FIRMA ELECTRÓNICA TRANSFRONTERIZA

Para América Latina y el Caribe

DESCRIPCIÓN BREVE

Este documento pretende abarcar los puntos más relevantes para la creación de una Infraestructura de Clave Pública. En base a eso marcar requerimientos los mínimos necesarios para la Interoperabilidad Transfronteriza

Ing. Jorge Prego

Marzo de 2020

Programa de Bienes Públicos Regionales

Índice

Antecedentes 1
Objetivos 2
Generalidades de la Interoperabilidad 2
Generación de la lista de confianza 4
Modelo de operación de la autoridad certificadora y autoridad registradora 7
Plan de administración de claves criptográficas 15
Estructura de certificados digitales 16
Estructura de listas de revocación de certificados 19
Algoritmos criptográficos para firma electrónica 21
Algoritmos Hash para firma electrónica 21
Servicio OCSP 22
Ciclo de vida de los certificados 22
Auditorias de tercera parte 23
Pruebas de Ethical Hacking, penetración y escaneo de vulnerabilidades en la red 24
Administración del Registro de auditoria transaccional 24
Servicio de monitoreo y control de eventos de seguridad 25
Servicio de monitoreo y control de disponibilidad y capacidad de los componentes de red . 27
Garantías a través de pólizas de seguros 27
Infraestructura y recursos mínimos 27
Requisitos de aseguramiento para que los PSCA obtengan y mantengan la acreditación 28
Normas 29
Referencias Externas 30

Firma Electrónica transfronteriza para América Latina y el Caribe

BID & Red Gealc

Antecedentes

La Red de Gobierno Electrónico y América Latina y el Caribe (Red GEALC), integrada por las agencias de gobierno digital de la región, tiene en su plan de apoyar la instrumentación de la firma electrónica avanzada o firma digital transfronteriza, al igual que la identidad digital[1] y los servicios digitales transfronterizos asociados a ambos sistemas (firma e identidad) para acelerar su adopción regional, fortaleciendo las transacciones electrónicas confiables y seguras como impulso a la economía digital y el gobierno digital en un marco de integración, en base al modelo colaborativo definido por los países de la Red GEALC como bien público regional (BPR).

El potencial de las tecnologías como catalizador de nuevas formas de relacionamiento entre gobierno y ciudadanía junto a una nueva economía digital con visión de integración regional y global, ha sido tema de debate en los últimos años.

Al menos uno de cada dos países de la región cuenta con políticas integradoras de sus prioridades digitales, y existen diferentes esfuerzos de agendas digitales en el marco de mecanismos como el eLAC, la Alianza del Pacífico y el Mercosur. En todos los casos, la firma digital, la identidad digital y los servicios digitales interoperables están presentes en las agendas nacionales, subregionales y regionales, como factor fundamental para las transacciones electrónicas confiables y seguras, a nivel nacional y transfronterizo, con impacto en campos diversos, como el comercio, la salud, la educación y la movilidad de personas.

Debido a la situación actual sanitaria conocida y padecida por todos los países (epidemia de coronavirus o covid-19), estas herramientas, la *firma electrónica* y la *identidad digital,* pasan a ser piñones fundamentales de un andamiaje mayor para permitir a los gobiernos y a empresas privadas poder continuar funcionando en la situación sanitaria actual, tanto hacia el interior de los mismos como hacia el exterior, gracias a la interoperabilidad que permiten estos ecosistemas. Donde la realización de teletrabajo es fundamental para la continuidad de las tareas en forma ininterrumpida en un país, una empresa, una institución.

[1]La Identidad Digital será abordada en un próximo documento, de características similares a esté. Igualmente tentamos una definición de Identidad Digital la cual se basa en garantizar la identificación inequívoca de una persona y hacer posible que el servicio se entregue a la persona que realmente tiene derecho a él. Entonces, la Identidad Digital se define como el conjunto de atributos que identifican a una persona física en un entorno digital y le permita interactuar con los sistemas informáticos que así lo requieran.

Objetivos

El objetivo de este documento es proporcionar una serie de recomendaciones/sugerencias, enfocadas principalmente a colaborar con las decisiones y pasos que se deben tomar sobre la evolución y maduración del ecosistema de Firma Electrónica/Digital [2][3] en cada uno de los países para lograr a una interoperabilidad transfronteriza.

Con el objetivo principal de que se produzca un reconocimiento pleno de la firma electrónica/digital emitidas por entidades o prestadores de servicio de certificación. Por medio de homogeneizar estándares técnicos de los ecosistemas de firma electrónica/digital de cada país. Para lo cual se presentaran una serie de recomendaciones en con el objetivo de llegar a producir una lista de listas que relacione las listas de servicios de confianza de los países, lo cual permita a los países facilitar el reconocimiento de firmas electrónicas avanzadas o firmas digitales de manera transfronteriza.

Generalidades de la Interoperabilidad

Para hablar de interoperabilidad, en primera instancia, hay que convenir una serie de pautas mínimas para poder realizarla. Es así que surgen tres puntos sumamente importantes a mencionar;

Interoperabilidad técnica; refiere al certificado digital que es la "pieza" de intercambio a utilizar por todos los países. Su perfil deberá cumplir con estándares y especificaciones técnicas internacionales p.ej. ITU X.509, IETF RFC 5280, ETSI EN 319 411-1.

Según lo relevado en etapas anteriores de este proyecto, los países que comenzaron a utilizar certificados de firma electrónica/digital optaron por este perfil de certificado. Esto en si representa un paso importante hacia la interoperabilidad.

Los países que estén en etapas tempranas de la adopción de este tipo de soluciones deberían adoptar este camino. Esto les permitiría obtener avances significativos en poco tiempo, obtener conocimiento muy rápido de los países más adelantados en esta materia, conocer la adopción de estas tecnologías por parte de los terceros países. Un punto no menor estar preparados para la Interoperabilidad Transfronteriza desde el mismo punto de partida, un punto invaluable sin lugar a dudas.

Interoperabilidad semántica; posibilita la normalización de los datos intercambiados y su contexto para que puedan ser comprensibles e interpretados de igual manera por todos. Definiciones de los atributos contenidos en los certificados.

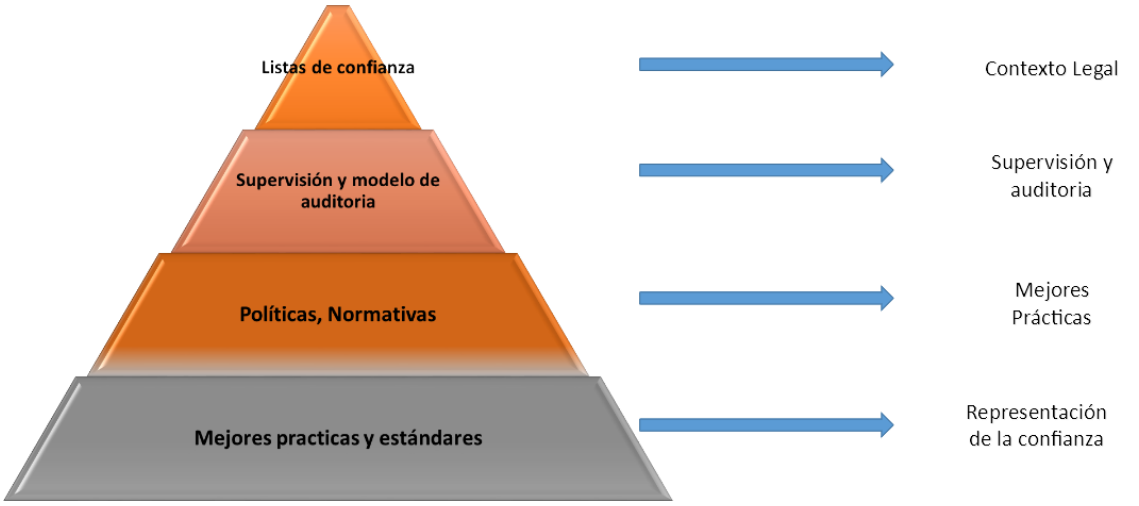
[2] Cabe realizar una salvedad que en este documento cuando se utiliza la denominación Firma Electrónica o Digital se refiere a la firma emitirá por un PSC acreditado en el país mediante un dispositivo seguro de creación de firma, es decir, la firma equivalente a la manuscrita.

[3] Sin perjuicio de lo mencionado en la nota 2, el proyecto es mucho más amplio queriendo lograr una interoperabilidad de todos los tipos de firma electrónica posible y de la identidad digital. El documento pretende marcar los primeros pasos de ese camino, comenzando por el tipo de firma electrónica que todos los países tienen.

Interoperabilidad organizativa; Definición de marcos de confianza para el reconocimiento de diferentes marcos legales como equivalentes.

Nomenclátor; punto no menor a tener en cuenta a la hora de enmarcar y definir pautas para la interoperabilidad. Por más que los países de la región en su mayoría son de habla hispana, existen diferencias dialécticas las cuales hay que convenir. Así es que tenemos distintos nombres para las mismas cosas, Firma Electrónica, Firma Electrónica Avanzada, Firma digital; Certificados de persona física, Certificados de persona natural, Certificados de persona humana, etc.

Es así que surge como modelo por adopción para la interoperabilidad ETSI draft TR 103 684, 2019, en el cual se basa este documento. A continuación se muestra el diagrama que ejemplifica el modelo



En general se ha adoptado como modelo de interoperabilidad el realizado por la Unión Europea (UE), si bien se ha implementado con algunos matices es el que prevalece a nivel global y es el que se recomienda en este documento. Dicho modelo se basa en la existencia de un marco normativo para toda la unión, el Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, conocido como el reglamento eIDAS, que sienta las bases de la identidad y servicios electrónicos de confianza en toda la unión. En relación a la interoperabilidad transfronteriza de firma electrónica avanzada o firma digital basada en certificados digitales, se utiliza el mecanismo de listas de confianza, que se puede ver en https://webgate.ec.europa.eu/tl-browser/#/. Cada estado miembro publica la lista de prestadores reconocidos en su territorio, que a su vez, se agregan en una lista de listas, con todos los prestadores reconocidos en la unión. Dicha lista de listas está disponible de manera pública, tanto visualizable por personas como automáticamente por máquinas, y es la que permite identificarse o firmar digitalmente con un certificado emitido por un prestador que aparezca en la misma con validez jurídica e interoperabilidad técnica en cualquier país de la unión.

En vista de lo mencionado anteriormente es que surge como instrumento natural el uso de Lista de Listas de confianza para la interoperabilidad transfronteriza de América Latina y el Caribe. Este instrumento nos permite una fácil integración hacia otras regiones del planeta, las

cuales usan plataformas de similares características, facilitando el comercio y cualquier trámite transfronterizo que se deba realizar tanto para personas como para empresas

Para llegar a la implementación de listas de confianza los países deben contar con una serie de condiciones o requerimientos de los cuales se mencionan los básicos e indispensables.

- Contar con un marco normativo y regulatorio de firma electrónica e identificación digital que habilite la creación de este ecosistema, un regulador y/o acreditador y le de validez jurídica.
- El Regulador, independiente del mercado, que genere las políticas por las cuales se va a regir el ecosistema de firma electrónica e identidad digital.
- El Regulador o Acreditador contará por marco normativo y regulatorio con funciones de acreditación de prestadores, los cuales podrán ser tanto entidades públicas como empresas privadas, para poder brindar el servicio de firma electrónica e identidad, control, instrucción, regulación y sanción, sobre los mismos. También marcara las pautas de evolución del ecosistema.

Generación de la lista de confianza

A continuación daremos una breve descripción de los requerimientos que se necesitan para la generación de listas de confianza. Para aquellos países que no tienen aún listas de confianza de prestadores, hay que generarlas. Dichas listas contarán con todos los datos necesarios para que desde el punto de vista tanto jurídico como tecnológico, se pueda obtener la información para asegurar la firma e identificación transfronteriza. Dichas listas consistirán en el conjunto de metadatos estandarizados;

- Se generara una lista de confianza para cada uno de los tipos de certificados que emitan los prestadores.
- La lista de confianza se compone de datos homogéneos relacionados con cada tipo de certificado, en cada prestador de servicios de confianza. Básicamente, se necesita un sistema que permita rellenar una serie de fichas con información, y agregar la misma en una lista.
- Las listas de confianza tienen que estar firmadas para dar validez a las mismas, y asegurar la autenticidad, integridad y no repudio. Entonces el sistema de información que genera las listas deberá poder firmar digitalmente la misma con el certificado electrónico de la institución responsable de generarla.

Publicación y puesta a disposición de la lista de listas: el objetivo final es tener un sistema que permita la consulta tanto por personas como máquinas, de la lista de listas de los distintos estados que interoperen. Algunas de las necesidades detectadas en el devenir de este proyecto son las siguientes:

- **Sitio web de publicación:** sea viable la descarga de la lista por parte de terceros sistemas para realizar verificaciones.

- **Publicación de la lista de país:** no todos los países tienen en la actualidad un lugar donde se publique la propia lista, por lo que se requiere que se pueda publicar, aparte de la lista de listas.

- **Funcionalidades:** se valorarán que el sitio web de publicación de la lista de listas contenga las siguientes funcionalidades:

- Actualización automática de la lista de listas, en virtud de la información de las listas del país;
- Información histórica acerca de cambios y modificaciones;
- Buscador sobre los distintos conceptos de la página;
- Punto neutro de validación e información, es decir, en la página de la lista de lista habrá un apartado para que, subido un certificado o un documento firmado con un certificado, extraiga la información de validez y demás datos relevantes;
- Remisión de información de cambios tanto en listas nacionales como en la lista de listas para suscriptores.

Para la generación de listas de confianza y la lista de listas, se encuentra disponible para los países, que forman parte de éste proyecto, *el software de TL Manager de la Comisión Europea*. Es una plataforma altamente probada, validada y usada para estos propósitos en especial por la UE.

Esta plataforma permite la creación, gestión y publicación de las listas de confianza del país. Existiendo documentación suficiente para su instalación y gestión.

Es importante mencionar que hay varios países en Latinoamérica que cuentan con esta plataforma instalada y en funcionamiento. En este caso son Colombia, Chile, Perú y Uruguay.

Como parte de este proyecto de interoperabilidad transfronteriza se está llevando adelante un piloto entre Chile y Uruguay, el cual se encuentra en las etapas finales. En breve se podrá culminar generando un conocimiento, sumamente relevante, a compartir con los demás países de la región para que su integración sea más rápida, sencilla y eficiente.

A su vez se ha generado la oportunidad de tener instalada la posibilidad de publicar Lista de Listas de Confianza dicha configuración se encuentra en Perú y Uruguay. Brindando la posibilidad de tener puntos focales en dos bloques importantes de América Latina, uno en Alianza del Pacifico (AP) y el otro en Mercosur. Facilitando la interoperabilidad entre ambos bloques comerciales. Quedando así, como una primera fase, dos instancias de listas de listas en donde y a las cuales se pueden ir adhiriendo terceros países de América Latina que vayan llegando a ese punto de madurez. De esta manera pudiéndose sumar rápidamente a grandes bloques y quedando interconectados e integrados de manera muy rápida.

Cabe recordar que esté es un documento técnico por lo cual sin perjuicio de eso, se asume que los países estarán llevando adelante conversaciones, en el marco de la RED GEALC, a nivel jurídico y diplomático para amalgamar las normativas individuales y poder internalizar estos aspectos en cada país, derivando en proceso y/o protocolos en pos de lograr una interoperabilidad plena.

Quedando a futuro la posibilidad de contar con puntos focales regionales en donde se publiquen las listas de listas regionales, esta sugerencia es una muy buena práctica. En este caso las regiones, en las cuales se pensó, se refiere a los bloques comerciales ya existentes.

La plataforma de *@firma* es una suite de servicios, programados con software libre, pensado para el manejo de firmas electrónicas e identidad digital. Así es que permite la validación de certificados electrónicos, también contiene una autoridad de sellado de tiempo, servicio de firma con certificados “en la nube”, una plataforma de identificación de personas físicas en base a los certificados electrónicos y un cliente que permite la generación de firmas en local (PC o dispositivo móvil) en diferentes formatos. Es una herramienta muy interesante para

poder generar un ecosistema de firma electrónica e identificación digital. Si a su vez se acompaña con el TL Manager, software que permite la creación de listas de confianza con las cuales podemos plantearnos la interoperabilidad. Dado que las listas de confianza son la base para la verificación de los certificados de firma e identidad que puedan provenir de otros países.

Con lo cual esto nos lleva a tener un sencillo modo de interoperabilidad entre los países de América Latina, sino que además facilitaría la comunicación con otros grandes bloques comerciales a nivel global como ser la UE, Japón, Corea del Sur, etc. Dado que una vez que se tiene en funcionamiento, la integración de un tercero es sumamente rápida y sencilla.

Interoperabilidad organizativa Legal:

Debido a la asimetría en los marcos jurídicos nacionales sobre la materia, es necesario suscribir acuerdos con base en los estándares internacionales a fin de promover un entendimiento de las estructuras legales y técnicas de las Partes intervinientes en la materia. Así se logrará garantizar la seguridad jurídica en el procesamiento automático. El reconocimiento mutuo, bajo las condiciones previstas en los siguientes artículos, de la eficacia jurídica de los certificados de firma digital emitidos en alguna de las Partes, a los fines de otorgar a la firma digital o firma electrónica avanzada el mismo valor jurídico y probatorio que el otorgado en ambas Partes a las firmas manuscritas.

Firma electrónica avanzada, definida como datos en forma electrónica anexos a un documento digital que permite identificar al firmante o signatario y garantiza la integridad del documento.

Los certificados de firma digital emitidos en una de las Partes tendrán la misma validez jurídica para la otra Parte, siempre que sean emitidos por un prestador de servicios de certificación conforme a las siguientes condiciones:

- Que respondan a estándares internacionales, conforme lo establezca la autoridad designada por cada Parte.
- Que contengan, como mínimo, datos que permitan:

    - Identificar inequívocamente a su titular y al prestador de servicios de certificación que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única.
    - Ser susceptible de verificación respecto de su estado de revocación, de manera gratuita.
    - Detallar la información verificada incluida en el certificado digital.
    - Contemplar la información necesaria para la verificación de la firma.
    - Identificar la política de certificación, siendo esta estándar e interoperable, bajo la cual fue emitido**.**

- Que hayan sido emitidos por un prestador de servicios de certificación acreditado bajo el sistema nacional respectivo de acreditación y control.

Los Países preverán la evaluación y armonización de los aspectos relacionados con el ambiente operativo, entre otros los relacionados con:

- El control de los accesos a servicios y perfiles.

- La separación de las tareas y atribuciones relacionadas con cada perfil.
- Los mecanismos de seguridad aplicados a los datos e informaciones sensibles.
- Los mecanismos de generación y almacenamiento de los registros de auditoría.
- Los mecanismos internos de seguridad que garanticen la integridad de los datos y los procesos críticos.
- Los aspectos referidos a la seguridad física y lógica de las instalaciones.
- Los mecanismos tendientes a garantizar la continuidad del funcionamiento de los sistemas críticos.
- Otros aspectos relativos a la eficacia y seguridad del uso de certificados de firma digital.

También los Países dispondrán la evaluación y armonización de los aspectos relacionados con el sistema de control de prestadores de servicios de certificación acreditados, en especial aquellos relacionados con:

- El alcance y la periodicidad de las inspecciones y/o auditorías, las cuales deben contemplar como mínimo la revisión de las políticas y prácticas de certificación de seguridad, del ambiente de seguridad física y lógica, la evaluación de tecnologías utilizadas, los controles sobre la administración de los servicios, la selección y administración del personal y los contratos de tercerización.
- La identificación de los eventos a ser registrados, la información mínima de cada uno de ellos y lo procedimientos para garantizar la integridad y veracidad de los mismos.
- La documentación de respaldo del ciclo de vida de los certificados de firma digital reconocidos.

Con base a los puntos mencionados en esta sección es que se debería basar un acuerdo de reconocimiento mutuo entre países, para llegar a una interoperabilidad total. Está se debería realizar en paralelo con las implementaciones técnicas y la generación de las listas de confianza y la lista de listas.

Por estos motivos es que se recomienda que se debe comenzar a realizar el reconocimiento mutuo con el Certificado de Persona Física/Natural/Humana. Esto se debe a que es un tipo de certificado que todos los países tienen y además con las mismas características. El Certificado de Persona Física establece una asociación directa entre la identidad del individuo y su clave pública, con el respaldo brindado por la Infraestructura Nacional de Certificación Electrónica. Esta asociación clave pública-individuo es un componente imprescindible para la realización de una Firma Electrónica/Digital, ya que es la que permite a alguien que verifica una firma identificar al firmante.

Ahora abordaremos con más profundidad los puntos que se necesitan para el armado de un ecosistema de firma electrónica/digital en un país.

Modelo de operación de la autoridad certificadora y autoridad de registro

A continuación se dan una serie de definiciones para no generar ambigüedades en nomenclatura, ni en conceptos a manejar en este documento.

A nivel conceptual, la Firma Electrónica/Avanzada/Digital/Cualificada (y sus acepciones de nomenclatura según normativas de los países) consiste en un par de claves criptográficas, una pública y otra privada, aplicadas mediante una función matemática a documentos

electrónicos. La clave privada siempre se encuentra en exclusivo control del firmante y es la utilizada para realizar firmas. La pública se divulga y es la utilizada para verificar una firma de otro sujeto.

Infraestructura Nacional de Certificación Electrónica, de ahora en más la llamaremos por su sigla INCE.

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.

Prestador de Servicios de Certificación Acreditado (PSCA): persona física o jurídica acreditada ante el regulador o acreditador (según sea el caso) y responsable de la operación de al menos una Autoridad Certificadora de la INCE.

Autoridad de Registro: responsable del registro y procesamiento de solicitudes de emisión, renovación y revocación de certificados, incluyendo la validación de la identidad de los suscriptores y/o de las solicitudes al inicio del proceso.

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.

Política de Certificación (CP – Certificate Policy): 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 el regulador.

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.

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.).

Solicitud de Firma de Certificado (CSR – Certificate Signing Request): 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.

FIPS (Federal Information Processing Standard) 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.

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

Protocolo de Estado de Certificados Online (OCSP - Online Certificate Status Protocol): protocolo para la validación online del estado de revocación de certificados, de implementación opcional para los PSCA.

Política de certificados

Una Política de Certificación es un conjunto de principios y normas que describen el perfil de un Certificado; sus usos permitidos, los derechos y obligaciones de todos los actores involucrados en su utilización, los procesos mediante los cuales se verifica la identidad del titular del Certificado, se generan las claves, se emite y se revoca el Certificado y las garantías tecnológicas de seguridad que el PSCA aplica en cada caso.

Declaración de prácticas de certificación

La CPS es el documento en el cual se declara los procedimientos administrativos y técnicos mediante los cuales un PSCA satisface lo exigido por la Política de Certificación.

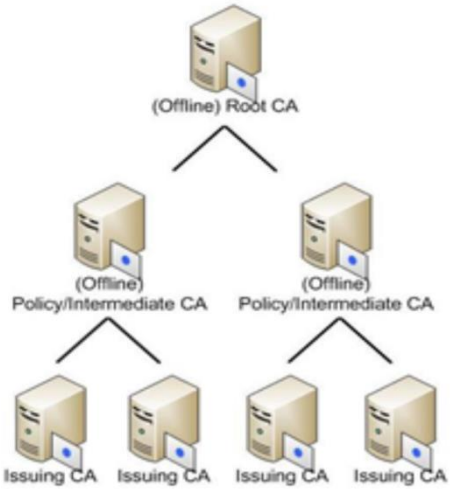


Figura 1

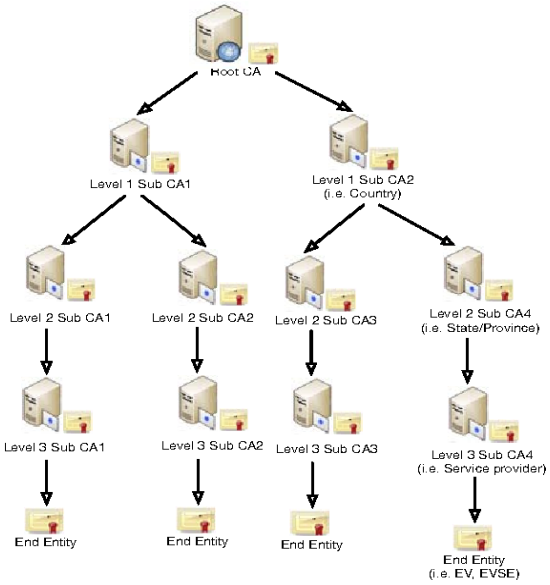


Figura 2

En las Figuras 1 y 2 se muestra una arquitectura típica de jerarquía de una PKI. En la primera se observa una arquitectura simplificada de solo 2 niveles en donde se ve el equipamiento offline y el que está en producción. En la figura 2 se una arquitectura jerárquica con una arquitectura más completa.

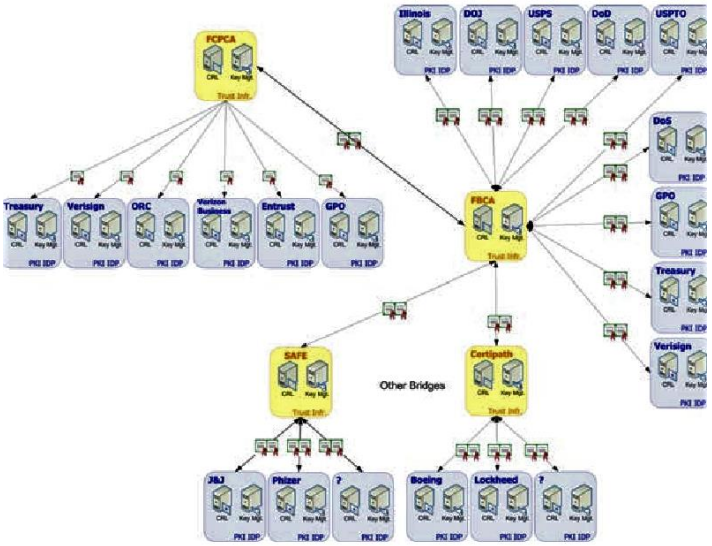


Figura 3

También existe una otro tipo de arquitectura, Figura 3, que es la federada donde existe más de una Raíz (Root CA), las cuales se cruzan certificados para manejar un mismo nivel de jerarquía.

Cabe aclarar que lo que se muestra en las Figuras 1,2 y 3 es el tipo de arquitectura que se puede adoptar para una PKI, indistintamente del modelo político de país. Esto es, sí un país es federal puede optar en implementar una arquitectura PKI federada o PKI jerárquica indistintamente, la elección será según su conveniencia a las necesidades internas. Lo mismo sucede sí un país es centralista su arquitectura PKI podrá ser una u otra dependiendo de sus necesidades.

Obligaciones de los PSCA

En el contexto del cual estamos conversando, estas son obligaciones que los PSC Acreditados, por el regulador, deben cumplir para la emisión de certificados:

- Desarrollar, mantener y publicar su propia Declaración de Prácticas de Certificación, en conformidad con lo pautado en la CP;
- Generar la clave privada de sus ACPA con aprobación del regulador, siendo la presencia de personal del regulador y de la ACRN una decisión de cada regulador en cada país, y de acuerdo a los requerimientos establecidos en la CP. Cumpliendo con los con los estándares Webtrust Principles and Criteria for Certification Authorities, como por ejemplo: la presencia de un auditor externo durante la ejecución de la ceremonia de claves, la presencia de un notario, o bien mediante video filmación.
- Proteger las claves privadas de sus ACPA.
- Solicitar la emisión del certificado de sus ACPA, de acuerdo a los procedimientos estipulados para tal fin en la Política de Certificación de la ACRN.
- Solicitar a la ACRN la revocación del certificado de sus ACPA ante sospecha real de compromiso de la clave privada asociada.
- Atender los requerimientos de revocación solicitados por el regulador o por los suscriptores, de acuerdo con la legislación vigente y con los procedimientos definidos en la CP.

- Utilizar el certificado de sus ACPA de acuerdo con los requerimientos de la Política de Certificación.
- La emisión y revocación de los certificados, generados de sus suscriptores;
- La emisión y publicación de su Lista de Certificados Revocados (CRL);
- Informar a sus suscriptores de la revocación de sus certificados, junto con la causal para dicha operación.
- Tener una disponibilidad de consulta de la CRL de 99.9% anual.
- Notificar a los suscriptores de los certificados emitidos por sus ACPA acerca de cualquier acontecimiento que pudiera ocasionar el compromiso de la clave privada de la ACPA y la emisión de un nuevo par de claves criptográficas, como también del procedimiento a seguir en ese caso.
- Garantizar el acceso permanente y gratuito de los suscriptores y Terceros aceptantes al sitio de publicación que contiene su propio certificado, y la lista de certificados revocados;
- Mantener y garantizar la seguridad de la información tratada (disponibilidad, integridad, no repudio o confidencialidad según corresponda)

Seguimos con otro punto crítico en lo que se refiere a la INCE, nos referimos a la Autoridad de Registro.

La Autoridad de Registro es la dependencia funcional que atiende y procesa las solicitudes de emisión, renovación o revocación de certificados de parte del Suscriptor. En este sentido, es el único punto de contacto requerido entre el PSCA y sus Suscriptores.

Puede o no estar integrada al PSCA, es decir puede ser un servicio dado por un tercero el cual se comunica con CA para que este genere el certificado electrónico correspondiente. Cuando el registro lo realiza el mismo PSCA se dice que tiene integrada una Autoridad de Registro y es el mismo el que realiza toda la operación hasta la emisión del certificado.

Como consecuencia de esto, la Autoridad de Registro es la responsable de la relación univoca persona física – certificado electrónico y quien da comienzo al procedimiento técnico de emisión, renovación o revocación de certificado. ***Único punto de unión entre la identidad de la persona física (identidad que tiene registrada el país en sus registros civiles) y la identidad de esta persona física en el mundo digital. Lo cual hace a esta función un punto de suma importancia en la cadena de confianza de un ecosistema PKI y a su vez uno de los puntos más críticos de dicha cadena, al cual hay que prestarle suma importancia y cuidado al momento de su funcionamiento. Dado que es aquí donde podrían suceder los casos de fraude o suplantación de identidad.***

Cabe aclarar que, no es objeto del documento la profundización en este punto, pero si se debe resaltar que la identidad digital de los ciudadanos de un país siempre estará relacionada con la identidad de la persona en el país como tal. Me refiero a la identidad que otorga la Institución mandatada a nivel Nacional para otorgar identidad a los ciudadanos de un país, típicamente el Registro Civil. Es decir, si existen problemas de subregistros, registros duplicados, que una persona tenga varios identificadores o hay inconvenientes con de identificación única, estos inconvenientes se trasladan a la identidad digital sí no se toman medidas adicionales que mitiguen estos inconvenientes.

La Autoridad de Registro hace entrega de los medios de control exclusivo de la clave privada o medios de creación de la firma electrónica al Suscriptor y le informa las buenas prácticas de

uso. Debe además, previo a la entrega del certificado, asegurarse que se firme el acuerdo con las Condiciones para la Utilización de Firma Electrónica.

Los Suscriptores contraen derechos y obligaciones al utilizar certificados electrónicos según se describe en la Política de Certificación

Los Terceros Aceptantes, al autenticar a una persona física o al aceptar una Firma Electrónica Avanzada, están obligados a comprobar la validez del certificado. Para ello, deberán seguir las etapas estipuladas en la Política de Certificación. En caso contrario, el Tercero Aceptante no contará con las garantías ni respaldo de la INCE, asumiendo su total responsabilidad.

Las obligaciones de las Autoridades de Registro de las ACPA, son asumidas por el PSCA en el caso que esta le pertenezca, o por las instituciones que hayan sido mandatadas, son las siguientes:

Recibir y procesar las solicitudes de emisión, renovación o revocación de certificados emitidos por la ACPA, de acuerdo a los requerimientos estipulados.

Comprobar la identidad de la persona física, la calidad de esta identificación está directamente relacionada, vincula, con la calidad de la identidad digital que tenga esa persona. Es importante para esto ***tener un criterio de unicidad de identificación***, esto es sí un país tiene más de una forma de identificar a sus ciudadanos este deberá optar por una de las opciones presentes. Se recomienda que sea por la opción más confiable y de mayor cobertura para permitir el uso masivo de estas tecnologías.
Aclarado el punto de la comprobación de Identidad, continuamos con los puntos referidos a las funciones de la Autoridad de Registro.

Entonces, comprobar la identidad de la persona física que solicita la emisión, renovación o revocación presencial, mediante la validación del documento de identidad presentado, de acuerdo a lo estipulado. En el caso de certificado de persona física, en caso de otro tipo de certificado deberá validar la documentación necesaria para el caso.

Notificar a los suscriptores de certificados emitidos por alguna de sus ACPA ante la ocurrencia de un evento que así lo requiera según lo estipulado en la Política de Certificación en la cual está basado el certificado.

A modo de ejemplo se realiza una descripción de cómo se debería realizar el procedimiento para un certificado para persona física.

Registró inicial,
Una Persona Física podrá solicitar la emisión de los certificados ante la Autoridad de Registro del PSCA. Dichos certificados serán emitidos bajo la presente Política de Certificación. La persona deberá demostrar ante dicha Autoridad de Registro su identidad, presentando la documentación que lo acredite.

Existe también la posibilidad de realizar registros a distancia (no presencial), pero para estos casos es fundamental tener un sistema robusto y confiable de identificación de las personas. Este registro a distancia debe basarse en ese sistema primario de identificación para tener

todas las garantías que la persona que se registra es quien dice ser. Esto lo puede hacer basado en el registro nacional de identificador de cada país o en un registro previo en una Autoridad de Registro en un ecosistema PKI.

La Autoridad de Registro del PSCA validará la autenticidad del documento presentado, así como también la identidad de la persona que solicita el registro, de acuerdo a los requerimientos de validación para el documento presentado.

Nominación
Una vez validada la identidad del solicitante, el nombre que se colocará en el certificado será el nombre completo del mismo, de la forma que figura en el documento presentado. De la misma forma se determinarán los datos de tipo y número de documento.

También, de ser posible y eso dependerá de la infraestructura de cada país, que los datos que se coloquen en el certificado provengan directamente del registro civil o la autoridad local encargada de realizar la identificación de los ciudadanos.

Formato del Nombre Distinguido

Para el nombre de la Persona se deberá utilizar el campo “Subject” del certificado emitido a través de la ACPA. El formato para indicar el nombre de la Persona deberá ser X.500 (Distinguished Name).

Dicho formato, se aplicará de la siguiente forma:

Country (C): País emisor del documento presentado, según la nomenclatura ISO 3166-1 (utilizando el código de dos letras).

Common Name (CN): Nombre Completo (Nombres y Apellidos) de la Persona Física titular del certificado, tal y como están escritos en el documento de identidad presentado y usando sólo letras mayúsculas.

givenName: Nombres de la Persona Física titular del certificado, tal y como están escritos en el documento de identidad presentado y usando sólo letras mayúsculas. Los distintos nombres deberán estar separados por comas.

surname: Apellidos de la Persona Física titular del certificado, tal y como están escritos en el documento de identidad presentado y usando sólo letras mayúsculas. Los distintos apellidos deberán estar separados por comas.

serialNumber: tipo de documento DNI o PSP, según se define en el perfil, más su número de documento de identidad. DNI corresponde a un certificado solicitado con Documento de Identidad Nacional, mientras que PSP corresponde a un certificado solicitado con Pasaporte.

A modo de ejemplo, para la persona “Juan José Pérez Gómez”, con DNI número 1.111.111-1, su nombre distinguido se conformaría de la siguiente manera:

- C=UY
- CN=JUAN JOSÉ PEREZ GÓMEZ
- givenName: JUAN, JOSÉ
- surname: PEREZ, GÓMEZ
- serialNumber=DNI11111111

En el caso de que el PSCA opere de forma independiente la Autoridad de Registro y la ACPA, debe implementar un mecanismo que asegure la integridad y autenticidad de la información asociada a los certificados y que transita de un sitio a otro.

En ningún momento, durante el procesamiento de la solicitud de certificado, el PSCA ni la Autoridad de Registro (sí está es independiente del PSCA) puede acceder a la clave privada del Solicitante ni al PIN que la protege.

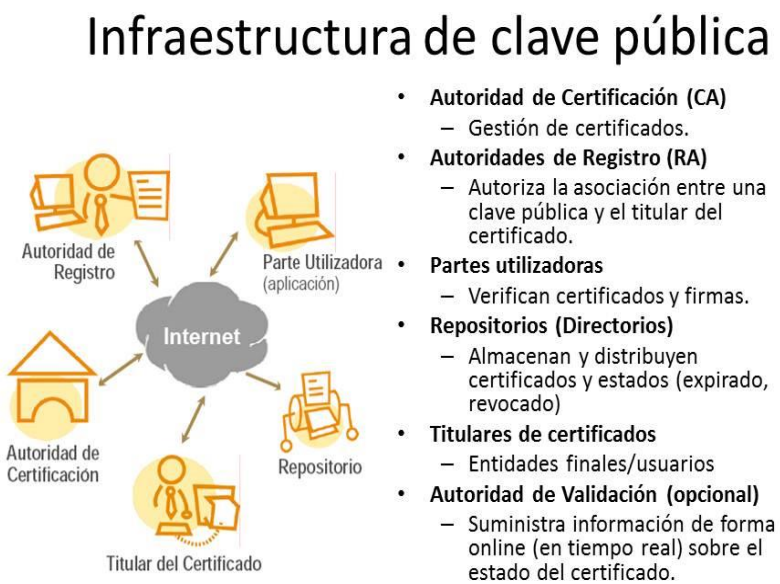


Figura describe una infraestructura mínima de PKI

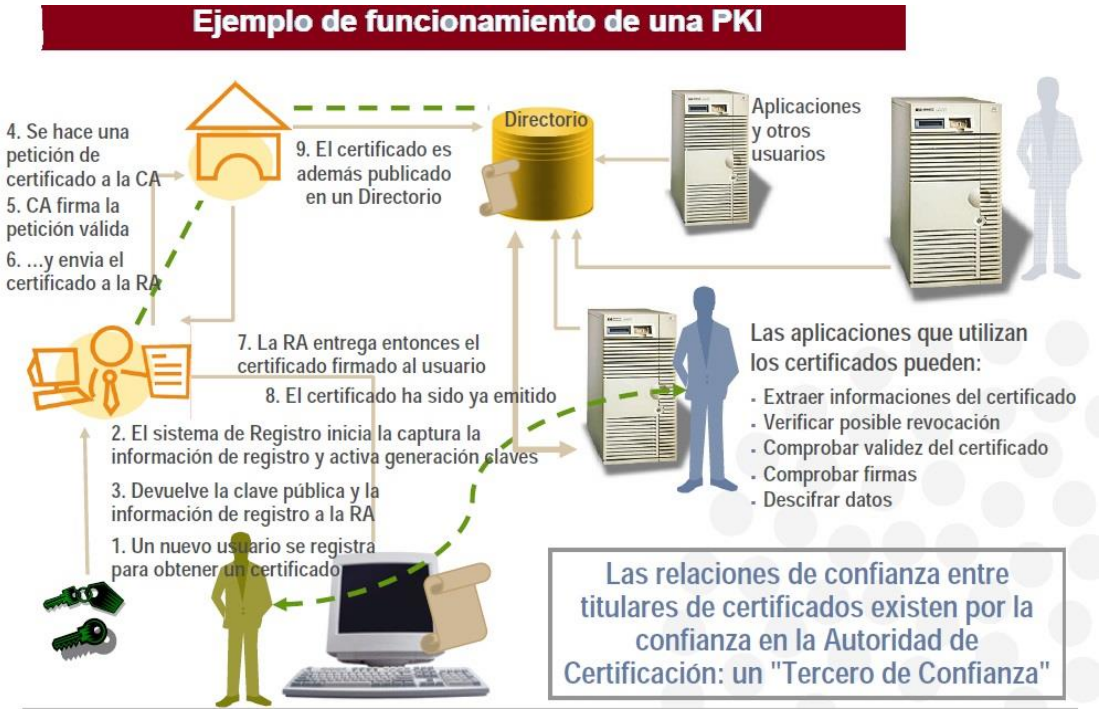


Figura esquemática del funcionamiento de una PKI a alto nivel

Plan de administración de claves criptográficas

El período de validez máximo del certificado de la ACRN es de veinte (20) años.
El período de validez máximo de los certificados emitidos por la ACRN bajo los certificados de las ACPA es el máximo posible al momento de la emisión, según la fecha de expiración del certificado de la ACRN. El período de validez del certificado emitido deberá ser el período comprendido entre la fecha de emisión y la fecha de expiración del certificado de la ACRN, excepto que sea revocado con anterioridad dicha fecha. Sin perjuicio de lo establecido, en caso que la evolución tecnológica pueda generar riesgo criptográfico, obsolescencia de sistemas o problemáticas afines, el regulador podrá determinar por vía regulatoria la obligatoriedad de efectuar las adecuaciones que entienda pertinentes.

La protección de la llave privada de la ACRN y de las ACPA debe realizarse con módulos criptográficos (HSM) que cumplan con la normativa FIPS 140-2 nivel 3.

Recomendación para los certificados de personas físicas el periodo de validez del mismo varía entre 2 años y 5 años como máximo eso dependiendo de la tecnología en la cual fue entregado al suscriptor. A modo de ejemplo; en un token criptográfico se recomienda 2 años máximos y en documento de identidad nacional puede llegar hasta 5 años.

Estructura de certificados digitales

Se utilizarán los siguientes campos del formato X.509 versión 3, definido en la RFC 5280.

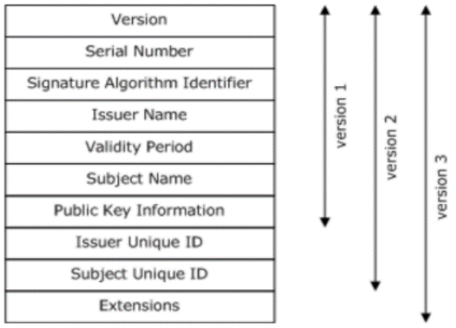


Figura muestra los campos que se utilizan según la versión del formato X.509

A modo de ejemplo se va a mostrar el perfil de un certificado de la ACRN.

Atributos	**Contenido**	
Versión (Version)	V3	
Número de Serie (Serial Number)	Número asignado por la ACRN	
Algoritmo de Firma (Signature Algorithm)	sha256RSA	
Nombre Distintivo del Emisor (Issuer DN)	CN =Autoridad Certificadora Raíz Nacional de País O = Nombre Institución que la Opera C = Código de País	
Validez (Valid From / Valid To)	20 Años (en formato desde/hasta)	
Nombre Distintivo del Suscriptor (Subscriber DN)	CN =Autoridad Certificadora Raíz Nacional de País O = Nombre Institución que la Opera C = Código de País	
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 4096 bits	
Atributos	**Criticidad**	**Contenido**
Identificador de la clave del suscriptor (Subject Key Identifier)	No Crítica.	Hash de 20 bytes del atributo Subject Public Key
Uso de Claves (Key Usage)	Critica	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0

Políticas de Certificación (Certificate Policies)	OID: X.XX.XXX.XXXXXXXX.XXXXX.X URI: donde se publica la política que genera el tipo de certificado OID: OID asignado a la CPS URI: URL de publicación de la CPS
Restricciones Básicas (Basic Constraints)	CA = TRUE Largo indefinido
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

A modo de ejemplo se va a mostrar el perfil de las ACPA

Atributos	**Contenido**
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACRN
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	CN =Autoridad Certificadora Raíz Nacional de País O = Nombre Institución que la Opera C = Código de País
Validez (Valid From / Valid To)	Período de validez asignado al momento de la emisión (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	Country: País del Prestador Organization: Nombre legal o de fantasía del prestador. Common Name: Nombre de la Autoridad Certificadora del Prestador
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 4096 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)	Identificador de la Clave Pública de la ACRN
Uso de Claves (Key Usage)	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1

	EncipherOnly = 0 DecipherOnly = 0
Uso de Claves Extendido (Extended Key Usage)	clientAuth, emailProtection
Políticas de Certificación (Certificate Policies)	OID: X.XX.XXX.XXXXXXXX.XXXXX.X URI: donde se publica la política que genera el tipo de certificado OID: OID asignado a la ACPA URI: URL de publicación de la CPS
Restricciones Básicas (Basic Constraints)	CA = TRUE Largo 0
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
Informacion de Acceso de la Autoridad Certificadora (Authority Information Access)	URI = URL donde se encuentra publicado el certificado público de la Raiz

A modo de ejemplo se va a mostrar el perfil de un certificado de persona física.

Atributos	**Contenido**
Versión (Version)	V3
Número de Serie (Serial Number)	Número asignado por la ACPA emisora
Algoritmo de Firma (Signature Algorithm)	sha256RSA
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 separados por comas. surname = Apellidos de la Persona Física serparados por coma.
Clave Pública del Suscriptor (Subject Public Key)	Clave pública RSA de 2048 bits o más
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: X.XX.XXX.XXXXXXXX.XXXXX.X URI: donde se publica la política que genera el tipo de certificado 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

Estructura de listas de revocación de certificados

El PSCA deberá actualizar la Lista de Certificados Revocados (CRL) de sus ACPA cuando ocurra al menos uno de los siguientes hechos:

- Se produzca la revocación de un certificado, con un margen de tiempo de 2 horas luego de la revocación;

- Transcurran como máximo 24 horas luego de la última emisión de CRL.

La CRL de la ACRN deberá ser actualizada cada 3 meses o cuando se produzcala revocación de un certificado. La CRL del PSCA deberá ser actualizada cada vez que revoque un certificado emitido y en caso de no haber revocaciones cada 2 días como máximo deberá actualizarla. Las CRL deben ser UTF-8.

En el perfil de la CRL se utilizarán los siguientes campos del formato X.509 versión 2, definido en la RFC 5280.

Atributos	Contenido
Versión (Version)	V2
Algoritmo de Firma (Signature Algorithm)	sha256RSA
Nombre Distintivo del Emisor (Issuer DN)	DN de la ACPA tal cual figura en su certificado
Día y Hora de Emisión (Efective Date)	Día y hora de la emisión de esta CRL
Próxima Actualización (Next Update)	Día y hora de la próxima actualización planificada de la CRL
Certificados Revocados (Revoked Certificates)	Lista de los certificados revocados. Incluye número de serie (Serial Number), fecha de revocación (Revocation Date) y motivo (Reason Code).
Extensiones	
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	Valor de la Extensión Subject Key Identifier del certificado de la ACPA
Número de CRL (CRL Number)	Secuencial que se incrementa con cada CRL emitida

Causas para la revocación

Las causas de revocación de un certificado son las siguientes:

- solicitud del Suscriptor;
- pérdida, sospecha de compromiso o destrucción del dispositivo criptográfico que contiene la clave privada del certificado;
- pérdida, sospecha de compromiso o destrucción de la clave privada del certificado;
- datos erróneos o inexactos en el certificado;
- fallecimiento del Suscriptor;
- revocación de la ACPA del PSCA que emitió el Certificado;
- resolución judicial que así lo determine;
- otros.

Algoritmos criptográficos para firma electrónica

RSA (Rivest, Shamir y Adleman): Sistema criptográfico asimétrico, o "de clave pública", utilizado para cifrado o para firmas electrónicas.
Usa RSA de SHA-256.

La ACRN deberá firmar los certificados emitidos con alguno de los siguientes algoritmos:

Sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11 }
Sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12 }
Sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 10 }

Si la ACRN firma certificados usando RSA con "PSS padding", la CA emisora podrá usar los siguientes algoritmos y OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Las ACPAs podrán generar pares de claves usando los siguientes algoritmos:

RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) idpublicKeyType(2) 1 }

Algoritmos Hash para firma electrónica

Actualmente se está utilizando para el par de claves generado el algoritmo RSA y tener un largo mínimo de 2048 bits.

El formato de los certificados de Persona Física deben cumplir con lo especificado en el estándar ITU-T X.509 versión 3 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile),

La codificación de caracteres de los certificados debe ser UTF-8

La clave privada no debe ser extraíble del dispositivo en que fue generada.

Se debe estar atento a la evolución de este algoritmo y los anuncios de cuando han sido vulnerados. Actualmente hay varios algoritmos a estudio pero aun ninguno se ha puesto en producción en la firma electrónica

Servicio OCSP

El servicios de OCSP es un servicio automático que permite a terceros consultar la revocación de un certificad de firma electrónica en un PCSA determina. El mismo es un servicio crítico el cual debe ser protegido de terceros maliciosos y mantener un tiempo de no disponibilidad mínimos.

Los mensajes OCSP debe ser UTF-8.

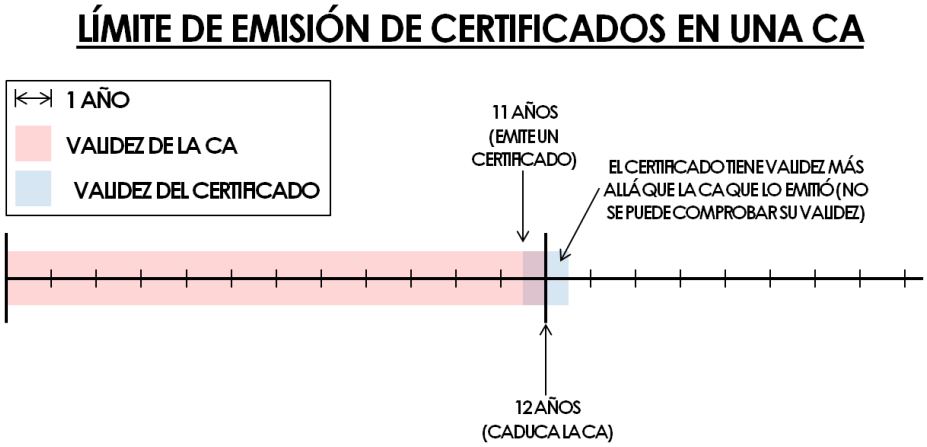
Ciclo de vida de los certificados

Una vez que están definidos los periodos de validez de los certificados para cada elemento de la PKI, se puede obtener el momento de renovación de cada uno de esos elementos. Es importante no confundir el momento en el que una CA deja de ser válida con el momento en el que hay que renovarla:

- **Fecha de caducidad del certificado de una CA:** es el día en el que el certificado de la CA deja de ser válido.
- **Fecha de renovación de una CA:** es el día en el que la CA ya no puede emitir certificados, porque la validez de los certificados que emita irá más allá de la validez del suyo propio.

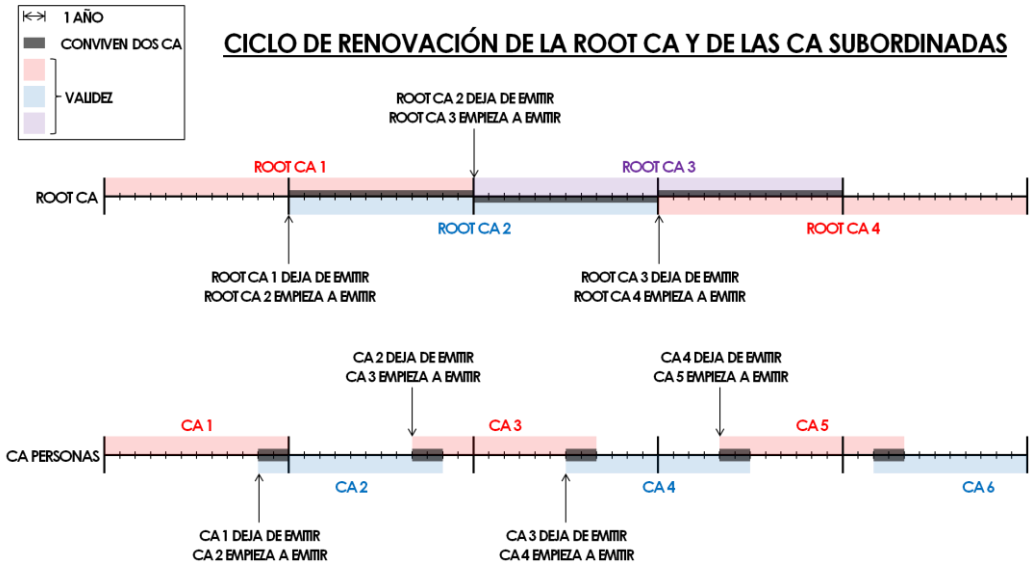
Pero sigue estando activa ya que su certificado sigue siendo válido. Se genera otra CA para que el sistema pueda seguir emitiendo certificados.

En la Figura a continuación se explica ejemplifica de una forma más clara.



Esta regla se puede generalizar de forma que, conociendo los periodos de validez de todos los elementos de una PKI, se puede deducir la fecha de caducidad y la fecha de renovación para cada uno de ellos. La fecha de caducidad coincidirá siempre con la fecha de caducidad de su certificado. Y para obtener la fecha de renovación, hay que restar a la fecha de caducidad la duración del certificado más corto que emita ese elemento.

La fecha de caducidad coincide con la validez del certificado de ese elemento. Mientras que la fecha de renovación coincide con la fecha de caducidad menos la duración del certificado más corto que emite ese elemento.
A modo de ejemplo, se usan los siguientes datos duración del certificado de la ACRN (para la figura de ejemplo RootCA) es de 24 años, certificado de la CA tiene una duración de 12 años, certificados emitidos a consumidores finales tienen una duración de 2 años.
Para la ACRN (RootCA, en la figura de ejemplo), su fecha de renovación se obtiene restando 24 años menos 12 años (ya que emite certificados a las CA). Y para las CA, se operaría de la misma forma. Como todas emiten certificados con una validez máxima de 2 años, su fecha de renovación será de 10 años. Esto significa que a los 10 años, dejarán de emitir certificados y habrá que crear otra que la sustituya para que el servicio siga operativo.



Auditorias de tercera parte

En este punto es donde cada integrante de la PKI realiza una auditoria por terceras partes, donde verifica y comprueba que sus procesos están cumpliendo con su declaración de prácticas. En caso de observarse desvíos realizar los ajustes necesarios para conservar la confianza en sus suscriptores y en el ecosistema mismo. Estas auditorías deberían realizarse en ciclos no mayores a dos años (los tiempos dependen de las realidades de cada mercado). Deben ser realizada por auditoras de renombre y con experiencia en este tipo de servicios e infraestructuras (a modo de ejemplo; Deloitte, KPMG, PWC, EY o empresas que cumplan con los requisitos antes mencionados). A modo de ejemplo también se mencionan algunos aspectos relevantes sobre la experiencia requería para las empresas que realicen esta tarea, deberán contar con diez años o más en auditorias de sistemas, cinco años en ISO 27001 y al menos tres años en infraestructura de llave pública (PKI).
Los resultados de estas auditorías realizadas por un PSCA deben ser reportados al regulador del ecosistema. Esto es para mantener la salud del ecosistema y del PSCA mismo.

Las mismas se deben basar en Web Trust 3.1 o superior, otra alternativa para una auditoría independiente de terceros es una auditoría que cumpla con ETSI EN 319 411-1 o ETSI EN 319 411-2, contemplando todos los aspectos legales y técnicos relacionados con el ciclo de vida de los certificados.
Se recomienda que haya una rotación de la empresa auditora a la hora de realizar las mismas. Procurando que la misma empresa auditora no realice la auditoria por más de dos veces consecutivas.

Pruebas de Ethical Hacking, penetración y escaneo de vulnerabilidades en la red

Una vez instalada la infraestructura es importante la realización de estas pruebas, en particular en las aplicaciones expuestas, para comprobar las vulnerabilidades de los sistemas instalados y la infraestructura de comunicación entre los mismos. También es recomendable la utilización de WAF (Web Aplication Firewal) delante de las páginas web de los servicios que se exponen a Internet.
Se recomienda que la empresa que realice los Ehtical Hacking así como los test de penetración y escaneo de vulnerabilidades no sea la misma empresa que en ese año haya realizado la auditoria de tercera parte. Dicha empresa cuente con un mínimo de dos años de experiencia en la realización de ese tipo de tareas.
También se recomienda incluir un análisis de riesgo de topología de red.
La frecuencia con la cual se deban realizar estas pruebas depende de la normativa generada por el regulador o acreditador en cada país.

Administración del Registro de auditoria transaccional

Tanto la ACRN como las ACPA deben tener definida una política de registros de auditoría (*logs*) que defina qué o*peraciones* se registran y c*ómo se* garantiza la integridad de esos registros. Mínimamente se deben registrar todas las actividades relativas a la gestión de claves (generación, destrucción, activación, desactivación, etc.), a la gestión de certificados (emisión, revocación, renovación, etc.) y a la emisión de CRLs y/o respuestas a consultas OCSP.

Estos controles deben ser implementados con el objetivo de registrar los eventos sucedidos. De esa manera puede realizarse un monitoreo continuo y la eventual reconstrucción de los eventos en caso de un incidente de seguridad.

Es importante mantener los registros de auditoria transaccional de los servicios que entrega el PCSA. Una buena práctica seria mantener mínimamente por seis meses estos registros o lo que estipule la legislación y normas de cada país.

También se deben implementar procedimientos para la revisión periódica de registros y detección de anomalías.

Los registros deben ser protegidos contra su eliminación o modificación implementando medidas administrativas y técnicas de control de acceso. El Oficial de Seguridad debe asumir la responsabilidad de su protección y deben adoptarse esquemas de contraposición de intereses en caso de ser necesario. Es clave la protección de la integridad y disponibilidad de los registros generados, por lo tanto los mismos deben ser almacenados de tal manera que no puedan ser destruidos ni borrados (a excepción de la transferencia a un medio de larga vida) por cualquier periodo de tiempo que se requiera retenerlos.

Servicio de monitoreo y control de eventos de seguridad

También es muy importante mantener un control y monitoreo sobre eventos de seguridad que puedan ocurrir en la Infraestructura instalada. Debiéndose realizar evaluaciones de vulnerabilidades cubriendo todos los activos relacionados a los productos y servicios de emisión de certificados. Las evaluaciones deben realizarse en las posibles amenazas internas como en las externas.

Recomendándose realizar periódicamente escaneo de vulnerabilidades a la red. Este ciclo podría ser de cada tres meses. Tener actualizado el/los WAFs con las ultimas reglas de detección. Por cada cambio de versión de los sistemas, mínimamente, realizar un testeo de penetración para verificar que no hayan surgido nuevas vulnerabilidades.

Mínimamente se deben implementar los siguientes controles:

- Controles para el acceso físico del personal a las instalaciones;
- Definición de perímetros de seguridad en función de la criticidad de la información;
- Inventario de activos físicos de información y controles periódicos de inventario;
- Controles para el ingreso y egreso de activos físicos de información;
- Controles para la protección de la infraestructura contra incendios e inundaciones;
- Controles para la protección contra factores climáticos tales como humedad y temperatura;
- Procedimiento para disposición de información.

Controles procedimentales
Los procesos que permiten el funcionamiento de la ACPA deberán estar documentados y basarse en la contraposición de intereses para las operaciones más críticas.
Cada PSCA deberá definir al menos los siguientes roles para la operación de sus ACPA:

- Custodio de clave.
- Oficial de Seguridad.
- Administrador de Sistemas.

Custodio de clave tienen asignada la responsabilidad de proteger la clave privada de la ACPA, tanto su copia de producción como su copia de respaldo.
Por esta razón, este rol debe ser ejercido por personas de confianza del PSCA, deben ser seleccionados de acuerdo a procedimientos que verifiquen sus referencias, antecedentes laborales y valores éticos y profesionales. Los Custodio de clave deben firmar con el PSCA un contrato de responsabilidad al asumir el rol.
Los custodios de clave participarán en la activación de la clave privada de la ACPA. Se entiende por procedimiento de activación de la clave privada, el procedimiento necesario para que la ACPA pueda realizar emisiones de certificados y CRL. Para este procedimiento, se requiere conocimiento dividido y contraposición de intereses. Esto significa que la clave privada no podrá ser activada únicamente por un custodio sino que se requerirá un mínimo de dos. Las ACPA podrán implementar un esquema del tipo M de N para la activación de la ACPA. En este esquema, se requerirán M custodios cualesquiera, con M mayor o igual a 1, de los N totales, mayor o igual a 2, para activar la ACPA. En cualquier caso, el PSCA será responsable porque siempre exista un conjunto de custodios de clave disponibles para activar la ACPA.

Un custodio de clave puede desempeñar otros roles, siempre y cuando se respete el esquema M de N al momento de operar con la clave privada de la ACPA.
Quienes desempeñen el rol de Oficial de Seguridad deberán revisar los registros generados durante la aplicación de los procedimientos internos de la ACPA. En esta revisión, deberán comprobar la aplicación de los controles y medidas de seguridad estipulados. A su vez, deberán contrastar estos registros con los registros de auditoría de los sistemas de información e informar en caso de existir datos que no se correspondan.

El Oficial de Seguridad no puede participar con otro rol en los procedimientos que revisa.

El Administrador de Sistemas es el responsable de implementar las medidas y controles técnicos de seguridad en los sistemas de información de la ACPA.

Controles de seguridad del personal

Mínimamente se deben implementar los siguientes controles:

- Ingreso de personal (políticas de selección, evaluación e inducción)
- Cambio de rol de la persona (asignación de permisos, cambio de privilegios de su cuenta de usuario, firma de contrato de confidencialidad o responsabilidad, etc.)
- Capacitación del personal (capacitación inicial y capacitaciones periódicas por rol, material utilizado para capacitación, planes de entrenamiento)
- Retiro temporal o definitivo del personal (bloqueo o eliminación de sus cuentas de usuario)
- Políticas para el trabajo de personal contratado (externo a la ACPA)
- Política de sanciones para incumplimiento de las normas de seguridad de la ACPA (acceso no autorizado, uso inadecuado de los sistemas, uso indebido de privilegios, etc.).

Controles para registros de auditoría
Estos controles deben ser implementados con el objetivo de registrar los eventos sucedidos. De esa manera puede realizarse un monitoreo continuo y la eventual reconstrucción de los eventos en caso de un incidente de seguridad. Es clave la protección de la integridad y disponibilidad de los registros generados.

Se deben implementar como mínimo los siguientes controles:

- Se deben registrar todas las actividades realizadas por individuos o por sistemas informáticos durante el ciclo de vida de los certificados:
    - registro y procesamiento de solicitudes;
    - emisión, renovación y revocación de certificados en la ACPA;
    - generación de la clave privada -en caso de que aplique-;
    - Firma de las Condiciones para la Utilización de Firma Electrónica.
- Los registros relativos a la validación de solicitudes y a la generación de claves así como aquéllos relativos a la información contenida en los certificados de los suscriptores y los certificados mismos deberán ser almacenados por un período compatible con las disposiciones normativas vigentes en materia de prescripciones.
- Los registros deben ser protegidos contra su eliminación o modificación implementando medidas administrativas y técnicas de control de acceso. El Oficial de Seguridad debe asumir la responsabilidad de su protección y deben adoptarse esquemas de contraposición de intereses en caso de ser necesario.

- Deben implementarse procedimientos de respaldo de los registros de auditoría y deben protegerse estos respaldos con los mismos requerimientos de seguridad que los registros originales.
- Deben implementarse procedimientos para la revisión periódica de registros y detección de anomalías o incidentes de seguridad.

Procedimientos para recuperación de desastres
Deben establecerse procedimientos que permitan la recuperación de los sistemas, continuidad de las operaciones y la protección de la información en el caso de que ocurra un desastre o el compromiso de un sistema o clave. Es especialmente crítica la continuidad de los servicios de revocación de certificados y publicación de CRL.
Se debe contar con un plan de continuidad de negocio para afrontar estas circunstancias.

Servicio de monitoreo y control de disponibilidad y capacidad de los componentes de red

Deben implementarse medidas adecuadas de protección para la operación de la ACRN y las ACPA si se encuentran conectadas en red. Por ejemplo, división de la red de la organización en capas, ubicando la ACPA en un segmento crítico al que no sea posible el acceso desde Internet. Si la Autoridad de Registro de la ACPA cuenta con un portal *online* y además está conectada a la ACPA para la emisión de certificados *online*, esta conexión debe estar sujeta a estrictos controles de seguridad a nivel de red, como por ejemplo mediante firewalls, controles de acceso y auditoría (logs).

Garantías a través de pólizas de seguros

De acuerdo con las normas establecidas (Ley de creación de firma electrónica) establece la obligación de constituir garantía de solvencia económica para quienes pretendan devenir en Prestadores de Servicios de Certificación Acreditados. Estos deberán constituir un seguro de responsabilidad civil para afrontar el riesgo frente a posibles daños y perjuicios que puedan ocasionar, el cual puede ser sustituido total o parcialmente mediante aval bancario.

Además los PSCA deberán cumplir con toda normativa que rija en su país respecto de cubrir pérdidas sufridas por los suscriptores y terceros de buena fe.

Infraestructura y recursos mínimos

Para tener un mínimo de infraestructura y poder armar un sistema de certificados de firma electrónico, se necesita contar con una arquitectura jerárquica de 2 niveles en donde se encuentre una ACRN y un PSCA.

En el caso de la ACRN, además de los procedimientos de operación que se deben declarar en la CP y la CPS, se necesitara como mínimo un operador del sistema, un oficial de seguridad, tres custodios de clave (M de N) y un administrador. Como infraestructura un servidor, un HSM, el software de generación de claves y el de creación de políticas.

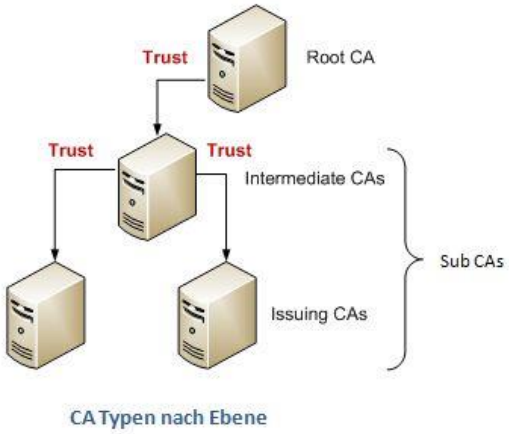


Figura muestra una arquitectura mínima de INCE.

En el caso de un PSCA es bastante distinto porque aquí no solo es necesario el equipamiento para la creación de certificados electrónicos sino también toda la infraestructura de red para publicar servicios, CRLs, comunicación con la Autoridad de Registro, etc. Además de los controles de seguridad de red, de acceso lógico y físico respecto de la infraestructura del PSCA.

Requisitos de aseguramiento para que los PSCA obtengan y mantengan la acreditación

Para obtener que una empresa obtenga la acreditación de parte del Regulador o Acreditador, según aplique, y poder operar convertirse en un PSCA, deberá cumplir todos los requerimientos que se hayan puesto en las normativas nacionales de cada país, esto es Leyes y Decretos, además de las que mencione el regulador. Estos últimos de forma general fueron descriptos a lo largo de este documento.

El mantenimiento de la acreditación dependerá mayormente del PSCA el cual cumpla con las normativas estipuladas por el regulador o entidad acreditadora (según sea el caso), realice las auditorias establecidas y no tengo fallos de seguridad, ni errores no subsanables a la hora de emitir certificados. Igualmente en el caso de eventos de infortunio por parte del PSCA el mantenimiento de la acreditación dependerá, claramente, de los criterios adoptados por el regulador.

Normas

A continuación se listan las normas a las cuales mínimamente se debe consultar para la generación de una INCE.

- ITU X.509: Information technology – Open Systems Interconnection – The Directory.
- IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate.
- Revocation List (CRL) Profile.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI draft TR 103 684: Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services.
- ETSI TS 119 612: Electronic Signatures and Infrastructures (ESI); Trusted Lists.
- IETF RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- ISO 8601: DATE AND TIME FORMAT.
- IETF RFC 5646: Tags for Identifying Languages.
- ISO 3166-1: COUNTRY CODES.
- ISO 27001: Information Security Management.
- NIST Cyber Security Framework.
- XAdES BES: Basic Electronic Signature.
- XAdES EPES: Explicit Policy-based Electronic Signature
- (RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP)
- Norma ETSI TS 102 42, para definiciones básicas del modelo de operación de la autoridad de certificación.
- ISO/IEC 9594-8 Information technology -- Open Systems Interconnection -- The Directory -- Part 8: Public-key and attribute certificate frameworks.

Referencias Externas

1. Chokhani, Ford, Sabett, Wu. RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Internet Engineering Task Force (IETF), 2003.

2. 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.

3: CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, 2011-2013.

4: ITU-T Study Group 17, International Standar ISO/IEC 9594-8 | Recommendation ITU-TX.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2012.

5. Unidad de Certificación Electrónica. Política de Certificación de la Autoridad Certificadora Raíz Nacional, 2011. Infraestructura Nacional de Certificación Electrónica República Oriental del Uruguay

6. Unidad de Certificación Electrónica. Condiciones para la Utilización de Firma Electrónica Avanzada, 2012. Infraestructura Nacional de Certificación Electrónica República Oriental del Uruguay

7. Resumen Ejecutivo, Decreto de Servicios de Confianza, Unidad de Certificación Electrónica. Julio 2017.

8. Implementación de una infraestructura de clave pública – PKI Institución Universitaria Politécnico Grancolombiano, 2013.

9. Digital Certificates, Indiana State University, Octubre 2015.

10. Diseño e implementación de una infraestrutura PKI, Universidad de Oviedo, Febrero 2019.

11. Documento de recomendaciones para facilitar la interoperabilidad de los certificados, Banco Interamericano de Desarrollo (BID), 2019.

12. TDR firma digital transfronteriza, Programa para el fortalecimiento de las transacciones electrónicas transfronterizas en América Latina y el Caribe, RG-T3314, 2019.

13. Checklist de requisitos técnicos e infraestructura, Everis – Astrea, 2018.