadas en la tarjeta deben cumplir con las especificación de GlobalPlatform Card v 2.1.1 o superior incluida la especificación GlobalPlatform para el API de Java Card.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Para lograr la comunicación entre los computadores y la aplicación PKI de la tarjeta, el fabricante debe suministrar el middleware IDProtect, asociado a la aplicación PKI LASER para acceder la funcionalidad PKI dentro de la tarjeta. El middleware debe proveer las siguientes interfaces: Un CSP con soporte a CryptoAPI Un minidriver Una librería PKCS#11 Un driver Tokend para Mac	De conformidad con los puntos 6 y 7 de los Requisitos de Participación, se debe entregar el disco compacto que contenga las versiones más recientes del middleware con las interfaces para acceder los certificados y las llaves del dispositivo criptográfico solicitadas. Respecto a la certificación solicitada para el minidriver, en el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento denominado "Certificación Microsoft" cuyo contenido sea la certificación dada por Microsoft. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. El cumplimiento de este punto se verificará en la página "Windows Certified Products List" https://sysdev.microsoft.com/en-us/hardware/lpl/.	
El CSP debe operar en sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.		
El minidriver debe estar oficialmente certificado por Microsoft y debe cumplir con el "Windows Smart Card Minidriver Specification" con soporte a Base CSP y KSP para los sistemas operativos Windows oficialmente soportados por Microsoft como fabricante.		
La librería PKCS#11 debe ser provista para las plataformas Windows, Mac OS y Linux; en las versiones oficialmente soportadas por cada fabricante.		

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
El middleware debe permitir que los certificados digitales, las llaves y la funcionalidad de la aplicación PKI puedan ser accedidos en aplicaciones de usuario final que corren, como mínimo, en los navegadores nativos de las plataformas Windows (IE Explorer) y Mac OS (Safari) y en Mozilla Firefox y Google Chrome; en las versiones oficialmente soportadas por cada fabricante.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	
El fabricante debe garantizar que los certificados emitidos a través del minidriver sean utilizables también por medio de los otros drivers solicitados (PKCS#11 y Tokend). Es decir, que las tarjetas con certificados emitidos en un sistema operativo Microsoft a través del minidriver puedan ser utilizadas en otros sistemas operativos distintos a Microsoft.	Su cumplimiento se verificará en las pruebas de funcionamiento.	
El uso de cada contacto y las interfaces eléctricas en los dispositivos criptográficos debe cumplir las especificaciones de los estándares ISO/IEC 7816-3, ISO/IEC 7816-10 e ISO/IEC 7816-12, según los tipos de interfaces que el dispositivo provea y a la asignación de cada contacto conforme al Anexo A del estándar ISO/IEC 7816-2.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir un documento electrónico con la certificación emitida por un laboratorio autorizado, la cual evidencie que las tarjetas fueron sometidas a las pruebas respecto al estándar ISO/IEC 10373-3. De conformidad con lo requerido en	

Dispositivos criptográficos (Tarjetas inteligentes) – PKI sobre Tarjetas de Pago certificadas por EMV		
Requerimientos Técnicos	**Evidencia de Cumplimiento**	**Detalle de Cumplimiento**
Para permitir la interoperabilidad de los dispositivos criptográficos entre diferentes organizaciones, los elementos de datos del dispositivo deben cumplir con las especificaciones del estándar ISO 7816-6.	el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico.	
Los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-7 en el uso de los comandos para el lenguaje SCQL.		
Las funciones criptográficas implementadas en el chip de los dispositivos criptográficos deben cumplir con las especificaciones del estándar ISO/IEC 7816-15, de forma que se garantice la compatibilidad de las aplicaciones criptográficas con varios emisores de dispositivos.		
Las pruebas realizadas para demostrar que dispositivos criptográficos cumplen con las especificaciones del estándar ISO/IEC 7816 partes 6 y 15 deben haberse realizado en cumplimiento con los métodos de prueba estipulados en el estándar ISO/IEC 10373-3.		
Las tarjetas deben ser compatibles con lectores de tarjetas estándar, en cumplimiento de las especificaciones PC/SC y del ISO 7816 partes 1 a 3. Además, deben soportar como mínimo los protocolos de transmisión T=0 o T=1.	En el disco compacto solicitado en el punto e) de los Requisitos de Participación, se debe incluir la documentación electrónica que evidencie el cumplimiento de este punto. De conformidad con lo requerido en el punto b) de los Requisitos de Participación, en la copia de esta tabla se debe indicar el nombre de dicho documento electrónico. Adicionalmente, su cumplimiento se verificará en las pruebas de funcionamiento.	

Configuración de la plantilla del perfil del dispositivo criptográfico en FIM		
Parámetro	**Explicación**	**Valor**
Valor inicial de clave de administración	Es un valor hexadecimal que se utiliza para poder hacer labores de administración en los dispositivos criptográficos. Por ejemplo para realizar la inicialización del mismo antes de generar los certificados	El valor requerido para los dispositivos criptográficos de pruebas es: 303030303030303030303030303030303030303030303030303030
Diversificar clave de administración	Este valor indica que luego de inicializar el dispositivo criptográfico, el valor de la clave de administración se cambia por un valor aleatorio que nadie conoce, únicamente el FIM	Sí. El dispositivo criptográfico debe ser capaz de diversificar la clave de administración.
Tipo de proveedor de inicialización de del dispositivo	Define el tipo de proveedor que se utiliza para inicializar el dispositivo criptográfico. Por lo general se usa el proveedor predeterminado de FIM.	Predeterminado
Directiva de NIP de usuario	Determina como el FIM genera el PIN del dispositivo antes de que el mismo sea establecido por el usuario	Aleatorio El dispositivo criptográfico debe ser capaz de permitir que se establezca un PIN aleatorio
Juego de caracteres de NIP de usuario	Determina el juego de caracteres que se utilizará para establecer el PIN mencionado en el parámetro anterior	Numérico El dispositivo criptográfico debe ser capaz de aceptar un PIN con caracteres numéricos

A continuación se muestra un ejemplo de la configuración en FIM.

Configuración de tarjeta inteligente

En esta sección se muestra la configuración de tarjeta inteligente, incluida la información acerca del proveedor de tarjetas y los certificados

Nombre de proveedor:	Microsoft Smart Card Base CSP
Id. de proveedor:	MSBaseCSP
Inicializar tarjeta nueva antes del uso:	✓
Volver a usar tarjeta retirada:	✓
Usar inserción de clave segura:	✗
Instalar certificados de CA:	✗
Texto de etiqueta de certificado:	{Template!displayName}
Número máximo de certificados:	Sin límite
Diversificar clave de administración:	✓
Tipo de proveedor de inicialización de tarjeta:	Predeterminado
Datos del proveedor de inicialización de tarjeta:	
Valor inicial de clave de administración:	303030303030303030303030303030303030303030303030
Sustitución de NIP de administrador:	✗
Longitud de NIP de administrador:	No aplicable
Juego de caracteres de NIP de administrador:	No aplicable
Valor inicial de NIP de administrador:	No aplicable
Directiva de NIP de usuario:	Aleatorio
Juego de caracteres de NIP de usuario:	Numérico
Imprimir tarjeta:	✗

ACUERDO DE CONFIDENCIALIDAD

Este Acuerdo de Confidencialidad denominado de ahora en adelante "El Acuerdo", es realizado y efectivo desde el ___ de _____ del _____. Por este medio _____, documento de identidad número _____, en su calidad de _____ de la empresa _____ fabricante de las tarjetas inteligentes marca _____ y modelo _____ denominado de ahora en adelante **PARTICIPANTE DEL PROCESO DE HOMOLOGACIÓN**, se compromete a cumplir con las cláusulas establecidas en el presente acuerdo. De igual forma, quedan comprometidos los funcionarios de la empresa, involucrados en la generación de las tarjetas inteligentes que se someterán al proceso de homologación.

El objetivo del presente acuerdo es fijar los términos y condiciones bajo los cuales el fabricante mantendrá la confidencialidad de la información sensible. Lo anterior, en relación con la presentación de las tarjetas inteligentes, documentación y software para el proceso de Homologación de dichas tarjetas para el almacenamiento de certificados de firma digital de la Autoridad Certificadora del SINPE – Persona Física.

1. Información Sensible

Para los efectos del presente acuerdo se considera información sensible los valores que el fabricante asigne al conjunto de llaves que define Global Platform para proteger los comandos de administración de la tarjeta (también conocidas como “ISD Keys”, a saber las llaves MAC, ENC y DEK).

2. Obligaciones del fabricante

a) Generar la información sensible de manera exclusiva para la Autoridad Certificadora para personas físicas del Sistema Nacional de Pagos Electrónicos (SINPE) del Banco Central de Costa Rica (BCCR), conocida como CA SINPE – PERSONA FISICA.

b) Bajo ninguna circunstancia, la información sensible deberá ser concedida a un tercero, divulgada, duplicada o utilizada para otros fines que los descritos en este acuerdo, por el fabricante, excepto para configurar las tarjetas inteligentes que serán utilizadas en este proceso de homologación.

c) Si como producto de eventuales procesos de compra que pudieran realizar las entidades asociadas al SINPE que operen como Oficinas de Registro de la CA SINPE – PERSONA FISICA, el fabricante considera que utilizará la misma información sensible para configurar las tarjetas inteligentes que entregaría como resultado de esos procesos de compra, el fabricante se compromete a mantener la confidencialidad de la información sensible desde el momento de su generación y llegado el momento de la compra dar a conocer la información sensible únicamente al personal autorizado de la CA SINPE – PERSONA FISICA del BCCR, utilizando para ello los controles apropiados para salvaguardar su confidencialidad.

d) El fabricante se compromete a velar por el buen uso de toda la tecnología disponible para generar y acceder a dicha información.

e) El fabricante se responsabiliza de que sus colaboradores se sujeten a las limitaciones establecidas en este acuerdo.

f) El fabricante se compromete a destruir la información sensible de los medios tecnológicos o físicos en donde ésta haya sido almacenada, una vez que el fabricante tenga certeza de que no utilizará para ocasiones futuras dicha información.

g) El fabricante se compromete a notificar inmediatamente al BCCR, cuando por causas fuera de su control, tenga conocimiento que la información sensible esté siendo mal usada o haya sido divulgada y cooperará en forma razonable para ayudar a la CA SINPE – PERSONA FISICA a mitigar las consecuencias de este acto.

h) El fabricante garantiza que las tarjetas que está entregando a la CA SINPE – PERSONA FISICA, como parte de este proceso de homologación han sido configuradas con el valor "SECURED" en la variable correspondiente al "Estado del ciclo de vida de las tarjetas", de acuerdo al estándar Global Platform.

3. Plazo

Las obligaciones del fabricante en relación con este acuerdo permanecerán vigentes por diez años a partir de la fecha de firmado el presente acuerdo.

4. Otra Información

El fabricante no tendrá ninguna obligación bajo este acuerdo con respecto a cualquier otra información no considerada sensible de conformidad a lo estipulado en el punto uno que: (i) se convierta de conocimiento público sin que exista violación a este acuerdo por parte del fabricante; (ii) sea legítimamente comunicada o recibida por la CA SINPE – PERSONA FÍSICA sin obligaciones de confidencialidad; o (iii) sea desarrollada por el fabricante sin violación de este acuerdo; sin embargo, dicha información no podrá ser divulgada hasta treinta (30) días hábiles después de haber dado aviso por escrito al BCCR la intención de divulgación por parte del fabricante, junto con los argumentos que justifican realizar la divulgación, a menos que el acceso sea requerido por un proceso legal, en cuyo caso se deberá dar aviso lo más pronto posible por escrito al BCCR dicho requerimiento.

5. Ley Correspondiente

La ley que gobierna este acuerdo será interpretada con base en las leyes de Costa Rica. El fabricante irrevocablemente consiente exclusividad a la jurisdicción y las cortes situadas en la provincia de San José de Costa Rica para cualquier conflicto resultante de este acuerdo. El fabricante conviene que ante el acontecimiento de cualquier violación o amenaza de violación de este acuerdo, el BCCR puede obtener, además de cualquier otro arreglo o reparación legal que pueda estar disponible, una compensación necesaria que le permita protegerse contra cualquier violación o amenaza de violación.

6. Acuerdo Definitivo

Este acuerdo es en firme.

Este acuerdo se puede modificar solamente por otro documento escrito que haya sido debidamente redactado por el BCCR.

7. No Delegación

El fabricante no puede delegar este acuerdo o cualquiera de sus partes sin el consentimiento anteriormente expreso por escrito del BCCR.

8. Validez

Si cualquier término de este acuerdo es considerado por una corte de la jurisdicción competente como inválido o inaplicable, todos los términos restantes conservarán en forma completa su validez y efecto tal y como si tal término inválido o inaplicable nunca hubiera sido incluido.

9. Notificaciones

Cualquier aviso requerido por este acuerdo o relacionado con él, deberá hacerse por escrito, ya sea en forma personal o por correo certificado.

Notificaciones a Banco Central de Costa Rica deberán entregarse a:

Atención: Ing. Miguel Carballo Chavarría, Ejecutivo del Área de Seguridad Departamento de Seguridad y Arquitectura

Banco Central de Costa Rica

Avenidas Central y Primera, Calles 2 y 4, San José, Costa Rica

Tel. (506) 2243-3692 email carballocm@bccr.fi.cr

Notificaciones al fabricante deberán entregarse a:

Atención: _____

Dirección_____

_____

Tel. _____Fax. _____

Email: _____

10. Títulos

Los títulos usados en este acuerdo se proporcionan por conveniencia solamente y no deberán ser utilizados para interpretar el significado o la intención de este documento.

El **fabricante** firma en la fecha de emisión de este documento presentada al inicio del mismo.

Sr./Sra. _____,

Firma: _____,

Fecha: _____

7. Disposiciones transitorias

7.1. De los requerimientos condicionados

Cada OR debe cumplir con los requerimientos establecidos en el presente Estándar Físico; sin embargo para iniciar el servicio de Firma Digital sin mayores contratiempos, se podrá autorizar la entrada en operación de una OR sin el cumplimiento de los requisitos que se detallan a continuación siempre y cuando la OR se comprometa a implementarlos en un máximo de 6 meses después de ser dada de alta.

Los requerimientos sobre los cuales se permite la flexibilización expuesta en el párrafo anterior son:

- Cumplimiento de las facilidades de accesibilidad contempladas en la Ley 7600 “Igualdad de Oportunidades para las personas con Discapacidad” para el Trámite de Certificados Digitales y el Quiosco de activación de certificados digitales.
- Un mecanismo de anti - coacción.
- Prevención de incendios.
- Protección contra fallas en el fluido eléctrico.
- Iluminación de emergencia