PROCEDIMIENTOS OPERACIONALES MÍNIMOS PARA ORGANIZACIONES QUE REQUIERAN EL ALMACENAMIENTO DE CLAVES PRIVADAS

DE LA

PKI - Paraguay

LIZ ROSANNA CRAMER CAMPOS

Firmado digitalmente por LIZ ROSANNA CRAMER CAMPOS
Fecha: 2020.09.30 16:55:31 -04'00'

DOC-PKI-09

Versión 1.0

Control de Cambio

Documento	
Título: PROCEDIMIENTOS OPERACIONALES MÍNIMOS PARA ORGANIZACIONES QUE REQUIERAN EL ALMACENAMIENTO DE CLAVES PRIVADAS DE LA PKI - Paraguay	**Nombre Fichero:**DOC-PKI-09 V1.0
Código: DOC-PKI-09	**Soporte Lógico:** https://www.acraiz.gov.py
Fecha: 30/09/2020	**Ubicación Física:** DGFDyCE
Versión: 1.0	

Registro de Cambios		
Versión	**Fecha**	**Motivo de Cambio**
1.0	30/09/2020	Versión Inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
Autoridad Certificadora (CA)	Prestadores de Servicio de Certificación (PSC)
Documento Público	https://www.acraiz.gov.py

Control del Documento		
Elaborado por:	**Verificado por:**	**Aprobado por:**
JENNY ELIZABETH RUIZ DIAZ LEZCANO Digitally signed by JENNY ELIZABETH RUIZ DIAZ LEZCANO Date: 2020.09.30 14:19:06 -04'00'	MARIA LUJAN OJEDA CHAMORRO Firmado digitalmente por MARIA LUJAN OJEDA CHAMORRO Fecha: 2020.09.30 15:24:11 -04'00'	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO Fecha: 2020.09.30 15:37:30 -04'00'
JENNY RUÍZ DÍAZ	***LUJAN OJEDA***	***LUCAS SOTOMAYOR***

Contenido

1 - DESCRIPCIÓN GENERAL 4

1.1. DEFINICIONES, SIGLAS Y ACRÓNIMOS 5

1.1.1 DEFINICIONES 5

1.1.2 SIGLAS Y ACRÓNIMOS 8

2 - REQUISITOS PARA ALMACENAMIENTO DE CLAVES PRIVADAS 9

2.1 ALMACENAMIENTO DE CLAVES PRIVADAS Y CERTIFICADOS DIGITALES. 9

2.2 MECANISMO DE AUTENTICACIÓN PARA ACCESO A LA CLAVE PRIVADA 10

2.3 PROTOCOLOS 11

2.4. REQUISITOS PARA SERVICIOS DE USO DE CLAVES PRIVADAS 11

2.4.1. DEFINICIONES PARA LA INTERFAZ DE LOS SERVICIOS 11

2.4.2 LISTA DE SERVICIOS PROPORCIONADOS POR LA ORGANIZACIÓN 12

2.4.3. AUTORIZACIÓN Y AUTENTICACIÓN PARA SOLICITUD DE SERVICIOS. 13

3. SERVICIO DE FIRMA DIGITAL Y VERIFICACIÓN DE FIRMA DIGITAL 14

3.1. INTRODUCCIÓN 14

3.2. CREACIÓN DE FIRMAS 14

3.3. DISPOSITIVOS PARA LA CREACIÓN DE FIRMAS 15

3.4. INTERFAZ DE APLICACIÓN CON EL DISPOSITIVO DE CREACIÓN DE FIRMA. 15

3.5. SUITES DE FIRMA 16

3.6. FORMATOS DE FIRMA 16

3.7. LA FIRMA CON EL SELLO DE TIEMPO 16

3.8. VALIDACIÓN DE FIRMAS 17

4 - REFERENCIAS 18

4.1 REFERENCIAS 18

4.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay 19

1 - DESCRIPCIÓN GENERAL

El objetivo de este documento es regular los requisitos mínimos de seguridad y los procedimientos operacionales que deben adoptar las Organizaciones que requieran el almacenamiento de claves privadas de la PKI-Paraguay correspondientes a sus empleados o funcionarios.

El almacenamiento referido en el párrafo anterior, deberá exclusivamente realizarse en hardware criptográfico tipo HSM el cual deberá ser de propiedad o estar bajo el control de la Organización y atender las aplicaciones demandadas por ella, con acceso exclusivo por medio de una red interna. El almacenamiento de claves privadas de los empleados o funcionarios de la Organización deberá corresponder a certificados con datos adicionales relacionados a dicha organización. La Organización podrá almacenar en dicho HSM su clave privada y su certificado digital correspondiente.

Complementa, para estas Organizaciones, los reglamentos contenidos en los documentos DOC-PKI-03 [1], DOC-PKI-04 [2] y DOC-PKI-06 [3].

El cumplimiento de los requisitos aplicables a la Organización, contenidos en este documento deberán ser acreditados por el PSC emitente de los certificados.

La Organización debe utilizar sistemas y productos fiables, incluidos canales de comunicación electrónicos seguros, aplicar procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea confiable y que los datos de creación de firma se utilicen bajo el control exclusivo del titular del certificado. Además, deben custodiar y proteger los datos de creación de firma frente a cualquier alteración, destrucción o acceso no autorizado así como garantizar su disponibilidad.

El dispositivo HSM debe estar homologado por el MIC y para el efecto deberán considerarse las disposiciones aplicables de este documento y la norma DOC-PKI-06 [3], sea el caso para almacenamiento de claves privadas de usuarios finales, para creación de firma o ambos.

Este documento define los estándares operacionales y de seguridad que deberán ser aplicadas por la Organización, para el almacenamiento de claves privadas y en los servicios de firma digital y verificación de firma digital.

A continuación, serán informados los requisitos que deben ser observados en términos mínimos para el almacenamiento de claves privadas y servicios de firma digital y verificación de firma digital.

1.1. DEFINICIONES, SIGLAS Y ACRÓNIMOS

1.1.1 DEFINICIONES

1) **Autenticación:** proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por ésta, y al cual se le vincula. Este proceso no otorga certificación notarial ni fe pública.

2) **Autoridad de Aplicación:** Ministerio de Industria y Comercio a través de la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio y Servicios.

3) **Autoridad de Certificación:** entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI-Paraguay, son Autoridades de Certificación, la CA Raíz-Py y el PSC.

4) **Autoridad de Certificación Raíz del Paraguay:** órgano técnico, cuya función principal es coordinar el funcionamiento de la PKI-Paraguay. La CA Raíz-Py tiene los certificados de más alto nivel, posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza. Las funciones de la CA Raíz-Py son ejercidas por la AA.

5) **Certificado Digital:** es un documento electrónico, generado y firmado por una CA legalmente habilitada para el efecto, el cual vincula un par de claves con una persona física o jurídica confirmando su identidad.

6) **Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido de manera que sólo pueda leerlo la persona que disponga de la clave del cifrado adecuada para decodificarla.

7) **Claves criptográficas**: valor o código numérico que se utiliza con un algoritmo criptográfico para transformar, validar, autenticar, cifrar y descifrar datos.

8) **Datos de activación:** valores de los datos, distintos al par de claves, que son requeridos para operar los módulos criptográficos y que necesitan estar protegidos.

9) **Declaración de Prácticas de Certificación:** declaración de las prácticas que emplea una CA al emitir certificados y que define la infraestructura, políticas y procedimientos que utiliza la CA para satisfacer los requisitos especificados en la CP vigente.

10) **Emisión de certificado:** es la autorización de la emisión del certificado en el sistema del PSC previa comprobación de la concordancia de los datos de solicitud del certificado con los contenidos en los documentos presentados.

11) **Firma Digital:** es una firma electrónica certificada por un prestador habilitado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincula únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.

12) **Infraestructura de Clave Pública:** es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consultas de vigencia y validez de los mismos.

13) **Integridad:** característica que indica que un mensaje de datos o un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

14) **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas.

15) **Módulo de Seguridad de Hardware:** dispositivo basado en un módulo criptográfico tipo hardware que genera, almacena y protege claves criptográficas.

16) **Normas Internacionales:** requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

17) **No Repudio:** refiere que la posesión de un documento electrónico y la firma digital asociada al mismo será prueba efectiva del contenido y del autor del documento.

18) **Política de Certificación:** documento en el cual la CA, define el conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad particular y/o una clase de aplicaciones con requisitos comunes de seguridad.

19) **Organización**: es una entidad pública o privada que acredita las condiciones ante un PSC, para prestar servicios de almacenamiento de claves privadas, así como para prestar servicios de firma digital y de verificación de firmas digitales en documentos y transacciones electrónicas, para usuarios finales que se constituyen en empleados o funcionarios de la organización.

20) **Prestador de Servicios de Certificación:** entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI-Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz-Py y solo podrá emitir certificados a usuarios finales.

21) **Solicitante de Certificado:** persona física o jurídica que solicita la emisión de un certificado a una CA.

22) **Solicitud de Firma de Certificado:** petición de certificado digital que se envía a la CA. Mediante la información contenida en el CSR, la CA, puede emitir el certificado digital una vez realizadas las comprobaciones que correspondan.

23) **Suscriptor:** persona física o jurídica titular de un certificado digital emitido por una CA. Un suscriptor puede ser un PSC o un usuario final.

24) **Usuario final:** persona física o jurídica que adquiere un certificado digital de un PSC.

25) Verificación de firma: determinación y validación de que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su firma digital fue creada.

1.1.2 SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla / Acrónimo	Descripción
CA	Autoridad de Certificación (CA por sus siglas en inglés Certificate Authority)
CAdES	CMS Advanced Electronic Signature
CA Raíz-Py	Autoridad Certificadora Raíz del Paraguay
CSR	Solicitud de firma de Certificado (CSR por sus siglas en inglés, Certificate Signing Request)
CI	Cédula de Identidad
HSM	Módulo de seguridad criptográfico basado en Hardware (HSM por sus siglas en inglés, Hardware Security Module)
MIC	Ministerio de Industria y Comercio
PAS	Pasaporte
PAdES	PDF Advanced Electronic Signatures
PKCS	Norma de criptografía de clave pública (PKCS por sus siglas en inglés, Public Key Cryptography Standard)
PKI	Infraestructura de Clave Pública (PKI por sus siglas en inglés, Public Key Infrastructure).
PKI-Paraguay	Infraestructura de Claves Públicas del Paraguay
PSC	Prestador de Servicios de Certificación
Py	Paraguay

RFC	Petición de Comentarios (RFC por sus siglas en inglés, Request For Comments)
RUC	Registro Único del Contribuyente
TLS	Capa de conexión segura (TLS por sus siglas en inglés, Transport Layer Security)
TOTP	Time-based One-Time Password algorithm
XAdES	XML Advanced Electronic Signatures
XML	eXtensible Markup Language

2 - REQUISITOS PARA ALMACENAMIENTO DE CLAVES PRIVADAS

2.1 ALMACENAMIENTO DE CLAVES PRIVADAS Y CERTIFICADOS DIGITALES.

Las claves privadas de los usuarios finales, para los certificados del Tipo F3 o C3 obligatoriamente deben ser generados y almacenados en hardware criptográficos tipo HSM. Las mismas deben estar almacenadas dentro de los espacios de la frontera criptográfica, o equivalente dentro del contexto de seguridad del HSM. Se exige que las claves sean activadas y utilizadas únicamente dentro del hardware físico de dicho HSM bajo control exclusivo del usuario titular del certificado.

Los HSM deben presentar esquema de gestión de claves apto para, además de proteger las mismas, asegurar el intercambio de información a través de un marco de seguridad.

Los HSM deberán cumplir los siguientes requisitos:

1) garantizar como mínimo, por medios técnicos y de procedimiento adecuados, que:
   a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma utilizados para la creación de firmas digitales;
   b) los datos de creación de firma utilizados para la creación de firma digital sólo puedan aparecer una vez en la práctica;

c) exista la seguridad razonable de que los datos de creación de firma utilizados para la creación de firma digital no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la Tecnologías disponible en el momento; y

d) los datos de creación de la firma utilizados para la creación de firma digital puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.

2) No alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

Los espacios para el almacenamiento de las claves privadas de los usuarios finales podrán ser liberados desde que no haya renovación por parte del usuario o revocación de las claves.

La Organización y el PSC deberán documentar cuales son los procedimientos concretos que pone en práctica para garantizar que la clave privada del Solicitante fue generada en su módulo criptográfico (HSM) de custodia centralizada, y que el titular tiene el control exclusivo del mecanismo de autenticación que protege el uso de su clave privada generada.

2.2 MECANISMO DE AUTENTICACIÓN PARA ACCESO A LA CLAVE PRIVADA

El acceso a las claves privadas de los usuarios debe ser de uso, conocimiento y control exclusivo del titular del certificado, sin la posibilidad de ingreso por parte de otros titulares en el mismo HSM, cualquier empleado/funcionario de la Organización o dependiente de otras claves criptográficas.

La Organización debe proporcionar mecanismos de por lo menos 1 (un) factor de autenticación al titular del certificado para el acceso a su clave privada, debiendo ser dentro del límite de la frontera criptográfica del HSM.

El mecanismo de autenticación deben emplear un método o protocolo de validación que proteja los datos de transmisión y los datos de autenticación por medio de criptografía y los siguientes requisitos técnicos:

i. Usuario y contraseñas: de acuerdo con las reglas que establezca la CA Raíz-Py;

ii. PIN de firma (PIN/PUK): de acuerdo con las reglas que establezca la CA Raíz-Py;
iii. OTP: de acuerdo con las reglas de RFC 6238 (TOTP), RFC 6287, RFC 4226 (HOTP);
iv. Biometría: de acuerdo con las reglas que establezca la CA Raíz-Py; o
v. Otras autenticaciones semánticas de acuerdo con este documento y previamente aprobadas por CA Raíz-Py.

2.3 PROTOCOLOS

Los HSM homologados por el MIC deben soportar una interfaz PKCS#11 o similar, atendiendo las exigencias de especificación de la CA Raíz-Py y además de los informados en este documento, cumpliendo con los siguientes requisitos generales:

a) ejecutar los algoritmos que sean parte de las funciones *core* de una firma digital en forma interna al hardware del HSM;
b) generar y destruir claves simétricas y asimétricas en forma interna al hardware del HSM;
c) activar y desactivar claves en forma interna al hardware del HSM cuando su titular lo autorice;
d) proteger las claves privadas y sólo habilitar su activación y uso en forma interna del hardware del HSM; y
e) habilitar el uso de punteros, manejadores, alias o tokens de claves privadas a las aplicaciones que se conecten, evitando el uso directo de las mismas en claro desde el exterior en forma interna al hardware del HSM.

Los HSM homologados por el MIC podrán soportar el Protocolo KMIP (Key Management Interoperability Protocol), versión 1.3 o superior o otras de acuerdo con este documento y previamente aprobadas por CA Raíz-Py.

2.4. REQUISITOS PARA SERVICIOS DE USO DE CLAVES PRIVADAS

2.4.1. DEFINICIONES PARA LA INTERFAZ DE LOS SERVICIOS

Deberá ser utilizado el protocolo TLS, definido por RFC 5246 o su versión actualizada, para la comunicación con los servicios.

Deberá ser utilizado el framework OAuth 2.0 (RFC 6749 y RFC 7636) para la implementación de la interfaz con los servicios del PSA.

Adicionalmente, podrá ser implementada otra interfaz para servicios, siempre que se proporcione el software necesario para permitir al titular utilizar sus claves privadas de forma segura.

2.4.2 LISTA DE SERVICIOS PROPORCIONADOS POR LA ORGANIZACIÓN

a) Servicios Obligatorios

1) Servicio de autorización:

I. Código de Autorización (Authorization Code Request): servicio para obtener del Titular del Certificado la autorización de uso de su clave privada o autorizar una autenticación sin uso la clave privada.

II. Token de Acceso: después de obtener el código de autorización, el Token de Acceso debe ser solicitado. Los tokens de acceso son credenciales que se utilizan para acceder o utilizar recursos protegidos por el Titular, como ser datos de información u otros atributos del titular, incluyendo sus datos de creación de firmas;

2) Firma: servicio de firma digital conforme al ítem 6, para el cual deberá tener un token de acceso válido; y

3) Registro de Aplicaciones: servicio de registro de una aplicación en la Organización a través de un servicio o una operación administrativa en la plataforma.

b) Servicios Opcionales

1) Recuperación de Certificado: servicio para recuperar un certificado almacenado en la Organización. La aplicación deberá tener un token de acceso válido;

2) Localización del Titular: servicio para encontrar a un titular a través del número CI, PAS o RUC; y

3) Autorización con credencial de titular: servicio para obtener autorización del titular del certificado para utilizar su clave privada, con solicitud de factores de autenticación.

2.4.3. AUTORIZACIÓN Y AUTENTICACIÓN PARA SOLICITUD DE SERVICIOS.

La Organización deberá disponibilizar los servicios web (o APIs web) de autorización y autenticación atendiendo a la finalidad de sus funciones.

Dichos servicios son consumidos por las aplicaciones cliente de firma.

2.4.3.1. Flujo básico para Uso de Servicios de confianza.

a) Seguido del flujo de autorización establecido por el RFC 6749, el uso de claves privadas en la Organización deberá ir precedido de una solicitud exitosa, por parte de las aplicaciones. Este requerimiento se aplica para los siguientes servicios:
   - Servicios de Autorización (Código de Autorización y Token de Acceso); y
   - Firma.

b) Cuando fuera necesario utilizar un servicio destinado únicamente a la autenticación del titular, es decir, sin el uso de una clave privada, deberá ir precedido de una solicitud exitosa, por parte de las aplicaciones. Este requerimiento se aplica para los siguientes servicios:
   - Servicios de Autorización (Código de Autorización y Token de Acceso); y
   - Recuperación de certificado.

2.4.3.2. Tránsito de los Factores de Autenticación.

Se deberán implementar los mecanismos de autenticación contemplando los requerimientos de acceso exclusivo a clave del titular del certificado según indicado en el presente documento.

Las aplicaciones no deberán recopilar factores de autenticación del titular del certificado. Para este fin, La Organización deberán comunicarse directamente con el equipo o sistema del titular, previamente identificado y registrado en la Organización de forma segura.

El Servicio de "*Autorización con Credencial*" *de* Titular se encuentra exento de esta regla.

2.4.3.3. Autenticación de aplicaciones de Firma.

Para que una aplicación pueda utilizar los servicios de la Organización tiene que solicitar el registro en la plataforma de firma y obtener un mecanismo de acceso para su conexión. Por tanto, en cuanto a la autenticación de aplicaciones de firma: para obtener acceso a los servicios de confianza, las Organizaciones deberán implementar obligatoriamente un *Servicio de Registro de Aplicaciones*.

El *Servicio de Registro de Aplicaciones* podrá estar basado en certificados digitales o en mecanismos sin certificados pero que utilicen una API Key dentro del modelo OAuth.

Las Organizaciones podrán implementar, para las aplicaciones, otros métodos de acceso a sus servicios, siempre que se evalúen los riesgos asociados y se permita la trazabilidad.

3. SERVICIO DE FIRMA DIGITAL Y VERIFICACIÓN DE FIRMA DIGITAL.

3.1. INTRODUCCIÓN

Los siguientes requisitos se basaron en los estándares para crear y validar firmas definidas en las especificaciones del ETSI. Independientemente de la implementación del servicio de firma, en todo momento se deberá asegurar el exclusivo control del firmante sobre su clave privada de firma digital en custodia.

3.2. CREACIÓN DE FIRMAS

El propósito de crear firmas es generar una firma que cubra un documento electrónico (texto, sonido, imagen, entre otros) del firmante, el certificado de firma o una referencia a ese certificado, así como los atributos de firma que la respaldan.

Un modelo funcional básico de un ambiente para crear firmas está constituido por:

i. firmante que quiere crear una firma en un documento electrónico;
ii. una aplicación conductiva que representa un ambiente de usuario (por ejemplo, una aplicación comercial) que el suscriptor usa para acceder a la funcionalidad de firma; y
iii. un sistema de creación de firma, que implementa la funcionalidad de firma, ubicada en la Organización.

Antes de procesar la petición de firma, la Organización debe garantizar que el usuario titular del certificado sea autenticado y debe verificar la validez de dicho certificado.

La participación humana de un firmante no siempre es necesaria. La firma puede ser un proceso automatizado e implementado en la aplicación en el entorno del usuario.

3.3. DISPOSITIVOS PARA LA CREACIÓN DE FIRMAS

Son sistemas o equipos configurados para implementar códigos y/u otros mecanismos que permiten la activación de la clave privada del firmante para la creación de firmas digitales.

Los dispositivos para creación de firmas, además de poder verificar los datos de autenticación del firmante, deben contener:

i. la clave privada del firmante; y
ii. el correspondiente certificado digital relacionado a esa clave privada o tener una referencia inequívoca a él.

La Organización deberá utilizar un HSM y sistemas de software correspondiente para brindar los servicios que expone, permitiendo que el titular del certificado tenga acceso, control y uso exclusivo de sus datos de creación de firmas. Dichos componentes están delimitados dentro de la frontera criptográfica del HSM y dentro del ambiente seguro de la primera interfaz de comunicación con el HSM.

3.4. INTERFAZ DE APLICACIÓN CON EL DISPOSITIVO DE CREACIÓN DE FIRMA.

La interfaz entre la aplicación de firma y el dispositivo o equipo de creación deben garantizar que solo con la autenticación del titular del certificado, el cual debe tener el control exclusivo de la clave privada, sea posible requerir la creación de datos de una firma digital.

El uso del dispositivo de creación debe requerir que el usuario ingrese datos específicos de autenticación del firmante. Toda la información intercambiada entre la aplicación y el dispositivo debe viajar en forma cifrada.

Se debe usar al menos un mecanismo de autenticación para proporcionar una garantía de autenticación suficiente.

El mecanismo de autenticación de un firmante debe evitar los ataques de suplantación.

La naturaleza del mecanismo de autenticación y de los datos de autenticación del firmante son determinados por el dispositivo de creación de firmas. Existen estándares para diferentes interfaces, tipos de dispositivos o equipos y mecanismos de autenticación.

En algunos casos, el uso de datos de autenticación del firmante será obligatorio y se pueden imponer otros requisitos sobre la naturaleza de los mecanismos e interfaces de autenticación.

3.5. SUITES DE FIRMA

Todos los algoritmos y tamaños de clave involucrados en el cálculo de cualquier elemento de la firma digital se definen en el documento DOC-PKI-06 [3].

3.6. FORMATOS DE FIRMA

Las políticas de firmas podrán proporcionar firmas en los formatos CAdES, XAdES y PAdES.

La Organización debe implementar firmas digitales basadas en políticas de firma estandarizadas conforme al DOC-PKI-06 [3] atendiendo como referencia las disposiciones establecidas en los siguientes documentos:

- ETSI. ASN.1 Format for Signature Policies. Number TR 102 272.
- ETSI. XML Format for Signature Policies. Number TR 102 038.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. TS 102 778-3.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile. TS 102 778-4.

3.7. LA FIRMA CON EL SELLO DE TIEMPO

Una firma digital con una marca de tiempo muestra que la firma digital ya existía en la fecha contenida en la marca de tiempo. Los Sellos de tiempo son emitidos por las Autoridades de Sello de Tiempo, proporcionan la fecha/hora como una propiedad añadida a una firma digital y su aplicación es de carácter opcional.

La Organización podrá utilizar políticas de firma que requieran el uso de la marca de tiempo basadas en normas internacionales.

El modelo de sello de tiempo adoptado en su infraestructura debe seguir como referencia las recomendaciones estipuladas en los siguientes documentos:

- RFC 2030, IETF - Simple Network Time Protocol (SNTP) version 4.0.
- RFC 2527, IETF - Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Frame work, março de 1999.
- RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.
- RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, November 2003.
- ETSI TS 101.861 Technical Specification/Time Stamping Profile.
- ETSI TS 102.023 Technical Specification / Policy Requirements for Time Stamping Authorities.

3.8. VALIDACIÓN DE FIRMAS

Consiste en primer lugar, determinación y validación de que la firma digital fue creada durante el periodo operacional de un certificado válido por la clave privada correspondiente a la clave pública que se encuentra en el certificado y que el mensaje no ha sido alterado desde que su firma digital fue creada.

El proceso de validación de una firma digital debe ser realizado conforme una política de firma digital explícita, que consiste en un conjunto de restricciones de validación, denominada Política de firma, y debe generar un informe que indique el estado de validación (Válido, Inválido o Indeterminado), que proporciona los detalles de la validación técnica de cada una de las restricciones aplicables, que pueden ser relevantes para la aplicación exigente en la interpretación de los resultados.

El firmante crea una firma digital de acuerdo con una política de firma. y el verificador evalúa la validez de una firma digital utilizando la misma política de firma utilizada en la creación de esa firma digital. El ítem 3.6 define los formatos y perfiles que podrán ser utilizados.

4 - REFERENCIAS

4.1 REFERENCIAS

- Ley N° 4017/2010 "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Ley N° 4610/2012 "Que modifica y amplía la Ley Nº 4017/10 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- Decreto N° 7369/2011 "Por el cual se aprueba el reglamento general de la Ley Nº 4017/2010 "de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico".
- RFC 6238: TOTP: Time-Based One-Time Password Algorithm
- RFC 6287: OCRA: OATH Challenge-Response Algorithm
- RFC 4226 HOTP: An HMAC-Based One-Time Password Algorithm
- ETSI TS 102 231 - Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information.
- RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OS.
- RFC 2527: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework.
- RFC 3161: Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)
- RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 5246: The Transport Layer Security (TLS) Protocol. Version 1.2
- RFC 6749: The OAuth 2.0 Authorization Framework.
- RFC 7636: Proof Key for Code Exchange by OAuth Public Clients
- ETSI TS 101.861 - Technical Specification/Time Stamping Profile.

- ETSI TS 102.023 - Technical Specification/Policy Requirements for Time Stamping Authorities.
- ETSI. ASN.1 Format for Signature Policies. Number TR 102 272.
- ETSI. XML Format for Signature Policies. Number TR 102 038.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. TS 102 778-3. V1.2.1. 2010.
- ETSI. Electronic Signatures and Infrastructures; PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile. TS 102 778-4. V1.1.1. 2009.

4.2 REFERENCIAS A DOCUMENTOS QUE COMPONEN LA PKI-Paraguay

Tabla Nº 2 – Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la declaración de prácticas de certificación de los prestadores de servicios de certificación de la PKI-Paraguay.	DOC-PKI-03
[2]	Directivas obligatorias para la formulación y elaboración de la política de certificación de los prestadores de servicios de certificación de la PKI-Paraguay.	DOC-PKI-04
[3]	Normas de algoritmos criptográficos de la PKI-Paraguay.	DOC-PKI-06