ポルトガル語版

SERVIÇOS DE CERTIFICAÇÃO PÚBLICA PARA

INDIVÍDUOS PELO GOVERNO LOCAL

AUTORIDADE CERTIFICADORA DA PROVÍNCIA DE HOKKAIDO DECLARAÇÃO DE PRÁTICAS

Versão. 1.5

08 de Julho de 2013

PROVÍNCIA DE HOKKAIDO

Histórico da Revisão

Versão	Data	Conteúdo da Revisão
1.0	2004/01/29	1ª. edição impressa
1.1	2005/01/19	Revisão referente a implementação de alteração regulamentar
1.2	2006/11/01	~~Revisão referente a revisão da lei~~
1.3	2008/09/19	Revisão referente a atualização da chave secreta da autoridade certificadora
1.4	2009/04/01	Revisão referente a mudança de contato
1.5	2013/07/08	Revisão referente a execução da lei (Ano 2009 Lei No.77) para emendar uma parte da Lei do Livro de Registro Básico de Residentes

1.INTRODUÇÃO

Esta Declaração de Práticas define a política de administração dos serviços de certificação de cada autoridade certificadora estadual dos Serviços de Certificação Pública para Indivíduos (a seguir designada " Autoridade Certificadora (AC) da província de Hokkaido"). A fim de realizar a digitalização dos procedimentos de pedidos e notificações entre as instituições das entidades públicas estaduais ou locais, e os moradores, emite certificados digitais (a seguir designado como "certificado digital", o certificado do usuário) da pessoa registrada no Livro de Registro Básico de Residentes.

Além disso, a configuração/constituição desta Declaração de Práticas na IETF (Internet Engineering Task Force) de acordo com a PKIX(Public-Key Infrastructure X.509) Working Group, conforme/corresponde a RFC(Request For Comments) 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

No entanto, supõe-se que a parte que se refere a outras regras tenha um conteúdo de referência explícito, deixando apenas o título.

1-1 Sumário

A autoridade certificadora da província de Hokkaido, às pessoas registadas no Livro de Registro Básico de Residentes, pertencentes aos municípios dentro da área desta província , dependendo da solicitação, emite certificados digitais, e também emite certificados que são necessários para o funcionamento das AC de outras províncias. Ademais, para realizar a autenticação mútua e de outras autoridades certificadoras (de infraestrutura de autenticação pública, de cada unidade estadual) relacionadas aos Serviços de Certificação Pública para Indivíduos, se faz a troca pela emissão de certificados de autenticação mútua com a ponte de autoridade certificadora de Serviços de Certificação Pública para Indivíduos a ser instalado (a seguir designado "Certificação Para Indivíduos BCA").

Além disso, elabora *informações de revogação* (refere-se a informações relativas à revogação de certificados digitais. O mesmo se aplica para o seguinte), *registros de revogação* (LCR/LAR) (refere-se a informações registradas relativas à revogação de certificados digitais, etc. O mesmo se aplica para o seguinte) e *arquivos de informações de revogação* (refere-se ao arquivo de registro de informações (LCR) .O mesmo se aplica para o seguinte) e toma providências em resposta ao pedido do verificador da assinatura, previsto no artigo 17, parágrafo 4, ou do verificador de assinatura em grupo, previsto no parágrafo 6 º do mesmo artigo: "leis para os Serviços de Certificação das entidades públicas sobre assinatura digital" (a seguir designada como "Lei de base").

Também a Autoridade Certificadora da província de Hokkaido, não se supondo que a PC (política de certificação) e a DPC (Declaração de Práticas de Certificação) sejam independentes uma da outra, posiciona esta Declaração de Práticas como uma política administrativa de serviços de certificação da Autoridade Certificadora da província de Hokkaido

1-2 Identificação

O identificador da política de certificação da Autoridade Certificadora da província de Hokkaido deve ser a seguinte:

Política de certificação digital, etc. da AC da província de Hokkaido

Política de certificação digital e política de certificação de autenticação mútua da AC da província de Hokkaido

1.2.392.200149.8.5.1.1.10

Política de certificação digital para teste e política de certificação de autenticação mútua da AC da província de Hokkaido

1.2.392.200149.8.5.1.0.10

Política de certificação do servidor de verificação de certificado de posição governamental

1.2.392.200149.8.5.1.200

Política de certificação do servidor de verificação de certificado de posição governamental para teste

1.2.392.200149.8.5.1.0.200

Política de certificação respondedor OCSP

1.2.392.200149.8.5.1.300

Política de certificação respondedor OCSP para teste

1.2.392.200149.8.5.1.0.300

1-3 Sistema operacional e campo de aplicação do certificado

1-3-1 Participantes

(1) Ministro de Assuntos Internos e Comunicações

O Ministro de Assuntos Internos e Comunicações, pelas disposições de um decreto do método de base, faz a designação do órgão de certificação designado.

(2) Associação Estadual para JPKI

A Associação Estadual para JPKI (a seguir designada "Associação") realiza trabalhos relacionados à comunicação e coordenação em questões importantes sobre a implementação de uma administração centralizada do sistema de certificação pública para indivíduos

(3) Governador da Província de Hokkaido

O Governador da Província de Hokkaido tem a seguinte função na AC da província de Hokkaido (Autoridade Certificador da Província)

(4) AC da província de Hokkaido

AC da província de Hokkaido, em colaboração e cooperação mútua com os prefeitos de municípios, emite certificados digitais e outros tipos de certificados, faz registros de revogação（LCR/LAR）, realiza serviços como fornecer meios para confirmar a validade do certificado digital nas emissões de certificados e controle de registros de revogação.

Adota medidas de emergência em caso de desastres e também no comprometimento de chaves do Governador da Província de Hokkaido

Também, para o usuário, fornece um meio de confirmar a eficácia do certificado de responsabilidade e posições governamentais necessários na verificação da assinatura digital, quando este recebe documentos on-line dos órgãos das entidades públicas estaduais ou locais.

(5) Certificação Para Indivíduos BCA

A Certificação Para Indivíduos BCA, seguindo a declaração de práticas formulada pela Associação, realiza emissões tais como as de certificados da AC da província de Hokkaido de autenticação mútua das autoridades certificadoras de cada unidade estadual e de ponte de infraestrutura de certificação pública (a seguir designado "Infraestrutura de Certificação Pública BCA").

(6) Órgão de Certificação Designado

O Órgão de Certificação Designado, pelas disposições de uma Lei de Base em resposta à delegação do Governador, realiza trabalhos sobre a execução dos serviços de certificação (a seguir designado "Trabalhos de Certificação").

(7) Prefeitos de Municípios

Os prefeitos dos municípios dentro da área desta província de Hokkaido fazem a distribuição dos certificados digitais emitidos pela AC da província de Hokkaido, identificação do requerente, a aceitação de solicitação de emissão ou revogação de certificados digitais.

(8) Requerente / Usuário

De acordo com o previsto no artigo 3, parágrafo 1º da Lei de Base, o solicitante refere-se a pessoa que solicita a emissão do certificado digital. (A solicitação também pode ser realizada por um agente. No entanto, neste caso, "Decreto para a aplicação da lei para os Serviços de Certificação das entidades públicas sobre assinatura digital" (a seguir designado como "Regras da Lei de Base") e deverá atender aos requisitos do artigo 5.). O usuário refere-se a pessoa registrada no Livro de Registro Básico de Residentes que tenha obtido a emissão do certificado digital.

O usuário, quanto aos pedidos e notificações on-line entre as instituições das entidades públicas estaduais ou locais, pode utilizar os certificados digitais. Para o Órgão de Certificação Designado e o Governador da Província de Hokkaido, sobre as informações dos serviços de certificação referentes a eles próprios (refere-se ao registro de emissão de certificados digitais, informações de revogação de arquivo e informações de revogação. O mesmo se aplica para o seguinte), requer a divulgação desta Para obter informações de serviços de certificação relativas à divulgação, é possível requerer a inclusão ou exclusão ou a correção da totalidade ou de uma parte deste conteúdo. Também, se há objeção no trabalho de certificação, etc. é possível requerer uma investigação baseada na Lei do Recurso Administrativo para o Ministro dos Assuntos Internos e Comunicações. Além disso, confirma a eficácia do certificado de responsabilidade e posições governamentais necessária na verificação da assinatura digital, quando este recebe documentos on-line dos órgãos das entidades públicas estaduais ou locais.

(9) Verificador de Assinatura

Entre os seguintes, refere-se à pessoa que tenha sido concedido acesso, previamente notificado de acordo com o disposto no artigo 17, parágrafo 1º do método de base, para receber a disponibilização de meios a fim de confirmar a eficácia do certificado digital.

① Órgãos Administrativos, etc. (a seguir designado como "órgãos administrativos, etc.") previsto no artigo 2, Lei No. 2. Lei sobre o uso de Tecnologia de Informação e Comunicação em Procedimentos Administrativos, etc.

② Tribunal

③ Por causa dos itens que são necessários nos pedidos, notificações e outros procedimentos relacionados aos órgãos governamentais, recebe uma oferta pelo método eletromagnético e fornece isto, por si mesmo, aos órgãos governamentais. A pessoa que o órgão administrativo designou, registrou, autorizou e aprovou com base nas disposições da lei como a pessoa que realiza serviços de responder conforme a consulta.

④ Operadores de certificação acreditados, definidos no artigo 8 "Lei a respeito dos serviços de certificação e assinatura digital" (a seguir designado como "Lei de Assinatura Digital")

⑤ Aquele autorizado pelo Ministro dos Assuntos Internos e Comunicações, como estando em conformidade com os padrões estabelecidos
"Para a Aplicação da Lei para os Serviços de Certificação das entidades públicas sobre assinatura digital" (a seguir designado "Decreto de Lei de Base"), prescrito no artigo 2, parágrafo 3 º da lei de assinatura digital, para realizar serviços de certificação específicos.

⑥ A solicitação ao tribunal e órgãos administrativos é constituída por uma organização que fornece os procedimentos de notificação, solicitação e outros, exigidos no registro eletromagnético, estabelecida por um Decreto de Lei de Base.

A AC da província de Hokkaido por sua vez verifica a assinatura digital dos pedidos e notificações on-line do usuário, aceita o fornecimento de meios para confirmar a eficácia do certificado digital e faz a prestação de registros de revogação（LCR/LAR）.

(10) Verificador de assinatura

Refere-se à pessoa estabelecida por um Decreto de Lei de Base, de acordo com o disposto no artigo 17, Parágrafo 5º da Lei de Base.

O verificador de assinatura de grupo, estabelecido abaixo, verifica a assinatura digital dos pedidos e notificações on-line do usuário, aceita o fornecimento para confirmar os resultados da eficácia do certificado digital

(11) Verificador de assinatura de grupo

Entre os seguintes, refere-se à pessoa que tenha sido concedido acesso, previamente notificado de acordo com o disposto no artigo 17, parágrafo, 5º da Lei de Base, para receber a disponibilização de meios a fim de confirmar a eficácia do certificado digital.

① Estabelecida por um Decreto de Lei de Base, no grupo a que pertence, a pessoa que realiza entre outros, os procedimentos de notificação, solicitação ao tribunal e órgãos administrativos em resposta ao pedido de outros, em conformidade com as disposições da lei

② Estabelecida por um Decreto de Lei de Base, no grupo ou órgão a que pertence, a pessoa que fornece entre outros, os procedimentos de notificação, solicitação

exigidos no registro eletromagnético, ao tribunal e órgãos administrativos, etc.

A AC da província de Hokkaido, oferece entre outros, registros de revogação (LCR/LAR) , aceita o fornecimento de meios para confirmar a eficácia do certificado digital, confirma a eficácia dos certificados digitais anexados aos pedidos e notificações on-line enviados pelo revisor de assinatura que recebeu do usuário e notifica esse resultado ao titular

(12) Verificador de assinatura, etc.

Refere-se a um verificador de assinatura em grupo e também verificador de assinatura.

1-3-2 Aplicabilidade e ambiente de aplicação

Os tipos e usos/utilidades de serviço são os 4 a seguir:

① Emissão de certificados digitais para as seguintes aplicações:
- Assinaturas digitais dos pedidos e notificações on-line nos/dos procedimentos realizados nos tribunais e órgãos administrativos
- O verificador de assinatura faz a identificação
- O revisor de assinatura faz a identificação

O período de validade do certificado digital se faz vigente a partir da data que o certificado digital for emitido, por 3 anos.

② Emissão de certificados de autenticação mútua para as seguintes aplicações:
- Autenticação mútua e Infraestrutura de Certificação BCA, através da Certificação Para Indivíduos BCA. O período de validade do certificado de autenticação mútua se faz vigente a partir da data que o certificado de autenticação mútua for validado, por 5 anos.

③ Emissão de certificados de servidor de verificação/validação de certificados governamentais para as seguintes aplicações:
- Fornecimento de meios para confirmar a eficácia dos certificados de responsabilidade e posições governamentais necessária na verificação da assinatura digital, quando o usuário recebe documentos on-line dos órgãos das entidades públicas estaduais ou locais.

O período de validade do certificado de servidor de verificação/validação de certificados governamentais se faz vigente a partir da data que o certificado de servidor de verificação/validação de certificados governamentais for validada, por 1 ano.

④ Emissão de certificados respondedor OCSP para as seguintes aplicações:
- O verificador de assinatura fornece meios para confirmar a eficácia dos certificados digitais pelo método de consulta respondedor OCSP.

O período de validade do certificado respondedor OCSP se faz vigente a partir da data que o certificado respondedor OCSP for validada, por 1 ano.

1-3-3 Responsável pela Declaração de Práticas

O responsável por esta Declaração de Práticas é o Governador da Província de Hokkaido

1-3-4 Contato

Segue abaixo o guichê para consultas sobre esta Declaração de Práticas

Província de Hokkaido

Endereço: Kita 3-jo, Nishi 6-chome, Chuo-ku, Sapporo 060-8588
Departamento:Departamento de política geral O científico IT Agência de Promoção
Seção de política de informação
Horário de Atendimento: das 8h45min às 17h30min
Telefone: 011-204-5171
Fax: 011-232-3692
Endereço eletrônico: sogo.joho2@pref.hokkaido.lg.jp

2. Disposições Gerais

2-1 Obrigações

2-1-1 Obrigações do Ministro dos Assuntos Internos e Comunicações

(1) Designação do órgão de certificação designado, permissão para suspensão ou anulação, destituição da designação, notificação ao governador da província
(2) Ordens necessárias de supervisão ao órgão de certificação designado
(3) Relatórios necessários na execução de inspeções no local e exigências ao órgão de certificação designado
(4) Ordem de demissão e aprovação de eleição e demissão do oficial do órgão de certificação designado
(5) Ordem de mudança e também aprovação do plano de negócios da declaração operacional da certificação formulada do órgão de certificação designado
(6) Resposta a apelação referente a uma disposição que o órgão de certificação designado fez
(7) Desenvolvimento de normas técnicas para as instalações a serem utilizadas para os serviços de certificação
(8) Pesquisa, estudo sobre a avaliação da tecnologia referente aos serviços de certificação
(9) Trabalhos relacionados certificação do verificador de assinatura
(10) Solicitação de relatórios necessários sobre o estado de execução de serviços para o verificador de assinatura, etc.
(11) Publicidade e conhecimento para o usuário das informações relativas aos Serviços de Certificação Pública para Indivíduos

2-1-2 Obrigações do Governador da Província de Hokkaido

(1) Endereço, sexo, data de nascimento, nome do requerente pelo prefeito do município (a seguir designado como "Informação Básica 4 "(Se o requerente é residente estrangeiro, ou no caso em que um nome popular é listado no atestado de residência pertencente aos residentes estrangeiros, Nome Popular e Informação Básica 4. O mesmo se aplica para o seguinte) e emissão de certificados digitais com base na notificação da chave pública.
(2) Troca de certificado de autenticação mútua e apresentação de informações precisas referente a autenticação mútua entre a AC da província de Hokkaido e Certificação Para Indivíduos BCA
(3) Emissão de certificado assinado pelo próprio
(4) Emissão de certificado de ligação
(5) Emissão de certificado relacionado para a prática
(6) Elaboração de informações de revogação e identificação quando recebe solicitação de revogação do usuário on-line.
(7) Elaboração de informações de revogação quando recebe solicitação de revogação do usuário nos municípios
(8) Elaboração de informações de revogação em casos de morte e mudança de nome ou endereço do usuário
(9) Elaboração de informações de revogação nos casos em que, com relação aos itens do certificado digital do usuário, são encontradas características diferentes das registradas no dito certificado digital
(10) Relatório para Certificação Para Indivíduos BCA e elaboração de informações de revogação de todos certificados emitidos pela chave secreta nos casos de comprometimento de chaves do Governador da Província de Hokkaido (refere-se a

perda da chave secreta e devido a vazamentos, etc. se torna incontrolável ou quando há suspeita dessa. O mesmo se aplica para o seguinte)

(11) Fornecimento de registros de revogação（LCR/LAR）, método para confirmar a eficácia de certificados digitais para os verificadores de assinatura, etc. (método para responder a consulta de informações de revogação usando o protocolo OCSP (a seguir designado "método de consulta respondedor OCSP")).

(12) Fornecimento de métodos para confirmar a eficácia dos certificados de responsabilidade e posições governamentais dos órgãos das entidades públicas estaduais ou locais para o usuário

(13) Publicação e elaboração de relatório da disponibilidade de informações de revogação e seus respectivos arquivos

(14) Divulgação para solicitação da divulgação de informações de serviços de certificação

(15) Correção,. da solicitação da correção, de informações de serviços de certificação,etc.

(16) Controle seguro de chave secreta e geração de par de chaves do governador da província de Hokkaido

(17) Execução da auditoria, execução da melhoria com base nos resultados da auditoria

(18) Instalação de equipamentos para a execução de serviços de autenticação

(19) Basear-se nessa Declaração de Práticas com relação aos serviços de revogação, atualização e emissão de cada certificado.

(20) Período necessário de armazenamento referente a todos registros de revogação（LCR/LAR）e certificados já emitidos, bem como registros de auditoria sobre a revogação, atualização e emissão de cada certificado e período necessário de armazenamento para as informações serem armazenadas

(21)Ter como objetivo 24 horas de funcionamento estável em que a monitorização de operação do sistema seja realizada com precisão todas as vezes

(22)Emitir a cada 24 horas as informações de revogação que tem a validade de 72 horas do registro de revogação（LCR/LAR）.

(23) Resposta as consultas e reclamações do usuário

(24) Notificação pública, relatório ao Ministro dos Assuntos Internos e Comunicações e comissão de trabalhos de certificação para o órgão de certificação designado

(25) Notificação de mudança e informação de revogação do órgão de certificação designado

(26) Instruções ao órgão de certificação designado se necessário

(27) Relatórios necessários na execução de inspeções no local e exigências ao órgão de certificação designado

(28) Notificação pública, relatório ao Ministro dos Assuntos Internos e Comunicações e cancelamento da comissão para o órgão de certificação designado

(29) Aprovação do fornecimento de informações de taxas e taxa definida de emissão de certificado do órgão de certificação designado

(30) Distribuição e execução de consulta das despesas de trabalho de certificação do órgão de certificação designado

(31) Execução do trabalho de certificação no caso do órgão de certificação designado anular ou suspender o trabalho de certificação

(32) Conclusão de acordos com o verificador de assinatura, etc.

(33) Solicitação de relatórios necessários sobre o estado de execução de serviços para o verificador de assinatura, etc.

(34) Manuseio adequado das informações sobre os serviços de certificação

(35) Sigilo das informações dos serviços de certificação
(36) Publicidade e conhecimento para o usuário das informações relativas aos Serviços de Certificação Pública para Indivíduos
(37) Decisão e elaboração dessa Declaração de Práticas

2-1-3 Obrigações do prefeito do município

(1) Identificação (identidade, veracidade) do requerente de revogação e do requerente na revogação e emissão
(2) Confirmação de que o procurador do requerente é um representante genuíno
(3) Sobre a solicitação de revogação, confirmação de requisitos de revogação
(4) Confirmação de que os outros procedimentos da solicitação estão sendo realizados corretamente
(5) Fornecimento de um aparelho para gerar um par de chaves que tenha resistência adequada (aparelho para gerar um par de chaves do requerente, (a seguir designado "aparelho gerador de par de chaves").
(6) Notificação ao governador da província de Hokkaido do requerente da chave pública e do requerente da Informação Básica 4
(7) Notificação ao governador da província de Hokkaido da solicitação de revogação
(8) Distribuição ao usuário do certificado assinado pelo próprio governador da província de Hokkaido e certificado digital
(9) Explicação ao usuário / requerente das penalidades relacionadas ao uso ilegal, restrição do propósito de uso de certificados digitais
(10) Manutenção do sistema de controle de segurança dos terminais de recepção e aparelho gerador de par de chaves
(11) Execução da auditoria, execução da melhoria com base nos resultados da auditoria
(12)Manuseio adequado das informações sobre os serviços de certificação
(13) Sigilo das informações dos serviços de certificação
(14) Cobrança da taxa de emissão pelo requerente do certificado digital emitido
(15) Aceitação de solicitação, etc. de correção e solicitação da divulgação de informações dos serviços de certificação
(16) Inicialização da senha baseada na solicitação do usuário, desbloqueio (refere-se a liberação do estado no qual o cartão IC fica inutilizável, como medida de prevenção de abuso quando houve falsa entrada da senha por mais de 5 vezes.), remoção, tais como de pares de chaves
(17) Apoio ao usuário na obtenção de software para o cliente usuário (software necessário na utilização do certificado digital) do terminal do usuário
(18) Resposta as consultas e reclamações do usuário
(19) Publicidade e divulgação, para o usuário, das informações relativas aos Serviços de Certificação Pública para Indivíduos

2-1-4 Obrigações do órgão de certificação designado

(1)Execução do trabalho de certificação, pela comissão do Governador da Província de Hokkaido (execução dos itens (1) ao (13), (16) e (18) ao (22) do "2-1-2 Obrigações do Governador da Província de Hokkaido dessa Declaração de Práticas)
(2) Desenvolvimento de regulamentos administrativos de certificação
(3) Apresentação de liquidação de contas e relatório de negócios e elaboração de orçamento de despesas e plano de negócios
(4) Instalação de comissão de proteção de informações de serviços de certificação

(5) Manuseio adequado das informações sobre os serviços de certificação
(6) Sigilo das informações dos serviços de certificação
(7) Divulgação para solicitação da divulgação de informações de serviços de certificação
(8) Correção, etc. para a solicitar a correção, etc. de informações de serviços de certificação
(9) Correspondência às consultas e reclamações do usuário
(10) Cobrança da taxa de fornecimento de informações pelo verificador de assinatura, etc.

2-1-5 Obrigações do usuário

(1) Descrição exata do conteúdo ao solicitar a emissão do certificado digital, revogação, etc.
(2) Controle seguro do cartão IC que contém a chave secreta
(3) Controle seguro e mudança regular de senha para ativar a chave secreta armazenada no cartão IC
(4) Rápida solicitação de revogação como nos casos de comprometimento da chave secreta
(5) Proibição do uso do certificado digital para outros fins
(6) Pagamento da taxa de emissão

2-1-6 Obrigações do verificador de assinatura

(1) A verificação da assinatura digital foi concedida por meio de um certificado digital emitido pela AC da província de Hokkaido
(2) Verificação da assinatura digital do certificado digital emitido pela AC da província de Hokkaido (se o dito certificado digital foi ou não emitido pelo governador da província de Hokkaido, se o dito certificado digital foi revogado ou não)
(3) Proibição do uso do certificado digital para outros fins que não sejam os de realizar a certificação do usuário através da realização de uma verificação da assinatura digital quando pedidos e notificações, etc. on-line são feitos pelo usuário
(4) Conclusão de acordos com o governador da província de Hokkaido ao receber a oferta de informações de revogação e seus respectivos arquivos
(5) Execução e aceitação dos requisitos de informação provenientes do Governador da Província de Hokkaido e do Ministro dos Assuntos Internos e Comunicações
(6) Uso adequado e sigilo tais como os de informações de revogação
(7) Garantir a segurança tais como a de informações de revogação
(8) Pagamento da taxa de fornecimento de informações

2-1-7 Obrigações do verificador de assinatura de grupo

(1) Confirmar se não houve revogação do certificado digital emitido pelo Governador da Província de Hokkaido
(2) Proibição do uso do certificado digital para outros fins que não sejam os de realizar a certificação do usuário através da realização de uma verificação da assinatura digital que o usuário recebeu do revisor de assinatura
(3) Conclusão de acordos com o governador da província de Hokkaido ao receber a oferta de informações de revogação e seus respectivos arquivos
(4) Execução e aceitação dos requisitos de informação provenientes do Governador da Província de Hokkaido e do Ministro dos Assuntos Internos e Comunicações

(5) Uso adequado e sigilo tais como os de informações de revogação
(6) Garantir a segurança tais como a de informações de revogação
(7) Pagamento da taxa de fornecimento de informações

2-1-8 Obrigações do revisor de assinatura

(1) A verificação da assinatura digital foi concedida por meio de um certificado digital emitido pela AC da província de Hokkaido
(2) Verificação da assinatura digital do certificado digital emitido pela AC da província de Hokkaido (se o dito certificado digital foi ou não emitido pelo governador da província de Hokkaido , se o dito certificado digital foi revogado ou não)
(3) Proibição do uso do certificado digital para outros fins que não sejam os de realizar a certificação do usuário através da realização de uma verificação da assinatura digital quando pedidos e notificações, etc. on-line são feitos pelo usuário
(4) Uso adequado e sigilo das respostas recebidas pelo verificador de assinaturas de grupo
(5) Garantir a segurança das respostas recebidas pelo verificador de assinaturas de grupo

2-1-9 Obrigações do repositório

A AC da província de Hokkaido, após elaborar o registro de revogação (LCR/LAR) , ao publicar no repositório, possibilita o verificador de assinatura confirmar a eficácia do certificado digital.

2-2 Responsabilidades

2-2-1 Responsabilidade do Ministro dos Assuntos Internos e Comunicações

O Ministro de Assuntos Internos e Comunicações, pelas disposições de um decreto do método de base, faz a designação do órgão de certificação designado e é responsável pelo controle e supervisão desse para realizar trabalhos de certificação seguros e adequados

2-2-2 Responsabilidade do governador da província de Hokkaido

O governador da província de Hokkaido, para com o verificador de assinatura e também para com o usuário, quando do fornecimento de meios para confirmar a eficácia dos certificados (de responsabilidade, posições governamentais e digitais) na emissão de certificados necessários para a operação de serviços entre outros, certificados digitais, de autenticação mútua, assinado pelo próprio Governador, de ligação e na elaboração de registros de revogação (LCR/LAR) em conformidade com esses certificados, realiza os serviços, de forma adequada, baseando-se nessa Declaração de Práticas.

Além disso, se se faz uma comissão de trabalhos de certificação, é responsável pelo controle e supervisão do órgão de certificação designado para realizar trabalhos de certificação seguros e adequados

2-2-3 Responsabilidades do prefeito de um município

O prefeito de um município, com relação a aceitação de pedidos de revogação e

emissão de certificados digitais, mediante identificação, etc. realiza os serviços de forma adequada, baseando-se nessa Declaração de Práticas

2-2-4 Responsabilidades do órgão de certificação designada

O órgão de certificação designado em resposta ao mandato do Governador realiza os seguintes trabalhos de certificação: para com o verificador de assinatura e também para com o usuário, quando do fornecimento de meios para confirmar a eficácia dos certificados (de responsabilidade, posições governamentais e digitais), na emissão de certificados necessários para a operação de serviços entre outros, certificados digitais, de autenticação mútua, assinado pelo próprio Governador, de ligação e na elaboração de registros de revogação (LCR/LAR) em conformidade com esses certificados, realiza os serviços de forma adequada, baseando-se nessa Declaração de Práticas.

2-2-5 Responsabilidades do usuário

O usuário utiliza este serviço de acordo com essa Declaração de Práticas.

2-2-6 Responsabilidades do verificador de assinatura

O verificador de assinatura verifica os certificados digitais de acordo com essa Declaração de Práticas.

2-2-7 Responsabilidades do verificador de assinatura de grupo

O verificador de assinatura de grupo confirma a eficácia dos certificados digitais de acordo com essa Declaração de Práticas.

2-2-8 Responsabilidades do revisor de assinatura

O revisor de assinatura verifica os certificados digitais de acordo com essa Declaração de Práticas.

2-3 Responsabilidades financeiras

O governador da província de Hokkaido não assume qualquer responsabilidade por danos causados pelo ato sem razões imputáveis a responsabilidade da AC da província.

Se houver razões imputáveis a responsabilidade da AC da província, supõe-se que o governador da província de Hokkaido indenize na medida estabelecida em leis e regulamentos.

2-4 Interpretação e execução

2-4-1 Legislação aplicável

Confia na Lei de Base e outras leis e regulamentos aplicáveis

2-4-2 Subdivisão e integração de serviço, notificação e mudança do sistema operacional

Quando há mudança, etc. no sistema operacional, anuncia ao usuário e ao verificador de assinatura, etc. o mais rápido possível, das seguintes maneiras:

- Web da Associação
- Web da Província de Hokkaido

Também, o órgão de certificação designado, se há mudança deste nome ou da localização da sede principal, o Governador da Província de Hokkaido e Ministro dos

Assuntos Internos e Comunicações são informados.

2-4-3 Aceitação da ordem de supervisão e inspeção do local e elaboração de relatório

Se houver ordens necessárias para a supervisão da execução de serviços de certificação, etc. do Ministro dos Assuntos Internos e Comunicações e se receber instruções à adequada execução do trabalho de certificação do Governador da Província de Hokkaido, o órgão de certificação designado deverá aceitar isto.

2-4-4 Procedimentos de resolução de disputa

No caso de surgir um processo sobre esta Declaração de Práticas, todas as partes ficarão à jurisdição exclusiva do tribunal de primeira instância, o tribunal distrital de Sapporo

2-5 Tarifas

As tarifas referentes a divulgação de informações de serviços de certificação, fornecimento de informações de revogação e de seus respectivos arquivos e emissão de certificados digitais, devem ser fornecidas de acordo com os regulamentos da Lei de Base.

2-6 Publicação e Repositório

2-6-1 Publicação de informações da Autoridade Certificadora (AC) da província

A AC da província de Hokkaido publica as seguintes informações, na Web da Associação:

- Lei de Base e leis e regulamentos aplicáveis
- Esta Declaração de Práticas
- Nome da AC que fez a autenticação mútua com a AC da província de Hokkaido
- Nome da AC que fez o cancelamento a autenticação mútua com a AC da província de Hokkaido
- Informações referentes ao comprometimento da chave secreta do Governador da Província de Hokkaido

A AC da província de Hokkaido publica as seguintes informações no repositório dos Serviços de certificação pública para Indivíduos:

- certificados de assinatura própria
- certificados de autenticação mútua
- certificados de ligação
- (LAR) registros de revogação dos certificados de ligação, de autenticação mútua e de assinatura própria
- registros de revogação (LCR) de certificados digitais, tais como do usuário

2-6-2 Frequência de publicação

A frequência de atualização das informações a serem publicadas deve ser a seguinte:

- Os regulamentos desta Declaração de Práticas e as leis e regulamentos aplicáveis bem como a Lei de Base publicam na Web sempre as suas versões mais recente
- Publicam a cada atualização / emissão os certificados de ligação, de autenticação mútua e assinados por ela própria

・Atualizam-se 1 vez por dia, todos os dias, os registros de revogação（LCR/LAR）

2-6-3 Controles de acesso à publicação de informações

Com relação aos regulamentos desta Declaração de Práticas e as leis e regulamentos aplicáveis bem como a Lei de Base, não se estabelecem restrições de acesso. No repositório, também, não se estabelecem restrições de acesso às seguintes informações:

・certificados de assinatura própria
・certificados de autenticação mútua
・certificados de ligação
・(LAR) registros de revogação dos certificados de ligação, de autenticação mútua e de assinatura própria

No entanto, quando se publica no repositório o registro de revogação (LCR) do certificado digital do usuário, restringe-se o acesso.

2-6-4 Requisitos para o repositório

O repositório está disponível durante 1 ano, 365 dias, 1 dia, 24 horas. No entanto, em alguns casos de manutenção periódica, etc. o repositório não está disponível temporariamente.

2-7 Auditoria de conformidade

2-7-1 Frequência de Auditoria de conformidade

O Governador da Província de Hokkaido realiza auditorias de conformidade pelo auditor periodicamente, 1 vez por ano

E, além da auditoria periódica, se necessário, a auditoria é realizada a qualquer momento.

2-7-2 Identificação e qualificação do auditor

A auditoria da AC da província de Hokkaido é realizada pelos especialistas em serviços de certificação e serviços de auditoria.

2-7-3 Relacionamento do departamento auditado e auditores

OGovernador da Província de Hokkaido seleciona como auditor uma pessoa que não tenha interesse com a AC da província de Hokkaido

2-7-4 Itens de auditoria

Os serviços de certificação conduzem principalmente, o que é realizado em conformidade com esta Declaração de Práticas e as leis e regulamentos aplicáveis bem como a Lei de Base.

2-7-5 Manuseio dos resultados da auditoria

Os resultados da auditoria são entregues na forma de relatório de auditoria ao Governador da Província de Hokkaido pelo auditor. O Governador da Província de Hokkaido informa o relatório de auditoria ao órgão de certificação designado e a cada prefeito de município, se necessário.

2-7-6 Resposta aos resultados da auditoria

O órgão de certificação designado confirma os resultados da auditoria e fornece

respostas apropriadas à urgência e importância destes. O Governador da Província de Hokkaido confirma se o órgão de certificação designado está implementando medidas com relação aos resultados da auditoria.

2-8 Proteção de informações pessoais e sigilo

2-8-1 Informações consideradas sigilosas e manuseio de dados pessoais

A AC da província de Hokkaido considera como sigilosas informações que, devido ao vazamento, podem ter a confiabilidade dos serviços de certificação da AC da província de Hokkaido comprometida. Também protege adequadamente os dados pessoais do usuário.

As informações, incluindo dados pessoais e informações sigilosas, estabelecer o representante administrativo de mídia de armazenamento eletromagnéticas e documentos que contêm as ditas informações (Refere-se ao representante administrativo da autoridade certificadora desta Declaração de Práticas, no item" 5-2-1 , pessoal da AC da província de Hokkaido") para controlar com segurança. Quando há vazamento de dados pessoais, toma medidas com base no procedimento indicado separadamente

2-8-2 Informações que não são consideradas sigilosas

Nas informações mantidas pela AC da província de Hokkaido , não são consideradas sigilosas aquelas apresentadas explicitamente como informações a serem publicadas tais como esta Declaração de Práticas, certificados assinados por ela própria, de ligação, de autenticação mútua, do servidor de verificação de certificado de posição governamental, do respondedor OCSP e as respectivas informações de revogação destes certificados.

2-8-3 Publicação de informações de revogação de certificados

AC da província de Hokkaido publica informações de revogação de certificados relacionados para a operação e certificados assinados por ela própria, de ligação, de autenticação mútua a serem emitidos. Os detalhes do motivo da revogação não são publicados. Também as informações de revogação dos certificados digitais limitam-se ao verificador de assinatura e fornecem, baseando-se na Lei de Base.

2-8-4 Aplicação da lei na divulgação de informações

Não se aplica.

2-8-5 Divulgação de informações do processo civil

Não se aplica

2-8-6 Divulgação de informações baseada no princípio da terceira parte confiável

Se houver um pedido do usuário de divulgação das informações de serviços de certificação dele mesmo, faz-se a identificação e divulga.

2-8-7 Divulgação de informações baseada em outras razões

Não se aplica.

2-8-8 Correção de informações baseada no princípio da terceira parte confiável

Se houver um pedido do usuário tal como o de correção das informações de serviços de certificação dele mesmo, faz-se a identificação e realiza-se a correção.

2-9 Direito de propriedade intelectual

Não se aplica.

3. Identificação e certificação

3-1 Registro do primeiro certificado emitido

3-1-1 Tipos de nomes

O nome do usuário e o nome de publicação do certificado digital são definidos de acordo com o formato Nome Distinto X.500 (ND: Nome Distinto).

3-1-2 Requisitos para o significado de nomes

O nome de publicação do certificado digital é registrado de acordo com o cargo oficial do Governador.

subjectAltName		
	common Name	Nome (Se o usuário é residente estrangeiro ou no caso em que um Nome Popular é listado no atestado de residência pertencente aos residentes estrangeiros, Nome e Nome Popular)
	dateOfBirth	Data de Nascimento
	gender	Sexo
	address	Endereço

3-1-3 Regras para interpretação do formato do nomes

Segue as regras do Nome Distinto X.500.

3-1-4 Singularidade de Nomes

Atribui-se um único campo de assunto do certificado digital emitido pela AC da província de Hokkaido

3-1-5 Procedimentos de resolução de disputa de nomes

Não se aplica.

3-1-6 Reconhecimento, certificação e papel de marcas registradas

Não se aplica.

3-1-7 Tipo e formato de nomes registrados na área de expansão do certificado digital

Registram-se em números arábicos, alfabeto, Katakana, Hiragana e Kanji o nome do usuário, Nome Popular (Limita-se a pessoa que tem intenção de receber o certificado digital e é residente estrangeiro ou, no caso em que um nome popular é listado no atestado de residência pertencente aos residentes estrangeiros), endereço, data de nascimento e sexo.

3-1-8 Regras sobre o método de registro na área de expansão do certificado digital

Os Kanjis utilizados no registro de nomes, etc. são aqueles que só estão disponíveis os tipos de caracteres （JISX0208、JISX0212）dos Kanjis que os terminais de recepção dos domicílios dos municípios adotam

Caso haja no nome algum Kanji, etc. que não se possa utilizar, utiliza-se Kanji semelhante existente (a seguir designado “Caractere Alternativo”), baseado na escolha do usuário.

Se utilizar o “Caractere Alternativo”, exibir este fato na área de expansão.

3-1-9 Requisitos para a identificação e certificação do usuário

Na 1ª vez do requerimento de emissão, a identificação do requerente ocorre da seguinte maneira:

No entanto, se surgirem dúvidas quanto a identificação, não se emite o certificado digital.

① Ao se fazer a combinação dos itens registrados no Livro de Registro Básico de Residentes com a Informação básica 4 escrita na solicitação de emissão, confirmar se a pessoa registrada no Livro de Registro Básico de Residentes é a dita requerente (Confirmação da Realidade).

② Confirmar pela apresentação, etc. de documento emitido por órgão público com foto anexa como o de identificação (documentos que estão previstos no artigo 6, Parágrafo 1 º das Regras da Lei de Base) que o requerente é a própria pessoa que está registrada no Livro de Registro Básico de Residentes (Confirmação da Identidade).

3-1-10 Requisitos para a identificação e certificação em caso de solicitação por representação

No caso de solicitação por um agente, a identificação do agente e a confirmação da presença da agência ocorrem da seguinte maneira:

① Procuração com o carimbo e assinatura do requerente em pessoa, certificado de registo de carimbo referente à logomarca, ao dito requerente, confirmação dos documentos que o prefeito do domicílio municipal considera adequados e carta de resposta ao que foi consultado por escrito

② Confirmação da identificação do agente, pela apresentação de documento de identificação, etc. (documentos que estão previstos no artigo 5, Parágrafo 1 º das Regras da Lei de Base) com foto anexada, emitido por órgão público.

3-1-11 Procedimento de verificação para comprovar a posse de chave secreta

O usuário, utilizando o aparelho gerador de par de chaves que está instalado no domicílio municipal, baseando-se na Lei de Base e outras leis e regulamentos aplicáveis, faz gerar um par de chaves.

3-2 Atualização do Certificado Digital

Na atualização do certificado digital, a identificação do usuário ocorre das seguintes maneiras:

*No entanto, se surgirem dúvidas quanto a identificação, não se emite o certificado digital.

① Ao se fazer a combinação dos itens registrados no Livro de Registro Básico de Residentes com a Informação básica 4 escrita na solicitação de atualização, confirmar se a pessoa registrada no Livro de Registro Básico de Residentes é a dita requerente (Confirmação da Realidade).

② Confirmar pela apresentação do documento como o de identificação com foto anexa, emitido por órgão público que o requerente é a própria pessoa que está

registrada no Livro de Registro Básico de Residentes (Confirmação da Identidade).

Deve notar-se que a chave secreta de acordo com o certificado digital expira, com a atualização, o usuário a apaga por um método predeterminado

3-3 Nova emissão após a revogação

Realiza-se o procedimento de identificação semelhante ao de nova emissão, no momento da solicitação.

3-4 Solicitação de revogação

3-4-1 Solicitação de revogação de retirada de utilização do serviço

É realizada por solicitação escrita no guichê do domicílio municipal ou solicitação on-line que é indicado pela assinatura digital da chave secreta do usuário.

A identificação do usuário é realizada através da verificação assinatura digital para solicitação on-line. No caso de uma solicitação por escrito na janela do domicílio municipal, é realizada através de um procedimento de identificação semelhante ao da emissão de certificados digitais.

3-4-2 Solicitação de revogação para o caso de comprometimento de chave secreta do usuário

Imediatamente dirija-se a janela de domicílio municipal para realizar a solicitação da revogação por escrito.

A identificação do usuário é realizada através de um procedimento de identificação semelhante ao da emissão de certificados digitais.

4. Requisitos operacionais

4-1 Solicitação de emissão de certificado digital

4-1-1 Solicitação de emissão / procedimento de aceitação

A solicitação de emissão / procedimento de aceitação dos certificados digitais são realizadas da seguinte maneira:

① O requerente submete um cartão IC e também uma solicitação emitida pelo domicílio municipal. No caso de atualização, submete um cartão IC armazenado pelo certificado digital.

② O prefeito do domicílio municipal, ao combinar os conteúdos gravados do Livro de Registro Básico de Residentes, além de confirmar a existência do usuário, realiza-se a confirmação da identidade do requerente pela apresentação de documentação de identificação com a foto anexa emitida por um órgão público, tal como passaporte, a carteira de motorista, etc. No entanto, se surgirem dúvidas quanto a identificação, não se emite o certificado.

③ O usuário, utilizando o aparelho gerador de par de chaves que se compõe no guichê do domicílio municipal, gera o par de chaves. Do par de chaves gerados, notifica no guichê do domicílio municipal a chave pública.

Além disso, através do procedimento seguinte, a solicitação também pode ser realizada por um agente. No entanto, com relação aos （1）e（2）, se surgirem dúvidas quanto a identificação, não se emite o certificado.

(1) O agente, procuração com o carimbo e assinatura do requerente em pessoa (limita-se ao carimbo estar anexado ao certificado de registro de carimbo) e para confirmar a identificação do agente, apresentar ou exibir o passaporte ou carteira de motorista.

(2) O agente, sobre a solicitação da emissão de certificados digitais, a fim de confirmar que a dita solicitação baseia-se na intenção da própria pessoa e que o requerente é ele mesmo, por métodos que o prefeito do domicilio municipal considera apropriados como o correio e outros, apresenta documentos e submete a sua carta de resposta ao que foi consultado para o dito requerente.

(3) O agente gera o par de chaves, utilizando o aparelho gerador de par de chaves, e notifica o domicilio municipal. No entanto, o prefeito do domicilio municipal digita a senha (ativação da chave secreta).

4-1-2 Estilo de solicitação de emissão, itens necessários mencionados

Ao requerente da emissão estabelece-se o seguinte:

・Data da solicitação

・Nome (Furigana), Nome Popular (Limita-se a pessoa que tem intenção de receber o certificado digital e é residente estrangeiro ou, no caso em que um nome popular é listado no atestado de residência pertencente aos residentes estrangeiros), endereço, data de nascimento e sexo.

Nome, Nome Popular, endereço de acordo com o Caractere Alternativo

・No caso de solicitação pelo agente, além do referido acima, nome do agente e endereço.

4-1-3 Mídia de gravação eletromagnética das chaves privadas

Armazena-se o cartão IC com algo inviolável.

4-2 Emissão do certificado digital

4-2-1 Procedimentos de emissão

O procedimento de emissão do certificado digital ocorre da seguinte maneira:

① O prefeito do domicilio municipal notifica a chave pública e a Informação Básica 4 do requerente ao Governador da Província de Hokkaido.

② O Governador da Província de Hokkaido emite o certificado digital e notifica o prefeito do domicilio municipal.

4-2-2 Formato do certificado digital

De acordo com X.509 (03/2000), recomendação ITU-T, na área de expansão do usuário, registram-se o nome do usuário, Nome Popular, Endereço, Data de nascimento, sexo em números arábicos, alfabeto, Hiragana Katakana e Kanji.

E, no caso de usar Caractere Alternativo no registro do nome, Nome Popular, Endereço registrados na área de expansão, registra-se estes fatos na área de expansão.

subjectAltName		
		Nome (Se o usuário é residente estrangeiro ou no caso em que um Nome Popular é listado no atestado de residência pertencente aos residentes estrangeiros, Nome e Nome Popular)
	dateOfBirth	Data de Nascimento
	gender	Sexo
	address	Endereço
	substituteCharacterOfCommonName	Informação de uso do caractere alternativo do nome
	substituteCharacterOfAddress	Informação de uso do caractere alternativo do endereço

4-2-3 Negação da solicitação de emissão

O Governador da Província de Hokkaido nega a solicitação de emissão quando os seguintes motivos são aplicáveis:

・Já obteve um certificado digital válido, mas não foi publicado no registro de revogação (LCR)

No caso, se for emitido 2 vezes, porventura, o Governador da Província de Hokkaido deverá revogar imediatamente o certificado digital da data mais recente, assim que encontrá-lo.

4-3 Entrega do certificado digital

4-3-1 Procedimentos de entrega

A distribuição do certificado digital se realiza da seguinte maneira:

① O prefeito do domicilio municipal registra o certificado assinado pelo próprio Governador da Província de Hokkaido e o certificado digital no cartão IC do

requerente.

② Ao requerente, o prefeito do domicilio municipal distribui a cópia do certificado digital e também avisa as observações em relação a este serviço

4-3-2 Avisos

O prefeito do domicilio municipal ao usuário, observa o seguinte:

・Deve ser rigorosamente controlada sob a responsabilidade do usuário, a senha para ativar o cartão IC, sua mídia de gravação eletromagnética, e a chave secreta

・Quando há perda ou roubo da chave secreta ou do cartão IC que é a sua mídia de gravação eletromagnética, realizam-se a solicitação de revogação e a notificação ao guichê do domicilio do município, sem demora.

4-4 Suspensão e revogação de certificado digital

4-4-1 Razão da revogação da autoridade

4-4-1-1 Razão da revogação da autoridade

As razões da revogação da autoridade do certificado digital são as seguintes:

・mudança da "Informação Básica 4" do usuário

・se itens como os que estão descritos no certificado digital do usuário forem encontrados, sendo diferentes dos itens contidos no Atestado de Residência do usuário

・caso encontre um certificado digital emitido por 2 vezes

・comprometimento da chave secreta do Governador da Província de Hokkaido

4-4-1-2 Quem pode revogar um certificado

O Governador da Província de Hokkaido realiza.

4-4-1-3 Procedimentos de revogação devido ao comprometimento da chave secreta do Governador da Província de Hokkaido

Se houver o comprometimento da chave secreta do Governador da Província de Hokkaido revogar pela autoridade oficial todos os certificados digitais assinados com a chave secreta, além de registrar na revogação de registros, publicar estes fatos na Web, etc.

4-4-2 Revogação por solicitação do usuário

4-4-2-1 Revogação por solicitação do usuário

As razões da solicitação de revogação são as seguintes:

・solicitação do usuário para cancelar o uso deste serviço

・solicitação segundo a qual havia o comprometimento da chave secreta do usuário

4-4-2-2 Procedimentos para solicitação de revogação para retirar a utilização do serviço

Para procedimentos de revogação para retirar a utilização do serviço, é realizada por uma das duas maneiras.

① Aceita solicitação on-line em que é dada a assinatura digital. Notificar on-line o usuário, o fato de ter recebido a solicitação de revogação.

③ Aceitar uma solicitação de revogação por escrito no balcão do domicílio

municipal. Pedir para o Governador da Província de Hokkaido o processamento da revogação. Entregar documento ao usuário informando o fato de que recebeu a solicitação de revogação.

4-4-2-3 Procedimentos de solicitação de revogação devido ao comprometimento da chave secreta do usuário

Caso haja comprometimento da chave secreta do usuário, os procedimentos de revogação são os seguintes:

② Aceitar uma solicitação de revogação por escrito no domicílio municipal.

③ Pedir para o Governador da Província de Hokkaido o processamento da revogação. Entregar documento ao usuário informando o fato de que finalizou o processo de revogação.

4-4-2-4 Meios de recuperação quando o certificado digital do usuário expirou

Uma vez feito o processamento de revogação, a recuperação do certificado digital não é realizada, emitindo um novo certificado digital, mediante novo procedimento de solicitação.

4-4-2-5 Meios de recuperação quando a chave secreta do usuário ficou comprometida

Emite-se um novo certificado digital, mediante novo procedimento de solicitação.

4-4-3 Requisitos do registro de revogação （LCR/LAR）

Para refletir as informações de revogação que concluiu a sua recepção até um tempo pré-determinado, uma vez todos os dias, elabora um novo registro de revogação（LCR/LAR, e divulga prontamente, para o verificador de assinatura autorizado, etc. o registro de revogação（LCR/LAR）criado.

Além disso, para o verificador de assinatura autorizado, o fornecimento do registro de revogação（LCR/LAR）está disponível 1 dia 24horas, 1 ano 365 dias. No entanto, pode não ser possível utilizar temporariamente, devido ao trabalho de manutenção periódica, etc.

4-4-4 Método de fornecimento das informações de revogação

4-4-4-1 Método de fornecimento das informações de revogação

Os métodos para confirmar a eficácia do certificado digital estabelece-se das 2 seguintes maneiras:

① Consulta o OCSP responders (utilizando o protocolo OCSP que está regulamentado no RFC2560)

② Registro de revogação（LCR/LAR) método de fornecimento (utilizando o protocolo LDAPV3 que está regulamentado no RFC2251)

4-4-4-2 Conteúdo das respostas a consulta do OCSP responder

Responde as razões da revogação, se o dito certificado digital estiver revogado, for diferente de revogação ou desconhecido, da eficácia deste, no momento da consulta, para as consultas on-line por número de série e informações para a identificação do emissor do certificado digital

Razões da revogação		
1	keyCompromise	Comprometimento da chave secreta do usuário
2	cACompromise	Comprometimento da chave secreta do Governador da Província de Hokkaido
3	affiliationChanged	Quando ocorre mudança do conteúdo descrito no certificado digital
4	superseded	Atualização do certificado digital
5	cessationOfOperation	Não há necessidade de um certificado digital (deixou de utilizar).

4-4-4-3 Requisitos para os métodos de consultas do OCSP responder

Submeter o relatório ao governador da província de Hokkaido com antecedência sendo necessário receber uma concessão para o acesso.

4-4-4-4 Conteúdo da resposta do método de fornecimento do registro de revogação

O formato do registro de revogação （LCR/LAR） baseia-se no X.509(03/2000) recomendação ITU-T.

O registro de revogação (LCR), em princípio, cria segmentos LCR por municípios, descrevendo a data de validade, razão da revogação (tal como a razão da revogação desta Declaração de Práticas, no item" 4-4-4-2 Conteúdo das respostas a consulta do OCSP responder"), número de série do certificado digital que foi revogado. O verificador de assinatura verifica o certificado digital através da obtenção adequada de registros revogados (CRL / ARL) que foram armazenados no repositório.

4-4-4-5 Requisitos necessários no fornecimento do registro de revogação （LCR/LAR）

Submeter o relatório ao governador da província de Hokkaido com antecedência sendo necessário receber uma concessão para o acesso.

4-4-5 Requisitos para a suspensão

Não se faz a suspensão do certificado digital emitido pelo governador da província de Hokkaido.

4-4-6 Requerente da suspensão

Não se aplica.

4-4-7 Procedimentos para solicitação de suspensão

Não se aplica.

4-4-8 Período de suspensão

Não se aplica.

4-4-9 Frequência de emissão do registro de revogação （LCR/LAR）

O prazo do registro de revogação（LCR/LAR） é de 72 horas, sendo emitido a cada 24horas. No entanto, se ocorrer o comprometimento da chave secreta ou similar do

governador da província de Hokkaido, emite imediatamente o registro de revogação (LCR/LAR).

4-4-10 Período de atraso máximo de emissão do registro de revogação

Emitir um novo registro de revogação (LCR/LAR) antes do período de validade, dos registros de revogação (LCR/LAR) emitidos por último, expirar.

4-4-11 Verificação do registro de revogação

O verificador de assinatura deve confirmar a eficácia dos certificados digitais dos registros de revogação (LCR/LAR) emitidos pelo governador da província de Hokkaido.

4-5 Relatório de disponibilidade para informações de revogação

O órgão de certificação designado elabora um relatório para a disponibilidade de informações de revogação e seus respectivos arquivos relacionados ao armazenamento. O órgão de certificação designado publica o relatório no Diário Oficial, além disso coloca em preparação no escritório do órgão de certificação designado e deixa-o disponível para consulta pública por cinco anos.

Os itens descritos no relatório são os seguintes:

- destino das informações de revogação
- data (ano/mês) do fornecimento das informações de revogação
- número de informações de revogação fornecidas
- método de fornecimento das informações de revogação

4-6 Solicitação de emissão de certificados de autenticação mútua

A solicitação de emissão do certificado de autenticação mútua para a Certificação Para Indivíduos BCA é realizada com base no procedimento estabelecido pela Certificação Para Indivíduos BCA.

4-7 Emissão de certificados de autenticação mútua

O governador da província de Hokkaido de acordo com o procedimento prescrito, confirma a autenticidade da pessoa que vai operar a Certificação Para Indivíduos BCA.

Emite certificados de autenticação mútua anexado a assinatura do Governador da Província de Hokkaido, ao pedido de emissão do certificado submetido pela Certificação Para Indivíduos BCA, após o término do teste de conexão com base no procedimento estabelecido pela Certificação Para Indivíduos BCA

4-8 Recebimento de certificados de autenticação mútua

O Governador da Província de Hokkaido de acordo com o procedimento prescrito, recebe os certificados de autenticação mútua que foram emitidos pela Certificação Para Indivíduos BCA passando o recibo a esta. Da mesma forma, o Governador da Província de Hokkaido de acordo com o procedimento prescrito, passa certificados de autenticação mútua emitidos pela Certificação Para Indivíduos BCA a ela, e recebe o recibo. Feita a confirmação dos recebimentos de ambos, conclui-se, recebendo a reciprocidade do certificado de autenticação mútua.

Ainda, o Governador da Província de Hokkaido gera um par de certificados de autenticação mútua com os certificados de autenticação mútua que foram trocados com a Certificação Para Indivíduos BCA mutuamente como um par e se inscreve no repositório.

4-9 Atualização de certificados de autenticação mútua

O Governador da Província de Hokkaido atualiza os certificados de autenticação mútua e seus respectivos pares, nos seguintes casos, de(1) a (4):

Aqui, cada procedimento de recebimento, emissão e solicitação de emissão referente a atualização do certificado de autenticação mútua, baseia-se nos itens "4-6 Solicitação de emissão de certificados de autenticação mútua", "4-7 Emissão de certificados de autenticação mútua" e "4-8 Recebimento de certificados de autenticação mútua" desta Declaração de Práticas. Além disso, no repositório o par de certificados de autenticação mútua é substituído por outro mais novo, imediatamente.

(1) Se os certificado de autenticação mútua, emitido pela Certificação Para Indivíduos BCA, estiver perto da data de validade

(2) Se o certificado de autenticação mútua que foi emitido para Certificação Para Indivíduos BCA está com a data de validade perto

(3) Se houver alterações na descrição do certificado de autenticação mútua emitido pela Certificação Para Indivíduos BCA

(4) Se houver alterações na descrição do certificado de autenticação mútua que foi emitido para Certificação Para Indivíduos BCA

4-10 Revogação de certificados de autenticação mútua

4-10-1 Razões da revogação

A AC da província de Hokkaido revoga o certificado de autenticação mútua emitido na Certificação Para Indivíduos BCA, e esta revoga o mesmo certificado emitido na AC da província de Hokkaido, em casos de o seguinte ocorrer na Certificação Para Indivíduos BCA e AC da província de Hokkaido:

- Comprometimento da chave secreta
- Atualização do certificado de autenticação mútua
- Fim da autenticação mútua (Incluindo nos casos de termino de autenticação mútua devido as violações de normas desta autenticação)

4-10-2 Requerente de revogação

A solicitação de revogação a AC da província de Hokkaido pela Certificação Para Indivíduos BCA, o responsável da Certificação Para Indivíduos BCA faz

4-10-3 Procedimentos de invalidação e solicitação de revogação

A solicitação de revogação dos certificados de autenticação mútua se realiza baseada nos procedimentos da Certificação Para Indivíduos BCA

4-11 Procedimentos de Auditoria de Segurança

4-11-1 Procedimentos de Auditoria de Segurança

Os auditores internos (consulte o item "5-2-1 Membro de quem é exigida alta confiabilidade e seu papel" desta Declaração de Práticas) faz uma auditoria de segurança verificando eventos anormais tais como operações ilegais, e agrupa com os registros de operação de serviços, etc. um log que registra os eventos de ocorrência no repositório e sistema da AC da província de Hokkaido

4-11-2 Informações registradas no log de auditoria

Para direcionar as questões importantes referentes a segurança no repositório e sistema da AC da província de Hokkaido, registra o log de auditoria, log operacional e log de acesso, etc.

- logs de funcionamento e operacional relativos ao procedimento de emissão
- logs de funcionamento e operacional relativos ao procedimento de revogação
- todos os logs de funcionamento e operacional relativos à eficácia
- log operacional relativo à geração do par de chaves do governador da província de Hokkaido
- log de acesso a um sistema, a vários livros de contabilidade
- registro de entrada e saída de equipamentos a AC da província de Hokkaido

No log de auditoria, incluem-se as seguintes informações:

- Tipo de evento ou processamento
- data e hora da ocorrência
- resultado do processamento
- informações de identificação de fonte de evento (ID do operador, nome do sistema, etc.)

4-11-3 Ciclo de inspeção do log de auditoria

O auditor interno realiza uma auditoria de segurança semanalmente.

4-11-4 Período de retenção do log de auditoria

Mantém por 1 ano.

4-11-5 Proteção do log de auditoria

O log de auditoria realiza medidas contra a adulteração. Ademais, o backup do log de auditoria chega na mídia de armazenamento externa mensalmente, e é armazenado em um cofre com fechadura instalado em uma sala, onde é realizado o controle apropriado de entrada e saída.

Além disso, os auditores internos fazem devidamente a navegação e exclusão do log de auditoria.

4-11-6 Procedimentos para o Backup do log de auditoria

Faz um backup diariamente, chega na mídia de armazenamento externa mensalmente.

4-11-7 Notificação de inspeção do log de auditoria

A inspeção do log de auditoria é realizada sem a necessidade de notificar a pessoa que causou o evento.

4-11-8 Avaliação de vulnerabilidade

Ao examinar o registro de auditoria, avaliam-se as vulnerabilidades de segurança na superfície do sistema e aspectos operacionais.

4-11-9 Sistema de coleta de dados do log de auditoria

A função de coleta do log de auditoria como uma das funções do sistema da AC da província de Hokkaido, coleta como log de auditoria desde a inicialização do sistema os eventos importantes relacionados à segurança.

4-12 Arquivamento de registros

4-12-1 Informações arquivadas em papel

4-12-1-1 Tipos de informações arquivadas

As informações a seguir são arquivadas:

(Governador da Província de Hokkaido)

- documentos relativos à elaboração desta Declaração de Práticas
- documentos relativos à execução da cerimônia de chave
- documentos relativos aos acordos com o verificador de assinatura, etc.
- documentos relativos à correção e divulgação de informações de serviços de certificação
- relatório de auditoria, outros

(órgão de certificação designado)

- documentos relativos à mudança/designação do órgão de certificação designado
- regulamentos administrativos de certificação
- documentos relativos a medidas de segurança e equipamentos
- documentos relacionados com o plano de negócios, equilibrar o orçamento
- relatório de negócios, declaração de rendimentos
- documentos relativos à correção e divulgação de informações de serviços de certificação
- Relatório que fornece o estado do arquivo de informações de revogação e informações de revogação
- documentos relativos às taxas, etc.

(Prefeito de município)

- documentos relativos à solicitação de emissão de certificado digital (solicitação de emissão, etc.)
- documentos relativos à solicitação de revogação de certificado digital (solicitação de revogação, etc.)
- documentos relativos à correção e divulgação de informações de serviços de certificação, etc.

4-12-1-2 Período de retenção para arquivo

O período de retenção para arquivo é de 10 anos. No entanto, para os documentos relativos à solicitação de emissão de certificados digitais, o período é de 13 anos.

4-12-1-3 Proteção de informações de arquivo

As informações arquivadas no órgão de certificação designado são armazenadas em um cofre com fechadura instalado em uma sala, onde é realizado o controle apropriado de entrada e saída. São aplicadas medidas de proteção em consideração ao meio ambiente tais como temperatura, umidade e contra a adulteração. As informações a serem armazenadas nos municípios e províncias são armazenadas num local apropriado.

4-12-1-4 Verificação de informações de arquivo

Realiza-se 1vez por ano a verificação da legibilidade, da condição do papel onde as informações de arquivo foram descritas.

4-12-2 Informações arquivadas como dados digitais

4-12-2-1 Tipos de informações arquivadas

As informações a seguir são arquivadas no órgão de certificação designado:

・solicitação de revogação (no caso de solicitação on-line ao Governador da Província de Hokkaido)
・certificado digital
・certificado de autenticação mútua
・certificados assinados por ela própria
・certificados de ligação
・certificados do servidor de verificação de certificado de posição governamental
・certificado do respondedor OCSP
・informações de revogação
・registro de revogação（LCR/LAR）
・arquivo de registro de revogação
・registro de revogação（LCR/LAR） Histórico de uso do método de fornecimento
・Histórico de uso do método de consultas do OCSP responder
・Vários logs (log de monitoramento, log de “iniciar e parar”, log operacional)

4-12-2-2 Período de retenção para arquivo

O período de retenção para arquivo é de 10 anos. No entanto, para os certificados digitais já emitidos, 13 anos, a partir da data do registro de informações de revogação até a data de expiração, do período do certificado digital, relativa a estas informações

4-12-2-3 Proteção de informações de arquivo

Às informações de arquivo, são aplicados o controle de acesso e medidas contra a adulteração.

As informações de arquivo são armazenadas em um cofre com fechadura instalado em uma sala, onde é realizado o controle apropriado de entrada e saída e chegam na mídia de armazenamento externa mensalmente.

4-12-2-4 Procedimentos de backup de informações de arquivo

As informações de arquivo fazem um backup diariamente, chegam na mídia de armazenamento externa mensalmente.

4-12-2-5 Requisitos do carimbo de tempo para ser aplicado ao registo

Às informações de arquivo são dados o carimbo de tempo (informações do horário).

4-12-2-6 Verificação de informações de arquivo

As informações de arquivo fazem 1 vez por ano a confirmação da possibilidade da mídia de armazenamento externa ter sido registrada.

4-13 Atualização da chave do Governador da Província de Hokkaido

Ocorre a atualização do par de chaves do Governador da Província de Hokkaido a

cada 5 anos.

Na atualização do par de chaves, publica no repositório o certificado de ligação da construção de um caminho da chave pública nova para a chave pública antiga.

4-14 Recuperação de desastre e comprometimento da chave

4-14-1 Medidas na destruição de dados, software e hardware

Se os dados, software e hardware foram destruídos, faz o trabalho de restauração o mais rápido possível pelos dados, software e hardware de backup.

4-14-2 Medidas no comprometimento de chave do Governador da Província de Hokkaido

Trata-se do seguinte:

- parada do serviço de emissão dos certificados digitais
- divulga todos os certificados digitais assinados por esta chave secreta, faz a revogação de certificados de autenticação mútua, e registra nos registros de revogação （LCR/LAR）
- notifica à Certificação Para Indivíduos BCA

4-14-3 Garantia de equipamento na ocorrência de desastres

Se o equipamento tiver sido danificado pelo desastre, etc., realiza as operações usando os dados de backup e garante uma máquina de reposição.

4-15 Processamento de consultas, reclamações

O Governador da Província de Hokkaido, órgão de certificação designado e prefeitos de municípios, quanto as consultas e reclamações relativas aos trabalhos de certificação, devem esforçar-se no processamento destas, de forma adequada e rápida.

4-16 Sistema operacional

Realizar um sistema operacional segura e adequada. Para maiores informações, determinar separadamente.

4-17 Encerramento do serviço de certificação

Não se aplica.

4-18 Extinção do trabalho de certificação

O órgão de certificação designado, se anula ou interrompe uma parte ou todos trabalhos de certificação, etc., deve obter a permissão do Ministro dos Assuntos Internos e Comunicações

Além disso, se para isto, o Governador da Província de Hokkaido realiza o trabalho de certificação, o órgão de certificação designado deverá realizar os seguintes itens:

- suceder ao Governador da Província de Hokkaido os trabalhos de certificação que devem ser sucedidos
- suceder ao Governador da Província de Hokkaido a mídia eletromagnética, documentos e livros de contabilidade relativos aos trabalhos de certificação que devem ser sucedidos

Entre outros, realizar itens que o Governador da Província de Hokkaido ou o Ministro dos Assuntos Internos e Comunicações admitem serem necessários.

5. Controles de segurança física, de procedimento e de pessoal

5-1 Controles de segurança física

5-1-1 Autoridade Certificadora (AC) da província de Hokkaido

5-1-1-1 Construção e localização das instalações

As instalações da AC da província foram colocadas num local que não sofra danos de desastre tais como incêndio, terremoto, inundação e, na estrutura do edifício, tomaram medidas para a prevenção contra intrusões, incêndio, terremotos

5-1-1-2 Acesso físico

Com relação a cada sala nas instalações internas da AC da província de Hokkaido , dependendo da importância do trabalho a ser realizado, faz-se o controle de acesso em vários níveis de segurança. A certificação ocorre por um dispositivo de autenticação biométrica e pela autoridade de operação que possa identificar o Cartão CI.

O diretor administrativo da autoridade certificadora da AC da província de Hokkaido concede autoridade de entrada e saída para cada quarto, dependendo do serviços de cada um dos funcionários, decidido no item “5-2 Controles de segurança de procedimento” desta Declaração de Práticas.

As instalações da AC da província de Hokkaido realizam a vigilância 24 horas, 365 dias, colocando o observador pelo sistema de vigilância.

5-1-1-3 Energia e ar condicionado

A AC da província de Hokkaido toma medidas como de flutuações de tensão e frequência, falta de energia e interrupções, além de assegurar o poder de capacidade suficiente para o funcionamento do equipamento. No caso em que a energia não é fornecida, muda-se para o fornecimento de energia pelo gerador dentro de um determinado período. Ao instalar o equipamento de ar condicionado, mantém o ambiente de trabalho para o pessoal e o ambiente de operação do equipamento adequadamente.

5-1-1-4 Exposição à água

O edifício para instalar os equipamentos da AC da província de Hokkaido, instala a máquina de detecção de vazamento na sala e adota medidas à prova d'água no chão e teto.

5-1-1-5 Medidas contra terremoto

O edifício para instalar os equipamentos da AC da província de Hokkaido, possuindo um estrutura sísmica, adota medidas para evitar a queda de mobiliário e de equipamentos.

5-1-1-6 Medidas contra incêndio

O edifício para instalar os equipamentos da AC da província de Hokkaido fortifica o equipamento de combate a incêndios com uma construção resistente ao fogo e salas com divisão de prevenção de incêndios.

5-1-1-7 Medidas contra ondas eletromagnéticas

Sob as instalações de cada quarto da AC da província de Hokkaido dependendo da importância do serviço a ser realizado, providencia-se equipamento para evitar o

vazamento de informações de ondas eletromagnética e ataque das mesmas.

5-1-1-8 Armazenamento da mídia (outros meios magnéticos)

A mídia, incluindo o armazenamento de informações, dados de backup além de ser armazenada em um cofre com fechadura instalado em uma sala, onde é realizado o controle apropriado de entrada e saída, permite controlar a carga e descarga adequadamente, com base nos procedimentos previstos.

5-1-1-9 Eliminação de resíduos

Para documentos e mídias de armazenamento que contém informações confidenciais, realiza-se a eliminação adequada com base nos procedimentos prescritos

5-1-1-10 Backup off-site

Não se aplica.

5-1-2 Instalações dos municípios

5-1-2-1 Construção e localização das instalações

Instalações dos domicílios municipais.

5-1-2-2 Acesso físico

O aparelho gerador de par de chaves e oterminal do guichê de recepção são instalados em local onde o monitoramento de pessoal é feito pelos funcionários dos domicílios municipais.

5-1-2-3 Controle de informações de armazenamento

O documento referente ao item "4-12-1-1 Tipos de informações arquivadas" desta Declaração de Práticas é armazenado num local apropriado.

5-1-2-4 Processamento de eliminação de resíduos

Sobre a eliminação de documentos, mídias de armazenamento, terminais do guichê de recepção, aparelho gerador de par de chaves, entre outros, realiza-se o processamento de eliminação adequado com base nos procedimentos prescritos.

5-2 Controles de segurança da parte de procedimento

5-2-1 Membro de quem é exigida alta confiabilidade e seu papel

5-2-1-1 Membros na AC da província de Hokkaido

Os membros envolvidos na operação do sistema da AC são as seguintes:

(1) diretor administrador da autoridade certificadora

O diretor administrador da autoridade certificadora é responsável pela operação da AC da província de Hokkaido realizando os seguintes serviços:

- Correspondência de apoio em casos de desastre e emergência, ou no compromisso de geração da chave secreta do governador da província de Hokkaido
- confirmação de trabalho e instruções de trabalho para os membros, etc.
- manutenção de chave para controlar as funções (a seguir designada "chave de controle") do HSM (aparelho que controla com segurança a chave

secreta do governador da província de Hokkaido)

- normas de correspondência do pedido de divulgação de informações de serviços de certificação
- controle de correspondência do pedido de correção de informações de serviços de certificação, etc.
- controle de correspondência dos processamentos de reclamações / consultas
- controle da Comissão para a Proteção das informações de serviços de certificação
- preparação de livros relacionados aos serviços de certificação
- elaboração de relatório do estado de fornecimento de informações de revogação, etc.
- controle de entrada e saída
- correspondência às auditorias de conformidade e controle de aplicação correto aos itens especificados
- matriz relativa a operação e administração da AC da província de Hokkaido, entre outros
- controle dos dados pessoais

(2) controlador da chave secreta

O controlador da chave secreta realiza os seguintes serviços e é o responsável no que se refere ao serviço de usar a chave secreta, etc. do Governador da Província de Hokkaido:

Além disso, o trabalho e realizado por várias pessoas controladoras da chave secreta.

- controle de armazenamento de mídia de backup da chave secreta, etc. do Governador da Província de Hokkaido
- operação para o HSM do certificado assinado por ele mesmo no momento da emissão, geração de chave secreta, etc. do Governador da Província de Hokkaido
- operação para o HSM na atualização da chave secreta, etc. do Governador da Província de Hokkaido
- operação para o HSM quando da restauração do backup, backup da chave secreta, etc. do Governador da Província de Hokkaido

(3) encarregado da recepção

O encarregado da recepção realiza o controle dos documentos de solicitação, etc. e trabalho de coordenação com a Certificação Para Indivíduos BCA, recebimento da solicitação de revogação e atualização e emissão de certificados de autenticação mútua.

(4) encarregado de exame

O encarregado de exame realiza os serviços de exame das solicitações de revogação e atualização e emissão de certificados de autenticação mútua.

(5) aprovador de exame

O aprovador de exame realiza serviços de aprovação referentes aos resultados de exame das solicitações de revogação e atualização e emissão de certificados de autenticação mútua do encarregado de exame.

(6) operador sênior

O operador sênior realiza os seguintes serviços para usar a chave secreta do Governador da Província de Hokkaido

・ativação e desativação do HSM
・ processamento de revogação, atualização e emissão de certificados assinados por ele mesmo
・processamento de revogação, atualização e emissão de certificados de autenticação mútua
・processamento de revogação, atualização e emissão de certificados do servidor de verificação de certificado de posição governamental
・processamento de revogação, atualização e emissão de certificados do respondedor OCSP
・mudança e política de registro de estabelecimento dos certificados digitais da AC da província de Hokkaido
・controle de serviços operacionais do sistema da AC da província de Hokkaido, entre outros

(7) operador de repositório

O operador de repositório realiza serviços no controle de estabelecimento de repositório.

(8) operador geral

O operador geral realiza a manutenção e operação dos equipamentos de rede.

(9) auditor interno

O auditor interno realiza serviços no log e sistema de repositório e da AC da província de Hokkaido

・inspeção de log de auditoria
・exclusão de registro auditado

5-2-1-2 Membros nos municípios

Os membros dos municípios realizam o controle adequado dos trabalhos relacionados com a emissão e a revogação e identificação rigorosa, no momento da emissão e revogação de certificados digitais, bem como de equipamentos utilizados nestes trabalhos.

5-2-2 Instruções de trabalho e separação da autoridade administrativa de cada membro na AC da província de Hokkaido

Cada membro realiza as instruções de trabalho e separação da autoridade administrativa que são definidas como se segue:

① separação da autoridade

Para ajudar a separar as funções sob o ponto de vista da segurança humana, realiza o controle e operação das instalações pelos vários membros a quem foram concedidas a autoridade.

② autoridade do diretor administrativo da autoridade certificadora

O diretor administrativo da autoridade certificadora instrui baseado nos procedimentos prescritos e estabelece separadamente para cada membro as instruções dos serviços importantes

③ autoridade do operador sênior

Ao operador geral, o operador sênior realiza a confirmação dos resultados e instruções para diversos trabalhos com base nos procedimentos prescritos estabelecidos separadamente. Também, emite certificados e registros dependendo da autoridade dos membros.

5-2-3 Requisitos de identificação e certificação de cada membro na AC da província

- Quando cada membro realiza o sistema operacional, o sistema para realizar a identificação e certificação operacional de membros, é uma autoridade válida.
- É realizada utilizando uma senha ou certificação de cartão IC para cada membro
- minimiza as informações confidencias que podem ser acessadas de acordo com o papel que cada membro

5-3 Controles de segurança de pessoal na AC da província de Hokkaido

5-3-1 Procedimentos de permissão e verificação de antecedentes dos membros

Segue os procedimentos de análise necessários para realizar verificações de antecedentes (currículo, cartas de recomendação, etc.) com os documentos do emprego anterior.

5-3-2 Procedimentos de formação de cada membro

Implementa a formação necessária para cada membro, de acordo com o plano de educação e formação.

5-3-3 Sequência e frequência de mudança de obrigações entre os membros

De acordo com o documento do diretor administrativo da autoridade certificadora define-se o método de rotação de serviços.

5-3-4 Ações não autorizadas

No caso da realização de uma ação não autorizada ao membro, impõe-se uma medida disciplinar.

5-3-5 Documentação fornecida aos membros

É possível encontrar (procedimentos de operação, livro de procedimentos operacionais, etc.), documentos de acordo com os direitos de acesso para cada membro.

6. Controles técnicos de segurança

6-1 Geração e Instalação do Par de Chaves

6-1-1 Chave do governador da província de Hokkaido

6-1-1-1 Pessoa que gera o par de chaves do governador da província de Hokkaido, método de geração

O par de chaves do governador da província de Hokkaido, o controlador da chave secreta de várias pessoas é gerado utilizando o equipamento estabelecido no item "6-1-1-3 Hardware / software para gerar um par de chaves" desta Declaração de Práticas.

6-1-1-2 Chefe da chave

Usa uma chave de 2048 bits com base no sistema de criptografia RSA.

6-1-1-3 Hardware / software para gerar um par de chaves

HSM equivalente de FIPS140-1 Nível 3

6-1-1-4 Finalidade da utilização da chave secreta

Para assinatura digital.

6-1-1-5 Recebimento da chave pública da Certificação Para Indivíduos BCA

Quanto a troca do certificado de autenticação mútua da AC da província de Hokkaido, recebe a chave pública da Certificação Para Indivíduos BCA de forma confiável e segura.

6-1-1-6 Distribuição da chave pública do Governador da Província de Hokkaido

O certificado com a própria assinatura do Governador da Província de Hokkaido é armazenado no cartão IC no momento da emissão do certificado digital e é entregue ao usuário. Também é distribuído para o verificador de assinatura, etc. de forma confiável e segura.

6-1-2 Chave secreta do usuário

6-1-2-1 Pessoa que gera o par de chaves do usuário, método de geração

O próprio usuário gera pelo aparelho gerador de par de chaves do domicílio municipal.

6-1-2-2 Método para fornecer com segurança a chave pública do usuário ao domicílio municipal

Quanto ao domicílio municipal, recebe a chave pública armazenada no cartão CI diretamente do usuário.

6-1-2-3 Chefe de chave

Usa uma chave de 1024 bits com base no sistema de criptografia RSA.

6-1-2-4 Hardware / software para gerar um par de chaves

Aparelho gerador de par de chaves do domicílio municipal.

6-1-2-5 Finalidade da utilização da chave secreta

Para assinatura digital.

6-2Proteção da chave secreta

6-2-1 Chave secreta do Governador da Província de Hokkaido

6-2-1-1 Armazenamento da chave secreta, critérios exigidos

Armazena baseado no HSM equivalente de FIPS140-1 Nível 3

6-2-1-2 Controle de várias pessoas da chave secreta

Armazenam a chave secreta no HSM controlado por várias pessoas administradoras da chave secreta.

6-2-1-3 Custódia da chave secreta (escrow)

A custodia da chave secreta não se realiza.

6-2-1-4 Backup da chave secreta

O backup da chave secreta realiza-se pela operação de vários administradores da chave secreta. A chave secreta da qual foi feito o backup pelo HSM armazena-se com segurança criptografando-se. No entanto, o administrador de chaves privada não pode trazer para fora da sala destinada a armazenar a mídia de backup.

6-2-1-5 Armazenamento (arquivamento) da chave secreta

O arquivamento da chave secreta não se realiza.

6-2-1-6 Armazenamento de chave secreta para um módulo criptográfico

A chave secreta armazena-se para um módulo criptográfico, gerada dentro do HSM por meio da operação de vários administradores da chave secreta.

6-2-1-7 Ativação da chave secreta

A chave secreta é ativada pela operação de vários administradores da chave secreta.

6-2-1-8 Desativação da chave secreta

A chave secreta é desativada pela operação de vários administradores da chave secreta.

6-2-1-9 Destruição da chave secreta

A destruição da chave secreta no módulo criptográfico é realizada por vários administradores da chave secreta, pelo método de inicialização do módulo criptográfico deixando num estado que não pode ser totalmente utilizado. Além disso, se leva o módulo criptográfico para o exterior da sala, destrói-se o módulo criptográfico

fisicamente. Ademais, assume-se que o módulo criptográfico de backup da chave secreta também destrói-se.

6-2-2 Chave secreta do usuário

6-2-2-1 Armazenamento da chave secreta, critérios exigidos

É equipado com um cartão de aplicação que esteja em conformidade com os "Serviços de Certificação Pública para Indivíduos, Cartão de aplicação externa de interface especificação versão 1.1" protegido por um cartão IC, a chave secreta não pode ser lida fisicamente sendo uma inviolável.

6-2-2-2 Custódia da chave secreta (escrow)

O Governador da Província de Hokkaido não recebe a custodia da chave secreta do usuário. Além disso, não permitem que o usuário deposite esta chave secreta a terceiros.

6-2-2-3 Backup da chave secreta

A chave secreta armazena dentro do cartão CI e não faz o backup.

6-2-2-4 Armazenamento de chave secreta para um módulo criptográfico (cartão CI)

A chave secreta do usuário é gerada no aparelho gerador de par de chaves do domicílio municipal, armazenando-se no cartão CI. Depois do armazenamento no cartão CI, a chave secreta gerada no aparelho gerador de par de chaves, supõe-se que é completamente removido do aparelho gerador de par de chaves.

6-2-2-5 Ativação da chave secreta

A chave secreta do usuário é ativada com uma senha pelo usuário.

6-2-2-6 Desativação da chave secreta

Pela operação do cartão CI é desativada.

6-2-2-7 Destruição da chave secreta

No caso da destruição da chave secreta do usuário, o usuário destrói no aparelho gerador de par de chaves ou no terminal do guichê do domicílio municipal do usuário.

6-3 Outros aspectos do controle da geração de par de chaves

6-3-1 Chave do governador da província

6-3-1-1 Armazenamento da chave pública

A chave pública está incluída no certificado com a própria assinatura, armazenando no arquivo submetido a medidas contra adulteração como consta no item "4-12 Arquivamento de registros (arquivos)" desta Declaração de Práticas, especificando o período.

6-3-1-2 Período de utilização da chave secreta, chave pública

A validade do certificado com a própria assinatura do Governador da Província de Hokkaido é de 10 anos. O período de utilização da chave secreta é de 5 anos a partir da

data em que a chave foi gerada, e é realizada uma atualização de chave a cada 5 anos.

6-3-2 Chave do usuário

O período de utilização da chave secreta e chave pública do usuário é de 3 anos. Porém, se for determinado que a segurança criptográfica tornou-se vulnerável, considerar em mudar o método criptográfico e naquele momento, é o caso de realizar a atualização de chave.

6-4 Dados de ativação

6-4-1 Chave do Governador da Província de Hokkaido

6-4-1-1 Geração e instalação dos dados de ativação

Os dados de ativação do HSM para armazenar a chave secreta do Governador da Província de Hokkaido são fixados pelo administrador de chave.

6-4-1-2 Proteção dos dados de ativação

Armazena-se com segurança o administrador de chave necessário para a ativação do HSM para armazenar a chave secreta do Governador da Província de Hokkaido

6-4-2 Chave do usuário

6-4-2-1 Geração e instalação dos dados de ativação

Os dados de ativação da chave secreta do usuário (senha), para o próprio usuário no aparelho gerador de par de chaves, definem-se como o cartão IC, ao gerar o par de chaves.

6-4-2-2 Proteção dos dados de ativação

Os dados de ativação da chave secreta do usuário devem ser armazenados de forma segura e mudados regularmente.

6-5 Controles de segurança computacional

6-5-1 Requisitos funcionais de segurança computacional

O sistema da AC da província de Hokkaido usa o sistema operacional que é confiável, e fornece recursos de recuperação das funções, coleta dos dados do arquivo e log de auditoria, função de certificação e identificação de cada membro, controle de acesso.

6-5-2 Avaliação de segurança computacional

É realizada a partir de tempo para avaliação do sistema de segurança.

6-6 Controles de segurança do ciclo de vida

6-6-1 Controles de segurança no desenvolvimento do sistema

O desenvolvimento do sistema deste serviço com relação a mudança ou correção, realiza um trabalho em um ambiente e organização confiável, baseando-se no procedimento prescrito.

6-6-2 Controles de segurança nos aspectos do sistema operacional

6-6-2-1 AC da província de Hokkaido

A fim de manter o sistema deste serviço realiza-se regularmente a checagem da

segurança dos softwares e do OS. Também passa por escrito o resultado desta verificação e armazena.

6-6-2-2 Municípios

A fim de manter o sistema deste serviço, realiza adequadamente o controle de segurança dos softwares ou aparelho gerador de par de chaves ou o terminal do guichê do domicílio municipal do OS.

6-7 Controles de segurança de rede

Impede o acesso não autorizado, requer-se o mínimo de serviço de rede que permite a passagem de uma rede externa. Além disso, realiza a proteção de medidas de segurança de detecção de intrusão suficiente, etc. A informação a ser publicada da informação armazenada no repositório, é fornecida através do firewall.

6-8 Controles técnicos do módulo criptográfico

Esta Declaração de Práticas estabelece-se nos itens “6-1-1-3 Hardware / software para gerar um par de chaves” “6-2-1-1 Armazenamento da chave secreta, critérios exigidos”.

7. Certificados e registros de revogação (LCR/LAR)

7-1 Certificados

7-1-1 Certificados digitais

São estabelecidas as seguintes informações no certificado digital. O perfil para mais detalhes define-se no manual do projeto.

- número de versão (X.509 Número de versão do formato do certificado)
- número de série (Número para a identificar o certificado emitido dentro da AC da província de Hokkaido)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para o certificado digital)
- informações do emissor (o nome do Governador da Província de Hokkaido que emitiu o certificado digital é descrito no nome distinto X.500)
- data de início do período de validade (dia de emissão do certificado digital)
- data de encerramento do período de validade (3 anos após a data de emissão)
- chave pública (chave pública do usuário)
- maiores informações (Informação Básica 4 do usuário, finalidade da utilização da chave secreta serão descritos)

7-1-2 Certificados de autenticação mútua

Ao realizar as Certificação Para Indivíduos BCA e autenticação mútua, para a necessária autenticação mútua, são estabelecidas as seguintes informações: O perfil para mais detalhes define-se no manual do projeto.

- número de versão (X.509 Número de versão do formato do certificado)
- número de série (Número para a identificar o certificado emitido dentro da AC da província de Hokkaido)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para o certificado de autenticação mútua)
- informações do emissor (o nome do Governador da Província de Hokkaido que emitiu o certificado de autenticação mútua é descrito no nome distinto X.500)
- data de início do período de validade (dia de emissão do certificado de autenticação mútua)
- data de encerramento do período de validade (5 anos após considerar válido o certificado de autenticação mútua)
- chave pública (chave pública da autenticação mútua AC)
- maiores informações

7-1-3 Certificados de assinatura própria

No certificado de assinatura própria do Governador da Província de Hokkaido são estabelecidas as seguintes informações: O perfil para mais detalhes define-se no manual do projeto.

- número de versão (X.509 Número de versão do formato do certificado)
- número de série (Número para a identificar o certificado emitido dentro da AC da província de Hokkaido)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para o certificado de assinatura própria)
- informações do emissor (o nome do Governador da Província de Hokkaido que

emitiu o certificado de assinatura própria é descrito no nome distinto X.500)
- data de início do período de validade (dia de emissão do certificado de assinatura própria)
- data de encerramento do período de validade (10 anos após a data de emissão)
- chave pública (chave pública do Governador da Província de Hokkaido)
- maiores informações

7-1-4 Certificados de ligação

No certificado de ligação, quando da necessidade de atualização da chave do Governador da Província de Hokkaido, são estabelecidas as seguintes informações: O perfil para mais detalhes define-se no manual do projeto.

- número de versão (X.509 Número de versão do formato do certificado)
- número de série (Número para a identificar o certificado emitido dentro da AC da província de Hokkaido)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para o certificado de ligação)
- informações do emissor (o nome do Governador da Província de Hokkaido que emitiu o certificado de ligação é descrito no nome distinto X.500)
- data de início do período de validade (OldWithNew : Dia que criou um par de chaves da velha geração / NewWithOld : Dia que gerou um par de chaves da nova geração)
- data de encerramento do período de validade: （OldWithNew : data de encerramento do período de validade do certificado de própria assinatura da velha geração / NewWithOld : data de encerramento do período de validade do certificado de própria assinatura da velha geração)
- chave pública（OldWithNew：chave pública da velha geração, NewWithOld：chave pública da nova geração）
- maiores informações

7-2 Registro de revogação（LCR/LAR）

7-2-1 Registro de revogação（LCR） do certificado digital

No registro de revogação do certificado digital são estabelecidas as seguintes informações: O perfil para mais detalhes define-se no perfil da LCR do manual do projeto.

- informação de versão (número da versão do formato da LCR)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para a LCR)
- informações do emissor (o nome do Governador da Província de Hokkaido que emitiu a LCR é descrito no nome distinto X.500)
- data de início do período de validade (data que a LCR se faz válida)
- data de encerramento do período de validade (3 dias após considerar válida a LCR)
- próxima data de atualização (1 dia após considerar válida a LCR)
- informações do certificado revogado (número de série, data de revogação, razão da revogação)
- maiores informações

7-2-2 Registro de revogação (LAR) do certificado de autenticação mútua

No registro de revogação do certificado de autenticação mútua (LAR) são estabelecidas as seguintes informações: O perfil para mais detalhes define-se no perfil da LAR do manual do projeto.

- informação de versão (número da versão do formato da LAR)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para a LAR)
- informações do emissor (o nome do Governador da Província de Hokkaido que emitiu a LAR é descrito no nome distinto X.500)
- data de início do período de validade (data que a LAR se faz válida)
- data de encerramento do período de validade (3 dias após considerar válida a LAR)
- próxima data de atualização (1 dia após considerar válida a LCR)
- informações do certificado revogado (número de série, data de revogação, razão da revogação)
- maiores informações

7-2-3 Registro de revogação (LAR) do certificado de assinatura própria

No registro de revogação do certificado de assinatura própria (LAR) são estabelecidas as seguintes informações: O perfil para mais detalhes define-se no perfil da LAR do manual do projeto.

- informação de versão (número da versão do formato da LAR)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para a LAR)
- informações do emissor (o nome do Governador da Província de Hokkaido que emitiu a LAR é descrito no nome distinto X.500)
- data de início do período de validade (data que a LAR se faz válida)
- data de encerramento do período de validade (3 dias após considerar válida a LAR)
- próxima data de atualização (1 dia após considerar válida a LCR)
- informações do certificado revogado (número de série, data de revogação, razão da revogação)
- maiores informações

7-2-4 Registro de revogação (LAR) do certificado de ligação

No registro de revogação do certificado de ligação (LAR) são estabelecidas as seguintes informações: O perfil para mais detalhes define-se no perfil da LAR do manual do projeto.

- informação de versão (número da versão do formato da LAR)
- identificador algoritmo (o Governador da Província de Hokkaido utiliza as informações algoritmo no momento da assinatura para a LAR)
- informações do emissor (o nome do Governador da Província de Hokkaido que emitiu a LAR é descrito no nome distinto X.500)
- data de início do período de validade (data que a LAR se faz válida)
- data de encerramento do período de validade (3 dias após considerar válida a LAR)
- próxima data de atualização (1 dia após considerar válida a LCR)
- informações do certificado revogado (número de série, data de revogação, razão da

revogação)
・maiores informações

8. Controle da Declaração de Práticas

8-1 Mudança do controle da Declaração de Práticas

O Governador da Província de Hokkaido faz alterações nesta Declaração de Práticas se necessário.

8-2 Publicação e notificação

Se alterações forem feitas nesta Declaração de Práticas, o Governador da Província de Hokkaido publica as Declarações de Práticas da Web que mudaram o mais breve possível. A partir desta, se faz a notificação ao usuário, verificadores de assinatura e identificador de assinatura, etc.

8-3 Procedimentos de aprovação da Declaração de Práticas

A partir da decisão do Governador da Província de Hokkaido se faz eficaz.