Política de Certificados

Para los Titulares de certificados digitales

Los certificados digitales emitidos por la Autoridad Certificadora ETECSA (AC ETECSA) pueden ser utilizados por personas jurídicas y naturales radicadas en el territorio nacional, bajo su total responsabilidad y cuidado, para trámites nacionales o internacionales –en este último caso, si la otra parte reconoce y acepta como válidos los certificados emitidos por la AC ETECSA -, bajo total reconocimiento según el marco legal vigente en Cuba.

Procedimiento de Registro

La solicitud de cualquier tipo de certificado digital recorre el mismo flujo de operaciones.

- La primera inserción de datos de un solicitante en la PGCD es efectuada por su Representante. El Representante es aprobado por la máxima autoridad de la Unidad Organizativa solicitante del Servicio, para el caso de personas jurídicas, y es el responsable de verificar los datos personales del solicitante a través de la presentación del C.I e introducirlos en la PGCD, según el tipo de certificado objetivo.
  - Durante la primera etapa de funcionamiento de la AC, los solicitantes son trabajadores de ETECSA. Su identidad será recuperada de los sistemas de información de trabajadores (BDUT-ETECSA[1]) con que cuenta la Empresa.
  - Para el caso de personas naturales, en una primera etapa de comercialización, se registrarán presencialmente en las Oficinas Comerciales de ETECSA, presentando su C.I.
  - Durante la etapa de comercialización electrónica, los mecanismos de verificación se efectuarán usando chequeos cruzados entre bases de datos de información bancaria, telefónica y de la Ficha Única del Ciudadano.
- La solicitud hecha por el Representante es enviada a un Funcionario ER para ser *aprobada*.
  - Un Funcionario ER puede listar las solicitudes de acuerdo al tipo de certificado, de la más antigua a la más reciente, verifica en los detalles de cada solicitud si los datos correspondientes a cada campo están completos.
- Se establece un periodo máximo de 72 H para la aprobación de una solicitud por un Funcionario ER.
- La aprobación de una solicitud genera en la interfaz de un Funcionario EC una petición de Emisión –si el modo de operación de la AC está configurado como *Manual*- la cual este emitirá, una a una-. Con este proceso finalizado quedará finalmente emitido un certificado digital.
  - Si el modo de operación de la AC está configurado como Automático, tras aprobarse la solicitud, la PGCD comprueba la integridad de los datos contenidos en esta y emitirá el certificado digital.
- La emisión de un certificado genera una cadena de notificaciones por correo electrónico al Titular del certificado, a su Representante y al Funcionario ER que aprobó la solicitud, confirmando dicha acción.

[1] Este sistema es manejado por el personal del área de RR.HH.

- El Titular, además de la confirmación de emisión, recibirá un enlace de descarga y una contraseña aleatoria para proceder a la descarga del archivo .p12 correspondiente a su solicitud.

Usos del certificado

Aun cuando los certificados digitales tienen múltiples propósitos en el mundo tecnológico actual, los generados por la AC ETECSA enmarcan su aplicación en correspondencia con su tipo.

- De Entidad Final:
  - Firma de documentos digitales, Firma de certificados, Firma de CRL, No Repudio.
  - Acuerdo de Llave, Cifrado de Llave.
- De SSL y VPN:
  - Autenticación Servidor Web TLS, Autenticación Cliente Web TLS.

Las aplicaciones mayormente experimentadas por los Titulares de certificados digitales se remiten a la firma de documentos digitales, asegurando no solo su integridad sino también el reconocimiento de los firmantes. Esta variante debe constituir una alternativa importante en el ahorro de materiales de oficina, en el ahorro de tiempo de traslado de documentos impresos y por consiguiente de combustible, en la conservación y almacenamiento por prolongados periodos de tiempo; así como la posibilidad de realizar copias de seguridad de dichos documentos.

Limitaciones en el uso de certificados

Los certificados digitales emitidos por la AC ETECSA no deben utilizarse para: cifrar datos, ficheros, correos electrónicos u otro tipo de información.

No se acepta como práctica la utilización de estos certificados en actividades fraudulentas, que perjudiquen la integridad de personas o instituciones nacionales o extranjeras.

Obligaciones de las partes del PSCC y los Titulares

De la Entidad de Certificación

- La Entidad de Certificación está en la obligación de emitir los certificados digitales de Entidad Final, SSL y VPN; con la mejor tecnología vigente en materia de seguridad y confianza;
- Asegurar la entrega confiable y respaldada de los certificados emitidos al Titular;
- Se responsabiliza por mantener informados a los Representantes sobre el estado de los certificados que han solicitado;
- Garantizar 24x7 el acceso al repositorio de certificados digitales emitidos, la disponibilidad de los canales de validación de estos usando CRL y el protocolo OCSP;
- Informar a los Titulares sobre usos permitidos, limitantes, responsabilidades, recomendaciones de seguridad y software para firma digital;
- Proteger la información personal e institucional de los Titulares de certificados;
- Proteger los activos que conforman el PSCC;
- Notificar a todos los que utilizan el Servicio de Llave Pública proporcionado por la AC ETECSA, de la ocurrencia de afectaciones del este, por los motivos que sean, orientarlos sobre buenas prácticas o de la actualización de los modos de operación de la Autoridad;

- No divulgar información personal o institucional de los solicitantes con los que trabaja;

De la Entidad de Registro

- La Entidad de Registro se encarga a través de sus funcionarios de revisar los datos contenidos en cada solicitud de certificado y, si estuviesen correctos, aprobarlas;
- Realizar el proceso de solicitud de certificados digitales si tuviese la responsabilidad de Representar a una persona natural;
- Recoger, guardar y custodiar los datos documentales solicitados a los Representantes y mantener con ellos estrecho seguimiento de las operaciones sobre sus certificados;
- Exigir a los Representantes y Usuarios sobre la entrega oportuna de cualquier documentación requerida para el correcto uso del Servicio;
- No divulgar información personal o institucional de los solicitantes con los que trabaja.

De los Representantes

- El Representante de una Unidad Organizativa es el responsable de validar los datos del solicitante utilizando para ello el C.I de este;
- Insertar correctamente en la PGCD los datos del solicitante de un certificado digital;
- No divulgar información personal o institucional de los solicitantes con los que trabaja;
- Informar a la ER correspondiente sobre la ocurrencia de eventualidades con sus certificados.

De los Titulares

- Es el único responsable de la custodia del certificado digital que se le ha emitido;
- Notificar a su Representante o a la ER correspondiente sobre alguna eventualidad con su certificado;
- Está en la obligación de utilizar los certificados según se establece en esta política.

De los Terceros de buena fe

- Estos usuarios deben chequear la validez de cada firma contenida en los documentos digitales que manipulen;
- Deben considerar un documento como "*no confiable*" y no procesar su contenido una vez compruebe, a través de la aplicación de lectura del mismo, que ha sido modificado o sus firmas son inválidas;
- Puede constatar directamente a través de los repositorios de certificados en línea provistos por otras autoridades, y preferiblemente por la AC ETECSA, el estado de determinado certificado, si la comprobación habitual ha fallado;
- Está en la obligación de comunicar a la AC ETECSA, usando los canales de soporte habilitados por esta, la ocurrencia de eventualidades con sus certificados.

De la Privacidad y Protección de los datos

- Los datos personales e institucionales recogidos en la PGCD referentes a sus usuarios, deben ser verificados e insertados -por ese orden- por los funcionarios de la AC ETECSA, a partir de la información proporcionada por el propio titular de estos o usando bases de datos que los almacenan;

- Los datos insertados en la PGCD deben ser veraces, exactos y correctos; y se almacenan y protegen por un periodo de 15 años;
- Los datos suministrados por los Titulares tienen como finalidad reconocer a la persona natural o jurídica a través de un certificado digital que lo haya solicitado, para su utilización a título personal o empresarial, evitando acciones fraudulentas como la suplantación de identidad;
- La llave privada correspondiente a cada Titular está protegida por una frase con estructura robusta y una longitud mínima de 2048 bits;
- Cada Titular, como único responsable de los certificados que se le soliciten a su nombre, no puede compartir con terceros ni su llave privada ni la clave que lo protege;
- Para la verificación del estado de un certificado digital, la AC ETECSA comparte con Terceros de buena fe, con otros PSCC y con sus Titulares, la Lista de Certificados Revocados (CRL) y una validación en línea usando protocolo OCSP (con un canal por HTTP).

De la suspensión y revocación de un certificado

- La revocación de un certificado digital se debe realizar inmediatamente que se detecte que se cumple al menos una de las condiciones listadas en el artículo 32, Res 2/16 emitida por el MININT;
- Las solicitudes de Revocación son manejadas a través de la PGCD y pueden ser solicitadas por el Titular del certificado digital o por su Representante;
- El solicitante debe especificar el motivo que respalda la revocación para poder insertarla con tal efecto en la PGCD. Si el motivo no se especifica, no procederá la solicitud de revocación del certificado y permanecerá como “*Emitido”*, y en tal caso, constituye una irresponsabilidad;
- La PGCD notificará al correo del Representante y del propio Titular sobre la revocación efectuada.