Comparando políticas de certificação

Jeroen van de Graaf
Laboratório de Computação Científica
Universidade Federal de Minas Gerais
Avenida Antônio Carlos 6627
31270-901 Belo Horizonte (Pampulha) – MG
jvdg@lcc.ufmg.br

08 de janeiro de 2006

Resumo

Este documento compara várias Declarações de Políticas de Certificação. Todas usam RFC2527 como base, e as seções contêm o trecho de texto correspondendo com este ítem, facilitando a comparação e redação de uma nova DPC.

A maioria dos documentos não está disponível em formato texto, mas apenas em html ou pdf. Por isto foram convertidos ou escaneados. Este processo não é perfeito, causando distorções: na ortografia de várias palavras e no lay-out. Porém, o resultado é suficiente claro e não compensa resolver estas imperfeições.

Comparamos o texto dos seguintes documentos: rfc2527, cclrc, nasa, serpro e ICP-Brasil.

O texto da DPC da ICP-Brasil é o da Resolução 7 do Comitê Gestor. No entanto, ele foi modificado pelas Resoluções 11, 13, 21, 26, 28 e 31. Se a resolução mais recente que se aplica a uma seção não for a Resolução 7, aparece o número desta resolução entre “[”e “]”.

1 INTRODUÇÃO

1.1 Visão Geral

Este documento estabelece requisitos mínimos de observância obrigatória pelas Autoridades Certificadoras (AC) integrantes da Infra-estrutura de Chaves Públicas Brasileiras (ICP-Brasil) na elaboração de suas Políticas de certificados (PC). Toda Política de Certificado elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento. São 8 (oito) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 4 (quatro) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir: Tipos de Certificados de Assinatura Digital:

- Tipo A1;
- Tipo A2;
- Tipo A3;
- Tipo A4;

Tipos de Certificados de Sigilo:

- Tipo S1;
- Tipo S2;
- Tipo S3;
- Tipo S4;

Os tipos de A1 a A4 e de S1 a S4, indicados acima, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos. Certificados de quaisquer dos tipos relacionados acima, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas AC para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações. Outros tipos de certificado, além dos oito anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor (CG) da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescidas aos tipos de certificados aceitos pela ICP-Brasil.

1.2 Identificação

Neste item deve ser identificada a Política de Certificado e indicado, no mínimos, o tipo de certificado a que está associada. Exemplo: ”Política de Certificado de Assinatura Digital, tipo A1, do(a) < nome da instituição >. O OID (Object Identifier) da PC deve também ser incluído neste item. No âmbito da ICP-Brasil, os OID das PC serão atribuídos na conclusão do processo de credenciamento da AC, conforme a tabela I a seguir:

Tipo de Certificado	OID
A1	2.16.76.1.2.1.n
A2	2.16.76.1.2.2.n
A3	2.16.76.1.2.3.n
A4	2.16.76.1.2.4.n
S1	2.16.76.1.2.101.n
S2	2.16.76.1.2.102.n
S3	2.16.76.1.2.103.n
S4	2.16.76.1.2.104.n

Tabela 1: OID de PC na ICP-Brasil

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridades Certificadoras

Neste item deve ser identificada a AC integrante da ICP-Brasil que implementa a PC. Deve também ser identificado o documento Declaração de Práticas de Certificação (DPC) dessa AC, onde estarão descritas suas práticas e procedimentos de certificação.

1.3.2 Autoridades de Registro [26]

Neste item devem ser identificadas as Autoridades de Registro (AR) utilizadas pela AC para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes.

1.3.2.1. Novos endereços de instalações técnicas

A Autoridade de Registro já credenciada na ICP-Brasil poderá abrir novos endereços de instalações técnicas desde que encaminhe, por intermédio da cadeia de Autoridades Certificadoras operacionalmente viculadas, solicitação de funcionamento à Autoridade Certificadora Raiz, acompanhada dos seguintes documentos: a) formulário constante dos itens 1 e 2 do Anexo II-A da Resolução n. 6, de 22 de novembro de 2001 indicando os novos endereços; b) indicação dos procedimentos que serão adotados quanto aos aspectos de segurança e operacionais; c) relação das pessoas responsáveis por cada um dos novos postos da AR. Estando a documentação regular, a AC Raiz autorizará o funcionamento dos novos postos mediante intimação da solicitante, que a partir deste momento disponibilizará os novos endereços em seu sítio. A AC Raiz poderá, a qualquer tempo, verificar a conformidade dos procedimentos e atividades dos postos das Autoridades de Registro autorizados com as práticas e regras estabelecidas pelo CG da ICP-Brasil. Constatada qualquer irregularidade em uma das instalações técnicas, a AC Raiz cassará imediatamente a autorização de funcionamento deste posto e verificará a conformidade dos procedimentos de qualquer outro posto da mesma AR. Verificando-se mais uma vez irregularidades, todos os postos que adotarem os mesmos procedimentos também terão sua autorização cassada.

1.3.2.2. Posto provisório de instalação técnica

A Autoridade de Registro já credenciada na ICP-Brasil poderá, ainda, abrir postos provisórios de instalações técnicas desde que encaminhe, por intermédio da cadeia de Autoridades Certificadoras operacionalmente viculadas, solicitação de funcionamento à Autoridade Certificadora Raiz, com no mínimo 10 (dez) dias de antecedência, acompanhada dos seguintes documentos:
a) formulário contante do Anexo II-B da Resolução n. 6, de 22 de novembro de 2001;
b) indicação dos procedimentos que serão adotados quanto aos aspectos de segurança e operacionais;
c) indicação da pessoa responsável pelo posto provisório;
d) relação dos agentes de registro que trabalharão no posto provisório. Estando a documentação regular, a AC Raiz autorizará o funcionamento do posto provisório mediante intimação da solicitante."

1.3.3 Titulares de Certificado [21]

Neste item devem ser caracterizadas as entidades pessoas físicas ou jurídicas - que poderão ser titulares dos certificados emitidos segundo a PC. NOTA 1: Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais. NOTA 2: Em se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

1.3.4 Aplicabilidade [21]

Neste item devem ser relacionadas as aplicações para as quais são adequados os certificados definidos pela PC e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados. As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer Autoridade Certificadora credenciada pela AC Raiz. Na definição das aplicações para o certificado definido pela PC, a AC responsável deve levar em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, freqüência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado, apresentados na tabela constante do Anexo I. Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações. Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

1.4 Dados de Contato

Neste item devem ser incluídos nome, endereço, telefone e outras informações da AC responsável pela PC. Devem ser também informados o nome, os números de telefone e de fax e o endereço eletrônico de uma pessoa para contato.

2 DISPOSIÇÕES GERAIS

2.1 Obrigações e direitos

2.1.1 Obrigações da AC [21]

Neste item devem ser incluídas as obrigações da AC responsável pela PC, contendo, no mínimo, as abaixo relacionadas:

- operar de acordo com a sua Declaração de Práticas de Certificação (DPC) e com as PC que implementa;
- tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
- gerar e gerenciar os seus pares de chaves criptográficas;
- assegurar a proteção de suas chaves privadas;
- notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- distribuir o seu próprio certificado;
- emitir, expedir e distribuir os certificados de AC de nível imediatamente subseqüente ao seu ou os certificados de AR a ela vinculadas e os certificados de usuários finais;
- informar a emissão do certificado ao respectivo solicitante;
- revogar os certificados por ela emitidos;
- emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR) e, quando aplicável, disponibilizar consulta on
- line de situação do certificado (OCSP - On-line Certificate Status Protocol);
- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICPBrasil;
- publicar em sua página Web sua DPC e suas PC aprovadas.
- adotar as medidas de segurança e controle previstas na PC, DPC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

- manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- manter e testar regularmente seu Plano de Continuidade do Negócio;
- informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC; e
- não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações das AR [26]

Neste item devem ser incluídas as obrigações das AR vinculadas à AC responsável pela PC, contendo, no mínimo, as abaixo relacionadas:

- receber solicitações de emissão ou de revogação de certificados;
- confirmar a identidade do solicitante e a validade da solicitação, de acordo com os requisitos estabelecidos pelos itens 3 e 4 da PC;
- encaminhar a solicitação de emissão ou de revogação de certificado à AC responsável utilizando VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade;
- utilizar VPN (virtual private network
- rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
- informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;
- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil.
- manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada;
- manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP Brasil;
- oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9.

2.1.3 Obrigações do Titular do Certificado [21]

Neste item devem ser incluídas as obrigações dos titulares de certificados emitidos de acordo com a PC, que integrarão o contrato de que trata o item 4.1, contendo, no mínimo, as abaixo relacionadas:

- fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

- garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
- conhecer os seus direitos e obrigações, contemplados pela PC, pela DPC da AC emitente e por outros documentos aplicáveis da ICP-Brasil;
- informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente. NOTA: Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, estas obrigações se aplicam ao responsável pelo uso do certificado.

2.2 Responsabilidades

2.2.1 Responsabilidades da AC [21?]

Neste item devem ser relacionadas todas as responsabilidades da AC responsável pela PC, contendo, no mínimo, as abaixo relacionadas:

- adotar as medidas de segurança e controle previstas na PC, DPC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- manter e testar regularmente seu Plano de Continuidade do Negócio; e
- informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC. A AC responsável pela PC responderá solidariamente pelos atos das AC das cadeias a ela subordinadas.

2.2.2 Responsabilidades das AR"[21?]

Neste item devem ser relacionadas todas as responsabilidades das AR credenciadas juntamente com a AC responsável contendo, no mínimo, as abaixo relacionadas:

- manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada; e
- manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

2.3 Responsabilidade Financeira

2.3.1 Indenizações devidas pela terceira parte (Relying Party)

Neste item devem ser estabelecido a inexistência de responsabilidade da terceira parte (Relying Party) perante a AC ou AR a elas vinculadas, exceto na hipótese de prática de ato ilícito.

2.3.2 Relações Fiduciárias [21]

Neste item deve constar que a AC responsável ou AR vinculada indenizará integralmente os danos o que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3 Processos Administrativos

Neste item devem ser relacionados os processos administrativos cabíveis relativos às operações da AC e das AR Vinculadas.

2.4 Interpretação e Execução

2.4.1 Legislação

Neste item deve ser identificada a legislação que ampara a PC.

2.4.2 Forma de interpretação e notificação

Neste item devem ser relacionadas as providências a serem tomadas na hipótese de uma ou mais das disposições da PC ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável. Deve também ser definida a forma pela qual serão realizadas as notificações, as solicitações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas m PC.

2.4.3 Procedimentos de solução de disputa

Neste item devem ser definidos os procedimentos a serem adotados em caso de conflito entre a PC e outras políticas, planos, acordos, contratos e documentos que a AC adotar. Deve também ser estabelecido que a PC da AC responsável não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.5 Tarifas de Serviço

Nos itens a seguir devem ser especificadas pela AC responsável pela PC as políticas tarifária e de reembolso aplicáveis.

2.5.1 Tarifas de emissão e renovação de certificados

2.5.2 de acesso a certificados

2.5.3 Tarifas de revogação ou de acesso à informação de status

2.5.4 Tarifas para outros serviços

2.5.5 Política de reembolso

2.6 Publicação e Repositório

2.6.1 Publicação de informação da AC [26]

Neste item devem ser definidas as informações a serem publicadas pela AC responsável, o modo pelo qual serão disponibilizadas e a sua disponibilidade, que deverá ser, no mínimo, de 99 por cento (noventa e nove por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. As seguintes informações, no mínimo, deverão ser publicadas pela AC em serviço de diretório ou página Web:

- seu próprio certificado;
- suas LCR;
- sua DPC;
- as PC que implementa;
- os endereços das instalações técnicas das AR vinculadas

2.6.2 Freqüência de publicação

Neste item deve ser informada a freqüência de publicação das informações de que trata o item anterior. A freqüência de publicação das LCR é tratada no item 4.4.9.

2.6.3 Controles de acesso

Neste item devem ser descritos os controles e as eventuais restrições para acesso, leitura e escrita das informações publicadas pela AC, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

2.6.4 Repositórios

Neste item devem ser descritos todos os requisitos aplicáveis aos repositórios utilizados pela AC, tais como:

- localização lógica;
- disponibilidade;
- protocolos de acesso;
- requisitos de segurança.

2.7 Auditoria de Conformidade

A AC responsável pela PC deverá disponibilizar à AC Raiz e às AC de nível imediatamente superior relatórios anuais de auditoria das AR e prestadores de serviço de suporte a ela vinculados. Considera-se prestador de serviço de suporte aquele que desempenha atividade descrita neste documento ou na DPC da AC responsável. Os itens seguintes da PC devem detalhar aspectos relacionados a esse processo de auditoria. 2.7.1 Freqüência de auditoria de conformidade 2.7.2 Identidade e qualificações do auditor 2.7.3 Relação en1re auditor e parte auditada 2.7.4 Tópicos cobertos pela auditoria 2.7.5 Medidas adotadas em caso de não conformidade 2.7.6 Comunicação de resultados 2.8 Sigilo [21] A chave privada de assinatura digital da AC credenciada será gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC será de sua inteira responsabilidade. A PC deve informar que os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves. A PC deve informar também as medidas necessárias para preservação do sigilo dessas chaves privadas. No caso de PC referente a certificado de sigilo, devem ser delimitadas as responsabilidades pela manutenção e pela garantia do sigilo da respectiva chave privada.

2.8.1 Tipos de informações sigilosas [21]

Neste item devem ser identificados os tipos de informações consideradas sigilosas pela AC responsável pela PC e pelas AR a ela vinculadas, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil. Como princípio geral, todo documento, informação ou registro fornecido à AC ou às AR será sigiloso."

2.8.2 Tipos de infom1ações não sigilosas

Neste tem devem ser indicados os tipos de informações consideradas não sigilosas pela AC e pelas AR a ela Vinculadas, compreendendo, entre outros:

- os certificados e as LCR emitidos pela AC;
- informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
- as PC implementadas pela AC;
- a DPC da AC;
- versões públicas de Políticas de Segurança;
- resultados finais de auditorias.

2.8.3 Divulgação de informação de revogação e de suspensão de certificado [21]

Neste item devem ser descritas as formas previstas pela AC para a divulgação de informação de revogação dos certificados por ela emitidos. O item deve informar também a política adotada pela AC para a divulgação ou não divulgação das razões para a revogação dos certificados para terceiros. As razões para revogação do certificado sempre serão informadas para o seu titular, e serão tornadas públicas desde que haja autorização expressa deste. A PC deve ainda informar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

2.8.4 Quebra de sigilo por motivos legais

Este item deve asseverar o dever da AC responsável pela PC de fornecer documentos, informações ou registros sob sua guarda, mediante ordem judicial.

2.8.5 Informações a terceiros

Este item deve estabelecer como diretriz geral que nenhum documento, informação ou registro sob a guarda da AC responsável pela PC deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê -10 e corretamente identificada.

2.8.6 Divulgação por solicitação do titular

Neste item devem ser descritas as condições sob as quais o titular de certificado, ou Sal representante legal, poderá ter acesso a quaisquer dos seus dados ou identificações, ou poderá autorizar a divulgação de seus registros a outras pessoas. A PC deve estabelecer que qualquer liberação de informação somente será permitida mediante autorização formal do titular do certificado.

2.8.7 Outras circunstâncias de divulgação de informação

Neste item da PC devem ser descritas, quando cabíveis, outras circunstâncias em que poderão ser divulgadas informações sigilosas.

2.9 Direitos de Propriedade Intelectual

Neste item da PC devem ser tratadas as questões referentes aos direitos de propriedade intelectual de certificados, políticas, procedimentos, nomes e chaves criptográficas, de acordo com a legislação vigente.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Registro Inicial [26]

Neste item e nos seguintes, a PC deve descrever em detalhes os requisitos e procedimentos utilizados pelas AR vinculadas no processo inicial de identificação do solicitante do certificado. A AR realizará a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de, no mínimo, dois agentes de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

3.1.1 Tipos de nomes [21]

Neste item, devem ser descritos os tipos de nomes admitidos para os titulares de certificados emitidos segundo a PC, tais como nomes no padrão ITU X.500, endereços de correio eletrônico ou endereços de página Web (URL). A PC deve estabelecer ainda que um certificado emitido para uma pessoa jurídica deverá incluir o nome da pessoa física responsável pelo seu uso.”

3.1.2 Necessidade de nomes significativos

Neste item, a PC deve definir a necessidade do uso de nomes significativos -isto é, nomes que possibilitem determinar a identidade da pessoa ou organização a que se referem -para a identificação dos titulares dos certificados.

3.1.3 Regras para interpretação de vários tipos de nomes

Neste item devem ser descritas, quando aplicáveis,’ as regras para a interpretação das várias formas de nomes admitidas pela PC.

3.1.4 Unicidade de nomes

Neste item, a PC deve estabelecer que identificadores do tipo ”Distinguished Name ”(DN) deverão ser únicos para cada titular de certificado, no âmbito da AC emitente. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo .

3.1.5 Procedimento para resolver disputa de nomes

Neste item, a PC deve reservar à AC emitente o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes diversos de certificados. Deve estabelecer também que, durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

Neste item a PC deve estabelecer que os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse de chave privada

A PC deve indicar os procedimentos executados pela AC responsável ou pelas AR a ela vinculadas para confirmar que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital, podendo u para isso as referências contidas na RFC 2510, relativas a POP (proof of possession).

3.1.8 Autenticação da identidade de uma organização [31]

A confirmação da identidade de pessoa jurídica deverá ser feita mediante a apresentação dos seguintes documentos:

- registro comercial,no caso de empresa individual;
- ato constitutivo,estatuto ou contrato social em vigor,devidamente registrado,em se tratando de sociedades comerciais ou civis, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
- prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- prova de inscrição no Cadastro Específico do INSS (CEI),se aplicável.

A pessoa física responsável referida no item 3.1.1 também deverá ser identificada,na forma descrita no item seguinte.

3.1.9 Autenticação da identidade de um indivíduo [31]

Neste item devem ser definidos os procedimentos empregados pelas AR vinculadas para a confirmação da identidade de um indivíduo. Essa confirmação deverá ser realizada, mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos. Deverão ser mantidos arquivos com o tipo e os detalhes da identificação utilizada em cada caso. 3.1.9.1 Documentos para identificação Deve ser apresentada uma foto recente e, no mínimo, os seguintes documentos acompanhados de cópia:

- Cédula de Identidade ou Passaporte, se estrangeiro;
- Cadastro de Pessoa Física;

- Comprovante de Residência;
- Número de Identificação Social
- NIS (Cadastro do Programa de Integração Social
- PIS, Cadastro do Programa de Formação do Patrimônio do Servidor Público
- PASEP ou Cadastro de Contribuintes Individuais do INSS-CI), se aplicável; Cadastro Específico do INSS-CEI,se aplicável;
- Título de Eleitor,se aplicável;
- mais um documento oficial com fotografia,no caso de certificados de tipos A4 e S4;e
- os documentos acima relacionados do responsável,caso o solicitante seja incapaz.

NOTA:Entende-se por cédula de identidade as carteiras instituídas por lei, desde que contenham foto e às mesmas seja atribuída fé pública em todo o território nacional, tais como: Carteira de Identidade emitida pela Secretaria de Segurança Pública, Carteira Nacional de Habilitação, Carteira de Identidade Funcional,Carteira de Identidade Profissional.

3.2 Geração de novo par de chaves antes da expiração do atual [21]

Neste item, a PC deve estabelecer o processo de identificação do solicitante exigido para a geração do novo par de chaves, e de seu correspondente certificado, antes da expiração do certificado vigente. Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

- adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado; ou
- solicitação por meio eletrônico, assinada digitalmente com uso de certificado vigente, que seja pelo menos do mesmo nível de segurança, limitada a 3(três) ocorrências sucessivas.

3.3 Geração de novo par de chaves após revogação

Neste item, a PC deve estabelecer que os procedimentos utilizados para confirmação da identidade de uma entidade solicitante de novo certificado, após a revogação do certificado dessa entidade, deverão ser os mesmos exigidos na solicitação inicial de um certificado. .

3.4 Solicitação de Revogação

Neste item, a PC deve descrever os procedimentos utilizados para a confirmação da identidade do solicitante de uma revogação de certificado. A PC deve estabelecer também a forma pela qual as solicitações de revogação de certificado deverão ser documentadas.

4 REQUISITOS OPERACIONAIS

4.1 Solicitação de Certificado [26]

Neste item da PC devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC responsável para as solicitações de emissão de certificado. Esses requisitos e procedimentos, que deverão ser atendidos e executados pelas AR vinculadas e pelos solicitantes, deverão compreender, no mínimo:

- a comprovação de atributos de identificação constantes do certificado, conforme item 3.1;
- a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes a de um certificado de nível A3;
- um termo de titularidade assinado pelo titular do certificado e um termo de responsabilidade assinado pelo responsável pelo uso do certificado, se for o caso, estabelecendo as condições de uso deste.

A PC deve observar que a solicitação de certificado para AC de nível imediatamente subseqüente ao da AC responsável somente será possível após o processo de credenciamento e a autorização de funcionamento no âmbito da ICP-Brasil (Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil). Nesse caso, aquela AC deverá encaminhar a solicitação de seu certificado à AC emitente por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#1.

4.2 Emissão de Certificado

Neste item devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC responsável pela PC para a emissão de certificado e para a notificação da emissão à entidade solicitante. A PC deve observar ainda que um certificado é considerado válido a partir do momento de sua emissão.

4.3 Aceitação de Certificado [21]

Neste item devem ser descritos todos os requisitos e procedimentos operacionais referentes à aceitação de um certificado por seu titular. A PC deve garantir que a aceitação de todo certificado emitido seja declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, a declaração deverá ser feita pela pessoa física responsável por esses certificados."

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

Neste item, devem ser caracterizadas as circunstâncias nas quais um certificado poderá ser revogado. Este item deve também estabelecer que um certificado deverá obrigatoriamente ser revogado:

- quando constatada emissão imprópria ou defeituosa do mesmo;
- quando for necessária a alteração de qualquer informação constante no ; ou
- no caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

A PC deve observar ainda que a AC emitente deverá revogar, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, nomes e regras estabelecidas para a ICP-Brasil.

4.4.2 Quem pode solicitar revogação

A PC deve estabelecer que a revogação de um certificado somente poderá ser feita:

- por solicitação do titular do certificado;
- por solicitação do responsável pelo certificam, no caso de equipamentos, aplicações e pessoas jurídicas;
- por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- pela AC emitente;
- por uma AR vinculada; ou
- por determinação do CG da ICP Brasil ou da AC Raiz.

4.4.3 Procedimento para solicitação de revogação

Neste item devem ser detalhadamente descritos os procedimentos estabelecidos pela AC para a solicitação de revogação de certificados. A AC deverá garantir que todos os agentes habilitados conforme o item 4.4.2 possam, facilmente e a qualquer tempo, solicitar a revogação de seus certificados. A PC deve garantir que:

- o solicitante da revogação de um certificado será identificado, conforme item 3.4;
- as solicitações de revogação, bem como as ações delas decorrentes, realizadas pela AC, serão registradas e armazenadas;
- as justificativas para a revogação de um certificado serão documentadas;
- o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC.

Tipo de Certificado	Tempo limite para revogação (em horas)
A1 e S1	72
A2 e S2	54
A3 e S3	36
A4 e S4	18

Tabela 2: Tempo limite para revogação do certificado

A Tabela 2, a seguir, apresenta os prazos máximos admitidos para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para cada tipo de certificado previsto pela ICP-Brasil.

A PC deve garantir que a AC responsável responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.4.4 Prazo para solicitação de revogação

A PC deve observar neste item que a solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no seu item 4.4.1. A PC deve também estabelecer o prazo para a aceitação do certificado por seu titular (item 4.3), dentro do qual a revogação desse certificado poderá ser solicitada sem cobrança de tarifa pela AC.

4.4.5 Circunstâncias para suspensão

A PC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.6 Quem pode solicitar suspensão

A PC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.7 Procedimento para solicitação de suspensão

A PC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil

4.4.8 Limites no período de suspensão

A PC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil

4.4.9 Freqüência de emissão de LCR

Neste item deve ser definida a freqüência de emissão da LCR associada à PC. A Tabela 3, a seguir, estabelece os prazos máximos admitidos para a emissão de LCR, para cada tipo de certificado previsto pela ICP-Brasil.

Tipo de Certificado	Prazos Máximos para Emissão de LCR
A1 e S1	a cada 48 horas
A2 e S2	a cada 36 horas
A3 e S3	a cada 24 horas
A4 e S4	a cada 12 horas

Tabela 3: Prazos Máximos para Emissão de LCR

4.4.10 Requisitos para verificação de LCR

Neste item, deve -se observar que todo certificado emitido deverá ter a sua validade verificada, na respectiva LCR da AC emitente, antes de ser utilizado. A PC deve observar ainda que a autenticidade da LCR também deverá ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR

4.4.11 Disponibilidade para revogação ou verificação de status on-line

Neste item, a PC deve informar , se for o caso, as disponibilidades de recursos da AC responsável para revogação on-line de certificados ou para verificação on-line de status de certificados. A verificação da situação de um certificado poderá ser feita diretamente na AC emitente, por meio do protocolo OCSP (On-line Certificate Status Protocol)o

4.4.12 Requisitos para verificação de revogação on-line

Neste item, a PC deve definir, quando cabíveis, os requisitos para a verificação on-line de informações de revogação de certificados, plas terceiras partes (re/ying parties).

4.4.13 Outras formas disponíveis para divulgação de revogação.

Neste item, a PC deve informar, quando existirem, outras formas utilizadas das pela AC responsável para a divulgação de informações de revogação de certificados.

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

Neste item, a PC deve definir, quando cabíveis, os requisitos para a verificação das formas de divulgação indicadas no item anterior, de infonmações de revogação de certificados, pelas terceiras partes(relying parties).

4.4.15 Requisitos especiais para o caso de comprometimento de chave

Neste item devem ser definidos os requisitos específicos aplicáveis à revogação de certificado provocada pelo comprometimento da chave privada correspondente. A PC deve observar que, nessa circunstância, o titular do certificado deverá comunicar o fato imediatamente à AC emitente. A PC deverá fazer referência às determinações da DPC da AC responsável que definam os meios utilizados para comunicação de comprometimento ou de suspeita de comprometimento de chave.

4.5 Procedimentos de Auditoria de Segurança

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável pela PC ou incluídos procedimentos específicos para a PC. 4.5.1 Tipos de eventos registrados 4.5.2 Freqüência de auditoria de registros (logs) 4.5.3 Período de retenção para registros (logs) de auditoria 4.5.4 Proteção de registro (log) de auditoria. 4.5.5 Procedimentos para cópia de segurança (backup) de registro (log) de auditoria 4.5.6 Sistema de coleta de dados de auditoria 4.5.7 Notificação de agentes causadores de eventos 4.5.8 Avaliações de vulnerabilidade

4.6 Arquivamento de Registros

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável pela PC ou incluídos procedimentos específicos para a PC.

4.6.1 Tipos de registros arquivados

4.6.2 Período de retenção para arquivo 4.6.2 Período de retenção para arquivo 4.6.3 Proteção de arquivo 4.6.3 Proteção de arquivo 4.6.4 Procedimentos para cópia de segurança (backup) de arquivo 4.6.4 Procedimentos para cópia de segurança (backup) de arquivo 4.6.5 Requisitos para datação (time-stamping) de registros 4.6.5 Requisitos para datação (time-stamping) de registros 4.6.6 Sistema de coleta de dados de arquivo 4.6.6 Sistema de coleta de dados de arquivo 4.6.7 Procedimentos para obter e verificar informação de arquivo 4.6.7 Procedimentos para obter e verificar informação de arquivo

4.7 Troca de chave

A PC pode definir prazo anterior à data de expiração de um certificado válido, no qual a AC ou urna AR vinculada comunicará o seu titular para que seja solicitada a emissão de um novo certificado. Os procedimentos aplicáveis detalhados também devem estar descritos neste item.

4.8 Comprometimento e Recuperação de Desastre

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável pela PC ou incluídos procedimentos específicos para a PC. 4.8.1 Recursos computacionais, software ou dados são corrompidos 4.8.1 Recursos computacionais, software ou dados são corrompidos 4.8.2 Certificado de entidade é revogado 4.8.2 Certificado de entidade é revogado 4.8.3 Chave de entidade é comprometida 4.8.3 Chave de entidade é comprometida 4.8.4 Segurança dos recursos após desastre natural ou de outra natureza 4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

4.9 Extinção da AC [21]

Este item da PC deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da AC responsável ou de uma AR a ela vinculada. Devem ser descritos os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivo. O responsável pela guarda desses dados e registros deverá observar os mesmos requisitos de segurança exigidos para a AC extinta. As chaves públicas dos certificados emitidos por AC dissolvida serão armazenadas por outra AC, após aprovação da AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC que encerra as suas atividades. A AC que encerra as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas. Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.”

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável pela PC ou incluídos procedimentos específicos para a PC.

5.1 Controles Físicos

5.1.1 Construção e localização das instalações

5.1.2 Acesso físico 5.1.2 Acesso físico 5.1.3 Energia e ar condicionado 5.1.3 Energia e ar condicionado 5.1.4 Exposição à água 5.1.4 Exposição à água 5.1.5 Prevenção e proteção contra incêndio 5.1.5 Prevenção e proteção contra incêndio 5.1.6 Armazenamento de mídia 5.1.6 Armazenamento de mídia 5.1.7 Destruição de lixo 5.1.7 Destruição de lixo 5.1.8 Instalações de segurança (backup) externas (off-site) 5.1.8 Instalações de segurança (backup) externas (off-site)

5.2 Controles Procedimentais

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável pela PC ou incluídos procedimentos específicos para a PC. 5.2.1 Perfis qualificados 5.2.1 Perfis qualificados 5.2.2 Número de pessoas necessário por tarefa 5.2.2 Número de pessoas necessário por tarefa 5.2.3 Identificação e autenticação para cada perfil 5.2.3 Identificação e autenticação para cada perfil

5.3 Controles de Pessoal

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável pela PC ou incluídos procedimentos específicos para a PC. subsection5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade subsection5.3.2 Procedimentos de verificação de antecedentes subsection5.3.3 Requisitos de treinamento . subsection5.3.4 Freqüência e requisitos para reciclagem técnica subsection5.3.5 Freqüência e seqüência de rodízio de cargos subsection5.3.6 Sanções para ações não autorizadas subsection5.3.7 Requísitos para contratação de pessoal subsection5.3.8 Documentação fornecida ao pessoal

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC deve definir as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC. Devem também ser definidos outros controles técnicos de segurança utilizados pela AC e pelas AR vinculadas na execução de suas feições Operacionais.

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves [21]

Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado. Neste item, a PC deve descrever todos os requisitos e procedimentos referentes ao processo de geração de chaves aplicável ao certificado que define. Ao ser gerada, a chave privada da entidade titular deverá ser gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme a Tabela 4. A chave privada deverá trafegar cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento. O meio de armazenamento da chave privada deverá assegurar, por meios técnicos e procedimentais adequados, no mínimo, que:

- a chave privada é única e seu sigilo é suficientemente assegurado;
- a chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
- a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.2 Entrega da chave privada à entidade titular

Item não aplicável.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (requisitos mínimos)
A1 e S1	Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha
A2 e S2	Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha
A3 e S3	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico aprovado 10 CG da ICP-Brasil
A4 e S4	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico aprovado 10 CG da ICP-Brasil

Tabela 4: Mídias Armazenadoras de Chaves Criptográficas

6.1.3 Entrega da chave pública para o emissor de certificado

A PC deve detalhar os procedimentos utilizados para a entrega da chave pública de titular de certificado à AC responsável. Nos casos em que houver solicitação de certificado pelo seu titular ou por AR vinculada, deverá ser adotado forma compatível com o padrão PKCS#10.

6.1.4 Disponibilização de chave pública da AC para usuários

Neste item, a PC deve definir as formas para a disponibilização do certificado da AC responsável, e de todos os certificados de sua cadeia de certificação, para os usuários da ICP-Brasil, formas essas que poderão compreender, entre outras:

- formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- diretório;
- página Web da AC;
- outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

Este item deve definir o tamanho das chaves criptográficas associadas aos certificados emitidos segundo a PC. A Tabela 5 define os tamanhos mínimos admitidos para as chaves criptográficas, para cada tipo de certificado previsto pela ICP-Brasil.

Tipo de Certificado	Tamanho da chave criptográfica (em bits)
A1 e S1	1024
A2 e S2	1024
A3 e S3	1024
A4 e S4	2048

Tabela 5: Prazos Máximos para Emissão de LCR

6.1.6 Geração de parâmetros de chaves assimétricas

A PC deve prever que os parâmetros de geração de chaves assimétricas das entidades titulares de certificados adotarão o padrão FIPS 140- f ou equivalente estabelecido pelo CG da ICP-Brasil.

6.1.7 Verificação da qualidade ros parâmetros

Os parâmetros deverão ser verificados de acordo com as normas estabe1ecidas pelo CMVP (Cryptographic Module Validation Program) do NIST f/: national lnstitute 01 Standards and Technology).

6.1.8 Geração de chave por hardware ou software

O processo de geração de chaves criptográficas definido pela PC deverá ser realizado, para cada tipo correspondente de certificado previsto pela ICP-Brasil, conforme a Tabela 6 seguinte:

Tipo de Certificado	Processo de Geração de Chave Criptográfica
A1 e S1	Software
A2 e S2	Hardware
A3 e S3	Hardware
A4 e S4	Hardware

Tabela 6: Prazos Máximos para Emissão de LCR

6.1.9 Propósitos de uso de chave (conforme o campo "key usage"na X509v3)

Neste item, a PC deve especificar os propósitos para os quais poderão ser utilizadas as chaves criptográficas dos titulares de certificados, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes (item 1.3.4).

6.2 Proteção da Chave Privada

Nos itens seguintes, a PC deve definir os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos segundo a PC.

6.2.1 Padrões para módulo criptográfico

Neste item, quando cabíveis, devem ser especificados os padrões -como, por exemplo, o padrão FIPS (Federal Information Processing Standards) 140-1 -requeridos para os módulos de geração de chaves criptográficas.

6.2.2 Controle "n de m"para chave privada

Item não aplicável.

6.2.3 Recuperação (escrow) de chave privada .

Neste item, a PC deve observar que não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4 Cópia de segurança (backup) de chave privada

Como diretriz geral, qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada. A AC responsável pela PC não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido. Em qualquer caso, a cópia de segurança deverá ser armazenada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, e protegida com Wll nível de segurança não inferior àquele definido para a chave original. Além das observações acima, a PC deve descrever todos os requisitos e procedimentos aplicáveis ao processo de geração de uma cópia de segurança.

6.2.5 Arquivamento de chave privada

Neste item de uma PC que defina certificados de sigilo, devem ser descritos, quando cabíveis, os requisitos para arquivamento de chaves privadas. Não devem ser arquivadas chaves privadas de assinatura digital. Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente. .

6.2.6 Inserção de chave privada em módulo criptográfico

Neste item, quando aplicáveis, devem ser definidos os requisitos para inserção da chave privada de titular em módulo criptográfico.

6.2.7 Método de ativação de chave privada

Neste item da PC devem ser descritos os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular. Devem ser definidos os agentes autorizados a ativar essa chave, o método de confirmação da identidade desses agentes (senhas, tokens ou biometria) e as ações necessárias para a ativação.

6.2.8 Método de desativação de chave privada

Neste item da PC devem ser descritos os requisitos e os procedimentos necessários para desativação da chave privada de entidade titular. Devem ser definidos os agentes autorizados, o método de confirmação da identidade desses agentes e as ações necessárias.

6.2.9 Método de destruição de chave privada

Neste item da PC devem ser descritos os requisitos e os procedimentos necessários para destruição da chave privada de titular e de suas cópias de segurança. Devem ser definidos os agentes autorizados, ó método de confirmação da identidade desses agentes e as ações necessárias, tais como destruição física, sobrescrita ou apagamento das mídias de armazenamento.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A PC deve prever que as chaves públicas de titulares dos certificados de assinatura digital por ela definidos deverão permanecer armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2 Períodos de uso para as chaves pública e privada

Caso a PC se refira a certificados de assinatura digital, ela deve prever que as chaves privadas dos respectivos titulares deverão ser utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utiliZ2das durante todo o período de tempo detem1inado pela legislação aplicável para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados. Caso a PC se refira a certificados re sigilo, ela deve definir os períodos de uso das chaves correspondentes. A Tabela 7, seguinte, define os períodos máximos de validade admitidos para cada tipo de certificado previsto pela ICP-Brasil:

Tipo de Certificado	Período Máximo de Validade do Certificado (em anos)
A1 e S1	1
A2 e S2	2
A3 e S3	3
A4 e S4	3

Tabela 7: Períodos de Validade dos Certificados

6.4 Dados de Ativação

Nos itens seguintes da PC devem ser descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 Geração e instalação dos dados de ativação

A PC deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão únicos e aleatórios.

6.4.2 Proteção dos dados de ativação

A PC deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão protegidos contra uso não autorizado.

6.4.3 Outros aspectos dos dados. de ativação

Neste item, quando for o caso, devem ser definidos outros aspectos referentes aos dados de ativação. Entre esses outros aspectos podem ser considerados alguns daqueles tratados, em relação às chaves, nos itens de 6.1 a 6.3.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

A PC deve descrever os requisitos de segurança computacional do equipamento onde serão gerados os pares de chaves criptográficos:as dos titulares de certificados.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

Caso a AC responsável exija um software específico para a utilização dos certificados emitidos segundo a PC, nos itens seguintes devem ser descritos os controles implementados no desenvolvimento e no gerenciamento de segurança referentes a esse software.

6.6.1 Controles de desenvolvimento de sistema

Neste item da PC devem ser abordados aspectos tais como: segurança do ambiente e do pessoal de desenvolvimento, práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros.

6.6.2 Controles de gerenciamento de segurança

Neste item devem ser descritos os procedimentos e as ferramentas empregados para garantir que o software e seu ambiente operacional implementem os níveis configurados de segurança.

6.6.3 Classificações de segurança de ciclo de vida

Neste item deve ser informado, quando disponível, o nível de maturidade atribuído ao ciclo de vida do software, com base em critérios como: Trusted Software Development Methodology (TSDM) ou o Capability Maturity Model 00 Software Engineering Institute (CMM-SEI).

6.7 Controles de Segurança de Rede

Caso o ambiente de utilização do certificado definido pela PC exija controles específicos de segurança de rede, esses controles devem ser descritos neste item da PC, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

6.8 Controles de Engenharia do modulo Criptográfico

Este item da PC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado. Poderão ser indicados padrões de referência, como o FIPS (Federal lnfonnation Processing Standards) 140-1.

7 PERFIS DE CERTIFICADO E LCR

Os itens seguintes devem especificar os formatos dos certificados e das LCR gerados segundo a PC. Devem ser incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes deverão ser obrigatoriamente atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC responsável, segundo a Pc, deverão estar em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão

Todos os certificados emitidos pela AC responsável, segundo a PC, deverão implementar a versão 3 de certificado definida no padrão nu X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2 Extensões de certificado [31]

Neste item, a PC deve descrever todas as extensões de certificado utilizadas e sua criticalidade. A ICP-Brasil define como obrigatórias as seguintes extensões:

- ”Authority Key Identifier”, não crítica:o campo keyIdentifier deve conter o hash SHA-1 da chave pública da AC;
- ”Key Usage”,crítica:em certificados de assinatura digital, somente os bits digitalSignature, nonRepudiation e keyEncipherment podem estar ativados; em certificados de sigilo, somente os bits keyEncipherment e dataEncipherment podem estar ativados;
- ”Certificate Policies”, não crítica: deve conter o OID da PC correspondente e o endereço Web da DPC da AC que emite o certificado;
- ”CRL Distribution Points”,não crítica:deve conter o endereço na Web onde se obtém a LCR correspondente;

A ICP-Brasil também define como obrigatória a extensão ”Subject Alternative Name”, não crítica e com os seguintes formatos: Para certificado de pessoa física, 3 (três)campos otherName, contendo:

- OID =2.16.76.1.3.1 e conteúdo =nas primeiras 8 (oito)posições,a data de nascimento do titular, no formato ddmmaaaa;nas 11 (onze) posições subseqüentes,o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o Número de Identificação Social-NIS (PIS, PASEP ou CI); nas 11 (onze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.
- OID =2.16.76.1.3.6 e conteúdo =nas 12 (doze)posições o número do Cadastro Específico do INSS (CEI)da pessoa física titular do certificado.
- OID =2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subseqüentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subseqüentes, o município e a UF do Título de Eleitor.

Para certificado de pessoa jurídica,4 (quatro)campos otherName,contendo,nesta ordem:

- OID =2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas (onze) posições subseqüentes,o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o Número de Identificação Social-NIS (PIS,PASEP ou CI); nas (onze) posições subseqüentes, o número do RG do responsável;nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;
- OID =2.16.76.1.3.2 e conteúdo =nome do responsável pelo certificado;
- OID =2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado; OID =2.16.76.1.3.7 e conteúdo =nas 12 (doze)posições o número do Cadastro Específico do INSS (CEI)da pessoa jurídica titular do certificado.

Os campos otherName definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

- O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING;
- Quando os números de CPF,NIS (PIS,PASEP ou CI),RG,CNPJ,CEI ou Título de Eleitor não estiverem disponíveis,os campos correspondentes devem ser integralmente preenchidos com caracteres ”zero”;
- Se o número do RG não estiver disponível,não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF,se não houver número de inscrição do Título de Eleitor;
- Todas informações de tamanho variável referentes a números,tais como RG,devem ser preenchidas com caracteres ”zero”a sua esquerda para que seja completado seu máximo tamanho possível;
- As 6 (seis)posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo,devendo ser utilizadas apenas as posições necessárias ao seu armazenamento,da esquerda para a direita.

O mesmo se aplica às 22 (vinte e duas)posições das informações sobre município e UF do Título de Eleitor. Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados,não sendo permitidos caracteres especiais,símbolos,espaços ou quaisquer outros. Campos otherName adicionais,contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC,poderão ser utilizados com OID atribuídos ou aprovados pela AC- Raiz. Os outros campos que compõem a extensão ”Subject Alternative Name”poderão ser utilizados,na forma e com os propósitos definidos na RFC 2459.

7.1.3 Identificadores de algoritmo

Neste item da PC devem ser indicados os OID (Object Identifiers) dos algoritmos criptográficos utilizados. São os seguintes os algoritmos, e seus OID, admitidos no âmbito da ICP-Brasil:

- RSA, OID = 1.2.840.113549.1.1.1;
- SHA-1 com RSA, OID = 1.2.840.113549.1.1.5;
- MD5 com RSA, OID= 1.2.840.113549.1.1.4;
- SHA-1 com DSA, OID= 1.2.840.10040.4.3.

7.1.4 Formatos de nome [21]

O nome do titular do certificado, constante do campo ”Subject”, deverá adotar o ”Distinguished Name”(DN) do padrão ITU X.500/ISO 9594, da seguinte forma:
C = BR
O = ICP-Brasil
CN = nome do titular do certificado

Em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica); em um certificado de equipamento ou aplicação, o identificador CN deverá conter o URL correspondente. NOTA: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura

7.1.5 Restrições de nome

Neste item da PC, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados. A icp-brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

- não deverão s utilizados sinais de acentuação, tremas ou cedilhas;
- além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

(veja tabelo no final deste capítulo)

7.1.6 OID (Object Identifier) de Política de Certificado

Neste item, deve ser infom1ado o OID atrIbuído à Política de certificado. Todo certificado emitido segundo a PC deverá conter, na extensão ”Certificate Policies”, o OID correspondente

7.1.7 Uso da extensão ”Policy Constraints”

Item não aplicável

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo a PC, o campo policy Qualifiers da extensão ”Certificate Policies”deverá conter o endereço Web (URL) da DPC da AC responsável

7.1.9 Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 2459.

7.2 Perfil de LCR

7.2.1 Número de versão.

As LCR geradas pela AC responsável,’ segundo a PC, deverão implementar a versão 2 de LCR definida no padrão !TU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2 Extensões de LCR e de suas entradas

Neste item, a PC deve descrever todas as extensões de LCR utilizadas e sua criticalidade. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

- ”Authority Key Identifier”: deve conter o hash SHA-l da chave pública da AC que assina a LCR.
- ”CRL Number”, não crítica: deve conter um número seqüencial para cada LCR emitida.

Caractere	Código NBR9611 (hexadecimal)
branco	20
!	21
”	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
	5C

Tabela 8: Caracteres especiais admitidos em nomes

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

OS itens seguintes devem definir como será mantida e administrada a PC.

8.1 Procedimentos de mudança de es cificação

Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na PC. Qualquer alteração na PC deverá ser submetida à aprovação do CG da ICP-Brasil.

8.2 Políticas de publicação e notificação

Neste item devem ser descritos os mecanismos empregados para a distribuição da PC à contabilidade envolvida.

8.3 Procedimentos de aprovação [13]

Toda DPC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável, conforme o determinado pelo documento Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil.