CPS
de
ID-digital

Declaración de las políticas de certificación de ID-digital para firma electrónica

Versión 4.00

Fecha de Publicación: Septiembre del 2002
Actualizada: Agosto 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 para Firma Electrónica, no aplica para Firma electrónica Avanzada (solicitud, emisión, aceptación, renovación, reemisión, suspensión y revocación de certificados). 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 de ID-digital en firma Electrónica, este documento y demás documentos afines, ya sean estos anexos o documentación adicional, estarán disponibles en http://www.iddigital.com.uy.

ID-digital, como Autoridad Certificadora (CA) 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 / suspensión del certificado establecidas en la presente CPS, es necesario informar inmediatamente a ID-digital para proceder a la suspensión 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 el Directorio de Certificados publicado por ID-digital que el certificado en el que pretende confiar es válido y no ha caducado o ha sido suspendido o 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.

1.2 Identificación

1.2.1 Identificación

Referencia de la CPS / OID (Object Identifier Digital): 1.3.6.1.4.1.9310.0.1.0

1.2.2 Publicación

El presente documento está publicado en formato electrónico en la siguiente URL: http://www.iddigital.com.uy/portal/resources/crl_id_digital.crl

1.3 Comunidad de usuarios y ámbito de aplicación

1.3.1 Autoridad de Certificación

La presente CPS especifica la actuación de ID-digital como Autoridad de Certificación (CA, Certification Authority, desde ahora CA) 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.

1.3.2 Autoridad de Registro

La Autoridad de Registro (RA, Registry Authority, desde ahora RA) 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 CA de ID-digital.

Este servicio de Certificación podrá estar otorgado además de por la propia RA de ID-digital por otras RA adicionales elegidas por ID-digital. Las cuales podrán llevar a cabo el servicio de identificación de los Solicitantes de Certificados de acuerdo a las normas de esta CPS y del acuerdo suscrito con la CA.

1.3.3 Suscriptor

Como suscriptor se entiende una Persona física o jurídica con una vinculación contractual con ID-digital.

El suscriptor estará sujeto a las obligaciones y responsabilidades que se derivan de lo establecido en esta CPS y en las prácticas de certificación de las RA para cada tipo de Certificado.

El suscriptor actuará como intermediario entre el solicitante y la RA de ID-Digital.

1.3.4 Entidades Finales

1.3.4.1 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 RA.

1.3.4.2 Usuario

Como Usuario del Certificado se entiende la persona que confía y hace uso de los Certificados de la CA de ID-digital.

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

1.3.5 Ámbito de Aplicación

1.3.5.1 Tipos de Certificados

Existen distintos tipos de certificados emitidos por ID-digital para firma electronica, cada unos de los cuales están definidos por medio de esta CPS y por cada una de las respectivas prácticas de certificación emitidas por una RA vinculada a la CA de ID-digital

Dentro de la definición de cada certificado esta 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.

1.3.5.2 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 digitales pueden ser utilizados con los siguientes propósitos:

- Identificación: El suscriptor del certificado digital puede identificarse e identificar a la persona jurídica a la que representa en una red de comunicaciones demostrando el acceso a la clave privada asociada con la clave pública que se incluye en el certificado digital.
- Integridad: El uso de la Infraestructura de Clave Pública le permite comprobar a una parte confiante que un mensaje de datos recibido no ha sido alterado entre el envío y la recepción del mismo ni en ningún otro momento.
- Confidencialidad: La clave pública del suscriptor puede ser usada para cifrar todos los documentos que se le envían, impidiendo que terceras personas tengan acceso a las comunicaciones que se transmiten a través de comunicaciones electrónicas abiertas. La utilización de la clave pública por parte del suscriptor para encriptar la información deberá en todo caso ajustarse a las prescripciones legales colombianas o de cualquier otro país del mundo en donde se utilice el sistema de certificación digital en materia de tecnologías de encriptación de la información.
- No repudio: La persona que recibe un mensaje de datos firmado digitalmente y respaldado por un certificado digital permite que, cumplidos todos los requisitos de procedimiento del Sistema de Certificación Digital, el suscriptor no pueda negar el envío de dicho mensaje de datos.

El uso y adecuación de los certificados digitales a las necesidades del suscriptor le corresponde de manera exclusiva a éste.

1.3.5.3 Puntos de solicitud de certificados

Los Servicios de Certificación de ID-digital son ofrecidos en todas las oficinas o agencias habilitadas para brindar servicios electrónicos de ID-digital.

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

1.3.5.4 Servicios ofrecidos

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

- Firma de certificados
- Emisión de certificados
- Revocación de certificados
- Publicación de los Certificados emitidos

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. 7163

Fax 29245825 int 524-526

Correo Electrónico: pki@id.com.uy o pki@abitab.com.uy

1.5 Certificado de la Autoridad

1.5.1 Introducción

El certificado de la Autoridad de certificación de los Servicios de Certificación de ID-digital para firma electrónica, es el certificado de nivel más alto en la jerarquía de dicha autoridad. 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.

1.5.2 Certificado

El certificado de los Servicios de Certificación de ID-digital es un certificado X.509 versión 3

1.5.3 Nombre

El certificado esta emitido a nombre de:

- **Correo Electrónico** : pki@id.com.uy
- **Nombre:** Abitab CA Root
- **Unidad :** pki
- **Organización:** Abitab
- **Localidad :** Montevideo
- **País:** UY

1.5.4 Clave

La clave privada y pública de los Servicios de Certificación de ID-digital son claves RSA de un largo de 4096 bits.

1.5.5 Firma

El certificado de los Servicios de Certificación de ID-digital esta auto-firmado.

1.5.6 Algoritmo

El algoritmo de firma utilizado es SHA-1 con RSA.

1.5.7 Validez

El periodo de validez del certificado de los Servicios de Certificación de ID-digital es de 20 años.

2. Reglamento general

2.1 Obligaciones

2.1.1 Obligaciones de la CA

La CA de ID-DIGITAL está obligada a operar según las obligaciones que impone la presente CPS, y de acuerdo a la normativa aplicable sobre Certificación Digital para firma electrónica en Uruguay.

Estas obligaciones son:

- Operar según lo especificado en esta CPS.
- Almacenar y proteger sus claves privadas.
- La emisión de certificados digitales de acuerdo a las Prácticas de Certificación de cada tipo de certificado.
- La emisión de certificados se hará sobre la información proporcionada para su emisión, y libre de errores de datos.
- La publicación de la presente CPS y las Prácticas de Certificación para cada tipo de certificado que se establezca.
- La revocación de certificados de acuerdo a lo establecido en la presente CPS, y la publicación en la CRL del directorio de ID-Digital de los certificados revocados o suspendidos.
- En el supuesto de cese de actividad, deberá comunicarlo con un tiempo prudencial antes de este cese a los titulares de certificados emitidos por esta CA.

2.1.2 Obligaciones de la RA

La RA de ID-DIGITAL, o aquellas que operen bajo la jerarquía de ID-DIGITAL, están obligadas a operar siempre dependiendo de la CA de ID-DIGITAL, y cumpliendo las siguientes obligaciones:

- Operar según las obligaciones que impone la presente CPS.
- Almacenar y proteger sus claves privadas.
- La emisión de certificados digitales se hará de acuerdo a las Prácticas de Certificación específicas de cada tipo de certificado.
- Comprobar correctamente la identidad y datos personales relevantes de los Suscriptores de certificados, y del Solicitante y organización que este represente, todo ello de acuerdo a los procedimientos establecidos en la presente CPS y en las Prácticas de Certificación para cada tipo de Certificado, utilizando cualquiera de los medios admitidos en derecho.
- Formalizar el Contrato de Certificación pertinente con el Suscriptor según los términos establecidos por la Política de Certificación de la CA.
- Almacenar de forma segura y permanente (el periodo que quede estipulado en la Política de Certificación) la documentación aportada por el Suscriptor para los procesos de emisión de certificados y de suspensión / revocación del mismo.
- Deberá permitir el acceso a la CA de ID-DIGITAL a la información y a los procedimientos de conservación asumidos por la RA, y ante cualquier indicio o sospecha de infracción de la presente CPS y/o de las Prácticas de Certificación por parte de la RA o cualquier poseedor de un Certificado a investigar sobre este hecho.

- La RA estará obligada a informar a la CA de cualquier indicio o sospecha de infracción de la presente CPS y/o de las Prácticas de Certificación.
- Es también obligación de la RA de ID-DIGITAL cualquier otra función que se determine de acuerdo a lo establecido en la presente CPS.

Para garantizar la seguridad y validez de los certificados emitidos por la CA, esta mantendrá el derecho y la responsabilidad de revocar la prestación de los servicios de la RA, y realizar cualquier acción necesaria sobre los certificados emitidos, sin necesidad de aviso previo de las acciones a emprender.

Excepcionalmente, la CA de ID-DIGITAL podrá desempeñar de forma directa todas las funciones atribuidas a la RA, siempre y cuando no exista conflicto con los derechos reconocidos a ésta contractualmente, por lo que todos los puntos y referencias de la presente CPS relativas a la RA quedan establecidas también a la CA de ID-DIGITAL.

2.1.3 Obligaciones del Suscriptor

- 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 CA o con la RA.
- Cualquier obligación que se pueda derivar del contenido de esta CPS o de las Prácticas de Certificación.

2.1.4 Obligaciones del Solicitante

- Abonar las tarifas de registro establecidas para los servicios de certificación que se soliciten.

2.1.5 Obligaciones de los Usuarios

- Un usuario como parte que confía, y hará uso, de los Certificados emitidos por la CA tiene como obligación la verificación de la validez de las firmas emitidas por la CA.
- Si los Usuarios no proceden a esta verificación de las firmas, haciendo uso de la CRL publicada, la CA 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 o suspensiones 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, 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 o suspensiones de certificados (CRL).
  - Las políticas y procedimientos que rijan 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.
- 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 y en las practicas de certificación, por los cuales se garantiza la prestación de los servicios de certificación.

2.2 Responsabilidad

2.2.1 Responsabilidad de la CA

La CA 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 RA, 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 CA.
- 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 CA 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 CA o la RA, 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 RA

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 CA.

2.2.3 Responsabilidad del Suscriptor

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

2.3 Responsabilidad financiera

Este punto esta incluido en las responsabilidades de la CA.

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 electrónica vigentes, 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 CA 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 CA 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 CA 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 RA.

Cada RA 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 CA

La presente CPS es publica, y estará disponible a título informativo en el sitio de Internet: http://www.iddigital.com.uy/portal/resources/cp_id_FirmaElectronica.pdf los originales estarán depositados en las oficinas de la CA de ID-Digital.

En el sitio de Internet anteriormente citado se encuentran disponibles y de manera pública; el certificado de la CA de ID-Digital, los certificados emitidos por la CA 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 CA dirigiéndose a sus oficinas o a las de cualquier RA, o bien, solicitándolo a la dirección de correo pki@abitab.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.iddigital.com.uy/portal/resources/cp_id_FirmaElectronica.pdf

2.7 Auditorias

La CA, a través del reglamento interno de seguridad, establecerá los procedimientos y frecuencia de las auditorias.

Los puntos que contendrá serán los siguientes:

- Frecuencia de la auditoria.
- Auditor.
- Ámbito de la auditorias.
- Acciones a emprender en supuesto de deficiencias detectadas.
- Donde se publican los resultados.

2.8 Política de confidencialidad

2.8.1 Tipo de información considerada confidencial

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

De manera expresa se declara información confidencial:

- Acerca de la claves privadas:
  - Las claves privadas de las entidades que componen los servicios de certificación de ID-Digital.
  - Las claves privadas de los suscriptores.
  - ID-Digital garantiza no tener conocimiento de las claves de firma criptográfica privadas durante el proceso de generación. Toda información sobre medidas y procedimientos de seguridad, control, y auditoria.

- 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.

2.8.2 Tipo de información considerada no confidencial

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

2.8.3 Divulgación de información de revocación / suspensión de certificados

La información de la revocación o suspensión de certificados se proporciona en el sitio de Internet: http://www.iddigital.com.uy/portal/resources/crl_id_digital.crl

2.8.4 Divulgación a petición del propietario

Al Solicitante de servicios de la CA 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 CA 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 Prácticas de certificación, requerirá el consentimiento previo del Solicitante.

El Solicitante y el Usuario de certificados de la CA 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.

2.9 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 CA 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 prohibida 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.

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 Métodos de prueba de posesión de la clave privada

Si el par de claves es generado por la entidad final, este deberá probar la posesión de la clave privada correspondiente a la clave pública que solicita que se certifique mediante el envío de la solicitud de certificación.

3.1.8 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.

3.1.9 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.

3.2 Renovación rutinaria de la clave

La autenticación para la renovación se define en la Práctica de Certificación aplicable a cada tipo de certificado.

3.3 Renovación de la clave después de una revocación

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial.

3.4 Solicitud de revocación

El proceso de solicitud de revocación se define en la Práctica de Certificación aplicable a cada tipo de certificado.

4. Requisitos operativos

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.

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.

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.

4.4 Revocación y suspensión de certificados

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

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 el, de acuerdo a lo establecido en este documento y en la prácticas de certificación aplicables.

Se prohíbe el uso del certificado digital, del soporte físico 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 o cualquier tercero 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.

El tercero que inicie un procedimiento de revocación de certificados digitales será el único responsable de los perjuicios que produzca dicha revocación al usuario y a terceros de buena fe.

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

El procedimiento seguirá los siguientes pasos:

- **PASO 1.-** Recepción de solicitudes de revocación:
  - La solicitud de revocación de certificados digitales podrá hacerse telefónicamente llamando a cualquiera de los números que ID-digital ha destinado para el efecto.
  - Si la persona que expone una causa que da lugar a la revocación del certificado digital no es el usuario o en caso de ser este último no puede identificarse satisfactoriamente, o no pueden comprobar de manera fehaciente la existencia de la causa de revocación, deberá dirigirse personalmente a casa central de ID-digital en horarios de oficina, con la prueba de la existencia de la causa de revocación respectiva, sin perjuicio de que ID-digital disponga de las medidas que se establezcan para la seguridad del Sistema de Certificación Digital.
  - Las conversaciones telefónicas que se mantengan con el Call Center podrán ser grabadas y registradas por ID-digital con fines probatorios.
- **PASO 2.-** Decisión de revocar:
  - Si ID-digital lo considera necesario realizará, personalmente o por intermedio de terceras personas, las averiguaciones y gestiones pertinentes para comprobar la existencia de la causa de revocación que sea invocada. Dichas gestiones podrán incluir la comunicación directa con el usuario y la presencia física del tercero que invoca la causa de revocación.
  - Si la causa es comprobada, ID-digital revocara el certificado digital. De lo contrario, dará por terminado el proceso de revocación del certificado digital.
- **PASO 3.-** Comunicación y Publicación de la revocación:
  - La decisión de revocar el certificado digital será comunicada por ID-digital al usuario mediante correo ordinario certificado y correo electrónico.
  - La revocación del certificado digital comenzará a producir efectos a partir de su publicación por parte de ID-digital en la base de datos de certificados digitales revocados/suspendidos, salvo que la causa de revocación sea el cese de actividades de ID-digital, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

4.4.4 Frecuencia de emisión de CRLs

ID-digital publicará una nueva CRL en su repositorio cada 7 días o en el momento que se produzca cualquier revocación/suspensión.

4.4.5 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.

4.4.6 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/resources/crl_id_digital.crl para la verificación del estado de los certificados que emite.

4.5 Expiración, renovación y reemisión de certificados

4.5.1 Expiración 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

La renovación de certificados es el procedimiento mediante el cual el usuario, cuyo certificado este a punto de caducar, solicita un nuevo certificado con las mismas características que el certificado que expira.

En este caso, la CA emitirá un nuevo certificado y se generarán nuevas claves; y se llevarán a cabo medidas de comprobación, puesto que alguno de sus datos adicionalmente puede haber cambiado o que ya no es posible confiar en el certificado.

Los certificados emitidos por ID-digital tienen un plazo de validez de un año, salvo en los casos de certificados que se estipule en sus prácticas de certificación otro periodo. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación de ID-digital si concurren los extremos generales que a continuación se detallan.

4.5.2.1 Requisitos previos

Deberán concurrir los siguientes:

- Que el certificado no haya caducado.
- Que queden menos de 30 días para su caducidad.
- Que la solicitud se realice siguiendo las instrucciones y normas que ID-digital especifica a tal efecto.
- Que no haya habido ninguna causa de revocación/suspensión del certificado.
- Que no hayan pasado más de cuatro años desde la emisión del primer certificado. Si hubieran pasado más de cuatro años, es decir, la emisión de un certificado y tres renovaciones consecutivas posteriores, el usuario deberá someterse a los trámites correspondientes para la emisión de un certificado como cualquier otro solicitante que solicita su certificado por primera vez.
- Que se solicite la renovación, esto es un certificado de igual categoría y características que el certificado que expira.

4.5.2.2 Cómo solicitar la renovación

El solicitante tiene que realizar el procedimiento para la petición de emisión de un nuevo certificado.

4.5.2.3 Procedimiento de renovación de certificados

El procedimiento de renovación de certificados es el mismo de la petición de emisión de un nuevo certificado.

4.5.3 Reemisión 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 CA

En el evento en que ID-digital deba por cualquier circunstancia cesar sus actividades deberá:

- Comunicar la extinción mediante el envío de un correo electrónico dirigido a todos los suscriptores cuyos certificados digitales permanezcan en vigor y la publicación de un anuncio en dos diarios de amplia circulación nacional. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.
- Procurar establecer, cuando ello fuera posible, acuerdos con terceras personas para transmitir todas sus obligaciones y derechos dentro del sistema de certificación con la intención de continuar el servicio. Si se produce la subrogación, a la cual el suscriptor da su consentimiento de manera expresa, esta Declaración de Prácticas de Certificación seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.
- Proceder, en caso de no haberse podido llevar a cabo trasferencia de derechos y obligaciones a otra entidad, a la revocación de todos los certificados digitales una vez transcurrido el plazo de dos meses desde la comunicación.
- Cualquier otra obligación que establezca la ley.

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

La CA de ID-Digital considera de vital importancia los controles de seguridad física, de procedimientos y de personal, por esta razón, y para reforzar estos controles se encuentra desarrollado de manera específica un reglamento interno de funcionamiento que regula todos estos aspectos. Parte del contenido de este reglamento se considera de carácter confidencial para garantizar todos los controles de seguridad necesarios.

6. Controles de seguridad técnica

Los controles específicos de seguridad técnica se encuentra desarrollado en un reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, siendo este punto de la CA tan solo un desglose de los requerimientos básicos de seguridad que ha de observar esta.

6.1 Generación e instalación del Par de claves

6.1.1 Generación del par de claves

- El software y la información de la CA correrá en una estación de trabajo dedicada a tal fin y sin conexión física ni lógica a ningún tipo de dispositivo externo.
- 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.
- El intercambio de datos entre la estación de trabajo de la CA y el resto del mundo se realizará a través de mecanismos en línea. El acceso a esta estación requiere autenticación fuerte y siempre estarán presentes 2 personas, el operador de la CA y un supervisor elegido a este efecto.
- Los pares de claves para entidades finales se generan en función de lo establecido en las Prácticas de Certificación para cada tipo de certificado.

6.1.2 Entrega de la clave privada a la entidad

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.1.3 Entrega de la clave pública al emisor del certificado

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.1.4 Entrega de la clave pública de la CA a los usuarios

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.1.5 Tamaño de las claves

- La clave de firma de la CA tendrá una longitud de 4096 bits.
- Las claves de los certificados emitidos por ID-digital serán de una longitud mínima de 1024 bits

6.1.6 Parámetros de generación de la clave pública

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.1.7 Comprobación de la calidad de los parámetros

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.1.8 Hardware/Software de generación de las claves

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.1.9 Fines de uso de la clave

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.2 Protección de la clave privada

La clave privada estará protegido por módulos criptográficos denominados HSM FIPS 140-2.

6.3 Otros aspectos de la Gestión del par de claves

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.4 Datos de activación

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, y en la Prácticas de Certificación para cada tipo de certificado.

6.5 Controles de seguridad informática

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, considerándose esta información de carácter confidencial.

6.6 Controles de seguridad del ciclo de vida

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, considerándose esta información de carácter confidencial.

6.7 Controles de seguridad de la red

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, considerándose esta información de carácter confidencial.

6.8 Controles de ingeniería de los módulos criptográficos

Se encuentra desarrollado en el reglamento interno de funcionamiento que regula todos los aspectos de seguridad de la CA, considerándose esta información de carácter confidencial.

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

7.1 Características del Certificado

7.1.1 Número de versión

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

7.1.2 Extensiones del certificado

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

7.1.3 Identificadores de objeto (OID) de los algoritmos

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

7.2 Perfil de CRL

ID-DIGITAL publicará la lista de certificados suspendidos o revocados (CRL) estando a disposición de los usuarios en la página web de la CA http://www.iddigital.com.uy/portal/resources/crl_id_digital.crl a partir de los ficheros generados por la CA. De igual manera los certificados una vez emitidos se publicarán en una base de datos o repositorio disponible públicamente en el mismo sitio de Internet.

Se estipula que los Certificados suspendidos y revocados aparecerán publicados como tales en la CRL durante un período mínimo de tres años, eliminando los datos del Certificado definitivamente de la CRL pasado este tiempo y depositándolos en las oficinas de la CA durante un periodo de doce años.

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 CA ponga a disposición de los usuarios en cada momento.

7.2.1 Número de Versión

La CA de ID-Digital soporta CRL's X.509 v2.

8. Especificaciones administrativas

8.1 Procedimientos de especificación de cambios

La CA 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.

8.2 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 CA http://www.iddigital.com.uy y en las oficinas de la CA y las RA.

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.

8.3 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 CA, 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:

CPs de ID-Digital

Firma Electrónica

PRÁCTICAS DE CERTIFICACIÓN DE ID-Digital

Versión 4.00

Fecha de Publicación: Marzo del 2002
Fecha de Actualización: julio de 2013

Contenido

9. Introducción a las prácticas de certificación

9.1 Clases de certificados emitidos por ID-digital para Firma electrónica.

En función del perfil del usuario final del certificado y por tanto del uso que va a dar a este, ID-digital como Autoridad Certificadora (CA) tiene definidas las siguientes clases de certificados:

- Certificados personales
- Certificados para empresas
- Certificados para sitios

Independientemente del tipo de certificado todos los certificados emitidos por ID-digital son certificados X.509 v3.

9.2 Por qué distintos certificados

Los certificados emitidos por Autoridades Certificadoras pueden clasificarse de acuerdo con diferentes criterios:

- **Objeto de la certificación**. Puede ser firma digital, intercambio de claves para confidencialidad, garantizar la identidad del usuario, atributos de usuario, credenciales de pago electrónico, etc.
- **Tipo de entidad identificada**, en el caso de certificados de identidad. Puede ser un ciudadano, una organización, un equipo informático, etc.
- **Aplicación** para la que puede utilizarse el certificado. Incluye mensajería segura, servicios web, acceso remoto, etc.
- **Nivel de garantía** del certificado.

De acuerdo a estos criterios una CA o Autoridad Certificadora puede disponer el emitir distintos tipos de certificados para garantizar la máxima calidad y seguridad de uso a cada tipo de usuario del certificado.

9.3 Información mínima contenida en un certificado de ID-digital.

Todos los certificados de ID-digital contienen la siguiente información mínima:

- Identidad del poseedor de la clave pública e identidad de la CA.
- Identificación del propio certificado.
- Versión del formato del certificado.
- Periodo de validez del certificado.
- Información de algoritmos utilizados en la firma.
- Clave pública que se certifica.

10. Solicitud y emisión de certificados

10.1 Introducción

En la presente sección se detallara el proceso a realizar para solicitar un certificado. En particular se describe las formas de autenticación e identificación y las convenciones utilizadas para nombrar a los solicitantes.

10.2 Proceso de solicitud y emisión de certificados

10.2.1 Tipos de solicitud

Existen tres tipos de solicitudes correspondientes a los distintos tipos de servicios ofrecidos:

- Solicitud de certificados personales
- Solicitud de certificados para empresas
- Solicitud de certificados para sitios.

10.2.2 Certificados personales

Los certificados personales son emitidos para personas mayores de edad legalmente que desean realizar operaciones y transacciones electrónicas.

Los certificados varían dependiendo de la comunidad Banco Central, Banco República, Comercio Electrónico la Banca, certificado en PC o Dispositivo Externo.

10.2.2.1 Dispositivo Externo

10.2.2.1.1 Proceso de solicitud

- Antes de iniciar la solicitud de dicho certificado, deberá poseer el kit de tarjeta criptográfica o token.
- Instalar el dispositivo en su máquina y comprobar de que funciona correctamente.

- El solicitante deberá ingresar a la página www.iddigital.com.uy

- Ingresara en ***Solicitudes → y la opción dependerá del uso (Banco Central, Banco República, Comercio Electrónico, etc)***
- Ingresara sus datos personales solicitados en la página web.
- Para la generación de las claves deberá tener colocado el dispositivo externo (la tarjeta en el lector o el token en usb del pc)
- Luego de generar las claves, se le enviara un mail al solicitante para que verifique si los datos que ingreso en el mismo son correctos.
- Luego de verificar los datos, el solicitante se dirigirá a uno de los locales habilitados por ID-digital, con el siguiente material:

- Presentar cédula de identidad si el solicitante es ciudadano de Uruguay o pasaporte vigente en caso de personas extranjeras.
- Entregar fotocopia de la cédula de identidad (dos caras) o fotocopias de las páginas con información personal del pasaporte.
- Cumplir con la tarifa de pago estipulada.
- formulario de solicitud de certificados que se le fue enviado por mail.

- El empleado de ID-digital o suscriptor deberá entonces:
  - Verificar la validez del documento y la identidad del solicitante.
  - Verificar que la edad del solicitante coincide con los requisitos del certificado.
  - Verificar que los datos del formulario coinciden con la del documento.
  - Firmar el contrato entre partes, de la suscripción del servicio.
  - Aprobar la solicitud del certificado.
  - Aceptar el pago.
  - Adjuntar la fotocopia del documento identificatorio al formulario y la copia del contrato Firmado.
  - Remitir la información del solicitante a la RA de ID-digital.

10.2.2.1.2 Proceso de Generación y Entrega del certificado

Una solicitud para un certificado personal será generada y notificada al solicitante de la siguiente forma

- Las solicitudes remitidas a la RA desde los suscriptores se autorizaran por parte de la RA por medios de validación entre la información física y digital, para posteriormente ser aprobado por la CA.
- La CA trabajando en línea autenticara a la RA y procederá a firmar las solicitudes de certificados.
- La CA genera los certificados y comunicara a la RA los certificados firmados, la RA recepciona los mismo y envía notificaciones al los Solicitantes comunicándoles que ya puede bajar su certificado firmado por la CA.

10.2.2.1.3 Proceso de Aceptación del certificado

La aceptación por parte del usuario o solicitante de un certificado habrá de cumplir:

- El solicitante deberá poner la tarjeta en el lector o el token en el puerto usb del pc, ingresar al link que se le especifica en el mail, si todo esta bien su certificado quedara instalado con éxito en su tarjeta criptográfica pronto para su uso.
- Tiempo de validez de esta operación 30 días después de haberse comunicado por parte de la RA de la generación del certificado, al usuario.

10.2.2.2 Navegadores

10.2.2.2.1 Proceso de solicitud

- El solicitante deberá ingresar a la página www.iddigital.com.uy
- Ingresara en ***Solicitudes → Certificado en PC***
- Luego de generar las claves, se le enviara un mail al solicitante para que verifique si los datos que ingreso en el mismo son correctos.
- Luego de verificar los datos, el solicitante se dirigirá a uno de los locales habilitados por ID-digital, con el siguiente material:

- Presentar cédula de identidad si el solicitante es ciudadano de Uruguay o pasaporte vigente en caso de personas extranjeras.
- Entregar fotocopia de la cédula de identidad (dos caras) o fotocopias de las páginas con información personal del pasaporte.
- Cumplir con la tarifa de pago estipulada.
- formulario de solicitud de certificados que se le fue enviado por mail.

- El empleado de ID-digital o suscriptor deberá entonces:
  - Verificar la validez del documento y la identidad del solicitante.
  - Verificar que la edad del solicitante coincide con los requisitos del certificado.
  - Verificar que los datos del formulario coinciden con la del documento.
  - Firmar el contrato entre partes, de la suscripción del servicio.
  - Tomar la huella dactilar y comparar con la base de datos.
  - Aprobar la solicitud del certificado.
  - Aceptar el pago.
  - Adjuntar la fotocopia del documento identificatorio al formulario y la copia del contrato firmado.
  - Remitir la información del solicitante a la RA de ID-digital.

10.2.2.2.2 Proceso de Generación y Entrega del certificado

Una solicitud para un certificado personal será generado y notificado al solicitante de la siguiente forma

- Las solicitudes remitidas a la RA desde los suscriptores se autorizaran por parte de la RA por medios de validación entre la información física y digital, para posteriormente ser aprobado por la CA.
- La CA trabajando en línea autenticara a la RA y procederá a firmar las solicitudes de certificados.
- La CA genera los certificados y comunicara a la RA los certificados firmados, la RA recepciona los mismo y envía notificaciones al los Solicitantes comunicándoles que ya puede bajar su certificado firmado por la CA.

10.2.2.2.3 Proceso de Aceptación del certificado

La aceptación por parte del usuario o solicitante de un certificado habrá de cumplir:

- El solicitante deberá ingresar al link que se le especifica en el mail, si todo esta bien su certificado quedara instalado con éxito en su navegador pronto para su uso.
- Tiempo de validez de esta operación 30 días después de haberse comunicado por parte de la RA de la generación del certificado, al usuario.

10.2.3 Certificados de Empresas

Los certificados para empresas son solicitados por personas mayores de edad legalmente en representación de empresas que desean realizar transacciones y operaciones electrónicas. Estas personas deben poseer representatividad legal en nombre de la empresa solicitante.

10.2.3.1.1 Proceso de solicitud

- Una solicitud para un certificado de empresa es igual al proceso para certificado personal.
- El empleado de ID-digital o suscriptor verificará los datos básicos idéntico al proceso para certificado personal.
- Se exigirá la siguiente información adicional para este tipo de certificados certificado notarial que demuestre la representatividad de esa persona con la empresa
- El empleado de ID-digital o suscriptor remitirá toda la documentación a la RA de ID-Digital.

10.2.3.1.2 Proceso de Generación y Entrega del certificado

Una solicitud para un certificado de empresa será generado y notificado al solicitante de la siguiente forma:

- Las solicitudes remitidas a la RA desde los suscriptores se autorizaran por parte de la RA por medios de validación entre la información física y digital, particularmente la verificación del certificado notarial por un idóneo en la materia, para posteriormente ser aprobado por la CA.
- La CA trabajando en línea autenticara a la RA y procederá a firmar las solicitudes de certificados.
- La CA genera los certificados y comunicara a la RA los certificados firmados, la RA recepciona los mismo y envía notificaciones al los Solicitantes comunicándoles que ya puede bajar su certificado firmado por la CA.

10.2.3.1.3 Proceso de Aceptación del certificado

La aceptación por parte del usuario o solicitante de un certificado habrá de cumplir:

- El solicitante deberá ingresar al link que se le especifica en el mail, si todo esta bien su certificado quedara instalado con éxito en el medio que haya generado las claves pronto para su uso.
- Tiempo de validez de esta operación 30 días después de haberse comunicado por parte de la RA de la generación del certificado, al usuario.

10.2.4 Certificados de Servidores de Internet

Los certificados de sitio son emitidos para servidores de publicación de páginas Web, para el acceso seguro a la información publicada, dando garantías a los clientes que consultan las páginas publicadas.

10.2.4.1.1 Proceso de solicitud del certificado

Una solicitud para un certificado de Servidor se procesa de la siguiente forma:

- Una solicitud para un certificado de Servidor es igual al proceso para certificado personal.

- El empleado de ID-digital o suscriptor verificará los datos básicos idéntico al proceso para certificado personal.

- Se exigirá la siguiente información adicional para este tipo de certificados, el nombre del dominio a usar en el certificado y acreditación por parte de esa empresa de la propiedad de ese dominio.

- El empleado de ID-digital o suscriptor remitirá toda la documentación a la RA de ID-Digital.

10.2.4.1.2 Proceso de Generación y Entrega del certificado

Una solicitud para un certificado de web será generada y notificada al solicitante de la siguiente forma:

- Las solicitudes remitidas a la RA desde los suscriptores se autorizaran por parte de la RA por medios de validación entre la información física y digital, particularmente la verificación del certificado de propiedad del dominio por un idóneo en la materia, para posteriormente ser aprobado por la CA.
- La CA trabajando en línea autenticara a la RA y procederá a firmar las solicitudes de certificados.
- La CA genera los certificados y comunicara a la RA los certificados firmados, la RA recepciona los mismo y envía notificaciones al los Solicitantes comunicándoles que ya puede bajar su certificado firmado por la CA.

10.2.4.1.3 Proceso de Aceptación del certificado

La aceptación por parte del usuario o solicitante de un certificado habrá de cumplir:

- El solicitante deberá ingresar al link que se le especifica en el mail, si todo esta bien su certificado quedara instalado con éxito en el medio que haya generado las claves pronto para su uso.
- Tiempo de validez de esta operación 30 días después de haberse comunicado por parte de la RA de la generación del certificado, al usuario.

10.3 Proceso de Revocación y suspensión de certificados

10.3.1 Certificados personales

Este apartado se desarrolla de manera general en el documento de CPS publicado por la CA, y para este certificado concreto las prácticas generales se aplicarán en todos sus puntos en los procesos de Revocación y Suspensión de certificados.

10.3.2 Certificados de empresas

Este apartado se desarrolla de manera general en el documento de CPS publicado por la CA, y para este certificado concreto las prácticas generales se aplicarán en todos sus puntos en los procesos de Revocación y Suspensión de certificados.

10.3.3 Certificados de Servidores de Internet

Este apartado se desarrolla de manera general en el documento de CPS publicado por la CA, y para este certificado concreto las prácticas generales se aplicarán en todos sus puntos en los procesos de Revocación y Suspensión de certificados.

10.4 Convenciones de nombres.

10.4.1 Estándares de nombres usados

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)**

10.4.2 Componentes de los nombres

- Componente: País (C=) Valor:
  - El que corresponda según la norma descrita arriba.
- Componente: Organización (O=) Valor:
  - ID-digital
  - o, el nombre de la organización que es representada por la persona o servidor
- Componente: Sección (OU=) Valor:
  - Certificados Personales
  - O, la sección de la organización que es representada por la persona o servidor.
  -
- Componente: Nombre (CN) Valor:
  - En el caso de personas: Nombre y apellido más nº de cédula o pasaporte.
  - En el caso de servidores: nombre completo de dominio.
  - En el caso de empresas, el nombre de la empresa o el nombre del representante.
- Componente : E-mail (EA=) Valor:
  - E-mail correspondiente al solicitante (Solo para casos de certificados personales o de empresa)