Presidência da República
Casa Civil da Presidência da República

PARTE I-1
POLÍTICA DE CERTIFICADO DA ICP-BRASIL
ASSINATURA DIGITAL
NÍVEL 4

1 Introdução

1.1 Visão Geral

Este documento tem como objetivo especificar a Política de Certificado (PC) para assinatura digital de nível 4 de segurança pertinente à Infra-Estrutura de Chave Pública Brasileira (ICP-Brasil). Esta política é responsável pelo estabelecimento de um conjunto de regras específicas à aplicabilidade dos certificados em conformidade com os requisitos de segurança estabelecidos na Política de Segurança da ICP-Brasil.

A Autoridade Certificadora Raiz (AC Raiz), as Autoridades de Registro (AR) e demais Autoridades Certificadoras (AC) são consideradas entidades constituintes da ICP-Brasil.

A AC Raiz poderá realizar certificação cruzada com outras ICP externas, desde que aprovada pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil).

São oito (8) os tipos de certificados digitais de usuários da ICP-Brasil. Estes certificados estão classificados quanto à segurança, sendo quatro (4) relacionados com assinatura digital e quatro (4) com sigilo, conforme descrito abaixo:

Certificados de Assinatura Digital:

- Nível 1 - nível alto de segurança para assinatura digital;
- Nível 2 - nível médio de segurança para assinatura digital;
- Nível 3 - nível básico de segurança para assinatura digital;
- Nível 4 – nível ordinário de segurança para assinatura digital;

Certificados de Sigilo:

- Nível 1 - nível alto de segurança para sigilo;
- Nível 2 - nível médio de segurança para sigilo;
- Nível 3 - nível básico de segurança para sigilo;
- Nível 4 – nível ordinário de segurança para sigilo.

Quaisquer tipos de certificados listados acima, de assinatura ou sigilo, poderão conforme a necessidade ser emitidos para pessoas físicas, jurídicas, equipamentos ou aplicações.

As AC integrantes da ICP-Brasil só podem emitir os tipos de certificados descritos acima, porém não são obrigadas a implementar todos os tipos.

Esta política de certificado para assinatura digital especifica aspectos quanto à gerência e utilização dos certificados de usuários.

1.2 Identificação da Política

Os certificados emitidos sob esta Política devem possuir, na extensão de Política de Certificado conforme definido na RFC 2459, quando disponível, o seu identificador de objeto (“object identifier” ou OID). Enquanto o OID específico não estiver disponível deverá ser utilizado o OID = 2.5.29.32.0, correspondente à “any policy”, com o atributo ID-QT-CPS(1.3.6.1.5.5.7.2.1) com a URI da página Web que contém a Declaração de Regras Operacionais (DRO) desta Autoridade Certificadora (AC).

Esta política foi projetada para identificar regras específicas e responsabilidades para as AC na emissão deste tipo de certificado, e para as AR na execução de suas tarefas.

O certificado de assinatura digital nível 4 corresponde ao mínimo necessário para a validação de uma assinatura eletrônica no âmbito da ICP-Brasil.

Cada AC terá uma Lista de Certificados Revogados (LCR), na qual este certificado, quando revogado, estará armazenado. As regras de revogação de certificados pela AC serão abordadas nesta política.

As chaves privadas da assinatura digital não poderão ter cópias, a não ser a cópia de segurança feita pelo próprio usuário e mantida em seu poder, ou serem armazenadas em locais não apropriados. A responsabilidade pela sua guarda e manutenção de seu sigilo é exclusivo do usuário da mesma.

Qualquer informação pessoal armazenada pela AC não estará disponível, a menos que solicitada via meios legais.

Qualquer AC estará sujeita a possíveis inspeções, quanto a sua operacionalidade, de acordo com as regras definidas pelo CG ICP-Brasil.

1.3 Abrangência e Aplicabilidade

1.3.1 Autoridade Certificadora Raiz (AC Raiz)

A AC Raiz é a responsável pela emissão e manutenção dos certificados das demais Autoridades Certificadoras integrantes da ICP-Brasil. A AC Raiz é a única Autoridade Certificadora da ICP-Brasil que emite certificados auto-assinados.

O certificado da AC Raiz é o certificado de mais alto nível hierárquico presente nos serviços da ICP-Brasil. Ele contém a chave pública que corresponde à chave privada usada para assinar os certificados das AC participantes da ICP-Brasil e para assinar a LCR da AC Raiz publicada em diretório ou página web.

Detalhes de identificação do Nome Distinto (ND) da AC Raiz:

C = BR
O = ICP-Brasil
OU = Autoridade Certificadora Raiz
OU = Instituto Nacional de Tecnologia da Informação – ITI

SP = São Paulo
L = Campinas
CN = Autoridade Certificadora Raiz Brasileira

Comprimento das chaves criptográficas

O comprimento das chaves privada e pública RSA da AC Raiz é de, no mínimo, 2048 bits, devendo ser este valor revisto periodicamente, de acordo com as definições estabelecidas pelo CG ICP-Brasil.

Auto-assinatura

O certificado próprio da AC Raiz é auto-assinado.

Algoritmo de assinatura

O certificado próprio da AC Raiz utilizará o algoritmo SHA-1, ou outro de segurança superior, com cifração RSA, devendo estes algoritmos serem revistos periodicamente, de acordo com as definições estabelecidas pelo CG ICP-Brasil.

1.3.2 Autoridades Certificadoras (AC) integrantes da ICP-Brasil

São todas as Autoridades Certificadoras de órgãos e entidades públicas e privadas licenciadas pelo CG ICP-Brasil.

A lista de Autoridades Certificadoras que podem aceitar solicitações para serviços da ICP-Brasil pode ser encontrada em: http://www.ICPBrasil.gov.br/listaAC

1.3.3 Autoridades de Registro

As AR são responsáveis por receberem as requisições de emissão ou de revogação de certificados digitais de usuários, confirmarem a identidade destes usuários e a validade de sua requisição e encaminharem esses documentos à AC responsável.

As AR serão definidas pelas AC licenciadas, estando estas sujeitas às auditorias, normas e sanções previstas pelo CG ICP-Brasil.

A lista de Autoridades Registradoras que podem aceitar solicitações para serviços da ICP-Brasil pode ser encontrada em: http://www.ICPBrasil.gov.br/listaAC

1.3.4 Repositórios

Cada AC integrante da ICP-Brasil manterá diretório ou página Web para armazenamento de seus certificados emitidos, do certificado da AC Raiz, das LCR da AC e da AC Raiz, da PC e de outras informações julgadas úteis pela AC ou definidas pelo CG ICP-Brasil. Estas informações quando disponibilizadas em página Web terão a sua integridade assegurada pela AC.

Para AC públicas ou privadas que prestarem serviço ao governo, o uso de diretório será obrigatório.

1.3.5 Usuários dos Certificados Digitais

A AC Raiz emitirá certificados digitais para as demais AC integrantes da ICP-Brasil.

As AC emitirão os certificados, aos quais esse documento faz referência, para os seguintes usuários:

- Pessoas Físicas ou Jurídicas;
- Equipamentos (estações de trabalho, roteadores e servidores);
- Aplicações.

1.3.6 Aplicabilidade

As regras e práticas especificadas neste documento aplicam-se a todo e qualquer serviço de sigilo, de autenticação e de integridade de dados, de irrevogabilidade e de irretratabilidade das transações eletrônicas e das aplicações que utilizem certificados digitais no âmbito da ICP-Brasil.

1.3.7 Aplicações

As aplicações que utilizam os certificados digitais da ICP-Brasil devem ser capazes de:

- Manipular de forma correta a transferência e a utilização de chaves públicas e privadas;
- Verificar e validar os certificados com os seus níveis de segurança; e
- Informar ao usuário qualquer problema ocorrido durante a transação.

1.4 Dados de Contato

Esta Política de Certificado é administrada pelo CG ICP-Brasil :

Contato*:*_____
Instituição: _____
Endereço: _____
Telefone: _____
Fax: _____
Correio Eletrônico: _____

2 Disposições Gerais

2.1 Obrigações

2.1.1 Obrigações da AC Raiz

A AC Raiz é responsável por todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais das AC licenciadas, de acordo com as práticas e regras dispostas neste documento e na DRO da AC Raiz, incluindo:

- emissão de certificados;
- revogação de certificados;
- renovação de certificados;
- emissão de Lista de Certificados Revogados - LCR;
- publicação de LCR em diretório ou página Web;
- gerência de chaves criptográficas;
- publicação de DRO;
- fiscalizar o cumprimento desta política pelas AC.

O pessoal da AC Raiz no desempenho de suas atribuições deve ter suas ações registradas de modo que cada ação realizada esteja associada à pessoa que a realizou.

A AC Raiz deve informar a emissão do certificado à AC que a requisitou, e deve publicar no Diário Oficial da União e Diretório ou página Web da AC Raiz, disponível a todos os integrantes da ICP-Brasil.

Quando a AC Raiz emite um certificado, ela garante que as informações contidas nesse certificado foram verificadas de acordo com este documento e a DRO da AC Raiz.

A AC Raiz deve garantir que a emissão do certificado ocorra em no máximo duas horas após a requisição do mesmo.

A AC Raiz deve seguir os procedimentos de revogação e renovação de certificados descritos neste documento.

A AC Raiz deve garantir que sua chave privada de assinatura será utilizada apenas para assinar os certificados das AC integrantes da ICP-Brasil e sua LCR.

2.1.2 Obrigações das AC

A AC operará de acordo com a sua Declaração de Regras Operacionais (DRO) e esta Política de Certificação (PC), quando da emissão de certificados que se submetam a esta PC.

A AC tomará as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento dos seus respectivos direitos e obrigações com respeito a operação e gerenciamento de quaisquer chaves, certificados ou “hardware” e “software” usados nas operações de certificação.

A AC é responsável por todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais de acordo com as práticas e regras dispostas neste documento, incluindo:

- emissão de certificados;
- revogação de certificados;
- renovação de certificados;
- emissão de Lista de Certificados Revogados - LCR;
- publicação de LCR em diretório ou página Web;
- disponibilização de consulta on-line à situação do certificado (OCSP) quando requerida;
- gerência de chaves criptográficas;
- publicação de sua DRO;
- fiscalização do cumprimento desta política pelos usuários.

O pessoal da AC no desempenho de suas atribuições deve ter suas ações registradas de modo que cada ação realizada esteja associada à pessoa que a realizou.

As AC devem informar a emissão do certificado ao usuário que o requisitou.

As AC integrantes da ICP-Brasil devem assegurar a proteção de suas chaves privadas conforme definido neste documento.

A AC irá informar aos usuários os direitos e obrigações previstos nesta PC. Esta notificação pode ser na forma de termo de acordo ou termo de aceitação de uso da PC. A notificação descreverá: o uso permitido dos certificados emitidos em acordo com esta PC; as obrigações dos usuários quanto à proteção das chaves; procedimentos para comunicações entre o usuário e a AC ou AR.

Os usuários serão notificados quando ocorrer suspeita de comprometimento de chave, renovação de chave ou certificado, cancelamento de serviço e resolução de disputas.

A AC deve garantir que a emissão do certificado ocorra em no máximo cinco (5) dias úteis após a requisição do mesmo e entrega da documentação necessária.

A AC deverá assegurar que os procedimentos de expiração, revogação e renovação dos certificados estarão em conformidade ao previsto nesta PC e serão previstos no Termo de Acordo dos usuários ou outro documento que descreva os termos e condições de uso desta PC.

A AC deve assegurar os procedimentos de troca de chave de acordo com o item 4.7 (Troca de Chaves)

A AC deve assegurar que a informação de revogação seja enviada a LCR dentro dos limites estabelecidos nos itens 4.4.3 (Procedimentos para solicitação de Revogação) e 4.9 (Extinção de AC).

A AC deve assegurar que as chaves privadas serão protegidas e ativadas de acordo com os itens 4 (Requisitos Operacionais) e 6 (Controles Técnicos de Segurança).

Uma AC integrante da ICP-Brasil deve garantir que sua chave privada de assinatura será utilizada apenas para assinar os certificados de usuários da ICP-Brasil e sua LCR.

2.1.3 Obrigações das AR

Cabe a AR receber as requisições de certificados ou revogação de certificados por usuários, confirmar a identidade destes usuários e a validade de sua requisição, encaminhar esses documentos à AC responsável e entregar, se assim previsto, os certificados assinados pela AC aos seus respectivos solicitantes.

As ações executadas nos serviços da AR devem se individualmente identificadas e registradas.

A AR é obrigada a informar os usuários da emissão ou revogação de certificados.

A AR deve reconhecer a identidade do usuário de acordo com os itens 3 (Identificação e Autenticação) e 4 (Requisitos Operacionais), quando for submeter informação de usuário para a AC.

A AR deve assegurar a proteção das chaves privadas utilizadas em sua operação conforme definido neste documento.

A AR deve garantir que os certificados emitidos para sua operação serão utilizados apenas com esse propósito.

2.1.4 Obrigações dos usuários

Os certificados devem ser utilizados de forma apropriada, conforme previsto neste documento.

Os direitos e obrigações de um usuário membro da ICP-Brasil são contemplados por esta política. Os usuários de outras ICP que façam uso da ICP-Brasil terão seus direitos e obrigações cobertos por um acordo de certificação cruzada.

Antes de um certificado ser dado como válido, deve-se verificar a ausência do mesmo na LCR de acordo com os procedimentos estabelecidos no item 4.4.10. Como parte desse processo de verificação, a assinatura digital da LCR deve ser realizada.

Toda informação necessária para identificação do usuário deve ser fornecida de forma completa e precisa. O usuário é responsável, ao aceitar o certificado emitido, por todas as informações contidas no mesmo.

O usuário deve garantir a proteção de suas chaves privadas, senhas e equipamentos criptográficos conforme previsto neste documento.

O usuário deve utilizar suas chaves privadas apenas para os usos previstos neste documento.

O usuário deve informar a AC e solicitar a revogação do certificado de imediato caso exista qualquer comprometimento da chave privada.

2.1.5 Obrigações dos responsáveis por sistemas que empregam certificação digital

Sistemas e aplicações que façam uso de certificados digitais, referenciados nesta PC, devem obedecer aos seguintes requisitos:

- a segurança provida pelo sistema ou aplicação segue as regras e práticas descritas neste documento;
- o propósito da utilização de certificados digitais deve ser legal e previsto neste documento;
- deve ser realizada a verificação do estado dos certificados digitais e somente os certificados válidos podem ser aceitos pelas aplicações, de acordo com os procedimentos estabelecidos no item 4.4.10 (Requisitos para Verificação de LCR);
- verificar a validade do certificado do usuário e de toda a sua cadeia até a AC Raiz da ICP-Brasil;
- verificar as assinaturas de todos os certificados até a AC Raiz da ICP-Brasil.

2.1.6 Obrigações do Repositório

Em caso de uso de repositório, o mesmo deve estar disponível para consulta durante 24 horas por dia. Certificados e LCRevogados devem ser atualizados de acordo com os requisitos estabelecidos no item 4.4.9 (Freqüência de atualização das LCR).

2.2 Responsabilidades

É responsabilidade das entidades participantes da ICP-Brasil:

- adotar as medidas de segurança e controle, envolvendo os processos, procedimentos e atividades, de modo a garantir a segurança e a confiabilidade da ICP-Brasil;
- manter os processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas para a ICP-Brasil;
- manter e garantir a integridade e a segurança dos dados sob a sua guarda; e
- manter e testar regularmente planos de contingência e de recuperação de desastres.

2.3 Responsabilidade Financeira

É responsabilidade das entidades participantes da ICP-Brasil arcar com os custos de implementação, gerenciamento e manutenção de todos os seus processos e atividades inerentes, devendo, portanto, dispor de recursos para manter suas operações e cumprir suas obrigações, além de ter condições de arcar com responsabilizações por erros ou omissões, podendo ter cobertura de seguro.

O governo brasileiro não se responsabiliza por perdas financeiras que ocorram a qualquer usuário da ICP-Brasil.

2.4 Interpretação e conflito de cláusulas

No evento de qualquer conflito ou inconsistências entre esta PC e outras leis ou contratos, o detentor do Certificado ficará sujeito às cláusulas desta PC, exceto no que diz respeito a outros contratos (i) pré-datando a primeira edição pública da PC ou (ii) expressamente substituindo esta PC com base na qual o contrato será redigido no que diz respeito às partes dispostas e exceto no caso das cláusulas desta PC serem proibidas por lei.

As leis do Brasil devem regular a exigibilidade, interpretação e validade desta PC, independente do contrato ou outra opção de disposições legais.

Antes de recorrer a qualquer mecanismo de resolução de controvérsias (incluindo litígio ou arbitragem, conforme detalhado abaixo), em se tratando de uma controvérsia envolvendo qualquer aspecto da PC ou um certificado emitido por uma AC da ICP-Brasil, as partes que se julguem lesadas devem notificar a AC pertinente e qualquer outra parte visando buscar a resolução da controvérsia entre eles.

Se a controvérsia não for resolvida em 15 (quinze) dias após a notificação inicial, uma das partes poderá enviar a controvérsia por escrito, ou através de formulário eletrônico, para o CG da ICP-Brasil solicitando avaliação do caso. Como resposta, o CG da ICP-Brasil irá reunir fatos relevantes com a finalidade de facilitar a resolução da controvérsia. A parte solicitante deve enviar uma cópia do argumento a todas as partes. Qualquer uma das partes que não tiver apresentado a questão poderá fornecer as informações adequadas ao CG da ICP-Brasil em uma (1) semana, após a data em que a controvérsia foi enviada ao mesmo. O CG da ICP-Brasil deverá finalizar e comunicar suas recomendações às partes dentro de 3 (três) semanas (a menos que as partes concordem mutuamente em estender este período para uma data especificada) depois que a questão tiver sido enviada ao mesmo. O CG da ICP-Brasil poderá comunicar-se por meio de correio eletrônico, teleconferência, mensageiros e correios. As recomendações do CG da ICP-Brasil não obrigarão as partes.

2.5 Taxas

As taxas, quando aplicáveis, deverão ser definidas de acordo com as regras estipuladas pelo CG da ICP-Brasil.

2.6 Publicação e Repositório

Uma AC deve:

- Incluir nos seus certificados emitidos a URL ou site Web de referência da AC.
- Assegurar a publicação de sua PC, podendo ser assinada digitalmente por um representante autorizado da AC.
- Assegurar o acesso ao repositório, quando existente, apenas para pessoal autorizado para as operações de escrita ou modificação.
- Fornecer uma versão completa da DRO quando solicitada para os propósitos de auditoria, inspeção e licenciamento.

A publicação de LCR deve estar em conformidade com os requisitos operacionais.

2.7 Auditoria

A auditoria deve verificar se todos os processos, procedimentos e atividades das AC da ICP-Brasil estão em conformidade com a DRO da AC, esta PC e normas de segurança da ICP-Brasil.

2.7.1 Periodicidade da Auditoria

As AC participantes da ICP-Brasil deverão sofrer auditoria:

- antes do seu licenciamento na ICP-Brasil;
- anualmente para fins de continuidade do licenciamento; e
- a qualquer tempo, sem aviso prévio, por determinação do CG da ICP-Brasil ou da AC Raiz.

2.7.2 Identidade e qualificação do auditor da AC

Pessoa ou entidade, credenciada pelo CG da ICP-Brasil, que possuir larga experiência nas tecnologias de ICP, criptografia e na operação de softwares de ICP.

2.7.3 Relação entre as partes (auditor e auditado)

O auditor deverá ser totalmente independente da AC auditada.

Nenhuma pessoa poderá ser designada como auditor se for: sócio ou membro de empresa que possua algum tipo de relação com membros da AC auditada.

O auditor será declarado impedido de realizar auditoria, quando:

- houver motivo íntimo declarado;
- for amigo intimo ou inimigo capital de membros da AC auditada;
- tiver recebido, nos últimos 5 anos, da AC auditada, pagamentos referentes à prestação de serviços;
- estiver interessado no resultado da auditoria da AC auditada; e
- houver relacionamento de fato ou de direito, como cônjuge, parente, consangüíneo ou afim, com algum dos membros da AC auditada, em linha reta ou na colateral até o terceiro grau.

2.7.4 Tópicos cobertos pela auditoria

As inspeções de conformidade verificarão todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de requisição, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.

Todos os eventos significativos ocorridos em um sistema de AC/AR devem ser guardados em trilhas seguras de auditoria, onde cada entrada possua o registro de data, hora e tipo de evento, com assinatura, para garantir que as entradas não possam ser falsificadas.

2.7.5 Ações a serem tomadas em caso de não conformidade

Cabe à entidade inspecionada cumprir, no prazo estipulado pelo CG da ICP-Brasil, as recomendações dos inspetores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará no cancelamento da licença da entidade inspecionada.

No caso de algum comprometimento crítico, cabe à AC Raiz tomar todas as medidas cabíveis a fim de garantir a segurança e a confiabilidade da ICP-Brasil. Neste caso, o licenciamento da entidade inspecionada será cancelado imediatamente.

2.7.6 Comunicação dos resultados

Os resultados das inspeções de conformidade terão sempre caráter sigiloso, sendo informados pelos inspecionados somente à entidade inspecionada e à AC Raiz, que estipulará o prazo para o cumprimento das recomendações dos inspetores. O não cumprimento dos prazos acarretará no cancelamento da licença da entidade inspecionada. No caso de comprometimento crítico, o CG da ICP-Brasil poderá determinar o cancelamento da licença imediatamente.

Cabe ao CG da ICP-Brasil manter os integrantes da ICP-Brasil informados do licenciamento ou de seu cancelamento.

2.8 Sigilo

Certificados e LCR, e informação corporativa ou pessoal que apareçam neles e em diretórios públicos, não são considerados informações públicas. Todas as outras informações pessoais ou corporativas mantidas pela AC ou uma AR não podem ser divulgadas sem consentimento prévio do usuário, a menos que por determinação judicial.

A chave privada da Assinatura Digital de cada usuário é para ser mantida somente pelo usuário devendo o mesmo assegurar seu sigilo. Qualquer divulgação da chave privada de assinatura pelo usuário será de sua inteira responsabilidade.

Informação de inspeção é considerada sensível e não deve ser divulgada a ninguém em nenhuma hipótese a menos para os propósitos de inspeção ou por exigência legal.

Qualquer divulgação de informação está sujeita aos requisitos estabelecidos na legislação em vigor.

2.9 Direitos de propriedade intelectual

Não estipulado

3 Identificação e Autenticação

3.1 Registro inicial

3.1.1 Tipos de nomes

Essa política não permite o uso de pseudônimos no certificado.

Os tipos de nomes possíveis estão definidos no item 7.

3.1.2 Necessidade de nomes que possuam significados

Todos os certificados emitidos pela ICP-Brasil devem incluir um identificador que represente o indivíduo para o qual o certificado foi emitido. Esse identificador deve ser definido de modo a permitir identificar a identidade real do usuário de forma individual.

Caso o certificado esteja associado com uma função ou posição, o certificado deve conter a identificação da pessoa que ocupa a função ou posição.

O certificado emitido para um equipamento ou aplicação deve incluir no Nome Distinto (ND), conforme o padrão X.509 v3, o nome da pessoa ou organização responsável pelo equipamento ou aplicação.

3.1.3 Regra para interpretação de forma de nomes variados

Não definido

3.1.4 Unicidade de nomes

Nomes Distintos devem ser únicos para cada usuário de uma AC. Para cada usuário números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo RDN, conforme o padrão X.509 v3. A facilidade de “Unique Identifiers” para diferenciar usuários como nomes idênticos não será suportada.

3.1.5 Procedimentos para disputa de nomes

A AC reserva-se o direito de tomar todas as decisões referentes aos nomes das entidades em todos os seus certificados emitidos. A parte que está solicitando o certificado deve provar o seu direito de uso de um nome específico.

A AC deve assegurar por meio de contrato as situações de disputa de nome em repositórios que não estejam sob o controle da AC.

3.1.6 Método para comprovar posse de chave privada

Deve ser verificado pela AC ou pela AR se o usuário possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital.

O protocolo de transferência de chave descrito na RFC 2510 é indicado para este fim.

3.1.7 Autenticação da identidade de um indivíduo

A identificação e autenticação de um indivíduo tem de ser executada através de uma das seguintes formas:

- a AR irá comparar a identidade do indivíduo com dois (2) tipos de identificação (fotocópia autenticada ou original). Pelo menos um destes deve ser um documento de identificação legalmente aceito com fotografia; ou
- por meio de processo realizado em empresa ou órgão onde a identidade de seus funcionários já foi previamente estabelecida, utilizando procedimentos que atendam aos requisitos da PC.

Deve-se manter um arquivo com o tipo e detalhes da identificação utilizada.

3.1.8 Autenticação de equipamentos ou de aplicações

Uma solicitação de emissão de certificado para um equipamento ou aplicação deve ser realizada por uma pessoa física a qual será responsabilizada legalmente por sua utilização.

A identificação e autorização do requerente deve seguir o descrito na PC. A AR deve verificar também a sua autorização para recebimento das chaves relativas àqueles equipamentos ou aplicações.

Deve-se manter um arquivo com o tipo e detalhes da identificação utilizada.

3.2 Autenticação para rotina de renovação de chave

Esta PC não permite a renovação de chave sem a repetição do processo de autenticação.

3.3 Autenticação para renovação de chave após revogação

Esta PC não permite a renovação de chave após sua revogação.

3.4 Autenticação para requisição de revogação

Toda solicitação de revogação deve autenticar a origem.

Uma AC deve estabelecer e tornar publicamente disponível tanto o procedimento pelo qual ela recebe tais solicitações, quanto os meios pelos quais ela estabelecerá a validade da solicitação.

Solicitações para revogação de certificados devem ser documentadas.

4 Requisitos Operacionais

4.1 Solicitação de emissão de um certificado

As AC/AR devem assegurar que todos os procedimentos e requisitos que se relacionam a solicitação de emissão de um certificado estejam previstos na DRO ou em um documento público disponível.

As AC/AR devem assegurar que cada solicitação seja acompanhada, quando cabível, por:

- prova da identidade do usuário;
- comprovação dos atributos de identificação constantes do certificado;
- uma notificação de reconhecimento, no caso de funcionários ou servidores; e
- um acordo assinado, que dispõe os termos e condições aplicados ao uso do certificado.

4.1.1 Acordos de Certificação Cruzada

Os acordos de certificação cruzada e mapeamento de políticas entre a ICP-Brasil e outras ICP externas serão aprovados pelo CG da ICP-Brasil, mediante análise criteriosa da conformidade, da oportunidade, da viabilidade e de outros princípios julgados cabíveis pelo CG da ICP-Brasil.

O estabelecimento de acordo de certificação cruzada deve ser precedido de um estudo profundo, pelo Comitê Gestor, de pelo menos os seguintes itens:

- PC e DRO da ICP em análise; e
- o resultado de uma auditoria, comprovando e validando os níveis de segurança estabelecidos na ICP em análise.

No caso do CG da ICP-Brasil autorizar a utilização de certificação cruzada de uma AC de ICP externa, esta AC será certificada pela AC-Raiz da ICP-Brasil.

4.2 Emissão de Certificado

A emissão e a publicação de um certificado por uma AC indica que o mesmo foi total e completamente aprovado e validado em todas as etapas e processos da referida AC.

4.3 Aceitação de Certificado

Uma AC deve garantir que um usuário reconheça a aceitação dos seus certificados. No caso de objetos, este reconhecimento deve ser feito pelo indivíduo ou organização responsável pelos respectivos equipamentos.

4.4 Suspensão e Revogação de Certificados

4.4.1 Circunstâncias para Revogação

Um certificado deve ser revogado:

- quando for alterada qualquer informação constante do mesmo; ou
- no caso de comprometimento da chave privada ou da sua respectiva

mídia armazenadora.

Uma AC poderá, a seu critério, revogar o certificado do usuário que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas.

O CG da ICP-Brasil poderá, a seu critério, revogar o certificado ou a certificação cruzada, conforme o caso, da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas.

4.4.2 Quem pode solicitar Revogação

A revogação de um certificado somente pode ser requerida:

- à AR, pelo usuário em cujo nome foi emitido o certificado, que encaminha à AC emitente;
- pela AC emitente; ou
- pela AR associada.

A revogação de uma certificação cruzada somente poderá ser requerida:

- pela AC cuja certificação cruzada foi aceita; ou
- pelo CG da ICP-Brasil.

4.4.3 Procedimentos para solicitação de Revogação

Uma AC deve garantir que todos os seus usuários possam, facilmente e a qualquer tempo, solicitar revogação de certificado. As solicitações de revogação autenticadas, juntamente com as respectivas ações resultantes das AC, devem ser registradas e armazenadas. Quando um certificado é revogado, todas as justificativas para a revogação devem ser documentadas.

As revogações de certificados devem ser publicadas nas LCR correspondentes. As revogações de certificações cruzadas são publicadas na LCR da AC-Raiz.

4.4.4 Duração do Processo de Revogação

O processo de revogação de um certificado deve estar concluído, com o respectivo certificado revogado, em até vinte e quatro (24) horas após o recebimento da solicitação de revogação.

4.4.5 Circunstâncias para Suspensão

A suspensão de certificados não é prevista pelo CG da ICP-Brasil.

4.4.6 Quem pode solicitar Suspensão

Não aplicável.

4.4.7 Procedimentos para solicitação de Suspensão

Não aplicável.

4.4.8 Limites para o período de Suspensão

Não aplicável.

4.4.9 Freqüência de atualização das LCR

Uma AC deve garantir que sua LCR é atualizada pelo menos a cada vinte e quatro (24) horas.

Uma AC deve também garantir que seu repositório, se utilizado, seja sincronizado com o diretório da ICP-Brasil, assegurando a acessibilidade dos usuários às LCR mais recentes.

Quando um certificado é revogado devido ao comprometimento da chave, a atualização da LCR deve ser imediata.

4.4.10 Requisitos para verificação de LCR

Todos os certificados devem ter a validade verificada, nas respectivas LCR das AC emitentes, antes de serem utilizados. Opcionalmente pode-se consultar a situação de um certificado diretamente na AC emitente, através do uso do protocolo OCSP. Também deve ser verificada a autenticidade das AC na LCR da AC-Raiz.

4.4.11 Requisitos especiais relativos ao comprometimento de chave privada

No caso do comprometimento da chave privada de assinatura digital de um usuário dos serviços da ICP-Brasil, o usuário deverá notificar imediatamente a AC que emitiu o certificado.

Uma AC deverá garantir que a sua DRO contém determinações que definam os meios que serão utilizados para se notificar um comprometimento ou suspeita de comprometimento.

4.5 Procedimentos de auditoria do sistema de segurança

4.5.1 Tipos de eventos registrados

Uma AC deve registrar em arquivos de registro de auditoria todos os eventos relacionados à segurança do sistema de certificação. Os seguintes eventos devem obrigatoriamente estar incluídos no arquivo de registro:

- inicialização e desligamento do sistema de certificação;
- inicialização e desligamento de aplicação de certificação;
- tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC;
- mudanças na configuração da AC e/ou nas suas chaves;
- mudanças nas políticas de criação de certificados, por exemplo, mudança no período de validade dos certificados;
- tentativas de acesso (*login*) e de saída do sistema (*logoff*);
- tentativas não-autorizadas de acesso ao sistema de certificação através da rede de computadores;
- tentativas não-autorizadas de acesso aos arquivos de sistema;

- geração de chaves próprias da AC ou de chaves de usuário;
- criação e revogação de certificados;
- tentativas de inicializar, remover, habilitar e desabilitar usuários, e atualizar e recuperar suas chaves; e
- operações falhas de escrita e leitura no diretório de certificados e da LCR.

Todos os registros de auditoria,sejam eletrônicos ou manuais, devem conter a data e a hora do evento e a identidade do usuário que causou o evento.

Uma AC deve também coletar e consolidar, seja eletronicamente ou manualmente, informações de segurança não geradas diretamente pelo sistema de certificação, tais como:
- registros de acessos físicos;
- manutenção e mudanças na configuração do sistema;
- mudanças de pessoal;
- relatórios de discrepância e comprometimento; e
- registros de destruição de mídia contendo chaves criptográficas, datas de ativação de certificados ou informação pessoal de usuário.

Uma AC deve garantir que a DRO indique que informações são registradas.

Para facilitar a tomada de decisões, todos os acordos e documentações relacionados aos serviços da AC deverão ser coletados e consolidados, eletronicamente ou manualmente, num local único, conforme a Política de Segurança da ICP-Brasil.

4.5.2 Freqüência de auditoria dos registros

A AC deve garantir que seus registros de auditoria serão analisados pelo pessoal operacional da AC diariamente e que todos os eventos significativos serão explicados num relatório de auditoria de registros. Tal análise envolverá a verificação que os registros não foram alterados, uma inspeção breve de todos os registros seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nos registros.

Todas as ações tomadas em decorrência da análise deverão ser documentadas.

4.5.3 Período de retenção de um registro de auditoria

Uma AC deverá manter localmente os seus registros de auditoria por pelo menos dois meses e, subseqüentemente, deverá armazená-las da maneira descrita em 4.6 (Arquivo de Registros).

4.5.4 Proteção do registro de auditoria

O sistema de registro de eventos de auditoria deve incluir mecanismos para proteger os arquivos de registros contra leitura, modificação e remoção, não autorizadas.

Informações manuais de auditoria também devem ser protegidas contra leitura, modificação e remoção não autorizadas.

4.5.5 Procedimentos para cópia de segurança dos registros de auditoria

Os registros de eventos e sumários de auditoria devem ter cópias de segurança periódicas.

4.5.6 Sistema de Armazenamento de registro de auditoria

A AC deve identificar seu conjunto de sistemas de auditoria na DRO.

4.5.7 Notificação de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria, nenhuma notificação deve ser enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8 Avaliação das vulnerabilidades

Uma parte dos eventos gerados nos processos de auditoria serão registrados para monitorar as vulnerabilidades do sistema. A AC deve assegurar que a avaliação de vulnerabilidades foi realizada, revista e revisada, após o exame desses eventos monitorados.

4.6 Arquivo de registros

Os certificados de assinatura digital, chaves privadas armazenadas pela AC, AR e LCR, geradas pela AC, devem ser retidas, no mínimo por um ano após a data de expiração. Esta exigência não inclui a cópia de segurança das chaves de assinatura privada.

As informações de auditoria como detalhado no item 4.5, contratos de usuários e qualquer informação de identificação e autenticação devem ser retidas no mínimo por 06 (seis) anos.

As chaves privadas que estão na cópia de segurança da AC devem ser protegidas no nível físico e também por criptografia com os mesmos requisitos de segurança, ou superiores, que os das instalações do site da AC.

Uma segunda cópia de todo o material retido ou da cópia de segurança deve ser armazenada em local que não seja o site da própria AC devendo receber o mesmo tipo de proteção utilizada pela AC. Esse site secundário deve possuir proteção adequada contra ameaças do ambiente, tais como temperatura, umidade e eletromagnética.

A AC deverá verificar a integridade das cópias de segurança a cada seis (6) meses.

4.7 Troca de Chaves

A AR deverá solicitar a troca de par de chaves dos usuários três (3) meses antes da data em que a mesma estará expirando, de forma que o seu certificado ainda não tenha sido revogado. Uma AC deverá certificar-se que os detalhes deste processo estão descritos em sua DRO.

Usuários que não tenham seu par de chaves válido devem passar por todo o processo de identificação previsto, devendo a AC verificar se houve algum fato comprometedor que impediu a renovação.

As chaves não devem ser renovadas utilizando chave de assinatura digital que já expirou.

4.8 Comprometimento e Recuperação de Desastre

4.8.1 Recursos Computacionais, Aplicativos e/ou Dados Corrompidos

Uma AC deve estabelecer um Plano de Contingência que estabeleça os passos a serem tomados no caso de corrupção ou perda dos recursos computacionais, dos aplicativos e/ou dos dados.

4.8.2 Revogação do Certificado de uma Autoridade Certificadora

No caso de revogação do Certificado de Assinatura Digital de uma AC, ela deverá imediatamente informar:

- a AC Raiz e o CG da ICP-Brasil;
- todas as AC subordinadas;
- todos os usuários e usuários;
- todas as pessoas e organizações que façam uso do seu certificado em alguma aplicação ou dispositivo.

A AC também deverá publicar o número do certificado na LCR pertinente.

Depois de verificar os fatores que levaram a revogação, a AC deverá:

- gerar um novo par de chaves de assinatura digital;
- reemitir os certificados de todos os seus usuários e usuários, certificando-se que todas as LCR, sob sua responsabilidade, estão assinados com a nova chave.

4.8.3 Comprometimento da Chave de uma Autoridade Certificadora

Caso haja o comprometimento, ou suspeita de comprometimento, da chave privada de assinatura de uma AC, ela deverá notificar a AC Raiz e o CG da ICP-Brasil imediatamente.

Caso haja o comprometimento do par de chaves de assinatura de qualquer usuário, este deverá notificar imediatamente a AC responsável.

Uma AC deve garantir que sua DRO e seus acordos operacionais especifiquem de maneira clara a forma como será divulgada o comprometimento ou suspeita do comprometimento de uma chave.

4.8.4 Procedimentos de Segurança Após Qualquer Tipo de Desastre Natural

Uma AC deve estabelecer um Plano de Continuidade de Negócios que descreva os passos a serem tomados no intuito de restabelecer sua operação de maneira segura.

4.9 Extinção de AC

Caso uma AC deixe de operar, os seus usuários devem ser notificados imediatamente quanto ao término das operações, aos acordos de continuidade da guarda das chaves e demais informações a respeito.

Todos os dados e arquivos devem ser mantidos obedecendo os critérios e prazos indicados no item 4.6 (Arquivo de Registros).

5 Segurança Física, Procedimental e de Pessoal

5.1 Controles Físicos

5.1.1 Localização

A localização e o sistema de certificação da AC não deverão ser publicamente identificados.

5.1.2 Acesso Físico

Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação.

Controles duplicados sobre o inventário e cartões/chaves de acesso deverão ser estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves deverá ser mantida.

5.1.3 Energia elétrica e sistemas de condicionamento de ar

Devem existir sistemas que garantam o provimento de energia elétrica e a manutenção do sistema de condicionamento de ar nas instalações das AC.

5.1.4 Exposição à água

Devem ser adotadas meditas de proteção quanto exposição à água.

5.1.5 Prevenção e proteção contra incêndios

Devem ser adotadas medidas de prevenção e proteção contra incêndios.

5.1.6 Armazenamento de mídia

Os meios magnéticos devem ser protegidos contra danos, furtos ou roubos, devendo ser adotados os procedimentos de cópia de segurança definidos.

5.1.7 Procedimentos com manuseio de lixo sensível

Devem ser adotados procedimentos de segurança no trato de lixo sensível.

5.1.8 Estrutura de armazenamento de cópia de segurança

As cópias de segurança devem ser armazenadas em instalações separadas das quais elas são geradas.

5.2 Procedimentos de Controle

5.2.1 Cargos de Confiança

5.2.1.1 Cargos de Confiança da AC

A AC deve garantir a separação das tarefas para funções críticas, prevenindo que um funcionário utilize maliciosamente o sistema da AC sem ser detectado. Cada usuário do sistema de acesso está limitado a aquelas ações para as quais foi designado e definidas nas suas responsabilidades.

A AC deve estabelecer um mínimo de dois (2) cargos distintos para ICP, distinguindo as operações do dia-a-dia do sistema da ICPe as do gerenciamento e auditoria dessas operações. Uma sugestão de divisão das responsabilidades entre os dois (2) cargos pode ser:

Usuário Mestre da ICP:

- configuração e manutenção do hardware e software da AC;
- início e término dos serviços da AC.

Administrador da ICP:

- gerenciamento dos operadores da ICP;
- configuração das políticas de segurança da ICP;
- verificação dos logs de auditoria;
- verificação e cumprimento da PC e DRO;
- gerenciamento dos processos de inicialização dos usuários;
- criação, renovação ou revogação de certificados;
- distribuição de cartões (tokens), quando for o caso.

Somente os funcionários responsáveis por tarefas descritas para o Usuário Mestre da ICP e Administrador de Sistema devem ter acesso ao software e hardware de controle de operação da AC.

5.2.1.2 Cargos de Confiança da AR

A AR deve garantir que seu pessoal tenha conhecimento de sua responsabilidade na identificação e autenticação dos futuros usuários e realizar as seguintes funções:

- aceitar uma solicitação, uma mudança em certificado, uma revogação ou uma requisição de recuperação de chave;
- verificação de identidade do requerente e autorizações; e
- transmissão das informações do requerente para a AC.

5.2.2 Número de funcionários necessários por tarefa

Controle multiusuário também é requerido para a geração da chave de AC como descrito em 6.2.2. Todas as outras tarefas associadas com os cargos da AC podem ser executados por um único funcionário.

Uma AC deve garantir que qualquer processo de verificação terá a supervisão, em todas as atividades executadas, por detentores de cargo com

privilégios na AC.

5.2.3 Identificação e autenticação para cada cargo

Todo o funcionário da AC deve ter sua identidade e autorização verificados antes de ser:

- incluído em uma lista de acesso do site da AC;
- incluído em uma lista para acesso físico ao sistema da AC;
- dado um certificado para executar o seu papel na AC;
- dado uma conta no sistema de ICP.

Cada um desses certificados e contas (com exceção do certificado de assinatura da AC) deve:

- ser diretamente atribuído a um funcionário;
- não pode ser compartilhado;
- ser restrito para as ações definidas para o cargo no uso do software da AC, sistema operacional e procedimentos de controle.

Uma AC deve possuir mecanismos robustos de autenticação forte e criptografia para seu acesso, tais como cartões inteligentes e sistemas de identificação biométrica, dentre outros.

5.3 Controles de segurança pessoal

As AC e AR devem garantir que todos os seus funcionários que executam tarefas operacionais devem:

- ser registrados por escrito;
- ter contrato onde regule os termos e as condições da posição que estarão ocupando;
- ter recebido treinamento adequado para que possam executar as tarefas a eles destinadas;
- ter registrado no contrato o compromisso de não divulgar informações sensíveis de segurança da AC ou informações de usuários;
- não ser designado para tarefas que possam causar conflito de interesses.

5.3.1 Histórico pessoal, qualificações, experiência, e requisitos de permissão

As AC e AR devem garantir que todo o pessoal que realiza atividades relativas às suas operações deverá ter sido aprovado conforme a Política de Segurança da ICP-Brasil.

5.3.2 Requisitos de treinamento

As AC e AR devem garantir que todo o pessoal que realiza atividades relativas à operação da AC ou de uma AR remota tenham recebido treinamento em nível de domínio sobre os temas:

- os princípios e os mecanismos de segurança de AC e AR;
- todas as versões de softwares de ICP em uso na AC;
- todas as atividades de ICP que eles devem realizar; e
- procedimentos de recuperação de desastres e de continuidade de

negócios.

5.3.3 Requisitos e freqüência de novo treinamento

Os requisitos de 5.3.2 devem ser mantidos atualizados para adaptar eventuais mudanças no sistema da AC e da AR. Treinamentos de reciclagem devem ser realizados periodicamente e a AC e a AR devem revisar estes requisitos, pelo menos, uma vez ao ano.

5.3.4 Rotatividade de funcionários

Não estipulado.

5.3.5 Sanções para ações não autorizadas

No evento de uma ação não autorizada, real ou suspeita, realizada por uma pessoa responsável por atividades de operação de uma AC ou uma AR, a AC deverá suspender o seu acesso ao sistema de certificação.

5.3.6 Pessoal contratado

A AC deve garantir que o acesso à AC de pessoal terceirizado de firma contratada esteja de acordo com 5.1.2.

5.3.7 Documentação fornecida ao pessoal

A AC Raiz deve tornar disponível, para o pessoal das AC e das AR, as suas PC, a sua DRO e quaisquer contratos ou políticas que forem relevantes para suas atividades.

6 Controles Técnicos de Segurança

6.1 Instalação e Geração do par de Chaves

6.1.1 Geração de par de chaves

Todo portador de certificado a ser emitido deverá gerar o pares de chaves usando equipamento da AR e um algoritmo aprovado pelo CG da ICP-Brasil.

A chave privada de assinatura, ao ser gerada, deverá ser gravada em um meio físico de armazenamento lógico (disquete, token ou cartão inteligente), protegida pela senha do usuário, e, em nenhuma hipótese, será realizada cópia dessa chave. A guarda da chave privada de assinatura é de responsabilidade do usuário.

6.1.2 Entrega de chave pública para o emissor do certificado

A chave pública deverá ser entregue para a AC pela AR ou pelo próprio usuário utilizando formato compatível com padrão PKCS#10.

6.1.3 Entrega do certificado da AC para os usuários

O certificado da AC deverá ser entregue à AR por meio seguro definido pelo CG da ICP-Brasil.

6.1.4 Tamanho das chaves assimétricas

A AC deve assegurar que o tamanho das chaves das entidades da ICP-Brasil devam ser de, no mínimo 512 bits (RSA), sendo recomendável o uso de pelo menos 1024 bits (RSA).

6.1.5 Geração de Parâmetros de Chave Pública

Os parâmetros de geração de chave pública devem estar de acordo com as determinações do CG da ICP-Brasil e das legislações em vigor.

6.1.6 Verificação de Qualidade dos Parâmetros

Não aplicável.

6.1.7 Geração de Chaves Via Hardware/Software

O par de chaves de assinatura digital da AC deve ser gerado em um módulo de criptografia em hardware ou em software. O par de chaves de assinatura digital nível 4 de todos os usuários pode ser gerado em um módulo de criptografia em hardware ou em software

6.1.8 Propósito de Utilização de Chave

As chaves devem ser utilizadas para autenticação, irretratabilidade e integridade das mensagens. Também poderão ser utilizadas para a

cifração/decifração de chaves de sessão. A chave de assinatura da AC será a única com permissão para assinar os certificados e as LCR.

6.2 Proteção da Chave Privada

O usuário é responsável pela manutenção do sigilo de sua chave privada de modo que a mesma não seja de conhecimento de terceiros.

6.2.1 Padrões para o Módulo de Criptografia

A ser definido pelo CG da ICP-Brasil.

6.2.2 Controle múltiplo (mais de uma pessoa) no processo de geração da chave privada

Deve haver um controle múltiplo (mais de uma pessoa) quando da geração de chaves da AC. Pelo menos duas pessoas integrantes da AC atuando na função de Usuário Mestre da ICP ou Gerente da ICP têm de participar do processo de geração de chaves.

6.2.3 Recuperação de cópia da chave privada

As chaves de assinatura digital não deverão implementar o esquema de recuperação de cópia da chave privada do usuário.

6.2.4 Cópia de segurança da chave privada

Uma entidade poderá, opcionalmente, manter a cópia de segurança de sua própria chave privada de Assinatura Digital. Se este for o caso, as chaves devem ser copiadas e armazenadas cifradas e protegidas a um nível não inferior àquele que o definido para a versão original da chave.

6.2.5 Armazenamento da chave privada

A chave privada deve ser gravada em um meio físico de armazenamento lógico, protegida:

a) na AC-Raiz, por senha, dispositivo de controle de acesso em hardware (“token”) e/ou biometria, utilizando-se o controle múltiplo descrito no sub-item 6.2.2;

b) nas outras AC, do mesmo modo definido acima;

c) pelos usuários em cartão inteligente, “token” ou disquete, por métodos de controle de acesso em conformidade com aqueles definidos no item 6.2.7.

6.2.6 Inserção da chave privada no módulo criptográfico

A chave privada deverá ser inserida no módulo criptográfico de acordo com o Protocolo de Gerenciamento de Certificado da RFC 2510 ou via qualquer outra maneira segura que tenha sido aprovada pelo CG da ICP-Brasil.

6.2.7 Método de ativação da chave privada

O usuário deve ser autenticado via módulo criptográfico antes da ativação da chave privada. Quando desativadas, as chaves devem ser mantidas cifradas.

Como requisitos mínimos, tal autenticação deverá realizada por senha, dispositivo de controle de acesso em hardware (“token”) e biometria.

6.2.8 Método de desativação da chave privada

Quando as chaves forem desativadas elas devem ser eliminadas da memória antes da liberação de memória. Qualquer espaço em disco, onde as chaves estavam armazenadas, tem de ser sobrescrito antes que o mesmo seja disponibilizado para o Sistema Operacional. O módulo criptográfico tem de automaticamente desativar a chave privada após um período pré-estabelecido de inatividade.

6.2.9 Método de destruição da chave privada

Após o término de utilização da chave privada, todas as cópias da chave privada na memória do computador e espaço em disco compartilhado devem ser destruídas de maneira segura conforme o estabelecido pelo CG da ICP-Brasil .

6.3 Outros Aspectos da Gerência de Chaves

6.3.1 Arquivamento da chave pública

A AC que emitiu o certificado deve manter todas as chaves públicas para verificação.

6.3.2 Períodos de uso do par de chaves

Todas as chaves devem ser válidas por um período menor do que vinte anos.

Sugestão de período de validade:
- chave privada de assinatura de usuário – dois anos;
- certificado de assinatura de usuário – dois anos;

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Quaisquer dados de ativação devem ser únicos e imprevisíveis. Os dados de ativação, em conjunto com outros meios de controle de acesso, devem ter um nível apropriado de segurança, para que as chaves ou os dados sejam protegidos.

Onde forem usadas senhas, as entidades que as utilizam devem poder alterá-las a qualquer instante.

6.4.2 Proteção aos dados de ativação

Dados usados para a inicialização de entidades devem ser protegidos contra uso não autorizado através de mecanismos de criptografia e de controle de acesso físico.

As chaves privadas das entidades devem ser protegidas contra uso não autorizado através de mecanismos de criptografia e de controle de acesso físico. O nível de proteção deve ser adequado para deter qualquer tipo de ataque.

6.4.3 Outros aspectos dos dados de ativação

Não estipulado

6.5 Controle de Segurança Computacional

6.5.1 Requisitos técnicos

Cada computador servidor das AC deve possuir as seguintes funcionalidades:

- controle de acesso aos serviços da AC e seus papéis na ICP-Brasil;
- clara separação dos deveres relacionados a cada papel da AC na ICP-Brasil;
- identificação e autenticação dos papéis na ICP-Brasil e identidades associadas;
- limpeza da memória RAM após o uso;
- uso de criptografia para comunicação de seções e segurança da base de dados;
- arquivo do histórico e dos dados de auditoria da AC e entidades clientes;
- auditoria dos eventos relacionados à segurança;
- auto-teste de segurança relacionados aos serviços da AC;
- caminhos confiáveis para identificação dos papéis da AC na ICP-Brasil e identidades associadas;
- mecanismos de cópia de segurança do sistema e das chaves armazenadas.

Estas funcionalidades podem ser providas pelo sistema operacional ou através da combinação do sistema operacional, softwares da ICP-Brasil e segurança física.

6.6 Controles técnicos do ciclo de vida

6.6.1 Controle de desenvolvimento de sistemas

A AC deve utilizar um software que tenha sido projetado e desenvolvido através de uma metodologia formal rigorosa, específica para ambientes de segurança crítica.

Os processos de projeto e o desenvolvimento devem prover documentação suficiente para suportar verificações externas de avaliação de

segurança dos componentes da AC, além de serem fundamentados por:

- verificações externas de conformidade dos processos; e
- análises contínuas de riscos visando minimizar o risco residual.

6.6.2 Controles de gerenciamento da segurança

A configuração do sistema da AC, assim como qualquer modificação ou atualização, deve ser documentada e controlada. Deve haver um método para detecção de alterações não autorizadas no software ou na configuração da AC.

A AC deve possuir um processo de gerenciamento de configuração capaz de suportar a evolução do seu sistema.

Na instalação, e pelo menos uma vez por trimestre, a integridade do sistema da AC deve ser verificada.

6.7 Controles de segurança de rede

O computador servidor da AC deve ser protegido contra ataques provenientes de quaisquer das redes a que estiver conectado. Esta proteção deve ser provida através da instalação de um dispositivo configurado para permitir somente protocolos e comandos requerido para o controle da AC.

6.8 Controles do Módulo de Criptografia

A ser definido pelo CG da ICP-Brasil.

7 Perfis de Certificados e de LCR

7.1 Modelos de Certificados

7.1.1 Definição do Certificado

A AC deverá emitir certificados e LCR segundo o padrão X.509 v3, de acordo com a RFC 2459, e os *softwares* usuários de certificados, devem suportar os campos básicos do X.509 v3:

Versão - inteiro {v3 (2)};

Emissor - nome da Autoridade Certificadora;

Validade - data de geração e de expiração do certificado;

Assinatura - algoritmo utilizado pela AC para assinar o certificado;

Usuário - entidade associada com a chave pública;

Informação da Chave Pública do Usuário - chave pública do usuário; e

Número Serial - número do certificado (identificação única dentro de uma AC).

7.1.2 Extensões do Certificado

O software do usuário de certificados deve suportar os padrões de extensão previstos no item 4.2.1 da RFC 2459.

7.1.3 OID de algoritmos criptográficos

A AC deve usar e as entidades finais devem suportar os seguintes algoritmos para assinatura e verificação :

- RSA 512/1024 de acordo com o PKCS#1 - [OID a ser definido];
- SHA-1 de acordo com o FIPS 180-1 e ANSI X.930 (Parte 2) - [ID shaWithRSAEncryption, OID 1 2 840 113549 1 1 5, Autoridade de emissão RSADSI];

Entidades devem usar os seguintes algoritmos para assinatura e verificação :

- RSA 512/1024 de acordo com o PKCS#1 - [OID a ser definido];
- DSA de acordo com DSS (FIPS PUB 186) e ANSI X.930 (Parte 1) – [OID a ser definido];
- MD5 de acordo com a RFC 1231 – [OID a ser definido];
- SHA-1 de acordo com FIPS 180-1 e ANSI X.930 (Parte 2) – [ID sha1WithRSAEncryption, OID 1 2 840 113549 1 1 5, Autoridade de emissão RSADSI];

O algoritmo simétrico deverá ser aprovado pelo CG da ICP-Brasil.

7.1.4 Formato de nomes

Cada Nome Distinto deve atender o formato X.501 “printableString”.

7.1.5 Restrições de nomes

Os Nomes Distintos para os campos Subject (Usuário) e Issuer (Emissor) devem estar em conformidade com o padrão PKIX e devem estar presentes em todos os certificados.

7.1.6 OID para a Política de certificado

A AC deve assegurar que o OID da política seja incluída em cada certificado emitido.

7.1.7 Uso da extensão policyConstraints

A AC deve preencher e definir como crítica a extensão policyConstraints.

7.1.8 Sintaxe e semântica do policyQualifiers

A AC deve preencher o campo de extensão policyqualifiers com a URL da sua DRO. Se a AC preencher o campo de extensão userNotice, o texto deve estar em conformidade com o texto descrito no item 2.1.1 .

7.1.9 Processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme definição do padrão PKIX.

7.2 Perfil de LCR

7.2.1 Número de versão

A AC deve publicar a LCR no formato X.509 v2 de acordo com o padrão PKIX de certificado e perfil de LCR.

7.2.2 LCR e LCR extensões de entrada

Todo software de ICP de entidade deve processar corretamente todas as extensões de LCR identificadas no padrão PKIX de certificado e perfil de LCR. A DRO deve definir o uso de todas as extensões suportadas pela AC.

8 Especificação de Administração

8.1 Alterações

8.1.1 Itens que podem ser alterados sem notificação

Nenhum

8.1.2 Notificações necessárias para alteração

A fim de proceder com qualquer alteração nesta PC o CG da ICP-Brasil deve comunicar às AC integrantes da ICP-Brasil bem como todas as AC com as quais a AC Raiz possui acordos de certificação cruzada.

8.1.2.1 Mecanismos de notificação

O CG da ICP-Brasil notificará por escrito todas as AC integrantes da ICP-Brasil bem como as AC com as quais a AC Raiz possui acordos de certificação cruzada. Na notificação deverá constar as alterações exigidas.

8.2 Procedimentos de publicação e notificação

As alterações serão publicadas em DOU.