AGENCIA DE SISTEMAS DE INFORMACIÓN DEL GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES

AUTORIDAD CERTIFICANTE

POLITICA DE CERTIFICACIÓN

1.- INTRODUCCION

Descripción General

El presente documento establece las políticas aplicables a las relaciones entre el Sector Público de la Ciudad Autónoma de Buenos Aires, los solicitantes y los suscriptores de los certificados digitales emitidos por la Autoridad Certificante del Gobierno de la Ciudad Autónoma de Buenos Aires, en adelante GCABA, y los terceros usuarios de dichos certificados.

Identificación

Título del Documento: Política de Certificación de la Agencia de Sistemas de Información, en adelante la ASI, Autoridad Certificante de la Ciudad Autónoma de Buenos Aires en adelante la (AC).

Versión: 2

Fecha: marzo 2023.

URL: https//pki.buenosaires.gob.ar

Lugar: Ciudad Autónoma de Buenos Aires, Argentina.

Participantes y aplicabilidad

Autoridad Certificante

La Autoridad Certificante (AC) que puede emitir certificados acordes con esta política es la Agencia de Sistemas de Información, creada por Ley Nº 2689 perteneciente al Gobierno de la Ciudad Autónoma de Buenos Aires.

Autoridad de Registro

Son Autoridad de Registro (en adelante AR), quienes sean designados por la AC como tales.

Suscriptor de Certificado

Se entiende por suscriptor de un certificado digital a la persona física, que solicita y obtiene un certificado digital emitido por la AC prevista en la presente política.

Aplicabilidad

Los certificados emitidos en el marco de la presente Política de Certificación verifican la autoría e integridad de:

a) documentos electrónicos presentados por personas físicas externas al Sector Público de la Ciudad de Buenos Aires.

b) documentos electrónicos emitidos por el Sector Público de la Ciudad de Buenos Aires.

Contactos

Esta Política de Certificación pertenece a la Agencia de Sistemas de Información, en su carácter de AC del Gobierno de la Ciudad Autónoma de Buenos Aires.

Nombre: Agencia de Sistemas de Información (ASI)
Dirección: Avda. Independencia 635, Ciudad Autónoma de Buenos Aires, República Argentina
Teléfono: (54) (11) 4323-9300
E-mail: pki@buenosaires.gov.ar

2.- ASPECTOS GENERALES DE LA POLITICA DE CERTIFICACION

Obligaciones

De la Autoridad Certificante

Informar a quien solicita un certificado digital con carácter previo a su emisión, las condiciones precisas de utilización del certificado digital, sus características y efectos de la revocación de su propio certificado digital. Esta información deberá estar libremente accesible, en redacción fácilmente comprensible en idioma nacional.

Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación y/o acceso a terceros no autorizados.

Mantener la confidencialidad de toda información que no figure en el certificado digital y a la que tenga acceso en ejercicio de las funciones definidas en la presente política.

Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados revocados (CRL), la política de certificación, la información pertinente de la última auditoría de que hubiera sido objeto, y demás documentación asociada a la presente política.

Revocar certificados digitales emitidos en caso de ser necesario.

Comunicar a la Autoridad que corresponda cualquier irregularidad que contravenga la normativa aplicable a la presente.

Mantener actualizados los repositorios de certificados revocados.

Comprobar por medio de una Autoridad de Registro la identidad y cualquier otro dato de los solicitantes considerado relevante.

Efectuar los controles funcionales de la AR a fin de verificar el cumplimiento de las responsabilidades y procedimientos de acuerdo a la presente política de certificación y demás documentos asociados.

Publicar en el Boletín Oficial de la Ciudad de Buenos Aires durante un (1) día, el certificado de clave pública correspondiente a la política para la cual obtuvo licenciamiento.

De la Autoridad de Registro

Designar los agentes que bajo su responsabilidad y dependencia se desempeñarán como autoridades de registro.

Recibir, autenticar, validar y autorizar las solicitudes de emisión y/o revocación de certificados digitales y remitirlas a la AC.

Comprobar la identidad y autenticar los datos de las personas físicas que soliciten un certificado digital y se presenten ante ella a tales efectos.

Archivar y conservar toda la documentación respaldatoria que surja del procedimiento de validación de identidad.

Mantener la confidencialidad de los datos personales de los suscriptores.

De los suscriptores del certificado

Proveer de modo completo y preciso toda la información necesaria para la emisión del certificado.

Mantener el control exclusivo de los datos de creación de firma digital, no compartirlos e impedir su divulgación.

Informar a la Autoridad de Registro el cambio de alguno de los datos contenidos en el certificado digital.

Solicitar la revocación de su certificado digital ante cualquier sospecha de compromiso de la clave o circunstancia que pueda haber comprometido la llave privada del certificado.

Tomar debido conocimiento, a través del procedimiento previsto en cada caso, del contenido de la Política de Certificación y de cualquier otro documento asociado.

De los terceros usuarios

Son terceros usuarios aquellas personas físicas o jurídicas que al recibir un documento firmado digitalmente generan una consulta a fin de verificar su validez.

Como tales están sujetos a las siguientes obligaciones:

- Tomar conocimiento de la presente política de certificación y sus documentos asociados.

- Limitar la fiabilidad de los certificados a los usos permitidos de los mismos, en conformidad con lo expresado en las extensiones del certificado y la Política de Certificación pertinente.

- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en aquellos.

Del Servicio de Repositorio

La AC debe mantener cierta información disponible en forma permanente y gratuita permitiendo su acceso público:

- A la lista de certificados revocados
- A la política de certificación y otros documentos relacionados
- A la información pertinente de los informes de auditoría de que fuera objeto la AC
- A su dirección y números telefónicos
- Cualquier otra información que determine el Ente Licenciante.

Responsabilidades

La AC será responsable, en caso de corresponder, ante terceros por el incumplimiento de sus obligaciones en relación con la emisión de los

certificados, y por la falta de revocación de aquellos en la forma y plazos previstos.

Particularmente la AC no será responsable de los siguientes supuestos:

- Utilización incorrecta de los certificados digitales ni de cualquier daño indirecto que pueda resultar de la utilización de un certificado digital o de la información suministrada por la AC.

- Daños derivados de/o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del suscriptor, acordes a esta Política de Certificación.

- No ejecución o retraso en la ejecución de cualquiera de las obligaciones en virtud de la presente Política de Certificación, si tal falta de ejecución o retraso fuera consecuencia de un supuesto de fuerza mayor o caso fortuito.

Interpretación y aplicación de las normas

Legislación Aplicable

La normativa aplicable en relación a la validez y ejecución de esta Política de Certificación es, la Ley Nacional Nº 25.506, en los aspectos pertinentes, la Ley N° 4736, y demás normativa complementaria que resulte aplicable.

Procedimientos de resolución de conflictos

La resolución de los reclamos individuales que se susciten en torno a la presente política y sus documentos asociados será resuelta en sede administrativa por el Ente Licenciante de la Ciudad Autónoma de Buenos Aires, de acuerdo a la Ley de Procedimiento Administrativo de la Ciudad Autónoma de Buenos Aires.

Publicación y repositorio de certificados y listas de certificados revocados

Publicación de información del certificador

La publicación de la información de la AC se realizará en la página https://pki.buenosaires.gob.ar.

En este sitio se puede consultar la siguiente información:

- El certificado digital de la AC.

- Los datos de contacto de la ASI.

- La Política de Certificación, y toda otra documentación asociada de carácter público, en sus versiones actuales y anteriores.

- La lista de certificados revocados (CRL).

- Información pertinente de los datos de la última auditoría de que hubiera sido objeto la ASI.

- Enlaces al Marco Normativo de Seguridad de la ASI (Resolución Nº 177/2013/ASI) y demás normativa relevante dictada por la ASI en carácter de órgano rector en materia de tecnologías de la información y telecomunicaciones del Poder Ejecutivo del Gobierno de la Ciudad de Buenos Aires.

Frecuencia de publicación

Toda información contenida en la página será actualizada y publicada inmediatamente después de hacerse disponible.

La lista de certificados revocados (CRL) será actualizada y publicada según lo estipulado en la presente política.

Controles de acceso a la información

El acceso a la información mencionada es libre y estará disponible durante las 24 horas los 7 días de la semana.

Repositorio de certificados y listas de revocación

Provee información de la lista de certificados revocados (CRL) correspondientes a la presente Política de Certificación.

Auditorías

La AC estará sujeta a auditorías por parte del Ente Licenciante.

La información que surja del último informe de auditoría será publicada en el sitio de publicación de la AC, la que será reemplazada por la información pertinente de un informe posterior.

Confidencialidad

Información Confidencial

Se considerará información confidencial y, por lo tanto no será divulgada a terceros excepto que sea exigida judicialmente:

- La clave privada de la AC.

- Toda la información relativa a las transacciones que lleve a cabo la AC.

- Toda la información relativa a seguridad, control y procedimientos de auditoría.

- Los datos de carácter personal proporcionados por los suscriptores durante el proceso de registro, con la salvedad de la información que se incluye en el certificado.

- Cualquier otra información que pudiera llegar a comprometer el desarrollo de la infraestructura de firma digital.

Información no confidencial

Se considerará información de carácter público:

- La información contenida en las Políticas de Certificación y otros documentos relacionados.

- La información del estado de validez de los certificados emitidos

- Las lista de certificados revocados (CRL)

Publicación de Información sobre la revocación de un certificado

Las listas de certificados revocados (CRL) no se consideran confidenciales y se encuentran publicadas en el sitio https://pki.buenosaires.gob.ar.

Divulgación de información como parte de un proceso administrativo

La información de carácter confidencial podrá ser revelada ante requerimiento de autoridad competente como parte de un proceso administrativo.

Divulgación de información por solicitud del suscriptor

Toda divulgación de información en relación a los datos de identificación del suscriptor de un certificado, salvo en los casos expuestos anteriormente, solo podrá efectuarse previa autorización de dicho suscriptor, excepto cuando dicha información se hubiere obtenido de fuentes de acceso público no restringidas.

El suscriptor de un certificado digital puede acceder a sus datos de identificación u otra información relacionada con su certificado digital presentando la correspondiente solicitud de información ante la AR.

3.- IDENTIFICACION Y AUTENTICACION

Registro Inicial

La solicitud de un certificado digital debe iniciarla el interesado.

El interesado debe cumplir con todos los pasos detallados en "El procedimiento de solicitud" que es publicado en el sitio https://pki.buenosaires.gob.ar.

Tipos de nombres

Será admitido solamente el nombre y apellido que figure en el documento de identidad del solicitante.

Los nombres contenidos en los certificados están restringidos a distinguished names x.500 únicos y no ambiguos.

Necesidad de nombres distintivos

Los siguientes atributos son incluidos en los certificados e identifican unívocamente al suscriptor:

- OID (Identificador de Objetos): .3.6.1.4.1. 58031.1.x (siendo x variable según tipo de certificado).
- "common Name: nombre común": se corresponde exactamente con el nombre que figura en el documento de identidad del suscriptor. - "serial number: número de serie": Aleatorio consecutivo
- "OU del Suscriptor" contiene su número de CUIT/CUIL.

- “e-mail address”: correo electrónico” está presente en todos los certificados y contiene la dirección de correo electrónico del suscriptor declarada por este durante el proceso de solicitud del certificado.

- “country name: código de país”: debe representar la nacionalidad de la AC.

Unicidad de nombres

El nombre distintivo de cada certificado es único para cada suscriptor.

Si 2 o más suscriptores tuvieran el mismo nombre y apellido, la unicidad queda resuelta por medio del atributo del CUIT/CUIL.

Existe la posibilidad de suscribir más de un certificado conigual CUIT/CUIL ya que el número de serie de uno u otro certificado será diferente.

Métodos para comprobar la posesión de la clave

Deben cumplirse los siguientes pasos:

- Durante el proceso de solicitud de certificado el solicitante es requerido para la generación de un par de claves criptográficas asimétricas.

- El par de claves es generado y almacenado en el dispositivo criptográfico del solicitante o de la AC.

- Los datos de la solicitud y el requerimiento con la clave pública del solicitante, en formato PKCS#10 son enviados a la aplicación de la AC, de esta forma se garantiza que la posesión de la clave privada la tiene exclusivamente el solicitante del certificado digital.

- La aplicación de la AC valida el requerimiento PKCS#10

- La aplicación de la AC, una vez que emite el certificado, eliminará automáticamente el requerimiento PKCS#10 asociado a ese certificado con el fin de evitar que se genere un nuevo certificado con dicho requerimiento.

- El personal de la AR involucrado en el proceso de solicitud de un certificado digital deberá abstenerse de generar, exigir, tomar conocimiento o acceder bajo ninguna circunstancia a la clave privada del suscriptor.

Autenticación de la Identidad de Personas físicas

El solicitante de un certificado digital debe presentarse ante la AR en forma personal para que ésta proceda a acreditar su identidad según el "Procedimiento de Solicitud de Certificados".

El personal de la AR que corresponda verificará que la documentación presentada por el solicitante corresponda a la persona que lo exhibe.

La AR deberá conservar toda la documentación de respaldo del procedimiento de solicitud.

Requerimiento de revocación

El requerimiento de revocación de un certificado digital puede ser hecho por su suscriptor, por el GCABA y/o por las autoridades judiciales, de acuerdo al "Procedimiento de revocación de certificados".

4.- CICLO DEL CERTIFICADO: REQUERIMIENTOS OPERATIVOS

Solicitud del Certificado

Un certificado digital es generado y luego almacenado utilizando un software y/o dispositivo criptográfico diseñado para tal fin que brinda un alto nivel de seguridad.

La solicitud debe realizarse según el Procedimiento de Solicitud de Certificados.

Emisión del Certificado

La emisión del certificado tendrá lugar una vez que la AC lo firme.

La emisión del certificado al suscriptor implica su autorización para utilizarlo según los alcances definidos en la presente Política de Certificación.

Aceptación del Certificado

El suscriptor acepta el certificado al momento de generar la solicitud.

La aceptación del certificado implica el conocimiento y aceptación de la Política de Certificación y los documentos asociados a la misma por parte del suscriptor.

Revocación del certificado

La forma de realizar la solicitud de revocación dependerá del caso y deberá hacerse según las especificaciones que se encuentran en el "Procedimiento de Revocación de Certificados" publicado en https//pki.buenosaires.gob.ar.

La AC es la única autorizada para revocar certificados digitales.

Dicha revocación podrá realizarse a partir de una solicitud del:

- Suscriptor
- GCABA por medio de la AC, la AR, el Ente Licenciante y otras autoridades para casos específicos.
- La autoridad judicial

Casos de revocación:

- **Por el suscriptor con su firma digital**

  El suscriptor deberá solicitar la revocación de su certificado utilizando su firma digital cuando:

  - Lo considere necesario
  - La información contenida en el certificado haya dejado de ser válida o se haya desactualizado.
  - La clave privada hubiere sido comprometida o se encontrare bajo serio riesgo de serlo.

- **Por el suscriptor sin su firma digital:**

  El suscriptor que no se encuentre en posesión de su clave privada (ya sea por pérdida física o lógica) deberá solicitar su revocación.

- **Por el GCABA**

  A través de su AC, AR o Ente Licenciante, se deberá solicitar la revocación del certificado del suscriptor de manera obligatoria:

- Cuando éste incumpla con las obligaciones establecidas en la presente política y demás documentos asociados a ella y en la normativa vigente que sea aplicable al certificado.

- Cuando se tuviere conocimiento o serios motivos para sospechar que su clave privada ha sido comprometida.

- A solicitud del suscriptor.

- Si el certificado digital fue emitido sobre la base de información falsa.

- Si se determina que los procedimiento de emisión y/o verificación han dejado de ser seguros.

- Por Resolución del Ente Licenciante, debidamente fundada.

- Por fallecimiento del titular debidamente comunicado al GCABA.

- Por declaración judicial de ausencia con presunción de fallecimiento del titular debidamente comunicada al GCABA.

- Por declaración judicial de incapacidad del titular debidamente comunicada al GCABA.

- Por solicitud fundada de la autoridad máxima de la jurisdicción en la que se desempeñe el titular del certificado digital.

A través de otras autoridades del Sector Público de la Ciudad de Buenos Aires en casos específicos previstos en el "Procedimiento de revocación de certificados" publicado en https//pki.buenosaires.gob.ar.

- **Por Resolución de una Autoridad Judicial.**

Solicitud de revocación

Plazo para la publicación de revocación

El plazo máximo que debe transcurrir entre la recepción de la solicitud de revocación y la efectiva publicación de la revocación es de veinticuatro (24) horas.

Frecuencia de emisión de listas de certificados revocados

La revocación se realizará de forma inmediata al procesamiento de cada solicitud verificada como válida, actualizándose el repositorio en forma inmediata y emitiendo una nueva CRL dentro de las veinticuatro (24) horas siguientes.

Requisitos para la verificación de la lista de certificados revocados

Los usuarios están obligados a verificar el estado de validez de los certificados mediante el control de la lista de certificados revocados (CRL) o mediante el servicio de consultas en línea sobre el estado de los certificados (OCSP).

Disponibilidad del servicio de consulta sobre revocación y de estado del certificado

Los servicios de CRL y OCSP se encuentran disponibles las veinticuatro (24) horas los siete (7) días de la semana sujetos a un razonable calendario de mantenimiento.

Requisitos para la verificación en línea del estado de revocación

El uso del protocolo OCSP permite, mediante su consulta, determinar el estado de validez de un certificado digital y representa una alternativa a la consulta a la CRL, la que también estará disponible. El servicio OCSP se provee por medio del sitio web https://pki.buenosaires.gob.ar/va

Procedimientos de auditoría de seguridad

La ASI registra todos los eventos relacionados con la seguridad, en archivos de transacciones de auditoría, conservándolos por un período mínimo de 10 años.

Tanto las normas para los controles de seguridad física e informática, como para la realización de las auditorías están regulados en el Marco Normativo de Seguridad de la ASI, aprobado por Resolución Nº 177/ASINF/2013, y publicado en el sitio http//pki.buenosaires.gob.ar.

Archivos de registro de eventos registrados

Toda la información recopilada en el proceso de certificación, será almacenada en un lugar seguro y de acceso restringido sólo a personal autorizado, según se establece en el Marco Normativo de Seguridad de la ASI.

Cambio de claves criptográficas de la AC

El par de claves criptográficas de la AC para ésta política tendrá una duración de 25 años.

El par de claves criptográficas de la SUB-AC para ésta política tendrá una duración de 13 años.

Plan de contingencia y recuperación ante desastres

En presencia de alguna contingencia que obligue a la suspensión del servicio, se seguirán las pautas establecidas en los procedimientos definidos en las Políticas de Certificación y en el Marco Normativo de Seguridad de la ASI.

Estos procedimientos aseguran:

- la restauración inmediata de la operatoria mínima, esto incluye registración de solicitudes de revocación y publicación y consulta de listas de certificados revocados (CRLs).

- el restablecimiento del servicio completo dentro de las 24 horas.

Compromiso de la clave privada de la AC

En el caso de compromiso de la clave privada de la AC se revocarán todos los certificados emitidos vigentes, debiendo informar a los suscriptores.

Estos procedimientos contemplarán:

- Informar a los suscriptores acerca de la revocación de sus certificados y la restricción al uso de las claves privadas asociadas a esos certificados.
- Revocar los certificados de los suscriptores
- Publicar en el sitio de publicación que se ha revocado el certificado de la AC, notificando por ese medio a los terceros usuarios que no deben considerarlo como un certificado confiable.

Plan de Cese de Actividades

En el caso que la AC vaya a discontinuar sus operaciones, procederá a notificar fehacientemente y con una antelación mayor a 60 días a todos los suscriptores.

El procedimiento a seguir para el término de actividades, así como las medidas a tomar para el archivo de los registros y documentación necesaria, estará en el "Plan de Cese de Actividades" publicado en el sitio https//pki.buenosaires.gob.ar, de conformidad con la Normativa vigente y el Marco Normativo de Seguridad de la ASI.

5.- CONTROLES DE SEGURIDAD FISICA, FUNCIONALES Y PERSONALES

Controles de seguridad física

A fin de resguardar en todo momento la seguridad de operación así como de las instalaciones y el personal que opera y administra la AC existen diversos procedimientos, políticas y controles de seguridad. Estas prácticas y procedimientos de seguridad deberán ser regularmente revisados.

Todas las instalaciones que forman parte de la AC se encuentran debidamente protegidas mediante dispositivos y personal de vigilancia durante las 24 horas los 7 días de la semana, que restringen el acceso a los equipos, programas y datos sólo a aquellas personas autorizadas.

Esto implica la implementación de controles de:

- Construcción y ubicación de las instalaciones
- Acceso físico
- Energía eléctrica y aire acondicionado
- Exposición al agua e inundaciones
- Prevención y protección contra incendio
- Medios de almacenamiento de información
- Descarte de medios de almacenamiento de información

Controles funcionales

Mediante normas de seguridad establecidas en el Marco Normativo de Seguridad, se limita el acceso a los recintos, obligando a hacerlo en compañía del personal habilitado para cada caso.

Sobre las actividades realizadas por cada empleado que ingresa a la AC se realizan auditorias periódicas.

El personal que interviene, es capacitado en forma permanente en la implementación de políticas y procedimientos de seguridad.

- Definición de roles afectados al proceso de certificación:

• Responsable de la AC: encargado de garantizar el correcto funcionamiento de la AC, seleccionar y designar a los agentes para cada uno de los roles.

- Responsable de Seguridad Informática: encargado de definir las herramientas de seguridad informática de acuerdo a Manual Normativo de Seguridad, verificar y controlar su cumplimiento en cuanto a los accesos a la información se refiere, revisar logs de transacciones y del sistema e informar al Responsable de la AC y al Auditor Interno, y de autorizar las solicitudes de altas, bajas o modificaciones de accesos a la aplicación.

- Responsable de las Aplicaciones: tiene a su cargo diseñar, desarrollar, implementar y mantener los sistemas aplicativos requeridos para el funcionamiento de AC, de acuerdo a las disposiciones establecidas en el Manual de Prácticas de Certificación.

- Auditor Interno: debe verificar y controlar el cumplimiento de todas las disposiciones de la AC (Seguridad, Procedimientos, Certificación), verificar y controlar la preparación de los procesos de emergencia (Plan de Contingencia) verificar y controlar la preparación de los procesos de finalización (Plan Cese de Actividades) e informar al Responsable de la AC respecto de las desviaciones, incumplimientos o situaciones de riesgo que se detecten.

Número de personas requerido por función:

Cada rol tiene un titular y un sustituto designado .

Identificación y autentificación para cada rol:

Todos los usuarios autorizados de la AC se identifican mediante certificados digitales emitidos por la propia PKI y se autentifican por medio de dispositivos criptográficos portátiles en el caso de ser requeridos.

- En el caso de las AR, la AC efectuará los controles funcionales pertinentes, verificando el cumplimiento de las responsabilidades y procedimientos según lo dispuesto en la presente Política de Certificación y demás documentación asociada.

6.- CONTROLES DE SEGURIDAD TECNICA

Generación e instalación del par de claves criptográficas

- Generación del par de claves criptográficas

La AC generará un par de claves criptográficas en un ambiente seguro y en un hardware criptográfico FIPS 140-2 Nivel 3. Utilizando algorítmo RSA de 4096 bits. Este acto se realizará con presencia y participación de personal autorizado.

El par de claves criptográficas del suscriptor de un certificado emitido en los términos de esta política debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y permanente conocimiento y control.

El suscriptor es considerado titular del par de claves; como tal, no debe revelar su clave privada a terceros bajo ninguna circunstancia.

La clave pública del suscriptor del certificado debe ser transferida a la AC de manera tal que se asegure que no pueda ser cambiada durante la transferencia.

- Entrega de la clave privada al suscriptor

La clave privada del suscriptor es generada por este durante el proceso de solicitud del certificado. La AC no debe generar, exigir, tomar conocimiento o acceder a los datos de creación de la firma.

Las claves del firmante pueden ser generadas mediante dispositivos hardware y/o software autorizados por ASI-GCABA.

- Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.
- En certificados en dispositivo de creación de firma la clave privada se genera y se almacena debidamente protegida en el interior de dicho dispositivo.
- En certificados en dispositivo centralizado la clave privada del firmante se genera en un área privada del firmante en un HSM remoto. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o intercepción por el sistema de generación y custodia remota. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

- Entrega de la clave pública a la AC

La clave pública del suscriptor es entregada a la AC durante el proceso de solicitud del certificado. El proceso de solicitud utiliza el formato PKCS#10 para implementar la “prueba de posesión” remitiendo los datos del solicitante y su clave pública dentro de una estructura firmada con su clave privada.

- Disponibilidad de la clave pública

La clave pública de la AC se puede descargar de https://pki.buenosaires.gob.ar

- Propósitos de utilización de claves (campo “key usage” en certificados x.509 v.3)

Las claves contenidas en los certificados emitidos por la AC tienen como propósito su utilización para firmar digitalmente, por lo que los valores a

utilizar en la extensión “KeyUsage” de los certificados son Firma Digital (“digitalSignature”) y No Repudio (“nonRepudiation”).

Protección de la clave privada

- Estándares para dispositivos criptográficos

Se requiere que el módulo utilizado para la creación de claves utilizadas por la AC cumpla con la certificación FIPS140-2 de nivel 3.

Se requiere que para la generación y almacenamiento de las claves criptográficas de los agentes de la AR sean dispositivos criptográficos certificados FIPS 140-2 Nivel 2.

Para los suscriptores con certificados de nivel de seguridad Alto, se requiere que para la generación y almacenamiento de las claves criptográficas sean dispositivos criptográficos certificados FIPS 140-2 Nivel 2.

- Control M de N de la clave privada

La clave privada de la AC está sujeta a un control multi-personal.

Cuando se genera la clave privada por primera vez, se divide en múltiples fragmentos que son distribuidos cifrados con una clave de activación.

Los módulos criptográficos que manejan las claves privadas, tanto para su generación como eventual recuperación posterior, son activados usando claves de activación, las cuales son administradas sólo por personal autorizado.

- Recuperación de la clave privada

La AC posee procedimientos para la recuperación de su clave privada a partir de copias de respaldo.

Esta recuperación solo puede ser realizada por personal autorizado y de conformidad a los lineamientos detallados en el Marco Normativo de Seguridad de la ASI.
No existen mecanismos de recuperación de la clave privada de la autoridad de registro o de los suscriptores. En estos casos se deberá revocar el certificado de conformidad a los procedimientos descriptos en la presente política.

- Copia de seguridad de la clave privada

Las copias de back-up de las claves privadas de la AC se almacenan en dispositivos de hardware criptográfico con certificación FIPS 140-2 de nivel 3.

- Método de activación de claves privadas

La activación de la clave privada de la AC utiliza un esquema de control compartido (M de N), por lo que se necesita la intervención simultánea de varios actores autorizados para ello.

- Método de desactivación de claves privadas

La desactivación de la clave privada de la AC debe seguir el procedimiento establecido a tal fin y se realiza exclusivamente por:

- tareas de mantenimiento
- utilización de equipamiento de respaldo

El procedimiento deberá realizarse exclusivamente por personal capacitado a tal efecto que garantice el éxito de la operación.

- Método de destrucción de claves privadas

Si por cualquier motivo deja de utilizarse la clave privada de la AC para crear firmas digitales, aquella será destruida bajo las mismas medidas de seguridad que se emplearon para su creación.

Otros aspectos de administración de claves

- Archivo permanente de la clave pública

La AC mantiene un archivo de todos los certificados emitidos por un período de 10 años.
El archivo se denomina repositorio de certificados digitales y puede consultarse en el sitio https//pki.buenosaires.gob.ar.

- Período de uso de clave pública y privada

Los certificados emitidos por la AC a los suscriptores tienen una validez de máximo dos (2) años desde que se emiten.
El certificado de la AC tiene una validez de veinticinco (25) años y la SUB-AC de trece (13) años, transcurrido dicho plazo todos los certificados emitidos por la AC expirarán automáticamente perdiendo su validez.

Datos de activación

- Generación e instalación de datos de activación

Los datos de activación del dispositivo criptográfico donde se genera y almacena la clave privada de la AC tiene un control "M de N" siendo "M" el número mínimo de presenciales poseedores de las claves de activación de un total de "N" poseedores.

El procedimiento y metodología así como los parámetros utilizados y el personal involucrado queda asentado al inicio de actividades en el Acta respectiva y en el libro rubricado para tal fin.

- Protección de los datos de activación

Los datos de activación de la AC son confidenciales y por ello las personas responsables de su guarda están obligadas a no divulgarlos.

Controles de seguridad informática

La AC efectúa los controles de Seguridad Informática de acuerdo a las normas especificadas en el Marco Normativo de Seguridad de la ASI que cumple los requerimientos establecidos en la legislación y estándares vigentes.

- Requisitos técnicos específicos

El acceso a las instalaciones y sistemas que intervienen en el proceso de certificación solo es autorizado a personal previamente validado y autenticado para cumplir funciones en el proceso de certificación de conformidad con esta política y el Marco Normativo de Seguridad de la ASI.

Controles de seguridad de red

La AC efectúa por medio de Seguridad Informática los controles de acuerdo a las normas especificadas en el Marco Normativo de Seguridad de la ASI que cumple los requerimientos establecidos en la legislación y estándares vigentes.

Asimismo la publicación de datos y servicios que realiza la AC utiliza sistemas tecnológicos debidamente protegidos para garantizar su seguridad.

Controles de ingeniería de dispositivos criptográficos

El dispositivo criptográfico utilizado por el certificador está certificado por el NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 3.

Los dispositivos criptográficos utilizados por las AR están certificados por NIST (National Institute of Standards and Technology) sobre la base del Estándar FIPS 140-2 Nivel 2.

7.- PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS

Perfil del Certificado

Los certificados emitidos por la AC cumplen con los requerimientos de la DA 6/2007 y lo establecido en la especificación ITU X.509 versión 3 (ISO/IEC 9594-8).

- Se usarán los siguientes campos del formato x.509 v3 en el Certificado de la AC:

Certificados X.509	Contenido
Versión	3
Número de serie	Asignado por la AC del GCABA
Algoritmo de firma	SHA256 con RSA
Nombre distinguido del emisor	CN=GCABA ROOT CA UO= PKI - GCABA O= Gobierno de la Ciudad Autonoma de Buenos Aires
	C=AR
Validez	No válido antes de (hora estándar de AR) No válido después de (hora estándar de AR) 25 años
Nombre distinguido del suscriptor	CN=GCABA ROOT CA UO= PKI - GCABA O= Gobierno de la Ciudad Autonoma de Buenos Aires C=AR
Clave pública del suscriptor	Encripción RSA 4096

EXTENSION	
Uso de clave	Uso= Firma digital, Firma de Certificados, Firma CRL sin conexión, Firla de lista de revocación de certificados (CRL)
Restricciones básicas	Entidad de Certificación (CA)
Nombre alternativo del titular	pki@buenosaires.gob.ar

- Se usarán los siguientes campos del formato x.509 v3 en el Certificado de la SUBAC:

Certificados X.509	Contenido
Versión	3
Número de serie	Asignado por la AC del GCABA
Algoritmo de firma	SHA256 con RSA
Nombre distinguido del emisor	CN= GCABA ROOT CA UO= PKI - GCABA O= Gobierno de la Ciudad Autonoma de Buenos Aires
	C=AR
Validez	No válido antes de (hora estándar de AR) No válido después de (hora estándar de AR) 13 años
Nombre distinguido del suscriptor	CN= GCABA Subordinate CA 01 UO= PSC - GCABA O= Gobierno de la Ciudad Autonoma de Buenos Aires C=AR
Clave pública del suscriptor	Encripción RSA 4096
EXTENSION	

Uso de clave	Uso= Firma digital, Firma de Certificados, Firma CRL sin conexión, Firla de lista de revocación de certificados (CRL)
Restricciones básicas	Entidad de Certificación (CA)
Nombre alternativo del titular	pki@buenosaires.gob.ar

- Se usarán los siguientes campos del formato x.509 v3 en el Certificado de los Suscriptores de Certificados de la AC:

Certificados X.509	Contenido
Versión	3
Número de serie	Asignado por la AC del GCABA
Algoritmo de firma	SHA256 con RSA
Nombre distinguido del emisor	CN= GCABA Subordinate CA 01 UO= PSC - GCABA O= Gobierno de la Ciudad Autonoma de Buenos Aires C=AR

Validez	No válido antes de (Hora estándar de AR) No válido después de (Hora estándar de AR
Nombre distinguido del suscriptor	CN=Nombre y Apellido del suscriptor OU=CUIL/CUIT DC=ar
Clave pública del suscriptor	Encripción RSA 2048 Uso= Encriptar, Verificar, Ajustar, Derivar

EMail	Correo electrónico del suscriptor
EXTENSION	
Uso de clave	(2.5.29.15) Crítico = SI Firma digital, Sin rechazo, Encriptación de la clave, Codificación de datos, Sólo codificar, Sólo descodificar
Restricciones básicas	(2.5.29.19)
Uso de clave ampliada	(2.5.29.37) Crítico = NO IPSec, SSHClient, PDFSigning
Identificador de clave del sujeto	(2.5.29.14) Crítico = NO
Identificador de clave de entidad emisora	(2.5.29.35) Crítico = NO
Puntos de distribución de CRL	(2.5.29.31) Crítico = NO https://pki.buenosaires.gob.ar/crl/subca.crl
Acceso a la información de la entidad de certificación	(1.3.6.1.5.5.7.1.1) Crítico = NO Protocolo de estado del certificado en línea (1.3.6.1.5.5.7.48.1) URL= https://pki.buenosaires.gob.ar/va

Perfil de la lista de certificados revocados

El formato de las CRLs utilizadas en la presente política es el especificado en la versión 2 (v2), X.509 v2.

Se usarán los siguientes campos del formato especificado para la lista de Certificados Revocados de la AC de la Agencia de Sistemas de Información:

Certificados X.509	Contenido
Versión	**2**
Número de CRL	**Consecutivo al anterior**
Algoritmo de firma	**SHA256 con RSA**
Nombre distinguido del emisor	**CN=GCABA Subordinate CA 01** **UO=PSC - GCABA** O= Gobierno de la Ciudad Autonoma de Buenos Aires L=Buenos Aires **C=AR**
Fecha efectiva	**Nombre día, Fecha_día de Mes de Año hh:mm:ss**
Próxima actualización	**24 horas**
Nombre distinguido del suscriptor	**CN= GCABA Subordinate CA 01**
	UO=PSC - GCABA O= Gobierno de la Ciudad Autonoma de Buenos Aires L=Buenos Aires **C=AR**
Lista de revocaciones	**Número de serie de certificados revocados Fecha de revocación.**

8.- ADMINISTRACION DE ESPECIFICACIONES

Procedimientos de cambio de especificaciones

Toda nueva versión de la presente política de certificación deberá ser sometida a la aprobación del Ente Licenciante del GCABA.

Procedimientos de publicación y notificación

Las sucesivas versiones de la presente política de certificación o de cualquiera de los documentos asociados , una vez aprobadas, deberán ser publicadas en el sitio de publicación de la AC, http//pki.buenosaires.gob.ar.

GLOSARIO

Browser: Navegador. Programa utilizado para visualizar las páginas web. Los más utilizados son Internet Explorer y Mozilla Firefox.

AC: Autoridad certificante – AC o CA por sus siglas en idioma inglés Certification Authority, es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la firma electrónica y digital.

Ente Licenciante: la autoridad del GCABA encargada de otorgar las licencias a los organismos que así lo soliciten a fin de que, una vez aprobada, estos se conviertan en Autoridad Certificante del GCABA.

AR: Autoridad de Registro es la que controla la generación de certificados para los miembros de una entidad. Previa identificación del solicitante de un certificado, la Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes del suscriptor del certificado.

Solicitante: todo potencial suscriptor de un certificado digital provisto por la AC del GCABA.

Suscriptor: toda persona física a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en aquel.

Terceros usuarios: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente.

Certificado Digital: es un documento digital mediante el cual un tercero confiable –una autoridad de certificación- garantiza la vinculación entre la identidad de un sujeto y su clave pública.

CRL: lista de certificados que han sido dejados sin efecto en forma permanente por el certificador licenciado (AC), la cual ha sido firmada digitalmente y publicada por dicha autoridad.

Drivers: pequeño programa cuya función es controlar el funcionamiento de un dispositivo de la PC.

Firma Digital o firma electrónica: es un tipo de tecnología que permite identificar al firmante y poder detectar cualquier alteración del documento digital con posterioridad a su firma. La diferencia entre ambas radica en que, en el caso del documento firmado digitalmente, si es verificado correctamente, se presume salvo prueba en contrario, que proviene del suscriptor del certificado digital y que no fue modificado. Tal situación no ocurre en caso de que el documento se encuentre firmado electrónicamente, ya que se invierte la carga probatoria, y de ser desconocida esta firma, corresponde a quien invoca su autenticidad acreditar su validez.

FIPS 140: la Federal Information Processing Standard 140 son una serie de publicaciones que especifican los requerimientos para los módulos criptográficos.
HSM: módulo de seguridad por hardware

LOG's: es un registro oficial de eventos durante un período de tiempo en particular

PIN: número de identificación personal, es generalmente un valor numérico usado para identificarse y poder tener acceso a ciertos sistemas o artefactos, como un teléfono móvil o un cajero automático.

PKI: Infraestructura de clave pública, es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías, de operaciones como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Una PKI debe permitir:

- Autenticidad: la firma digital tendrá la misma validez que la manuscrita
- Confidencialidad: de la información transmitida entre las partes
- Integridad: debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado
- No repudio: de un documento firmado digitalmente

Protocolo PKCS#10: es un formato electrónico estandarizado para realizar requerimientos de certificados digitales.

Servicio OCSP: servicio de verificación en línea del estado de los certificados

RSA: algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye y otra privada la cual es guardada en secreto por su titular.

SHA: es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).

Control M de N: sistema de confianza y garantía para la ejecución de tareas o comandos críticos dentro de un sistema informático, que exige la concurrencia mínima de M entidades distintas (personas) de un total designado de N, para poder ejecutar dicha tarea o comando. N se elige mayor que M para garantizar el quórum adecuado para este sistema de confianza.

TOKEN: Dispositivo criptográfico que permite el almacenamiento seguro de la clave privada del suscriptor.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
"1983-2023. 40 Años de Democracia"

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2023-11903927-GCABA-DGSEI

Buenos Aires, Miércoles 22 de Marzo de 2023

Referencia: Política de Certificación - PKI

El documento fue importado por el sistema GEDO con un total de 29 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.03.22 18:16:56 -03'00'

Gustavo Linares
Director General
D.G SEGURIDAD INFORMATICA
MINISTERIO JEFATURA DE GABINETE

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.03.22 18:16:57 -03'00'