POLÍTICA DE CERTIFICACIÓN NACIONAL

EAC (EXTENDED ACCESS CONTROL) PASAPORTE, DOCUMENTOS DE VIAJE Y PERMISO DE RESIDENCIA

POLÍTICA DE CERTIFICACIÓN NACIONAL

OID: 2.16.724.1.2.7.2.3.1.0

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

TABLA DE CONTENIDOS

1. INTRODUCCIÓN

El objetivo de la Política de Certificación Común es lograr la confianza y suficiente interoperabilidad entre las Autoridades de Certificación del País de Verificación (CVCA) y los Verificadores de Documentos (DV) de los distintos Estados Miembros para la realización del Control de Acceso Extendido EAC-PKI – Infraestructura de Clave Pública, basado en la guía técnica [BSI-EAC][1]. Asimismo, cada Estado Miembro DEBE designar un Coordinador PKI Nacional, que será responsable de los integrantes de la misma en su relación con los otros Estados Miembros.

La Política de Certificación (CP) Común se ajusta a lo establecido en las Decisiones de la Comisión relativas a las especificaciones técnicas sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros y en las especificaciones técnicas sobre normas para las medidas de seguridad y datos biométricos en los permisos de residencia para ciudadanos de terceros países.

La Política de Certificación Común hace referencia únicamente, al uso de certificados para controlar el acceso a los datos biométricos de las impresiones dactilares en los pasaportes, documentos de viaje y permisos de residencia electrónicos; lo que permite el Control de Acceso Extendido, a efectos de verificar la autenticidad del documento y la identidad del titular del mismo, cuando las leyes exijan la presentación del pasaporte, documento de viaje o permiso de residencia electrónico.

El alcance de la Política de Certificación Común es la emisión de certificados que permiten el acceso de lectura a los documentos de viaje de Estados miembros extranjeros conforme al Reglamento del Consejo (EC) 2252(2004)[2] y Reglamento del Consejo (EC) 1030/2002[3] en sus versiones modificadas.

La CP Común establece una serie de requisitos mínimos que cada SPOC, CVCA y DV de un Estado Miembro debe cumplir cuando actúa como suscriptor bajo la CVCA del Estado extranjero.

La CP Nacional está basada en la CP Común, detallada en la norma BSI TR-03139[4].

La CP Nacional cumple, como mínimo, las normas de la Política de Certificación Común, pero puede establecer más restricciones en cuanto al control y uso de certificados en el Estado Miembro. Por el contrario, los Estados Miembros no pueden exigir que los DV de otros Estados Miembros adopten restricciones superiores a las establecidas en la Política de Certificación Común como requisito previo para expedir un certificado a ese DV.

En la CP Nacional se contempla, además, la expedición de certificados por una CVCA a los DV nacionales.

La Dirección General de la Policía es un Prestador de Servicios de Confianza conforme al Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de Julio de 2014 (eIDAs) considerando las normas ETSI EN 319 401, ETSI EN 319 411-2.

En este sentido, tanto para las CVCA como para los DV, en aquellos aspectos que les sean de aplicación se podrá tener en cuenta la norma europea ETSI EN 319 401[5] como buena

1 Bundesamt für Sicherheit in der Informationstechnik: Technical Guideline TR-03110 'Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC)', Part 1 and Part 3

2 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:ES:PDF

3 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:157:0001:0007:ES:PDF

4 Bundesamt für Sicherheit in der Informationstechnik: Technical Guideline TR-03139 'Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Member'

5 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

práctica de seguridad y calidad en apoyo a la implementación de la Política de Certificación.

1.1 DEFINICIONES

Las palabras clave "DEBE", "NO DEBE", "REQUERIDO", "DEBERÁ", "NO DEBERÁ", "DEBERÍA", "NO DEBERÍA", "RECOMENDADO", "PUEDE", y "OPCIONAL" en este documento son para ser interpretadas como se describe en [RFC2119].

Un **Estado Miembro** es aquel que participa según la definición recogida en la Regulación (EC) Nº 2252(2004), en la Regulación (EC) 1030/2002 y así como en sus últimas versiones modificadas. Asimismo,

- Nacional (o doméstico) se define al mismo Estado Miembro.
- Extranjero se define a otro Estado Miembro o país asociado.

Una clave válida es aquella donde el tiempo actual se encuentra dentro del período de validez del correspondiente certificado de suscriptor y este certificado, a su vez, se considera válido.

Conforme a esta CP, se entenderá como **documento de viaje** al Pasaporte y al Permiso de Residencia electrónicos.

Una **suspensión** de una CVCA, de un DV o de un IS debe ser definido como sigue:

Hay dos estados de registro de una CVCA, de un DV o de un IS; por defecto, el estado se considera no suspendido.

- La suspensión del estado de registro de la CVCA se configura por su Autoridad de Registro; el DV o el IS serán suspendidos por la Autoridad de Registro nacional /extranjera.
- Los certificados emitidos o las solicitudes de certificados enviadas por una CVCA, un DV o un IS suspendidos NO DEBERÁN ser de confianza, ni procesados, ni reenviados[6].

Esto es así porque la suspensión o revocación de certificados no es posible dentro de la EAC-PKI debido a motivos técnicos.

Otras definiciones y acrónimos utilizados en la CP Común aparecen en el anexo A (Definiciones y Acrónimos).

1.2 VISIÓN GENERAL

La CP Común se rige dentro de la Infraestructura de Clave Pública descrita en [BSI-EAC].

Las reglas generales para la interacción de las CVCAs de los Estados Miembros dentro del alcance de la CP Común son:

- Cada Estado Miembro DEBERÁ designar un Coordinador de PKI Nacional, que será responsable de los integrantes de la misma en su relación con los otros Estados Miembros.
- Cuando actúa como suscriptor bajo la CVCA de un Estado Miembro extranjero, cada CVCA y cada DV DEBEN cumplir los requisitos de la CP común.
- Un Estado Miembro NO DEBE requerir a un Estado Miembro extranjero que adopte restricciones superiores a las de la CP Común, como pre-requisito para la emisión de un certificado a un DV del Estado Miembro extranjero.

[6] Excepto por razones de auditoría

- En la CP Nacional se PUEDEN contemplar, además de los requisitos mínimos de la CP Común, la expedición de certificados por una CVCA a los DV nacionales. Los requisitos de una CP Nacional de una CVCA, NO DEBERÁN entrar en conflicto con los requisitos de seguridad de la CP Común.
- Así, para el cumplimiento de los requisitos de la CP se requiere que sea implementada una infraestructura de comunicación robusta para las comunicaciones habituales entre países, cubriendo la emisión de certificados DV. El protocolo definido en [CSN 36 9791:2018], DEBERÁ utilizarse como habitual en el intercambio de datos indicados en EAC PKI.

1.3 NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Nombre del documento	Política de Certificación Nacional – EAC (Extended Access Control) Pasaporte, Documentos de viaje y Permiso de residencia
Versión del documento	1.0
Estado del documento	Aprobado
Fecha de emisión	21/09/2021
Fecha de caducidad	No aplicable
OID	2.16.724.1.2.7.2.3.1.0
Ubicación de la CP	http://pki.policia.es/cvca/publications

1.4 ENTIDADES Y PERSONAS INTERVINIENTES

En esta sección se proporciona una visión general del Coordinador de la PKI Nacional, las Autoridades de Certificación, las Autoridades de Registro, los suscriptores, los terceros de confianza (o partes de confianza) y los Puntos Únicos de Contacto (SPOC) de la (EAC-PKI).

	Autoridad de Certificación (CA)	**Autoridad de Registro (RA)**	**Suscriptor**	**Partes de Confianza**
Coordinador de PKI Nacional		X		
SPOC		X		X
CVCA	X	X		X
DV	X	X	X	X
IS			X	X
MRTD				X

1.4.1 Coordinador PKI Nacional

Es el responsable de interactuar con los Estados Miembros extranjeros para el intercambio de certificados DV y en todo lo relacionado con la CP Común. Asimismo, es el único punto de contacto, responsable de la distribución de los certificados emitidos para el Pasaporte,

para los Documentos de Viaje y para los Permisos de Residencia electrónicos a los Estados Miembros extranjeros.

El Coordinador PKI Nacional DEBERÁ asegurar que toda la información recibida de otro Estado Miembro será distribuida al SPOC, a la CVCA y al DV nacionales, cuando sea necesario para la seguridad y la funcionalidad de sus deberes.

1.4.2 Autoridades de Certificación

Autoridad de Certificación del País de Verificación

La Autoridad de Certificación Raíz (CA) de la EAC-PKI nacional se denomina Autoridad de Certificación del País de Verificación (CVCA).

Las claves públicas de una CVCA nacional están contenidas tanto en los Certificados CVCA autofirmados como en los certificados de enlace de la CVCA, siendo ambos denominados Certificados CVCA. La CVCA nacional establece los derechos de acceso a los datos sensibles almacenados en los chips de los MRTD nacionales de todos los DVs (nacionales y extranjeros), mediante la expedición de certificados DV que conceden atributos de control de acceso.

La CVCA nacional emite certificados a sus Titulares de Certificados (**Suscriptores**). En este documento, un suscriptor de una CVCA se denomina Verificador de Documentos (DV). Un DV es una unidad organizativa que gestiona Sistemas de Inspección (IS) conjuntos.

En la CP Nacional se da por hecho que la Autoridad de Registro (RA) forma parte de la CVCA y se utilizará únicamente el término CVCA.

Autoridad de Certificación del Verificador de Documentos

Cada DV DEBERÁ estar relacionado con una única CVCA nacional, que firma solicitudes de certificados de DV, bien a las CVCA nacionales o bien a las CVCA extranjeras.

A través de una CA, el DV emite certificados para sus Sistemas de Inspección (IS). Los certificados de los Sistemas de Inspección emitidos por los DV heredan los derechos de acceso y el periodo de validez del certificado DV emisor. El DV DEBERÍA restringir el período de validez de los certificados IS y PUEDE optar por restringir aún más los derechos de acceso.

1.4.3 Autoridades de Registro

Para facilitar la emisión de certificados entre los Estados Miembros e incrementar la seguridad, la mayor parte de las funciones de la Autoridad de Registro de una CVCA, firmando solicitudes de certificado de un DV, DEBERÁN transferirse a la Autoridad de Registro de la CVCA nacional de este DV. La comunicación, la interacción y el registro inicial con los Estados Miembros extranjeros DEBE ser realizado por el Coordinador Nacional de PKI.

Autoridad de Registro del País de Verificación (CVRA)

Por cada CVCA nacional hay únicamente una Autoridad de Registro (RA) que, normalmente, forma parte de la propia CVCA.

La CVRA nacional es responsable de:

- El registro de los DV nacionales y de la CVCA de los Estados Miembros extranjeros que estén autorizados a la lectura de los datos sensibles de los MRTDs nacionales;
- Proveer y cambiar, si fuese necesario, el estado de suspensión de la CVCA y de los DV registrados;
- Inventariar los DVs nacionales o extranjeros incluyendo su estado de suspensión;

- Identificar y autenticar las peticiones de certificados de los Verificadores de Documentos;
- Suspender los DVs nacionales si no están autorizados a solicitar certificados de Estados Miembros extranjeros;
- Suspensión del registro de Estados Miembros nacionales o extranjeros en caso de incidentes de seguridad;
- Proporcionar información a todos los Estados Miembros extranjeros si un DV nacional no está autorizado a solicitar certificados de los Estados Miembros y debe ser suspendido;
- Iniciar la emisión de certificados a los Verificadores de Documentos;

Autoridad de Registro del Verificador de Documentos (DVRA)

En cada Estado Miembro DEBERÁ operar una Autoridad de Registro por cada DV.

Las DVRA son responsables de:

- Registro de Sistemas de Inspección nacionales;
- Identificar y autenticar las solicitudes de certificación de los Sistemas de Inspección;
- Suspensión de Sistemas de Inspección nacionales si no están autorizados a la solicitud de certificados;
- Reenvío inmediato a la CVCA nacional de información sobre incidentes de seguridad del DV o del IS;
- Inicio de la emisión de certificados a los Sistemas de Inspección;

Según la CP Nacional, se entenderá que la DVRA forma parte del DV y se utilizará solamente el término DV.

1.4.4 Suscriptores

Los suscriptores con arreglo a esta política son los Verificadores de Documentos (DV) y los Sistemas de Inspección (IS).

A efectos de esta CP, se entiende por Sistema de Inspección la infraestructura, el hardware y el software necesarios para obtener certificados de los DV de los Estados Miembros; almacenar y administrar dichos certificados y obtener datos biométricos de impresiones dactilares de los MRTD que utilicen esos certificados, incluidos los mecanismos de control de acceso a los Sistemas de Inspección.

1.4.5 Partes de Confianza

Las partes de confianza de una EAC-PKI son la CVCA, el DV, el IS, el SPOC y los MRTDs.

Una parte de confianza es una entidad que verifica la firma de un certificado o una petición de certificado, utilizando una cadena de certificación de confianza.

1.4.6 SPOC – Comunicación entre participantes

Un SPOC actúa como un interface para la comunicación entre los Estados Miembros. Permite la comunicación online eficiente para llevar a cabo tareas relacionadas con la gestión de claves. Los detalles técnicos de SPOC se definen en [CSN 36 9791:2018], llamada CSN-SPOC.

Cada Estado Miembro DEBERÁ operar con un SPOC que DEBERÁ cumplir con los requisitos indicados en el Anexo C y en la norma CSN-SPOC. Lo que significa, que el SPOC de un

Estado Miembro es el interfaz de comunicación técnica hacia otros Estados Miembros para la emisión de certificados de Pasaporte o documentos de viaje y de Permiso de Residencia electrónicos.

Para la comunicación entre los Estados Miembros todas las CVCAs DEBEN ser capaces de llevar a cabo la misma utilizando el SPOC. Toda la gestión de claves DEBE ser llevada a cabo utilizando el SPOC.

Se DEBERÁ utilizar un canal de comunicación adicional, a través de correo electrónico, en el caso de que el canal de comunicación del SPOC no se encuentre disponible. La dirección de correo electrónico utilizada en este contexto forma parte del registro del Estado Miembro. Esto significa que los Estados pueden utilizar la comunicación por correo electrónico para intercambiar manualmente solicitudes/certificados, incluso si el sistema SPOC automático de uno o ambos Estados aún no se ha implementado o está fuera de servicio.

En el caso de interrupción del canal de comunicación habitual, el Estado Miembro DEBE notificar que las peticiones de certificados DEBERÍAN ser enviadas por el canal alternativo. Esto DEBERÁ realizarse en una franja de tiempo que minimice el riesgo de la expiración del certificado. Cuando la comunicación a través del SPOC sea posible de nuevo, DEBERÁ comunicarse a todos los SPOCs de los Estados Miembros registrados, a través de un General Message (GM).

Tanto el SPOC como la comunicación por correo electrónico sólo DEBERÁ ser utilizada una vez que se hayan realizado con éxito el intercambio diplomático de la información de registro.

1.4.7 Uso de los Certificados

Los certificados del IS se utilizan para habilitar acceso de lectura a las impresiones biométricas almacenadas en el MRTDs según se indica en el Reglamento Nº 2252/2004.

Para cada Estado Miembro de la CVCA, los pares de claves y certificados se utilizan con el siguiente propósito:

- La clave privada del CVCA DEBERÁ ser utilizada para firmar certificados de CVCA, certificados de enlace, certificados DV nacionales y extranjeros y las peticiones de certificados DV que se proporcionen a la CVCA de Estados Miembros autorizados extranjeros.
- Los certificados CVCA SERÁN utilizados para verificar firmas de certificados de DV de Estados Miembros nacionales o extranjeros, Certificados de Enlace emitidos por la CVCA y peticiones de DV firmadas por la CVCA.
- Las claves privadas del DV SERÁN utilizados para firmar certificados IS nacionales y peticiones DV sucesivas.
- Los certificados DV SERÁN utilizados para verificar firmas de certificados IS emitidos por el DV.

Nota: cada DV e IS tienen diversos pares de claves (y certificados) en uso a la misma vez, necesitando un par de claves por cada Estado Miembro (incluyendo uno nacional propio) que ha emitido el MRTD. Una CVCA tiene sólo un par de claves en uso a la misma vez, excluyendo el corto intervalo necesario para firmar el Certificado de Enlace de la CVCA.

La ruta de certificación de confianza para el MRTD nacional que es leída por un IS de un Estado Miembro extranjero autorizado, está formado por lo siguiente:

- Certificado IS del Estado Miembro extranjero autorizado,
- Correspondiente certificado de DV del Estado Miembro extranjero autorizado, firmado por el certificado CVCA nacional correspondiente al MRTD y

- Cero o más Certificados de Enlace CVCA nacionales, completando una cadena de certificación de la clave pública CVCA nacional almacenada en MRTD.

Los certificados y rutas de certificados serán validados e interpretados por las partes de confianza conforme a [ISO 7816-4] y [BSI-EAC].

1.4.8 La Dirección General de la Policía como Órgano responsable del Pasaporte, Documento de Viaje y Permiso de Residencia

Nombre	Dirección General de la Policía (Ministerio del Interior) Subdirección General de Logística e Innovación Unidad de Informática y Comunicaciones Área de Informática		
Dirección e-mail	mrtd-spain@policia.es		
Dirección	Ctra Guadarrama - El Escorial Km 5,500		
Teléfono	+34 918968464	**Fax**	+34 918902018

2. Repositorios y Publicación de Información

La Comisión Europea es responsable de mantener una lista de datos de contactos de los Coordinadores de PKI Nacionales a nivel europeo. El contenido y la integridad de esta lista se protegerán por medios diplomáticos. La información correspondiente está disponible en Internet, en la Dirección General de Justicia, Libertad y Seguridad (DG-HOME) de la Comisión Europea.

2.1 Repositorios

En cada **CVCA** se DEBE tener un repositorio que contenga los certificados y las solicitudes firmadas por la CVCA (certificados CVCA, certificados de enlace, certificados de DV y peticiones de DV), así como datos de registro de DV nacionales y extranjeros y listas de estado de suspensión de DV extranjeras. Los certificados SERÁN almacenados en el repositorio, al menos, el tiempo de validez de dicho certificado más el tiempo de validez del MRTD. El certificado puede ser utilizado por un período superior a seis meses.

Nota: cada CVCA DEBERÁ tener acceso completo y control sobre su repositorio; si dos CVCA operan en la misma localización PODRÁN utilizar el mismo repositorio físico.

Cada **DV** DEBE tener un repositorio que contenga los certificados y las peticiones firmadas por el DV (certificados DV, solicitudes DV y certificados IS), así como los datos de registro del IS. Los certificados en los repositorios de DV DEBERÁN ser almacenados, al menos, el período de validez de dicho certificado más un año.

3. Identificación y Registro

3.1 Nombres

Según lo definido en la [BSI-EAC], la Referencia de la Autoridad de Certificación (CAR) se utiliza para identificar la clave pública que debe utilizarse para verificar la firma de la Autoridad de Certificación (CVCA o DV).

El CAR DEBE ser igual a la Referencia del Titular del Certificado (CHR) en el correspondiente certificado de la autoridad de certificación.

El CHR DEBERÁ identificar una clave pública del titular del certificado. DEBE tratarse de un identificador único en relación con la Autoridad de Certificación emisora. DEBERÁ basarse en los siguientes elementos concatenados:

1. El código [ISO 3166-1] ALPHA-2 del país del titular del certificado;
2. Un código mnemónico [ISO/IEC 8859-1] que represente al titular del certificado con una longitud de hasta 9 caracteres;
3. Un número de secuencia [ISO/IEC 8859-1] numérico o alfanumérico consistente en 5 caracteres. El número de secuencia PUEDE reiniciarse si se agotan todos los números de secuencia disponibles.

Se RECOMIENDA comenzar el número de secuencia con el código [ISO 3166-1] ALPHA-2 del país de la Autoridad certificadora. Si se sigue esta recomendación, los tres caracteres restantes DEBERÁN ser asignados como un número de secuencia alfanumérica.

Nota: en general, no está garantizado que la Referencia del Titular del Certificado (CHR) sea un identificador único. No hay problema, si dos DVs de diferentes Estados Miembros tienen el mismo Titular Mnemónico en el CHR de las solicitudes de DV y Certificados siempre que también contengan el código de país del DV del Estado nacional. Si el Estado Miembro extranjero tiene más de un CVCA, las solicitudes y certificados siguen siendo únicos debido al CAR interno.

La identidad de la Autoridad de Certificación y los titulares de certificados (suscriptores) DEBERÁN definirse como sigue:

– Certificado CVCA:

- Referencia de la Autoridad de Certificación (CAR): identidad CVCA nacional;
- Referencia del Titular del Certificado (CHR): identidad CVCA nacional;

– Certificado DV:

- Referencia de la Autoridad de Certificación (CAR): identidad CVCA nacional u otra identidad CVCA de un Estado Miembro autorizado extranjero;
- Referencia del Titular del Certificado (CHR): identidad DV nacional[7];

– Certificado IS:

- Referencia de la Autoridad de Certificación (CAR): identidad DV nacional;
- Referencia del Titular del Certificado (CHR): identidad IS nacional.

3.2 REGISTRO

3.2.1 Validación de identidad inicial de la CVCA nacional

Cada Estado Miembro DEBERÁ identificar claramente quien es el responsable de la autenticación y definición de la identidad de cada CVCA y el Coordinador de PKI Nacional.

[7] El nemotécnico Titular del DV siempre está definido por su CVCA o el propio DV

3.2.2 Registro de un Estado Miembro extranjero

El Registro del Estado Miembro DEBERÁ llevarse a cabo bajo la supervisión de la Comisión Europea. El registro de una CVCA de un Estado Miembro consta de dos pasos:

Paso 1 – **Envío del registro a través de la Comisión Europea**

Un Coordinador de la PKI Nacional del Estado Miembro DEBERÁ enviar el formulario de registro firmado oficialmente y completado (Anexo D Formulario de Registro) a la Comisión Europea, para su distribución a otros Estados Miembros por medios diplomáticos asegurando la autenticidad e integridad de la información. Esta parte de registro PUEDE ser también realizada de forma bilateral entre Estados Miembros, pero la Comisión Europea DEBERÍA ser informada sobre el registro.

Paso 2 – **Implementación de la información de registro en la CVCA nacional**

La información de registro DEBE ser distribuida al Coordinador de la PKI Nacional de los Estados Miembros, a su CVCA y a su SPOC, para asegurar la autenticidad e integridad de los datos.

Al recibir los datos de registro, el Coordinador de la PKI Nacional de un Estado Miembro, a través de la CVCA y del SPOC, DEBE verificar si la integridad de la información no ha sido comprometida.

Particularmente crítico, es que los datos del certificado digital de la CVCA del Estado Miembro y del certificado raíz SPOC, DEBEN ser cotejados con las huellas criptográficas que figuran en el formulario de registro.

Sólo si estas comprobaciones resultan ser positivas, los datos de registro DEBERÁN ser implementados en la CVCA y por lo tanto, el registro DEBERÁ ser completado; solicitando nuevos certificados CVCA desde el Estado Miembro registrado a través del SPOC ("GetCACertificates" según la CSN-SPOC).

En el caso de un cambio en cualquiera de los datos de la información de los registros anteriores, el Coordinador de PKI Nacional DEBERÁ enviar una nueva versión actualizada a la Comisión Europea para su distribución a los otros Estados Miembros participantes. Antes de llevar a cabo la actualización, la Autoridad de Registro DEBE verificar si la integridad de la información no ha sido comprometida.

El Coordinador de PKI Nacional del Estado Miembro que haya solicitado el registro DEBERÁ ser informado si el registro ha sido aceptado o rechazado (incluyendo el motivo) en las siguientes cuatro semanas a la recepción de la solicitud por parte del Estado Miembro. El mensaje DEBERÍA ser enviado por los Coordinadores de PKI Nacionales de los Estados Miembros.

3.2.3 Registro de un DV

El registro inicial de un DV se realiza por la RA de la CVCA nacional de ese mismo DV. En el proceso de registro DEBERÁ efectuarse una comprobación adecuada de la identidad del DV, la autenticidad de los datos de registro (incluyendo solicitudes de certificados iniciales), la CP del DV (basada en la CP Común) y, si fuese de aplicación, la parte pública de la declaración de prácticas de certificación y los permisos que el DV DEBERÁ tener para solicitar los certificados.

Sólo si todos estos datos son correctos, la CVCA nacional DEBERÁ registrar el DV y firmar las peticiones iniciales de DV a las CVCAs nacionales o a las CVCAs de un Estado Miembro extranjero.

El registro de un DV en una CVCA de un Estado Miembro extranjero se realiza en base a los datos de Referencia del Titular (CHR) del certificado del DV y se completa al aceptar la solicitud inicial del DV firmada por un certificado de CVCA conocido y válido de su CVCA nacional. El CHR de un DV DEBERÁ ser definido por la CVCA del DV o por el propio DV.

A partir de entonces, en la CVCA del Estado Miembro DEBERÁ aparecer el DV como válido y no suspendido hasta que se produzca la notificación de un incidente relacionado con el cumplimiento de los requisitos de seguridad conforme a la CP o hasta que la caducidad del DV sea conocida.

3.2.4 Registro de un IS

El DV DEBERÁ disponer de un mecanismo adecuado para identificar un Sistema de Inspección autenticado. La generación de clave de un Sistema de Inspección DEBERÁ ser procesada bajo la consideración del capítulo 4.4.3 (Certificados emitidos por el DV al IS), del capítulo 5 (Requerimientos de seguridad) y del capítulo 6 (Seguridad del par de claves). La solicitud inicial de un IS DEBE ser transmitida al DV de forma segura. El DV DEBE verificar si la integridad y la autenticidad de los datos de la solicitud no están comprometidas.

4. Requisitos Operacionales para el Ciclo de Vida de los Certificados

4.1 Perfil de Certificados

Los certificados CVCA, los certificados de enlace, los certificados de DV y los certificados IS DEBERÁN ser generados conforme al perfil del certificado especificado en la [BSI-EAC] "CV Certificates".

4.2 Certificados Iniciales y Peticiones

Un certificado inicial de un DV o de un IS se define como:

- El primer certificado del titular o
- El primer certificado después de que una suspensión haya sido cancelada o
- Un nuevo certificado después de que el certificado previo haya caducado antes de que una nueva solicitud o certificado de enlace pueda ser generado.

Un certificado inicial de un DV o de un IS DEBERÁ ser emitido basado en la petición inicial del DV o de un IS conforme a la [BSI-EAC].

Los certificados NO DEBEN ser emitidos sin generar un nuevo par de claves del correspondiente certificado.

4.3 Certificados Sucesivos y Peticiones (Renovación)

Un certificado sucesivo es todo certificado del titular (suscriptor) excepto el inicial.

Un certificado sucesivo DEBERÁ ser sólo emitido conforme a las siguientes reglas:

a) El titular del certificado genera un nuevo par de claves.
b) El certificado contiene un número de secuencia sucesivo diferente en el CHR que el de los certificados anteriores del Titular del Certificado.
c) El certificado se emite conforme al capítulo 4.4 "Solicitud del Certificado y Emisión".

d) Si la clave privada se ve comprometida por un incidente de seguridad, la causa del incidente, DEBE ser detectada y el problema de seguridad correspondiente DEBE ser resuelto antes de que pueda emitirse un nuevo certificado inicial (ver capítulo 4.2 "Certificados Iniciales y Peticiones").

Un certificado sucesivo de un DV o de un IS DEBERÁ emitirse cuando se cumpla una de las siguientes condiciones:

a) El certificado de DV o de IS está a punto de caducar, en este caso se DEBE seguir el capítulo "Peticiones de Certificado" de [BSI-EAC].
b) Cuando un certificado requiere una modificación debido a cambios en los atributos en el DV/IS.

Los certificados NO DEBEN ser emitidos sin generar un nuevo par de claves del correspondiente certificado.

4.4 SOLICITUD DE CERTIFICADOS Y EMISIÓN

Las Autoridades de Certificación (CVCA y DV) DEBERÁN adoptar las medidas oportunas contra la falsificación de certificados y asegurarán que el procedimiento de emisión de certificados se encuentra vinculado de forma segura al del registro.

4.4.1 Certificados emitidos de una CVCA a otra CVCA

Cada Estado Miembro DEBERÁ definir qué entidad es responsable de autorizar la creación de una CVCA.

Una CVCA DEBERÁ emitir un certificado autofirmado CVCA o un certificado de enlace CVCA a un certificado CVCA anterior de la misma CVCA[8]. Esto será realizado durante la ceremonia de claves, la cual debe cumplir, al menos, los requisitos de seguridad del capítulo 5 (Requisitos de seguridad) y del capítulo 6 (Seguridad del par de claves) de la CP Común. Una CVCA debe comprobar que la petición de certificados está autorizada y es válida.

Cuando la validez de un certificado CVCA está próxima a su fin, la CVCA DEBERÁ generar un nuevo par de claves y emitir un certificado autofirmado CVCA y un certificado[9] de enlace.

El certificado de enlace DEBERÁ contener según la [BSI-EAC]:

- La clave pública del nuevo par de claves,
- La firma generada con la clave privada del certificado CVCA anterior,
- El mismo periodo de validez del nuevo certificado CVCA que contiene la misma clave pública.

El certificado de CVCA y el certificado de enlace DEBERÁN ser distribuidos automáticamente a todos los Estados Miembros extranjeros registrados en la CVCA vía "Send Certificates" conforme a CSN-SPOC.

La CVCA o el SPOC que reciban un nuevo certificado CVCA y su correspondiente certificado de enlace DEBERÁN comprobar la validez y autenticidad del certificado:

[8] o un nuevo CVCA que sustituya a un CVCA finalizado conforme al capítulo 5.4 "Finalización CVCA o DV"

[9] El certificado CVCA de enlace será emitido como parte de la cadena de confianza para la lectura del MRTD y probar la autenticidad del nuevo certificado CVCA y el certificado autofirmado CVCA es utilizado para probar la posesión y fiabilidad operativa de la clave privada correspondiente

- Si el certificado es correcto de acuerdo con la sintaxis, autenticidad y validez, la CVCA receptora DEBERÁ actualizar la información de registro de la CVCA emisora, estableciendo una nueva confianza con el nuevo certificado CVCA y con el certificado de enlace.
- Si el certificado no es correcto el Estado Miembro receptor DEBERÁ informar al Estado emisor de la CVCA y del certificado de enlace. Esto se PUEDE realizar mediante respuesta automática "Send Certificates" conforme a CSN-SPOC.

4.4.2 Certificados emitidos por una CVCA a un DV

Una vez efectuado el registro satisfactoriamente, como se indica en el capítulo 3.2.3 (Registro de un DV), la solicitud de certificado de DV DEBERÁ ser llevada a cabo conforme a la [BSI-EAC] (capítulo "Solicitud de Certificados" y "Verificadores de Documentos").

La solicitud de certificado DV DEBERÁ siempre contener el CAR (esto sólo se recomienda en la [BSI-EAC]) para distinguir entre las diferentes CVCAs, en el caso de que hubiese más de una en el Estado Miembro que recibe la petición de certificado. De lo contrario, es posible que los Estados Miembros no puedan identificar la CVCA responsable de firmar el certificado DV correspondiente. Todas las peticiones de DV DEBEN contener una firma externa según la siguiente tabla para garantizar la integridad y autenticidad de la petición.

4.4.2.1 Solicitud de Certificados

Los siguientes pasos DEBEN ser procesados si un certificado DEBE ser emitido por una CVCA de un Estado Miembro extranjero a un DV nacional:

Paso Número	Indicación	Petición Inicial	Petición sucesiva[10]	Parte involucrada
1	Generar par de claves	El DV genera un par de claves conforme a la [BSI-EAC] y teniendo en cuenta los requisitos de seguridad de los capítulos 5 y 6 de la CP.		DV
2	Generar Petición de certificado	El DV genera una petición de certificado a partir de la nueva clave pública, nombrada según el capítulo 3.1 y la [BSI-EAC] y genera la firma interna con la correspondiente clave privada.		DV
3	Generar firma externa (petición sucesiva)		La petición DEBE ser firmada con la clave privada del certificado DV válido emitido por el mismo Estado Miembro al que	DV

[10] Petición inicial/sucesiva relativa a la CVCA del Estado Miembro que firma el certificado DV.

			se le enviará la petición.[11]	
4	Enviar petición a una CVCA / SPOC	La petición DEBE ser enviada a la CVCA nacional[12] del DV de forma segura.	La solicitud firmada DEBE ser enviada a través del SPOC.	DV
5	Comprobar estado suspensión (nacional)	La CVCA o el SPOC nacional DEBE comprobar si el DV está autorizado a solicitar certificados de Estados Miembros extranjeros (por ejemplo, no está suspendido antes de procesar la petición. Una solicitud de un DV suspendido DEBE ser rechazada).		CVCA / SPOC nacional
6	Comprobar integridad	La CVCA DEBE comprobar si la autenticidad e integridad de la petición del DV es correcta, sino la petición es rechazada.	Se RECOMIENDA comprobar la autenticidad e integridad de la petición dentro de la CVCA / SPOC de forma automática.	CVCA / SPOC nacional
7	Generar firma externa (petición inicial)	Se añade una firma externa a la petición por parte de la CVCA nacional. Entonces se envía la solicitud al SPOC nacional.		CVCA nacional
8	Enviar petición a SPOC extranjero	La petición DEBERÁ ser enviada al SPOC extranjero siguiendo los requisitos de la CSN-SPOC.		SPOC nacional
9	Comprobar firma externa	SPOC / CVCA extranjero DEBE comprobar si la firma externa de la petición está creada por la clave válida, relacionada con:		CVCA/ SPOC extranjero
		El Certificado raíz válido de la CVCA nacional del DV.	El Certificado válido del DV emitido por la CVCA de un Estado Miembro extranjero.	

[11] Si una clave privada de una CVCA, DV o IS es inutilizable por motivos no críticos, como por ejemplo retraso en la petición sucesiva, una nueva petición inicial será generada

[12] nacional/extranjero significa, en el contexto de esta tabla, el mismo/otro Estado Miembro que el DV

10	Comprobar estado suspensión (extranjero)	La CVCA del Estado Miembro extranjero DEBE comprobar si DV está autorizado a enviar certificados, en relación con la información proporcionada por el DV de la CVCA nacional o si el Estado Miembro extranjero ha suspendido el DV, por ejemplo, comprobando el estado de registro del DV.	CVCA / SPOC extranjero
11	¿Emitir certificado?	Si ambas comprobaciones son positivas la CVCA extranjera DEBE generar el certificado correspondiente a la petición recibida. De otra forma, la petición DEBE ser rechazada.	CVCA extranjero
12	Enviar respuesta	El SPOC del Estado Miembro extranjero envía mensaje de respuesta, conteniendo el certificado DV o su rechazo, al SPOC nacional.	SPOC extranjero
13	Comprobar certificado	El SPOC nacional comprueba la sintaxis del certificado por medios automáticos y envía el resultado de la comprobación como respuesta al SPOC extranjero.	SPOC nacional
14	Reenviar respuesta	El SPOC nacional del DV reenvía la respuesta de la CVCA del Estado Miembro al DV.	SPOC nacional
15	Incorporar certificado	DV incorpora el certificado.	DV

En el supuesto, de que una CVCA nacional emita un certificado a un DV nacional se deben seguir los siguientes pasos:

Número de paso	Indicación	Petición inicial	Petición sucesiva	Parte involucrada
1	Generar par de claves	El DV genera un par de claves conforme a la [BSI-EAC] y teniendo en cuenta los requisitos de seguridad de los capítulos 5 y 6 de la CP.		DV nacional
2	Generar Petición de certificados	El DV genera una petición de certificado a partir de la nueva clave pública, nombrada según el capítulo 3.1 y la [BSI-EAC] y genera la firma interna con la correspondiente clave privada.		DV nacional

3	Generar solicitud	La petición debe ser generada por parte del DV nacional.	La petición debe ser firmada con la clave privada del certificado de DV válido.	DV nacional
4	Enviar petición a la CVCA	La petición DEBE ser enviada a la CVCA nacional del DV de forma segura.	La petición firmada DEBE ser enviada a la CVCA nacional.	DV nacional
5	Comprobar estado suspensión (nacional)	La CVCA nacional DEBE comprobar si el DV está autorizado a solicitar certificados (por ejemplo, no está suspendido antes de procesar la petición. Una solicitud de un DV suspendido DEBE ser rechazada).		CVCA nacional
6	Comprobar integridad	La CVCA DEBE comprobar si la autenticidad e integridad de la petición del DV es correcta, si no la petición será rechazada.	Se RECOMIENDA comprobar la autenticidad e integridad de la petición dentro de la CVCA de forma automática.	CVCA nacional
7	¿Emitir certificado?	Si ambas comprobaciones son positivas, la CVCA DEBE generar el certificado correspondiente a la petición recibida. En caso contrario, la petición DEBE ser rechazada.		CVCA nacional
8	Enviar respuesta	La CVCA envía mensaje de respuesta, conteniendo el DV o su rechazo.		CVCA nacional
9	Incorporar certificado	El DV incorpora el certificado.		DV nacional

4.4.2.2 Periodo de solicitud y tiempo de respuesta

La CVCA DEBE procesar la petición de certificado en el transcurso de 7 días.

Si el sistema de la CVCA no está operativo por un período superior al anteriormente mencionado, se DEBE informar a todos los DV nacionales y a las CVCAs de los Estados Miembros extranjeros si esa pérdida del servicio fuese planificada antes de 7 días o tan pronto como sea posible, en el caso de una pérdida imprevista del mismo.

La generación de un nuevo certificado DV DEBERÍA ser programada, al menos con 11 días de antelación; se DEBERÍA ampliar con 3 días adicionales en el caso de caída del servicio, lo que se comunicaría por correo electrónico.

Este período de tiempo ha sido calculado de la siguiente forma:

- Ceremonia de claves y evaluación de calidad interna (1/2 día)
- Generación de la petición de certificado (1/2 día)
- Envío de la petición a la autoridad firmante vía SPOC nacional (1 día)
- Tiempo de respuesta de la autoridad firmante (7 días)
- Obtención del certificado a través del SPOC nacional (1 día)
- Importación del certificado (1 día)

Si el tipo de instalación de una infraestructura de DV requiere una gran cantidad de tiempo para uno de los pasos anteriores, el DV DEBERÍA incrementar el rango de tiempo para generar una nueva petición de certificado DV de forma acorde.

4.4.3 Certificados emitidos de un DV a un IS

Los ISs PUEDEN enviar peticiones de certificados tras la finalización del registro con éxito, como se indica en el punto 3.2.4 arriba mencionado.

Un DV sólo DEBERÁ emitir un certificado a un IS, si cumple con la CP y si utiliza los certificados conforme al capítulo 4.6 (Uso de Certificados) del documento.

Número Paso	Indicación	Petición Inicial	Petición sucesiva[13]	Parte involucrada
1	Generar par de claves	El IS genera un par de claves conforme a la [BSI-EAC] y en consideración a los requisitos de seguridad de los capítulos 5 y 6.		IS
2	Generar Petición de certificados	El IS genera una petición de certificado a partir de la nueva clave pública, nombrada según el capítulo 3.1 y la [BSI-EAC] y genera la firma interna con la correspondiente clave privada.		IS
3	Generar firma externa (petición sucesiva)		La petición DEBERÍA contener una firma exterior generada con la clave privada	IS

[13] Petición inicial/sucesiva relativa a la CVCA del Estado Miembro que firma el certificado DV

			correspondiente al certificado IS todavía válido. Si no se utiliza este mecanismo, DEBE utilizarse otro mecanismo de seguridad equivalente.	
4	Enviar petición	La petición DEBERÁ ser enviada al DV de forma que se garantice que cualquier compromiso de su integridad y su autenticidad sea detectado. Por ejemplo, mediante la presentación de una huella digital criptográfica de la petición a través de un canal distinto.	La petición DEBE ser enviada al DV.	IS
5	Comprobar petición	El DV DEBE comprobar si la autenticidad e integridad de la petición de IS no está comprometida y que la petición cumple los requisitos conforme a la [BSI-EAC] y al capítulo 3.1 de la CP.	El DV DEBE comprobar si la firma externa es correcta y está generada con la clave privada del certificado IS válido y que cumple los requisitos conforme a la [BSI-EAC] y al capítulo 3.1 de la CP.	DV
6	Comprobar estado registro	El DV DEBE comprobar si el IS está autorizado a solicitar certificados, por ejemplo, si el registro del IS no está suspendido.		DV
7	¿Emitir certificado?	El DV PUEDE emitir un certificado correspondiente a la petición si ambas comprobaciones anteriores son positivas. De otra forma, la petición del IS debe ser rechazada.		DV

8	Enviar respuesta	El DV DEBE enviar mensaje de respuesta al IS, conteniendo el certificado IS o su rechazo.	DV
9	Incorporar el certificado	El IS incorpora el certificado.	IS

4.5 ACEPTACIÓN DE CERTIFICADOS

Al final de la ceremonia de claves, los certificados autofirmados CVCA DEBEN ser aceptados por la entidad responsable de la CVCA.

En un DV o IS se considerará que ha aceptado un certificado cuando haya sido recibido.

4.6 USO DE CERTIFICADOS

La CVCA, el DV y el IS deberán cumplir requisitos según proceda:

- Asegurarse de que se presente a la CVCA/DV información exacta y completa de conformidad con los requisitos de la Política de Certificación Nacional, particularmente con relación al registro;
- El par de claves solamente se utilizará de conformidad con las limitaciones impuestas por esta Política de Certificación Nacional;
- Asegurarse que no se utiliza la clave privada sin autorización;
- Las claves se generarán de conformidad con la guía técnica BSI-EAC;
- Sólo se utilizarán las claves privadas para firmar o descifrar en un dispositivo criptográfico seguro según lo descrito en el capítulo 6.2;
- Se notificarán a la CVCA/DV, en un plazo razonable, las situaciones siguientes hasta el fin del periodo de validez indicado en el certificado:
    - La pérdida, robo o peligro potencial de una clave privada; o
    - La pérdida de control sobre la clave privada debido a la sospecha de riesgo con respecto a los datos de activación (por ejemplo, código PIN) u otras razones; y/o
    - La inexactitud o cambios en el contenido del certificado, según lo notificado al suscriptor o al interesado.
- En caso de sospecha de riesgo, se interrumpirá inmediata y permanentemente el uso de una clave privada.
- En caso de que se informe de riesgo que corre una clave privada de una CVCA o DV, las CVCA, los DV y los IS no deberán otorgar fiabilidad a los certificados firmados mediante estas claves privadas y deberán actuar debidamente.

El uso de certificados y pares de claves será el que indique el emisor del certificado (CVCA o DV) en la casilla <<autorización del titular del certificado>> del certificado.

Los DV e IS solamente deberán utilizar la clave privada correspondiente al certificado DV e IS recibido para los fines siguientes:

- El descrito en el capítulo 1.4.7 <<Uso de los certificados>> de esta Política de Certificación Nacional;
- De conformidad con el contenido de los certificados expedidos.

4.7 PERIODO DE VALIDEZ DE CERTIFICADOS

Los períodos de validez de los certificados están definidos en la siguiente tabla:

Entidad	Mínimo periodo de validez	Máximo periodo de validez
Certificado CVCA (enlace y autofirmado)	6 meses	3 años
Certificado DV	2 semanas	3 meses
Certificado IS	1 día	1 mes

5. REQUISITOS DE SEGURIDAD

5.1 CONTROLES FÍSICOS

Cada CVCA y cada DV DEBERÁN asegurar que sus servicios operan en un entorno seguro. Esto DEBERÁ incluir:

- Localización y construcción: la CVCA y el DV están situados en un área protegida físicamente.
- Acceso físico: el acceso a la CVCA y al DV estarán controlados y auditados. Sólo personas autorizadas tienen acceso físico al entorno de la CVCA y el DV.
- Almacenamiento de los medios: se encuentran protegidos contra el uso no autorizado o accidental, acceso, divulgación o daño de personas y otras amenazas (por ejemplo, fuego, agua).
- Eliminación de residuos: se implementarán los procedimientos para la eliminación de residuos con el fin de evitar el uso no autorizado, el acceso o la divulgación de datos sensibles.
- Backup Off-site: se PUEDE instalar un backup off-site de datos críticos.

5.2 CONTROLES DE PROCEDIMIENTO Y GESTIÓN DE ACCESO AL SISTEMA

Cada CVCA y cada DV DEBERÁN implementar medidas de seguridad que protejan la autenticidad, integridad y confidencialidad de sus datos y el correcto funcionamiento de sus sistemas IT. Se DEBERÁ definir un Concepto de Seguridad por cada CVCA y por cada DV que:

- Describa cualquier sistema IT que sea parte de la Autoridad de Certificación, Autoridad de Registro o SPOC, estando directamente conectado a uno de estos o maneje los datos para el proceso de certificación o registro;
- Describa cualquier proceso que forme parte de las tareas de la CVCA, del DV o del SPOC;
- Describa los roles necesarios (ver abajo);
- Describa las medidas de seguridad y la gestión de las incidencias.

Los siguientes puntos DEBERÁN referirse al Concepto de Seguridad de una CVCA y de un DV:

- **Protección de los sistemas IT**: se DEBERÁN implementar mecanismos de seguridad IT (por ejemplo, firewalls) para proteger los dominios de red internos de los dominios de red externos, accesibles por terceros. Se DEBERÁN implementar las medidas de seguridad adecuadas a cada interfaz de los sistemas IT.

- **Roles de confianza**: los procesos de tareas del SPOC, de la CA y de la RA DEBERÁN tener asignados al menos los siguientes roles de confianza: administrador de sistemas, auditor, operador de RA y operador de CA. Esto se realizará mediante medidas organizativas y controles IT y DEBERÁN incluir la administración de cuentas de usuario, la auditoría y la modificación puntual o eliminación de los accesos.
- **Separación de roles de confianza**: los sistemas IT DEBERÁN proporcionar los suficientes controles de seguridad informáticos para la separación de roles de confianza. La misma persona NO DEBE adoptar distintos roles de confianza.
- **Control de accesos**: los sistemas IT DEBERÁN forzar la autenticación de los roles en los sistemas de acceso. El acceso a los datos o a las funcionalidades DEBERÁN solamente garantizarse mediante roles de confianza, asignando las correspondientes tareas.
- **Principio de dos personas**: se DEBERÁ establecer una separación de funciones de tareas críticas a través del principio de ejecución de dos personas.
- **Concepto de sustitución**: en el caso de indisponibilidad de personal con roles de confianza se DEBERÁ planificar su sustitución. En caso de sustitución, una misma persona NO DEBERÁ tener la posibilidad de realizar [varios] roles separados.
- **Sistemas separados**: se DEBE asegurar la comunicación entre sistemas IT separados ante la manipulación y el acceso de terceros. Los sistemas IT DEBERÍAN estar separados según sus necesidades de: disponibilidad, de comunicación de internet (por ejemplo, SPOC) y de confidencialidad e integridad de los datos (por ejemplo, CA).
- **Datos sensibles**: los datos sensibles DEBERÁN ser protegidos ante los accesos o modificaciones no autorizados. El intercambio de datos sensibles entre redes no seguras DEBERÁN estar protegido igualmente (por ejemplo, mediante cifrado o utilizando mecanismos de protección de la integridad/autenticidad).
- **Suspensión de suscriptores**: cada CVCA y cada DV DEBERÁN proporcionar mecanismos adecuados para la suspensión de **suscriptores** registrados (CVCA extranjeros). Estos mecanismos DEBERÁN controlar la emisión de certificados o firmas de peticiones de certificados de **suscriptores suspendidos**.
- **Logging**: cada modificación de datos sensibles, incluyendo operaciones de clave privada, así como información de registro y estado, DEBERÁN ser registrados. El capítulo 5.2.1 define los detalles sobre los requisitos del Registro.
- **Archivo**: se DEBERÁN conservar los registros archivados durante un periodo de tiempo apropiado, para proporcionar las pruebas legales necesarias de conformidad con la legislación aplicable del Estado Miembro.
- **Personal**: se DEBERÁ utilizar los sistemas IT por personal cualificado y con experiencia. El capítulo 5.2.2 define los detalles de los requisitos de personal.
- **Ciclo de vida de las medidas de seguridad**: se DEBERÁ actualizar de forma periódica las medidas de seguridad durante el ciclo de vida de la PKI. El capítulo 5.2.3 define detalles de los requisitos del ciclo de vida.
- **Sistemas de prueba**: se RECOMIENDA utilizar sistemas de prueba construidos de forma muy similares a los sistemas reales de SPOC y de certificación y registro, para probar nuevas medidas de seguridad, actualización de software e interoperabilidad con sistemas IT de Estados Miembros extranjeros.

Por cada IS se DEBERÁ definir un Concepto de Seguridad que describa:

- El tipo y la estructura del IS,
- Cada sistema IT que forme parte o aloje parte del IS,

- Las medidas de seguridad y la gestión de incidencias.

Los siguientes puntos DEBERÁN hacer mención al Concepto de Seguridad de un IS:

- **Protección del IS**: se DEBERÁ implementar mecanismos de seguridad IT (por ejemplo, firewalls, software antivirus) de cada sistema IT que forme parte o aloje parte del IS[14]. Se DEBERÁ implementar medidas de seguridad adecuadas en cada interfaz de los sistemas IT utilizados.
- **Control de accesos**: en los accesos se DEBERÁN autenticar los roles para los sistemas IT. Los accesos a datos o a funcionalidades DEBERÁN sólo garantizarse mediante roles de confianza asignados a tareas correspondientes.
- **Sistemas separados**: si es aplicable, la comunicación entre sistemas IT separados DEBERÁ ser protegida contra la manipulación y el acceso de terceros. Los sistemas IT DEBERÍAN estar separados de acuerdo a su necesidad de disponibilidad, de comunicación a internet, de confidencialidad y a la integridad de sus datos.
- **Datos sensibles**: se DEBERÁN proteger los datos sensibles contra los accesos o modificaciones no autorizadas. Los datos sensibles DEBERÁN estar protegidos cuando se intercambian entre redes no seguras (por ejemplo, mediante cifrado o utilizando mecanismos de protección de la integridad/autenticidad).
- **Logging**: el capítulo 5.2.1 define los detalles sobre los requisitos del Registro para el IS.
- **Archivo**: se DEBERÁN conservar registros archivados durante un período de tiempo apropiado para proporcionar pruebas legales necesarias de conformidad con la legislación aplicable del Estado Miembro.
- **Personal:** los IS DEBERÁN ser operados y administrados por personal cualificado y con experiencia. El capítulo 5.2.2 define los detalles de los requisitos de personal.
- **Ciclo de vida de las medidas de seguridad**: se DEBERÁN actualizar de forma periódica las medidas de seguridad durante el ciclo de vida de la PKI. El capítulo 5.2.3 define detalles de los requisitos del ciclo de vida.

5.2.1 Logging (Registro)

Cada SPOC, CVCA, DV e IS DEBEN implementar procedimientos apropiados de registro para analizar y reconocer cualquier utilización correcta o incorrecta de su sistema dentro de EAC-PKI.

El SPOC, la CVCA y el DV DEBERÁN garantizar:

- **El registro de los siguientes eventos**:
  - Creación, uso y destrucción de **claves y certificados**,
  - Creación y modificación de las **entradas del registro**,
  - Todas las peticiones e informes relativos a la **notificación de incidentes y suspensión de registros**, así como el resultado de las acciones;
- **Modo de registro**: se registrará el momento preciso de los eventos y, si es aplicable, los roles de confianza que han ejecutado el evento que ha sido registrado;
- **Integridad y confidencialidad**: se mantiene la confidencialidad e integridad del registro actual y del archivado. Los eventos serán registrados de tal forma que no puedan ser fácilmente borrados o destruidos dentro del período de tiempo

[14] Los mecanismos de seguridad dependen del tipo y estructura del IS

REQUERIDO para su conservación (excepto en la transferencia a medios de larga duración);

- **Archivo:** si el medio original no puede retener los datos durante el período requerido, se establecerá otro mecanismo para transferir periódicamente los datos archivados a un nuevo medio. Se DEBERÁ restringir el acceso a los archivos sólo a operadores autorizados.
- **Documentación**: los eventos específicos y los datos registrados serán documentados.

El IS DEBERÁ cumplir los siguientes requisitos para el registro:

- **Gestión de claves**: un IS DEBERÁ registrar cada evento de gestión de claves, como puede ser la generación y el borrado de claves privadas;
- **Gestión de certificados**: un IS DEBERÁ registrar la emisión de peticiones de certificados y si los certificados correspondientes se han recibido;
- **Control de accesos**: un IS DEBERÁ registrar cada intento de obtener acceso a sus funcionalidades;
- **Protección**: el registro será protegido contra su modificación o eliminación;
- **Registros de Auditoría**: los registros se DEBERÁN conservar durante un tiempo razonable para facilitar la detección de usos indebidos;
- **Registros prohibidos**: los Sistemas de Inspección NO DEBERÁN registrar ni transmitir las huellas dactilares obtenidas de los MRTDs. Cualquier rastro de los datos biométricos DEBERÁ ser borrado de inmediato después de finalizar el proceso de comparación entre las impresiones adquiridas de la persona portadora y las impresiones leídas del MRTD.

5.2.2 Personal

El personal del SPOC, de la CVCA, del DV o del IS DEBERÁ reunir los siguientes requisitos:

- **Conocimiento**: el personal DEBERÁ poseer el conocimiento necesario, experiencia y cualificación necesaria de los servicios ofrecidos y de la función laboral;
- **Fiabilidad**: el personal DEBERÁ someterse a un control de seguridad interno apropiado para el papel que está desempeñando;
- **Conflicto de intereses**: el personal DEBERÁ estar libre de conflictos de intereses;
- **Completar comprobaciones**: el personal NO DEBERÁ tener acceso a las funciones de confianza hasta que las comprobaciones necesarias sean completadas;
- **Instrucciones claras**: el personal DEBERÁ recibir instrucciones claras sobre sus deberes y tareas;
- **Responsabilidad**: el personal DEBERÁ ser responsable de sus actividades.

5.2.3 Ciclo de vida de las Medidas de Seguridad

La seguridad del SPOC, de la CVCA, del DV y del IS DEBERÁ estar sustentada mediante el cumplimiento de los siguientes requisitos:

- **Búsqueda de noticias de seguridad**: los Administradores DEBERÁN buscar noticias relativas a los riesgos de la seguridad, de los ataques y de las contramedidas relacionadas con el hardware, el software, los algoritmos y los protocolos utilizados, al menos una vez al mes;

- **Actualización de seguridad**: los nuevos parches de seguridad para software, algoritmos o protocolos DEBERÍAN ser inmediatamente implementados después de ser probados adecuadamente;
- **Cierre de brechas**: las medidas de seguridad DEBERÁN ser actualizadas inmediatamente si se descubre una brecha de seguridad;
- **Control de cambios**: los procedimientos de control de cambios DEBEN formar parte del Concepto de Seguridad y deben estar documentados; así como, utilizarse para lanzamientos de versiones, modificaciones y correcciones de software de emergencia y para cualquier software operacional de la CVCA, del DV y del IS.
- **Formación en seguridad**: el personal DEBERÁ ser formado en nuevos riesgos de seguridad y contramedidas, al menos, una vez cada seis meses;
- **Formación en actividades**: el personal DEBERÁ ser reciclado en labores y tareas, al menos, una vez al año;
- **Revisión del concepto de seguridad**: el Concepto de Seguridad DEBERÁ ser revisado y actualizado, al menos, una vez al año;

5.3 GESTIÓN DE INCIDENTES

5.3.1 Suspensión del Suscriptor

Una CVCA, un DV o un IS DEBERÁ suspenderse en caso de:

- Cualquier incidente, como compromiso de claves u otras vulnerabilidades de seguridad
- No ser conformes con esta Política de Certificación

Un DV o un IS DEBERÁN también ser suspendidos si no están autorizados a solicitar certificados de Estados Miembros extranjeros.

La suspensión DEBE ser procesada por todos los SPOCs, las CVCAs y los DVs que hayan registrado la CVCA, el DV o el IS suspendido.

5.3.2 Compromiso y Recuperación de Desastres

Las CVCAs DEBERÁN adoptar las medidas razonables para asegurar que la continuidad del servicio se mantiene, incluyendo:

- Medidas para minimizar el impacto de la interrupción de los servicios de energía;
- Medidas para minimizar el impacto de eventos tales como inundaciones o incendios;
- Medidas para minimizar el impacto de la pérdida de disponibilidad del personal clave;

5.3.3 Procedimientos de Gestión de Compromisos e Incidentes

Cualquier CVCA, DV e IS, DEBERÁN asegurar en caso de desastre, incluyendo el compromiso de la clave privada de los participantes, que las operaciones serán restauradas tan pronto como sea posible. Se cumplirán los siguientes requisitos:

- Cada CVCA DEBERÁ definir y mantener un plan de continuidad para actuar en caso de desastre.

- Se DEBERÁN realizar copias de seguridad de los datos de los sistemas de la CVCA necesarios para reanudar sus operaciones y se almacenarán en lugares seguros para permitir a la CVCA volver a las operaciones en caso de incidentes/desastres de manera oportuna.
- Las funciones de copias de seguridad y restauración DEBERÁN ser realizadas por roles de confianza.
- El plan de continuidad de negocio (o de recuperación frente a desastres) de la EAC-PKI DEBERÁ abordar el compromiso o sospecha de compromiso de una clave privada como un desastre y DEBERÁN llevar a cabo los procesos planificados (capítulo 5.3.4).

Si la clave privada de la CVCA, del DV o del IS es inutilizada por razones no críticas, como por ejemplo por peticiones sucesivas retrasada, una nueva solicitud inicial DEBERÁ ser llevada a cabo tal como se describe en el capítulo 4.2 "Certificados Iniciales y peticiones".

Si la clave privada de la CVCA, del DV y del IS es inutilizada por razones críticas, como por ejemplo el compromiso de clave, primero se DEBE resolver el problema de seguridad que ha causado el compromiso, antes de llevar a cabo una nueva solicitud inicial, tal como se describe en el capítulo 4.2 "Certificados Iniciales y peticiones".

5.3.4 Procedimientos de Compromiso de Claves Privadas de Entidad

Un Verificador de Documentos DEBERÁ informar inmediatamente a su Coordinador de PKI Nacional, el cual informará a todos los Coordinadores de los Estados Miembros que hayan emitido certificados para el DV, sobre el compromiso o el uso incorrecto de la clave privada. Las CVCAs nacionales o extranjeras inmediatamente DEBERÁN **suspender** el DV.

Tras la suspensión de la CVCA o del DV por su CVCA nacional, se interrumpirá el uso de la clave privada de manera permanente e inmediata.

Si se roba o pierde un Sistema de Inspección o su clave privada es comprometida o se pierde el control de la clave privada, el responsable del DV DEBERÁ ser informado. El DV DEBERÁ inmediatamente suspender el IS para evitar la emisión de un nuevo certificado. En caso de compromiso de la clave privada que incluya la posibilidad de su uso no autorizado, los Estados Miembros afectados DEBEN ser informados.

Posteriormente a la suspensión de un IS, se interrumpirá el uso de la clave privada de manera permanente e inmediata.

La información del incidente a los Estados Miembros extranjeros DEBERÁ ser distribuida vía SPOC a través del Coordinador de PKI Nacional utilizando la redacción del anexo C.4 "Envío de notificaciones".

El informe del incidente y la solución al problema de seguridad que haya causado el incidente DEBERÍAN ser compartidos con todos los Estados Miembros.

5.4 Finalización de la CVCA o el DV

En el caso de que finalicen las operaciones, la CVCA DEBERÁ cumplir los siguientes requisitos:

- **Notificación a los Coordinadores de la PKI Nacional extranjeros**: la CVCA DEBERÁ notificar a cada Coordinador de PKI extranjero registrado y a aquellos que están siendo registrados, su finalización y la nueva CVCA que se hará cargo de sus tareas;
- **Notificación a la Comisión Europea**: se DEBERÁ notificar a la Comisión Europea la finalización de la CVCA a través del Coordinador de la PKI Nacional del Estado Miembro;

- **Continuidad de la ruta de certificación**: ante cualquier reemplazo de la CVCA, se DEBE continuar proporcionando certificados para el MRTDs emitidos bajo la CVCA original. Por esta razón, se DEBE emitir un Certificado de Enlace que contenga la primera clave pública de la nueva CVCA y que esté firmado por la clave privada válida de la CVCA reemplazada;
- **Destrucción de claves**: la CVCA DEBERÁ destruir o retirar de su uso, sus claves privadas;

En el caso de la finalización de las operaciones de un DV:

- **Notificación de la CVCA nacional**: el DV DEBERÁ notificar a su CVCA nacional
- **Notificación a la CVCA extranjera**: el Coordinador de la PKI Nacional del DV DEBERÁ notificar a los Coordinadores de PKI de la CVCA extranjera cuyo DV esté registrado.[15][14]
- **Suspensión del registro del DV**: todas las CVCAs notificadas DEBERÁN suspender el registro de los DVs para la posterior emisión de certificados.
- **Destrucción de claves**: el DV DEBERÁ destruir o retirar de su uso, sus claves privadas.

6. Seguridad del Par de Claves

6.1 Generación del Par de Claves

La CVCA y el DV DEBERÁN asegurar que sus claves son generadas:

- En circunstancias controladas conforme al capítulo 5.1 "Controles Físicos" de este documento;
- Dentro de un módulo criptográfico que cumple con el Anexo B;
- Y distribuido conforme con la [BSI-EAC] y esta política;
- La CVCA y el DV DEBERÁN asegurar que la integridad y autenticidad de sus claves públicas y todos los parámetros asociados, será mantenida durante la distribución a los DV y al IS.

6.2 Controles de Ingeniería del Módulo Criptográfico y Protección de la Clave Privada

Las claves privadas de la CVCA, del DV y del IS DEBERÁN ser conservadas y utilizadas siguiendo las siguientes reglas:

- **Dispositivo de confianza**: las claves privadas DEBERÁN ser conservadas y utilizadas dentro de un módulo criptográfico que cumpla con el Anexo B "Requerimientos Hardware" y DEBERÁN sólo salir del módulo criptográfico con la finalidad de realizar copias de seguridad conforme al capítulo 6.3 "Custodia, Copia de Seguridad y Recuperación de Clave".
- **Ciclo de vida del dispositivo de confianza**: la seguridad de los dispositivos de confianza DEBE estar garantizada durante su ciclo de vida, asegurando que el módulo criptográfico no sea manipulado durante el transporte y el almacenamiento, que funcione correctamente cuando está en funcionamiento y que las claves privadas almacenadas en el equipo se destruyan al retirarse del módulo.

[15] En el caso que un DV no disponga aún del primer certificado de las CVCAs pero lo haya solicitado

- **Control de acceso del dispositivo de confianza**: donde las claves están almacenadas en un módulo criptográfico, que DEBERÁ tener controles de acceso para garantizar que las claves no sean accesibles fuera del módulo criptográfico. Las medidas DEBERÁN implementarse para evitar el uso no autorizado de claves privadas.
- **Destrucción de clave**: las claves privadas de firma NO DEBEN utilizarse tras el final de su ciclo de vida y todas las copias de la clave DEBERÁN ser destruidas o inutilizadas al final de dicho ciclo.

6.3 CUSTODIA, COPIA DE SEGURIDAD Y RECUPERACIÓN DE CLAVE

Las copias de seguridad de las claves privadas de la CVCA o el DV, DEBEN ejecutarse de acuerdo con los requisitos descritos en el capítulo 6.2 "Controles de Ingeniería del Módulo Criptográfico y Protección de la Clave Privada" y las siguientes reglas:

- Las copias de seguridad de la clave privada DEBERÁN ser almacenadas y recuperadas sólo por personal con roles de confianza, utilizando, al menos, control dual en un entorno físicamente seguro. El número de personal autorizado para llevar a cabo esta función DEBERÍA ser el mínimo imprescindible, pero DEBERÍA permitir la redundancia de personal en caso de indisponibilidad de personal clave.
- Las copias de seguridad de las claves privadas DEBERÁN ser protegidas de tal forma, que se garantice el mismo o un mayor nivel de protección que el provisto por el módulo criptográfico.
- Las copias de seguridad de las claves privadas de la CVCA nacional NO DEBEN ser usadas en ningún lugar, excepto para la restauración del servicio del módulo criptográfico nacional.

No se DEBERÁ realizar depósitos de la clave privada de la CVCA, del DV o del IS. No se DEBERÁN realizar copias de seguridad de las claves privadas del IS. No se DEBERÍAN realizar copias de seguridad y/o recuperación de las claves privadas de DV.

Según se muestra en la siguiente tabla:

	CVCA	DV	IS
Copia de Seguridad	DEBERÍA	NO DEBERÍA	NO DEBERÁ
Depósitos (escrow)	NO DEBERÁ	NO DEBERÁ	NO DEBERÁ

Si una clave privada de un DV o de un IS se inutiliza por razones no críticas, el DV o el IS DEBERÍAN generar un nuevo par de claves y solicitar un nuevo certificado en su autoridad de firma (ver capítulo 5.3.3).

Se DEBERÍA hacer una copia de seguridad de la clave privada de la CVCA para asegurar la cadena de certificación necesaria para obtener acceso a la lectura de los MRTDs.

7. CUMPLIMIENTO CON LA POLÍTICA DE CERTIFICACIÓN (CP)

La distribución de certificados es un requisito previo para el acceso a los datos biométricos almacenados en el chip y es independiente de la evaluación del cumplimiento de esta Política de Certificación, es decir, la distribución de certificados es efectiva de forma inmediata y no requiere una evaluación previa.

Los Estados miembros DEBEN asegurarse de que el cumplimiento del DV con esta Política de certificación esté garantizado en todo momento.

El cumplimiento DEBERÁ evaluarse como parte de la Evaluación de Schengen de conformidad con el REGLAMENTO (UE) No 1053/2013 DEL CONSEJO de 7 de octubre de

2013 por el que se establece un mecanismo de evaluación y seguimiento para verificar la aplicación del acervo de Schengen y se deroga la Decisión del Comité Ejecutivo de 16 de septiembre 1998 creación de un Comité Permanente sobre la evaluación y aplicación de Schengen o durante visitas ad hoc.

El cumplimiento (solo DV) de esta Política de Certificación DEBE ser evidenciado por un certificado emitido por una empresa / organización acreditada o por un certificado emitido por una autoridad de control designada.

El cumplimiento PUEDE ser evidenciado por un certificado emitido de acuerdo con ISO / IEC 27001 e ISO / IEC 27002 o ETSI 319401 u otra norma equivalente.

El certificado de cumplimiento DEBE evidenciar el cumplimiento de todos los requisitos relevantes de DV de los capítulos 5 y 6 de este CCP.

La autoridad de control elegida DEBERÁ llevar a cabo una revisión al menos cada tres años y DEBERÁ enviar el informe a la Comisión.

En caso de que se detecte una violación de la seguridad o de que la evaluación de Schengen arroje un hallazgo de deficiencias graves, el Estado Miembro emisor PUEDE decidir suspender la emisión de certificados al Estado Miembro evaluado hasta que se solucione.

8. ANEXO A DEFINICIONES Y ACRÓNIMOS

8.1 DEFINICIONES

1. Autoridad de Certificación (CA): entidad que expide certificados.

2. Lista de certificados revocados (CRL): lista de certificados que han sido revocados.

3. Política de Certificación (CP): conjunto de normas que indican la aplicabilidad de un certificado a una comunidad en particular o a una clase de aplicación con requisitos comunes de seguridad.

4. Declaración de la Práctica de Certificación (CPS): declaración de la práctica que una autoridad de certificación emplea para expedir, gestionar, revocar o renovar certificados.

5. Política de Certificación Común (CCP): política general de certificación publicada por la Comisión que establece los requisitos mínimos que deben cumplir las políticas de certificación nacionales de los Estados Miembros, para poder ser incluidas en la EAC-PKI.

6. Criterios Comunes (CC): criterios comunes para evaluar la seguridad de la tecnología de la información. Título de un conjunto de documentos que describen un conjunto particular de criterios de evaluación de la seguridad de la IT.

7. Infraestructura de Clave Pública del Control de Acceso Extendido (EAC-PKI): infraestructura necesaria para controlar el acceso a los datos biométricos de las impresiones dactilares en los pasaportes, documentos de viaje y permisos de residencia electrónicos utilizando el control de acceso extendido.

8. Verificador de Documentos (DV): entidad de la EAC-PKI que solicita certificados desde CVCA y, sobre la base de dichos certificados, expide certificados a los sistemas de inspección.

9. Nivel de Garantía de la Evaluación (EAL): grado numérico asignado a un sistema IT o a un producto tras la realización de una evaluación de la seguridad con arreglo a los criterios comunes.

10. Sistema de Inspección (IS): sistema operativo que lee los datos biométricos de impresiones dactilares de los MRTD.

11. Organización Internacional de Aviación Civil (ICAO): organismo de la ONU encargado de fomentar la planificación y el desarrollo del transporte aéreo internacional. A este respecto, fija normas internacionales para los MRTD.

12. Ceremonia de Clave: procedimiento por el que se genera un par de claves utilizando un módulo criptográfico y por el que se certifica la clave pública.

13. Certificado de Enlace (Link): certificados que garantizan la continuidad de una actividad sin intercambiar un nuevo certificado CA raíz de la CVCA sin seguir los cauces normales establecidos.

14. Documento de Viaje de Lectura Mecánicamente (MRTD): documento de viaje internacional que contiene datos legibles a simple vista y mecánicamente.

15. Política de Certificación Nacional (NCP): Política de Certificación de los Estados Miembros para la gestión del proceso de expedición y recepción de certificados para DV nacionales.

16. Coordinador de PKI Nacional: persona o grupo de personas responsables de interactuar con Estados Miembros extranjeros en relación al intercambio de certificados DV y la Política de Certificación Común.

17. Identificador de Objeto (OID): secuencia numérica única que permite la identificación de un documento.

18. Parte pública de la declaración de la práctica de certificación: subconjunto de disposiciones de una CPS completa que hace pública una CA.

19. Autoridad de registro (RA): entidad que establece los procedimientos de inscripción de los solicitantes de certificados, realiza la identificación y la autenticación de los solicitantes de certificados, inicia o divulga incidentes y suspende información de suscriptores y aprueba solicitudes para la renovación de certificados en nombre de la CA.

20. Concepto de Seguridad: es una documentación de todas las tareas, deberes, personal involucrado, sistemas IT e interfaces de CA/RA. Además, describe en detalle las contramedidas que se adoptaran contra las amenazas y las medidas de seguridad (organizacionales y técnicas) a ser realizadas.

21. Punto Único de Contacto (SPOC): interfaz de comunicación técnica conforme a CSN-SPOC.

22. Ruta de certificación fiable: cadena de varios certificados necesarios para validar un certificado que contenga la clave pública requerida. Una cadena de certificados consta de uno o más certificados de la CVCA, los certificados de enlace necesarios, un certificado del DV y el certificado IS.

8.2 Acrónimos

CA: Autoridad de Certificación

CC: Criterios Comunes

CDP: Punto de Distribución de la Lista de certificados revocados

CP: Política de Certificación

CPS: Declaración de la Práctica de Certificación

CRL Lista de Certificados Revocados

CVRA: Autoridad de Registro del país de verificación

CVCA: Autoridad de Certificación del país de verificación

EAC-PKI: Infraestructura de Clave Pública del Control de Acceso Ampliado

DV: Verificador de Documentos

EAC: Extended Access Control (Control de Acceso Ampliado)

EAL: Nivel de Garantía de la Evaluación

ICAO: Organización Internacional de Aviación Civil

IS: Sistema de inspección

MRTD: Machine Readable Travel Document (Documento de viaje de lectura mecánica)

OID: Identificador de Objeto

RA: Autoridad de Registro

SPOC: Punto Único de Contacto

9. ANEXO B REQUERIMIENTOS HARDWARE

Los módulos criptográficos utilizados por las Autoridades de Certificación o por los Sistemas de Inspección DEBERÁN ser evaluados y certificados conforme a uno de los siguientes estándares:

- FIPS PUB 140-2 nivel 3 o superior[16]
- [PP-SSCD[17]]/[PP-QSCD[18]]
- BSI Nivel de Seguridad de Módulos Criptográficos "aumentado"[19] /CEN Perfil De Protección para Módulos Criptográficos del TSP [CEN EN 419221-5] [20]

10. ANEXO C REQUERIMIENTOS SPOC

El SPOC es una interfaz de comunicación y, por lo tanto, no es inherentemente relevante para la seguridad. Todos los objetos enviados o recibidos (excepto los mensajes generales) a través del SPOC están firmados por la CVCA del Estado Miembro que envía/recibe. Los certificados CVCA que actúan como cadenas de confianza se intercambian de manera confiable durante el registro. Por lo tanto, el SPOC no tiene requisitos de seguridad especiales adjuntos y tampoco necesita ser auditado. Dado que el intercambio de certificados también es posible a través de otros medios, por ejemplo, correo electrónico, tampoco hay requisitos de disponibilidad para el SPOC.

10.1 C1 REGISTRO INICIAL SPOC

Se RECOMIENDA hacer un registro inicial del SPOC, junto con el registro CVCA del Estado Miembro según se indica en el capítulo 3.2 y en el anexo D.

10.2 C2 REQUISITOS CA SPOC

[16] NIST: Requisitos de seguridad para módulos criptográficos (FIPS PUB 140-2)

[17] CEN: CEN/TC 224: prEN 14169-1 Protection profiles for Secure signature creation device - Part 2: Device with key generation

18 CEN: CEN: EN 419 211-2: Protection Profile for Secure signature creation device — Part 2: Device with key generation

[19] BSI: BSI-PP-0045-2009: Cryptographic Modules Security level "Enhanced" Version 1.01

[20] CEN: CEN: EN 419 221-5: Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services

10.2.1 C2.1 Aseguramiento de Certificados y Contenido

La CA que emite certificados de comunicación SPOC DEBERÁ estar bajo control gubernamental. Los certificados emitidos por la CA del SPOC DEBERÁN cumplir con los requisitos definidos en CSN-SPOC (nombre, uso de la clave, extensiones).

La Política de Certificación de la CA Raíz del SPOC DEBE asegurar que los OIDs que identifican los certificados SPOC, están asignados sólo a certificados que pertenezcan al SPOC.

10.2.2 C2.2 Información de Revocación de Certificados

Los certificados DEBERÁN contener extensiones válidas de puntos de distribución de certificados (CDP). Al menos un punto de distribución DEBERÁ ser alcanzable vía HTTP. La frecuencia de emisión de la Lista de Certificados **Revocados** (CRL) DEBE ser como máximo de 90 días; en el caso de que un certificado sea **revocado**, se DEBE publicar una CRL en un período máximo de 72 horas posteriores a la revocación del certificado. La CRL correspondiente se DEBERÁ verificar en cada establecimiento de conexión TLS mediante la comunicación del SPOC.

10.2.3 C2.3 Requisitos Organizacionales y Técnicos

La CA Raíz del SPOC DEBERÁ cumplir el mismo nivel de requisitos que la CVCA, recogidos en el capítulo 5 "Requisitos de Seguridad" y en el capítulo 6 "Seguridad del par de claves".

Las claves privadas del Servidor y Cliente utilizadas para la comunicación en el SPOC DEBERÍAN ser almacenadas en un módulo criptográfico seguro, mientras que la clave privada de la CA Raíz del SPOC DEBERÁ ser almacenada en un módulo criptográfico seguro. El módulo que contiene la clave privada de la CA Raíz del SPOC DEBERÁ cumplir los requisitos indicados en Anexo B.

10.2.4 C2.4 Períodos de Validez

Los certificados utilizados para las comunicaciones del SPOC DEBERÁN tener los siguientes períodos de validez:

- Período de validez del certificado de CA Raíz del SPOC:
  - Hasta 13 años si el certificado CSCA es utilizado como certificado Raíz del SPOC
  - 5-7 años si cualquier otro certificado de CA es utilizado como certificado Raíz del SPOC
- Periodo de validez de los certificados de servidor y cliente del SPOC: 6 – 18 meses

10.2.5 C2.5 Distribución de Certificados Raíz SPOC sucesivos

La emisión de un certificado CA Raíz SPOC sucesivo, DEBERÁ comprender la emisión de los Certificados de Enlace entre el actual certificado de la CA Raíz del SPOC y el sucesivo. El pathLenght-Constraint en el certificado SPOC CA-Raíz PUEDE ser 0, 1 o 2_{22}.

La emisión de un certificado CA Raíz SPOC sucesivo, DEBERÁ ser comunicado 90 días antes de que los certificados TLS[23], firmados por este certificado, se utilicen para la comunicación. La comunicación DEBERÁ incluir la última fecha de uso de los certificados antiguos y la primera fecha de uso de los nuevos.

La comunicación de un certificado CA Raíz SPOC sucesivo DEBERÁ hacerse vía SPOC con un mensaje general y, de forma adicional, será enviado a la Comisión Europea.

El certificado CA Raíz SPOC sucesivo y el correspondiente Certificado Enlace DEBERÍAN ser distribuidos por correo electrónico, al menos con 10 días de antelación de su primer uso, utilizando la dirección del formulario de registro del SPOC. Además, se DEBE completar el formulario de registro (parte II) con los datos del nuevo certificado y será enviado a la Comisión Europea.

Si no es posible la emisión de un Certificado Enlace, por ejemplo, después de un incidente de seguridad, el nuevo certificado CA Raíz SPOC DEBE ser distribuido al igual que el certificado inicial conforme al capítulo 3.2.2 "Registro de un Estado Miembro extranjero".

10.3 C3 Prioridades de Comunicación

Siempre que sea posible, se DEBERÁ utilizar un interfaz de servicio web automatizado para el intercambio de datos. Cuando el interfaz del servicio web del respectivo SPOC no se encuentre disponible por más de 72 horas, el cliente (iniciador de la conexión TCP) DEBERÁ contactar con el SPOC, utilizando la información de registro para encontrar una solución a las peticiones de comunicación urgentes.

10.4 C4 Envío de Notificaciones

Se DEBERÁ utilizar el SPOC para el envío de notificaciones. Para enviar la notificación se DEBERÁ utilizar el mensaje general, así definido en la CSN-SPOC. Para propósitos adicionales de mensajes generales se puede utilizar la redacción individual según sea necesario. Se RECOMIENDA utilizar las siguientes expresiones para el sujeto y cuerpo del mensaje

Referencia a Política	**Sujeto**	**Cuerpo mensaje**
[EUCP] ap. 1.4.6	Interrupción del canal de comunicación de la CVCA	El interfaz del servicio web SPOC del país no estará en funcionamiento desde (fecha, hora) hasta (fecha, hora). Durante ese período se utilizará el correo electrónico.
[EUCP] ap. 1.4.6	Suspensión del servicio de la CVCA	El servicio de la CVCA estará suspendido desde [fecha] hasta [fecha].
[EUCP] ap. 1.4.6	Reactivación del servicio SPOC	El interfaz del servicio web SPOC del país ha sido reactivado.
[EUCP] ap. 5.3.4	Clave privada [IS|DV|CVCA] [perdida/robada/comprometida]	La clave privada perteneciente a [referencia del titular del certificado CHR] ha sido [perdida/robada/comprometida] el [fecha].
[EUCP] ap. 4.5	Certificado inexacto	El Certificado adjunto es inexacto.
[EUCP] ap. 5.4	Finalización [CVCA/DV]	La CVCA o el DV identificado por [CHR] finalizará su uso desde [fecha]. Para más información contactar [detalles de contacto].
[EUCP] ap. 7	El DV no conforme	El DV [CHR] no es compatible con los requisitos de la Política.

11. ANEXO D FORMULARIO DE REGISTRO

Este capítulo contiene los formularios de registro que DEBERÁN ser utilizados para el registro de la CVCA de un Estado Miembro en la CVCA del Estado Miembro extranjero de acuerdo con el capítulo 3.2. El formulario de inscripción se compone de cuatro partes:

- Una primera parte que contiene la información de registro del Estado Miembro, el Coordinador de PKI Nacional y la Declaración de Conformidad con la CP.
- La segunda parte contiene la información sobre el SPOC.
- La tercera parte contiene información del certificado CVCA. Si un Estado Miembro desea registrar más de una CVCA, DEBERÁ completar esta parte del formulario una vez por cada certificado CVCA.
- La cuarta parte contiene información sobre los Verificadores de Documentos. Si un Estado Miembro quiere registrar más de un DV, se DEBERÁ completar esta parte del formulario una vez por cada certificado DV[24].

El formulario de registro puede encontrarse en las siguientes páginas.

11.1 D.1 COMENTARIO DEL FORMULARIO DE REGISTRO

Certificado CVCA:

El certificado CVCA utilizado para el registro DEBERÍA ser el certificado más antiguo almacenado como cadena de confianza en los documentos de viaje todavía válidos. Lo que significa que el certificado CVCA sea válido en el día x:

- x = fecha actual – (validez documento de viaje + validez certificado CVCA)

o el certificado CVCA más cercano después del día x[25]

Codificación del certificado:

El certificado CVCA DEBE ser binario y el certificado Raíz del SPOC DEBE estar con la codificación DER para el intercambio de certificado y generación de huellas criptográficas.

Algoritmo Hash:

Los valores hash necesarios para el formulario de inscripción estarán en SHA-256 pero se PUEDEN añadir valores hash y algoritmos adicionales. Los formularios de inscripción rellenados de acuerdo con la versión anterior de la CCP utilizan SHA-1 como algoritmo hash y siguen siendo válidos.

11.2 D.2 HOJAS DE FORMULARIO DE REGISTRO

Las hojas de inscripción se pueden encontrar en las siguientes páginas.

11.2.1 Información de Registro del Estado Miembro – Parte I (Coordinador de PKI Nacional)

Con este documento el Coordinador de PKI Nacional del Estado Miembro abajo indicado declara la Autoridad de Certificación / Autoridad de Registro de cada CVCA y cada SPOC conforme a la Política de Certificación Común y Nacional. Cada CVCA sólo concederá el permiso para solicitar certificados DV de los Estados Miembros extranjeros, a los DV nacionales que hayan declarado su conformidad con la Política de Certificación Común y Nacional.

Estado Miembro	
Nombre de la Organización[21]	
Dirección Postal	
Datos de contacto físico	
Número de Teléfono	
Número de Fax (Opcional)	
Correo electrónico[22] de contacto	

_____ (Sello)

(Fecha, Firma)

11.2.2 Información de Registro del Estado Miembro – Parte II (Certificado Raíz SPOC y URL)

URL[23] SPOC	
Nombre Común (CN)	
Huella criptográfica del Certificado Raíz SPOC (SHA-256)	
El certificado será emitido desde (Fecha)	
El certificado está vinculado a[24]: Nombre Común, Número de Serie	
En caso de cambio de certificado: El certificado actual será utilizado hasta (Fecha)	

Datos adicionales necesarios:

- Certificado de Autoridad de Certificación Raíz de SPOC

_____ (Sello)

(Fecha, Firma)

[21] La organización de la cual es parte el Coordinador de la PKI nacional

[22] Debe ser la dirección de correo electrónico del grupo del Coordinador de PKI Nacional

[23] Ver CSN 36 9791 para detalles

[24] Sólo se debe completar en el caso de que el certificado Raíz de SPOC sea sucesivo

11.2.3 Información de Registro del Estado Miembro – Parte III (Certificado CVCA)

Referencia del titular de certificado (CHR)	
Huella criptográfica del Certificado CVCA (SHA-256)	
Descripción[25] de la CVCA	

Datos adicionales necesarios:

- Certificado CVCA

_____ (Sello)

(Fecha, Firma)

[25] Información del tipo: Usos del certificado

11.2.4 Información de Registro del Estado Miembro – Parte IV (Verificadores de Documentos)

Nombre de la Organización	
Mantenimiento de la CVCA nacional (Nombre y Titular nemónico)	
Titular nemónico de un Verificador de Documentos	
Propósito para la lectura de impresiones dactilares de MRTD	
Suscripción de Sistemas de Inspección[26]	

_____ (Sello)

(Fecha, Firma)

[26] Lista de organizaciones que utilizan los Sistemas de Inspección suscritos al DV