CPS

ID-digital Firma Electrónica Avanzada

Declaración de las prácticas de certificación de ID-digital

Versión 2.00

Fecha de Publicación: Diciembre del 2013

Derechos y obligaciones fundamentales

El presente documento y todos los documentos anexos al mismo sirven de base para regular cualquier aspecto concerniente a la vida de los certificados generados por ID-digital (solicitud, emisión, aceptación, renovación, remisión y revocación de certificados) en carácter de Prestador de Servicios de Certificación Acreditada (PSCA) bajo la Autoridad Certificadora Raíz Nacional (ACRN) y regulados por la Unidad de Certificación Electrónica (UCE). De manera adicional, el presente documento regula el régimen jurídico que se establece entre el Solicitante, ID-digital, los Usuarios y terceros. Asimismo se establece la responsabilidad de ID-digital y de los Solicitantes y Usuarios, así como la limitación de la misma ante una posible reclamación por daños y perjuicios.

Con objeto de dar a conocer tanto a los Solicitantes como a los Usuarios las normas y reglas especificas a aplicar en el sistema de certificación para Firma Electrónica Avanzada de ID-digital, este documento y demás documentos afines, ya sean estos anexos o documentación adicional, estarán disponibles en http://www.id.com.uy.

ID-digital, como ACPA emite diversos tipos de certificados, cada uno de ellos de acuerdo a las condiciones establecidas en la presente CPS y en las correspondientes prácticas de certificación, por esta razón, el Solicitante de un certificado de ID-digital deberá conocer todas las cláusulas y condiciones para el tipo de certificado a usar, de manera que pueda proceder correctamente a la solicitud y uso del mismo.

Para garantizar los mecanismos de seguridad y validez de los certificados de ID-digital, el Solicitante o el Usuario debe ser responsable de la custodia de las claves privadas de su certificado, siendo consciente que de no tomar las medidas adecuadas, la seguridad y validez del certificado se podría ver comprometida. Por esta razón, si sucede alguna causa de revocación del certificado establecidas en la presente CPS, es necesario informar inmediatamente a ID-digital para proceder a la revocación del certificado y de esta manera evitar un uso ilegítimo por parte de un tercero no autorizado.

Es también obligación de los solicitantes o de los usuarios comunicar a ID-digital cualquier modificación o variación de los datos que se aportaron para obtener el certificado, tanto si éstos aparecen en el propio certificado como si no. Así como es obligatorio que los Usuarios comprueben en la CRL de Certificados publicado por ID-digital que el certificado en el que pretende confiar es válido y no ha caducado o ha sido revocado.

Contenido

1. Introducción

1.1 Presentación

El presente documento constituye el **Documento de Practicas de Certificación** (Certificate Practice Statement) de ID-digital (a partir de aquí **CPS)**.

El alcance y objetivo del presente documento está limitado a la definición y descripción de las políticas, prácticas y procedimientos empleados por ID-digital para brindar Servicios de Certificación. De esta manera se pretende dar transparencia al conjunto de tareas relacionadas con la provisión de estos servicios.

Esta CPS asume que el lector conoce los conceptos de PKI, certificado y firma digital, en caso contrario se recomienda al lector que se forme en el conocimiento de los anteriores conceptos antes de continuar con la lectura del presente documento.

La presente CPS es conforme con la especificación del RFC 2527 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework ” propuesto por S. Chokhani y W. Ford, del Internet Engineering Task Force (IETF), para este tipo de documentos, y su actualización en la RFC 2547.

1.2 Identificación

1.2.1 Versión

Nombre: CPS Id-Digital firma electrónica avanzada
La Versión es la número: 1
Fecha de elaborada: 11/09/2013
Fecha de actualizada: 17/12/2013

Referencia de la CPS / OID (Object Identifier Digital): x.x.x.x.x.x.xxxx.x.x. *

*El numero de OID será suministrado por PKI Uruguay al momento de acreditarse.

1.2.2 Publicación

El presente documento está publicado en formato electrónico en la siguiente URL: http://www.id.com.uy/cps.pdf

1.3 Comunidad de usuarios y ámbito de aplicación

1.3.1 Unidad Reguladora

El rol de Unidad Reguladora en PKI Uruguay es desempeñado por la UCE, y sus funciones están estipuladas en la Política de Certificación de la ACRN.

1.3.2 Autoridad de Certificación

La presente CPS especifica la actuación de ID-digital como ACPA la cual se basa en la relación de una determinada clave pública con un sujeto concreto (ya sea este sujeto físico o fiscal) por medio de la emisión de un Certificado que avala esta relación.

Id-digital para firma electrónica avanzada será una Autoridad de Certificación Subordinada a ACRN, cumpliendo con todas las normativas y regulaciones que ello implica en materia de certificación.

1.3.3 Autoridad de Registro

La Autoridad de Registro (AR, Registry Authority, desde ahora AR) de ID-digital, será la encargada de la gestión de solicitudes de certificación. Entre las funciones de la gestión de solicitudes cabe destacar la de identificación de los Solicitantes de Certificados, esta identificación se llevara a cabo de acuerdo a las normas y procedimientos de esta CPS y siempre actuara en conjunto con la AC de ID-digital.

1.3.4 Autoridad de Registro Subcontratada

La autoridad de registro subcontratada en adelante ARSub se entiende una Persona física o jurídica con una vinculación contractual con ID-digital.

La autoridad de registro subcontratada estará sujeta a las obligaciones y responsabilidades que se derivan de lo establecido en esta CPS y en las prácticas de certificación de las AR para cada tipo de Certificado.

La autoridad de registro subcontratada actuará como intermediario o extensión de la AR de ID-Digital y el usuario final.

Esto está amparado en la resolución Nº 05 2011 emitida por UCE.

1.3.5 Personas Finales o Suscriptores

1.3.5.1 Solicitante

Como Solicitante se entiende la persona física autorizada para presentar la solicitud de un Certificado. La autorización estará regulada por cada una de las prácticas de certificación establecidas por las AR y la ACRN, detallado en las prácticas de certificación de ID-digital.

1.3.5.2 Usuarios Finales

Como Usuario del Certificado se entiende la persona que confía y hace uso de los Certificados de la AC de ID-digital, o tercero aceptante en las políticas de pki Uruguay.

El uso y el ámbito de aplicación de cualquier certificado de ID-digital está regulado por la presente CPS, por las prácticas de certificación aplicables en cada caso.

1.3.5.1 Terceros Aceptantes

En el contexto de PKI Uruguay, usuarios que validan y confían en certificados emitidos por una Autoridad de Certificación de la PKI, sea la ACRN o una de las ACPA.

1.3.6 Ámbito de Aplicación

1.3.6.1 Tipos de Certificados

Existen distintos tipos de certificados emitidos por ID-digital para firma Electrónica Avanzada, cada unos de los cuales están definidos por medio de esta CPS en función de las CPs emitidas por UCE.

Dentro de la definición de cada certificado está regulado la aplicabilidad de un certificado con relación a una comunidad de usuarios y unos usos determinados con unos requisitos de seguridad comunes de acuerdo a los términos de esta CPS.

1.3.6.2 Limitaciones de uso

El suscriptor sólo puede dar a los certificados digitales los usos que se especifican en esta Declaración de Prácticas de Certificación. Cualquier otro uso que se le dé se considerará una violación de esta CPS y constituirá una causa de revocación del certificado digital y de terminación del contrato con el suscriptor.

El suscriptor considera y acepta que los productos y servicios que se anuncian son tal y como se ofrecen individualmente, que no existe ningún tipo de información implícita que implique servicios o prestaciones adicionales a los expresamente mencionados y que la utilización de los mismos es de su exclusiva responsabilidad.

Si durante el periodo de vigencia parte o toda la información contenida en el certificado digital pierde actualidad o validez, el suscriptor deberá iniciar el procedimiento de revocación del mismo de conformidad con lo establecido en la sección de Revocación de certificados digitales de esta CPS.

Los certificados digitales deberán utilizarse tal y como son suministrados por ID-digital. Se encuentra terminantemente prohibida cualquier alteración de los mismos, sin excepción alguna.

Los certificados emitidos por ID-Digital para firma electrónica avanzada bajo la Política de Certificación de la ACRN y de acuerdo a sus prácticas de certificación para cada uno de los tipos existentes tiene el uso y alcance definidos por ACRN en sus CPs.

Los certificados no pueden ser utilizados con otro fin. La utilización de la llave privada asociada al certificado para otro fin es considerada causal de revocación del mismo (ver Política de Certificación de la ACRN). http://www.uce.gub.uy/acrn/cps_acrn.pdf

1.3.6.3 Puntos de solicitud de certificados

Los Servicios de Certificación de ID-digital son ofrecidos en todas las oficinas o agencias de Abitab S.A.

Una lista actualizada de dichas oficinas se encuentra en: http://www.abitab.com.uy

1.3.6.4 Servicios ofrecidos

Entre los servicios de certificación ofrecidos por ID-digital se incluyen:

- Firma de certificados
- Emisión de certificados
- Revocación de certificados
- Servicio de validación mediante OCSP y CRL

1.4 Detalles del contacto

Los servicios de certificación de ID-digital certifican claves en nombre de la institución detallada a continuación, la cual es la responsable del registro, mantenimiento e interpretación de esta política de certificación:

Nombre de la Institución: Abitab S.A.

Casa Central o Sede Social: Fernández Crespo 2143

Teléfono: 29245825 int. 7162
Fax 29245825 int 524-526
Correo Electrónico: pki@id.com.uy

1.5 Procedimiento de Aprobación

El sistema documental y de organización de la CPS de ID-Digital garantiza, a través de la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de esta Declaración de Prácticas de Certificación y de las especificaciones de servicios que están relacionados. Se prevé, de esta forma, el procedimiento de modificación de especificaciones del servicio y el procedimiento de publicación de especificaciones del servicio.
Las modificaciones finales de la Declaración de Prácticas de Certificación son aprobadas por la Gerencia del Servicio PKI de Abitab una vez haya sido comprobado el cumplimiento de los requerimientos establecidos en las diferentes secciones de la presente Declaración de Prácticas de Certificación.

1.6 Definiciones y Abreviaturas

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

Prestador de Servicios de Certificación Acreditado (PSCA): entidad acreditada ante la UCE y responsable de la operación de una Autoridad de Certificación de PKI Uruguay.

Autoridad Certificadora del Prestador Acreditado (ACPA): suscriptor de los certificados emitidos por la ACRN que, durante su operativa, emite certificados a usuarios finales bajo las prácticas de certificación que le fueron asignadas.

Terceros aceptantes: en el contexto de PKI Uruguay, usuarios que validan y confían en certificados emitidos por una Autoridad de Certificación de la PKI, sea la ACRN o una de las ACPA.

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 PKI Uruguay estas políticas son promovidas, aprobadas y mantenidas por la UCE.

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 la ACPA bajo el estándar PKCS#10 mediante el que solicita y provee información a la ACRN para la emisión de un certificado firmado por ella.

Escrow: acuerdo mediante el cual una clave privada puede ser custodiada por una entidad y, bajo ciertas circunstancias, ser devuelta a su legítimo dueño.

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.

La autoridad de Registro Subcontratada

La autoridad de registro subcontratada (ARSub) se entiende una Persona física o jurídica con una vinculación contractual con ID-digital.

1.7 Certificado de la Autoridad

1.7.1 Introducción

El certificado de la Autoridad Certificadora Raíz Nacional (ACRN) es el certificado de nivel más alto en la jerarquía de la Infraestructura Nacional de Certificación Electrónica (INCE). Este certificado es usado para verificar todas las firmas digitales realizadas por el Servicio de Certificación de ID-digital.

Este certificado contiene la clave pública correspondiente a la clave privada utilizada para firmar el certificado AC de los Servicios de Certificación de ID-digital para firma electrónica avanzada. Adicionalmente, dicho certificado contiene la información detallada en el punto 1.6.2.1

El certificado de ID-Digital es un certificado Subordinado al ACRN y el este certificado es usado para verificar todas las firmas digitales realizadas por el Servicio de Certificación de ID-digital.

Este certificado contiene la clave pública correspondiente a la clave privada utilizada para firmar todos los certificados emitidos por los Servicios de Certificación de ID-digital. Adicionalmente, dicho certificado contiene la información detallada a continuación 1.6.2.2

1.7.2 Certificado ACRN

El certificado de los Servicios de Certificación de ACRN es un certificado X.509 versión 3

1.7.2.1 Perfil

Ver la CPs de la ACRN

http://www.uce.gub.uy/acrn/cps_acrn.pdf

1.7.2.2 Certificado de ID-Digital

Ver la CPs de la ACRN

http://www.uce.gub.uy/acrn/cps_acrn.pdf

2. Reglamento general

2.1 Obligaciones

2.1.1 Obligaciones de la AC

Ver la CPs de la ACRN

http://www.uce.gub.uy/acrn/cps_acrn.pdf

2.1.2 Obligaciones de la AR

Ver la CPs de la ACRN

http://www.uce.gub.uy/acrn/cps_acrn.pdf

2.1.3 Obligaciones de la ARSub

- Asegurarse de que toda la información entregada en la solicitud del Certificado es cierta y completa. Asimismo, verificar la identidad del solicitante en el proceso de la aceptación de la solicitud.
- Cumplir todos los términos y condiciones del contrato con la AC o con la AR.
- Cualquier obligación que se pueda derivar del contenido de esta CPS o de las Prácticas de Certificación.

2.1.4 Obligaciones del Solicitante

Los solicitantes tienen las siguientes obligaciones:

a) Tomar conocimiento y aceptar los términos definidos en el presente documento, incluyendo y sin limitarse a:

i. garantías y usos aceptables del certificado de la ACRN;
ii. garantías y usos aceptables de los certificados emitidos por la ACRN a las ACPA;
iii. obligaciones de los Terceros aceptantes

b) Tomar conocimiento y aceptar los términos definidos en la política de certificación bajo la cual el PSCA le emitió el certificado al suscriptor final;

c) Verificar la validez del certificado de la ACRN. El certificado de la ACRN es considerado válido cuando:

i. Se encuentra dentro de su período de vigencia,
ii. Su firma electrónica avanzada puede ser verificada con el uso del mismo certificado de la ACRN, y no ha sido revocado según la CRL publicada por la ACRN.

d) Verificar la validez de los certificados emitidos por la ACRN a ID-Digital. El certificado es considerado válido cuando;

i. Se encuentra dentro de su período de vigencia,
ii. Su firma electrónica puede ser verificada con la clave pública del certificado de la ACRN, y no ha sido revocado según la CRL publicada por la ACRN.

e) Verificar que el certificado emitido por Id-Digital sea utilizado para los propósitos previstos en esta política de certificación;

Las verificaciones requeridas en los puntos anteriores deben ser realizadas cada vez que el tercero confíe en un certificado emitido por ID-Digital a un suscriptor final.

2.1.5 Obligaciones de los Usuarios

- Un usuario como parte que confía, y hará uso, de los Certificados emitidos por ID-digital tiene como obligación la verificación de la validez de las firmas emitidas por la AC.
- Si los Usuarios no proceden a esta verificación de las firmas, haciendo uso de la CRL publicada, la AC declina la responsabilidad del uso y confianza que los Usuarios hagan de estos Certificados, puesto que esta es responsabilidad de ellos.
- La confianza de una persona en una firma electrónica emitida a través de un Certificado de ID-digital se establece en la medida en que sea razonable hacerlo. Para determinar esto se tendrá en cuenta:
  - Los límites de uso de certificados permitidos de los mismos, de acuerdo a la lista que aparece en esta CPS. Si la operación que pretende avalar la Firma puede considerarse que vulnera la citada lista se considerará razonable no confiar en una firma emitida por un certificado de ID-digital.
  - Para confiar en un certificado se deberá determinar la validez en el momento de realizar o verificar cualquier operación basada en los mismos, en particular, si se ha comprobado que el certificado no esté caducado, suspendido o revocado. La caducidad del certificado deberá constar en el propio Certificado y la posible suspensión o revocación del Certificado deberán ser consultadas en la lista de revocaciones de certificados (CRL).
  - Las políticas y procedimientos que rigen la actividad de ID-digital con relación a las firmas emitidas mediante certificados por el emitidos y que se especifican en su CPS y en cada una de las Prácticas de Certificación emitidas para cada tipo de Certificado.
  - Cualquier otro elemento que se consideré oportuno.
- La confianza en un Certificado de ID-digital de deberá tener en la medida en que sea razonable hacerlo. Para determinar esto se tendrá en cuenta:
  - Cualquier restricción a que pueda estar sujeto el certificado, de acuerdo a lo establecido en la CPS y en cada una de las Prácticas de Certificación emitidas para cada tipo de Certificado.
  - Para confiar en un certificado se deberá determinar la validez en el momento de realizar o verificar cualquier operación basada en los mismos, en particular, si se ha comprobado que el certificado no esté caducado o revocado. La caducidad del certificado deberá constar en el propio Certificado y la posible revocación del Certificado deberán ser consultadas en la lista de revocaciones o suspensiones de certificados (CRL o OCSP).
  - Las políticas y procedimientos que rijan la actividad de ID-digital con relación a las firmas emitidas mediante certificados emitidos y que se especifican en su CPS y en cada una de las Prácticas de Certificación emitidas para cada tipo de Certificado.
  - Cualquier otro elemento que se consideré oportuno.
- Obligación de conocer las garantías y responsabilidades aplicables en la aceptación y uso de los certificados en los que y aceptar sujetarse a los términos, condiciones y límites contenidos en esta CPS por los cuales se garantiza la prestación de los servicios de certificación.

2.2 Responsabilidad

2.2.1 Responsabilidad de la AC

La AC de ID-DIGITAL no asume ninguna responsabilidad en los siguientes casos:

- Por daños derivados de o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo de la AR, del Suscriptor, del Solicitante, o del Usuario.
- Por el uso indebido o fraudulento de los Certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información suministrada por la AC.
- Por los posibles errores existentes en el Certificado que deriven de la información facilitada, habiendo actuado siempre con la máxima diligencia posible.
- Daños ocasionados por el uso de certificados incumpliendo las limitaciones de uso que se señalan en esta CPS y en las prácticas de certificación aplicables en cada caso.
- De la no ejecución o retraso en la ejecución de las obligaciones establecidas en la CPS si esto fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que la AC no pueda tener un control razonable.
- Del contenido de aquellos documentos firmados digitalmente por certificados de ID-DIGITAL, ni de aquellas páginas web que hagan uso de un certificado.

Independientemente de todo lo expuesto, cualquiera que sea la causa por la que pudiera reclamarse responsabilidad a la AC o la AR, la indemnización no será superior, salvo en el supuesto de culpa grave o dolo, de la cantidad de 5.000 U$S.

2.2.2 Responsabilidad de la AR

Es responsable de la realización de aquellas funciones que le corresponden en conformidad a la presente CPS y, en concreto, se asume toda la responsabilidad por la correcta y exacta autenticación y validación del Solicitante y del Suscriptor, asumiéndose las mismas limitaciones establecidas en el apartado anterior con relación a la AC.

2.2.3 Responsabilidad de la ARSub

En caso de incurrir en actos u omisiones culposos o dolosos por su parte, se compromete a indemnizar a la AC por los daños o perjuicios ocasionados, incluyendo los gastos judiciales, costas de Abogados y Procuradores, en que la AC pudiera incurrir por esta causa.

2.2.4 Responsabilidad del Usuario

Asumir toda responsabilidad en la correcta verificación de las firmas y certificados digitales, y por tanto de los riesgos derivados de la aceptación de un Certificado sin haber realizado previamente dicha verificación, dejando exenta a la AC de responsabilidad por dicho concepto.

2.3 Responsabilidad financiera

Este punto está incluido en las responsabilidades de la AC. Definido por los requerimientos de la UCE.

2.4 Interpretación y ejecución

2.4.1 Leyes aplicables

El presente documento y las Prácticas de Certificación aplicables en cada caso, se regirán por las leyes aplicables en Uruguay sobre certificación y firma digital vigente, de acuerdo a lo cual deberá ser interpretado su contenido.

2.4.2 Independencia, subrogación, y notificaciones

2.4.2.1 Independencia

En aquellos casos en que se pueda dar que, una o más cláusulas de este documento sea, o en un futuro lo sea, no valida, ilegal, o por motivos legales no pudiera llevarse a la práctica, este hecho no afectará a ningún otro punto o cláusula del presente documento. En este caso, el procedimiento a seguir será que aquel punto o puntos inaplicables de este documento se entenderán como si nunca hubieran estado contenidos en esta CPS, y de esta manera la interpretación de la misma podrá mantener el espíritu original.

La AC podrá modificar cualquiera de las cláusulas de la presente CPS en los términos previstos en esta CPS.

2.4.2.2 Subrogación

Se establece la posibilidad de que la AC de ID-Digital pueda transmitir a un tercero los servicios de certificación que presta, siempre junto con todas las obligaciones y derechos que se deriven de esta CPS.

Si se da en el futuro esta subrogación, la AC tendrá como responsabilidad la notificación de esta transmisión de servicio a los Usuarios cuyos Certificados estén en vigor con una antelación mínima de dos meses, los cuales, según los términos de esta CPS, aceptan esta posibilidad. El nuevo prestatario del servicio de certificación mantendrá esta CPS como el documento que regule las relaciones entre las partes hasta que no cree y publique un nuevo documento por escrito que reemplace a este.

2.4.2.3 Notificaciones

Cualquier notificación, demanda, solicitud, o en términos generales, cualquier comunicación que se requiera bajo las prácticas descritas en esta CPS se hará mediante mensaje electrónico firmado digitalmente , o por escrito ordinario certificado a cualquiera de las direcciones contenidas en el punto 1.4 (Detalles del contacto) de esta CPS.

La notificación será efectiva una vez recibidas por el destinatario de la comunicación.

2.4.3 Procedimiento de resolución de conflictos o disputa

En el supuesto de existir conflictos o disputas relacionados con esta CPS o con las Prácticas de Certificación, las partes, con renuncia a cualquier otro fuero que pudiera corresponderles se someten expresamente a los juzgados y tribunales de arbitraje que provea el estado de derecho en Uruguay.

2.5 Tarifas de registro por la expedición y renovación de Certificados

Las tarifas de emisión y renovación de cada tipo de certificado estarán disponibles en la Prácticas de Certificación que le sea de aplicación y que proveerá a los Solicitantes cada AR.

Cada AR o ARSub se reserva, dentro del ámbito de aplicación en el que presten sus servicios, poder plantear promociones especiales a sus clientes que pueden diferir de las tarifas previamente establecidas.

2.6 Publicación y repositorios

2.6.1 Publicación de información de la AC

La presente CPS es pública, y estará disponible a título informativo en el sitio de Internet: http://www.id.com.uy/cps.pdf los originales estarán depositados en las oficinas de la AC de ID-Digital.

En el sitio de Internet anteriormente citado se encuentran disponibles y de manera pública; el certificado de la AC de ID-Digital y la lista de certificados revocados por ID-Digital.

Independientemente de lo publicado de la manera anteriormente descrita, tanto los Usuarios como los Solicitantes y Suscriptores que hagan uso de los servicios de certificación, podrán tener acceso de forma fiable a la información de la AC dirigiéndose a sus oficinas o a las de cualquier AR, o bien, solicitándolo a la dirección de correo pki@id.com.uy a través de la cual se remitirá la información firmada con la clave privada de ID-digital.

2.6.2 Frecuencia de la publicación

No se establece una frecuencia de publicación. La última revisión de la presente CPS estará disponible a título informativo en: http://www.id.com.uy/cps.pdf

2.7 Auditorias

La AC de Id-digital, se regirá en esta materia en función de los requerimientos exigidos por la UCE y la ACRN.

2.7.1 Tipo de información considerada confidencial

ID-Digital considera a priori que toda información no considerada como pública tendrá el carácter de confidencial.

- Toda información de carácter personal proporcionada a ID-Digital, con la única excepción de lo especificado por la política de certificación aplicada, y el contrato de servicio.

A los efectos de la determinación del carácter de confidencial de la información recibida por ID-Digital se estará a los recaudos previstos de acuerdo con lo establecidoen la Ley Nº 18.381, del 17 de octubre de 2008.

La información personal queda regulada por las Leyes Nos. 18.331, de 8 de agosto de 2008 y 18.381, de 17 de octubre de 2008.

2.7.2 Tipo de información considerada no confidencial

Toda información recogida en el punto 2.6 (Publicación y repositorios) de este documento.

2.7.3 Divulgación de información de revocación de certificados

La información de la revocación de certificados se proporciona en el sitio de Internet:

http://www.iddigital.com.uy/portal/ crl id-digital pki uruguay.crt

y

http://www.iddigital.com.uy/asf/servlet/OCSPServlet/

2.7.4 Divulgación a petición del propietario

Al Solicitante de servicios de la AC de ID-Digital se le informa de la existencia de un fichero automatizado de datos de carácter personal, de acuerdo a la información proporcionada por este, y creado bajo la responsabilidad de ID-digital. Este fichero tiene como finalidad los usos previstos en esta CPS o en la Prácticas de certificación a aplicar, y el Solicitante consiente expresamente en la cesión de sus datos de carácter personal contenidos en dicho fichero

Es responsabilidad del Responsable del fichero poner todos los medios a su alcance para evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos de carácter personal contenidos en el citado fichero. Se declara, si no existe otra indicación específica de este punto, a ID-Digital como Responsable del fichero.

Si la AC de ID-Digital requiriera de los datos de carácter personal contenidos en el fichero para un uso no previsto en esta CPS o en la Practicas de certificación, requerirá el consentimiento previo del Solicitante.

El Solicitante y el Usuario de certificados de la AC tiene el derecho para acceder, rectificar o cancelar sus datos de carácter personal, en los términos recogidos por la normativa sobre tratamiento de datos de carácter personal.

2.8 Derechos de propiedad intelectual

Todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS pertenecen en exclusiva a la AC de ID-Digital, incluyendo la presente CPS, las Practicas de certificación vigentes en cada momento, los certificados y CRL's emitidos, así como cualquier documento propiedad de ID-Digital.

De acuerdo a estos derechos queda prohibido la reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos citados anteriormente sin la autorización expresa por parte de ID-Digital.

3. Identificación y autenticación

Este punto se encuentra desarrollado de manera específica para cada tipo de Certificado a través de las prácticas de certificación las cuales se consideran parte integrante de esta CPS, siendo los puntos siguientes las líneas generales sobre las que se debe actuar.

Ver Www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

3.1 Registro inicial

3.1.1 Tipos de nombres

El Servicio de certificación de ID-DIGITAL identificara a los poseedores de certificados de forma unívoca basándose en lo definido en: **ISO/IEC 9594 (X.500) Distinguished Name (DN).**

3.1.2 Necesidad de los nombres de ser significativos

Se establece que los nombres distintivos deben tener sentido, no permitiéndose en uso de seudónimos en los certificados.

3.1.3 Reglas para interpretar varios formatos de nombres

El Servicio de certificación de ID-DIGITAL interpretará los nombres distintivos de los certificados basándose en lo definido en: **ISO/IEC 9595 (X.500) Distinguished Name (DN).**

3.1.4 Unicidad de los nombres

Los nombres distintivos deben ser no ambiguos y únicos.

3.1.5 Procedimientos de resolución de disputas de nombres

Cualquier disputa o conflicto se regirá según lo establecido en el punto 2.4.3. de este documento.

3.1.6 Reconocimiento, autenticación, y función de las marcas registradas

No estipulado

3.1.7 Autenticación de la identidad de una organización

La responsable de la política de certificación asumirá la responsabilidad del establecimiento de los métodos necesarios para la verificación de la identidad de una organización.

3.1.8 Autenticación de la identidad de un individuo

El proceso de identificación individual se define en la Práctica de Certificación aplicable a cada tipo de certificado.

Ver Www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

3.2 Renovación rutinaria de la clave

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

3.3 Renovación de la clave después de una revocación

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

3.4 Solicitud de revocación

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

4. Requisitos operativos

Se describen los detalles particulares de id-digital pero todo con subordinado a las CPs de ACNR.

4.1 Solicitud de certificados

Este apartado se desarrolla de manera específica para cada tipo de Certificado a través de las prácticas de certificación las cuales se consideran parte integrante de esta CPS.

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

4.2 Emisión de certificados

Este apartado se desarrolla de manera específica para cada tipo de Certificado a través de las prácticas de certificación las cuales se consideran parte integrante de esta CPS y cumpliendo con la CP ACRN.

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

4.3 Aceptación de certificados

Este apartado se desarrolla de manera específica para cada tipo de Certificado a través de las prácticas de certificación las cuales se consideran parte integrante de esta CPS cumpliendo con la CP ACRN.

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

4.4 Revocación de certificados

Ante el caso de circunstancias por las cuales se comprometa la confianza en los certificados, se instrumentan los supuestos de revocación de certificados.

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

4.4.1 Circunstancias para la revocación

La revocación del certificado digital tiene como consecuencia la perdida de confiabilidad del mismo, provocando el fin del uso y de los servicios prestados por él, de acuerdo a lo establecido en este documento y en las prácticas de certificación aplicables.

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

Se prohíbe el uso del certificado digital, o de cualquier otro bien o servicio que ID-digital haya proporcionado al suscriptor, una vez haya sido revocado el certificado digital.

La revocación del certificado digital por causa imputable a ID-digital originará la emisión de un nuevo certificado digital a favor del solicitante por el plazo equivalente al restante

para concluir el período originario de validez del certificado digital revocado, asumiendo ID-digital el costo implícito en la nueva emisión. En los demás casos el costo del nuevo certificado digital será asumido por el solicitante.

Una vez cumplido el procedimiento de revocación, el certificado digital será publicado en la base de datos de certificados digitales revocados, para notificar a las partes confiantes que dicho certificado digital ha sido revocado.

4.4.1.1 Revocación voluntaria del usuario

El usuario podrá voluntariamente solicitar a ID-digital la revocación del certificado digital emitido, en cuyo caso ID-digital iniciará el procedimiento de revocación del certificado digital.

4.4.1.2 Otros supuestos de revocación

ID-digital revocará el certificado digital respecto del cual tenga conocimiento de que se ha producido alguno de los siguientes hechos:

- Compromiso de la clave privada del usuario por cualquier motivo o circunstancia.
- La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.
- Por muerte o incapacidad sobrevenida del usuario.
- Por liquidación de la persona jurídica representada que consta en el certificado digital.
- Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso, así como la ocurrencia de hechos nuevos que provoquen que los datos originales no se adecuen a la realidad.
- Por el compromiso de la clave privada de ID-digital o de su sistema de seguridad de manera tal que afecte la confiabilidad del certificado digital, por cualquier circunstancia, incluyendo las fortuitas.
- Por el cese de actividades de ID-digital, salvo que los certificados digitales expedidos sean transferidos a otra Entidad de Certificación.
- Por orden judicial o de entidad administrativa competente.
- Pérdida o inutilización del soporte físico del certificado digital que haya sido debidamente notificada a ID-digital.
- Por la terminación del contrato de suscripción, de conformidad con las causas establecidas en el contrato y en esta Declaración de Prácticas de Certificación.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la confiabilidad del certificado digital.
- El manejo indebido por parte del usuario del certificado digital.
- Por la concurrencia de cualquier otra causa especificada en la presente Declaración de Prácticas de Certificación o en las correspondientes Prácticas de Certificación establecidas para cada tipo de certificado digital.

4.4.2 Quien puede solicitar una revocación

El usuario que tenga conocimiento de la existencia de alguna de las causas que dan lugar a la revocación, podrá informársela a ID-digital para que la evalúe y proceda de conformidad con el procedimiento establecido.

En todo caso, ID-digital podrá iniciar de oficio el procedimiento de revocación de certificados digitales, en cualquiera de los casos previstos en el apartado anterior.

Las autoridades judiciales o administrativas podrán, en aquellos supuestos contemplados en la ley, ordenar a ID-digital la revocación de cualquier certificado digital.

4.4.3 Procedimiento para la petición de la revocación

Esto está definido en las prácticas de certificación

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

4.4.4 Periodo de gracia para la petición de revocación

Esto está definido en las prácticas de certificación

Ver www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

4.4.5 Frecuencia de emisión de CRLs

Esto está definido en la CP de ACRN.

4.4.6 Requisitos de comprobación de CRLs

Para cada uso individual de los certificados por parte de usuarios finales es obligatoria la verificación de estos en la CRL.

4.4.7 Disponibilidad de comprobación on-line de revocación y estado

ID-digital proporciona a los usuarios el sitio de Internet http://www.iddigital.com.uy/portal/crl id-digital pki uruguay.crt para la verificación del estado de los certificados que emite.

El servicio de estatus del servicio será de 24*7, salvo mantenimientos programados.

4.5 Expiración, renovación y remisión de certificados

4.5.1 Caducidad de certificados

La vigencia de los certificados digitales terminará por el transcurso del período operacional del mismo, el cual se especifica en éste.

La terminación de la vigencia del certificado digital producirá el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación digital. Cualquier uso que se haga del mismo se entiende una violación de la presente CPS y un uso indebido del Sistema de Certificación Digital.

La terminación de la vigencia de un certificado digital impide el uso legítimo del mismo por parte del suscriptor, de las partes confiantes o de cualquier otra persona.

4.5.2 Renovación de los servicios de certificación

El procedimiento en todos sus aspectos es idéntico al de emisión de un nuevo certificado.

4.5.3 Remisión de certificados

Este procedimiento se establece para los casos en que el Certificado de un solicitante sea declarado revocado por la existencia de inexactitudes en el Certificado o éste se haya dejado caducar sin que se haya llegado a instar la renovación con anterioridad a los treinta últimos días de su vigencia, el procedimiento en todos sus aspectos es idéntico al de emisión de un nuevo certificado.

4.6 Extinción de la AC

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, su extinción esta descrita y regulada por UCE, ver http://www.uce.gub.uy/acrn/cps_acrn.pdf

5. Controles de Seguridad Física, de Procedimientos, y de Personal

La AC de ID-Digital considera de vital importancia los controles de seguridad física, de procedimientos y de personal.

Cumpliendo con todos los controles establecidos por la certificación de PKI Uruguay, bajo auditorias autorizadas por UCE.

El objetivo de los controles administrativos, operativos y físicos es implementar medidas de protección para la clave privada utilizada por ID-digital y toda información relativa a la operativa de la PKI.

La Homologación de ID-digital en ACRN prevé que se cumplan los procedimientos con Políticas y Procedimientos para garantizar la seguridad en sus operaciones. Esta homologación está alineado con los requerimientos de WebTrust for Certification Authorities, y está enfocado a proteger el material criptográfico involucrado en el ciclo de vida de los certificados de la infraestructura de claves Publicas.

5.1.1 Controles de Seguridad Física

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, utiliza similares medidas de seguridad en la estructura de PKI, bajo la regulación de la UCE, ver Política de Seguridad de la Información de Abitab _ PKI en el punto 9

5.1.2 Control Procedimental

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, utiliza similares procesos en la estructura de PKI, bajo la regulación de la UCE, ver http://www.uce.gub.uy/acrn/cps_acrn.pdf en el punto 5.2

5.1.3 Seguridad Asociada al Personal

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, utiliza similares requerimientos y recomendaciones de seguridad asociados al personal en la estructura de PKI, bajo la regulación de la UCE, ver Política de Seguridad de la Información de Abitab _ PKI en el punto 8.

5.1.4 Registro de Auditorias

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, utiliza similares registros de actividades en la estructura de PKI, bajo la regulación de la UCE, ver Política de Seguridad de la Información de Abitab _ PKI en el punto 12.

5.1.5 Retención de Registros e Información

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, utiliza similares procesos de registro de información en la estructura de PKI, bajo la regulación de la UCE, ver Política de Seguridad de la Información de Abitab _ PKI en el punto 12

5.1.6 Cambio de Claves

Si existiera un cambio de Clave de la autoridad de Certificación ID-digital se guiara por las exigencias y recomendaciones que dicta la ACRN en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.http://www.uce.gub.uy/acrn/cps_acrn.pdf

5.1.7 Continuidad de Operaciones

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.
Ver documento Plan de Recuperacion de Desastres_PKI.

5.1.8 Terminación de Operaciones

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.
http://www.uce.gub.uy/acrn/cps_acrn.pdf

6. Controles de Seguridad Técnica

La AC de ID-Digital considera de vital importancia los controles de seguridad técnica.

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.
http://www.uce.gub.uy/acrn/cps_acrn.pdf Ver punto 6.1

ID-Digital debe cumplir con el documento "Requerimientos Técnicos para acreditarse como prestador de Servicios de Certificación"

6.1 Generación del par de claves

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.
http://www.uce.gub.uy/acrn/cps_acrn.pdf Ver punto 6.2

6.1.1 Protección de llave privada y controles de módulos criptográficos

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.
http://www.uce.gub.uy/acrn/cps_acrn.pdf ver punto 6.3

6.1.2 Sistema de Certificación

- El software y la información de la AC correrá en una estación de trabajo dedicada a tal fin.
- La estación de trabajo estará en un lugar seguro, con acceso físico restringido, y con todas las medidas de seguridad para limitar cualquier intromisión física o lógica de acuerdo a lo requerido por PKI Uruguay.
- El intercambio de datos entre la estación de trabajo de la AC y el resto del mundo se realizará a través de mecanismos seguros, y solo mantendrá un vínculo con la AR. El acceso a esta estación requiere autenticación fuerte y siempre estarán presentes n+1 personas.
- Los pares de claves para Personas finales se generan en función de lo establecido en las Prácticas de Certificación para cada tipo de certificado.

6.1.3 Entrega de la clave privada al Solicitante

La autoridad de certificación desconoce en todo el proceso del solicitante su clave privada en función de sus prácticas de certificación.

Ver Www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

6.1.4 Entrega de la clave pública al emisor del certificado

Esto está estipulado en las prácticas de certificación de id-digital.
Ver Www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

6.1.5 Entrega de la clave pública de la AC a los usuarios

La clave pública de la AC se encontrara disponible en el sitio web www.iddigital.com.uy o en el sitio de http://www.uce.gub.uy

6.1.6 Tamaño de las claves

- La clave de firma de la AC tendrá una longitud de 4096 bits.
- Las claves de los certificados emitidos por ID-digital dependerán de cada tipo de certificado emitido con un mínimo de 2048 como lo estipula la ACRN.

Ver Www.iddigital.com.uy/cp_id_firmaElectronicaAvanzada.pdf

6.1.7 Parámetros de generación de la clave pública

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.
Ver el punto 6.2

http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.1.8 Comprobación de la calidad de los parámetros

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias v que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE.

http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.1.9 Hardware/Software de generación de las claves

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE. Ver 6.3

http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.1.10 Fines de uso de la clave

El uso de la clave está estipulado en la CP de ACRN y UCE

http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.2 Protección de la clave privada

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE. Ver 6.3

http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.3 Otros aspectos de la Gestión del par de claves

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE. Ver 6.4

http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.4 Datos de activación

La activación de la clave privada de ID-digital se considera parte del proceso vital de funcionamiento de la Infraestructura, para eso la activación de la clave privada siempre es necesario varios custodios u operadores en un esquema de “M de N”.
El hsm se utiliza para salvaguardar la clave privada de la pki de Abitab, está configurado para que en su activación sea necesario 2 de 4 operadores “2 de 4”, un challenge y el token de owner.
El dispositivo HSM es Safenet cumpliendo con todas las normativas técnicas exigidas por ACRN y UCE.
La clave privada se activa para emitir certificados y CRLs.

6.5 Controles de seguridad informática

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE. Ver 6.5
http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.6 Controles de seguridad del ciclo de vida

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE. Ver 6.7
http://www.uce.gub.uy/acrn/cps_acrn.pdf

6.7 Controles de Seguridad de la red

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, bajo la regulación de la UCE.
Los servidores de la CA de ID-digital, están ubicados en una DMZ de forma aislada de otras máquinas, sin conexión con el mundo exterior, salvo una conexión autenticada y segura con la RA.
Esta DMZ está protegida con un Firewall y un IPS, estos equipos y su configuración están dentro de las políticas de seguridad que maneja Abitab S.A.

6.8 Controles de Ingeniería de los módulos criptográficos

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso.

Los módulos criptográficos utilizados por id-digital son idénticos a los que usa ACRN y cumplen con todos los estándares solicitados.

6.9 Sincronización Horaria

Siendo ID-digital Autoridad de Certificación Subordinada y homologada de ACRN, se guiara por las exigencias y recomendaciones que dicta la ACRN para este caso, en sus políticas y prácticas de Certificación, bajo la regulación de la UCE. Ver 6.9
http://www.uce.gub.uy/acrn/cps_acrn.pdf

ID-Digital utiliza la fecha y hora de la República Oriental del Uruguay al firmar los certificados que emite, con un margen de error máximo del orden del minuto.

Durante la Ceremonia de Claves se establece esta hora y es certificada ante escribano público. La sincronización horaria es objeto de control de las auditorías periódicas.

7. Características de los certificados y de las listas de certificados de ID-digital

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 O = AGESIC C = UY
Validez (Valid From / Valid To)	20 Años (en formato desde/hasta)
Nombre Distintivo del Suscriptor (Subscriber DN)	Abitab Autoridad Certificadora
Clave Pública del Suscriptor (Subject Public Key)	Clave pública generada
Extensiones	
Identificador de la clave de la Autoridad Certificadora (Authority Key Identifier)	Identificador de la clave pública de la ACRN
Identificador de la clave del suscriptor (Subject Key Identifier)	Hash de 20 bytes del atributo Subject Public Key
Uso de Claves (Key Usage)	DigitalSignature = 0 NonRepudiation = 0 KeyEncipherment = 0 DataEncipherment = 0 KeyAgreement = 0 KeyCertSign = 1 CRLSign = 1 EncipherOnly = 0 DecipherOnly = 0
Políticas de Certificación (Certificate Policies)	OID: 2.16.858.10000157.66565.0 URI: www.uce.gub.uy/informaciontecnica/politicas/cp_acrn.pdf OID: 2.16.858.10000157.66565.1 URI: www.agesic.gub.uy/acrn/cps_acrn.pdf
Restricciones Básicas (Basic Constraints)	CA = TRUE Largo 0
Puntos de distribución de las CRL (CRL Distribution Points)	URI = www.agesic.gub.uy/acrn/acrn.crl URI = www.uce.gub.uy/acrn/acrn.crl
Información de Acceso de la Autoridad Certificadora (Authority Information Access)	URI = www.agesic.gub.uy/acrn/acrn.cer

7.1 Características del Certificado

7.1.1 Número de versión

La AC de ID-Digital soporta certificados X.509 v3.

El detalle del certificado de ID-digital esta descrito dentro de la cp_acrn.pdf en el Certificado como parte de los requerimientos del prestador acreditado.

Esto se describe en el punto 7.2 perfil del certificado de las ACPA

7.1.2 Extensiones del certificado

Se definen en las Prácticas de Certificación específica para cada tipo de certificado.

Ver Certificado.

7.1.3 Identificadores de objeto (OID) de los algoritmos

Se definen en las Prácticas de Certificación específica para cada tipo de certificado.

Ver Certificado

7.1.4 Formatos de nombres

Los certificados emitidos por ID-Digital siguen el formato definido en **ISO/IEC 9594 (X.500) Distinguished Name (DN).**

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a nombres distinguidos X.500, únicos y no ambiguos.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

Se definen en las Prácticas de Certificación específica para cada tipo de certificado

Ver Certificado

7.2 Perfil de CRL

ID-DIGITAL publicará la lista de certificados revocados (CRL) estando a disposición de los usuarios en la página web de la AC http://www.iddigital.com.uy/portal/ crl id-digital pki uruguay.crt a partir de los ficheros generados por la AC.

Los Usuarios de Certificados de ID-Digital pueden consultar en cualquier momento el estado de un Certificado determinado, bien visitando la página web, bien realizando la solicitud correspondiente a través los mecanismos de contacto que la AC ponga a disposición de los usuarios en cada momento.

7.2.1 Número de Versión

La AC de ID-Digital soporta CRL's X.509

8. Auditorías de Cumplimiento y otros controles

8.1 Frecuencia o circunstancias de los controles para cada autoridad

Id-digital realizara auditorias de acuerdo a lo estipulado y regulado por la UCE, así como las frecuencias que ahí se estipulen.

8.2 Identificación/cualificación del Auditor

Todo equipo o persona designada para realizar una auditoría de seguridad sobre el Servicio de PKI de Abitab estará abalado por UCE.

8.3 Relación entre el Auditor y la Autoridad Auditada

El auditor deberá ser un auditor abalado y homologado por UCE.

8.4 Aspectos cubiertos por los controles

La auditoría estará basado en los requerimientos estipulados por la UCE y la ACRN.

8.5 Acciones a emprender como resultado de la detección de deficiencias

La identificación de carencias o problemas detectados como resultado de la auditoría dará lugar a la adopción de medidas correctivas.

8.6 Comunicación de Resultados

La empresa auditora comunicara los resultados a Id-digital.

9. Otros asuntos Legales y Comerciales

9.1 Plazo

Esta CPS entra en vigor desde el momento de su publicación en el sitio www.id.com.uy

Esta CPS estará en vigor mientras no se derogue expresamente por la emisión de una nueva versión o por la renovación de las claves de la CA Raíz, momento en que obligatoriamente se dictará una nueva versión.

9.2 Derogación de la DPC

Esta CPS será sustituida por una nueva versión con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad.

Cuando la CPS quede derogada se retirará del sitio www.id.com.uy, si bien se conservará como mínimo hasta el vencimiento del último certificado emitido bajo su vigencia.

9.3 Efectos de la finalización

Las obligaciones y restricciones que establece esta CPS, vencerán tras su sustitución o derogación por una nueva versión.

9.4 Procedimiento de publicación y notificación

Las modificaciones efectuadas sobre la CPS o las Prácticas de Certificación se harán públicas en la sitio web de la AC http://www.id.com.uy y en las oficinas de la AC y las AR.

Cuando se realicen modificaciones significativas en la CPS o en las Prácticas de Certificación, estas deberán notificarse a los usuarios y suscriptores afectados con un período de antelación de quince días a la aplicación de los cambios efectuados.

Se considerará como medio eficaz para la realización de notificaciones el correo electrónico firmado digitalmente y enviado a la dirección proporcionada por el Solicitante.

9.5 Procedimientos de especificación de cambios

La AC de ID-Digital, de manera ocasional, podrá realizar modificaciones a la presente CPS y a sus prácticas de certificación, sin que estos cambios impliquen una merma del nivel de calidad esencial de sus servicios de certificación y, siempre y cuando, la modificación a realizar se justifique desde un punto de vista jurídico, técnico o comercial.

9.6 Procedimiento de aprobación

Si en el transcurso del periodo especificado anteriormente no media comunicación escrita por parte del Solicitante o Usuario, en contra de las citadas modificaciones implicará su aceptación. La no aceptación de las modificaciones de esta CPS o de las Prácticas de Certificación realizadas por la AC, tendrá como consecuencia la rescisión de contrato con el solicitante.

Dicha aceptación implícita incluirá la aceptación de todos aquellos derechos, responsabilidades y obligaciones que se deriven de la misma.

ANEXO SSL/TLS

Índice

1 Procedimientos de validación

Se detallarán los diferentes métodos de comprobación, para solicitudes acreditadas de certificados SSL/TLS.

1.1 Método para probar posesión de la clave privada

Se verificará que la llave privada correspondiente a la llave pública del CSR (Certificate Signing Request) esté en posesión de la persona física que está solicitando el certificado y sea la misma utilizada para firmarlo. La persona física que solicita el certificado se convierte en el referente del

mismo, y del par de claves asociado. Se registrará internamente esta asociación entre la persona jurídica suscriptora y la persona física referente del certificado.

El método a utilizar, es el mecanismo por el cual un CSR se firma con la clave privada correspondiente.

1.2 Autenticación de la identidad de una organización

Para los Certificados de tipo OV, se requiere que los solicitantes indiquen el nombre de la organización y su dirección.
La validación de la identidad de la organización, del individuo y su correspondiente representación se deben realizar de igual manera que en la Política de Certificación de Persona Jurídica. Esto es, mediante certificado notarial emitido por escribano público.

El representante del solicitante deberá presentarse en cualquier ventanilla de registro de la PSCA, con su documento identificatorio personal y un certificado notarial acreditando su vinculación con el solicitante.

La PSCA deberá verificar que el certificado notarial, contiene los mismos datos de la persona jurídica y persona física que figuran en el formulario de solicitud, y que el suscriptor quien se presenta en la ventanilla de registro es efectivamente el representante del solicitante.

1.3 Autenticación de la identidad de un individuo

En el caso de los Certificados OV solicitados por un individuo se deberá verificar que toda información provista en el nombre del sujeto corresponda al Solicitante del Certificado, para lo cual se debe realizar la misma validación de identidad que en la Política de Certificación de Persona Física.

El solicitante deberá presentarse en cualquier ventanilla de registro de la PSCA y presentar su documento de identidad nacional. La PSCA deberá controlar visualmente la coincidencia del rostro de la persona física con la fotografía del documento identificatorio, y la información de solicitud con los datos de dicho documento.

1.4 Autenticación del dominio

Se asegurará que, a la fecha en que el Certificado fue emitido, el Solicitante, su casa matriz o una subsidiaria directa, cumple con alguno de los siguientes puntos:
• Tenía derecho a usar, o tenía el control del FQDN; o
• Fue autorizado por una persona que tenía derecho o control del FQDN que figuran en el Certificado.

Al momento de realizar una solicitud de certificado SSL/TLS para un dominio en el sitio público, el cliente podrá elegir entre 4 mecanismos para que la PSCA valide que efectivamente tiene posesión de dicho dominio.

Los mecanismos son:

1- Validación de Control de Dominio por DNS
2- Validación de Control de Dominio por publicación de contenido
3- Autorización del Titular o Contacto Administrativo del Dominio
4- Validación Manual con Certificado Notarial

1.4.1 Validación de Control de Dominio por DNS

En esta validación, el cliente demuestra posesión del Dominio a través del DNS. La PSCA validará el agregado de un registro “A” aleatorio. Esta validación será a través de nslookup.

1.4.2 Validación de Control de Dominio por publicación de contenido

El cliente demostrará control sobre un dominio, publicando un contenido html en la raíz de su sitio público. Dicho contenido será generado en forma aleatoria por la PSCA.

1.4.3 Autorización del Titular o Contacto Administrativo del Dominio

Consiste en realizar un control desafío-respuesta utilizando el mail del Contacto Administrativo del Dominio, obtenido de uno de los valores predefinidos por la CP ('admin', 'administrator', 'administrador', 'webmaster' o 'hostmaster'). El cliente podrá escoger uno de estos valores. La PSCA enviará un mail con cierto contenido, que el cliente deberá utilizar para continuar el procedimiento de solicitud. De esta forma se demostrará posesión de la dirección de mail y transitivamente la posesión del dominio, por definición en la CP.

1.4.4 Validación manual con Certificado Notarial

Si el cliente selecciona esta opción, deberá presentar la documentación necesaria para demostrar posesión del dominio, incluido un Certificado Notarial emitido por escribano público, acreditando la titularidad para dicho dominio.

1.5 Autenticación de las direcciones IP

Se asegurará que, a la fecha en que el Certificado fue emitido, el Solicitante tenía derecho a usar, o tenía el control de las direcciones IP que figuran en el Certificado mediante:
• Demostración de que el solicitante tiene control practico sobre la dirección IP haciendo un cambio acordado a la información encontrada en una página web identificada por una URI que contiene a la dirección IP;
• Obteniendo documentación acerca de la asignación de la dirección IP a través de LACNIC;
• Usando cualquier otro método de confirmación, de manera que el ACPA mantenga evidencia documentada que el solicitante tiene control sobre la dirección IP de por lo menos el mismo nivel de aseguramiento que los puntos anteriormente mencionados.

Al momento de realizar una solicitud de certificado SSL/TLS para una dirección IP en el sitio público, el cliente podrá elegir entre 4 posibilidades para que la PSCA valide que efectivamente tiene posesión de dicha IP.

Las posibilidades son:

1- Validación de Control de IP por publicación de contenido
2- Validación Manual con Certificado Notarial

1.5.1 Validación de Control de IP por publicación de contenido

El cliente demostrará control sobre una IP, publicando un contenido html en la raíz de su sitio público. Dicho contenido será generado en forma aleatoria por la PSCA.

1.5.2 Validación manual con Certificado Notarial

Si el cliente selecciona esta opción, deberá presentar la documentación necesaria para demostrar posesión de la IP, incluido un Certificado Notarial emitido por escribano público, acreditando la titularidad para dicha IP.