POLÍTICA DE CERTIFICACIÓN EADTRUST

(**E**uropean **A**gency of **D**igital **Trust,** S.L.)

Miembro de

Observatorio del Notariado para la Sociedad de la Información

UBL

cen European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

AENOR
Asociación Española de Normalización y Certificación

FORO evidencias electrónicas

Histórico de versiones			
Versión	Fecha	Documentos sustituidos	Descripción / Detalles
1	23/09/08	Ninguno	Política de certificación de la RootEADTrust
1.2	16/09/09	Versión 1	Política de certificación de la RootEADTrust
1.3	25/01/2010	Versión 1.2	Política de certificación de la RootEADTrust

Cambios desde la última versión
Aclaraciones y adaptaciones a los requerimientos del MITyC

Difusión	
Propietario:	EADTRUST European Agency of Digital Trust, S.L
Preparado por:	Ivan Basart, Santi Casas, Fernando Pino
Modificado por	Ivan Basart, Santi Casas, Fernando Pino
Aprobado por:	Julián Inza
Firma:	
Fecha:	25 de Enero 2010
Distribución:	Publica

Referencias de archivo	
Nombre archivo:	politica-de-certificacion-eadtrust(v1.3)

CONTENIDO

A. INTRODUCCIÓN

A.1 Presentación

El presente documento especifica la Política de Certificación de EADTrust Root y está basada en la especificación del estándar ETSI TS 102 042 Policy Requirements for certification authorities issuing public key certificates..

Esta política comprende las reglas y responsabilidades que debe seguir EADTrust y aquellas Autoridades de certificación, aprobadas por ésta, que deseen formar parte de la estructura de certificación de EADTrust.

De esta forma, cualquier AC que forme parte de la estructura de certificación de EADTrust, deberá ajustarse a los niveles de seguridad que se detallan en esta política de certificación y deberán informar a sus suscriptores de su existencia.

Las ACs intermedias que emitan certificados de entidad final deberán cumplir además lo dispuesto en las respectivas políticas de certificación en virtud de los certificados que emitan.

Los certificados emitidos bajo esta política requerirán la autenticación de la identidad de las AC's y la verificación de la adecuación de sus procedimientos a la presente política.

EADTrust revocará los certificados de las ACs intermedias según lo dispuesto en esta política.

EADTrust deberá conservar los registros e incidencias de acuerdo con lo que se establece en esta política.

Las funciones críticas del servicio deberán ser realizadas al menos por dos personas.

La actividad de las ACs intermedias podrá ser sometida a la inspección de la Autoridad de la Políticas (PA) o por personal delegado por la misma.

En lo que se refiere al contenido de esta Política de Certificación, se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto.Presentación

EADTrust podrá emitir diferentes tipos de sellos de tiempo descritos a continuación.

A.2 Certificados que se emiten

La presente política de Certificación permite la emsión de dos tipos de certificados:

- Certificados de Entidad Final
- Certificados de Autoridad de Certificación Intermedia

Se consideran Certificados de Entidad Final tanto certificados digitales de uso genérico como certificados digitales para la prestación de servicios avanzados como la emisión de sellos de Tiempo o la validación de certificados digitales.

Todas las funcionalidades de los Certificados de Entidad Final se contienen en un único certificado, pudiendo utilizarse diversos tipos de módulos de seguridad, incluyendo bienes de equipo criptográfico.

Los Certificados de Autoridad de Certificación Intermedia corresponden a los certificados emitidos a aquellas entidades que quieran emitir certificados bajo la jerarquía EADTrust según lo establecido en la presente política.

A.3 Identificación

Nombre de la Política:	Política de Certificación EADTrust Root
Descripción:	Define los criterios básicos a seguir por EADTrust y por las AC's que emitan certificados digitales bajo su jerarquía.
Versión:	1.0
Fecha de Emisión:	23 de septiembre de 2008
Referencia (OID):	
Localización:	policy.eadtrust.net

A.4 Participantes en los servicios de Certificación

A.4.1 Root eadtrust / eadtrust

Es la entidad encargada de autorizar y emitir los certificados de las Autoridades de Certificación intermedias y/o de entidad final.

A.4.2 Autoridad de Certificación intermedia (AC intermedia)

Es la entidad responsable de la emisión, y gestión de los certificados digitales y o la prestación de servicios avanzados de certificación, tales como la emisión de sellos de tiempo (Time Stamping Authority o TSA) o la validación de certificados digitales (Validation Authority o VA). Actúa como tercera parte de confianza, entre el Suscriptor y el Usuario, en las relaciones electrónicas,

vinculando una determinada clave publica con una persona (Suscriptor) relacionada a una entidad concreta, a través de la emisión de un Certificado o el suministro de servicios avanzados de certificación.

Pueden emitir Certificados bajo la jerarquía EADtrust, las Autoridades de Certificación cuya Política o CPS esté en conformidad con esta Política de Certificación y hayan sido previamente autorizados.

A.4.3 Autoridad de Registro (AR)

La recepción y procesamiento de las solicitudes de certificados es realizada por una o más "Autoridades de Registro" (AR). Estas efectúan tareas de emisión y gestión de los certificados, y en concreto, las tareas de:

- Contratación del servicio de certificación a entidades finales.
- Identificación y autenticación de la identidad y circunstancias personales de las personas que reciben los certificados.
- Generación de certificados y entrega de dispositivos seguros de creación de firma a los suscriptores en caso que así lo indique la política asociada.
- Almacenamiento de documentos en relación con los servicios de certificación.

Estas AR son parte de EADTrust u organismos independientes, pero que establecen y llevan a cabo sus operaciones sobre la base de una acreditación con EADTrust.

Adicionalmente, EADTrust puede acreditar a una o más "Autoridades Certificadoras" (PSC), para que emitan certificados, bajo las mismas políticas y procedimientos de EADTrust.

Para ello, EADTrust emite un certificado del tipo de "Autoridad de Certificación Intermedia", con el cual el PSC acreditado puede emitir los certificados digitales a los suscriptores finales.

Ente que actúa conforme esta Política de Certificación y, en su caso, mediante acuerdo suscrito con la AC, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y aquellas que se dispongan en las Políticas de Certificación concretas.

A.4.4 Entidades finales

Las entidades finales serán las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, y entre ellas, las siguientes:

1. *Solicitantes de certificados, que los solicitan para ellos o para terceras personas.*
2. *Suscriptores de certificados, que ostentan la titularidad de los certificados.*
3. *Poseedores de claves, que las emplean para las finalidades y aplicaciones previstas en los certificados.*
4. *Representados*.
5. Terceros que confían en certificados.

A.4.4.1 Solicitantes de certificados

Todo certificado debe ser solicitado por una persona, en su propio nombre o en nombre de una organización

Pueden ser solicitantes de certificados:

1. *La persona que va a ser el futuro suscriptor del certificado, y, en consecuencia, el poseedor de claves.*
2. *La persona que, sin ser el futuro suscriptor del certificado solicitado, va ser el poseedor de claves.*
3. *La persona que, sin ser el futuro suscriptor ni el futuro poseedor de claves del certificado, solicita el certificado para otra persona física, en los casos de delegación de facultades del solicitante.*

A.4.4.2 Suscriptores de certificados

Los suscriptores son las personas y las organizaciones titulares del certificado.

En certificados individuales, el suscriptor coincide con el poseedor de claves. En certificados de colectivo, el suscriptor es una entidad y el poseedor de claves, una persona física autorizada o apoderada para recibir y emplear el certificado.

La capacidad del poseedor de claves para actuar en nombre y representación del suscriptor de certificados de colectivo deberá establecerse en el propio certificado, de acuerdo con los requisitos de esta política.

A.4.4.3 Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves criptográficas. El poseedor de claves coincide con el concepto de firmante empleado en la legislación de firma electrónica, pero se denomina de esta forma genérica, dado que también puede emplear el certificado para otras funciones, como la autenticación o el descifrado.

Los poseedores de claves se encuentran debidamente identificados en el certificado, mediante su nombre y apellidos, o, en determinados casos, mediante el empleo de seudónimos.

La capacidad del poseedor de claves para actuar en nombre y representación del suscriptor de certificados de colectivo deberá establecerse en el propio certificado, de acuerdo con los requisitos de esta política.

A.4.4.4 Representados

Tendrán la consideración de representados las personas físicas o jurídicas en cuyo nombre los solicitantes solicitan certificados de representación, de persona jurídica o de entidad sin personalidad jurídica, sin perjuicio de su posible condición de suscriptor, en caso de certificados de colectivo.

A.4.4.5 Terceros que confían en certificados

Los terceros que confían en certificados son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, los terceros deben verificarlos.

A.5 Ámbito de Aplicación y Usos

A.5.1 Usos permitidos para los certificados

A.5.1.1 Certificado ROOT EADTrust

El Certificado Root de EADTrust será empleado tanto para la firma de certificados de ACs intermedias y firma de ARL's como para la emisión de certificados de entidad final y sus respectivas CRL's

A.5.1.2 Certificado Autoridad de Certificación Intermedia

La Declaración de Prácticas de Certificación correspondiente determinará los usos concretos de cada certificado emitido, de acuerdo con las normas establecidas en este documento.

A.5.2 Límites de uso

Los certificados se emplearán para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades. Los certificados pueden incorporar límites de uso por razón de la cuantía u otros conceptos.

Del mismo modo, los certificados deberán emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

A.5.3 Usos Prohibidos y no Autorizados

No se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta Política, en la CPS y en los contratos firmados con la Autoridad de Certificación.

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por EADTrust.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o prohibidos quedan a cargo del suscriptor. En ningún caso podrá el suscriptor, el poseedor de claves o los terceros perjudicados reclamar a Albalia Interactiva, compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para los usos limitados y/o prohibidos.

A.6 Contacto

La Política de Certificación de EADTrust Root, está administrada y gestionada por el órgano directivo de EADTrust, pudiendo ser contactado por los siguientes medios:

E-mail:	eadtrust@eadtrust.net
Teléfono:	902365612

B. Publicación de información y repositorio de certificados

B.1 Repositorio

El repositorio público de EADTrust permite realizar distintas operaciones dependiendo del tipo de certificado con el que se esté trabajando. Estas alternativas son explicadas en el documento de políticas de cada tipo de certificado.

La información relativa a la publicación y revocación de los certificados se mantendrá accesible al público.

EADTrust deberá mantener un sistema seguro de almacén y recuperación de certificados y un repositorio de certificados revocados, pudiendo delegar estas funciones en una tercera entidad.

El repositorio estará disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control del prestador de servicios de certificación, éste realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo

B.2 Publicación y repositorios

B.2.1 Publicación de información de la AC

B.2.1.1 Políticas y Prácticas de Certificación

La Root y las ACs intermedias estarán obligadas a publicar la información relativa a sus Políticas y Prácticas de Certificación.

La presente Política es pública y se encuentra disponible en el sitio de Internet http://policy.eadtrust.net

B.2.1.2 Términos y condiciones

EADTrust pondrá a disposición de las ACs intermedias y Usuarios los términos y condiciones del servicio.

B.2.1.3 Difusión de los certificados

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los certificados son accesibles para las ACs intermedias y Usuarios.

El certificado de la Root es público y se encontrará disponible en la página web www.eadtrust.net. Esta información estará disponible 24 horas al día, 7 días por semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de EADTrust, EADTrust hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

El tiempo transcurrido desde que se solicita revocar o suspender un certificado hasta que se actualiza la base datos no puede exceder 6 horas laborales.

La información de validación en línea de certificados está directamente conectada con la base de datos de revocaciones y suspensiones, por lo que queda actualizada en cuanto se ingresan las solicitudes al sistema.

B.2.2 Frecuencia de publicación

EADTrust deberá publicar la información contenida en el repositorio una vez que tenga conocimiento de la existencia o modificación de la misma.

B.2.3 Controles de acceso

El acceso a la información anterior será gratuito y estará a disposición de las ACs intermedias y usuarios

Se establecerán controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Repositorio, para proteger la integridad y autenticidad de la información de estado de revocación.

Se emplearán sistemas fiables para el Repositorio, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si el suscriptor ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

C. Identificación y AutenticaciónRegistro inicial

C.1.1 Tipos de nombres

C.1.1.1 Autoridades de Certificación

Todas las ACs intermedias requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.500.

Tanto las políticas como las prácticas implementadas por EADTrust en la validación de la identidad del solicitante de un certificado o servicio son presentadas en el documento de políticas escrito para cada tipo de certificado.

C.1.1.2 Certificados

Todos los certificados contendrán un nombre diferenciado de la persona y/o organización, identificados en el certificado, definido de acuerdo con lo previsto en la Recomendación ITU-T X.501 y contenido en el campo *Subject*, incluyendo un componente *Common Name*.

Los certificados podrán contener nombres alternativos de las personas y organizaciones identificadas en los certificados, principalmente en el campo *SubjectAlternativeName*, como el correo electrónico.

Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados deberán incluirse en atributos predefinidos en normas y especificaciones técnicas ampliamente utilizadas en el sector o sectores de actividad donde deban emplearse los certificados.

En caso de que determinadas circunstancias personales no sean fácilmente representables mediante las normas y especificaciones técnicas anteriormente reseñadas, EADTrust deberá establecer extensiones privadas de certificados y atributos privados para incluir dichas informaciones en los certificados.

C.1.2 Empleo de Anónimos y Pseudónimos

En ningún caso se pueden emitir certificados anónimos.

Se podrán admitir pseudónimos para los certificados de ACs intermedias. Podrán existir tipos de certificado, o políticas especiales de certificación que admitan el empleo de seudónimos.

C.1.3 Reglas utilizadas para interpretar varios formatos de nombres

Se atenderá en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

C.1.4 Unicidad de los nombres

EADTrust deberá confirmar la unicidad de los nombres de los certificados de CA.

Los nombres de los suscriptores de certificados serán únicos para cada Entidad de Certificación de EADTrust. En ningún caso se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente.

C.1.5 Procedimiento de resolución de disputas de nombres

Se atenderá a lo dispuesto en el apartado 9.9.4 de este documento

C.1.6 Reconocimiento, autenticación y función de las marcas registradas

Se podrá admitir la identificación en función de marcas registradas.

C.1.7 Métodos de prueba de la posesión de la clave privada

EADTrust deberá tomar las medidas necesarias que aseguren que se posee la clave privada correspondiente a la clave pública objeto de certificación.

El método de demostración de posesión de la clave privada será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método fiable aprobado por EADTrust

Este requisito no se aplica cuando el par de claves es generado por la entidad de registro, por delegación del suscriptor, durante el proceso de personalización o de entrega del dispositivo seguro de creación de firma al suscriptor o poseedor de claves.

En este caso, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del dispositivo seguro y del correspondiente certificado y par de claves almacenados en su interior.

C.1.8 Autenticación de la identidad de una organización

Ver D

C.1.9 Autenticación de la identidad de un individuo

Ver D

C.2 Renovación de la clave

Se podrán renovar certificados, durante su periodo de vigencia desde tres meses antes de su expiración.

Antes de renovar un certificado, EADTrust o las entidades de registro correspondientes deberán comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.

C.3 Reemisión después de una revocación

EADTrust no realizará reemisiones.

C.4 Solicitud de revocación

Todas las solicitudes de revocación deberán ser autenticadas y firmadas

D. Requerimientos Operacionales

D.1 Solicitud de certificados

EADTrust se asegurara que las solicitudes están correctamente identificadas y autorizadas y que la petición de generación del certificado es completa.

Registro

a. Antes de comenzar una relación contractual, EADTrust deberá informar a la AC intermedia de los términos y condiciones relativos a la prestación del servicio y el uso del certificado de CA.
b. EADTrust deberá comprobar, la identidad y los atributos específicos de la AC intermedia. La comprobación de la identidad se realizará en todo caso mediante la personación física de al menos un representante de la AC intermedia y la exhibición por éste de la información relativa a la existencia de la entidad y su propia vinculación con la entidad.
c. La AC intermedia deberá facilitar su dirección física u otros datos que permitan contactar con sus representantes.
d. EADTrust deberá registrar toda la información usada para comprobar la identidad de la AC intermedia.
e. EADTrust deberá guardar el contrato firmado con la AC intermedia.
f. EADTrust deberá cumplir con todos los requisitos impuestos por la legislación aplicable en materia de protección de datos.

D.2 Petición de certificación cruzada

La EADTrust identificará los procesos necesarios para realizar certificación cruzada.

EADTrust deberá revisar cualquier petición de certificación cruzada y aprobar o denegar dicha petición.

Una petición de certificación cruzada deberá incluir en todo caso su política de certificación, un informe de auditoria externa aprobando el nivel de seguridad establecido en la política de certificación y la clave pública de verificación de la AC.

D.3 Emisión de certificados

EADTrust deberá poner todos los medios a su alcance para asegurar que la emisión y renovación de certificados se realiza de una forma segura. En particular:

EADTrust empleará un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.

EADTrust utilizará sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

EADTrust deberá confirmar la unicidad de los DN asignados La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados entre distintos componentes del sistema de certificación.

La emisión de los certificados y la generación de las claves de las ACs intermedias deberá hacerse de acuerdo a una ceremonia de creación de clave que garantice la seguridad de todo el procedimiento.

D.4 Aceptación de certificados

La entrega del certificado y la firma del contrato de adhesión al sistema de certificación implicará la aceptación del La aceptación del certificado deberá realizarse de forma expresa y por escrito.

D.5 Uso por el tercero que confía en certificados

Es obligación del tercero que confía en certificados emitidos por EADTrust:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de EADTrust.
- No comprometer intencionadamente la seguridad de los servicios de certificación de EADTrust.

D.6 Publicación del certificado

EADTrust publicará el certificado en el Depósito a que se refiere la sección B.1 de esta política, con los controles de acceso pertinentes.

D.7 Revocación de certificados

D.7.1 Causas de revocación

Los Certificados de EADTrust deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

Que se detecte que las claves privadas de la Root o la AC intermedia han sido comprometidas, bien porque concurran las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otras circunstancias, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta a la AC intermedia.

Cambios en el contenido del certificado de la AC intermedia.

- Cese en la actividad de la AC intermedia como prestador de servicios de certificación salvo que los certificados expedidos por aquel sean transferidos a otro prestador de servicios.
- Por la decisión unilateral de la AC intermedia o EADTrust.
- Por incumplimiento por parte de la AC intermedia de las obligaciones establecidas en esta política.
- Por la resolución del contrato con la AC intermedia.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial o administrativa que lo ordene.
- Por la extinción de la entidad.
- Por la concurrencia de cualquier otra causa especificada en la presente política.

D.7.2 Quién puede solicitar la revocación

La revocación de un certificado podrá solicitarse únicamente por la AC intermedia o por la propia Root.

Todas las solicitudes deberán ser en todo caso autenticadas.

D.7.3 Procedimiento de solicitud de revocación

La AC intermedia cuyo certificado se haya revocado deberá ser informada del cambio de estado de su certificado. EADTrust utilizará todos los medios a su alcance para conseguir este objetivo, pudiendo intentar la mencionada comunicación por e-mail, teléfono, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

Una vez que un certificado es revocado, este no podrá volver a su estado activo. La revocación de un certificado es una acción, por tanto, definitiva.

La ARL, en su caso, será firmada por la Root o por una autoridad de confianza de la Root EADTrust.

La información relativa al estado de la revocación estará disponible las 24 del día, los 7 días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de EADTrust, que deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

Se deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la autenticidad y la confidencialidad de la información relativa al estado de los certificados.

La información relativa al estado de los certificados deberá estar disponible públicamente.

D.7.4 Periodo de revocación

La decisión de revocar o no un certificado no podrá retrasarse por un periodo máximo de 2 semanas.

D.7.5 Suspensión

No existe suspensión de certificados de CA

D.7.6 Procedimiento para la solicitud de suspensión

No aplicable

D.7.7 Límites del periodo de suspensión

No aplicable

D.7.8 Frecuencia de emisión de ARL's

EADTrust proporcionará la información relativa a la revocación de los certificados a través de una ARL.

EADTrust actualizará y publicará la ARL dentro de las 48 horas siguientes a la recepción de una solicitud de revocación que haya sido previamente validada, y al menos con una frecuencia anual si no se han producido cambios en la ARL.

D.7.9 Requisitos de comprobación de ARL's

Los usuarios deberán comprobar el estado de los certificados de las AC's intermedias en los cuales va a confiar, debiendo comprobar en todo caso la última ARL emitida.

D.7.10 Disponibilidad de comprobación on-line de la revocación

Se proporcionará un servicio on-line de comprobación de revocaciones, el cual estará disponible las 24 horas del día los 7 días de la semana. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de EADTrust, ésta deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo dispuesto en esta política.

D.7.11 Requisitos de la comprobación on-line de la revocación

No estipulado

D.7.12 Otras formas de divulgación de información de revocación disponibles

No estipulado.

D.7.13 Requisitos de comprobación para otras formas de divulgación de información de revocación

No estipulado

D.7.14 Requisitos especiales de revocación por compromiso de las claves

No estipulado

E. Controles de Seguridad Física, Procedimental y de Personal

E.1 Controles de Seguridad física

En este capítulo se detallan los controles y procedimientos establecidos para garantizar una operación de los servicios de certificación bajo un ambiente seguro, desde el punto de vista de la seguridad de las dependencias físicas, y las conductas y capacidad del personal.

La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados. En particular:

General

a. El acceso físico a las instalaciones vinculadas a la generación de certificados, entrega del dispositivo al suscriptor y servicios de gestión de revocaciones deberá ser limitado a las personas autorizadas y las instalaciones en las que se firman los certificados deberán ser protegidas de las amenazas físicas.
b. Se establecerán controles para impedir la perdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad
c. Se establecerán controles para evitar el compromiso o robo de información

Generación de certificados, entrega del dispositivo del suscriptor y gestión de revocaciones.

d. Las actividades relativas a la generación de certificados y gestión de revocaciones serán realizadas en un espacio protegido físicamente de accesos no autorizados al sistema o a los datos.
e. La protección física se conseguirá por medio de la creación de unos anillos de seguridad claramente definidos (p.ej. barreras físicas) alrededor de la generación de certificados y gestión de revocaciones. Aquellas partes de esta tarea compartidas con otras organizaciones quedarán fuera de este perímetro.
f. Los controles de seguridad física y ambiental serán implementados para proteger las instalaciones que albergan los recursos del sistema, los recursos del sistema en si mismos y las instalaciones usadas para soportar sus operaciones. Los programas de seguridad física y ambiental de la Root relativos a la generación de certificados y servicios de gestión de revocaciones estarán provistos de controles de acceso físico, protección ante desastres naturales, sistemas anti-incendios, fallos eléctricos y de telecomunicaciones, humedad y protección antirrobo.

g. g) Se implementarán controles para evitar que los equipos, la información, soportes y software relativos a los servicios de EADTrust sean sacados de las instalaciones sin autorización.

E.1.1 Ubicación y construcción

Las instalaciones de EADTrust deben estar ubicadas en una zona de bajo riesgo de desastres y que permita un rápido acceso a las mismas conforme al plan de contingencias.

Así mismo, las instalaciones estarán equipadas con los elementos y materiales adecuados para poder albergar información de alto valor.

E.1.2 Acceso físico

El acceso físico a las zonas de seguridad estará limitado al personal autorizado previa autenticación.

E.1.3 Alimentación eléctrica y aire acondicionado

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la alimentación eléctrica y el aire acondicionado son suficientes para soportar las actividades del sistema de certificación.

E.1.4 Exposición al agua

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema está protegido de la exposición al agua.

E.1.5 Protección y prevención de incendios

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema está protegido con un sistema anti-incendios.

E.1.6 Sistema de almacenamiento.

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de almacenamiento empleado está protegido de riesgos medioambientales como la temperatura, la humedad y la magnetización.

E.1.7 Eliminación de residuos

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los medios usados para almacenar o transmitir la información de carácter sensible como las claves, datos de activación o archivos serán destruidos, así como que la información que contengan será irrecuperable.

E.1.8 Backup remoto

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las instalaciones usadas para realizar back-up externo, que tendrán el mismo nivel de seguridad que las instalaciones principales.

E.2 Controles procedimentales

E.2.1 Roles de confianza

Los roles de confianza, en los cuales se sustenta la seguridad de la Root EADTrust, serán claramente identificados.

Los roles de confianza incluyen las siguientes responsabilidades:

- Responsable de seguridad: asume la responsabilidad por la implementación de las políticas de seguridad. Adicionalmente, aprobará la generación / revocación de certificados de CA.
- Administradores de sistema: están autorizados para instalar, configurar y mantener los sistemas de confianza de la Root EADTrust para la generación del certificado y gestión de la revocación.
- Operadores de sistema: responsable por el buen funcionamiento diario de los sistemas de confianza de la Root EADTrust. Está autorizado para realizar funciones relacionadas con el sistema de backup y de recuperación.
- Auditores del sistema: están autorizados para ver y mantener los archivos y los logs de los sistemas de confianza de la Root.

EADTrust debe asegurarse que existe una separación de tareas para las funciones críticas para prevenir que una persona use el sistema de la Root EADTrust y la clave de la AC sin detección.

La separación de los roles de confianza serán detallados en la CPS

E.2.2 Número de personas requeridas por tarea

Las siguientes tareas requerirán al menos un control dual:

- La generación, reconstrucción y activación de la clave privada de la Root EADTrust
- La recuperación y back-up de la clave privada de la Root EADTrust
- La emisión de certificados de las ACs intermedias.
- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la Root EADTrust

E.2.3 Identificación y autentificación para cada rol

EADTrust establecerá los procedimientos de identificación y autenticación de las personas implicadas en roles de confianza.

E.3 Controles de seguridad de personal

E.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal cumple con los requisitos mínimos razonables para el desempeño de sus funciones. En concreto:

General

a. EADTrust empleará personal que posea el conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto.

b. Los roles de seguridad y responsabilidades especificadas en la política de seguridad de EADTrust, serán documentados en la descripción del trabajo.

c. Se deberá describir el trabajo del personal de EADTrust (temporal y fijo) desde el punto de vista de realizar una separación de tareas, definiendo los privilegios con los que cuentan, los niveles de acceso y una diferenciación entre las funciones generales y las funciones especificas.

d. El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.

Registro, generación de certificados de CA y gestión de revocaciones

e. Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de PKI y esté familiarizado con procedimientos de seguridad.

f. Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de EADTrust.

g. El personal de la EADTrust será formalmente designado para desempeñar roles de confianza por el responsable de seguridad

h. EADTrust no asignará funciones de gestión a una persona cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

E.3.2 Procedimientos de comprobación de antecedentes

EADTrust no podrá asignar funciones que impliquen el manejo de elementos críticos del sistema a aquellas personas que no posean la experiencia necesaria que propicie la confianza suficiente en el empleado.

E.3.3 Requerimientos de formación

EADTrust debe realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el personal que realiza tareas de operaciones de PKI, recibirá una formación relativa a:

- Los principales mecanismos de seguridad de la Root EADTrust
- Todo el software de PKI y sus versiones empleados en el sistema de EADTrust
- todas las tareas de PKI que se espera que realicen
- los procedimientos de resolución de contingencias y continuidad de negocio.

E.3.4 Requerimientos y frecuencia de la actualización de la formación

La formación debe darse con una frecuencia anual para asegurar que el personal está desarrollando sus funciones correctamente.

E.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado

E.3.6 Sanciones por acciones no autorizadas

EADTrust deberá fijar las posibles sanciones por la realización de acciones no autorizadas.

E.3.7 Requerimientos de contratación de personal

Ya descrito en el apartado E.3.1

E.3.8 Documentación proporcionada al personal

Todo el personal de EADTrust deberá recibir los manuales de usuario en los que se detallen al menos los procedimientos para el registro de certificados, creación, actualización, renovación, suspensión, revocación y la funcionalidad del software empleado.

E.4 Procedimientos de Control de Seguridad

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relevante concerniente a un certificado de EADTrust es conservada durante el periodo de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales. En particular:

General

a. Se deberán realizar los esfuerzos que razonablemente estén a su alcance para confirmar la confidencialidad y la integridad de los registros relativos a los certificados de CA, tanto de los actuales como de aquellos que hayan sido previamente almacenados.
b. Los registros relativos a los certificados de EADTrust deberán ser almacenados completa y confidencialmente.
c. Los registros relativos a los certificados de EADTrust deberán estar disponibles si estos son requeridos a efectos probatorios en los procedimientos legales.
d. El momento exacto en que se produjeron los eventos relativos a la gestión de las claves y la gestión de los certificados de EADTrust deberá ser almacenado.
e. Los eventos se registrarán de manera que no puedan ser fácilmente borrados o destruidos (excepto para su transferencia a medios duraderos) durante el periodo de tiempo en el que deban ser conservados
f. Los eventos específicos y la fecha de registro serán documentados por EADTrust

Registro

g. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que todos los eventos relativos al registro, incluyendo las peticiones de renovación y revocación serán registrados.
h. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que toda la información relativa al registro es almacenada, incluyendo la siguiente:

La documentación presentada por la AC intermedia para el registro

Método empleado para comprobar la validez de los documentos identificativos, si existe

Generación del certificado

i. EADTrust registrará todos los eventos relativos al ciclo de vida de sus propias claves.

j. EADTrust registrará todos los eventos relativos al ciclo de vida de los certificados de EADTrust.

Gestión de la revocación

k. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las peticiones e informes relativos a una revocación, así como su resultado, son registrados.

E.4.1 Tipos de eventos registrados

Toda la información auditada y especificada en el apartado anterior deberá ser archivada.

EADTrust registrará y guardará los logs de todos los eventos relativos al sistema de seguridad de la Root. Estos incluirán eventos como:

- encendido y apagado del sistema
- encendido y apagado de la aplicación de la Root EADTrust
- intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- cambios en los detalles de la Root EADTrust y/o sus claves
- cambios en la creación de políticas de certificados
- intentos de inicio y fin de sesión
- intentos de accesos no autorizados al sistema de la Root EADTrust a través de la red.
- intentos de accesos no autorizados al sistema de archivos.
- generación de claves propias.
- creación y revocación de certificados de CA.
- intentos de dar de alta, eliminar, habilitar, deshabilitar y actualizar ACs intermedias.
- acceso físico a los logs.
- cambios en la configuración y mantenimiento del sistema.
- cambios personales.
- registros de la destrucción de los medios que contienen las claves, datos de activación.

E.4.2 Frecuencia de procesado de Logs

EADTrust deberá revisar sus logs periódicamente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente.

EADTrust deberá así mismo asegurarse de que los logs no han sido manipulados y deberán documentar las acciones tomadas ante esta revisión.

Periodos de retención para los Logs de auditoria

La información almacenada deberá ser conservada al menos durante 5 años

E.4.3 Protección de los Logs de auditoría

El soporte de almacenamiento de los logs debe ser protegido por seguridad física, o por una combinación de seguridad física y protección criptográfica. Además será adecuadamente protegido de amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

E.4.4 Procedimientos de backup de los Logs de auditoría

Debe establecerse un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

E.4.5 Sistema de recogida de información de auditoria

No estipulado

E.4.6 Notificación al sujeto causa del evento

No estipulado.

E.4.7 Análisis de vulnerabilidades

Se deberá realizar una revisión de riesgos de seguridad para la totalidad del sistema. Esta revisión cubrirá la totalidad de riesgos que pueden afectar a la emisión de certificados y se realizará con una periodicidad anual.

E.5 Archivo de registros

E.5.1 Tipo de archivos registrados

Los siguientes datos y archivos deben ser almacenados por EADTrust o por delegación de esta.

- todos los datos de la auditoría del sistema.
- todos los datos relativos a los certificados.
- solicitudes de emisión y revocación de certificados de CA.
- todos los certificados de ACs intermedias emitidos o publicados.
- ARL's emitidas o registros del estado de los certificados generados.
- historial de claves generadas.
- las comunicaciones entre los elementos de la PKI.

EADTrust es responsable del correcto archivo de todo este material

E.5.2 Periodo de retención para el archivo

La información archivada deberá ser conservada durante al menos 15 años.

E.5.3 Protección del archivo

El soporte de almacenamiento debe ser protegido por medio de seguridad física, o por una combinación de seguridad física y protección criptográfica. Además el soporte será adecuadamente protegido amenazas físicas como la temperatura, la humedad, el fuego y la magnetización.

E.5.4 Procedimientos de backup del archivo

Debe establecerse un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes estén disponibles en un periodo corto de tiempo las correspondientes copias de backup.

E.5.5 Requerimientos para el sellado de tiempo de los registros

EADTrust debe emitir los certificados y las ARLs con información fiable de fecha y hora.

No será necesario que esta información se encuentre firmada digitalmente.

E.5.6 Sistema de recogida de información de auditoria

No estipulado

E.5.7 Procedimientos para obtener y verificar información archivada

EADTrust dispondrá de un procedimiento adecuado que limite la obtención de información sólo a las personas debidamente autorizadas.

Este procedimiento deberá regular tanto los accesos a la información internos como externos, debiendo exigir en todo caso un acuerdo de confidencialidad previo a la obtención de la información.

E.6 Cambio de clave de la AC

Antes de que el uso de la clave privada de la Root EADTrust caduque se deberá realizar un cambio de claves. La vieja CA y su clave privada se desactivaran y se generara una nueva CA con una clave privada nueva y un nuevo DN.

Los siguientes certificados serán puestos a disposición publica en el directorio :

Clave publica de la nueva CA firmada por la clave privada de la vieja CA

Clave publica de la vieja CA firmada con la clave privada de la nueva CA.

E.7 Recuperación en caso de compromiso de la clave o desastre

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar en caso de desastre o compromiso de su clave privada que éstas serán restablecidas tan pronto como sea posible.

E.7.1 La clave de la Root EADTrust se compromete

El plan de la continuidad de negocio de EADTrust (o el plan de contingencia) tratará el compromiso o el compromiso sospechado de su clave privada como un desastre.

En caso de compromiso, EADTrust tomará como mínimo las siguientes medidas:

Informar a todos los usuarios y a las ACs intermedias del compromiso.

Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave pueden no ser válidos.

E.7.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre

EADTrust debe tener un plan apropiado de contingencias para la recuperación en caso de desastres.

EADTrust debe reestablecer los servicios de acuerdo con esta política dentro de las 48 horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal reestablecimiento.

E.8 Cese de la Root EADTrust

EADTrust cumplirá con lo expuesto en el artículo 21 de la ley 59/2003 de Firma Electrónica en lo que refiere al cese de la actividad

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se minimizan los posibles perjuicios que se puedan crear a las ACs intermedias o usuarios como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales. En particular:

a. Antes del cese de su actividad deberá realizar, como mínimo, las siguientes actuaciones:
   - Informar a todos los usuarios y ACs intermedias del cese.
   - Informar al Ministerio de Industria Turismo y Comercio del cese de la actividad
   - EADTrust revocará toda autorización para actuar en su nombre en el procedimiento de emisión de certificados.
   - EADTrust realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
   - Las claves privadas de la Root EADTrust serán destruidas o deshabilitadas para su uso.
b. Se establecerán en la CPS las previsiones hechas para el caso de cese de actividad. Estas incluirán:
   - informar a las entidades afectadas
   - transferencia de las obligaciones de EADTrust a otras partes
   - cómo debe ser tratada la revocación de certificados emitidos cuyo periodo de validez aun no ha expirado.
   - Comunicar al Ministerio de Ciencia y Tecnología la información relativa a los certificados cuya vigencia haya sido extinguida.

En particular, EADTrust deberá:

- informar puntualmente a todas las ACs intermedias, usuarios y al Ministerio de Industria, Turismo y Comercio con una anticipación mínima de 6 meses antes del cese.
- transferir todas las bases de datos importantes, archivos, registros y documentos a la entidad designada durante las 24 horas siguientes a su terminación.

F. Controles de Seguridad Técnica

F.1 Generación e instalación del par de claves

F.1.1 Generación del par de claves

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus propias claves y las de las ACs intermedias sean generadas de acuerdo a los estándares.

En particular:

a. La generación de la clave de la Root EADTrust se realizará en un entorno securizado físicamente por el personal adecuado según los roles de confianza y, al menos con un control dual. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS.

b. clave de la Root EADTrust se custodiará en un dispositivo que cumpla los requerimientos que se detallan en el FIPS 140-1, en su nivel 3 o superior.

F.1.2 Envío de la clave pública al emisor del certificado

Para la emisión de certificados bajo la jerarquía EADTrust, el método de remisión de la clave pública a EADTrust será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por EADTrust.

F.1.3 Entrega de la clave pública de la Root EADTrust a los Usuarios

La clave pública de cada Entidad de Certificación EADTrust se publicará en el Repositorio, en forma de certificado autofirmado.

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la integridad y la autenticidad de su clave pública y los parámetros a ella asociados son mantenidos durante su distribución a los usuarios.

En particular:

a. La clave pública de la Root estará disponible a los usuarios de manera que se asegure la integridad de la clave y se autentique su origen.

b. El certificado de la Root EADTrust y su fingerprint (huella digital) estarán a disposición de los usuarios a través de su página web.

F.1.4 Tamaño y periodo de validez de las claves del emisor

La Root EADTrust y las ACs intermedias deberán usar claves basadas en el algoritmo RSA con una longitud mínima de 2048 bits para firmar certificados.

El periodo de uso de una clave privada será como máximo de 30 años, después del cual deberán cambiarse estas claves.

El periodo de validez del certificado de la Root EADTrust se establecerá como mínimo en atención a lo siguiente:

El periodo de uso de la clave privada de la Root EADTrust, y

El periodo máximo de validez de los certificados de EADTrust firmados con esa clave

F.1.5 Parámetros de generación de la clave pública

No estipulado

F.1.6 Comprobación de la calidad de los parámetros

EADTrust podrá establecer métodos de comprobación de la calidad de los parámetros de las claves públicas.

F.1.7 Hardware/software de generación de claves

Las claves de la Root EADTrust y de las ACs intermedias deberán ser custodiadas en un módulo criptográfico validado al menos por el nivel 3 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

F.1.8 Fines del uso de la clave

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus claves son usadas para la firma de ACs intermedias y ARL's y las de las ACs intermedias son usadas para los propósitos de generación de certificados y para la firma de CRLs.

EADTrust deberá incluir la extensión *KeyUsage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas.

F.2 Protección de la clave privada

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus claves privadas continúan siendo confidenciales y mantienen su integridad. En particular:

a. La clave privada será mantenida y usada en un dispositivo criptográfico seguro, el cual cumple los requerimientos que se detallan en el FIPS 140-1, en su nivel 3 o superior.
b. Cuando la clave privada de la Root EADTrust esté fuera del módulo criptográfico esta deberá estar cifrada.
c. Se deberá hacer un back up de la clave privada de firma, que deberá ser almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro. El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en la CPS.
d. Las copias de back up de la clave privada de firma se regirán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

F.2.1 Estándares para los módulos criptográficos

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

F.2.2 Control multipersona (n de entre m) de la clave privada

Se requerirá un control multipersona para la reconstrucción y activación de la clave privada de la Root EADTrust.

Para el acceso a las claves privadas será necesaria la concurrencia de varios dispositivos criptográficos protegidos por una clave de acceso. La clave de acceso será conocida únicamente por una persona responsable de ese dispositivo. Ninguna de ellas conocerá más que una de las claves de acceso.

F.2.3 Depósito de la clave privada (key escrow)

La clave privada de la Root EADTrust debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

F.2.4 Copia de seguridad de la clave privada

La clave privada de las Entidades de Certificación de EADTrust deberá contar con una copia de respaldo realizada, almacenada en dependencia independiente de aquélla donde se almacena habitualmente, y recuperada en su caso, por personal sujeto a la política de confianza del personal. Este personal debe ser expresamente autorizado a estos fines, y debe limitarse a aquel que necesite hacerlo.

Los controles de seguridad a aplicar a las copias de respaldo de las Entidades de Certificación deberán ser de igual o superior nivel a los que se aplican a las claves habitualmente en uso.

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, deberán proveerse los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

F.2.5 Archivo de la clave privada

La clave privada de la Root EADTrust no podrá ser archivada una vez finalizado su ciclo de vida.

F.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se podrán generar directamente en los módulos criptográficos o en módulos criptográficos externos, de los que se exportarán las claves cifradas para su introducción en los módulos de producción.

Las claves privadas de las Entidades de Certificación quedarán almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no podrán ser extraídas)

Dichos dispositivos serán empleados para introducir la clave privada en el módulo criptográfico.

F.2.7 Método de activación de la clave privada

La clave privada de cada Entidad de certificación se activará mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección F.2.2

F.2.8 Método de destrucción de la clave privada

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que la clave privada no será usada una vez finalizado su ciclo de vida.

Todas las copias de la clave privada deberán ser destruidas de forma que la clave privada no pueda ser recuperada

F.3 Durante la destrucción de las claves, se registrarán y describirán los pasos realizados en un documento creado al efecto para dejar constancia de la acción realizada. Otros aspectos de la gestión del par de claves

F.3.1 Archivo de la clave pública

EADTrust deberá conservar todas las claves públicas de verificación

F.3.2 Periodo de uso para las claves públicas y privadas

Los periodos de utilización de las claves serán los determinados por la duración del certificado, transcurrido el cual no podrán continuar utilizándose.

F.4 Controles de seguridad informática

EADTrust empleará sistemas fiables y productos que estén protegidos contra modificaciones. En particular, los sistemas deberán cumplir las siguientes funciones:

- Se debe garantizar una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.
- Se debe garantizar que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema estará restringido y estrechamente controlado.
- El personal deberá ser identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.
- Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.
- Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma)

- El acceso a los depósitos públicos de la información (por ejemplo, certificados o información de estado de revocación) deberá contar con un control de accesos para modificaciones o borrado de datos.

F.4.1 Requerimientos técnicos de seguridad informática específicos

Cada servidor de EADTrust incluirá las siguientes funcionalidades:

- control de acceso a los servicios de EADTrust y gestión de privilegios.
- imposición de separación de tareas para la gestión de privilegios.
- identificación y autenticación de roles asociados a identidades.
- archivo del historial de los datos de auditoría.
- auditoria de eventos relativos a la seguridad.
- auto-diagnóstico de seguridad relacionado con los servicios de la Root.
- Mecanismos de recuperación de claves y del sistema de Root.

Las funcionalidades expuestas pueden ser provistas por el sistema operativo o mediante una combinación de sistemas operativos, software de PKI y protección física.

F.4.2 Valoración de la seguridad informática

No estipulado

F.5 Controles de seguridad del ciclo de vida

F.5.1 Controles de desarrollo del sistema

EADTrust empleará sistemas fiables y productos que estén protegidos contra modificaciones.

Se deberá realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de autoridad de certificación y de registro, para garantizar que los sistemas son seguros.

Se emplearán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

F.5.2 Controles de gestión de la seguridad

F.5.2.1 Gestión de seguridad

En este capítulo se describen una serie de controles de carácter técnico que permiten mantener un ambiente de operación seguro, tanto en la generación y administración de los certificados y claves asociadas a la Root EADTrust, así como sus ACs intermedias. Los controles de seguridad técnicos asociados a las claves de cada tipo de certificado emitido por las ACs intermedias son explicados en las políticas de certificados de cada tipo de certificado.

Todo el proceso de generación, respaldo y recuperación de las claves criptográficas de la Root EADTrust y sus ACs intermedias se encuentra descrito en un documento confidencial llamado "Manual de Operaciones de EADTrust". Este documento y su cumplimiento por parte de EADTrust ha sido auditado por los organismos auditores de EADTrust.

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los procedimientos administrativos y de gestión son aplicados, son adecuados y se corresponden con los estándares reconocidos.

En particular:

a. EADTrust será responsable por todos los aspectos relativos a la prestación de servicios de certificación, incluso si algunas de sus funciones han sido subcontratadas con terceras partes. Las responsabilidades de las terceras partes serán claramente definidas por EADTrust en los acuerdos concretos que EADTrust suscriba con esas terceras partes para asegurar que éstas están obligadas a implementar cualquier control requerido por EADTrust. EADTrust será responsable por la revelación de prácticas relevantes.

b. EADTrust deberá desarrollar la actividades necesarias para la formación y concienciación de los empleados en material de seguridad.

c. La información necesaria para gestionar la seguridad de la Root deberá mantenerse en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido deberá ser aprobado por el foro de gestión de EADTrust.

d. Los controles de seguridad y procedimientos operativos para las instalaciones de EADTrust, sistemas e información necesarios para los servicios de certificación serán documentados, implementados y mantenidos.

e. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que se mantendrá la seguridad de información cuando la responsabilidad respecto a funciones de la Root EADTrust haya sido subcontratada a otra organización.

F.5.2.2 Clasificación y gestión de información y bienes

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que sus activos y su información reciben un nivel de protección adecuado. En particular, EADTrust mantendrá un inventario de toda la información y hará una clasificación de los mismos y sus requisitos de protección en relación al análisis de sus riesgos.

F.5.2.3 Operaciones de gestión

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que los sistemas de EADTrust son seguros, son tratados correctamente, y con el mínimo riesgo de fallo. En particular:

a. se protegerá la integridad de los sistemas de la Root EADTrust y de su información contra virus y software malintencionado o no autorizado

b. los daños derivados de incidentes de seguridad y los errores de funcionamiento deberán ser minimizados por medio del uso de reportes de incidencias y procedimientos de respuesta.

c. Los soportes serán custodiados de manera segura para protegerlos de daños, robo y accesos no autorizados.

d. Se establecerán e implementarán los procedimientos para todos los roles administrativos y de confianza que afecten a la prestación de servicios de certificación.

Tratamiento de los soportes y seguridad

e. Todos los soportes serán tratados de forma segura de acuerdo con los requisitos del plan de clasificación de la información. Los soportes que contengan datos sensibles serán destruidos de manera segura si no van a volver a ser requeridos.

Planning del sistema

f. Se deberá controlar la capacidad de atención a la demanda y la previsión de futuros requisitos de capacidad para asegurar la disponibilidad de recursos y de almacenamiento.

Reportes de incidencias y respuesta

g. EADTrust responderá de manera inmediata y coordinada para dar respuesta rápidamente a los incidentes y para reducir el impacto de los fallos de seguridad. Todos los incidentes serán reportados con posterioridad al incidente tan pronto como sea posible.

Procedimientos operacionales y responsabilidades

h. Las operaciones de seguridad de la Root EADTrust serán separadas de las operaciones normales

F.5.2.4 Gestión del sistema de acceso

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas. En particular:

General

a. Se implementarán controles (p. Ej. Firewalls) para proteger la red interna de redes externas accesibles por terceras partes.

b. Los datos sensibles serán protegidos cuando estos sean transmitidos por redes no protegidas.

c. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la efectiva administración de acceso de usuarios (incluyendo operadores, administradores y cualquier usuario que tenga un acceso directo al sistema) para mantener el sistema de seguridad, incluida la gestión de cuentas de usuarios, auditorias y modificación o supresión inmediata de accesos.

d. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que el acceso a la información y a las funciones del sistema está restringido de acuerdo con la política de control de accesos, y que el sistema de la AC dispone de los controles de seguridad suficientes para la separación de los roles de confianza identificados en la CPS, incluyendo la separación del administrador de seguridad y las funciones operacionales. Concretamente, el uso de utilidades del sistema estará restringido y estrictamente controlado.

e. El personal de EADTrust será identificado y autenticado antes de usar aplicaciones críticas relativas a la gestión de certificados.

f. El personal de EADTrust será responsable de sus actos.

g. Se protegerán los datos sensibles contra medios de almacenamiento susceptibles de que la información sea recuperada y accesible por personas no autorizadas.

Generación del certificado y revocación

h. Las instalaciones de EADTrust estarán provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

F.5.2.5 Gestión del ciclo de vida del hardware criptográfico

EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la seguridad del hardware criptográfico a lo largo de su ciclo de vida. En particular, que:

a. el hardware criptográfico de firma de certificados no se manipula durante su transporte.

b. el hardware criptográfico de firma de certificados no se manipula mientras está almacenado.

c. el uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

d. el hardware criptográfico de firma de certificados está funcionando correctamente.

F.5.2.6 Evaluación de la seguridad del ciclo de vida

No estipulado.

F.6 Controles de seguridad de la red

Estipulado en el apartado F.5.2.4

F.7 Controles de ingeniería de los módulos criptográficos

Se debe garantizar que las claves de las Entidades de Certificación son generadas en equipamientos criptográficos, operados por personal de confianza de la Entidad y en un entorno seguro bajo control dual.

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por al menos el nivel 3 de FIPS 140-1 o por un nivel de funcionalidad y seguridad equivalente.

Los algoritmos de generación de claves deberán estar aceptados para el uso de la clave a que esté destinado.

G. PERFILES DE CERTIFICADO Y CRL

G.1 Perfil de Certificado

Los certificados tendrán el contenido y campos descritos en esta sección, incluyendo, como mínimo, los siguientes:

- Número de serie, que será un código único con respecto al nombre distinguido del emisor
- Algoritmo de firma.
- El nombre distinguido del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280
- Nombre distinguido del sujeto.
- Clave pública del sujeto, codificada de acuerdo con RFC 3280
- Firma, generada y codificada de acuerdo con RFC 3280

Los certificados serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, April 2002
- ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997, con sus actualizaciones y correcciones posteriores.

G.1.1 Número de versión

Deberá indicarse en el campo versión que se trata de la v.3

G.1.2 Campos del certificado

Version	V3
Algoritmo de Firma	sha1WithRsaSignature
Emisor (Issuer)	C= ES CN= EADTrust Root CA O= European Agency of Digital Trust OU = http://www.eadtrust.net
Asunto (Subject)	C= ES CN= EADTrust Root CA O= European Agency of Digital Trust OU = http://www.eadtrust.net
Periodo de Validez	29 años
Algoritmo de Clave Pública	rsaEncryption
Tamaño de Clave Pública	2048
Nombres alternativos del titular	EADTRUST
Uso de clave	Firma de certificados, Firma CRL sin conexión, Firma CRL
Punto de distribucion de CRL	http://crl.eadtrust.net/eadtrust_root.crl
Restricciones Básicas	CA: TRUE pathLenConstraint: 4
Identificador de clave de autoridad	Numero de serie del emisor
Políticas de Certificado	1.3.6.1.4.1.19126.1.50 Calificador de política (id-qt-cps) http://policy.eadtrust.net
User Notice	You can download this certificate from http://www.eadtrust.net/eadtrust_root.crt
Uso de claves mejorado	Autenticación del servidor Autenticación del cliente Correo seguro Firma de código Impresión de fecha 1.3.6.1.5.5.7.3.9

G.1.3 Identificadores de objeto (OID) de los algoritmos

SHA-1 with RSA Encryption (1.2 840.113549.1.1.5)

G.1.4 Restricciones de los nombres

No estipulado

G.2 Perfil de CRL

Version	V2
Emisor	C= ES CN= EADTrust Root CA O= European Agency of Digital Trust OU = http://www.eadtrust.net
Periodo maximo de valide	Días
Algoritmo de firma	
identificador de clave de autoridad	Id. de clave DN Emisor de certificado: Número de serie del certificado de emisor

G.2.1 Número de versión

Deberá indicarse en el campo versión que se trata de la .V.2

G.2.2 CRL y extensiones

Las CRLs emitidas por el sistema del DNIe serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework

H. AUDITORIAS

EADTrust debe realizar periódicamente una auditoría de cumplimiento para probar que cumple, una vez ha empezado a funcionar, los requisitos de seguridad y de operación necesarios.

H.1 Frecuencia de las auditorias

Se debe llevar a cabo una auditoría de conformidad anualmente, además de las auditorías internas que pueda llevar a cabo bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

H.2 Identificación y calificación del auditor

Si se dispone de un departamento de auditoría interno, éste podrá encargarse de llevar a cabo la auditoría de conformidad.

En el caso de no poseer ese departamento, o de considerarlos oportuno, se deberá acudir a un auditor independiente, el cual debe demostrar experiencia y conocimientos en seguridad informática, en sistemas PKI, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública.

H.3 Relación entre el auditor y EADTrust

La auditoria deberá ser realizada preferentemente por un auditor independiente y neutral.

No obstante, lo anterior no impedirá la realización de auditorías internas periódicas.

H.4 Tópicos cubiertos por la auditoria

La auditoria deberá verificar en todo caso:

- Que EADTrust tiene un sistema que garantice la calidad del servicio prestado
- Que la Root EADTrust cumple con los requerimientos de esta Política de Certificación
- Que la CPS y las Políticas concretas de EADTrust se ajustan a lo establecido en esta Política, con lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.

H.5 Auditoria en las ACs intermedias

Todas las ACs intermedias y las AR's empleadas por éstas, deben ser auditadas en las mismas condiciones que la Root EADTrust, pudiendo ser realizadas internamente.

H.6 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, EADTrust debe discutir, con la entidad que ha ejecutado la auditoría las deficiencias encontradas y desarrollar y ejecutar un plan correctivo que solvente dichas deficiencias.

Si EADTrust no es capaz de desarrollar y/o ejecutar el mencionado plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema deberá realizarse una de las siguientes acciones:

- Revocar la clave de las Entidades de Certificación
- Terminar los servicios de certificación

I. REQUISITOS COMERCIALES Y LEGALES

I.1 Tarifas

I.1.1 Tarifas de emisión o renovación de certificados

Albalia Interactiva establece una tarifa por emisión o por la renovación de certificados.

I.1.2 Tarifas de acceso a los certificados

El acceso a los certificados de CA emitidos será gratuito.

I.1.3 Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

La AC proveerá de un acceso a la información relativa al estado de los certificados de AC intermedia o de los certificados de AC intermedia revocados gratuito.

I.1.4 Tarifas por el acceso al contenido de estas Políticas de Certificación

El acceso al contenido de la presente Política de Certificación será gratuito.

I.1.5 Tarifa de otros servicios

Sin estipulación

I.1.6 Política de reintegro

Se establece la siguiente política de reintegro

Cuando una rectificación o modificación de la Declaración de Prácticas de Certificación implique una limitación de los derechos de uso o una restricción sobre el ámbito de aplicación de un certificado en vigor, el suscriptor del mismo puede instar la revocación del mismo y reclamar como máximo el reembolso del precio del certificado.

En los demás casos, el suscriptor no tendrá derecho alguno al reintegro del coste del certificado.

I.2 Confidencialidad

I.2.1 Informaciones confidenciales

Se determinará por EADTrust la información que deba ser considerada confidencial, debiendo cumplir en todo caso con la normativa vigente en materia de protección de datos y concretamente con lo dispuesto por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007.

Las políticas de privacidad de EADTrust se encuentran publicadas en

www.eadtrust.net.

En concreto, como mínimo, serán mantenidas confidenciales las siguientes informaciones:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por Albalia Interactiva
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Albalia Interactiva y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

I.2.2 Informaciones no confidenciales

La siguiente información será considerada no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por una Entidad de Certificación.
- El nombre y los apellidos del suscriptor del certificado o del poseedor de claves, según proceda, así como cualesquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.

- La dirección de correo electrónico del suscriptor del certificado o del poseedor de claves, según proceda, o la dirección de correo electrónico que corresponda.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.

Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.

La información contenida en el Depósito.

Toda otra información que no esté indicada en la sección anterior de esta política.

I.2.3 Divulgación de información de suspensión y revocación

La forma de difundir la información relativa a la suspensión o revocación de un certificado de AC intermedia se realizará mediante la publicación de las correspondientes ARLs.

I.2.4 Divulgación legal de información

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

Se indicarán estas circunstancias en la política de intimidad prevista en la sección I.4 de esta política.

I.2.5 Divulgación de información por petición de su titular

Se incluirá, en la política de intimidad prevista en la sección I.4 de esta política, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del poseedor de claves, directamente a los mismos o a terceros.

I.2.6 Otras circunstancias de divulgación de información

Sin estipulación.

I.3 Protección de datos personales

Para la prestación del servicio, se precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales. Tales informaciones serán recabadas directamente de los afectados, con su consentimiento explícito o en los casos es los que la ley permita recabar la información sin consentimiento del afectado.

Se recabarán los datos exclusivamente necesarios para la expedición y el mantenimiento del certificado.

Se deberá desarrollar una política de intimidad, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documentar en su Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Medidas de Seguridad. Dicha Declaración de Prácticas de Certificación tendrá la consideración de documento de seguridad.

No se divulgará ni cederá datos personales, excepto en los casos previstos en las secciones I.2.2 a 0 de esta política.

La información confidencial de acuerdo con la LOPD será protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 994/99, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

I.4 Derechos de propiedad intelectual

ALBALIA Interactiva es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Política de Certificación. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva de EADTrust sin la autorización expresa por su parte. No obstante, no necesitará autorización de EADTrust para la reproducción del Certificado cuando la misma sea necesaria para su utilización por parte del Usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta Política de Certificación.

Los documentos definidos cómo públicos pueden ser reproducidos respetando las restricciones indicadas en cada documento:

- Políticas de privacidad
- Políticas de certificados
- Prácticas de certificación

I.4.1 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, el poseedor de claves, conservará cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor será el propietario del nombre distinguido del certificado.

I.4.2 Propiedad de claves

Los pares de claves serán propiedad de los suscriptores de los certificados.

Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave serán propiedad del propietario de la clave.

I.5 Obligaciones

I.5.1 Root EADTrust

EADTrust está obligada a cumplir las siguientes obligaciones:

1. Respetar lo dispuesto en esta política
2. Proteger su información contra pérdidas, destrucciones y falsificaciones.
3. Respetar lo dispuesto por la legislación relativa a la protección de datos personales
4. Proteger sus claves privadas de forma segura
5. Emitir certificados a las ACs intermedias de forma segura
6. Revocar los certificados según lo dispuesto en esta política y publicar la correspondiente ARL.
7. Informar a las ACs intermedias de los cambios que se produzcan en las presentes políticas.
8. Mantenimiento de un registro electrónico actualizado con la lista de los certificados revocados y/o suspendidos, el cual puede ser consultado públicamente.
9. Ejecutar todas sus actividades de certificación acorde a las normas estipuladas en la CPS y CP pertinente a cada tipo de certificado.

10. Expedir o emitir los certificados con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente.
11. Revocar unilateralmente los certificados, en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido, y notificar a las partes correspondientes acorde a las normas estipuladas en estas CPS.
12. Mantener las herramientas tecnológicas para evitar cualquier falsificación y adulteración de las llaves privadas mantenidas por EADTrust.

Las obligaciones específicas, pertinentes a cada clase de certificado emitido se detallan en las "Políticas de Certificado" correspondiente, y disponible públicamente en www.eadtrust.net

I.5.2 AC

Cada AR o PSC acreditado por EADTrust deberá cumplir las normas y ser consecuente con lo establecido en este documento (CPS), en todas sus actividades. Específicamente, se obliga a:

1. Respetar lo dispuesto en esta Política.
2. Proteger sus claves privadas de forma segura.
3. Emitir certificados de entidad final conforme a esta Política y a los estándares de aplicación.
4. Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
5. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente.
6. Publicar los certificados emitidos en un directorio, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
7. Revocar los certificados según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la CRL
8. Informar a los Suscriptores de la revocación o suspensión de sus certificados.
9. Publicar esta Política y las Prácticas correspondientes en su página Web.
10. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia.

11. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante perdida o destrucción o falsificación
12. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

I.6 Responsabilidad

EADTrust será responsable del daño causado ante la AC intermedia o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

1. la exactitud de toda la información contenida en el certificado de la AC intermedia en la fecha de su emisión.
2. la garantía de que, en el momento de la entrega del certificado, obra en poder de la AC intermedia, la clave privada correspondiente a la clave pública dada o identificada en el certificado.
3. la garantía de que la clave pública y privada funcionan conjunta y complementariamente.
4. la correspondencia entre el certificado solicitado y el certificado entregado.
5. Cualquier responsabilidad que se establezca por la legislación vigente.

I.6.1 Exoneración de responsabilidad

EADTrust no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

1. Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor
2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Política de Certificación.
3. Por el uso indebido o fraudulento de los certificados o ARL's emitidos por la Root .
4. Por el uso de la información contenida en el Certificado o en la ARL.
5. Por el incumplimiento de las obligaciones establecidas para la AC intermedia, el Suscriptor o Usuarios en la normativa vigente, las Políticas de Certificación o en las CPS's.
6. Por el perjuicio causado en el periodo de verificación de las causas de revocación.
7. Fraude en la documentación presentada por la AC intermedia.

Los servicios de certificación de EADTrust no han sido diseñados, autorizados o destinados para su aplicación en transacciones relacionadas con actividades que requieran funcionamiento a prueba de errores, como es el caso de:

- instalaciones nucleares,
- sistemas de navegación o tráfico aéreo,
- sistemas de comunicación o de control de armamento,
- sistemas de equipos médicos o de todo otro sistema digital en que un error pueda conducir a la muerte, a las lesiones de personas, o a daños ambientales.

EADTrust no será responsable en caso de producirse daños por el uso de sus servicios de certificación en ámbitos como los indicados en esta cláusula.

I.6.2 Límite de responsabilidad en caso de pérdidas por transacciones

No aplicable.

I.7 Responsabilidad financiera

Albalia Interactiva deberá disponer de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios

Las indemnizaciones cubiertas por EADTrust dependen del tipo de certificado,y están detalladas en las Políticas de Certificado (CP) correspondientes.

I.8 Interpretación y ejecución

I.8.1 Legislación

La ejecución, interpretación, modificación o validez de las presentes Políticas se regirá por lo dispuesto en la legislación española vigente.

I.8.2 Independencia

La invalidez de una de las cláusulas contenidas en esta Política de Certificación no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

I.8.3 Notificación

Cualquier notificación referente a la presente Política de Certificación se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

I.8.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

J. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

J.1 Autoridad de las políticas

El órgano de gobierno constituye la autoridad de las políticas (PA) y es responsable de la administración de las políticas.

J.2 Procedimientos de especificación de cambios

Cualquier elemento de esta política es susceptible de ser modificado.

Todos los cambios realizados sobre las políticas serán inmediatamente publicados en la web de EADTrust.

En la web de EADTrust se mantendrá un histórico con las versiones anteriores de las políticas.

Los usuarios afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la publicación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la PA.

Si un cambio en la política afecta de manera relevante a un número significativo de usuarios de la política, la PA puede discrecionalmente asignar un nuevo OID a la política modificada.

J.3 Publicación y copia de la política

Una copia de esta política estará disponible en formato electrónico en la dirección de Internet: http://policy.eadtrust.com

J.4 Procedimientos de aprobación de la CPS

La aprobación y autorización de una AC intermedia y sus políticas de certificación deberán respetar los procedimientos especificados la presente política y por la PA. Las partes de la política de certificación o CPS de una AC intermedia que contenga información relevante en relación a su seguridad, toda o parte de esa CPS no estará disponible públicamente.

K. ANEXO I. ACRÓNIMOS

AC	Autoridad de Certificación
AR	Autoridad de Registro
ARL	*Authority Revocation List.* Lista de certificados revocados de ACs intermedias
CPS	*Certification Practice Statement*. Declaración de Prácticas de Certificación
CRL	*Certificate Revocation List.* Lista de certificados revocados
CSR	*Certificate Signing Request.* Petición de firma de certificado
DES	*Data Encryption Standard*. Estándar de cifrado de datos
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm.* Estándar de algoritmo de firma
DSCF	Dispositivo seguro de creación de firma
DSADCF	Dispositivo seguro de almacén de datos de creación de firma
FIPS	*Federal Information Processing Standard Publication*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization.* Organismo Internacional de Estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso a directorios
OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PA	*Policy Authority.* Autoridad de Políticas
PC	Política de Certificación
PIN	*Personal Identification Number*. Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA-1	*Secure Hash Algorithm.* Algoritmo seguro de Hash

SSL *Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.

TCP/IP *Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

L. ANEXO II. DEFINICIONES

AC intermedia	Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Usuario, vinculando una determinada clave pública con una persona.
ARL	Es la lista que contiene los certificados de ACs intermedias revocados
Autoridad de políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las políticas de certificación y CPS.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes e identificación y registro de los solicitantes de un certificado.
Certificación cruzada	El establecimiento de una relación de confianza entre dos AC's, mediante el intercambio de certificados entre las dos en virtud de niveles de seguridad semejantes.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del suscriptor y es firmada por la AC.
Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada **datos de verificación de firma.**
Clave privada	Valor matemático conocido únicamente por el suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada **datos de creación de firma.** La clave privada de la AC será usada para firma de certificados y firma de CRL's

CPS	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
Entidad	Dentro del contexto de las políticas de certificación de ALBALIA Interactiva, aquella empresa u organización de cualquier tipo a la cual pertenece o se encuentra estrechamente vinculado el suscriptor.
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a. que los datos no han sido modificados (integridad) b. que la persona que firma los datos es quien dice ser (identificación) c. que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre si matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc, que componen un sistema basado en la creación y gestión de certificados de clave pública.

Política de certificación	Conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y de utilización comunes.
Suscriptor	Dentro del contexto de las políticas de certificación de ALBALIA Interactiva, persona cuya clave pública es certificada por la AC y dispone de una privada válida para generar firmas digitales.
Usuario	Dentro del contexto de las políticas de certificación de ALBALIA Interactiva, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado.