ECD_CO_1001.09_Política Servicio de Emisión de Certificados

Lleida SAS
Colombia - Bogotá

Control de documentación

Histórico de versiones

Versión	Fecha	Autor	Descripción
1	13/12/2022	Gloria Salvador	Versión inicial
1.1	03/05/2023	Gloria Salvador	Referencias acreditación ONAC
1.2	19/09/2023	Gloria Salvador	Corrección redactado

Lista de distribución

Empresa
Lleida SAS

Clasificación y estatus

Clasificación	Estatus
Uso Interno	Aprobado

Documentos referenciados

Descripción

Tabla de contenido

1. Introducción

1.1 Objetivo

Dar a conocer al público en general los lineaminentos establecidos por Lleida SAS para prestar el servicio de Servicio de Firma Centralizada como ECD de acuerdo con los establecido en la Ley 527 de 1999, Ley 1437 de 2011 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia, según corresponde al Certificado de Acreditación expedido por ONAC a Lleida SAS (22-ECD-009.pdf (onac.org.co)

1.2 Alcance

Todos los miembros de Lleida SAS, Entidad de Certificación Digital, así como todas las terceras partes identificadas en el alcance del Sistema de Gestión de la Entidad de Certificación Digital

1.3 Distribución

Aprobada por la Dirección de Lleida SAS, esta Política debe ser accesible a todas las personas incluidas en la lista de distribución especificada en el control documental, mediante los canales adecuados, establecidas en el procedimiento ECD_CO-3001 - Gestión del repositorio de documentación.

1.4 Revisión

La presente Política de Servicio será revisada y aprobada anualmente por parte del Comité de Seguridad de Lleida.net. No obstante, si tuvieran lugar cambios relevantes para la Organización, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento.

2. Consideraciones previas

LLEIDA S.A.S., es una EDC de acuerdo a lo establecido en la Ley 527 de 1999, Ley 1437 de 2011 y sus reglamentos.

Este documento contiene la Política y Declaración Prácticas Servicio de Emisión de Certificados y del Servicio de creación de firmas asociado a los emitidos en un dispositivo centralizado.

- La creación de firmas mediante sistemas de firma centralizada, en el cual LLEIDA S.A.S. gestiona en nombre del firmante su dispositivo de creación de firma permitiéndole generar firmas electrónicas cualificadas asegurando el control exclusivo del firmante sobre sus claves de firma, ya sea mediante mecanismos de autenticación más OTP (usuario y password y PIN OTP), huella dactilar o mediante el uso de la APP móvil eSignaID, de acuerdo a la especificación técnica ETSI TS 119 431-1.

El presente documento es un documento público cuyo contenido es de acuerdo a la especificación técnica ETSI TS 119 431-1 y define las políticas y prácticas en la provisión de los servicios de firma centralizada.

La Política está conforme con los siguientes lineamientos:

- Criterios específicos de Acreditración para las Entidades de Certificación Digital CEA 3.0-07 (en adelante CEA) que deben ser cumplidos para obtener la acreditación como ECD, ante el Organismo Nacional de Acreditación de Colombia (en adelante ONAC)
- Ley 527 de 1999

Emisión de certificados digitales en dispositivos locales o centralizados	1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles. 3 Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la ley 527 de 1999 9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas.	RSA 2048 bits para entidad final RSA 4096 bits para la CA raíz y subordinadas SHA-256 RFC 5280 MAYO 2008 (pdte checklist o herramienta) ITU-T-X509 V3 OCTUBRE 2012 (pdte checklist o herramienta, revisar versión) ETSI EN 319 411-1 V1.1.1 (2016- 02) (pdte checklist o herramienta; revisar versión) RFC 3647 NOVIEMBRE 2003 RFC 6960 JUNIO 2013 (pdte checklist o herramienta) FIPS 140-2 NIVEL 3. DICIEMBRE 2002 RFC 4523 Junio 2006 ETSI TS 102 042 Febrero 2013 ITU-T-X-500 Octubre 2019 ETSI EN 319 412-2 julio de 2020

2.2 PKI PARTICIPANTES

ENTIDAD DE CERTIFICACIÓN LLEIDA S.A.S. (ECD LLEIDA S.A.S.)

LLEIDA S.A.S., en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

DATOS DE LA ENTIDAD PRESTADORA DE SERVICIOS DE CERTIFICACIÓN LEGAL

Razón social:	LLEIDA S.A.S.
N.I.T.	900571038-3
Dirección:	Calle 81 # 11 – 55 Oficina 903
Ciudad/País	Bogotá/Colombia
Teléfono:	+5713819903
Correo electrónico:	co@lleida.net
Página web:	www.lleida.net/co
Nº Certificado Acreditación	22-ECD-009
Certificado Acreditación	22-ECD-009.pdf (onac.org.co)

ENTIDAD DE REGISTRO LLEIDA S.A.S. (RA LLEIDA S.A.S.)

LLEIDA S.A.S., brinda también los servicios de Autoridad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

Las funciones de RA podrán ser tercerizadas. En este caso la RA de LLEIDA S.A.S. evaluará el cumplimiento de sus políticas realizando evaluaciones internas que determinen su cumplimiento a dicho tercero.

La RA puede tercerizar las funciones de verificación y registro sin ningún límite ni restricción, siempre dejando claro que el responsable final es la RA, siempre que se asegure la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión (lo cual se realiza a través de nuestra plataforma de PKI. Sin embargo, la responsabilidad legal frente al Organismo de supervisión, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Autoridad de Registro. El tercero debe garantizar la seguridad y protección de los datos personales y confidenciales de la RA, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, re-emisión, durante la ejecución de las actividades de tercerización, quedando claro que ante el Organismo de supervisión el responsable ante terceros es la RA.

Cabe indicar que LLEIDA S.A.S. suministra al tercero la Plataforma de RA para la creación de la solicitud y la emisión de los certificados, asegurando la integridad en todo el proceso, accediendo a la plataforma eSignaPKI con el certificado digital del agente.

DATOS DE LA ENTIDAD DE REGISTRO

La entidad de registro es la misma prestadora de servicios de certificación digital o las entidades en las que terceriza el servicio.

PROVEEDOR DE SERVICIOS DE FIRMA CENTRALIZADA Y (LLEIDA S.A.S.)

LLEIDA S.A.S. actúa como proveedor del servicio de aplicación de firma centralizada (SSASP) y no delega ninguna parte del servicio a entidades terceras.

LLEIDA S.A.S. es una ECD que emite certificados y sellos electrónicos cualificados de acuerdo con la legislación vigente.

El servicio de SSASC forma parte de los servicios operados por LLEIDA S.A.S. y permite prestar el servicio de firma electrónica centralizada a los firmantes que cuentan con un certificado electrónico definido para firma centralizada en su correspondiente Declaración Prácticas Servicio de Firma Centralizada.

En el presente documento LLEIDA S.A.S. es identificado como el SSASP.

TITULAR

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos publicados en la DPC de LLEIDA S.A.S.

La figura de Titular será diferente dependiendo de los distintos certificados emitidos por LLEIDA S.A.S. conforme lo establecido en la Política de Certificación.

SUSCRIPTOR

El Suscriptor es la persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

SOLICITANTE

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la DPC de LLEIDA S.A.S.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación LLEIDA S.A.S. a un titular. El Tercero que confía, a su vez puede ser o no titular.

ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

OTROS PARTICIPANTES

EL COMITÉ DE SEGURIDAD

El comité de seguridad es un organismo interno de la Entidad de Certificación LLEIDA S.A.S., que tiene entre otras funciones la aprobación de la DPC y las políticas de servicios como documentos iniciales, así como autorizar los cambios o modificaciones requeridas sobre la DPC y las políticas de servicios aprobadas y autorizar su publicación. El Comité de Seguridad es el responsable de integrar la DPC y las políticas de servicios, a la DPC de terceros prestadores de servicios de certificación.

LLEIDA S.A.S., es una EDC de acuerdo a lo establecido en la Ley 527 de 1999, Ley 1437 de 2011 y sus reglamentos.

Este documento contiene la Política y Declaración Prácticas Servicio de Emisión de Certificados y del Servicio de creación de firmas asociado a los emitidos en un dispositivo centralizado.

- La creación de firmas mediante sistemas de firma centralizada, en el cual LLEIDA S.A.S. gestiona en nombre del firmante su dispositivo de creación de firma permitiéndole generar firmas electrónicas cualificadas asegurando el control exclusivo del firmante sobre sus claves de firma, ya sea mediante mecanismos de autenticación más OTP (usuario y password y PIN OTP), huella dactilar o mediante el uso de la APP móvil eSignaID, de acuerdo a la especificación técnica ETSI TS 119 431-1.

El presente documento es un documento público cuyo contenido es de acuerdo a la especificación técnica ETSI TS 119 431-1 y define las políticas y prácticas en la provisión de los servicios de firma centralizada.

2.3 Peticiones, Quejas, Reclamos, Solicitudes y apelaciones

Las peticiones, quejas reclamos, solicitudes y apelaciones sobre los servicios prestados por Lleida SAS seran atendidas por varios mecanismos a disposición del subscriptor y seran resueltas por las personas pertinentes e imparciales.

- Por correo electrónico a clientes@lleida.net . Deberá adjuntarse la plantilla disponible en www.lleida.net/co ECD_CO 4501 Plantilla PQRSA Lleida SAS

- Por teléfono al +57 1 381 9903

En el plazo máximo de 15 días deberán ser resueltas y notificadas, previa radicación, análisis y redacción de reporte formal que será entregado al subscriptor.

3. Administración de políticas

La administración de las Políticas de Servicios están a cargo del proceso de Sistema Integrado de Gestión

Persona de contacto

Nombre: Eva Pané Vidal
Cargo: Supervisor de la ECD
Teléfono de contacto: +57 1 381 9903
Correo electrónico: compliance@lleida.net

Las políticas deben ser aprobadas por el Comité de Seguridad, una vez aprobadas es responsabilidad el Supervisor de la ECD la actualización en los portales web en su última versión.

4. Certificados tramitados por la Autoridad de Registro

A continuación, se indican los certificados que son tramitados por la autoridad de Registro de LLEIDA.NET

Nombre del certificado	OID	OID QCP	QCP
Políticas de Certificación Certificados de Persona Natural	1.3.6.1.4.1.53589.1.1.1		
Persona Natural Software	1.3.6.1.4.1.53589.1.1.1.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Persona Natural Hardware	1.3.6.1.4.1.53589.1.1.1.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)

Persona Natural eSignaId	1.3.6.1.4.1.53589.1.1.1.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Persona Natural Centralizado UP	1.3.6.1.4.1.53589.1.1.1.3.2	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Persona Natural Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.1.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificados de Pertenencia a Empresa	1.3.6.1.4.1.53589.1.1.2		
Pertenencia a Empresa Software	1.3.6.1.4.1.53589.1.1.2.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa Hardware	1.3.6.1.4.1.53589.1.1.2.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa eSignaId	1.3.6.1.4.1.53589.1.1.2.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa Centralizado UP	1.3.6.1.4.1.53589.1.1.2.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Pertenencia a Empresa Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.2.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificados Representación de Empresa	1.3.6.1.4.1.53589.1.1.3		
Representación de Empresa Software	1.3.6.1.4.1.53589.1.1.3.1.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Representación de Empresa Hardware	1.3.6.1.4.1.53589.1.1.3.2.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Representación de Empresa eSignaID	1.3.6.1.4.1.53589.1.1.3.3.1	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)

Representación de Empresa Centralizado UP	1.3.6.1.4.1.53589.1.1.3.3.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Representación de Empresa Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.3.3.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificados de Función Pública	1.3.6.1.4.1.53589.1.1.3.5		
Función Pública Software	1.3.6.1.4.1.53589.1.1.3.5.1	0.4.0.194112.1.0	QCP-n (LLEIDA SAS SUB CA CO 001)
Función Pública Hardware	1.3.6.1.4.1.53589.1.1.3.5.2	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Función Pública eSignald	1.3.6.1.4.1.53589.1.1.3.5.3	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Función Pública Centralizado UP	1.3.6.1.4.1.53589.1.1.3.5.4	0.4.0.194112.1.2	QCP-n-qscd (Lleida SAS SUB CA CO 001)
Función Pública Centralizado Huella dactilar	1.3.6.1.4.1.53589.1.1.3.5.5	0.4.0.194112.1.2	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Políticas de Certificación Certificado de Jurídica	1.3.6.1.4.1.53589.1.1.3.4	0.4.0.194112.1.1	
Persona Jurídica Software	1.3.6.1.4.1.53589.1.1.3.4.1	0.4.0.194112.1.1	QCP-l-Sello electrónico (LLEIDA SAS SUB CA CO 001)
Persona Jurídica Hardware	1.3.6.1.4.1.53589.1.1.3.4.2	0.4.0.194112.1.1	QCP-n-qscd (LLEIDA SAS SUB CA CO 001)
Persona Jurídica Centralizado UP	1.3.6.1.4.1.53589.1.1.3.4.4	0.4.0.194112.1.1	QCP-n-qscd (Lleida SAS SUB CA CO 001)

4.1 Requisitos técnicos de los soportes

Los certificados expedidos en tokens y tarjetas criptográficas NO pueden utilizarse en computadoras con sistema operativo Mac OS.

4.2 Características técnicas de los soportes

El dispositivo homologado por Lleida SAS desde donde emitir certificados cualificados es el smart cafe expert 7.0 que cuenta con las siguientes certificaciones:

Certificado FIPs 140-2 level 3

NIST: Certificate #2628

FIPS 140-2 Consolidated Validation Certificate

Certificado common Criteria

5. Usos de los certificados

5.1 Usos adecuados del certificado

Los usos adecuados de los Certificados emitidos se encuentran especificado en la Política de Certificación de LLEIDA.NET

Los Certificados emitidos indicados en el apartado 2.6.2.1 Certificados emitidos por la Autoridad de Registro bajo esta DPC pueden ser utilizados con los siguientes propósitos:

- Identificación del Titular: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.
- Integridad del documento firmado: La utilización del Certificado garantiza que el documento firmado es integro, es decir, garantiza que el documento no fue alterado o modificado después de ser firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.
- No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.
- Cifrado asimétrico o mixto, basado en certificados X.509v3

5.2 Usos prohibidos del certificado y exclusión de responsabilidad

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta DPC y concretamente en las Políticas de Certificación.

Se consideran indebidos aquellos usos que no están definidos en esta DPC y en consecuencia para efectos legales, LLEIDA.NET queda eximida de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según esta DPC.

No se podrán emplear los Certificados de entidad final expedidos por LLEIDA.NET para:

- Firmar o sellar otro Certificado, salvo supuestos expresamente autorizados previamente.
- Firmar o sellar software o componentes a excepción de los Certificados de componente de firma de código
- Generar sellos de tiempo para procedimientos de Fechado electrónico a excepción de los Certificados expedidos por LLEIDA.NET para Unidades de Sellado de Tiempo.

6. PRÁCTICAS DEL PROVEEDOR DE SERVICIOS DE CONFIANZA PARA EL SERVICIO DE CREACIÓN DE FIRMAS Y FIRMA CENTRALIZADA

DISPOSICIONES GENERALES DE LA POLÍTICA DEL SERVICIO

LLEIDA S.A.S. en la prestación de su servicio de firma centralizada emplea dispositivos criptográficos de creación y protección de firmas catalogados como cualificados (QSCD).

Los HSM son operados de acuerdo con su certificación FIPS 140-2 y/o Common Criteria EAL 4+ y la solución SSASC empleada está alineada con los requisitos de seguridad definidos en la norma EN 419 241-1 para poder actuar como un Trustworthy System Supporting Server Signing (TW4S) con Sole Control Level 2 (SCAL2).

NOMBRE E IDENTIFICACIÓN

1. Para el servicio de firma centralizada LLEIDANET tiene asignado el OID: 1.3.6.1.4.1.53589.1.5.1

• La política es conforme a la política "NSCP: Normalized SSASC Policy" definida en ETSI TS 119 431-1 V1.1.1 que tiene asignado el siguiente OID: 0.4.0.19431.1.1.2.

• La política es conforme a la política "EUSCP: EU SSASC Policy" definida en ETSI TS 119 431-1 V1.1.1 que tiene asignado el siguiente OID: 0.4.0.19431.1.1.3.

LLEIDA S.A.S. revisa periódicamente la conformidad de sus políticas con respecto a la especificación ETSI TS 119 431-1 y cambiará el identificador de sus políticas ante cualquier cambio en las políticas definidas en la sección 4.3.2 de dicha especificación.

La Declaración de Prácticas de Servicios de LLEIDA S.A.S., las Políticas de servicio y Plan de Privacidad y otra documentación relevante son publicados en la siguiente dirección:

https://www.lleida.net/es/politicas-y-practicas

RESPONSABILIDAD DE PUBLICACIÓN Y DEPÓSITO

Véase apartado de la DPC.

INICIALIZACIÓN DE LAS CLAVES DE FIRMA

GENERACIÓN DE CLAVES DE FIRMA

El SSASC utiliza la aplicación de firma en servidor "eSignaCrypto" en combinación con un módulo criptográfico (HSM) que actúa como SCDev / QSCD, el cual es un dispositivo cualificado de creación de firma.

El SSASC utiliza HSMs con certificación FIPS PUB 140-2 y Common Criteria EAL 4+ para realizar todas las operaciones criptográficas con las claves de los firmantes.

Las claves de los firmantes son claves RSA con una longitud de clave de 2048 bits.

Fuera del módulo HSM las claves se almacenan cifradas con el algoritmo AES y una longitud de clave de 128 bits. La clave de cifrado es única y se deriva de una clave maestra del módulo HSM y de una clave de firmante derivada o del PIN de activación que es transportado cifrado dentro del SAD.

Las operaciones de administración del módulo criptográfico requieren de control dual.

Antes de generar el certificado del firmante el par de claves del firmante no se encuentran activas en el servicio de firma centralizada y el SSA no permite su uso.

Junto a la clave del firmante se genera una petición de certificado en formato CSR o PKCS #10 que sirve como prueba de posesión de la clave privada del firmante en el proceso de registro del certificado y emisión del certificado por parte de la Autoridad de Certificación.

ASOCIACIÓN DE LOS MEDIOS DE IDENTIFICACIÓN ELECTRÓNICA DEL FIRMANTE

El proceso de generación de claves se realiza durante el enrolamiento del usuario. Todo el proceso se encuentra cifrado mediante SSL y a nivel de aplicación. El proceso seguido es el siguiente:

1. El Agente de RA de LLEIDA S.A.S. se autentica en la RA empleando su certificado electrónico.

2. A continuación, toma los datos requeridos para crear la identidad digital del usuario. La Autoridad de Registro validará la identidad del firmante de acuerdo con los requisitos establecidos en la Declaración de Prácticas de Certificación del certificado solicitado por el firmante con un nivel de garantía alto según los requisitos establecidos en UE 2015/1502.

3. LLEIDA S.A.S. no delega el proceso de identificación y autenticación del firmante a terceras partes.

4. Una vez tomados los datos, se realiza un primer registro de la información que desencadena la creación de un token de seguridad (código único) de un solo uso, necesario para completar el proceso de generación de claves e identidad.

5. Una representación del token (código único) se envía por correo electrónico al Usuario, dependiendo del perfil empleado, representado con un código QR o código de activación. Dicho token es escaneado o introducido por el Usuario con su dispositivo móvil y la aplicación eSignaID en el caso de firma centralizada en eSignaID o desde un computador en el caso de firma centralizada con huella dactilar o usuario/password.

6. La aplicación solicita al Usuario que seleccione una Contraseña de seguridad que protegerá el material criptográfico. Dicha contraseña nunca viaja fuera del dispositivo móvil o computador del usuario ni se almacenará en la ECD.

7. Al elegir la Contraseña de seguridad se generan las claves criptográficas de dispositivo, un par de claves pública/privada, y se envía una solicitud a la ECD para iniciar el proceso de creación de identidad. La solicitud va firmada con la clave privada y la ECD verifica la solicitud y asocia la clave pública del dispositivo.

8. La ECD crea las claves pública y privada de identidad del usuario en el HSM FIPS 140-2 y catalogado como QSCD, siguiendo el protocolo interno de generación del HSM. Seguidamente, se desnaturaliza la clave privada. En el caso de firmas centralizadas con el perfil de eSignaID se crean 2 fragmentos A y B. El fragmento A se enviará cifrado al

celular para que se almacene de forma segura y el fragmento B se almacena en la base de datos de la PKI cifrado con la clave maestra del servicio de firma centralizada residente en el mismo HSM. En el caso de firmas centralizadas con el perfil de Usuario/password y huella dactilar, la clave privada se cifra con esta misma clave maestra del HSM y con el PIN que introduce el usuario con cifrado AES. Finalmente, la ECD devuelve los datos necesarios para crear el CSR o PKCS#10 (Certificate Signing Request), junto con el algoritmo de generación de claves y otros datos de control.

9. La identidad de firma se compone de un par de claves RSA con longitud 2048 y el certificado electrónico que vincula la clave pública a la identidad del firmante

10. Hasta la efectiva asociación del certificado con su correspondiente par de claves, la identidad de firma es incompleta y el SSASC no permitirá el uso de las claves.

11. El SAA emplea los datos para crear las claves pública y privada de identidad del usuario y generar el CSR que envía a la PKI.

12. La RA verifica el CSR y genera un certificado asociado a la solicitud. Finalmente devuelve el certificado al SAA

13. SAA almacena el certificado y desnaturaliza la clave privada de dispositivo e identidad del usuario. En el caso de firmas centralizadas con el perfil de eSignaID se crean 2 fragmentos A y B. El fragmento A se almacena cifrado en el celular de forma segura y el fragmento B se almacena de nuevo cifrado en la PKI en un HSM FIPS 140-2. En el caso de firmas centralizadas con el perfil de Usuario/password y huella dactilar, la clave privada se cifra con la clave maestra del HSM y con el PIN que introduce el usuario con cifrado AES.

14. Con este proceso se finaliza la generación y avisa a Agente y Usuario.

Para poder hacer uso de la identidad, en el caso de Firma Centralizada con eSignaID el Usuario debe contar con el celular empleado en el proceso de enrolamiento que contiene el fragmento A de material criptográfico, realizar una autenticación contra la PKI para recuperar el fragmento B y poder regenerar el material criptgráfico con el fragmento A almacenado en el dispositivo.

Este mecanismo protege al Usuario y su identidad de una forma novedosa, con autenticación de doble factor.

Se adjunta diagrama de secuencia con el proceso de generación de claves.

Para el caso de firma centralizada con usuario/password o Huella dactilar se sigue el siguiente proceso:

1. Durante la emisión del certificado (operación que está autenticada por el agente de registro), se establece un canal seguro SSL de comunicación entre eSignaDesktop y el servidor de PKI y Firma Centralizada, se crea una conexión segura del Web Service seguro y adicionalmente se genera un canal seguro a nivel de aplicación entre eSignaCentralizedSign Module y el HSM, empleando una clave derivada S1.

2. eSignaDesktop envía al servidor de Firma Centralizada la clave S1 y el Usuario y Password usando la clave pública de Firma Centralizada del HSM para proteger todo el contenido.

3. El servidor de Firma Centralizada entrega la información encriptada al HSM, el cual desencripta mediante su clave privada la información y la almacena durante la operación de generación.

4. El HSM cifra mediante su Master Key (MK HSM (AES-256)) de Firma Centralizada, el Usuario-Password y se almacena en la base de datos encriptada.

5. Se genera en HSM un UUID y se deriva una clave DUUID. Se cifra el UUID también con la MK y se almacena por separado en otra tabla de la base de datos y relacionándola con el registro del Usuario-Password encriptado.

6. En este momento se generan las claves pública y privada de Usuario y se crea el certificado, momento en el que se cifran mediante S1 y se envían al cliente.

7. El cliente desencripta las claves mediante S1 y deriva una clave a partir del PIN del Usuario, se procesa las claves públicas y privadas para eliminar información e inutilizarlas y posteriormente se encripta el resultado, generando K.

8. Una vez hecho esto se envía K encriptado al HSM mediante S1, que desencripta K y lo encripta mediante DUUID.

9. Se almacena el resultado en la base de datos encriptada y se destruye todo el material criptográfico temporal del HSM y del cliente eSignaDesktop.

No se delegan partes del proceso de identificación y autenticación del firmante a terceras partes.

El SSA almacena la clave pública de activación en los metadatos asociados al par de claves del firmante. El PIN de activación se utiliza como parte para derivar la clave de cifrado con la que se protegen las claves del firmante.

El SSA protege la integridad de las claves de los firmantes y sus metadatos asociados mediante el cómputo de una función HMAC.

ASOCIACIÓN DEL CERTIFICADO DEL FIRMANTE

La identidad de firma se compone de un par de claves RSA con longitud 2048 y el certificado electrónico que vincula la clave pública a la identidad del firmante.

Hasta la efectiva asociación del certificado con su correspondiente par de claves, la identidad de firma es incompleta y el SSASC no permitirá el uso de las claves.

El SSASC solicitará al dispositivo QSCD la generación del par de claves de los firmantes antes de la emisión del certificado electrónico. Como requisito previo a la generación de las claves, el firmante deberá establecer el PIN/contraseña de activación de firma.

Así mismo, el SSASC solicitará a la correspondiente Autoridad de Certificación la emisión del certificado, el cual se pondrá a disposición del firmante a través del Portal de Gestión de Identidades.

El SSASC verifica que el certificado del firmante y la clave pública almacenada en el sistema se corresponden. En caso de que ambas claves públicas coincidan, el certificado queda vinculado al par de claves del firmante, completando la identidad de firma. La clave del firmante queda a partir de este momento operativa para realizar operaciones de firma.

La integridad de cada identidad de firma se garantiza mediante la firma electrónica de cada registro en el repositorio donde se almacenan.

REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LAS CLAVES DE FIRMA

ACTIVACIÓN DE LAS CLAVES DE FIRMA

El módulo SAM dentro del entorno protegido aplicará el control de acceso del usuario sobre sus claves de firma. Esto se materializará por medio de un protocolo de activación de la firma (SAP, Signature Activation Protocol) con el que se generará unos datos de activación de firma (SAD, Signature Activation Data) sobre los que el SAM aplicará las condiciones de acceso al material de firma en el QSCD, lo cual se realizará mediante la aplicación móvil eSignaID o eSignaDesktop

Las claves del firmante solo se pueden activar dentro del módulo HSM. La clave de un firmante sólo se podrá activar si completa el protocolo de activación autenticándose con sus credenciales de identidad, mediante su usuario/password, su huella dactilar o eSignaID según sea el caso. En todos los casos, la activación de las claves de firma requerirá el PIN/contraseña de firma, establecido previamente por el firmante.

El protocolo de activación de firma (SAP) está diseñado para prevenir ataques de man-in the middle y replay. Además de esto el mensaje SAD incorpora protecciones contra suplantación, robo de sesión, duplicación, robo de credenciales, phishing y adivinación, mediante la combinación de técnicas de cifrado, firma electrónica, funciones resumen, incorporación de números aleatorios y uso de dos factores de autenticación de diferente naturaleza.

Todas las comunicaciones con el SSASC son protegidas mediante el protocolo TLS 1.2.

Los controles de acceso implementados en el SSA garantizan que un firmante no tiene acceso las claves de otros firmantes ni a otros objetos y funciones del sistema que no sean las funciones de firma, ya que éstas se encuentran cifradas con el SAD introducido por el usuario y que sólo conoce él, además de por la MASTERKEY del HSM.

Una vez se activa la clave del firmante el SSASC solo permite un único uso para firmar el resumen criptográfico contenido en el mensaje SAD utilizado para la activación. Tras la realización de la operación de firma solicitada, se requerirá un nuevo SAD para generar una nueva firma.

Las claves de los firmantes se almacenan cifradas en la base de datos del SSA utilizando el algoritmo de cifrado AES y una longitud de clave de 256 bits. La clave de cifrado para cada clave y firmante es diferente y se deriva a partir de una clave maestra del módulo criptográfico y el PIN/contraseña de activación de clave que establece el firmante.

El SSA permite generar firmas electrónicas con el algoritmo RSA PKCS#1 v1.5 y algoritmo resumen SHA-256.

GESTIÓN DE LOS DATOS DE ACTIVACIÓN DE FIRMA

El mensaje con los datos de activación de firma (SAD) es generado en la aplicación SAA instalada en el teléfono inteligente del firmante o en la aplicación eSignaDesktop instalado en el computador del usuario.

El mensaje del SAD contiene el resumen(es) criptográfico(s) de los datos a firmar, referencias que permiten identificar la clave seleccionada e identificar al firmante, el PIN de activación de firma cifrado. Todo el mensaje del SAD se firma con la clave privada de activación de firma en la aplicación SAA para autenticar al firmante.

El SSASC solo permite que el firmante pueda utilizar su clave de activación de firma desde un único teléfono inteligente evitando así su duplicado.

La combinación de dos factores de autenticación de diferente naturaleza, la clave de activación y el PIN de activación, aseguran que el firmante tiene control exclusivo de sus datos de activación de firma.

El SAP consiste en la transmisión de un solo mensaje SAD a través de un canal seguro hasta el SSA. El módulo de activación de firma (SAM) es un sub-modulo del SSA.

BORRADO DE LAS CLAVES DE FIRMA

Las claves del firmante son borradas de forma inmediata, cuando el certificado del firmante es revocado.

Periódicamente LLEIDA S.A.S. ejecuta un proceso de borrado de la base de datos de aquellas claves de los firmantes cuyo certificado asociado ha caducado.

Los firmantes podrán solicitar la revocación de su certificado electrónico siguiendo los mecanismos establecidos en la Declaración de Prácticas de Certificación correspondiente. La revocación y caducidad del certificado supone en todos los casos la destrucción las claves asociadas.

COPIA DE SEGURIDAD Y RESTAURACIÓN DE LAS CLAVES DE FIRMA

Se mantienen copias de seguridad periódicas de la base de datos donde se encuentra las claves de los firmantes, y del resto de claves de infraestructura necesarias para garantizar la continuidad del servicio en caso de incidente. El número de copias de seguridad es el mínimo para garantizar la continuidad del servicio.

Las claves de infraestructura del SSASC son siempre almacenadas en contenedores cifrados.

El módulo criptográfico que contiene la clave maestra del SSASC que protege las claves de todos los firmantes requiere de control dual para su operación, copia de seguridad y restauración. La clave maestra del SSASC nunca abandona el módulo criptográfico en claro.

CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

Véase punto CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIÓN de la DPC.

GENERACIÓN DE REGISTROS

Se registran todos los eventos significativos de seguridad, incluyendo en cada registro la fecha y hora exacta de su realización, la cual no debe estar posibilitada de ser eliminada ni modificada del registro.

Los sistemas permiten la generación de los siguientes registros:

a) Intentos fallidos y exitosos de inicializar un usuario, renovar, habilitar, deshabilitar y actualizar o recuperar usuarios.

b) Intentos fallidos o exitosos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema, intentos de entrada y salida del sistema.

c) Intentos no autorizados de acceso a los registros o bases de datos del sistema.

d) Encendido y apagado del sistema principal.

El registro de auditoria de eventos debe registrar la hora, fecha e identificadores software y hardware.

Los registros generados durante la ejecución de los servicios, como son los cambios en la configuración, el personal e incidentes de acceso físico, deben ser gestionados por las organizaciones cliente que utiliza los sistemas de la SVA.

Compete a las organizaciones cliente la revisión, mantenimiento y protección del archivo de registros, así como los procesos de auditoría de estos registros.

PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

Véase apartado Procedimientos de registro de auditoría de la DPC. Además, en particular, en la prestación del servicio de firma electrónica en servidor:

1. El SSA guarda registro, al menos, de los siguientes eventos: - Inicialización de sistema, arranque, parada y cambios de configuración. - Eventos de gestión de claves del firmante (generación, activación, uso, desactivación y destrucción) - Uso de claves de los firmantes. - Autenticación de los firmantes (incluyendo intentos fallidos). - Gestión de los datos de activación de firma del firmante (cambios de PIN/contraseña) - Accesos al sistema por parte de los usuarios administradores.

2. El SSA genera un registro de auditoría continuo en el que solo es posible añadir nuevos eventos y no es posible eliminar o modificar los eventos anteriores. 61. El SSA

protege los eventos del registro de auditoría a nivel de entrada y de todo el registro aplicando una función HMAC que encadena cada registro con el anterior.

3. Todos los registros de eventos del registro de auditoría del SSA incluyen la siguiente información: - Fecha y hora del evento. - Tipo de evento. - Identidad de la entidad (firmante, administrador o proceso) responsable de la acción. - Resultado del evento (éxito o error)

4. El SSA comprueba en el arranque y periódicamente la integridad del registro de auditoría para detectar el borrado o modificación. Adicionalmente el SSA dispone de una funcionalidad para verificar la integridad del registro de auditoría a petición de un usuario con rol de auditor en el sistema.

5. Para garantizar la precisión de la fecha y hora de los eventos de auditoría el reloj de los sistemas se encuentra sincronizado por NTP utilizando como referencia el ROA (Real Observatorio de la Armada). Existen controles para detectar problemas que puedan comprometer la sincronización.

ARCHIVO DE REGISTROS

Véase apartado Procedimientos de registro de auditoría de la DPC.

RECUPERACIÓN FRENTE AL COMPROMISO Y DESASTRE

LLEIDA S.A.S. proporciona servicios de soporte de segundo nivel para la gestión de incidentes y recuperación de los sistemas de software que sustentan los servicios.

Corresponde a las organizaciones clientes, la implementación del Plan de Contingencias para el soporte del primer nivel y la recuperación en caso de incidentes en la infraestructura de hardware, firmware, comunicaciones y entorno.

CONTROLES DE SEGURIDAD TÉCNICA

GESTIÓN DE LOS SISTEMAS DE LA SEGURIDAD

El SSA implementa los siguientes roles de gestión:

- Responsable de seguridad (security officer): tiene la responsabilidad general de administrar e implementar las políticas de seguridad y tiene acceso a la información de seguridad.

- Administrador del sistema (system administrators): es el responsable de instalar, configurar y mantener el TW4S pero con acceso controlado a la información de seguridad.

- Operador del sistema (system operators): es el responsable de la operación del día a día del TW4S y las operaciones de copia de seguridad y restauración.

- Auditor del sistema (system auditor): está autorizado para revisar los archivos y registros de auditoría del TW4S para auditar que las operaciones del sistema están alineadas con la política de seguridad.

LLEIDA S.A.S. asigna estos roles a personal cualificado e implementa todos los controles de segregación de funciones definidos en la sección 6.2.1.2 de la norma CEN EN 419 241-1. 6.5.2.

OPERACIONES Y SISTEMAS

La entidad dispone de procedimientos para operar de forma correcta y segura el SSASC.

El componte software SSA y el módulo HSM son operados de acuerdo con sus manuales para su instalación, administración y operación para cumplir con los objetivos de seguridad definidos su certificación como dispositivo QSCD.

CONTROLES DE SEGURIDAD INFORMÁTICA.

Véase apartado de la DPC

GESTIÓN DE CICLO DE VIDA DE LAS CLAVES: (SISTEMAS AUTOMATIZADOS)

En relación a los controles de seguridad (generación e instalación de par de claves, protección de clave privada y controles de ingeniería de los módulos criptográficos, datos de activación, controles técnicos de ciclo de vida, ...) se encuentran ampliamente desarrollados en la DPC

GENERACIÓN DE LAS CLAVES

La Generación de las claves de firma del sistema automatizado deberá ser realizada en un ambiente asegurado físicamente, por personal que ocupa roles de confianza, bajo al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA.

La generación de la clave de firma del sistema automatizado deberá ser realizada en un módulo criptográfico que:

- Cumpla con los requerimientos FIPS 140-2 o Common Criteria EAL 4+
- Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2)

El algoritmo de generación, la longitud de la clave firma y el algoritmo de firma usado para firmar los sellos de tiempo deberán ser reconocidos por el Organismo supervisor.

PROTECCIÓN DE LA CLAVE PRIVADA

La clave privada de firma permanece confidencial y que se mantiene su integridad. La clave de firma del sistema automatizado estará protegida en un módulo criptográfico que:

- Cumpla con los requerimientos FIPS 140-2 o Common Criteria EAL 4+,
- Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2)

Si se realiza un respaldo de la clave de firma, esta deberá ser copiada, almacenada y recuperada sólo por personal que ocupa roles de confianza, usando al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA.

Cualquier copia de la clave deberá ser protegida por la clave secreta del módulo criptográfico antes de ser almacenada fuera del dispositivo.

DISTRIBUCIÓN DE LA CLAVE PUBLICA

La clave pública de firma debe ser disponible para los terceros que confían en un certificado de clave pública.

El certificado puede ser emitido por la misma entidad que opera el SVA o por otra ECD reconocida por el Organismo supervisor.

El certificado debe ser emitido por una ECD bajo una política que provea un nivel de seguridad equivalente o superior a la DPSVA.

Este certificado deberá ser reconocido por el Organismo supervisor.

RE-EMISIÓN DE LA CLAVE

El tiempo de vigencia del certificado no debe ser mayor que el periodo de vigencia de los algoritmos y tamaños de claves, conforme al reconocimiento del Organismo supervisor.

TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA

Las claves privadas no pueden ser usadas tras la expiración de su ciclo de vida:

a. Se establecen procedimientos técnicos u operacionales para asegurar que son generadas y utilizadas nuevas claves.

b. La clave privada de firma, o cualquier parte de la clave será destruida de tal modo que no pueda ser recuperada.

c. El sistema de generación de sellos de tiempos debe rechazar cualquier intento de emitir sellos de tiempo si la clave privada de firma ha expirado o se encuentra revocada.

CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

Durante la Gestión del ciclo de vida del módulo criptográfico se cumple que:

- El hardware del módulo criptográfico no debe ser manipulado durante su transporte.

- El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento.

- La instalación, activación y duplicación de la clave de firma en el hardware del módulo criptográfico deberá ser realizado solo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro.

- El hardware de firma de sellos de tiempo funciona correctamente.

- Las claves de firma que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado.

7. Mapa de controles

Norma	Apartado
CEA- 3.0-07	10.11