スペイン語版

Servicio Público para la Identificación

Personal por entidades públicas locales

Autoridad certificadora de la prefectura de Hokkaido Normas operativas

Ver.1.5

8 de julio de 2013

Prefectura de Hokkaido

Historial de modificaciones

Ver	Fecha	Detalles de revisión
1.0	29 de enero de 2004	Emisión de la 1ª edición
1.1	19 de enero de 2005	Revisión por modificaciones en las reglas de ejecución
1.2	1 de noviembre de 2006	Revisión por modificación de la ley
1.3	19 de septiembre de 2008	Revisión por actualización de la clave secreta de la autoridad certificadora
1.4	1 de abril de 2009	Revisión por cambio en la dirección de contacto
1.5	8 de julio de 2013	Revisión por ejecución de una ley (apartado 77 de la ley de 2009) que modifica parcialmente la Ley de Registro Básico de Residentes

1. Introducción

Estas normas operativas especifican las políticas de administración referentes al servicio de certificación en las autoridades certificadoras de cada prefectura (en adelante, referido como "CA de la prefectura de Hokkaido") para el Servicio Público para la Identificación Personal, las cuales se encargarán de expedir certificados digitales (los certificados de los usuarios quedarán denominados como "certificados digitales") para aquellas personas inscritas en el registro básico de residentes y con el objetivo de realizar la digitalización de los procedimientos de solicitudes y notificaciones de documentos entre los residentes y el gobierno central o las entidades públicas locales.

La estructura de estas normas operativas queda basada en la *RFC (Request For Comments) 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" del PKIX (Public-Key Infrastructure X.509) Grupo de Trabajo de la IETF (Internet Engineering Task Force)*. Sin embargo, para aquellas partes que se refieran a otras normas quedará indicado solo el título y los detalles de las mismas.

1-1 Sumario

La CA de la prefectura de Hokkaido expedirá los certificados digitales a aquellas personas inscritas en el registro básico de residentes según se soliciten. Mientras que expide los certificados necesarios para la operación de CA de la prefectura, expedirá e intercambiará certificados de identificación recíproca con las autoridades de certificación “Bridge” del Servicio Público para la Certificación Personal (en adelante, referida como "BCA de identificación personal") instaladas para la identificación recíproca con autoridades certificadoras de cada prefectura encargadas de dar otro Servicio Público para la Identificación Personal y con autoridades certificadoras de base gubernamental. Además se crearán la información de extinción de datos (datos de certificados digitales extinguidos y debajo denominados de la misma manera), los registros de extinción de datos (CRL/ARL) (registros de datos de certificados digitales extinguidos y debajo denominados de la misma manera) y los archivos de información de extinción de datos (archivos de registros de extinción de datos (CRL) y debajo denominados de la misma manera). También se hará entrega de los mismos según los solicite el verificador de firmas determinado en el párrafo 4 del artículo 17 o el verificador de firmas grupales determinado en el párrafo 6 del mismo artículo de la " ley acerca del servicio de certificación de las entidades públicas locales implicadas mediante firma digital" (debajo denominada "Ley Fundamental").

Además, la CA de la prefectura de Hokkaido tendrá estas normas operativas como sus políticas de administración para el servicio de certificación y no considerará la CP (política de certificados) y la CPS (normas de ejecución de identificación) como regulaciones independientes.

1-2 Diferenciación

Los elementos de diferenciación para la política de certificados de la CA de la prefectura de Hokkaido serán los siguientes.

Política de certificados digitales de la CA de la prefectura de Hokkaido

Política de certificados digitales y política de certificados de identificación recíproca de la CA de la prefectura de Hokkaido

1.2.392.200149.8.5.1.1.10

Política de certificados digitales de prueba y política de certificados de identificación recíproca de la CA de la prefectura de Hokkaido

1.2.392.200149.8.5.1.0.10

Política de certificados de servidor para verificación de certificados digitales emitidos por el gobierno central

1.2.392.200149.8.5.1.200

Política de certificados de servidor para verificación de certificados digitales emitidos por el gobierno centralde prueba

1.2.392.200149.8.5.1.0.200

Política de certificados de OCSP responder

1.2.392.200149.8.5.1.300

Política de certificados de OCSP responder de prueba

1.2.392.200149.8.5.1.0.300

1-3 Sistema de uso y límites en la aplicación de certificados

1-3-1 Personas y entidades involucradas

(1) Ministro de Asuntos Internos y Comunicaciones

El Ministro de Asuntos Internos y Comunicaciones designará los organismos de certificación designados según lo establecido en la Ley Fundamental.

(2) Asociación de Prefecturas para el JPKI

La Asociación de Prefecturas para el JPKI (debajo denominada como "Asociación") efectuará trabajos administrativos relacionados con la comunicación y el ajuste de asuntos de importancia para hacer posible una administración unificada del Servicio Público para la Identificación Personal.

(3) Gobernador de la prefectura de Hokkaido

El gobernador de la prefectura de Hokkaido contará con las funciones de la CA de la prefectura de Hokkaido (autoridad certificadora de la prefectura de Hokkaido) debajo indicadas.

(4) CA de la prefectura de Hokkaido

La CA de la prefectura de Hokkaido colaborará de manera mutua con los municipios expidiendo certificados digitales y otros certificados, creando registros de invalidación (CRL/ARL) a la vez que emite certificados digitales y efectúa labores de administración de información de extinción de datos para proveer de medios para la comprobación de la validez de los certificados digitales. Se encargará de solucionar incidencias en caso de que las claves secretas del gobernador de la prefectura de Hokkaido corran algún peligro o en situaciones de emergencia causadas por desastres o accidentes.

Además, proveerá a los usuarios de los medios para comprobar la validez de los certificados digitales emitidos por el gobierno central y por las entidades públicas locales requeridos para la verificación de firmas digitales de documentos recibidos por el usuario a través del gobierno central del país o las entidades públicas locales por Internet.

(5) BCA de identificación personal

La BCA de identificación personal efectuará la expedición de certificados para las autoridades certificadoras de cada prefectura y las autoridades certificadoras Bridge de base gubernamental (debajo denominada "BCA de identificación de base gubernamental") de la CA de la prefectura de Hokkaido siguiendo las normas operativas determinadas por la Asociación.

(6) Organismo de certificación designado

Los organismos de certificación designados y según lo establecido en la Ley Fundamental, recibirán la orden del gobernador de la prefectura de Hokkaido para efectuar labores administrativas relacionadas con el servicio de certificación (debajo denominadas "labores administrativas de identificación").

(7) Municipios

Los municipios de la prefectura de Hokkaido recibirán las solicitudes de expedición de certificados digitales y las solicitudes de invalidación, comprobarán la identidad del solicitante y efectuarán la entrega al solicitante de los certificados digitales expedidos por la CA de la prefectura de Hokkaido.

(8) Solicitantes/usuarios

Los solicitantes, según lo determinado en el párrafo 1 del artículo 3 de la Ley Fundamental, son aquellas personas que solicitan la expedición de un certificado digital (también podrá efectuar la solicitud un represente legal. Aunque en este caso se deberán cumplir con los requisitos del artículo 5 de las "Normas de ejecución de la Ley acerca del servicio de certificación de las entidades públicas locales implicadas mediante firma digital" (debajo denominadas "Normas de la Ley Fundamental"). Los usuarios son aquellas personas registradas en el registro básico de residentes y que son receptores del certificado digital.

Los usuarios podrán utilizar los certificados digitales en las solicitudes y notificaciones por Internet con el gobierno central o las entidades públicas locales. Podrán exigir que se les muestren aquellos datos relacionados con el servicio de certificación (registros de expedición de certificados digitales, información de invalidación y archivos de información de invalidación, debajo denominados de la misma forma) que tengan que ver con uno mismo al gobernador de la prefectura de Hokkaido o a los organismos de certificación designados y podrán exigir la modificación total o parcial, así como la nueva adicción o su eliminación, de los datos del servicio de certificación mostrados. Además, en caso de tener alguna queja contra dichas labores administrativas de identificación, se podrá exigir un arbitraje al Ministro de Asuntos Internos y Comunicaciones, según queda determinado en la Ley de Arbitraje de Quejas Administrativas. Además, comprobará la validez de los certificados digitales emitidos por el gobierno central y por las entidades públicas locales requeridos para la verificación de firmas digitales de documentos recibidos a través del gobierno central o las entidades públicas locales por Internet.

(9) Verificador de firmas

Se refiere a cualquiera de las siguientes personas o entidades que, en base al párrafo 1 del artículo 17 de la Ley Fundamental para recibir los medios para comprobar la validez de los certificados digitales, ha solicitado por anticipado y recibe los permisos de acceso.

①Organismos administrativos determinados en el apartado 2 del artículo 2 de la Ley relacionada con el Uso de Tecnología de Comunicaciones en procedimientos administrativos (debajo denominados "organismos administrativos").

②Juzgados

③Personas designadas, registradas, certificadas o aprobadas por la agencia administrativa en base a la ley para encargarse de recibir datos de forma electromagnética para su posterior entrega a los organismos administrativos o bien para responder a consultas de información según se requiera para efectuar solicitudes, notificaciones u otros procedimientos en los organismos administrativos.

④ Empresas de identificación certificadas según se determina en el artículo 8 de la "Ley relacionada con las Firmas Digitales y el Servicio de Certificación" (debajo denominada "Ley de Firmas Digitales").

⑤Personas que efectúan labores determinadas de identificación según se determina en el

párrafo 3 del artículo 2 de la Ley de Firmas Digitales y certificadas por el Ministro de Asuntos Internos y Comunicaciones como aptas según los estándares determinados en el "Decreto de Ley para la Ejecución de la Ley acerca del servicio de certificación de las entidades públicas locales implicadas mediante firma digital" (debajo denominado "Decreto de Ley para la Ley Fundamental").

⑥ Entidades determinadas por el Decreto de Ley para la Ley Fundamental proveedoras de los registros electromagnéticos necesarios para efectuar solicitudes, notificaciones u otros procedimientos con organismos administrativos y juzgados.

Recibirán de la CA de la prefectura de Hokkaido los registros de invalidación (CRL/ARL) a través de Internet.

(10) Examinador de firmas

Se refiere a aquellas personas determinadas por el decreto de ley de la Ley Fundamental determinado en el párrafo 5 del artículo 17 de la Ley Fundamental.

Recibirán de los verificadores de firmas grupales debajo determinados los resultados de comprobación de validez de los certificados digitales y verificarán las firmas digitales de las solicitudes y notificaciones hechas por los usuarios a través de Internet.

(11) Verificador de firmas grupales

Se refiere a cualquiera de las siguientes personas o entidades que, en base al párrafo 5 del artículo 17 de la Ley Fundamental para recibir los medios para comprobar la validez de los certificados digitales, ha solicitado por anticipado y recibe los permisos de acceso.

① Entidades determinadas según el Decreto de Ley para la Ley Fundamental a las que pertenece una persona que, en base a lo que determina la ley, recibe el encargo de otra persona para efectuar en su nombre solicitudes, notificaciones u otros procedimientos con organismos administrativos y juzgados.

② Entidades u organismos determinados por el Decreto de Ley para la Ley Fundamental a las que pertenece una persona proveedora de los registros electromagnéticos necesarios para efectuar solicitudes, notificaciones u otros procedimientos con organismos administrativos y juzgados.

Recibirán de la CA de la prefectura de Hokkaido los registros de invalidación (CRL/ARL) y los medios para comprobar la validez de los certificados digitales, comprobarán la validez de los certificados digitales adjuntos a las solicitudes y notificaciones de usuarios a través de Internet y que han recibido por parte del examinador de firmas y comunicarán los resultados al examinador de firmas.

(12) Verificadores de firmas

Se refiere a los verificadores de firmas y a los verificadores de firmas grupales.

1-3-2 Aplicación y condiciones de aplicación

Existen los siguientes 4 casos en los que se podrá utilizar este servicio.

① Expedición de certificados digitales para los siguientes casos.

- Firmas digitales relacionadas con solicitudes y notificaciones a través de Internet en organismos administrativos y juzgados.
- Comprobación de la identidad a efectuar por el verificador de firmas
- Comprobación de la identidad a efectuar por el examinador de firmas

El periodo de validez de los certificados digitales será de 3 años a partir del día de su expedición.

② Expedición de certificados de identificación recíproca para los siguientes casos.

- Identificaciones recíprocas con el BCA de identificación de base gubernamental y que pasen

a través del BCA de identificación personal.
El periodo de validez de los certificados de identificación recíproca será de 5 años a partir del día en el que se validan.

③ Expedición de certificados de servidor para verificación de certificados digitales emitidos por el gobierno central para los siguientes casos.

・Proveer de medios para comprobar la validez de los certificados digitales emitidos por el gobierno central y por las entidades públicas locales requeridos para la verificación de firmas digitales de documentos recibidos por el usuario a través del gobierno central o las entidades públicas locales por Internet.
El periodo de validez de los certificados de servidor para verificación de certificados digitales emitidos por el gobierno central será de 1 año a partir del día en el que se validan.

④ Expedición de certificados de OCSP responder para los siguientes casos.

・Proveer de medios al verificador de firmas para comprobar la validez de los certificados digitales de sistema de consulta OCSP responder.
Además, el periodo de validez de los certificados de OCSP responder será de 1 año a partir del día en el que se validan.

1-3-3 Responsables de las normas operativas

El responsable de estas normas operativas es el gobernador de la prefectura de Hokkaido

1-3-4 Dirección de contacto

Debajo queda indicada la ventanilla para consultas relacionadas con estas normas operativas.

Prefectura de Hokkaido
Dirección: Kita 3-jo, Nishi 6-chome, Chuo-ku, Sapporo 060-8588
Departamento:Departamento de política general El científico IT Escritorio de la Promoción
Sección de política de información
Horario de atención: de 8:45 de la mañana a 5:30 de la tarde
Teléfono:011-204-5171
Fax: 011-232-3962
Dirección de correo electrónico: sogo.joho2@pref.hokkaido.lg.jp

2. Reglas generales

2-1 Obligaciones

2-1-1 Obligaciones del Ministro de Asuntos Internos y Comunicaciones

(1) Designar a los organismos de certificación designados, autorizar aboliciones y suspensiones, revocar designaciones, emitir avisos y anuncios al gobernador de la prefectura de Hokkaido

(2) Emisión de órdenes a organismos de certificación designados según se requiera

(3) Demanda de aquellos informes necesarios a los organismos de certificación designados y ejecución de inspecciones oficiales

(4) Nombramientos así como autorizaciones y ordenes de destitución de ejecutivos en los organismos de certificación designados

(5) Autorizaciones y órdenes de modificación de las normas de administración de labores administrativas de identificación y planes empresariales determinados por los organismos de certificación designados

(6) Responder a alegaciones de disconformidad relacionadas con sanciones interpuestas por organismos de certificación designados

(7) Determinación de los estándares técnicos de las infraestructuras usadas en el servicio de certificación

(8) Investigación y estudio de las evaluaciones técnicas del servicio de certificación

(9) Labores administrativas relacionadas con la certificación de verificadores de firmas

(10)Demanda de aquellos informes necesarios sobre el estado de ejecución de las labores de trabajo a los verificadores de firmas

(11) Avisos y anuncios públicos a los usuarios sobre datos relacionados con el Servicio Público para la Identificación Personal

2-1-2 Obligaciones del gobernador de la prefectura de Hokkaido

(1) Expedición de certificados digitales a los municipios con el nombre, fecha de nacimiento, sexo y dirección (debajo denominados "Cuatro informaciones fundamentales" (en caso de que el solicitante sea un residente extranjero y tenga un nombre apelativo escrito en su certificado de residencia, se incluirán las cuatro informaciones fundamentales y el nombre apelativo. Debajo se denominará a estos datos de la misma forma)) de los solicitantes y según los avisos de clave pública.

(2) Muestra de información precisa relacionada con la identificación recíproca e intercambio de certificados de identificación recíproca entre la CA de la prefectura de Hokkaido y la BCA de identificación personal

(3) Expedición de certificados de firma propia

(4) Expedición de certificados Link

(5) Expedición de certificados relacionados con el uso del servicio

(6) Comprobación de identidad y creación de información de invalidación en el caso de recibir solicitudes de invalidación de usuarios a través de Internet

(7) Creación de información de invalidación en el caso de recibir solicitudes de invalidación de usuarios en la ventanilla de los municipios

(8) Creación de información de invalidación en caso de haber habido un cambio en la dirección o el nombre del usuario o al haber fallecido este

(9) Creación de información de invalidación en caso de encontrarse errores en los datos registrados en los certificados digitales de usuarios

(10) Creación de información de invalidación de todos los certificados expedidos con la clave secreta del gobernador de la prefectura de Hokkaido e informe al BCA de identificación personal en caso de que dicha clave corra algún peligro (en caso de haberse perdido la misma o haberse perdido su control a causa de una fuga de datos, o en el caso de sospecharse que haya ocurrido cualquiera de dichos casos. Debajo denominado de la misma forma).

(11) Proveer a los verificadores de firmas de sistemas para comprobar la validez de certificados

digitales (sistema que responda a las consultas de información de invalidación que empleen el protocolo OCSP (debajo denominado "sistema de consulta OCSP responder") y sistema para proveer registros de invalidación (CRL/ARL)).

(12) Proveer a los usuarios de sistemas para comprobar la validez de los certificados digitales emitidos por el gobierno central y los certificados digitales emitidos por las entidades públicas locales.

(13) Creación y publicación de informes sobre el estado de entrega de información de invalidación y los archivos de información de invalidación.

(14) Muestra de información al recibir demandas de muestra de información referentes a información del servicio de certificación

(15) Corrección de datos al recibir demandas de corrección de datos referentes a datos del servicio de certificación

(16) Creación de la doble clave del gobernador de la prefectura de Hokkaido y control de seguridad de la clave secreta

(17) Ejecución de inspecciones y ejecución de mejoras en el servicio según se determine en los resultados de inspección

(18) Instalación de infraestructuras para la ejecución del servicio de certificación

(19) Obedecer estas normas operativas para la expedición y renovación de certificados así como para las labores de invalidación

(20) Conservación de los certificados y registros de invalidación (CRL/ARL) ya expedidos durante el periodo de tiempo requerido, además de la conservación de los registros de supervisión y datos de conservación relacionados con la expedición y renovación de certificados así como con las labores de invalidación durante el periodo de tiempo requerido

(21) Tener como objetivo que el sistema funcione de manera estable las 24 horas efectuando una vigilancia continua y precisa del funcionamiento del mismo

(22) Expedir cada 24 horas los registros de invalidación (CRL/ARL) durante las 72 horas del periodo de vigencia de la información de invalidación

(23) Responder a las quejas y consultas de los usuarios

(24) Encargo de labores administrativas de identificación a organismos de certificación designados, informe al Ministro de Asuntos Internos y Comunicaciones y convocatoria pública

(25) Avisos a organismos de certificación designados de información de invalidación por cambio de personal

(26) Indicaciones a organismos de certificación designados según se requiera

(27) Demanda de aquellos informes necesarios a los organismos de certificación designados y ejecución de inspecciones oficiales

(28) Anulación de encargos a organismos de certificación designados, informe al Ministro de Asuntos Internos y Comunicaciones y convocatoria pública

(29) Aprobación de las tasas impuestas por los organismos de certificación designados a cobrar por la expedición de certificados o por proveer datos

(30) Deliberación con los organismos de certificación designados sobre los costes de las labores administrativas de identificación y su pago

(31) Ejecución de las labores administrativas de identificación en caso de interrupción de las labores administrativas de administración por parte de los organismos de certificación designados

(32) Concluir un acuerdo con los verificadores de firmas

(33)Demanda de aquellos informes necesarios sobre el estado de ejecución de las labores de trabajo a los verificadores de firmas

(34) Uso correcto de los datos relacionados con el servicio de certificación

(35) Conservación de secretos provenientes de datos del servicio de certificación

(36) Avisos y anuncios públicos a los usuarios sobre datos relacionados con el Servicio Público para la Identificación Personal

(37) Creación y aprobación de estas normas operativas

2-1-3 Obligaciones de los municipios

(1) Comprobación de identidad (de que existe realmente y de que es la persona en cuestión) del solicitante de la expedición del certificado o del invalidación en el momento de la expedición u extinción

(2) Comprobación de que en caso de solicitud por representante legal este es ciertamente el representante legal

(3) Comprobación de los requisitos de invalidación cuando se solicite una invalidación

(4) Comprobación de que el resto de procedimientos de solicitud se efectúan adecuadamente

(5) Proveer de dispositivo generador de doble clave que cree doble clave adecuadamente segura (dispositivo que cree doble clave de los solicitantes, debajo denominado "dispositivo generador de doble clave")

(6) Comunicación al gobernador de la prefectura de Hokkaido de las cuatro informaciones fundamentales y la clave pública del solicitante

(7) Comunicación al gobernador de la prefectura de Hokkaido de solicitudes de invalidación

(8) Entrega a los usuarios de certificados digitales y certificados de firma propia del gobernador de la prefectura de Hokkaido

(9) Explicación a los solicitantes y usuarios de los límites en el uso de certificados digitales y las sanciones aplicables al usarse estos de forma indebida

(10) Mantenimiento y control de la seguridad del dispositivo generador de doble clave y de los sistemas de las terminales de ventanilla

(11) Respuesta a inspecciones y ejecución de mejoras en el servicio según se determine en los resultados de inspección

(12) Uso correcto de los datos relacionados con el servicio de certificación

(13) Conservación de secretos provenientes de datos del servicio de certificación

(14) Recibir las tasas de expedición de los solicitantes de expedición de certificados digitales

(15) Recepción de demandas de muestra y corrección de datos referentes a datos del servicio de certificación

(16) Restablecimiento de contraseñas, anulación de bloqueos (se refiere a la anulación del estado en el que queda una tarjeta IC al haberse introducido incorrectamente la contraseña 5 veces o más para prevenir su uso indebido), extinción de la doble clave

(17) Soporte a usuarios en la adquisición del software de usuario de las terminales de usuario (software necesario para poder usar los certificados digitales)

(18) Responder a las quejas y consultas de los usuarios

(19) Avisos y anuncios públicos a los usuarios sobre datos relacionados con el Servicio Público para la Identificación Personal

2-1-4 Obligaciones de los organismos de certificación designados

(1) Ejecución de las labores administrativas de identificación según el encargo del gobernador de la prefectura de Hokkaido (ejecutar desde los puntos (1) al (13), el (16) y de los puntos (18) al (22) de las "2-1-2 Obligaciones del gobernador de la prefectura de Hokkaido" de estas normas operativas)

(2) Determinación de las normas de control de labores administrativas de identificación

(3) Creación del plan empresarial y del presupuesto de gastos e ingresos así como entrega del informe empresarial y de la hoja del balance de gastos e ingresos

(4) Establecer un comité para la protección de datos del servicio de certificación

(5) Uso correcto de los datos relacionados con el servicio de certificación

(6)Conservación de secretos provenientes de datos del servicio de certificación

(7) Muestra de datos al recibir demandas de muestra de datos referentes a datos del servicio de certificación

(8) Corrección de datos al recibir demandas de corrección de datos referentes a datos del servicio de certificación

(9) Responder a las quejas y consultas de los usuarios

(10) Recibir las tasas por oferta de información de los verificadores de firmas

2-1-5 Obligaciones de los usuarios

(1) Rellenar de manera precisa los campos requeridos en la solicitud de expedición y en la solicitud de invalidación de certificados digitales

(2) Conservar de forma segura la clave secreta y la tarjeta IC que contiene dicha clave secreta

(3) Conservar de forma segura y cambiar de forma periódica la contraseña que activa la clave secreta contenida en la tarjeta IC

(4) Solicitar la invalidación inmediata en caso de que la clave secreta esté en peligro

(5) No usar los certificados digitales para fines ajenos a los establecidos

(6) Abonar las tasas de expedición

2-1-6 Obligaciones de los verificadores de firmas

(1) Verificar las firmas digitales con los certificados digitales expedidos por la CA de la prefectura de Hokkaido

(2) Verificar los certificados digitales expedidos por la CA de la prefectura de Hokkaido (verificar si dicho certificado digital ha sido expedido por el gobernador de la prefectura de Hokkaido y si dicho certificado digital ha sido extinguido o no)

(3) No usar los certificados digitales para fines ajenos a la verificación de firmas digitales en solicitudes y notificaciones realizadas por usuarios a través de Internet y a la comprobación de los usuarios

(4) Concluir un acuerdo con el gobernador de la prefectura de Hokkaido en la recepción de información de invalidación y de archivos de información de invalidación

(5) Cumplimiento de las demandas de informes provenientes del Ministro de Asuntos Internos y Comunicaciones y del gobernador de la prefectura de Hokkaido

(6) Conservación y uso correcto de secretos provenientes de información de invalidación

(7) Asegurar la información de invalidación

(8) Abonar las tasas por oferta de información

2-1-7 Obligaciones de los verificadores de firmas grupales

(1) Comprobar que los certificados digitales expedidos por la CA de la prefectura de Hokkaido no han sido extinguidos

(2) No usar los certificados digitales para fines ajenos a la identificación de usuarios mediante la verificación de las firmas digitales de los usuarios y que han sido recibidas a través del examinador de firmas

(3) Concluir un acuerdo con el gobernador de la prefectura de Hokkaido en la recepción de información de invalidación y de archivos de información de invalidación

(4) Cumplimiento de las demandas de informes provenientes del Ministro de Asuntos Internos y Comunicaciones y del gobernador de la prefectura de Hokkaido

(5) Conservación y uso correcto de secretos provenientes de información de invalidación

(6) Asegurar la información de invalidación

(7) Abonar las tasas por oferta de información

2-1-8 Obligaciones de los examinadores de firmas

(1) Verificar las firmas digitales con los certificados digitales expedidos por la CA de la prefectura de Hokkaido

(2) Verificar los certificados digitales expedidos por la CA de la prefectura de Hokkaido (verificar si dicho certificado digital ha sido expedido por el gobernador de la prefectura de Hokkaido y si dicho certificado digital ha sido extinguido o no)

(3) No usar los certificados digitales para fines ajenos a la verificación de firmas digitales en solicitudes y notificaciones por usuarios a través de Internet y a la comprobación de los usuarios

(4) Conservación y uso correcto de secretos provenientes de respuestas recibidas a través de los verificadores de firmas grupales

(5) Asegurar las respuestas recibidas a través de los verificadores de firmas grupales

2-1-9 Obligaciones del repositorio

El CA de la prefectura de Hokkaido, tras crearse los registros de invalidación (CRL/ARL), y mediante su publicación al repositorio, hará posible que los verificadores de firmas comprueben la validez de los certificados digitales.

Además, se encargará de conservar y publicar otros tipos de datos.

2-2 Responsabilidades

2-2-1 Responsabilidades del Ministro de Asuntos Internos y Comunicaciones

El Ministro de Asuntos Internos y Comunicaciones, y según se determina en la Ley Fundamental, nombrará los organismos de certificación designados y controlará y supervisará a estas para que realicen las labores administrativas de identificación de forma segura y correcta.

2-2-2 Responsabilidades del gobernador de la prefectura de Hokkaido

El gobernador de la prefectura de Hokkaido ejecutará de forma apropiada sus labores según estas normas operativas, dirigidas a los usuarios y verificadores de firmas para la expedición de certificados digitales, certificados de identificación recíproca, certificados de firma propia, certificados Link y otros certificados necesarios para las labores, además de la creación de registros de invalidación (CRL/ARL) relacionados con dichos certificados y también proveer de los medios para comprobar la validez de certificados digitales, certificados digitales emitidos por las entidades públicas locales y certificados digitales emitidos por el gobierno central .

Además, en caso de haber encargado labores administrativas de identificación a los organismos de certificación designados, controlará y supervisará a estas para que realicen las labores administrativas de identificación de forma segura y correcta.

2-2-3 Responsabilidades de los municipios

Los municipios ejecutarán de forma apropiada sus labores según estas normas operativas para la recepción de las solicitudes de expedición de certificados digitales y las solicitudes de invalidación y la comprobación de la identidad del solicitante.

2-2-4 Responsabilidades de los organismos de certificación designados

Los organismos de certificación designados recibirán el encargo del gobernador de la prefectura de Hokkaido para realizar las siguientes labores administrativas de identificación. Ejecutarán de forma apropiada sus labores según estas normas operativas, dirigidas a los usuarios y verificadores de firmas para la expedición de certificados digitales, certificados de identificación recíproca, certificados de firma propia, certificados Link y otros certificados necesarios para las labores, además de la creación de registros de invalidación (CRL/ARL) relacionados con dichos certificados y también proveer de los medios para comprobar la validez de certificados digitales, certificados digitales emitidos por las entidades públicas locales y certificados digitales emitidos por el gobierno central.

2-2-5 Responsabilidades de los usuarios

Los usuarios usarán este servicio siguiendo estas normas operativas.

2-2-6 Responsabilidades de los verificadores de firmas

Los verificadores de firmas verificarán los certificados digitales siguiendo estas normas operativas.

2-2-7 Responsabilidades de los verificadores de firmas grupales

Los verificadores de firmas grupales comprobarán la validez de los certificados digitales siguiendo estas normas operativas.

2-2-8 Responsabilidades de los examinadores de firmas

Los examinadores de firmas verificarán los certificados digitales siguiendo estas normas operativas.

2-3 Responsabilidades financieras

El gobernador de la prefectura de Hokkaido no se hará responsable de daños y prejuicios originados por causas ajenas a aquellas bajo la responsabilidad de la CA de la prefectura de Hokkaido.

En caso de originarse causas bajo la responsabilidad de la CA de la prefectura de Hokkaido, el gobernador de la prefectura de Hokkaido se hará cargo de los daños y prejuicios según los márgenes que estipula la ley.

2-4 Interpretación y ejecución

2-4-1 Aplicación de la ley

Dependerá de la Ley Fundamental y otras leyes relacionadas.

2-4-2 División, integración del servicio, cambios y avisos en el sistema de administración

En caso de haber cambios en el sistema de administración, estos se deberán hacer públicos a los usuarios y verificadores de firmas inmediatamente en alguno de los siguientes medios.

- En el sitio Web de la Asociación
- En el sitio Web de la prefectura de Hokkaido

Además, en caso de que los organismos de certificación designados cambien su nombre o la dirección de sus oficinas, deberán informar de ello al Ministro de Asuntos Internos y Comunicaciones y al gobernador de la prefectura de Hokkaido.

2-4-3 Aceptación e informe de las órdenes de supervisión e inspecciones oficiales

Lao organismos de certificación designados, en caso de recibir por parte del Ministro de Asuntos Internos y Comunicaciones una orden de supervisión de las labores administrativas de identificación y en caso de recibir por parte del gobernador de la prefectura de Hokkaido indicaciones para la correcta ejecución de las labores administrativas de identificación, deberán de obedecer las mismas.

Además, los organismos de certificación designados, en caso de que reciban demandas de informe o de inspección oficial sobre las condiciones de ejecución de las labores administrativas de identificación por parte del Ministro de Asuntos Internos y Comunicaciones o del gobernador de la prefectura de Hokkaido, deberán de obedecer las mismas.

2-4-4 Procedimientos para la resolución de conflictos

Para aquellos pleitos judiciales relacionados con estas normas operativas, el juzgado competente para las partes interesadas en primera instancia será el juzgado de la región de Sapporo.

2-5 Tasas

Las tasas de expedición de certificados, oferta de datos y archivos de invalidación y muestra de información referente al servicio de certificación quedarán establecidas según la Ley Fundamental.

2-6 Publicación y repositorios

2-6-1 Publicación de información relacionada con la CA de la prefectura de Hokkaido

La prefectura de Hokkaido hará públicos las siguientes informaciones en el sitio Web de la Asociación.

- Ley Fundamental y leyes relacionadas
- Estas normas operativas
- Nombre de CA que hayan realizado identificaciones recíprocas con la CA de la prefectura de Hokkaido
- Nombre de CA que hayan cancelado identificaciones recíprocas con la CA de la prefectura de Hokkaido
- Información relacionada en caso de estar en peligro la clave secreta del gobernador de la prefectura de Hokkaido

La CA de la prefectura de Hokkaido, hará públicos en los repositorios del Servicio Público para la Identificación Personal las siguientes informaciones.

- Certificados de firma propia
- Certificados de identificación recíproca
- Certificados Link
- Registros de invalidación (ARL) de certificados de firma propia, certificados de identificación recíproca y certificados Link
- Registros de invalidación (CRL) de certificados digitales de usuarios

2-6-2 Frecuencia de las publicaciones

La información se actualizará y hará pública con la siguiente frecuencia.

- Se publicará de manera regular la versión actualizada de la Ley Fundamental, leyes relacionadas y de estas normas operativas.
- Se publicarán los certificados de firma propia, certificados de identificación recíproca y certificados Link cada vez que sean expedidos o renovados
- Se actualizarán una vez por día los registros de invalidación (CRL/ARL)

2-6-3 Control de acceso a información pública

No se restringirá el acceso a la Ley Fundamental, leyes relacionadas y a estas normas operativas.

Además, tampoco se restringirá el acceso a la siguiente información de los repositorios.

- Certificados de firma propia
- Certificados de identificación recíproca
- Certificados Link
- Registros de invalidación (ARL) de certificados de firma propia, certificados de identificación recíproca y certificados Link

Sin embargo, en los repositorios se restringirá el acceso a los registros de invalidación (CRL) de los certificados digitales de usuarios

.

2-6-4 Requisitos relacionados con los repositorios

Se facilitará el acceso a los repositorios 24 horas al día los 365 días del año. Sin embargo, a causa de labores de mantenimiento periódicas habrá casos en los que no se podrá acceder temporalmente al repositorio.

2-7 Supervisión para el control de cumplimiento con normas

2-7-1 Frecuencia de las supervisiones de control de cumplimiento de normas

A través de un supervisor, el gobernador de la prefectura de Hokkaido realizará 1 vez al año una supervisión periódica de control de cumplimiento de normas. Además se efectuarán supervisiones sorpresa según se estime necesario aparte de la supervisión periódica.

2-7-2 Identificación y certificación de supervisores

La supervisión de la CA de la prefectura de Hokkaido la efectuará una persona especializada en las labores de supervisión y el servicio de certificación.

2-7-3 Relación entre el supervisor y el departamento a supervisar

El gobernador de la prefectura de Hokkaido seleccionará como supervisor a una persona que no tenga un conflicto de intereses con la CA de la prefectura de Hokkaido.

2-7-4 Asuntos a supervisar

Se efectuará una supervisión centrada en comprobar si el servicio de certificación cumple con la Ley Fundamental, las leyes relacionadas y de estas normas operativas.

2-7-5 Uso de los resultados de supervisión

El supervisor entregará los resultados de supervisión al gobernador de la prefectura de Hokkaido en forma de informe de supervisión. El gobernador de la prefectura de Hokkaido transmitirá los informes de supervisión según se estime necesario a municipios y organismos de certificación designados.

2-7-6 Respuesta a asuntos nombrados en la supervisión

Los organismos de certificación designados comprobarán los asuntos nombrados en la supervisión y tomará medidas de respuesta apropiadas según la importancia y urgencia de los mismos. Se evaluarán estos resultados y se informará al gobernador de la prefectura de Hokkaido. El gobernador de la prefectura de Hokkaido comprobará que los organismos de certificación designado han tomado medidas contra los asuntos nombrados en la supervisión.

2-8 Preservación de secretos y protección de información personal

2-8-1 Datos que se considerarán secretos y uso de información personal

La CA de la prefectura de Hokkaido considerará datos secretos a aquellos que al producirse una fuga de los mismos puedan dañar la confianza en el servicio de certificación de la CA de la prefectura de Hokkaido. Además protegerá apropiadamente información personal de los usuarios.

Para controlar de forma segura aquellos datos considerados secretos y aquellos datos que contengan información personal de usuarios se determinará un responsable de control de los documentos y medios electromagnéticos que contengan estos datos (será el responsable de control de la autoridad certificadora determinado en el punto "5-2-1-1 Personal de la CA de la prefectura de Hokkaido" de estas normas operativas). En caso de producirse una fuga de información personal se tomarán medidas extra según los procedimientos establecidos.

2-8-2 Datos no considerados secretos

De los datos que posee la CA de la prefectura de Hokkiado, no se considerarán secretos los certificados de firma propia, certificados Link, certificados de identificación recíproca, certificados de servidor para verificación de certificados digitales emitidos por el gobierno central, certificados de OCSP responder, información de invalidación de estos certificados, estas normas operativas y aquellos datos que se especifican como públicos.

2-8-3 Publicación de información de invalidación de certificados

Se publicará la información de invalidación de certificados de firma propia, certificados Link, certificados de identificación recíproca y certificados relacionados con la administración del servicio que expide la CA de la prefectura de Hokkaido. No se harán públicos los detalles sobre la razón de invalidación. Además la información de invalidación de certificados digitales, en base a la Ley Fundamental, se proveerá de forma limitada a los verificadores de firmas.

2-8-4 Muestra de información a organismos judiciales

Queda sin determinar.

2-8-5 Muestra de información para procedimientos civiles

Queda sin determinar.

2-8-6 Muestra de información según las solicitudes de usuarios de certificados

Se mostrarán los datos en caso de presentarse una solicitud de muestra de datos referentes a información del servicio de certificación por parte de los propios usuarios una vez se haya comprobado su identidad personal.

2-8-7 Muestra de información en otros casos

Queda sin determinar.

2-8-8 Corrección de información según las solicitudes de usuarios de certificados

Se corregirán la información en caso de presentarse una solicitud de corrección de información referente al servicio de certificación por parte de los propios usuarios una vez se haya comprobado su identidad personal.

2-9 Derechos de propiedad intelectual

Queda sin determinar.

3. Diferenciación e identificación

3-1 Primera solicitud de expedición de certificados

3-1-1 Clase de nombre

El nombre oficial y el nombre de usuario del certificado digital se establecerá siguiendo el formato de nombre de identificación X.500 (DN: Distinguished Name).

3-1-2 Requerimientos del significado de los nombres

El nombre oficial del certificado digital lo registrará el gobernador.

Además las cuatro informaciones fundamentales contenidas en el certificado digital se registrarán en el área de memoria de expansión del certificado digital. Debajo se indica la información del área de memoria de expansión donde contiene las cuatro informaciones fundamentales de los usuarios.

subjectAltName		
	common Name	Nombre (en caso de que el usuario sea un residente extranjero y tenga un nombre apelativo escrito en su certificado de residencia, se incluirá su nombre y el nombre apelativo)
	dateOfBirth	Fecha de nacimiento
	gender	Sexo
	address	Dirección

3-1-3 Reglas para interpretar el formato del nombre

Se seguirán las normas del nombre de identificación X.500

3-1-4 Unicidad del nombre

El campo de "subject" de los certificados digitales que expida la CA de la prefectura de Hokkaido deberá asignarse de forma única y no repetible.

3-1-5 Medios de resolución de disputas relacionadas con nombres

Queda sin determinar.

3-1-6 Reconocimiento, identificación y función de logotipos

Queda sin determinar.

3-1-7 Tipos y formato de nombres registrados en el área de memoria de expansión del certificado digital

Se registrará con el nombre, nombre apelativo del usuario (solo en caso de que el receptor del certificado digital sea un residente extranjero y tenga un nombre apelativo escrito en su certificado de residencia, se incluirá su nombre y el nombre apelativo), dirección, fecha de nacimiento, sexo, en kanji, hiragana, katakana, letras del alfabeto y caracteres numéricos.

3-1-8 Reglas relacionadas con los sistemas de registro de nombres registrados en el área de memoria de expansión del certificado digital

En el registro del nombre solo se podrán usar caracteres de kanji (de tipo JISX0208, JISX0212) empleados en las terminales de ventanilla de recepción del municipio del lugar de residencia.

En caso de existir en el nombre kanjis que no se puedan utilizar, se dará a elegir al usuario entre

kanjis similares (debajo denominados "caracteres alternativos).

En caso de utilizarse caracteres similares, esto se deberá especificar en el área de memoria de expansión del certificado digital

3-1-9 Requisitos para la diferenciación e identificación de usuarios

En la primera solicitud de expedición se comprobará la identidad del solicitante de las siguientes formas. Sin embargo, en caso de haber dudas en la comprobación de identidad, no se expedirá el certificado.

① Se comprobará que el solicitante está registrado en el registro básico de residentes mediante la comparación de las cuatro informaciones fundamentales escritas en la solicitud de expedición con los datos registrados en el registro básico de residentes (comprobación de que existe realmente).

② Se comprobará que el solicitante es aquella persona registrada en el registro básico de residentes mediante la muestra de un certificado de identidad con foto que haya sido expedida por un organismo público (documentos determinados en el párrafo 1 del artículo 6 de las normas de la Ley Fundamental), (comprobación de que es la persona en cuestión).

3-1-10 Requisitos para la diferenciación e identificación en caso de solicitud por representante legal

En caso de solicitud por representante legal, se comprobará la identidad del representante legal y que posee los derechos de representación legal de la siguiente forma.

① Se comprobará la carta de encargo de representación con nombre y sello del solicitante, el certificado de registro de sello de dicho sello, una carta de respuesta a la petición del solicitante y algún otro documento que el municipio de residencia considere pertinente.

② Se comprobará la identidad del representante legal mediante la muestra de un certificado de identidad con foto que haya sido expedida por un organismo público (documentos determinados en el párrafo 1 del artículo 5 de las normas de la Ley Fundamental), (comprobación de que es la persona en cuestión).

3-1-11 Medios de comprobación de pruebas que acrediten la posesión de la clave secreta

Mediante la creación por parte del solicitante de la doble clave empleando un dispositivo generador de doble clave instalado en el municipio de residencia según la Ley Fundamental y leyes relacionadas.

3-2 Renovación de certificados digitales

En el momento de renovación de certificados digitales se comprobará la identidad del solicitante de las siguientes formas. Sin embargo, en caso de haber dudas en la comprobación de identidad, no se renovará el certificado.

① Se comprobará que el solicitante está registrado en el registro básico de residentes mediante la comparación de las cuatro informaciones fundamentales escritas en la solicitud de renovación con los datos registrados en el registro básico de residentes (comprobación de que existe realmente).

② Se comprobará que el solicitante es aquella persona registrada en el registro básico de residentes mediante la muestra de un certificado de identidad con foto que haya sido expedida por un organismo público (comprobación de que es la persona en cuestión).

Las claves secretas relacionadas con los certificados de digitales que sufran una invalidación causa de dicha actualización serán borradas por el usuario mediante los procedimientos establecidos.

3-3 Re-expedición tras la invalidación

Se ejecutarán los mismos procedimientos de comprobación de identidad que en el caso de solicitud de expedición nueva.

3-4 Solicitud de invalidación

3-4-1 Solicitudes de invalidación para dejar de utilizar este servicio

Se hará a través de Internet mediante firma digital con clave secreta del usuario o en ventanilla del municipio de residencia mediante solicitud documental.

En caso de hacerse a través de Internet, se comprobará la identidad del usuario verificando su firma digital. En caso de hacerse mediante solicitud documental en ventanilla del municipio de residencia, se harán los procedimientos de comprobación de identidad del mismo modo que en la expedición de certificados digitales.

3-4-2 Solicitudes de invalidación en caso de que la clave secreta del usuario esté en peligro

Se efectuará de manera inmediata la solicitud documental de invalidación en ventanilla del municipio de residencia.

Se harán los procedimientos de comprobación de identidad del mismo modo que en la expedición de certificados digitales.

4. Requerimientos para el uso

4-1 Solicitudes de expedición de certificados digitales

4-1-1 Solicitudes de expedición y procedimientos de recepción

Las solicitudes de expedición y procedimientos de recepción de certificados digitales se efectuarán de la siguiente forma.

① El solicitante hará entrega en su municipio de residencia de la solicitud de expedición y de su tarjeta IC. En caso de renovación, hará entrega de su tarjeta IC conteniendo el certificado digital.

② El municipio de residencia comparará los datos con el registro básico de residentes y al mismo tiempo que comprueba que el usuario existe realmente, comprobará que el solicitante es la persona en cuestión mediante la muestra de un certificado de identidad con foto que haya sido expedida por un organismo público como un carnet de conducir o un pasaporte. Sin embargo, en caso de haber dudas en la comprobación de identidad, no se expedirá el certificado.

③ El solicitante empleará un dispositivo generador de doble clave instalado en la ventanilla del municipio de residencia para generar la doble clave. De las dos claves, se informará a la ventanilla del municipio de residencia la clave pública.

Además, se podrá efectuar una solicitud por representante legal mediante los siguientes procedimientos. Sin embargo, en caso de haber dudas en la comprobación de identidad en los puntos (1) o (2), no se expedirá el certificado.

(1) El representante legal entregará o mostrará la carta de encargo de representación con nombre y sello del solicitante (solo en el caso de estar adjunto el certificado de registro de sello de dicho sello) y un carnet de conducir, pasaporte, etc. para comprobar que el representante legal es la persona en cuestión.

(2) El representante legal, para comprobar que la solicitud de expedición del certificado digital está hecha por el solicitante y que se hace con el consentimiento del mismo, al mismo tiempo que presenta un documento de respuesta a la petición del solicitante y algún otro documento que el municipio de residencia considere pertinente, por correo u otro medio que el municipio de la residencia considere adecuado.

(3) El representante legal empleará un dispositivo generador de doble clave para crear la doble clave y de las dos claves informará la clave pública al municipio de residencia. Sin embargo, será el municipio de residencia el que introduzca la contraseña (activará la clave secreta).

4-1-2 Formato y puntos requeridos en las solicitudes de expedición

Se escribirán los siguientes puntos en la solicitud de expedición.

・Fecha de solicitud

・Nombre (en furigana), nombre apelativo del usuario (solo en caso de que el receptor del certificado digital sea un residente extranjero y tenga un nombre apelativo escrito en su certificado de residencia), dirección, fecha de nacimiento, sexo y caracteres alternativos del nombre, del nombre apelativo y de la dirección

・En caso de solicitud por representante legal, se añadirá el nombre y la dirección del representante legal a los datos arriba descritos

4-1-3 Dispositivos de registro electromagnético de claves secretas

Se guardarán en una tarjeta IC con sistema de prueba de alteraciones.

4-2 Expedición de certificados digitales

4-2-1 Procedimientos de expedición

Los procedimientos de expedición de certificados digitales se efectuarán de la siguiente

forma.

① El municipio de residencia comunicará al gobernador de la prefectura de Hokkaido de las cuatro informaciones fundamentales y de la clave pública del solicitante.

② El gobernador de la prefectura de Hokkaido expedirá el certificado digital y se lo comunicará al municipio de residencia.

4-2-2 Formato de certificados digitales

En base a las recomendaciones ITU-T X.509 (03/2000), se registrará en el área de memoria de expansión el nombre, nombre apelativo, dirección, fecha de nacimiento y sexo del usuario en kanji, hiragana, katakana, letras del alfabeto y caracteres numéricos.

Además, en caso de usarse caracteres alternativos en el nombre, nombre apelativo y dirección registrados en el área de memoria de expansión, esto se deberá especificar en el área de memoria de expansión.

subjectAltName		
	commonName	Nombre (en caso de que el usuario sea un residente extranjero y tenga un nombre apelativo escrito en su certificado de residencia, se incluirá su nombre y el nombre apelativo)
	dateOfBirth	Fecha de nacimiento
	gender	Sexo
	address	Dirección
	substituteCharacterOfCommonName	Información de uso de caracteres alternativos en el nombre
	substituteCharacterOfAddress	Información de uso de caracteres alternativos en la dirección

4-2-3 Rechazo de solicitudes de expedición

El gobernador de la prefectura de Hokkaido rechazará la solicitud de expedición en los siguientes casos.

・Poseer ya un certificado digital válido y no estar especificado en el registro de invalidación (CRL)

En caso de que se haya expedido un duplicado del certificado, el gobernador de la prefectura de Hokkaido deberá inmediatamente extinguir los datos del certificado digital con la fecha más reciente.

4-3 Entrega de certificados digitales

4-3-1 Procedimientos de entrega

Los procedimientos de entrega de certificados digitales se efectuarán de la siguiente forma.

① El municipio de residencia registrará el certificado digital y el certificado de firma propia del gobernador de la prefectura de Hokkaido en la tarjeta IC del solicitante

② El municipio de residencia avisará al solicitante de los puntos de advertencia referentes al uso de este servicio y le hará entrega de una copia del certificado digital

4-3-2 Puntos de advertencia

El municipio de residencia avisará a los usuarios de los siguientes puntos.

・La clave secreta, el medio de registro electromagnético que es la tarjeta IC y la contraseña

para activar la tarjeta IC deberán ser conservados de forma segura por el usuario bajo su propia responsabilidad

・En caso de pérdida o robo de la clave secreta o el medio de registro electromagnético que es la tarjeta IC, deberá notificarse inmediatamente en la ventanilla del municipio de residencia y solicitar la invalidación

4-4 Invalidación e interrupción temporal de certificados digitales

4-4-1 Razones de invalidación de autoridad

4-4-1-1 Razones de invalidación de autoridad

Las razones de invalidación de autoridad de certificados digitales serán las siguientes.

・Cambios en las cuatro informaciones fundamentales del usuario

・Casos en los que los datos especificados en el certificado digital del usuario sean diferentes a aquellos especificados en el registro de residencia del usuario del certificado digital

・En caso de descubrirse que se ha expedido un duplicado del certificado digital

・En caso de estar en peligro la clave secreta del gobernador de la prefectura de Hokkaido

4-4-1-2 Personas que pueden extinguir datos de certificados

Los podrá extinguir el gobernador de la prefectura de Hokkaido

4-4-1-3 Procedimientos de invalidación cuando la clave secreta del gobernador de Hokkaido esté en peligro

En caso de que la clave secreta del gobernador de Hokkaido esté en peligro, la autoridad extinguirá los datos de los certificados firmados con dicha clave secreta y al mismo tiempo que se registra la extinción en el registro de invalidación (CRL/ARL) este se hará público en el sitio Web o por otros medios.

4-4-2 Invalidación por solicitud de usuarios

4.4-2-1 Razones de invalidación por solicitud de usuarios

Las razones aceptadas para la invalidación por solicitud serán las siguientes.

・Que el usuario quiera dejar de utilizar este servicio

・Que la clave secreta del usuario esté en peligro

4-4-2-2 Procedimientos en solicitudes de invalidación para dejar de utilizar este servicio

Los procedimientos de invalidación para dejar de utilizar este servicio se efectuarán de las siguientes formas.

① Recepción de solicitudes a través de Internet con firma digital. Se comunicará al usuario a través de Internet que se ha recibido la solicitud de invalidación.

② Recepción de solicitudes de invalidación de forma documental en ventanilla del municipio de residencia. Se solicitarán los procesos de invalidación al gobernador de la prefectura de Hokkaido. Se entregará al usuario un documento acreditando que se ha recibido la solicitud de invalidación.

4-4-2-3 Procedimientos en solicitudes de invalidación en caso de que la clave secreta del usuario esté en peligro

Los procedimientos de invalidación en caso de que la clave secreta del usuario esté en peligro se efectuarán de las siguientes formas.

① Recepción de solicitudes de invalidación de forma documental en el municipio de residencia.

③ Se solicitarán los procesos de invalidación al gobernador de la prefectura de Hokkaido. Se entregará al usuario un documento acreditando que se ha completado el proceso de invalidación.

4-4-2-4 Medios de recuperación en caso de haberse extinguido el certificado digital de usuarios

Se expedirá un nuevo certificado digital mediante un procedimiento nuevo de solicitud sin recuperar el certificado digital ya extinguido.

4-4-2-5 Medios de recuperación en caso de que la clave secreta del usuario esté en peligro

Se expedirá un nuevo certificado digital mediante un procedimiento nuevo de solicitud.

4-4-3 Requisitos de los registros de invalidación (CRL/ARL)

Se actualizará la información de invalidación que hayan sido terminado de ser recibidos hasta la hora estipulada, se creará un nuevo registro de invalidación (CRL/ARL) cada día y se mostrarán los registros de invalidación (CRL/ARL) creados a los verificadores de firmas autorizados.

Además, se habilitará la muestra de los registros de invalidación (CRL/ARL) a los verificadores de firmas autorizados 24 horas al día los 365 días del año. Sin embargo, a causa de labores de mantenimiento periódicas habrá casos en los que no se podrá acceder temporalmente.

4-4-4 Sistemas para proveer información de invalidación

4-4-4-1 Sistemas para proveer información de invalidación

Se proveerán los dos siguientes sistemas para verificar la validez de los certificados digitales.

① Sistema de consulta OCSP responder (utilizando el protocolo OCSP determinado en el RFC2560)

② Sistema de muestra de registros de invalidación (CRL/ARL) (utilizando el protocolo LDAPV3 determinado en el RFC2551)

4-4-4-2 Respuestas del sistema de consulta OCSP responder

Se responderá a consultas a través de Internet mediante información y números de serie que identifiquen a la persona que ha expedido el certificado digital, determinando si el determinado certificado digital está vigente, en estado desconocido o de invalidación, añadiendo la razón de la invalidación en caso de estarlo, en el momento en que se ha realizado la consulta sobre el certificado digital. Debajo quedan definidas las razones de invalidación.

Razón de invalidación		
1	keyCompromise	La clave secreta del usuario está en peligro.
2	cACompromise	La clave secreta del gobernador de la prefectura de Hokkaido está en peligro.
3	affiliationChanged	Ha habido un cambio en los contenidos del certificado digital.
4	superseded	El certificado digital ha sido renovado.
5	cessationOfOperation	El certificado digital ha dejado de ser necesario. (Ha dejado de usarse).

4-4-4-3 Requisitos del sistema de consulta OCSP responder

Se deberán solicitar por adelantado los permisos de acceso al gobernador de la prefectura de Hokkaido.

4-4-4-4 Respuestas de sistemas para proveer registros de invalidación (CRL/ARL)

El formato de los registros de invalidación (CRL/ARL) se basará en las recomendaciones ITU-T X.509 (03/2000).

Por norma general los registros de invalidación (CRL) se crearán divididos por unidad de municipio y se especificarán en ellos la razón de invalidación (de la misma manera que en las razones de invalidación de "4-4-4-2 Respuestas del sistema de consulta OCSP responder" de estas normas operativas) y la fecha de invalidación. El verificador de firmas obtendrá los registros de invalidación (CRL/ARL) del repositorio y efectuará la verificación de los certificados digitales.

4-4-4-5 Requisitos para proveer registros de invalidación (CRL/ARL)

Se deberán solicitar por adelantado los permisos de acceso al gobernador de la prefectura de Hokkaido.

4-4-5 Requisitos de suspensión temporal del servicio

No se efectuarán suspensiones temporales de certificados digitales expedidos por el gobernador de la prefectura de Hokkaido.

4-4-6 Solicitante de suspensión temporal del servicio

Queda sin determinar.

4-4-7 Procedimientos de demanda de suspensión temporal del servicio

Queda sin determinar.

4-4-8 Periodo de suspensión temporal del servicio

Queda sin determinar.

4-4-9 Frecuencia de expedición de los registros de invalidación (CRL/ARL)

Expedir cada 24 horas los registros de invalidación (CRL/ARL) durante las 72 horas del periodo de vigencia. Sin embargo, en caso de ponerse en peligro la clave secreta del gobernador de la prefectura de Hokkaido, se expedirán inmediatamente los registros de invalidación (CRL/ARL).

4-4-10 Tiempo máximo de espera en la expedición de los registros de invalidación (CRL/ARL)

Se expedirá un nuevo registro de invalidación (CRL/ARL) antes de que caduque el periodo de vigencia del último registro de invalidación (CRL/ARL) expedido.

4-4-11 Comprobación de registros de invalidación (CRL/ARL)

El verificador de firmas deberá verificar la validez de los certificados digitales mediante el uso de registros de invalidación (CRL/ARL) expedidos por el gobernador de la prefectura de Hokkaido.

4-5 Creación de informes sobre el estado de entrega de la información de invalidación

Los organismos de certificación designados deberán crear informes sobre el estado de entrega de la información de invalidación y los archivos de información de invalidación. Los organismos

de certificación designados publicarán en el boletín del estado dichos informes y también deberán habilitar su consulta durante 5 años en sus oficinas.

Los asuntos a especificar en los informes son los siguientes.

- Destino de la información de invalidación provista
- Año y mes en el que se proveyó la información de invalidación
- Número de información de invalidación provista
- Cómo se proveyó la información de invalidación

4-6 Solicitudes de expedición de certificados de identificación recíproca

Las solicitudes de expedición de certificados de identificación recíproca con la BCA de identificación personal se efectuarán según los procedimientos que establece la BCA de identificación personal.

4-7 Expedición de certificados de identificación recíproca

El gobernador de la prefectura de Hokkaido comprobará la autenticidad de la persona que administra la BCA de identificación personal según los procedimientos pertinentes. Una vez finalizadas las pruebas de conexión según los procedimientos determinados por la BCA de identificación personal, se expedirá el certificado de identificación recíproca con la firma del gobernador de la prefectura de Hokkaido respondiendo a la demanda de expedición de certificado entregada por la BCA de identificación personal.

4-8 Recepción de certificados de identificación recíproca

El gobernador de la prefectura de Hokkaido recibirá los certificados de identificación recíproca expedidos por la BCA de identificación personal según los procedimientos pertinentes y entregará un recibo a la BCA de identificación personal. De la misma manera, el gobernador de la prefectura de Hokkaido entregará los certificados de identificación recíproca expedidos para la BCA de identificación personal según los procedimientos pertinentes y recibirá un recibo de la BCA de identificación personal. Con la comprobación de estos recibos se dará por finalizada la recepción mutua de los certificados de identificación recíproca.

Además, el gobernador de la prefectura de Hokkaido creará una copia de los certificados de identificación recíproca igual a los certificados de identificación recíproca intercambiados con la BCA de identificación personal y los registrará en el repositorio.

4-9 Renovación de certificados de identificación recíproca

El gobernador de la prefectura de Hokkaido renovará los certificados de identificación recíproca y las copias de los certificados de identificación recíproca en los siguientes casos del (1) al (4).

Para los procedimientos de solicitud de expedición, expedición y recepción que se llevan a cabo en la renovación de certificados de identificación recíproca, se seguirán los puntos "4-7 Expedición de certificados de identificación recíproca" y "4-8 Recepción de certificados de identificación recíproca" de estas normas operativas. Además, se intercambiarán las copias de los certificados de identificación recíproca del repositorio por su versión más actualizada.

(1) Casos en los que el periodo de vigencia de los certificados de identificación recíproca expedidos por la BCA de identificación personal esté a punto de caducar

(2) Casos en los que el periodo de vigencia de los certificados de identificación recíproca expedidos para la BCA de identificación personal esté a punto de caducar

(3) Casos en los que haya habido cambios en el contenido de los certificados de identificación recíproca expedidos por la BCA de identificación personal

(4) Casos en los que haya habido cambios en el contenido de los certificados de identificación recíproca expedidos para la BCA de identificación personal

4-10 Invalidación de certificados de identificación recíproca

4-10-1 Razones de invalidación

En caso de darse los siguientes casos en la CA de la prefectura de Hokkaido o en la BCA de identificación personal, la CA de la prefectura de Hokkaido extinguirá los certificados de identificación recíproca expedidos para la BCA de identificación personal y la BCA de identificación personal extinguirá los certificados de identificación recíproca expedidos para CA de la prefectura de Hokkaido.

- Estar en peligro la clave secreta
- Renovación del certificado de identificación recíproca
- Término de la identificación recíproca (incluidos casos en los que se termine la identificación recíproca por violación de los estándares de identificación recíproca)

4-10-2 Solicitantes de invalidación

El responsable de la BCA de identificación personal será quien solicite la invalidación a la CA de la prefectura de Hokkiado.

El gobernador de la prefectura de Hokkaido será quien solicite la invalidación a la BCA de identificación personal.

4-10-3 Procedimientos de solicitud de invalidación y de procesos de invalidación

Las solicitudes de invalidación de certificados de identificación recíproca se efectuarán según los procedimientos que establece la BCA de identificación personal.

4-11 Procedimientos de vigilancia de seguridad

4-11-1 Procedimientos de supervisiones de seguridad

El supervisor interno (consultar el punto "5-2-1 Personal de alta confianza y sus funciones" de estas normas operativas) comparará los registros de sucesos en el sistema de la CA de la prefectura de Hokkaido y del repositorio con los registros de ejecución de labores y efectuará una función de supervisor de seguridad comprobando sucesos anómalos como la manipulación indebida del sistema, etc.

4-11-2 Información registrada en los registros de supervisión

Se registrarán los registros de acceso y registros de operación relacionados con asuntos de importancia referentes a la seguridad del sistema de la CA de la prefectura de Hokkaido y del repositorio.

- Registros de operaciones y funcionamientos relacionados con procedimientos de expedición
- Registros de operaciones y funcionamientos relacionados con procedimientos de invalidación
- Todos los registros de acceso y funcionamiento relacionados con comprobaciones de validez
- Registros de operaciones relacionados con la creación de doble clave del gobernador de la prefectura de Hokkaido
- Registros de acceso al sistema, listados, etc.
- Registros de entrada y salida a las instalaciones de la CA de la prefectura de Hokkiado

Se incluirán los siguientes datos en los registros de supervisión.

- Tipo de suceso o proceso
- Fecha en que se originó
- Resultado del proceso
- Datos de identificación del origen del suceso (identidad del operario, nombre del sistema, etc.)

4-11-3 Frecuencia de inspección de los registros de supervisión

El supervisor interno efectuará una supervisión de seguridad cada semana.

4-11-4 Periodo de conservación de los registros de supervisión

Se conservarán durante 1 año.

4-11-5 Protección de los registros de supervisión

Se tomarán medidas contra la manipulación de datos en los registros de supervisión. Además, se traspasará la copia de respaldo de los registros de supervisión a una unidad de memoria externa cada mes y se conservarán en un almacén que se pueda cerrar con llave instalado dentro de unas instalaciones donde se controle la entrada y salida de personas adecuadamente.

Además, el supervisor interno efectuará apropiadamente la consulta y borrado de los registros de supervisión.

4-11-6 Procedimientos de copia de respaldo de los registros de supervisión

Se hará una copia de respaldo cada día y se traspasará a una unidad de memoria externa cada mes.

4-11-7 Avisos de inspección de los registros de supervisión

Se efectuará la inspección de registros de supervisión sin avisar a la persona que haya provocado el suceso.

4-11-8 Inspección de fragilidad

Se evaluará la fragilidad de la seguridad en el uso del servicio y del sistema mediante la inspección de los registros de supervisión.

4-11-9 Sistema de recopilación de registros de supervisión

Se incorporará la función de registros de supervisión como una función del sistema de la CA de la prefectura de Hokkaido y se recopilarán los sucesos importantes relacionados con la seguridad como registros de supervisión desde el momento en que se encienda el sistema.

4-12 Conservación de registros (archivo)

4-12-1 Datos a conservar en documento

4-12-1-1 Tipos de datos a conservar

Se conservarán los siguientes datos.

(Gobernador de la prefectura de Hokkaido)

- Documentos relacionados con la creación de estas normas operativas
- Documentos relacionados con la ejecución de la ceremonia de claves
- Documentos relacionados con protocolos con los verificadores de firmas
- Documentos relacionados con la muestra y corrección de información del servicio de certificación
- Informes de supervisión

(Organismo de certificación designado)

- Documentos relacionados con nombramientos y cambios de los organismos de certificación designados
- Normas de control de labores administrativas de identificación
- Documentos relacionados con infraestructuras y medidas de seguridad

・Documentos relacionados con planes empresariales y presupuestos de gastos e ingresos
・Informes empresariales y hojas del balance de gastos e ingresos
・Documentos relacionados con la muestra y corrección de información del servicio de certificación
・Informes sobre el estado de entrega de la información de invalidación y los archivos de información de invalidación.
・Documentos relacionados con tasas etc.

(Municipios)

・Documentos relacionados con solicitudes de expedición de certificados digitales (documentos de solicitud de expedición, etc.)
・Documentos relacionados con solicitudes de invalidación de certificados digitales (documentos de solicitud de invalidación, etc.)
・Documentos relacionados con la muestra y corrección de datos del servicio de certificación, etc.

4-12-1-2 Periodo de conservación

Se conservarán durante 10 años. Sin embargo, los documentos relacionados con solicitudes de expedición de certificados digitales se conservarán durante 13 años.

4-12-1-3 Protección de datos conservados

Los datos conservados por el organismo de certificación designado, al mismo tiempo que se toman medidas contra la manipulación de datos, se conservará en un almacén que se pueda cerrar con llave instalado dentro de unas instalaciones donde se controle la entrada y salida de personas adecuadamente y serán objeto de medidas de protección que tendrán en cuenta la temperatura y humedad del ambiente. Los datos conservados en los municipios y las prefecturas se conservarán en lugares adecuados.

4-12-1-4 Revisión de protección de datos conservados

Una vez al año se efectuará la comprobación del estado y la legibilidad de los papeles donde se especifican los datos conservados.

4-12-2 Datos conservados de forma digital

4-12-2-1 Tipos de datos a conservar

Los siguientes datos serán conservados por el organismo de certificación designado

・Solicitudes de invalidación (en caso de solicitud a través de Internet al gobernador de la prefectura de Hokkaido)
・Certificados digitales
・Certificados de identificación recíproca
・Certificados de firma propia
・Certificados Link
・Certificados de servidor para verificación de certificados digitales emitidos por el gobierno central
・Certificados de OCSP responder
・Información de invalidación
・Registros de invalidación (CRL/ARL)
・Archivos de información de invalidación
・Historiales de uso de sistemas para proveer registros de invalidación (CRL/ARL)
・Historiales de uso de sistemas de consulta OCSP responder
・Otros historiales (historial de seguridad, historial de interrupción de encendido, historial de

operaciones) etc.

4-12-2-2 Periodo de conservación

Se conservarán durante 10 años. Sin embargo, para certificados digitales ya expedidos serán de 13 años y para información de invalidación será desde el día en que se registraron dichos datos hasta que se cumpla el periodo de vigencia de los certificados digitales con los que están relacionados.

4-12-2-3 Protección de datos conservados

Para los datos conservados se efectuarán un control de acceso al mismo tiempo que se toman medidas contra la manipulación de datos.

Además, se traspasarán los datos conservados a una unidad de memoria externa cada mes y se conservarán en un almacén que se pueda cerrar con llave instalado dentro de unas instalaciones donde se controle la entrada y salida de personas adecuadamente.

4-12-2-4 Procedimientos de copia de respaldo de datos conservados

Se hará una copia de respaldo de los datos conservados cada día y se traspasará a una unidad de memoria externa cada mes.

4-12-2-5 Requerimientos de la timestamp de registros

Se añadirá una timestamp (datos de fecha y hora) a los datos conservados.

4-12-2-6 Revisión de protección de datos conservados

Una vez al año se efectuará la comprobación de la legibilidad de las unidades de memoria externa donde quedan registrados los datos de conservación.

4-13 Renovación de las claves del gobernador de la prefectura de Hokkaido

Cada cinco años se efectuará la renovación de la doble clave del gobernador de la prefectura de Hokkaido

A la hora de renovar la doble clave se expedirá un certificado Link para establecer la ruta de identificación de la clave pública antigua y la clave pública nueva y se publicará en el repositorio.

4-14 Claves en peligro y restablecimiento en caso de desastres o accidentes

4-14-1 Medidas en caso de daños en el hardware, software o datos

En caso de dañarse algún hardware, software o dato, se efectuarán inmediatamente las labores de restablecimiento mediante el uso de hardware o software de repuesto o copias de respaldo de los datos.

4-14-2 Medidas en caso de que la clave secreta del gobernador de la prefectura de Hokkaido esté en peligro

Se tomarán las siguientes medidas.

- Interrupción de las labores de expedición de certificados digitales
- Invalidación de todos los certificados digitales y certificados de identificación recíproca firmados con dicha clave, registro en los registros de invalidación (CRL/ARL) y publicación de los mismos
- Aviso al BCA de identificación personal

4-14-3 Uso de infraestructuras al originarse desastres o accidentes

En caso de que las infraestructuras hayan recibido daños por desastre o accidente, se utilizarán el instrumental de repuesto y se continuará con el trabajo empleando los datos de respaldo.

4-15 Procesos de respuesta a quejas y consultas

El gobernador de la prefectura de Hokkaido, los organismos de certificación designados y los municipios deberán realizar una respuesta adecuada e inmediata a quejas y consultas relacionadas con las labores administrativas de identificación.

4-16 Empleo del sistema

Se efectuará un empleo del sistema seguro y adecuado. Los detalles se determinarán aparte.

4-17 Término del servicio de certificación

Queda sin determinar.

4-18 Aboliciones y suspensiones de las labores administrativas de identificación

Los organismos de certificación designados deberán recibir el permiso del Ministro de Asuntos Internos y Comunicaciones para abolir o suspender toda o parte de sus labores administrativas de identificación.

Además, en caso de que el gobernador de la prefectura de Hokkaido se vea obligado a efectuar las labores administrativas de identificación, los organismos de certificación designados deberán efectuar los siguientes puntos.

- Traspasar al gobernador de la prefectura de Hokkaido las labores administrativas de identificación que debe realizar
- Entregar al gobernador de la prefectura de Hokkaido los listados, documentos, papeles y unidades de memoria requeridas para el traspaso de las labores administrativas de identificación que debe realizar

Todos otros aquellos puntos que el Ministro de Asuntos Internos y Comunicaciones estime que el gobernador de la prefectura de Hokkaido vaya a requerir

5. Control de seguridad estructural, procesal y personal

5-1 Control de seguridad estructural

5-1-1 CA de la prefectura de Hokkaido

5-1-1-1 Ubicación y construcción de instalaciones

Las instalaciones de la CA de la prefectura de Hokkaido se construirán en un lugar donde no esté propenso a recibir daños por inundación, terremotos, incendios u otros desastres y se tomarán medidas en su fase de construcción para hacerlo resistente a terremotos, al fuego y con medidas anti-robo. Además, se colocará el instrumental a utilizar en ellas en un lugar seguro y protegido contra incendios y robos.

5-1-1-2 Acceso estructural

Se controlará la entrada y salida de cada habitación del interior de las instalaciones de la CA de la prefectura de Hokkaido con diferentes niveles de seguridad adecuados a la importancia de las labores que se realizan en su interior. Se identificará a los operarios autorizados mediante mecanismos de reconocimiento de tarjeta IC y de reconocimiento biométrico.

La autorización de entrada y salida a cada habitación la otorgará el responsable de control de la autoridad certificadora de la CA de la prefectura de Hokkiado según las labores del personal determinado en el punto "5-2 Control de seguridad procesal" de estas normas operativas.

Las instalaciones de la CA de la prefectura de Hokkaido serán vigiladas 24 horas al día los 365 días del año por personal de seguridad y el sistema de vigilancia.

5-1-1-3 Electricidad y acondicionamiento de aire

En la CA de la prefectura de Hokkaido, al mismo tiempo que se procura una fuente de energía con capacidad suficiente para el uso del instrumental, se tomarán medidas contra paros eléctricos, apagones y cambios en el voltaje y la frecuencia. En situaciones en las que no llegue la corriente eléctrica comercial, se usará un generador para proveer temporalmente de energía.

Se mantendrá un ambiente apropiado para el instrumental y el personal mediante la instalación de un sistema de aire acondicionado.

5-1-1-4 Medidas contra inundaciones

Se instalarán detectores de fuga de agua en los edificios y habitaciones de la CA de la prefectura de Hokkaido y se tomarán medidas de protección contra el agua en el techo y el suelo.

5-1-1-5 Medidas contra terremotos

Se construirán estructuras resistentes a terremotos en los edificios de la CA de la prefectura de Hokkaido y se tomarán medidas de protección contra caídas del instrumental.

5-1-1-6 Medidas contra incendios

Se construirán estructuras resistentes a incendios en los edificios y se designarán como área de defensa contra incendios las habitaciones de la CA de la prefectura de Hokkiado y se instalarán mecanismos de extinción de incendios.

5-1-1-7 Medidas contra ondas electromagnéticas

Se instalarán mecanismos contra la fuga de datos por medios electromagnéticos en cada habitación del interior de las instalaciones de la CA de la prefectura de Hokkiado adecuados a la importancia de las labores que se realizan en su interior.

5-1-1-8 Control de medios (de almacenaje magnéticos)

Aquellos medios de almacenaje que contengan datos conservados o datos de respaldo se

conservarán en un almacén que se pueda cerrar con llave instalado dentro de unas instalaciones donde se controle la entrada y salida de personas adecuadamente, y además se controlará adecuadamente el transporte de entrada y salida de los mismos según los procedimientos pertinentes.

5-1-1-9 Procesamiento de desechos

Se efectuarán adecuadamente los procesos de desecho de documentos y unidades de memoria que contengan datos considerados secretos siguiendo los procedimientos pertinentes.

5-1-1-10 Copia de respaldo fuera de las instalaciones

Queda sin determinar.

5-1-2 Instalaciones de los municipios

5-1-2-1 Ubicación y construcción de instalaciones

Serán instalaciones pertenecientes al municipio de residencia.

5-1-2-2 Acceso estructural

El dispositivo generador de doble clave y las terminales de ventanilla se instalarán en un lugar que pueda ser vigilado por el personal de los municipios de residencia. Además, se dará un mantenimiento adecuado al dispositivo generador de doble clave y las terminales de ventanilla.

Las terminales de ventanilla las operarán aquellas personas que efectúen la comprobación de identidad de los usuarios. Se efectuará una comprobación de la identidad del operario a través de un sistema de usuario y contraseña.

5-1-2-3 Control de datos conservados

Se conservarán en un lugar adecuado aquellos documentos relacionados con el punto "4-12-1-1 Tipos de datos a conservar" de estas normas operativas.

5-1-2-4 Procesamiento de desechos

Se efectuarán adecuadamente los procesos de desecho de documentos y unidades de memoria que contengan datos considerados secretos además de las terminales de ventanilla y el dispositivo generador de doble clave siguiendo los procedimientos pertinentes.

5-2 Control de seguridad procesal

5-2-1 Personal de alta confianza y sus funciones

5-2-1-1 Personal de la CA de la prefectura de Hokkaido

El personal encargado de la operación del sistema de la CA de la prefectura de Hokkaido será el siguiente.

(1) Responsable de control de la autoridad certificadora

El responsable de control de la autoridad certificadora será el responsable de administración de la CA de la prefectura de Hokkaido y desempeñará las siguientes labores.

- Dirección del servicio de certificación
- Dirección de respuesta en caso de emergencia, como cuando esté en peligro la clave secreta del gobernador de la prefectura de Hokkaido o suceda un desastre
- Instrucciones al personal y comprobación de resultados de operaciones
- Control del mantenimiento de la clave (debajo denominada "clave de control") que controla las funciones del HSM (dispositivo que controla de forma segura la clave

secreta del gobernador de la prefectura de Hokkaido)

- Control de respuestas al recibir demandas de muestra de datos referentes a información del servicio de certificación
- Control de respuestas al recibir demandas de corrección de datos referentes a información del servicio de certificación
- Control de procesos de respuesta a quejas y consultas
- Control del comité para la protección de información del servicio de certificación
- Preparación de listados relacionados con el servicio de certificación
- Creación de informes sobre el estado de entrega de la información de invalidación
- Control de entrada y salida

- Respuesta a supervisiones para el control de cumplimiento con normas y control de ejecución de medidas de corrección indicadas en ellas
- Dirección de la administración y operación de otros asuntos de la CA de la prefectura de Hokkaido
- Control de información personal

(2) Controlador de claves secretas

El controlador de claves secretas será el responsable de las labores que utilicen la clave secreta del gobernador de la prefectura de Hokkaido y desempeñará las siguientes labores. Estas labores se efectuarán por varios controladores de claves secretas.

- Control de la conservación de unidades de copia de respaldo de clave secreta del gobernador de la prefectura de Hokkaido
- Operaciones con el HSM cuando se cree la clave secreta del gobernador de la prefectura de Hokkaido o se expida un certificado digital de firma propia
- Operaciones con el HSM cuando se renueve la clave secreta del gobernador de la prefectura de Hokkaido
- Operaciones con el HSM cuando se haga una copia de respaldo de la clave secreta del gobernador de la prefectura de Hokkaido o cuando se recupere ésta a partir de la copia de respaldo

(3) Encargado de recepción

El responsable de recepción expedirá certificados de identificación recíproca, recibirá solicitudes de renovación y de invalidación, realizará labores de comunicación y coordinación con la BCA de identificación personal y administrará los documentos de solicitud.

(4) Encargado de inspección

El encargado de inspección realizará labores de inspección en solicitudes de expedición, renovación e invalidación de certificados de identificación recíprocos.

(5) Aprobador de inspección

El aprobador de inspección realizará labores de aprobación de aquellas solicitudes de expedición, renovación e invalidación de certificados de identificación recíprocos recibidas a través del encargado de inspección.

(6) Operario superior

El operario superior realizará las siguientes labores empleando la clave secreta del gobernador de la prefectura de Hokkaido. Además, estas labores se efectuarán por varios operarios superiores.

- Activación y desactivación del HSM

・Procesos de expedición, renovación e invalidación de certificados de firma propia
・Procesos de expedición, renovación e invalidación de certificados de identificación recíproca
・Procesos de expedición, renovación y extinción de certificados de servidor para verificación de certificados digitales emitidos por el gobierno central
・Procesos de expedición, renovación e invalidación de certificados de OCSP responder
・Registro de configuración y cambios de la política de certificados digitales de la CA de la prefectura de Hokkaido
・Otras labores de control de la operación del sistema de la CA de la prefectura de Hokkaido

(7) Operario de repositorio

El operario de repositorio realizará labores relacionadas con el control de la configuración del repositorio.

(8) Operario regular

El operario regular realizará la operación y el control del mantenimiento del instrumental de red.

(9) Supervisor interno

El supervisor interno realizará las siguientes labores relacionadas con el sistema y los registros de repositorio de la CA de la prefectura de Hokkaido.

・Inspección de registros de supervisión
・Borrado de registros ya inspeccionados

5-2-1-2 Personal de municipios

El personal de municipios efectuará una estricta comprobación de identidad del solicitante en el momento de la expedición e invalidación de certificados digitales, labores administrativas relacionadas con la expedición e invalidación y, un adecuado control del instrumental empleado para dichas labores administrativas.

5-2-2 Repartición de autorizaciones y ordenación de trabajos para el personal de la CA de la prefectura de Hokkaido

Debajo queda determinada la repartición de autorizaciones para el trabajo del personal y la ordenación de trabajos

① Repartición de autorizaciones
Una vez que se han repartido las autorizaciones desde los puntos de vista de la seguridad personal, varios miembros del personal autorizado administrarán y controlarán las instalaciones.

② Autorización del responsable de control de la autoridad certificadora
El responsable de control de la autoridad certificadora tendrá autorización para dar instrucciones al resto del personal según los procedimientos pertinentes para realizar labores importantes.

③ Autorización del operario superior
El operario superior tendrá autorización para dar instrucciones y comprobar resultados con los operarios regulares según los procedimientos pertinentes determinados aparte en cada una de las labores a realizar. Además expedirá registros y certificados adecuados a la autorización de cada miembro del personal.

5-2-3 Requisitos para la diferenciación e identificación de personal de la CA de la prefectura de Hokkaido

・El sistema efectuará una diferenciación e identificación del personal para acreditar que son personal autorizado cada vez que un miembro del personal opere el sistema.

・Se efectuará la identificación del personal empleando la tarjeta IC y la contraseña de cada miembro del personal. La contraseña se cambiará periódicamente.

・Se reducirán al mínimo la información a la que puede acceder cada miembro del personal según sus funciones.

5-3 Control de seguridad personal en la CA de la prefectura de Hokkaido

5-3-1Comprobación del historial del personal y procedimientos de aprobación

Se efectuará una inspección documental (con C.V, carta de recomendación, etc.) del historial del personal antes de su contratación según los procedimientos requeridos.

5-3-2 Procedimientos de entrenamiento de personal

Se le dará el entrenamiento necesario a cada miembro del personal según el plan de entrenamiento educacional.

5-3-3 Alternación de las labores del personal, frecuencia y orden

El responsable de control de la autoridad certificadora estipulará de manera documental un sistema de rotación para las labores.

5-3-4 Actos no permitidos

En caso de que los miembros del personal actúen de una forma que no esté permitida, se les sancionará según lo estipulado.

5-3-5 Documentos provistos a miembros del personal

Los miembros del personal podrán consultar documentos (manuales de procedimientos de uso, de operación, etc.) según los permisos de acceso de los que dispongan.

6. Control de seguridad técnica

6-1 Creación e instalación de la doble clave

6-1-1 Claves del gobernador de la prefectura de Hokkaido

6-1-1-1 Generador de la doble clave del gobernador de la prefectura de Hokkaido y método de creación

La doble clave del gobernador de la prefectura de Hokkaido será creado por varios controladores de claves secretas empleando el instrumental estipulado en el punto "6-1-1-3 Hardware/software de creación de doble clave" de estas normas operativas.

6-1-1-2 Longitud de claves

Se utilizará una clave de 2048 bits basándose en el sistema de encriptación RSA.

6-1-1-3 Hardware/software de creación de doble clave

Será un HSM con nivel 3 de FIPS 140-1.

6-1-1-4 Objetivos de uso de claves secretas

Se utilizarán en firmas digitales.

6-1-1-5 Recepción de la clave pública de la BCA de identificación personal

La CA de la prefectura de Hokkaido recibirá de forma segura y precisa la clave pública de la BCA de identificación personal en el intercambio de certificados de identificación recíproca.

6-1-1-6 Reparto de la clave pública del gobernador de la prefectura de Hokkaido

El certificado de firma propia del gobernador de la prefectura de Hokkaido se guardará en la tarjeta IC en el momento de la expedición del certificado digital y se le entregará al usuario. Además, se repartirá de forma segura y precisa a los verificadores de firmas.

6-1-2 Claves de los usuarios

6-1-2-1 Generador de la doble clave de los usuarios y método de creación

Será creada por el mismo usuario en el dispositivo generador de doble clave de los municipios de residencia.

6-1-2-2 Método de entrega segura de la clave pública de usuarios a municipios de residencia

Se recibirá personalmente del usuario la clave pública guardada dentro de la tarjeta IC en el municipio de residencia.

6-1-2-3 Longitud de claves

Se utilizará una clave de 1024 bits basándose en el sistema de encriptación RSA.

6-1-2-4 Hardware/software de creación de doble clave

Será el dispositivo generador de doble clave de los municipios de residencia.

6-1-2-5 Objetivos de uso de claves secretas

Se utilizarán en firmas digitales.

6-2 Protección de claves secretas

6-2-1 Clave secreta del gobernador de la prefectura de Hokkaido

6-2-1-1 Conservación de claves de secretas, estándares requeridos

Se protegerán con un HSM de nivel 3 de FIPS140-1.

6-2-1-2 Control por varias personas de claves secretas

Se protegerán las claves secretas en un HSM controlado por varios controladores de claves secretas.

6-2-1-3 Fideicomiso de claves secretas (Escrow)

No se podrá realizar fideicomiso con claves secretas.

6-2-1-4 Copia de respaldo de claves secretas

La copia de respaldo de claves secretas la efectuarán varios controladores de claves secretas.

Las copias de respaldo de clave secreta del HSM se encriptarán y conservarán de manera segura. Sin embargo, los controladores de claves secretas no podrán sacar las unidades en las que se guardan las copias de respaldo fuera de la habitación donde se deben ser conservados.

6-2-1-5 Conservación de claves secretas (archivos)

No se tendrán archivos con claves secretas.

6-2-1-6 Guardado de claves secretas en el módulo de encriptación

Las claves secretas se generarán en un HSM controlado por varios controladores de claves secretas y se guardarán en el módulo de encriptación.

6-2-1-7 Activación de claves secretas

Las claves secretas se activarán por varios controladores de claves secretas.

6-2-1-8 Desactivación de claves secretas

Las claves secretas se desactivarán por varios controladores de claves secretas.

6-2-1-9 Destrucción de claves secretas

La destrucción de claves secretas del módulo de encriptación se hará inutilizando totalmente su uso mediante una inicialización del módulo de encriptación por varios controladores de claves secretas. Además, en caso de transportar el módulo de encriptación fuera de la habitación, este deberá ser destruido físicamente.

También se deberá destruir de la misma forma los módulos de encriptación de copia de respaldo de dichas claves.

6-2-2 Claves secretas de los usuarios

6-2-2-1 Conservación de claves de secretas, estándares requeridos

Se protegerán mediante una tarjeta IC con una aplicación de tarjeta basada en el "Diseño del interfaz exterior de aplicaciones de tarjeta para el Servicio Público para la Identificación Personal Ver 1.1" y con sistema anti-intrusión que no permita la lectura de la clave de manera física.

6-2-2-2 Fideicomiso de claves secretas (Escrow)

El gobernador de la prefectura de Hokkiado no podrá recibir fideicomiso con claves secretas del usuario. Tampoco se aceptará el fideicomiso de claves secretas a terceros por parte del usuario.

6-2-2-3 Copia de respaldo de claves secretas

Las claves secretas se conservarán dentro de la tarjeta IC sin generar copia de respaldo.

6-2-2-4 Guardado de claves secretas en el módulo de encriptación (tarjeta IC)

Las claves secretas de los usuarios se crearán con el dispositivo generador de doble clave de los municipios de residencia y se guardarán en la tarjeta IC del usuario. Una vez la clave haya sido guardada en la tarjeta IC, la clave secreta creada en el dispositivo generador de doble clave deberá ser eliminada completamente.

6-2-2-5 Activación de claves secretas

La clave secreta de los usuarios se activará empleando la contraseña del usuario.

6-2-2-6 Desactivación de claves secretas

Se desactivará mediante el uso de la tarjeta IC.

6-2-2-7 Destrucción de claves secretas

En caso de querer destruir la clave secreta del usuario, el usuario deberá hacerlo desde la terminal de ventanilla y el dispositivo generador de doble clave del municipio de residencia.

6-3 Otros asuntos relacionados con el control de creación de doble clave

6-3-1 Claves del gobernador de la prefectura de Hokkaido

6-3-1-1 Conservación de claves públicas

La clave pública se incluirá en el certificado de firma propia y se conservará en unos archivos con medidas contra la manipulación de datos durante el periodo estipulado en el punto "4-12 Conservación de registros (archivo)" de estas normas operativas.

6-3-1-2 Periodo de utilización de claves públicas y secretas

La validez del certificado de firma propia del gobernador de la prefectura de Hokkaido será de 10 años. El periodo de utilización de la clave secreta será de 5 años contando desde el día de su creación y se renovará cada 5 años.

Sin embargo, en caso de que se determine que la seguridad de encriptación se ha debilitado, habrá casos en los que se considerará cambiar el sistema de encriptación y se renovará la clave en ese momento.

6-3-2 Claves de los usuarios

El periodo de utilización de las claves públicas y secretas de usuarios será de 3 años contando desde el día en que se crearon.

Sin embargo, en caso de que se determine que la seguridad de encriptación se ha debilitado, habrá casos en los que se considerará cambiar el sistema de encriptación y se renovará la clave en ese momento.

6-4 Datos de activación

6-4-1 Claves del gobernador de la prefectura de Hokkaido

6-4-1-1 Creación e instalación de datos de activación

Los datos de activación del HSM para el guardado de la clave secreta del gobernador de la prefectura de Hokkaido se configurarán empleando la clave de control.

6-4-1-2 Protección de datos de activación

La clave de control requerida para la activación del HSM para el guardado de la clave secreta del gobernador de la prefectura de Hokkaido se protegerá de forma segura.

6-4-2 Claves de los usuarios

6-4-2-1 Creación e instalación de datos de activación

Los datos de activación (contraseña) de la clave secreta de usuarios los introducirá en la tarjeta IC el mismo usuario mediante el dispositivo generador de doble clave cuando cree la doble clave.

6-4-2-2 Protección de datos de activación

Los datos de activación de la clave secreta de usuarios se cambiarán periódicamente y se conservarán de forma segura.

6-5 Control de seguridad de ordenadores

6-5-1 Requerimientos funcionales del control de seguridad

En los sistemas del CA de la prefectura de Hokkaido se deberá instalar un sistema operativo fiable, control de acceso, función de identificación y diferenciación del personal, función de recopilación de registros de supervisión y de datos de archivos y función de recuperación.

6-5-2 Evaluación de la seguridad de ordenadores

Se efectuarán evaluaciones de la seguridad del sistema según se estime necesario.

6-6 Control de seguridad del ciclo de vida

6-6-1 Control de seguridad en el desarrollo del sistema

El desarrollo, la corrección y las modificaciones de los sistemas de este servicio se deberán hacer con una organización fiable y bajo un ambiente adecuado según los procedimientos pertinentes. Para los sistemas desarrollados, corregidos o modificados se efectuarán pruebas en un ambiente de prueba y se implementarán los resultados una vez se haya recibido la aprobación del responsable de control de la autoridad certificadora. Además, las especificaciones del sistema y el informe de la prueba deberán quedar documentados y conservarse.

6-6-2 Control de seguridad en el empleo del sistema

6-6-2-1 CA de la prefectura de Hokkaido

Se harán pruebas de seguridad del sistema operativo y del software de forma periódica para asegurar el mantenimiento de este servicio. Además, los resultados de estas pruebas deberán quedar documentados y conservarse.

6-6-2-2 Municipios

Se efectuará un control de seguridad adecuado del sistema operativo y el software del dispositivo generador de doble clave y las terminales de ventanilla para asegurar el mantenimiento

de este servicio.

6-7 Control de seguridad de redes

Se reducirán al mínimo posible los servicios de red que permitan el paso a redes externas para prevenir los accesos no permitidos. Además, se tomarán las debidas medidas de seguridad empleando detectores de robo, etc.
La información a publicar que esté guardado en el repositorio se ofrecerá a través de un firewall.

6-8 Control técnico de módulos de encriptación

Queda definido en los puntos "6-1-1-3 Hardware/software de creación de doble clave" y"6-2-1-1 Conservación de claves de secretas, estándares requeridos" de estas normas operativas.

7. Contenidos de los certificados y los registros de invalidación (CRL/ARL)

7-1 Certificados

7-1-1 Certificados digitales

En los certificados digitales se anotarán los siguientes datos. Los detalles quedan determinados en el plano de perfiles.

- Nº de versión (Nº de versión del forma de certificado X.509)
- Nº de serie (Nº para la identificación de certificados ya expedidos dentro de la CA de la prefectura de Hokkaido)
- Algoritmos de firma (datos de algoritmos empleados en la firma de dicho certificado digital por el gobernador de la prefectura de Hokkaido)
- Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió dicho certificado digital quedará escrito con nombre de identificación X.500)
- Fecha de comienzo de validez (fecha en que se expide dicho certificado digital)
- Fecha de término de validez (3 años después de la fecha de expedición)
- Clave pública (clave pública del usuario)
- Datos de expansión (se anotarán las cuatro informaciones fundamentales y el objetivo de uso de la clave etc.)

7-1-2 Certificados de identificación recíproca

En los certificados de identificación recíproca requeridos para la identificación recíproca con la BCA de identificación personal se anotarán los siguientes datos. Los detalles quedan determinados en el plano de perfiles.

- Nº de versión (Nº de versión del forma de certificado X.509)
- Nº de serie (Nº para la identificación de certificados ya expedidos dentro de la CA de la prefectura de Hokkaido)
- Algoritmos de firma (datos de algoritmos empleados en la firma de dicho certificado de identificación recíproca por el gobernador de la prefectura de Hokkaido)
- Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió dicho certificado de identificación recíproca quedará escrito con nombre de identificación X.500)
- Fecha de comienzo de validez (fecha en que se valida dicho certificado de identificación recíproca)
- Fecha de término de validez (5 años después de la fecha en que se valida dicho certificado de identificación recíproca)
- Clave pública (clave pública de la CA de identificación recíproca)
- Datos de expansión

7-1-3 Certificados de firma propia

En los certificados de firma propia del gobernador de la prefectura de Hokkaido se anotarán los siguientes datos. Los detalles quedan determinados en el plano de perfiles.

- Nº de versión (Nº de versión del forma de certificado X.509)
- Nº de serie (Nº para la identificación de certificados ya expedidos dentro de la CA de la prefectura de Hokkaido)
- Algoritmos de firma (datos de algoritmos empleados en la firma de dicho certificado de firma propia por el gobernador de la prefectura de Hokkaido)
- Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió dicho certificado de firma propia quedará escrito con nombre de identificación X.500)
- Fecha de comienzo de validez (fecha en que se expide dicho certificado de firma propia)

・Fecha de término de validez (10 años después de la fecha en que se expide dicho certificado digital)
・Clave pública (clave pública del gobernador de la prefectura de Hokkaido)
・Datos de expansión

7-1-4 Certificados Link

En los certificados Link requeridos para renovar las claves del gobernador de la prefectura de Hokkaido se anotarán los siguientes datos. Los detalles quedan determinados en el plano de perfiles.

・Nº de versión (Nº de versión del forma de certificado X.509)
・Nº de serie (Nº para la identificación de certificados ya expedidos dentro de la CA de la prefectura de Hokkaido)
・Algoritmos de firma (datos de algoritmos empleados en la firma de dicho certificado Link por el gobernador de la prefectura de Hokkaido)
・Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió dicho certificado Link quedará escrito con nombre de identificación X.500)
・Fecha de comienzo de validez (OldWithNew: fecha de creación de la clave antigua, NewWithOld: fecha de creación de la clave nueva)
・Fecha de término de validez (OldWithNew: fecha de término de validez del certificado de firma propia antiguo, NewWithOld: fecha de término de validez del certificado de firma propia nuevo)
・Clave pública (OldWithNew: clave pública antigua, NewWithOld: clave pública nueva)
・Datos de expansión

7-2 Registros de invalidación (CRL/ARL)

7-2-1 Registros de invalidación (CRL) de certificados digitales

En los registros de invalidación (CRL) de certificados digitales se anotarán los siguientes datos. Los detalles quedan determinados en el perfil del CRL contenidos en el plano de perfiles.

・Datos de versión (Nº de versión de formato del CRL)
・Algoritmos de firma (datos de algoritmos empleados en la firma de dicho CRL por el gobernador de la prefectura de Hokkaido)
・Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió dicho CRL quedará escrito con nombre de identificación X.500)
・Fecha de comienzo de validez (fecha en que se valida dicho CRL)
・Fecha de término de validez (3 días después de la fecha en que se valida dicho CRL)
・Fecha prevista de renovación (día siguiente a la fecha en que se valida dicho CRL)
・Datos de certificados inválidos (Nº de serie, fecha de invalidación, razón de invalidación)
・Datos de expansión

7-2-2 Registros de invalidación (ARL) de certificados de identificación recíproca

En los registros de invalidación (ARL) de certificados de identificación recíproca se anotarán los siguientes datos. Los detalles quedan determinados en el perfil del ARL contenidos en el plano de perfiles.

・Datos de versión (Nº de versión de formato del ARL)
・Algoritmos de firma (datos de algoritmos empleados en la firma de dicho ARL por el gobernador de la prefectura de Hokkaido)
・Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió

dicho ARL quedará escrito con nombre de identificación X.500)
- Fecha de comienzo de validez (fecha en que se valida dicho ARL)
- Fecha de término de validez (3 días después de la fecha en que se valida dicho ARL)
- Fecha prevista de renovación (día siguiente a la fecha en que se valida dicho ARL)
- Datos de certificados inválidos (Nº de serie, fecha de invalidación, razón de invalidación)
- Datos de expansión

7-2-3 Registros de invalidación (ARL) de certificados de firma propia

En los registros de invalidación (ARL) de certificados de firma propia se anotarán los siguientes datos. Los detalles quedan determinados en el perfil del ARL contenidos en el plano de perfiles.

- Datos de versión (Nº de versión de formato del ARL)
- Algoritmos de firma (datos de algoritmos empleados en la firma de dicho ARL por el gobernador de la prefectura de Hokkaido)
- Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió dicho ARL quedará escrito con nombre de identificación X.500)
- Fecha de comienzo de validez (fecha en que se valida dicho ARL)
- Fecha de término de validez (3 días después de la fecha en que se valida dicho ARL)
- Fecha prevista de renovación (día siguiente a la fecha en que se valida dicho ARL)
- Datos de certificados inválidos (Nº de serie, fecha de invalidación, razón de invalidación)
- Datos de expansión

7-2-4 Registros de invalidación (ARL) de certificados Link

En los registros de invalidación (ARL) de certificados Link se anotarán los siguientes datos. Los detalles quedan determinados en el perfil del ARL contenidos en el plano de perfiles.

- Datos de versión (Nº de versión de formato del ARL)
- Algoritmos de firma (datos de algoritmos empleados en la firma de dicho ARL por el gobernador de la prefectura de Hokkaido)
- Datos del expedidor (el nombre del gobernador de la prefectura de Hokkaido que expidió dicho ARL quedará escrito con nombre de identificación X.500)
- Fecha de comienzo de validez (fecha en que se valida dicho ARL)
- Fecha de término de validez (3 días después de la fecha en que se valida dicho ARL)
- Fecha prevista de renovación (día siguiente a la fecha en que se valida dicho ARL)
- Datos de certificados inválidos (Nº de serie, fecha de invalidación, razón de invalidación)
- Datos de expansión

8. Control de las normas operativas

8-1 Control de cambios en las normas operativas

El gobernador de la prefectura de Hokkaido cambiará estas normas operativas según se estime necesario.

8-2 Muestras y notificaciones

En caso de cambiarse estas normas operativas, el gobernador de la prefectura de Hokkaido deberá publicar de forma inmediata las nuevas normas operativas en la Web. Con esto se notifica a los usuarios, verificadores de firmas y examinadores de firmas.

8-3 Procedimientos de aprobación de las normas operativas

Se validarán en el momento que el gobernador de la prefectura de Hokkaido lo determine.