CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

ALADI
Asociación Latinoamericana de Integración
Associação Latino-Americana de Integração

ESTADO DE SITUACIÓN DE LA IMPLEMENTACIÓN DE LA FIRMA DIGITAL EN CUBA

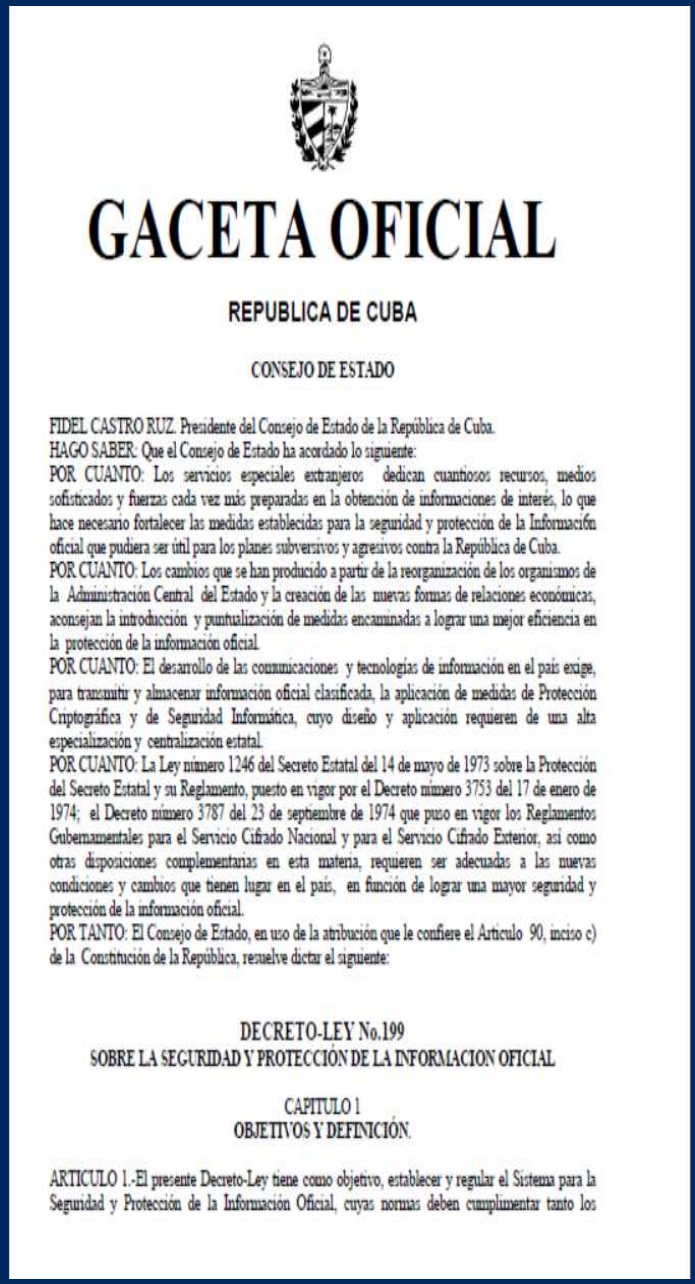
II Reunión de Expertos en Firma Digital
22 de mayo de 2018
Montevideo - Uruguay

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

Normativas que regulan la materia

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

El Decreto-Ley No. 199 del Consejo de Estado de la República de Cuba, “Sobre la Seguridad y Protección de la Información Oficial”, de 25 de noviembre de 1999, establece y regula el Sistema para la Seguridad y Protección de la Información Oficial y la Criptografía, y faculta al Ministerio del Interior para dictar cuantas disposiciones resulten necesarias para su cumplimiento.



GACETA OFICIAL

REPUBLICA DE CUBA

CONSEJO DE ESTADO

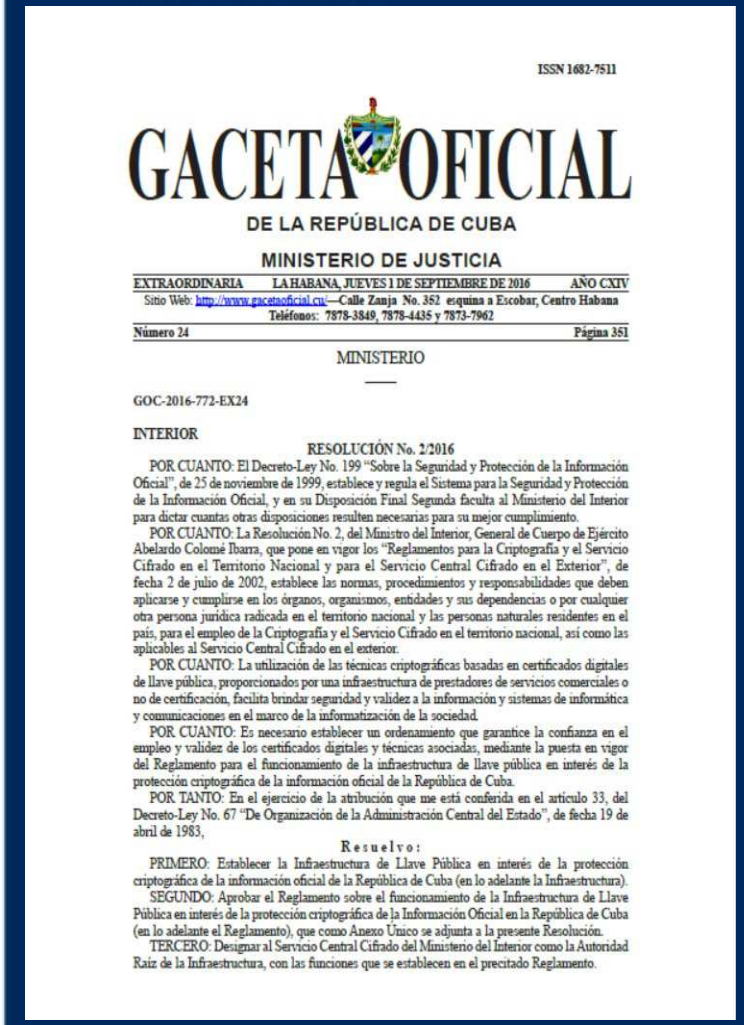
FIDEL CASTRO RUZ. Presidente del Consejo de Estado de la República de Cuba.
HAGO SABER: Que el Consejo de Estado ha acordado lo siguiente:
POR CUANTO: Los servicios especiales extranjeros dedican cuantiosos recursos, medios sofisticados y fuerzas cada vez más preparadas en la obtención de informaciones de interés, lo que hace necesario fortalecer las medidas establecidas para la seguridad y protección de la Información oficial que pudiera ser útil para los planes subversivos y agresivos contra la República de Cuba.
POR CUANTO: Los cambios que se han producido a partir de la reorganización de los organismos de la Administración Central del Estado y la creación de las nuevas formas de relaciones económicas, aconsejan la introducción y puntualización de medidas encaminadas a lograr una mejor eficiencia en la protección de la información oficial.
POR CUANTO: El desarrollo de las comunicaciones y tecnologías de información en el país exige, para transmitir y almacenar información oficial clasificada, la aplicación de medidas de Protección Criptográfica y de Seguridad Informática, cuyo diseño y aplicación requieren de una alta especialización y centralización estatal.
POR CUANTO: La Ley número 1246 del Secreto Estatal del 14 de mayo de 1973 sobre la Protección del Secreto Estatal y su Reglamento, puesto en vigor por el Decreto número 3753 del 17 de enero de 1974; el Decreto número 3787 del 23 de septiembre de 1974 que puso en vigor los Reglamentos Gubernamentales para el Servicio Cifrado Nacional y para el Servicio Cifrado Exterior, así como otras disposiciones complementarias en esta materia, requieren ser adecuadas a las nuevas condiciones y cambios que tienen lugar en el país, en función de lograr una mayor seguridad y protección de la información oficial.
POR TANTO: El Consejo de Estado, en uso de la atribución que le confiere el Artículo 90, inciso c) de la Constitución de la República, resuelve dictar el siguiente:

DECRETO-LEY No.199
SOBRE LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACION OFICIAL

CAPITULO I
OBJETIVOS Y DEFINICIÓN.

ARTICULO 1.-El presente Decreto-Ley tiene como objetivo, establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial, cuyas normas deben cumplimentar tanto los

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa



ISSN 1682-7511

GACETA OFICIAL
DE LA REPÚBLICA DE CUBA

MINISTERIO DE JUSTICIA

EXTRAORDINARIA — LA HABANA, JUEVES 1 DE SEPTIEMBRE DE 2016 — AÑO CXIV

Sitio Web: http://www.gacetaoficial.cu/—Calle Zanja No. 352 esquina a Escobar, Centro Habana
Teléfonos: 7878-3849, 7878-4435 y 7873-7962

Número 24 — Página 351

MINISTERIO

GOC-2016-772-EX24

INTERIOR

RESOLUCIÓN No. 2/2016

POR CUANTO: El Decreto-Ley No. 199 "Sobre la Seguridad y Protección de la Información Oficial", de 25 de noviembre de 1999, establece y regula el Sistema para la Seguridad y Protección de la Información Oficial, y en su Disposición Final Segunda faculta al Ministerio del Interior para dictar cuantas otras disposiciones resulten necesarias para su mejor cumplimiento.

POR CUANTO: La Resolución No. 2, del Ministro del Interior, General de Cuerpo de Ejército Abelardo Colomé Ibarra, que pone en vigor los "Reglamentos para la Criptografía y el Servicio Cifrado en el Territorio Nacional y para el Servicio Central Cifrado en el Exterior", de fecha 2 de julio de 2002, establece las normas, procedimientos y responsabilidades que deben aplicarse y cumplirse en los órganos, organismos, entidades y sus dependencias o por cualquier otra persona jurídica radicada en el territorio nacional y las personas naturales residentes en el país, para el empleo de la Criptografía y el Servicio Cifrado en el territorio nacional, así como las aplicables al Servicio Central Cifrado en el exterior.

POR CUANTO: La utilización de las técnicas criptográficas basadas en certificados digitales de llave pública, proporcionados por una infraestructura de prestadores de servicios comerciales o no de certificación, facilita brindar seguridad y validez a la información y sistemas de informática y comunicaciones en el marco de la informatización de la sociedad.

POR CUANTO: Es necesario establecer un ordenamiento que garantice la confianza en el empleo y validez de los certificados digitales y técnicas asociadas, mediante la puesta en vigor del Reglamento para el funcionamiento de la infraestructura de llave pública en interés de la protección criptográfica de la información oficial de la República de Cuba.

POR TANTO: En el ejercicio de la atribución que me está conferida en el artículo 33, del Decreto-Ley No. 67 "De Organización de la Administración Central del Estado", de fecha 19 de abril de 1983,

Resuelvo:

PRIMERO: Establecer la Infraestructura de Llave Pública en interés de la protección criptográfica de la información oficial de la República de Cuba (en lo adelante la Infraestructura).

SEGUNDO: Aprobar el Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública en interés de la protección criptográfica de la Información Oficial en la República de Cuba (en lo adelante el Reglamento), que como Anexo Único se adjunta a la presente Resolución.

TERCERO: Designar al Servicio Central Cifrado del Ministerio del Interior como la Autoridad Raíz de la Infraestructura, con las funciones que se establecen en el precitado Reglamento.

El Ministerio del Interior emite la Resolución No. 2/2016, publicada en la Gaceta Oficial No. 24 Extraordinaria de 1 de septiembre de 2016, la cual:

- Establece la Infraestructura de Llave Pública de la República de Cuba.
- Aprueba el Reglamento sobre el funcionamiento de la Infraestructura de Llave Pública.
- Designa al Servicio Central Cifrado del Ministerio del Interior como la Autoridad Raíz de la Infraestructura.

Entró en vigor el 1 de diciembre de 2016.

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

Requisitos de validez de los certificados digitales

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

1. **Permite identificar unívocamente al titular.**

- El máximo ejecutivo del organismo o entidad certifica, mediante documento oficial al PS, los datos del futuro titular y la función que realiza en el organismo o entidad.
- La Autoridad de Registro vinculada al PS verifica veracidad de datos mediante el Sistema Único de Identificación Nacional y otros mecanismos estatales establecidos.
- En el certificado digital aparece el nombre completo del titular, número de identidad permanente, organismo al que pertenece y función que realiza y no se admite el uso de alias.

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

2. Ser generado por un prestador de servicios acreditado.

- Todo PS tiene que estar acreditado por Resolución del Ministro del Interior, luego de pasar un proceso de evaluación, que demuestre cumple todos los requerimientos establecidos en el Reglamento.
- Todos los PS acreditados son controlados y auditados periódicamente por:
  - Autoridad certificadora superior y la Autoridad Raíz.
  - Órganos estatales encargados de la criptografía, seguridad y protección de la información y protección contra incendios.
  - Contraloría General de la República.
- El PS tendrá su certificado digital emitido y firmado por la autoridad certificadora superior.

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

3. Ser susceptible de verificar su estado de revocación.

- Todo PS está obligado a mantener permanentemente un servicio público para la descarga de las listas de certificados revocados y un protocolo para la verificación en línea del estado de los certificados.
- El modo de acceso a estos servicios tiene que estar incluido en los certificados digitales que genera.

Además, para los certificados de firma digital se debe cumplir:

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

4. Vinculado únicamente al titular.

- La llave privada la genera y custodia el suscriptor.
- Si la llave privada, a solicitud del titular o por razones técnicas o de seguridad se genera en la AC, su producción se realiza obligatoriamente, mediante separación de roles, por tres funcionarios y se entrega en un dispositivo informático o electrónico protegido con medidas de cifrado y control de acceso.
- La AC no guarda copia de la llave privada, con el objetivo de asegurar la posesión exclusiva de su titular, en la garantía de la no existencia de dudas en la unicidad total del ejercicio de firma y el no repudio en esta acción, de forma tal que no se pueda involucrar a la autoridad en hechos de falsificación o suplantación de la firma digital.

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

5. Control del medio de creación de firma por el titular.

Obligaciones de los suscriptores:

- Resguardar en lugar seguro, los dispositivos y llave privada para las operaciones criptográficas autorizadas a realizar.
- No transferir a otra persona, los dispositivos para las operaciones criptográficas, la llave privada y la clave personal de acceso al dispositivo de creación de firma.

6. Detectar cualquier modificación de los datos firmados.

El uso de funciones hash garantiza integridad de los datos. En la infraestructura se utilizan los algoritmos de firma:

- SHA2 con RSA
- SHA2 con ECDSA

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

7. **Poseer un dispositivo de creación de firma técnicamente segura y confiable.**

En la infraestructura se utilizan como contenedores de llave privada:

- Memorias flash cifradas
- eToken

8. **Identificar la política de certificación bajo la cual fue emitido.**

Todos los PS están obligados a publicar la Declaración de Prácticas y Políticas de Certificación.

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

Requisitos para el reconocimiento de certificados de firma digital emitidos por prestadores de servicios extranjeros

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

Aquellos que se establezcan en acuerdos y convenios aprobados por los órganos y organismos de la Administración Central del Estado competentes.

La Autoridad Raíz funge como autoridad de enlace técnico con las autoridades raíces de otros países y de organizaciones internacionales con las que se hayan establecido los acuerdos y convenios.

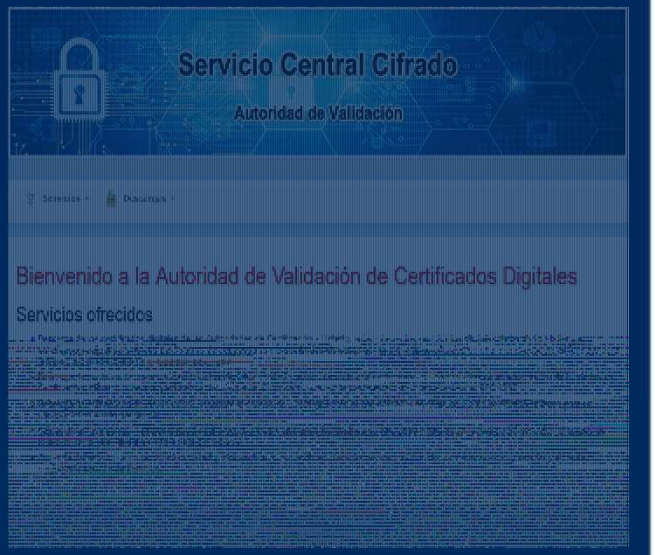
CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

Identificación de la Autoridad Certificadora Raíz de la República de Cuba

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

Autoridad de Certificación Servicio Central Cifrado (ACSCC)

- Certificado No. de serie: 02 54 0b e4 01
- Válido desde el 14 /12/2015 hasta 10/12/2030
- Algoritmo de firma: SHA512RSA
- Llave pública RSA de 8192 bits
- Huella digital: 67 f8 58 9b bb 97 e4 38 cd 30 79 02 cb 38 01 12 46 62 70 13




Autoridad de Certificación Raíz de la República de Cuba

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

AUTORIDAD DE CERTIFICACIÓN SERVICIO CENTRAL CIFRADO, AUTORIDAD RAÍZ DE LA INFRAESTRUCTURA DE LLAVE PÚBLICA DE LA REPÚBLICA DE CUBA

(Versión 1.0)

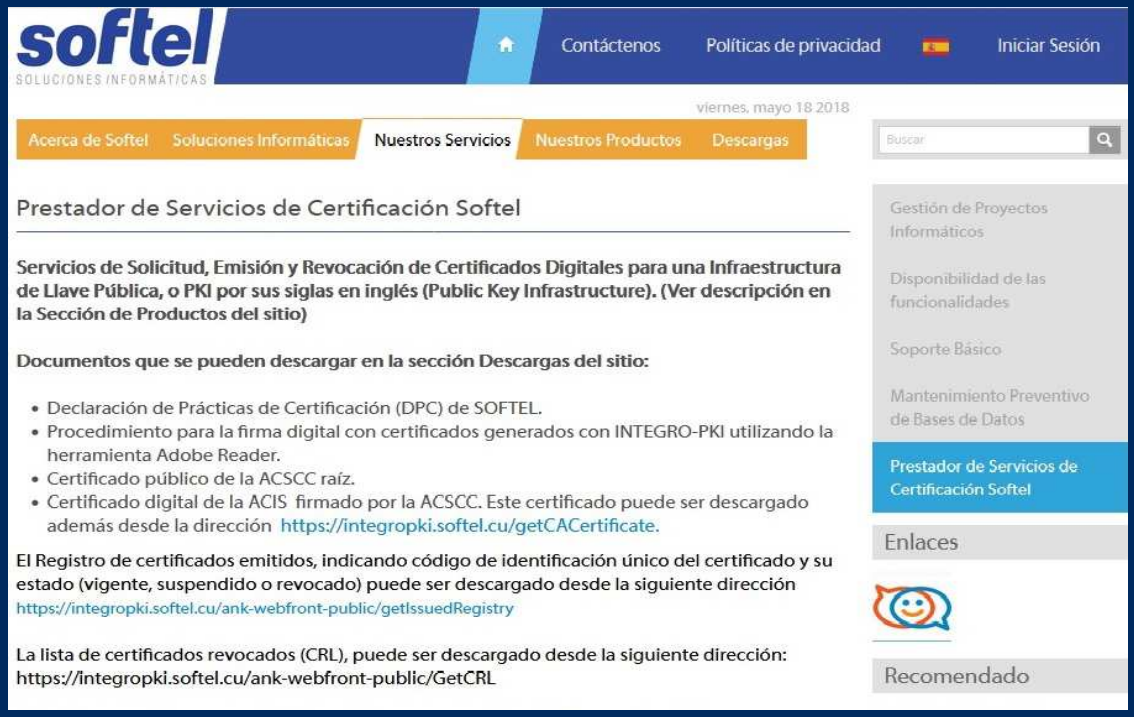
DICIEMBRE DE 2016
"AÑO 58 DE LA REVOLUCIÓN"

- Descarga de CRL
  http://crl.sercencif.cu/va/crls/search.cgi
- OCSP
  http://ocsp.sercencif.cu/va/status/ocsp

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

Identificación de los prestadores de servicios de certificación acreditados

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa



La empresa SOFTEL, actualmente en proceso de acreditación como PS en la infraestructura, es la contratada para la emisión de los certificados digitales para los FH de la Cámara de Comercio de la República de Cuba.

Hasta su acreditación oficial, los certificados serán generados por la Autoridad Raíz.

CÁMARA DE COMERCIO
DE LA REPÚBLICA DE CUBA
Nuestra Misión es su Empresa

ALADI
Asociación Latinoamericana de Integración
Associação Latino-Americana de Integração

ESTADO DE SITUACIÓN DE LA IMPLEMENTACIÓN DE LA FIRMA DIGITAL EN CUBA

II Reunión de Expertos en Firma Digital
22 de mayo de 2018
Montevideo - Uruguay