

Política de firma electrónica avanzada con custodia centralizada de Persona Física

Versión 2.0

Unidad de Certificación Electrónica

Infraestructura Nacional de Certificación Electrónica
República Oriental del Uruguay

Índice

1.	Introducción	4
1.1.	Descripción general.....	4
1.2.	Nombre del documento e identificación de la Política de Certificación.....	4
1.3.	Participantes de la INCE	5
1.3.1.	Unidad Reguladora	5
1.3.2.	Suscriptores	5
1.4.	Uso de los certificados.....	5
1.5.	Administración de la Política de Certificación	5
1.6.	Relación entre la Política de Certificación y otros documentos	6
1.7.	Procedimiento de Aprobación	6
1.8.	Definiciones y abreviaturas	6
2.	Aspectos generales de la Política de Certificación	9
2.1.	Obligaciones	9
2.1.1.	Obligaciones de la UCE	9
2.1.2.	Obligaciones de las Autoridades de Registro de los Prestadores de Servicios de Confianza Acreditados	9
2.1.3.	Obligaciones de los Prestadores de Servicios de Confianza	10
2.1.4.	Obligaciones de los Suscriptores de Certificados	10
2.2.	Responsabilidades	10
2.3.	Tarifas.....	11
3.	Acreditación de Prestadores de Servicios de Confianza.....	11
4.	Solicitud del certificado de Persona Física para el servicio de firma electrónica avanzada con custodia centralizada	11
4.1.	Registro de las solicitudes de certificados.....	12
5.	Perfil del certificado	12
6.	Servicio de firma electrónica avanzada con custodia centralizada	15
6.1.	Servicio de Firma	15
6.2.	Autenticación del suscriptor.....	16
7.	Protección de las claves privadas	16
8.	Migración de la clave privada.....	16

9. Suspensión y revocación de la acreditación de los Prestadores de Servicios de Confianza.....	16
10. Cese de actividades del Prestador de servicios de confianza acreditado.	17
Referencias Externas.....	17

1. Introducción

1.1. Descripción general

La presente Política es elaborada a partir del Decreto N° 70/018 de 19 de marzo de 2018 [1], que reglamenta los artículos 31 al 33 de la ley N° 18.600 de 21 de setiembre de 2009 [2], en la redacción dada por el artículo 28 de la Ley N° 19.535 de 25 de setiembre 2017, respecto a los servicios de confianza de identificación digital y firma electrónica avanzada con custodia centralizada, con el fin de regular a los Prestadores de Servicios de Confianza (PSCo).

El documento determina los aspectos de gestión, administrativos y técnicos que deberán ser tenidos en cuenta por los Prestadores de Servicios de Confianza (PSCo) en la prestación del servicio de generación, almacenamiento de certificados y firma de personas físicas.

Su objetivo es asegurar que el dispositivo de creación y almacenamiento de firmas electrónicas sea confiable y que el firmante tenga, con un alto nivel de confianza, el acceso exclusivo a su clave de firma electrónica avanzada de persona física en custodia centralizada.

Estos servicios permitirán firmar documentos evitando utilizar dispositivos adicionales para la firma como los Token o los lectores de cédula de identidad. Para ello, los Prestadores de Servicios de Confianza almacenarán los certificados y claves privadas de la persona física y firmarán en línea mediante la previa autorización del titular.

La confección del documento se realizó siguiendo el marco normativo vigente, los lineamientos para la documentación de Políticas y Declaración de Prácticas de Certificación estipulados en el RFC 3647 [3] y la Política de Certificación de Persona Física [4].

La presente Política describe una nueva modalidad de emisión de certificados de persona física, en conjunto con consideraciones para su utilización, generación y almacenamiento. En caso de existir alguna inconsistencia entre esta Política y lo definido en la Política de Certificación de Persona Física [4], ésta última [4] tiene prioridad.

1.2. Nombre del documento e identificación de la Política de Certificación

Nombre: Política de firma electrónica avanzada con custodia centralizada de Persona Física.

Versión: 2.0

Fecha de elaboración: 15/06/2018.

Fecha de última actualización: 12/11/2024

OID: 2.16.858.10000157.66565.12

Sitio web de publicación: <https://www.gub.uy/unidad-certificacion-electronica/comunicacion/publicaciones/politica-firma-electronica-avanzada-custodia-centralizada-persona-fisica>

1.3. Participantes de la INCE

1.3.1. Unidad Reguladora

El rol de Unidad Reguladora es desempeñado por la Unidad de Certificación Electrónica (UCE), según lo dispuesto por la Ley N° 18.600 del 21 de Setiembre de 2009 [2]. En su rol de regulador debe definir los estándares técnicos y operativos que deberán cumplir los Prestadores de Servicios de Certificación Acreditados (PSCA) y los Prestadores de Servicios de Confianza (PSCo), así como los procedimientos y requisitos de acreditación necesarios para su cumplimiento.

Además de su rol regulador, la UCE desempeña funciones de acreditación de Prestadores de Servicios de Certificación; control y auditoría de su actividad; instrucción, estableciendo criterios generales y asesoramiento en buenas prácticas de funcionamiento; y sanción en caso de incumplimiento. Puede encontrarse información detallada en la Política de Certificación de la Autoridad de Certificación Raíz Nacional (ACRN) [5] y en el artículo 14 de la Ley N° 18.600 de 21 de Setiembre del 2009 [2].

1.3.2. Suscriptores

En el contexto de la presente Política, los Suscriptores son personas físicas a quienes un PSCo les ha emitido, a través de un PSCA, uno o más certificados de Persona Física de la Infraestructura Nacional de Certificación Electrónica (INCE) – PKI Uruguay. El PSCo presta al Suscriptor, el servicio de firma electrónica avanzada con el certificado de Persona Física en custodia centralizada.

Los Suscriptores pueden utilizar certificados de Persona Física con fines de autenticación, Firma Electrónica Avanzada y cifrado.

Los Suscriptores contraen derechos y obligaciones al utilizar certificados de Persona Física según se describe en la Política de Certificación de Persona Física [4].

1.4. Uso de los certificados

Los usos habilitados y restricciones para los certificados emitidos bajo la presente Política están definidos en la Política de Certificación de Persona Física [4].

1.5. Administración de la Política de Certificación

La administración de la presente Política es responsabilidad de la UCE.

Por consultas o sugerencias, la UCE designa al siguiente contacto:

Nombre: Unidad de Certificación Electrónica

Dirección de correo: info@uce.gub.uy Teléfono: (+598) 2901 0065 opción 5

1.6. Relación entre la Política de Certificación y otros documentos

La presente Política se basa en la Ley N° 18.600 [2], en la redacción dada por el artículo 28 de la Ley N° 19.535, en el Decreto N° 436/011 de 8 de diciembre de 2011 [6], en el Decreto N° 70/018 [1], y en la Política de Certificación de Persona Física [3] y prevalece sobre ella la legislación vigente y las disposiciones particulares adoptadas por la UCE.

Los requerimientos definidos en esta Política deben ser instrumentados por los Prestadores de Servicios de Confianza (PSCo) y especificados en su Declaración de Prácticas de Certificación.

Esta Política tiene impacto en las Políticas de Seguridad de la Información y procedimientos administrativos del Prestador de Servicios de Confianza (PSCo).

1.7. Procedimiento de Aprobación

La aprobación de esta Política, así como toda modificación introducida en ella, es responsabilidad exclusiva de la UCE. La UCE aplicará sus procedimientos internos de administración documental para garantizar la calidad y trazabilidad de los cambios realizados. La Política modificada se publicará como una nueva versión, manteniéndose un registro de la fecha y cambios realizados.

1.8. Definiciones y abreviaturas

Las definiciones y abreviaturas generales de la Infraestructura Nacional de Certificación Electrónica (INCE) se encuentran definidas en la Ley N° 18.600 [2]. No obstante, las siguientes definiciones y abreviaturas son utilizadas a lo largo del presente documento, y, por lo tanto, son citadas también aquí.

Authenticator Assurance Level 2 (AAL2): representa un nivel específico de fortaleza para la autenticación electrónica definido por el Instituto Nacional de Estándares y Tecnología (NIST) [7]

Dicho nivel proporciona un alto grado de confianza, en qué el solicitante de una autenticación electrónica es poseedor de los medios de identificación electrónica o digital que le fueron asociados durante el proceso de registro de identificación digital.

Autenticación electrónica: proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital.

Autoridad Certificadora del Prestador Acreditado (ACPA): conjunto de sistemas, personal, políticas y procedimientos que el PSCA utiliza para emitir certificados a usuarios finales bajo las políticas de certificación que le fueron asignadas.

Autoridad Certificadora Raíz Nacional (ACRN): conjunto de sistemas informáticos, personal, políticas y procedimientos que, en la estructura de la INCE por herencia, constituyen la raíz de confianza. Permite certificar a otras entidades encargadas de emitir certificados dentro de la INCE.

Autoridad de Registro (AR): en el contexto de la presente política, es responsable del registro y procesamiento de solicitudes de emisión, renovación y revocación de certificados, incluyendo la validación de la identidad de los suscriptores/o de las solicitudes al inicio del proceso.

Certificado Electrónico (CE): documento electrónico firmado electrónicamente que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica.

Certificado Electrónico Reconocido (CER): certificado Electrónico emitido por la ACRN o por un PSCA a través de una de sus ACPA.

Certificado Electrónico Reconocido de Persona Física (CERPF): certificado Electrónico Reconocido cuyo suscriptor es una Persona Física, emitidos en exclusividad por los PSCA y sujetos a los requerimientos de la presente Política de Certificación.

Declaración de Prácticas de Certificación (CPS – Certificate Practice Statement): declaración de las prácticas que emplea una entidad certificadora en la gestión de los certificados emitidos por ella (emisión, revocación, renovación, etc.).

Dispositivo o Módulo Seguro de Creación de Firmas (DSCF): dispositivo que resguarda las claves y el certificado de un suscriptor, utilizado para generar su firma electrónica y que, al menos, garantiza:

- a) Que los datos utilizados para la generación de la firma solamente pueden producirse una vez y mantiene su confidencialidad;
- b) Que existe una expectativa razonable de que los datos utilizados para la generación de la firma no pueden ser descubiertos por deducción, y la firma está protegida contra falsificación por medio de la tecnología disponible a la fecha, siendo posible detectar cualquier alteración posterior.
- c) Que los datos empleados en la generación de la firma puedan ser protegidos de modo fiable por el firmante, contra su utilización por terceros.

Federal Information Processing Standard (FIPS) 140 nivel 3: estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos. En su nivel 3 asegura que los módulos sean resistentes a la intrusión física.

Firma electrónica avanzada con custodia centralizada: firma electrónica avanzada en la cual la clave privada del firmante se encuentra en custodia de un prestador de servicios de confianza acreditado, que realiza la firma bajo orden expresa del firmante.

Infraestructura nacional de certificación electrónica (INCE): conjunto de equipos y programas informáticos, dispositivos criptográficos, políticas, normas y procedimientos, dispuestos para la generación, almacenamiento y publicación de los certificados reconocidos, así como también para la publicación de información y consulta del estado de vigencia y validez de dichos certificados.

Medio de identificación electrónica o digital: unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante:

- a) su conocimiento;

- b) un dispositivo físico o lógico;
- c) algún rasgo físico o comportamental.

Módulo de Hardware de Seguridad (Hardware Security Module - HSM): dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas.

Prestador de Servicios de Certificación Acreditado (PSCA): persona física o jurídica acreditada ante la UCE y responsable de la operación de al menos una Autoridad Certificadora de la INCE.

Prestador de Servicios de Confianza (PSCo): persona física o jurídica, pública o privada, nacional o extranjera, que presta uno o más servicios de confianza.

Política de Certificación (Certificate Policy - CP): conjunto de políticas que indican la aplicabilidad de un certificado a una comunidad particular y/o clase de solicitud con requerimientos comunes de seguridad, y además definen los requisitos que cualquier prestador debe respetar para trabajar con ese tipo de certificado. En el contexto de la INCE estas políticas son promovidas, aprobadas y mantenidas por la UCE.

Registro de identificación digital: proceso de identificar a una persona, verificar sus datos, expedir o asociar uno o más medios de identificación digital a ésta, y almacenar dicha asociación para su posterior utilización.

Servicios de Confianza: servicios electrónicos que permiten brindar seguridad jurídica a los hechos, actos y negocios realizados o registrados por medios electrónicos, entre ellos:

- a) servicios de firma electrónica avanzada con custodia centralizada;
- b) servicios de identificación digital;
- c) servicios de sellado de tiempo;
- d) otros servicios establecidos por la Unidad de Certificación Electrónica.

Servicios de identificación digital: servicios que realizan registros de autenticación electrónica de personas para su verificación por terceros.

Solicitud de Firma de Certificado (Certificate Signing Request - CSR): en el contexto de la presente política, es un mensaje emitido por una persona física bajo el estándar PKCS#10 mediante el que solicita y provee información a una ACPA para la emisión de un certificado firmado por ella.

NIST (National Institute of Standards and Technology): Agencia del Departamento de Comercio de los Estados Unidos de América.

LACNIC: El Registro de Direcciones de Internet para América Latina y Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros recursos para la región de América Latina y el Caribe. Es uno de los 5 Registros Regionales de Internet en el mundo.

Curva Elíptica: La Criptografía de Curva Elíptica (del inglés: Elliptic curve cryptography, ECC) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas. Sus autores argumentan que la CCE puede ser más rápida y usar claves

más cortas que los métodos antiguos —como RSA— al tiempo que proporcionan un nivel de seguridad equivalente.

Curvas Edwards: En matemáticas, las curvas de Edwards son una familia de curvas elípticas estudiadas por Harold Edwards en 2007. El concepto de curvas elípticas sobre campos finitos se utiliza ampliamente en criptografía de curvas elípticas.

Curvas Brainpool: Son las curvas elípticas basadas en el RFC 5639. "Elliptic Cryptography (ECC) Brainpool Standard Curves and Curve Generation"

Curvas NIST: Refiere a las Curvas Elípticas definidas en el Standard RFC 6979 "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)".

2. Aspectos generales de la Política de Certificación

2.1. Obligaciones

2.1.1. Obligaciones de la UCE

La UCE asume las siguientes obligaciones adicionales a las obligaciones definidas en la Política de Certificación de la ACRN.

- a) Acreditar a los Prestadores de Servicios de Certificación que soliciten su inscripción en el registro de Prestadores de Servicios de Confianza y cumplan con los requisitos establecidos en la presente política.
- b) Realizar control de admisibilidad de las solicitudes según lo establecido en el artículo 15 del Decreto N° 436/011 [6].
- c) Aprobada técnicamente la solicitud de acreditación, se comunicará al solicitante quién dispondrá de 20 días corridos contados a partir del día siguiente a la notificación, para presentar la garantía prevista en el artículo 17 de la Ley N° 18.600 [2] a través de la contratación de un seguro de responsabilidad civil para afrontar el riesgo de la responsabilidad por daños y perjuicios que pudieran ocasionar en la prestación de sus servicios.
- d) Otorgar la acreditación al solicitante por el plazo que determine la UCE. Dicha acreditación estará sujeta a las inspecciones y auditorías que requiera.

2.1.2. Obligaciones de las Autoridades de Registro de los Prestadores de Servicios de Confianza Acreditados

Definidas en la Política de Certificación de Persona Física [4] en la sección 2.1.3.

2.1.3. Obligaciones de los Prestadores de Servicios de Confianza

Son obligaciones de los PSCo:

- a) Custodiar diligentemente la clave privada del firmante o signatario y asegurar los medios para su generación, protección y destrucción cumpliendo con lo definido en la presente política.
- b) Establecer mecanismos seguros para realizar firmas electrónicas por orden del firmante o signatario de acuerdo con la presente política.
- c) Disponer de mecanismos seguros para la autenticación electrónica de personas físicas, teniendo en cuenta los requisitos técnicos definidos en la presente política.
- d) Proporcionar a las personas físicas de mecanismos de control y trazabilidad sobre el uso de su clave privada de firma electrónica avanzada en custodia.
- e) Proveer un servicio de firma a la persona física para la utilización de su firma electrónica avanzada en custodia centralizada.
- f) Disponer de forma gratuita sobre la documentación de integración para desarrolladores con el servicio de firma.

2.1.4. Obligaciones de los Suscriptores de Certificados

En el contexto de la presente Política de Certificación, los suscriptores son Personas Físicas, ciudadanos nacionales o extranjeros, mayores de dieciocho años, bajo cuya responsabilidad recaerán las obligaciones citadas en este punto.

Los Suscriptores de certificados de Persona Física asumen las siguientes obligaciones adicionales a las obligaciones definidas en la Política de Certificación Persona Física:

- a) Proteger la información relacionada con la identificación y autenticación para la utilización de la firma electrónica avanzada con custodia centralizada.
- b) Solicitar la inmediata revocación del certificado emitido por un PSCo en el caso de compromiso o sospecha de compromiso de los medios de identificación digital para su uso.

2.2. Responsabilidades

La responsabilidad de los PSCo Acreditados se regirá por lo establecido para los Prestadores de Servicios de Certificación en el artículo 20 de la Ley N° 18.600 [2]

2.3. Tarifas

Los PSCo en custodia de claves centralizadas, bajo la presente Política, podrán percibir una prestación económica para sus servicios.

3. Acreditación de Prestadores de Servicios de Confianza

En el contexto de esta Política, los PSCo podrán acreditarse para brindar el servicio de “Generación, almacenamiento y firma de personas físicas”.

Son condiciones indispensables para ser PSCo Acreditado, las siguientes:

- a) Ser persona física o jurídica constituida en el país, dar garantía económica y solvencia suficiente para prestar los servicios.
- b) Contar con personal calificado con conocimientos y experiencia necesarios para la prestación de los servicios de confianza ofrecidos y con procedimientos de seguridad y de gestión adecuados.
- c) Utilizar estándares y herramientas adecuadas según lo establecido por la Unidad de Certificación Electrónica.
- d) Estar domiciliado en el territorio de la República Oriental del Uruguay, entendiéndose que cumple con este requisito cuando su infraestructura tecnológica y demás recursos materiales y humanos se encuentren situados en territorio uruguayo.

Los Prestadores de Servicios de Certificación acreditados ante la UCE podrán solicitar su inscripción en el Registro de Prestadores de Servicios de Confianza para brindar el servicio de “Generación, almacenamiento y firma de personas físicas”, en este caso deberán acreditar los requisitos específicos establecidos en esta Política.

El procedimiento de acreditación de los Prestadores de Servicios de generación, almacenamiento y firma se realizará de acuerdo con las disposiciones de la Ley N° 18.600 [2] y en el Capítulo V del Decreto N° 436/011 [6].

4. Solicitud del certificado de Persona Física para el servicio de firma electrónica avanzada con custodia centralizada

Las condiciones para una solicitud de certificado de persona física se encuentran definidas en la Política de Certificación de Persona Física [4] en la sección 4.1. En el contexto de la presente política se definen las condiciones adicionales para la solicitud de un certificado de firma electrónica avanzada de persona física en custodia centralizada.

4.1. Registro de las solicitudes de certificados

La solicitud del certificado de persona física puede iniciarse de forma presencial o remota (web, mail, etc.) según lo determine cada PSCo. En cualquier caso, el PSCo debe documentar la solicitud de certificado y dar comienzo a sus procedimientos internos de emisión.

El procedimiento de solicitud de certificado o el procedimiento de renovación deben contar con una instancia presencial donde se valide la identidad y documentación del solicitante, según lo especifica la sección

3.1.2 de la Política de Certificación de Persona Física [4].

Adicionalmente a las modalidades definidas en la Política de Persona Física

[4] en la sección 4.1.2, la presente política define una nueva modalidad de generación de claves para Persona Física:

- **Centralizada** – el par de claves y CSR los genera el PSCo en sus instalaciones. En esta modalidad, el PSCo generará la clave privada del Solicitante en su módulo criptográfico (HSM) de custodia centralizada. El PIN o contraseña que protege la clave privada será ingresado por el Solicitante y estará en control exclusivo de éste. No se permite el almacenamiento de la clave privada generada para el Solicitante en ningún otro medio que no sea el dispositivo en el que se generó. Durante el proceso de generación de la clave privada, se llevará a cabo el Registro de identificación digital donde se deberán asociar al menos dos medios de identificación digital (ver sección 6.2) al Solicitante del certificado. La emisión del certificado se realizará de acuerdo con los procedimientos de emisión del PSCA.

El PSCo deberá 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 Solicitante tiene el control exclusivo del PIN o contraseña que protege el uso de su clave privada generada.

El PSCo deberá informar al Solicitante la importancia que tiene el PIN y los medios de identificación digital para la protección del uso de su clave privada, así como dar pautas para un uso seguro.

Como parte del proceso de solicitud de certificado, el Solicitante debe firmar las Condiciones para la Utilización de Firma Electrónica Avanzada [8]. Este acuerdo, elaborado por el PSCo, registra la adhesión del Solicitante a la presente Política de Certificación y a la demás regulación aplicable emitida por la UCE. En caso de que el Solicitante no firme este Acuerdo, no se puede continuar con el proceso de emisión de certificado.

5. Perfil del certificado

Los certificados para firma electrónica avanzada en custodia centralizada se emiten con el atributo QCCompliance dentro de la extensión QcStatement cumpliendo con el estándar ITU-T X.509 versión 3 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile), definido en su versión más reciente en el RFC 5280 [10].

Adicionalmente, para los perfiles que contemplen curvas elípticas deberán ser con el estándar respectivo:

- Curvas NIST (RFC 6979)
- Curvas Brainpool (RFC 5639)
- Curvas Edwards (RFC 8032)

La inclusión del atributo se refiere a una declaración del emisor, en la cual se hace constar la calificación con la que es emitido el certificado, en este caso cumpliendo con las condiciones establecidas en esta Política.

En el contexto de la presente Política, se modifica el perfil del certificado de Persona Física definido en la sección 7.1 de la Política de Certificación Persona Física [4] para incluir el atributo mencionado

Atributos	Contenido
Versión (Version)	V3
Algoritmo de Firma (Signature Algorithm)	sha256RSA sha384RSA ECC-Brainpool (conforme RFC 5639) Curve25519 (Conforme RFC 7748) Ed25519 (PureEdDSA e HashEdDSA RFC 8032)
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA emisora tal cual figura en su certificado
Validez (Valid From / Valid To)	0 a 2 Años (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	CN = Nombre completo de la Persona Física C = País del Documento de identificación Presentado serialNumber = Código y número de documento givenName = Nombres de la Persona Física. surname = Apellidos de la Persona Física. (Ver sección 3.1.1.1)
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 2048 bits o más brainpoolP256r1 Curve25519 (256 bits) Ed25519 (256 bits) Nistp-256 (256 bits) Nistp-384 (384 bits)

Extensiones	
Identificador de la clave del suscriptor (Subject Key Identifier)	Hash de 20 bytes del atributo Subject Public Key
Identificador de la clave de la autoridad (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la ACPA emisora
Uso de Claves (Key Usage)	DigitalSignature = 1 NonRepudiation/contentCommitment = 1 KeyEncipherment = 1 DataEncipherment = 1 KeyAgreement = 0 KeyCertSign = 0 CRLSign = 0 EncipherOnly = 0 DecipherOnly = 0
Uso de Claves Extendido (Extended Key Usage)	clientAuth, emailProtection

Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.12 URI: https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/cp_custodiacentralizada_v2.0.pdf OID: OID asignado a la CPS del PSCA para la ACPA emisora URI: URL de publicación de la CPS
Restricciones Básicas (Basic Constraints)	CA = FALSE
Puntos de distribución de las CRL (CRL Distribution Points)	URI = URL primaria de publicación de la CRL URI = URL secundaria de publicación de la CRL
QCStatements	Id-etsi-qcs-QcCompliance Id-etsi-qcs-QcSSCD

Durante la generación del certificado, se deberá tener en cuenta la inclusión de este atributo por parte de la ACPA, reconociendo que la solicitud proviene de un PSCo acreditado que cumple con los requisitos establecidos por la presente Política.

Adicionalmente si se realizó la verificación biométrica en la etapa de registro de acuerdo a la sección 4.1.2.1 Registro con verificación biométrica adicional de la Política de Certificación de Persona Física [4], se deberá incluir el OID 2.16.858.10000157.66565.13 como es estipulado a continuación:

Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.12
	URI: https://www.gub.uy/unidad-certificacion-electronica/sites/unidad-certificacion-electronica/files/documentos/publicaciones/cp_custodiacentralizada_v2.0.pdf
	OID: OID asignado a la CPS del PSCA para la ACPA emisora
	URI: URL de publicación de la CPS OID: 2.16.858.10000157.66565.13
	User Notice: Verificación biométrica

6. Servicio de firma electrónica avanzada con custodia centralizada

Adicionalmente a la generación y almacenamiento de claves privadas de personas físicas, el PSCo deberá brindar el servicio de firma que facilite a los suscriptores la utilización de su clave privada de firma electrónica avanzada en custodia centralizada.

El servicio de firma ofrecido por el PSCo deberá establecer mecanismos seguros para realizar firmas electrónicas únicamente por orden del firmante.

A continuación, se definen una serie de consideraciones técnicas para el servicio de firma que permite el uso de la clave de firma electrónica avanzada en custodia centralizada.

6.1. Servicio de Firma

El servicio deberá ser desarrollado tomando en cuenta estándares internacionales para el desarrollo seguro como por ejemplo OWASP [9].

El PSCo deberá disponer de documentación para desarrolladores para la integración a su servicio de firma, quedando a criterio del PSCo la definición de las condiciones para su uso y/o integración.

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 electrónica avanzada en custodia.

6.2. Autenticación del suscriptor

Durante el proceso de solicitud de certificados definido en la sección 4, se asocian al Solicitante del certificado los medios de identificación digital necesarios para la autenticación electrónica requerida por el servicio de firma.

Es requisito para el PSCo, garantizar un nivel de fortaleza en el proceso de autenticación electrónica equivalente o superior a AAL2 definido por el NIST [7], y por tanto proporcionar un alto grado de confianza, en que la persona solicitante de una autenticación electrónica para el uso de su clave privada en custodia centralizada es poseedora de los medios de identificación digital que le fueron asociados durante el registro de identificación digital en la solicitud del certificado.

Los medios de identificación digital considerados seguros, son los definidos por la UCE tomando en cuenta el documento de lineamientos de identidad digital del NIST [7].

7. Protección de las claves privadas

Un PSCo deberá tener en cuenta los siguientes requisitos en conjunto con los establecidos para un PSCA que emite certificados de Persona Física bajo la Política de Certificación de Persona Física [4].

- a) Las claves privadas de firma electrónica avanzada de persona física en custodia del PSCo, deberán ser generadas y almacenadas en módulos criptográficos (HSM) que cumplan con la normativa FIPS 140-2 nivel 3.
- b) La contraseña o PIN de acceso a la clave privada de firma electrónica avanzada de persona física debe estar siempre protegida por módulos criptográficos (HSM) que cumplan con la normativa FIPS 140-2 nivel 3 y en control exclusivo de la persona física.

8. Migración de la clave privada

La clave privada de firma electrónica avanzada de persona física no podrá ser migrada entre diferentes Prestadores de Servicios de Confianza, ni modificar el medio de almacenamiento dentro del mismo prestador.

9. Suspensión y revocación de la acreditación de los Prestadores de Servicios de Confianza

La suspensión y revocación de la acreditación de los PSCo de generación, almacenamiento y firma electrónica avanzada, así como sus efectos, se regirán por lo establecido para los Prestadores de Servicios de Certificación según la Política de Certificación de la ACRN [5].

10. Cese de actividades del Prestador de servicios de confianza acreditado.

Los PSCo de generación, almacenamiento y firma electrónica avanzada que cesen en sus actividades estarán obligados a comunicarlo a través del Diario Oficial y cualquier otro medio electrónico o tradicional que considere pertinente.

Asimismo, el prestador deberá mantener o derivar el servicio de recepción de solicitudes de revocación, y actualizar y publicar en el Registro actualizado de certificados revocados hasta que haya vencido el último de los certificados emitidos.

Referencias Externas

1. Poder Ejecutivo, República Oriental del Uruguay. Decreto N° 70/018 de 19 de marzo de 2018. Reglamentación de los Arts. 31 a 33 de la Ley N° 18.600.
2. Poder Legislativo, República Oriental del Uruguay. Ley N° 18.600 de 21 de setiembre de 2009. Documento Electrónico y Firma Electrónica.
3. Chokhani, Ford, Sabett, Wu, RFC 3647 - Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework, 2003.
4. Unidad de Certificación Electrónica, Política de Certificación de Persona Física, 2015.
5. Unidad de Certificación Electrónica, Política de Certificación de la Autoridad Certificadora Raíz Nacional. 2011.
6. Poder Ejecutivo, República Oriental del Uruguay. Decreto 436/011 de 21 de setiembre de 2009. Reglamentación del Documento Electrónico y Firma Electrónica.
7. SP-800-63B NIST Special Publication, Digital Identity Guidelines - Authentication and Lifecycle Management, 2017.
8. OWASP Project, <https://www.owasp.org/>.
9. Unidad de Certificación Electrónica. Condiciones para la Utilización de Firma Electrónica Avanzada. 2012.
10. Cooper, Santesson, Farrell, Boeyen, Housley, Polk. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force (IETF), 2008.