ALCANCE

Este documento declara las Políticas de Certificación de 5B, los cuales dan cumplimiento a los requisitos establecidos en el Decreto 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, su reglamento, así como las normas técnicas que establece el Registro de Prestadores de Servicios de Certificación.

DESCRIPCIÓN DE LA POLÍTICA

Características de los Certificados

5N ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones de la siguiente forma:

Número OID	Políticas de certificados
1.3.6.1.4.1.51963.1.1.1	*Persona Natural*
1.3.6.1.4.1.51963.1.1.2	*Personal Natural Representante*
1.3.6.1.4.1.51963.1.2.1	*Persona Jurídica*

1.1. Participantes en los servicios de certificación

1.1.1. Prestador de Sercicios de Certificación

El prestador de servicios de certificación es la persona jurídica, que expide y gestiona certificados para entidades finales, empleando una Autoridad de Certificación, o presta otros servicios relacionados con la firma electrónica.

5B es un prestador de servicios de certificación que actúa de conformidad con las previsiones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, su reglamento, así como las normas técnicas que establece el Registro de Prestadores de Servicios de Certificación aplicables a la expedición y gestión de certificados de firma electrónica avanzada, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

1.1.2. Autoridad de Registro

Una Autoridad de Registro (RA) es la entidad encargada de:

- Tramitar las solicitudes de certificados.

- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado.
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

1.1.3. Entidades finales

Las entidades finales son las personas naturales destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.

Serán entidades finales de los servicios de certificación de 5B las siguientes:

1. Suscriptores del servicio de certificación
2. Firmantes
3. Partes usuarias

1.1.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las personas naturales que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.
- Las empresas, entidades, corporaciones u organizaciones que los adquieren a 5B (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados en el campo de organización.

1.1.3.2. Firmantes

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica avanzada. En el caso de que el suscriptor sea una persona natural conforme al apartado anterior, el suscriptor y firmante coincidirán en el mismo sujeto.

En los casos de certificados de este perfil cuyo suscriptor identificado sea una persona jurídica conforme al apartado 1.4.3.1. los firmantes serán personas naturales con una vinculación al suscriptor, pudiendo típicamente ser empleados, agentes, miembros vinculados como colegiados

profesionales o representante legales; incluyendo las personas al servicio de las Administraciones Públicas.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación inequívoco, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el prestador de servicios de certificación, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deben considerar las implicaciones de perder los medios exclusivos de su control.

1.1.3.3. Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta política de certificación y en la declaración de prácticas de certificación de 5B disponibles en https://www.5b.com.gt/identidad-digital.php

1.1.3.4. Tercero que confía

El tercero que confía incluye a todas aquellas personas naturales y/o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por 5B como Prestador de Servicios de Certificación. El tercero que confía puede ser suscriptor o no de un certificado.

Los terceros que confían en estos certificados deben estar en conocimiento de las limitaciones en su uso, tanto cuantitativas como cualitativas, de acuerdo a la Declaración de Prácticas de Certificación y estas Políticas.

1.2. Usos y Limitaciones

Esta sección lista las aplicaciones para las que puede emplearse el certificado, y establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.2.1. Período de Validez de los Certificados

El periodo de validez será el que se indique en el propio certificado, con un máximo de 3 años.

1.2.2. Usos permitidos para los certificados

1.2.2.1. Certificados de Persona Natural

Este certificado dispone del OID 1.3.6.1.4.1.51963.1.1.1. Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo a las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Este certificado garantiza la identidad del firmante y su vinculación con el suscriptor (si fuese distinto) del servicio de certificación, y permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo "key usage" tiene activadas y por tanto permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación).
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
c) Key Encipherment.

1.2.2.2. Certificados de Persona Natural Representante

Este certificado dispone del OID 1.3.6.1.4.1.51963.1.1.2. Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo a las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

El uso de este certificado garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y la entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

d) Autenticación en sistemas de control de acceso.
e) Firma de correo electrónico seguro.
f) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo "key usage" tiene activadas y por tanto permite realizar, las siguientes funciones:

d) Firma digital (Digital Signature, para realizar la función de autenticación).
e) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
f) Key Encipherment.

1.2.2.3. Certificados de Persona Natural Representante

Este certificado dispone del OID 1.3.6.1.4.1.51963.1.2.1. Es un certificado que se emite para la autenticación y la firma electrónica avanzada de una persona jurídica, de acuerdo a las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Estos certificados garantizan la identidad de la entidad, empresa u organización suscriptora identificada en el certificado, y en su caso la del responsable de gestionar el certificado (si se hubiese identificado). Este certificado permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante (entidad, empresa u organización) de manera única, permitiendo su identificación y ha sido generada utilizando medios que puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

g) Autenticación en sistemas de control de acceso.
h) Firma de correo electrónico seguro.
i) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo "key usage" tiene activadas y por tanto permite realizar, las siguientes funciones:

g) Firma digital (Digital Signature, para realizar la función de autenticación).
h) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica avanzada).
i) Key Encipherment.

1.2.3. Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades. Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable.

Los certificados no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, ni se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o

comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web de 5B.

El empleo de los certificados digitales en operaciones que contravienen esta Políticas de Certificación, la Declaración de Prácticas de Certificación de 5B, los documentos jurídicos vinculantes con cada certificado, o los contratos con las Autoridades de Registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a 5B, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

5B no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de 5B emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en estas Políticas de Certificación, en la Declaración de Prácticas de Certificación de 5B, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las autoridades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

2. Identificación y autenticación

2.1. Registro inicial

2.1.1. Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN o *distinguished name*) conforme al estándar X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona natural identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

2.1.1.1. Certificado de Persona Natural

Los nombres contenidos en los certificados de Personal Natural son los siguientes:

Organization (O)	Empresa, Entidad, Organización, Colegio u asociación profesional a la que está vinculado el firmante (si la hubiese)
Organization Unit (OU)	Unidad de la Organización a la que está vinculado el firmante, si se tratase de un profesional colegiado se especificará "Colegiado" (si la hubiese)
Organization Identifier	NIT de la Organización a la que está vinculado el firmante (si la hubiese)
Title	Cargo o especialidad de firmante (si la hubiese)
Surname	Apellido(s) del firmante
Given Name	Nombre(s) del firmante
Serial Number	DPI/Pasaporte/u otro número de identificación idóneo del firmante, reconocido en derecho
Common Name (CN)	Nombre(s) y apellido(s) del firmante

2.1.1.2. Certificado de Personal Natural Representante

Country (C)	Estado[1]
Organization (O)	Organización suscriptora que representa el firmante

[1] El campo "Estado" corresponderá Estado donde la persona jurídica suscriptora se encuentra registrada.

Organization Unit (OU)	Unidad de la Organización suscriptora a la que está vinculado el firmante
Organization Identifier	Número de identificación fiscal de la Organización suscriptora a la que representa el firmante
Title	Representante Legal – Cargo del firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número del Documento de Identidad utilizado para la identificación del firmante.
Common Name (CN)	Nombres y apellidos del representante, su número de identificación y el identificador fiscal de la persona jurídica.

2.1.1.3. Certificado de Persona Jurídica

Country (C)	Estado donde la entidad está registrada la Organización
Organization (O)	Nombre de la Organización
Organization Unit (OU)	Indica la naturaleza del certificado
Organization Identifier	Número de identificación fiscal de la Organización a la que está vinculado el certificado
Surname	Apellidos del responsable de la gestión certificado (si se hubiese identificado alguno)
Given Name	Nombre del responsable de la gestión del certificado (si se hubiese identificado alguno)
Serial Number	Número de identificación fiscal de la Organización a la que está vinculado el certificado electrónico
Common Name (CN)	Nombre descriptivo de subscriptor del certificado, que puede incluir el nombre de un departamento o unidad del suscriptor, o el proceso al que estará dedicado.

2.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

2.1.2.1. Emisión de certificados del set de pruebas y certificados de pruebas en general

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. “Test Organization”, “Test Nombre”, “Apellido1”) o se indique expresamente palabras que denoten su invalidez (ej. “TEST”, “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre UANATACA. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y/o permitir al ente regulador su evaluación.

2.1.3. Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Asimismo, en ningún caso se emiten certificados anónimos.

2.1.4. Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” o “estado” será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una persona natural, con independencia de la nacionalidad de la persona natural.

En el campo “número de serie” se incluye el DNI, Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

2.2. Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre 5B y el suscriptor, momento en el que se verifica la existencia del suscriptor mediante su documento oficial de identidad o las escrituras correspondientes según sea el caso, al igual que los poderes de actuación de la persona que presente como representante de una organización si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante la presentación de su documento oficial de

identificación o mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. En este último caso, el suscriptor producirá una certificación de los datos necesarios, y la remitirá a 5B, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

2.2.1. Autenticación de la identidad de una organización, empresa o entidad mediante representante

Las personas naturales con capacidad de actuar en nombre de las personas jurídicas u organizaciones suscriptoras en general, podrán actuar como representantes de las mismas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona natural y la organización de la que se trate, que exige su reconocimiento por 5B, sus autoridades de registro y/o terceros vinculados, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor se identificará ante un operador o persona autorizada por una Autoridad de Registro de 5B, acreditando el carácter y facultades que alegue poseer. Alternativamente, a los mismos efectos 5B podrá poner a disposición de los suscriptores un formulario para su cumplimentación previa.

2. El representante de la organización proporcionará la siguiente información y sus correspondientes soportes acreditativos:
    - Sus datos de identificación, como representante:
        - Nombre y apellidos
        - Lugar y fecha de nacimiento
        - Documento de identidad idóneo reconocido en derecho para la identificación del representante
    - Los datos de identificación del suscriptor al que representa:
    - Denominación o razón social.
        - Información de registro existente, que puede incluir los datos relativos a la constitución, personalidad jurídica, extensión y vigencia de las facultades de representación del solicitante.
        - Documento: documento acreditativo de la identificación fiscal de la organización suscriptora.
        - Documento: Documentos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de

constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

- Los datos relativos a la representación o la capacidad de actuación que ostenta:
  - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin) si resulta aplicable.
  - El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación.

3. El operador o personal autorizado de la Autoridad de Registro de 5B comprobará la identidad del representante mediante la presentación de su documento de identidad u otro medio idóneo reconocido en derecho para su identificación, así como el contenido de la representación con la documentación.

4. El operador o personal autorizado de la Autoridad de Registro de 5B verificará la información suministrada para la autenticación y le devolverá la documentación original aportada.

5. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador o personal autorizado de la Autoridad de Registro 5B, en cuyo caso los pasos 3 y 4 anteriores no serán precisos.

La prestación del servicio de certificación se formaliza mediante el oportuno contrato entre 5B y el suscriptor, debidamente representado.

2.2.2. Autenticación de la identidad de una persona natural

Esta sección describe los métodos de comprobación de la identidad de una persona natural identificada en un certificado.

2.2.2.1. En los certificados

La identidad de las personas naturales firmantes identificados en los certificados, se valida mediante la presentación de su documento oficial de identificación (Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación).

La información de identificación de las personas naturales identificadas en los certificados cuyo suscriptor sea una entidad pública o privada, con o sin personalidad jurídica, la información podrá ser validada comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, o bien con la documentación

que esta haya suministrado sobre la persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

2.2.2.2. Validación de la Identidad

Para la solicitud de certificados, el operador o personal autorizado de la Autoridad de Registro 5B valida la identidad del solicitante, para lo cual la persona natural deberá exhibir documento de identidad (DPI, documento de identidad de extranjeros, Pasaporte u otro medio idóneo reconocido en derecho para su identificación).

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica los mismos pueden ser tramitados cuando medie un documento idóneo para la verificación de los extremos establecidos en esta declaración de prácticas de certificación. Sin embargo, la entrega del certificado o de las respectivas credenciales de generación y acceso deben deberán realizarse a persona autorizada del suscriptor, con la correspondiente verificación de su identidad.

2.2.2.3. Vinculación de la persona natural

La justificación documental de la vinculación de una persona natural identificada en un certificado con la entidad, empresa y organización de derecho público o privado será producida por la entidad suscriptora.

2.3. Identificación y autenticación de solicitudes de renovación

2.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro de 5B comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona naturales identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- El uso del código “CRE” o “ERC” relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona natural identificada en el certificado, y que le permite renovar de forma automática su certificado.
- El empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa.

2.4. Identificación y autenticación de la solicitud de revocación, suspensión o reactivación

5B o un operador o personal autorizado de la Autoridad de Registro autentica las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación, suspensión o reactivación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:
    - Identificándose y autenticándose mediante el uso del Código de Revocación (CRE o ERC) a través de la página web de 5B en horario 24x7.
    - Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de 5B y/o Autoridades de Registro.
- Las autoridades de registro de 5B deberán identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado podrá ser pasado a estado de suspensión.

3. Requisitos de operación del ciclo de vida de los certificados

3.1. Solicitud de emisión de certificado

3.1.1. Legitimación para solicitar la emisión

La emisión de un certificado puede ser solicitada por el suscriptor o el firmante en cada caso, cumpliendo los requisitos previstos en esta Política de Seguridad y la Declaración de Prácticas de Certificación de 5B.

3.1.2. Procedimiento de alta y responsabilidades

5B gestiona las altas de las solicitudes de certificados basado en la información proporcionada por el suscriptor al momento de la solicitud. El suscriptor es responsable de la veracidad de esta documentación en los términos en esta Política de Seguridad y la Declaración de Prácticas de Certificación de 5B.

3.2. Procesamiento de la solicitud de certificación

3.2.1. Ejecución de las funciones de identificación y autenticación

5B se asegura antes de emitir un certificado que la solicitud cumpla con los requisitos previstos en esta Política de Seguridad y la Declaración de Prácticas de Certificación de 5B. Las evidencias recogidas en el proceso son resguardadas por 5B por el tiempo legal correspondiente.

3.2.2. Aprobación o rechazo de la solicitud

En caso que los datos se verifiquen correctamente, 5B aprueba la solicitud del certificado y proceder a su emisión y entrega.

3.3. Emisión del certificado

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, 5B:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo el propio Prestador de Servicios de Certificación o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

3.4. Entrega y aceptación del certificado

La aceptación del certificado por la persona natural identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

3.5. Uso del par de claves y del certificado

3.5.1. Uso por el firmante

Los firmantes se obligan a:

- Facilitar a 5B información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en las políticas y prácticas de certificación de 5B.
- Reconocer la capacidad de producción de firmas electrónicas avanzadas mediante el certificado emitido por 5B; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.

- Ser especialmente diligente en la custodia de su clave privada y/o las credenciales de acceso a la misma, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en esta Declaración de Prácticas de Certificación.
- Comunicar a 5B, Autoridades de Registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

Los firmantes se responsabilizan de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

3.5.2. Uso por el suscriptor

3.5.2.1. Obligaciones del suscriptor del certificado

5B obliga contractualmente al suscriptor a:

- Facilitar al Prestador de Servicios de Certificación información completa y adecuada, conforme a los requisitos de esta Política de Certificación y la Declaración de Prácticas de Certificación de 5B, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la utilización de un certificado.
- Emplear el certificado de acuerdo con lo establecido en las políticas y prácticas de certificación de 5B en su condición de Prestador de Servicios de Certificación.

- Comunicar a 5B, Autoridades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas naturales identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de 5B, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de 5B.

3.5.2.2. Responsabilidad civil del suscriptor de certificado

El suscriptor de un certificado a responsable de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

3.5.3. Uso por el tercero que confía en certificados

3.5.3.1. Obligaciones del tercero que confía en certificados

5B informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma electrónica o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas basadas en certificados emitidos por 5B como Prestador de Servicios de Certificación debidamente autorizado para operar como tal por el Registro de Prestadores de Servicios de Certificación, tienen la consideración legal de firmas electrónicas avanzadas; esto es, equivalentes a firmas manuscritas.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de 5B, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la 5B.

3.5.3.2. Responsabilidad civil del tercero que confía en certificados

5B informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

3.6. Revocación, suspensión o reactivación de certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

3.6.1. Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación un certificado puede solicitarlo directamente a 5B o a la Autoridad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web de 5B. La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación, suspensión o reactivación.
- Identidad del suscriptor/firmante.
- Nombre y título de la persona (si aplica) que pide la revocación, suspensión o reactivación.
- Información de contacto de la persona que pide la revocación, suspensión o reactivación.
- Razón para la petición de revocación.

La solicitud debe ser autenticada, por 5B, de acuerdo con los requisitos establecidos en la sección 2.4 de esta política, antes de proceder a la revocación, suspensión o reactivación.

El servicio de revocación, suspensión o reactivación se encuentra en la página web de 5B: https://www.5b.com.gt/identidad-digital.php

En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una persona natural identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a 5B o la correspondiente Autoridad de Registro.

La solicitud de revocación, suspensión o reactivación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona natural identificada en el certificado, acerca del cambio de estado del certificado.

Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de 5B.

3.6.2. Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por el Prestador de Servicios de Certificación 5B.

Las Listas de Revocación de Certificados se publican en el Depósito de la Autoridad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.uanataca.com/public/pki/crl/transacciones-y-transferencias-ca1.crl
- http://crl2.uanataca.com/public/pki/crl/transacciones-y-transferencias-ca1.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

3.6.3. Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

4. Perfiles de certificados y listas de certificados revocados

4.1. Perfil de certificado

Todos los certificados emitidos bajo esta declaración de prácticas de certificación cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.

4.1.1. Número de versión

UANATACA emite certificados X.509 Versión 3.

4.1.2. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

4.2. Perfil de la lista de revocación de certificados

4.2.1. Número de versión

Las CRL emitidas por 5B son de la versión 2.

4.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

RESPONSABLE DE LA ADMINISTRACIÓN

Este documento es administrado por el Oficial de Seguridad de la Información

RESPONSABLE DEL CUMPLIMIENTO

Todo el personal involucrado en el proceso, tanto personal interno y externo debe cumplir con lo establecido en el presente documento

SANCIÓN

N/A

5. Anexo I.- Definiciones y acrónimos

AAC	Autoridad Administrativa Competente
AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
CP	Certificate Policy. Políticas de Certificación
CPD	Centro de Procesacimiento de Datos.
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DCCF	Dispositivo Cualificado de Creación de Firma
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
EC	Entidad de certificación
ER	Entidad de Registro o Verificación
ERC	Código de Revocación
FIPS	Federal Information Processing Standard Publication
HSM	Hardware Security Module. Módulo de Seguridad Hardware
IOFE	Infraestructura Oficial de Firma Electrónica
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
LRC	Listas de revocación de certificados
NTP	Network Time Protocol (NTP
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PDS	Policy Disclosure Statements. Textos de divulgación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de llave pública
QSCD	Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
RA	Autoridad de Registro
ROA	Real Instituto y Observatorio de la Armada
RPS	Declaración de prácticas de registro o verificación
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
RUC	Registro Único de Contribuyentes
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol