

RESOLUÇÃO Nº 41, DE 18 DE ABRIL DE 2006

Aprova a versão 2.0 dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL

O COORDENADOR DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL faz saber que aquele Comitê, no uso das atribuições previstas nos incisos I, III, V e VI do art. 4º da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001 .

CONSIDERANDO a necessidade de unificar os critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil, hoje expressos na Resolução nº 06 e nos itens 1.3.2.1 e 1.3.2.2 das Resoluções 07 e 08 deste Comitê;

CONSIDERANDO a necessidade de complementar tais critérios e procedimentos, em especial no tocante ao credenciamento e descredenciamento das Autoridades de Registro, bem como à criação e extinção de suas instalações técnicas;

CONSIDERANDO a necessidade de clarificar as questões relativas à obrigatoriedade de preenchimento dos campos do certificado com informações do titular;

CONSIDERANDO ainda a demanda de diversos segmentos da sociedade pela inclusão, no conteúdo dos certificados da ICP-Brasil, de campo para informação do número de habilitação ou identificação profissional do titular;

CONSIDERANDO, por fim, a necessidade de prover maior agilidade na definição de algoritmos e protocolos criptográficos para utilização na ICP-Brasil, o que pode ser obtido com sua regulamentação sendo feita por meio de Instruções Normativas.

RESOLVE

Art. 1º Aprovar a versão 2.0 dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04), em anexo.

Art. 2º Ficam revogadas as Resoluções do Comitê Gestor da ICP-Brasil nº 07, de 02 de dezembro de 2001, nº 11, de 14 de fevereiro de 2002, nº 28, de 11 de novembro de 2003 e nº 35, de 21 de outubro de 2004 e convalidados os atos praticados durante as vigências desses normativos.

Art.3º As Autoridades Certificadoras - AC devidamente credenciadas deverão apresentar, no prazo máximo de 120 (cento e vinte) dias contados da publicação desta Resolução, alteração nas suas Políticas de Certificados, comprovando, sob pena de descredenciamento, a adequação de seus documentos e de seus procedimentos operacionais às alterações procedidas por esta Resolução.

Parágrafo único. As AC em processo de credenciamento deverão apresentar imediatamente alteração nas Políticas de Certificados apresentadas, adequando-as às modificações procedidas por esta Resolução.

Art. 4º Esta Resolução entra em vigor na data de sua publicação.

ANEXO

**REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL
DOC-ICP-04 - Versão 2.0**

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora

AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil

AR - Autoridades de Registro

CEI - Cadastro Específico do INSS

CG - Comitê Gestor

CMM-SEI - *Capability Maturity Model do Software Engineering Institute*

CMVP - *Cryptographic Module Validation Program*

CN - Common Name

CNE - Carteira Nacional de Estrangeiro

CNPJ - Cadastro Nacional de Pessoas Jurídicas -

COBIT - *Control Objectives for Information and related Technology*

COSO - *Comitee of Sponsoring Organizations*

CPF - Cadastro de Pessoas Físicas

DMZ - Zona Desmilitarizada

DN - *Distinguished Name*

DPC - Declaração de Práticas de Certificação

ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira

IDS - Sistemas de Detecção de Intrusão

IEC - *International Electrotechnical Commission*

ISO - *International Organization for Standardization*

ITSEC - *European Information Technology Security Evaluation Criteria*

ITU - *International Telecommunications Union*

LCR - Lista de Certificados Revogados

NBR - Norma Brasileira

NIS - Número de Identificação Social

NIST - *National Institute of Standards and Technology*

OCSP - *On-line Certificate Status Protocol*

OID - *Object Identifier*

OU - *Organization Unit*

PASEP - Programa de Formação do Patrimônio do Servidor Público

PC - Políticas de Certificado

PCN - Plano de Continuidade de Negócio

PIS - Programa de Integração Social

POP - *Proof of Possession*

PS - Política de Segurança

PSS - Prestadores de Serviço de Suporte

RFC - *Request For Comments*

RG - Registro Geral

SNMP - Simple Network Management Protocol

TCSEC - *Trusted System Evaluation Criteria*

TSDM - *Trusted Software Development Methodology*

UF - Unidade de Federação

URL - Uniform Resource Location

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1 Este documento estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras - AC integrantes da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2 Toda PC elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.1.3. 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:

a) Tipos de Certificados de Assinatura Digital:

- i. Tipo A1;
- ii. Tipo A2;
- iii. Tipo A3;
- iv. Tipo A4.

b) Tipos de Certificados de Sigilo:

- i. Tipo S1;
- ii. Tipo S2;
- iii. Tipo S3;
- iv. Tipo S4.

1.1.4. Os tipos de certificados indicados acima, de A1 a A4 e de S1 a S4, 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.

1.1.5. 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.

1.1.6. Outros tipos de certificado, além dos oito anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescentadas aos tipos de certificados aceitos pela ICP-Brasil.

1.2. Identificação

1.2.1. Neste item deve ser identificada a PC e indicado, no mínimo, 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.

1.2.2 No âmbito da ICP-Brasil, os OID das PC serão atribuídos na conclusão do processo de credenciamento da AC, conforme a tabela 1 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

1.3.1.1. Neste item deve ser identificada a AC integrante da ICP-Brasil que implementa a PC.

1.3.1.2. 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

1.3.2.1. Neste item deve ser identificado o endereço da página *web* (URL) onde estão publicados os dados a seguir, referentes às 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:

- a) relação de todas as AR credenciadas, com informações sobre as PC que implementam;
- b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
- c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
- d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;
- e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
- f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC responsável deverá manter as informações acima sempre atualizadas.

1.3.3. Prestador de Serviços de Suporte

1.3.3.1. Neste item deve ser identificado o endereço da página *web* (URL) onde está publicada a relação de todos os Prestadores de Serviços de Suporte – PSS vinculados à AC responsável, seja diretamente seja por intermédio de suas AR.

1.3.3.2. PSS são entidades utilizados pela AC ou pelas AR para desempenhar atividade descrita nesta PC ou na DPC implementada pela AC e se classificam em três categorias, conforme o tipo de atividade prestada,

- a) disponibilização de infra-estrutura física e lógica;
- b) disponibilização de recursos humanos especializados; ou
- c) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC responsável deverá manter as informações acima sempre atualizadas.

1.3.4. Titulares de Certificado

Neste item devem ser caracterizadas as entidades - pessoas físicas ou jurídicas - que poderão ser titulares dos certificados emitidos segundo a PC.

1.3.5. Aplicabilidade

1.3.5.1. Neste item devem ser relacionadas as aplicações para as quais os certificados definidos pela PC são adequados e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

1.3.5.2. 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 superior, emitido por qualquer AC credenciada pela AC Raiz.

1.3.5.3. 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, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado, apresentados na tabela constante do Anexo I.

1.3.5.4. Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.5. 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

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

2.1. Obrigações e direitos

2.1.1. Obrigações da AC

2.1.2. Obrigações das AR

2.1.3. Obrigações do Titular do Certificado

2.1.4. Direitos da terceira parte (*Relying Party*)

2.1.5. Obrigações do Repositório

2.2. Responsabilidades

2.2.1. Responsabilidades da AC

2.2.2. Responsabilidades da AR

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (*Relying Party*)

2.3.2. Relações Fiduciárias

2.3.3. Processos Administrativos

2.4. Interpretação e Execução

2.4.1. Legislação

2.4.2. Forma de interpretação e notificação

2.4.3. Procedimentos de solução de disputa

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e renovação de certificados

2.5.2. Tarifas 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

2.6.2. Frequência de publicação

2.6.3. Controles de acesso

2.6.4. Repositórios

2.7. Auditoria e Fiscalização

2.8. Sigilo

2.8.1. Tipos de informações sigilosas

- 2.8.2. Tipos de informações não sigilosas
- 2.8.3. Divulgação de informação de revogação e de suspensão de certificado
- 2.8.4. Quebra de sigilo por motivos legais
- 2.8.5. Informações a terceiros
- 2.8.6. Divulgação por solicitação do titular
- 2.8.7. Outras circunstâncias de divulgação de informação

2.9. Direitos de Propriedade Intelectual

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

3.1. Registro Inicial

- 3.1.1. Disposições Gerais
- 3.1.2. Tipos de nomes
- 3.1.3. Necessidade de nomes significativos
- 3.1.4. Regras para interpretação de vários tipos de nomes
- 3.1.5. Unicidade de nomes
- 3.1.6. Procedimento para resolver disputa de nomes
- 3.1.7. Reconhecimento, autenticação e papel de marcas registradas
- 3.1.8. Método para comprovar a posse de chave privada
- 3.1.9. Autenticação da identidade de um indivíduo
 - 3.1.9.1. Documentos para efeitos de identificação de um indivíduo
 - 3.1.9.2. Informações contidas no certificado emitido para um indivíduo
- 3.1.10. Autenticação da identidade de uma organização
 - 3.1.10.1. Disposições Gerais
 - 3.1.10.2. Documentos para efeitos de identificação de uma organização
 - 3.1.10.3. Informações contidas no certificado emitido para uma organização
- 3.1.11. Autenticação da identidade de equipamento ou aplicação
 - 3.1.11.1. Disposições Gerais
 - 3.1.11.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação
 - 3.1.11.3 - Informações contidas no certificado emitido para um equipamento ou aplicação

3.2. Geração de novo par de chaves antes da expiração do atual

3.3. Geração de novo par de chaves após expiração ou revogação

3.4. Solicitação de Revogação

4. REQUISITOS OPERACIONAIS

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

4.1. Solicitação de Certificado

4.2. Emissão de Certificado

4.3. Aceitação de Certificado

4.4. Suspensão e Revogação de Certificado

- 4.4.1. Circunstâncias para revogação
- 4.4.2. Quem pode solicitar revogação
- 4.4.3. Procedimento para solicitação de revogação
- 4.4.4. Prazo para solicitação de revogação
- 4.4.5. Circunstâncias para suspensão
- 4.4.6. Quem pode solicitar suspensão
- 4.4.7. Procedimento para solicitação de suspensão

- 4.4.8. Limites no período de suspensão
- 4.4.9. Frequência de emissão de LCR
- 4.4.10. Requisitos para verificação de LCR
- 4.4.11. Disponibilidade para revogação ou verificação de status *on-line*
- 4.4.12. Requisitos para verificação de revogação *on-line*
- 4.4.13. Outras formas disponíveis para divulgação de revogação
- 4.4.14. Requisitos para verificação de outras formas de divulgação de revogação
- 4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.5. Procedimentos de Auditoria de Segurança

- 4.5.1. Tipos de eventos registrados
- 4.5.2. Frequência 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

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

4.7. Troca de chave

4.8. Comprometimento e Recuperação de Desastre

- 4.8.1. Recursos computacionais, software ou dados são corrompidos
- 4.8.2. Certificado de entidade é revogado
- 4.8.3. Chave de entidade é comprometida
- 4.8.4. Segurança dos recursos após desastre natural ou de outra natureza
- 4.8.5. Atividades das Autoridades de Registro

4.9. Extinção dos serviços de AC, AR ou PSS

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

5.1. Controles Físicos

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

5.2. Controles Procedimentais

- 5.2.1. Perfis qualificados
- 5.2.2. Número de pessoas necessário por tarefa

5.2.3. Identificação e autenticação para cada perfil

5.3. Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2. Procedimentos de verificação de antecedentes

5.3.3. Requisitos de treinamento

5.3.4. Frequência e requisitos para reciclagem técnica

5.3.5. Frequência e seqüência de rodízio de cargos

5.3.6. Sanções para ações não autorizadas

5.3.7. Requisitos para contratação de pessoal

5.3.8. 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 funções operacionais.

6.1. Geração e Instalação do Par de Chaves

Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, publicando nova versão do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1. Geração do par de chaves

6.1.1.1. 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(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.2. Neste item, a PC deve descrever todos os requisitos e procedimentos referentes ao processo de geração de chaves aplicável ao certificado que define.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.4. Ao ser gerada, a chave privada da entidade titular deverá ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1], no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme a Tabela 2.

6.1.1.5. 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.

6.1.1.6. A mídia de armazenamento da chave privada deverá assegurar, por meios técnicos e procedimentais adequados, no mínimo, que:

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

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

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (requisitos mínimos)
---------------------	---

A1 e S1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima.
A2 e S2	Cartão Inteligente ou <i>Token</i> , ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica.
A3 e S3	Cartão Inteligente ou <i>Token</i> , ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica ou hardware criptográfico aprovado pelo CG da ICP-Brasil
A4 e S4	Cartão Inteligente ou <i>Token</i> , ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica ou hardware criptográfico aprovado pelo CG da ICP-Brasil

TABELA 2 – Mídias Armazenadoras de Chaves Criptográficas

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

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 formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

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:

a) no momento da disponibilização de um certificado para seu titular, usando formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1];

b) diretório;

c) página *web* da AC; e

d) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Este item deve definir o tamanho das chaves criptográficas associadas aos certificados emitidos segundo a PC.

6.1.5.2. Os algoritmos e o tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

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 estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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 4 seguinte:

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

TABELA 4 – Processos de Geração de Chaves Criptográficas

6.1.9. Propósitos de uso de chave (conforme o campo “*key usage*” na X.509 v3)

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 requeridos para os módulos de geração de chaves criptográficas, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

6.2.2. Controle “n de m” para chave privada

Item não aplicável.

6.2.3. Custódia (*escrow*) de chave privada

Neste item, a PC deve observar que não é permitida, no âmbito da ICP-Brasil, a custódia (*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

6.2.4.1. Como diretriz geral, qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. 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.

6.2.4.3. Em qualquer caso, a cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. 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

6.2.5.1. 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.

6.2.5.2. 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, o 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 e as LCR serão armazenadas pela AC emissora, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. 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 utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Caso a PC se refira a certificados de sigilo, ela deve definir os períodos de uso das chaves correspondentes.

6.3.2.3. A Tabela 5, 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 5 – 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 criptográficas dos titulares de certificados, observados os requisitos gerais previstos na DPC.

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* do *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 Módulo 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, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [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 ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

7.1.2. Extensões de certificado

7.1.2.1. Neste item, a PC deve descrever todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões:

a) "**Authority Key Identifier**", **não crítica**: o campo `keyIdentifier` deve conter o *hash* SHA-1 da chave pública da AC;

b) **"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;

c) **"Certificate Policies", não crítica:** deve conter o OID da PC correspondente e o endereço Web da DPC da AC que emite o certificado;

d) **"CRL Distribution Points", não crítica:** deve conter o endereço na Web onde se obtém a LCR correspondente.

7.1.2.3. A ICP-Brasil também define como obrigatória a extensão **"Subject Alternative Name", não crítica**, e com os seguintes formatos:

a) Para certificado de pessoa física:

a.1) 3 (três) campos otherName, obrigatórios, contendo:

b OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaa; 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 15 (quinze) 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.

ii. **OID = 2.16.76.1.3.6 e conteúdo** = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa física titular do certificado.

iii. **OID = 2.16.76.1.3.5 e conteúdo** = nas primeiras 12 (onze) 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.

a.2) campos otherName, não obrigatórios, contendo:

i. **OID = 2.16.76.1.4.n e conteúdo** = de tamanho variável correspondente ao número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente. A AC Raiz, por meio do documento ATRIBUIÇÃO DE OID NA ICP-BRASIL [2] regulamentará a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.

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

i. **OID = 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (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 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;

ii. **OID = 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;

iii. **OID = 2.16.76.1.3.3 e conteúdo** = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;

iv. **OID = 2.16.76.1.3.7 e conteúdo** = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa jurídica titular do certificado.

c) Para certificado de equipamento ou aplicação, 4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

i. **OID = 2.16.76.1.3.8 e conteúdo** = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;

ii. **OID = 2.16.76.1.3.3 e conteúdo** = Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;

iii. **OID = 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;

iv. **OID = 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (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 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.

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

a) O conjunto de informações definido em cada campo `otherName` deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING;

b) 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";

c) 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;

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;

e) 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;

f) 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;

g) 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.

7.1.2.5. 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.

7.1.2.6. Os outros campos que compõem a extensão "Subject Alternative Name" poderão ser utilizados, na forma e com os propósitos definidos na RFC 3280.

7.1.3. Identificadores de algoritmo

Neste item da PC deve ser indicado o OID (*Object Identifier*) do algoritmo criptográfico utilizado para assinatura do certificado, observados os algoritmos admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

7.1.4. Formatos de nome

O nome do titular do certificado, constante do campo "Subject", deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, como exemplo, da seguinte forma:

C = BR

O = ICP-Brasil

OU = nome da AC emitente

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 ou o nome da aplicação.

NOTA: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5. Restrições de nome

7.1.5.1. Neste item da PC, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

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

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 6 - Caracteres especiais admitidos em nomes

7.1.6. OID (*Object Identifier*) de Política de Certificado

Neste item, deve ser informado o OID atribuído à PC. 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 **policyQualifiers** 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 3280.

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 ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. Neste item, a PC deve descrever todas as extensões de LCR utilizadas e sua criticalidade.

7.2.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

a) “**Authority Key Identifier**”, **não crítica**: deve conter o *hash* SHA-1 da chave pública da AC que assina a LCR; e

b) “**CRL Number**”, **não crítica**: deve conter um número seqüencial para cada LCR emitida.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

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

8.1. Procedimentos de mudança de especificação

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 da AC Raiz.

8.2. Políticas de publicação e notificação

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

8.3. Procedimentos de aprovação

Toda PC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com este documento, deverá ser verificada a compatibilidade entre a PC e a DPC da AC responsável.

9. DOCUMENTOS REFERENCIADOS

9.1 Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

9.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01

ANEXO I

Tabela Comparativa de Requisitos Mínimos por Tipo de Certificado

Tipo de	Chave Criptográfica			Validade	Frequência	Tempo
	Tamanho (bits)	Processo de Geração	Mídia Armazenadora			
A1 e S1	1024	Software	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma do item 6.1.1	1	6	12
A2 e S2	1024	Software	Cartão Inteligente ou <i>Token</i> , ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica	2	6	12

A3 e S3	1024	Hardware	Cartão Inteligente ou <i>Token</i> , ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica ou <i>hardware</i> criptográfico aprovado pelo CG da ICP-Brasil	3	6	12
---------	------	----------	--	---	---	----

A4 e S4	2048	Hardware	Cartão Inteligente ou <i>Token</i> , ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica ou <i>hardware</i> criptográfico aprovado pelo CG da ICP-Brasil	3	6	12
---------	------	----------	--	---	---	----