# Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE SSL

**Classificação: Pública**
**Versão 1.0**
**Junho de 2018**

prodemge

Companhia de Tecnologia
da Informação do Estado
de Minas Gerais

## CONTROLE DE ALTERAÇÕES E VERSÕES

| VERSÃO | DATA | RESOLUÇÃO QUE APROVOU A ALTERAÇÃO | ITEM ALTERADO | DESCRIÇÃO DA ALTERAÇÃO |
|---|---|---|---|---|
| 1.0 | 07/06/2018 | - | - | Versão inicial |

SUMÁRIO


1. INTRODUÇÃO ..... 10

1.1. Visão Geral ..... 10

1.2. Identificação ..... 10

1.3. Comunidade e Aplicabilidade ..... 10

1.3.1. Autoridades Certificadoras ..... 10

1.3.2. Autoridades de Registro ..... 10

1.3.3. Prestador de Serviço de Suporte ..... 11

1.3.4. Titulares de Certificado ..... 11

1.3.5. Aplicabilidade ..... 11

1.4. Dados de Contato ..... 12

2. DISPOSIÇÕES GERAIS ..... 13

2.1. Obrigações e Direitos ..... 13

2.1.1. Obrigações da AC ..... 13

2.1.2. Obrigações das AR ..... 13

2.1.3. Obrigações do Titular do Certificado ..... 13

2.1.4. Direitos da Terceira Parte (Relying Party) ..... 13

2.1.5. Obrigações do Repositório ..... 13

2.2. Responsabilidades ..... 13

2.2.1. Responsabilidades da AC ..... 13

2.2.2. Responsabilidades das AR ..... 13

2.3. Responsabilidade Financeira ..... 13

2.3.1. Indenizações devidas pela terceira parte(Relying Party) ..... 13

2.3.2. Relações Fiduciárias ..... 13

2.3.3. Processos Administrativos ..... 13

2.4. Interpretação e Execução ..... 13

2.4.1. Legislação ..... 13

2.4.2. Forma de interpretação e notificação ..... 13

2.4.3. Procedimentos da solução de disputa ..... 13

2.5. Tarifas de Serviço ..... 13

2.5.1. Tarifas de emissão e renovação de certificados ..... 13

2.5.2. Tarifas de acesso ao certificado ..... 13

2.5.3. Tarifas de revogação ou de acesso à informação de status ..... 13

2.5.4. Tarifas para outros serviços ..... 13

2.5.5. Política de reembolso ..... 13

2.6. Publicação e Repositório ..... 13

2.6.1. Publicação de informação da AC ... 13
2.6.2. Frequência de publicação ... 13
2.6.3. Controles de acesso ... 13
2.6.4. Repositórios ... 13
2.7. Fiscalização e Auditoria de Conformidade ... 13
2.8. Sigilo ... 13
2.8.1. Disposições gerais ... 13
2.8.2. Tipos de informações sigilosas ... 13
2.8.3. Tipos de informações não sigilosas ... 13
2.8.4. Divulgação de informação de revogação ou suspensão de certificado ... 13
2.8.5. Quebra de sigilo por motivos legais ... 13
2.8.6. Informações a terceiros ... 13
2.8.7. Divulgação por solicitação do Titular ... 13
2.8.8. Outras circunstâncias de divulgação de informação ... 13
2.9. Direitos de Propriedade Intelectual ... 13
3. IDENTIFICAÇÃO E AUTENTICAÇÃO ... 14
3.1. Registro Inicial ... 14
3.1.1. Disposições Gerais ... 14
3.1.2. Tipos de nomes ... 14
3.1.3. Necessidade de nomes significativos ... 14
3.1.4. Regras para interpretação de vários tipos de nomes ... 14
3.1.5. Unicidade de nomes ... 14
3.1.6. Procedimento para resolver disputa de nomes ... 14
3.1.7. Reconhecimento, autenticação e papel de marcas registradas ... 14
3.1.8. Método para comprovar a posse de chave privada ... 14
3.1.9. Autenticação da identidade de um indivíduo ... 14
3.1.10. Autenticação da identidade de uma organização ... 14
3.1.11. Autenticação da identidade de equipamento ou aplicação ... 14
3.1.12. Autenticação de identificação de equipamento para certificado CF-e-SAT ... 14
3.2. Geração de novo par de chaves antes da expiração do atual ... 14
3.3. Geração de novo par de chaves após expiração ou revogação ... 14
3.4. Solicitação de Revogação ... 14
4. REQUISITOS OPERACIONAIS ... 15
4.1. Solicitação de Certificado ... 15
4.2. Emissão de Certificado ... 15
4.3. Aceitação de Certificado ... 15

**4.4. Suspensão e Revogação de Certificado** ..... 15
**4.4.1. Circunstâncias para revogação** ..... 15
**4.4.2. Quem pode solicitar revogação** ..... 15
**4.4.3. Procedimento para solicitação de revogação** ..... 15
**4.4.4. Prazo para solicitação de revogação** ..... 15
**4.4.5. Circunstâncias para suspensão** ..... 15
**4.4.6. Quem pode solicitar suspensão** ..... 15
**4.4.7. Procedimento para solicitação de suspensão** ..... 15
**4.4.8. Limites no período de suspensão** ..... 15
**4.4.9. Frequência de emissão de LCR** ..... 15
**4.4.10. Requisitos para verificação de LCR** ..... 15
**4.4.11. Disponibilidade para revogação ou verificação de status on-line** ..... 15
**4.4.12. Requisitos para verificação de revogação on-line** ..... 15
**4.4.13. Outras formas disponíveis para divulgação de revogação** ..... 15
**4.4.14. Requisitos para verificação de outras formas de divulgação de revogação** ..... 15
**4.4.15. Requisitos especiais para o caso de comprometimento de chave** ..... 15
**4.5. Procedimentos de Auditoria de Segurança** ..... 15
**4.5.1. Tipos de eventos registrados** ..... 15
**4.5.2. Frequência de auditoria de registros (logs)** ..... 15
**4.5.3. Período de retenção para registros (logs) de auditoria** ..... 15
**4.5.4. Proteção de registro (log) de auditoria** ..... 15
**4.5.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria** 15
**4.5.6. Sistema de coleta de dados de auditoria** ..... 15
**4.5.7. Notificação de agentes causadores de eventos** ..... 15
**4.5.8. Avaliações de vulnerabilidade** ..... 15
**4.6. Arquivamento de Registros** ..... 15
**4.6.1. Tipos de registros arquivados** ..... 15
**4.6.2. Período de retenção para arquivo** ..... 15
**4.6.3. Proteção de arquivo** ..... 15
**4.6.4. Procedimentos para cópia de segurança (backup) de arquivo** ..... 15
**4.6.5. Requisitos para datação (time-stamping) de registros** ..... 15
**4.6.6. Sistema de coleta de dados de arquivo** ..... 15
**4.6.7. Procedimentos para obter e verificar informação de arquivo** ..... 15
**4.7. Troca de chave** ..... 15
**4.8. Comprometimento e Recuperação de Desastre** ..... 15

4.8.1. Recursos computacionais, software, e dados corrompidos ..... 15
4.8.2. Certificado de entidade é revogado ..... 15
4.8.3. Chave da entidade é comprometida ..... 15
4.8.4. Segurança dos recursos após desastre natural ou de outra natureza ..... 15
4.8.5. Atividades das Autoridades de Registro ..... 15
4.9. Extinção dos serviços de AC, AR ou PSS ..... 15
5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL ..... 16
5.1. Controles Físicos ..... 16
5.1.1. Construção e localização das instalações ..... 16
5.1.2. Acesso físico nas instalações de AC ..... 16
5.1.3. Energia e ar condicionado nas instalações de AC ..... 16
5.1.4. Exposição à água nas instalações de AC ..... 16
5.1.5. Prevenção e proteção contra incêndio nas instalações de AC ..... 16
5.1.6. Armazenamento de mídia nas instalações de AC ..... 16
5.1.7. Destruição de lixo nas instalações de AC ..... 16
5.1.8. Instalações de segurança (backup) externas (off-site) para AC ..... 16
5.1.9. Instalações técnicas de AR ..... 16
5.2. Controles Procedimentais ..... 16
5.2.1. Perfis qualificados ..... 16
5.2.2. Número de pessoas necessário por tarefa ..... 16
5.2.3. Identificação e autenticação para cada perfil ..... 16
5.3. Controles de Pessoal ..... 16
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade ..... 16
5.3.2. Procedimentos de verificação de antecedentes ..... 16
5.3.3. Requisitos de treinamento ..... 16
5.3.4. Frequência e requisitos para reciclagem técnica ..... 16
5.3.5. Frequência e sequencia de rodízio de cargos ..... 16
5.3.6. Sanções para ações não autorizadas ..... 16
5.3.7. Requisitos para contratação de pessoal ..... 16
5.3.8. Documentação fornecida ao pessoal ..... 16
6.CONTROLES TÉCNICOS DE SEGURANÇA ..... 17
6.1. Geração e Instalação do Par de Chaves ..... 17
6.1.1. Geração do par de chaves ..... 17
6.1.2. Entrega da chave privada à entidade titular do certificado ..... 18
6.1.3. Entrega da chave pública para emissor de certificado ..... 18

6.1.4. Disponibilização de chave pública da AC para usuários ..... 18
6.1.5. Tamanhos de chave ..... 18
6.1.6. Geração de parâmetros de chaves assimétricas ..... 18
6.1.7. Verificação da qualidade dos parâmetros ..... 18
6.1.8. Geração de chave por hardware ou software ..... 18
6.1.9. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3) ..... 18
6.2. Proteção da Chave Privada ..... 18
6.2.1. Padrões para módulo criptográfico ..... 18
6.2.2. Controle “n de m” para chave privada ..... 18
6.2.3. Recuperação (escrow) de chave privada ..... 19
6.2.4. Cópia de segurança (backup) de chave privada ..... 19
6.2.5. Arquivamento de chave privada ..... 19
6.2.6. Inserção de chave privada em módulo criptográfico ..... 19
6.2.7. Método de ativação de chave privada ..... 19
6.2.8. Método de desativação de chave privada ..... 19
6.2.9. Método de destruição de chave privada ..... 19
6.3. Outros Aspectos do Gerenciamento do Par de Chaves ..... 19
6.3.1. Arquivamento de chave pública ..... 19
6.3.2. Períodos de uso para as chaves pública e privada ..... 20
6.4. Dados de Ativação ..... 20
6.4.1. Geração e instalação dos dados de ativação ..... 20
6.4.2. Proteção dos dados de ativação ..... 20
6.4.3. Outros aspectos dos dados de ativação ..... 20
6.5. Controles de Segurança Computacional ..... 20
6.5.1. Requisitos técnicos específicos de segurança computacional ..... 20
6.5.2. Classificação da segurança computacional ..... 20
6.6. Controles Técnicos do Ciclo de Vida ..... 20
6.6.1.Controles de desenvolvimento de sistema ..... 20
6.6.2. Controles de gerenciamento de segurança ..... 21
6.6.3. Classificações de segurança de ciclo de vida ..... 21
6.7. Controles de Segurança de Rede ..... 21
6.8. Controles de Engenharia do Módulo Criptográfico ..... 21
7. PERFIS DE CERTIFICADO E LCR ..... 22
7.1. Perfil do Certificado ..... 22
7.1.1. Número de versão ..... 22
7.1.2. Extensões de certificado ..... 22

7.1.3. Identificadores de algoritmo ..... 25
7.1.4. Formatos de nome ..... 25
7.1.5. Restrições de nome ..... 25
7.1.6.OID (Object Identifier) de Política de Certificado ..... 26
7.1.7. Uso da extensão “Policy Constraints” ..... 26
7.1.8. Sintaxe e semântica dos qualificadores de política ..... 26
7.1.9. Semântica de processamento para extensões críticas ..... 26
7.2. Perfil de LCR ..... 26
7.2.1. Número(s) de versão ..... 26
7.2.2.Extensões de LCR e de suas entradas ..... 26
8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO ..... 27
8.1. Procedimentos de mudança de especificação ..... 27
8.2. Políticas de publicação e notificação ..... 27
8.3. Procedimentos de aprovação ..... 27
9. DOCUMENTOS REFERENCIADOS ..... 28

## LISTA DE ACRÔNIMOS E SIGLAS

| Acrônimo e Sigla | Descrição |
|---|---|
| AC | Autoridade Certificadora |
| AC Raiz | Autoridade Certificadora Raiz da ICP-Brasil |
| AR | Autoridade de Registro |
| CEI | Cadastro Específico do INSS |
| CF-e | Cupom Fiscal Eletrônico |
| CG ICP-Brasil | Comitê Gestor da ICP-Brasil |
| CNE | Cadastro Nacional de Estrangeiro |
| CNPJ | Cadastro Nacional de Pessoa Jurídica |
| DN | Distinguished Name |
| DPC | Declaração de Práticas de Certificação |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| 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 |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PCI | Política de Classificação de Informação |
| PCN | Plano de Continuidade de Negócio |
| PJ | Pessoa Jurídica |
| POP | Proof of Possession |
| PS | Política de Segurança |
| PRD | Plano de Recuperação de Desastres |
| Prodemge | Companhia de Tecnologia da Informação do Estado de Minas Gerais |
| PSS | Prestadores de Serviço de Suporte |
| RFC | Request For Comments |
| SAT | Sistema Autenticador e Transmissor |
| SSL | Secure Socket Layer |

# 1. INTRODUÇÃO

## 1.1. Visão Geral

1.1.1. Este documento descreve as “Políticas de Certificado” (PC) de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE SSL na Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

1.1.2. A estrutura desta PC está baseada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC 3647 (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework).

1.1.3. Não se aplica.

1.1.4. Não se aplica.

1.1.5. Não se aplica.

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.1.8. Não se aplica.

## 1.2. Identificação

1.2.1. Esta PC é chamada “Política de Certificado de assinatura digital Tipo A1 da Autoridade Certificadora PRODEMGE SSL” e referida como “PC A1 da AC PRODEMGE SSL”. Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A1 no REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.1.95.

1.2.2. Não se aplica.

## 1.3. Comunidade e Aplicabilidade

### 1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC refere-se exclusivamente à AC PRODEMGE SSL no âmbito da ICP-Brasil.

1.3.1.2. As práticas e procedimentos de certificação da AC PRODEMGE SSL estão descritos na Declaração de Práticas de Certificação da AC PRODEMGE SSL (DPC da AC PRODEMGE SSL).

### 1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro (AR) utilizadas pela AC PRODEMGE SSL para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em endereço *web* da AC PRODEMGE SSL (https://www.prodemge.gov.br/certificacaodigital/atendimento/postos-de-atendimento):

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 PRODEMGE SSL, 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 PRODEMGE SSL mantém as informações acima sempre atualizadas.

### 1.3.3. Prestador de Serviço de Suporte

1.3.3.1. A relação de todos os Prestadores de Serviço de Suporte (PSS) vinculados diretamente a AC PRODEMGE SSL e/ou por intermédio de suas AR é publicada em endereço *web* da AC PRODEMGE SSL (http://icp-brasil.ac.prodemge.gov.br/repositorio/ac_prodemge_ssl/index.html).

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

a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados;
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC PRODEMGE SSL mantém as informações acima sempre atualizadas.

### 1.3.4. Titulares de Certificado

Pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras, podem ser titulares de Certificado.

### 1.3.5. Aplicabilidade

1.3.5.1. Neste item são relacionadas as aplicações para as quais os certificados definidos por esta PC são adequados.

1.3.5.2. As aplicações e demais programas que admitem o uso de certificado digital de um determinado tipo, contemplado pela ICP-Brasil, aceitam qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.3.5.3. A AC PRODEMGE SSL leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos 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.

1.3.5.4. Os certificados emitidos pela AC PRODEMGE SSL no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.5. Não se aplica.

1.3.5.6. Não se aplica.

1.3.5.7. Não se aplica.

### 1.4. Dados de Contato

| | |
|---|---|
| Empresa: | Companhia de Tecnologia da Informação do Estado de Minas Gerais - PRODEMGE |
| Endereço: | Rua da Bahia, 2277<br>Bairro de Lourdes<br>CEP: 30.160-012<br>Belo Horizonte - MG |
| Telefone Fixo: | 31 3339-1245 |
| Nome: | Jacira dos Reis Xavier |
| E-mail geral: | acprodemge@prodemge.gov.br |

## 2. DISPOSIÇÕES GERAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC PRODEMGE SSL.

**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 das 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 da solução de disputa**

**2.5. Tarifas de Serviço**
**2.5.1. Tarifas de emissão e renovação de certificados**
**2.5.2. Tarifas de acesso ao certificado**
**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. Fiscalização e Auditoria de Conformidade**

**2.8. Sigilo**
**2.8.1. Disposições gerais**
**2.8.2. Tipos de informações sigilosas**
**2.8.3. Tipos de informações não sigilosas**
**2.8.4. Divulgação de informação de revogação ou suspensão de certificado**
**2.8.5. Quebra de sigilo por motivos legais**
**2.8.6. Informações a terceiros**
**2.8.7. Divulgação por solicitação do Titular**
**2.8.8. Outras circunstâncias de divulgação de informação**

**2.9. Direitos de Propriedade Intelectual**

# 3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC PRODEMGE SSL.

**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
**3.1.12. Autenticação de identificação de equipamento para certificado CF-e-SAT**

**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 são referidos os itens correspondentes da DPC da AC PRODEMGE SSL.

**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, e dados corrompidos**
**4.8.2. Certificado de entidade é revogado**
**4.8.3. Chave da 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 são referidos os itens correspondentes da DPC da AC PRODEMGE SSL.

**5.1. Controles Físicos**
**5.1.1. Construção e localização das instalações**
**5.1.2. Acesso físico nas instalações de AC**
5.1.2.1. Níveis de acesso
5.1.2.2. Sistemas físicos de detecção
5.1.2.3. Sistema de controle de acesso
5.1.2.4. Mecanismos de emergência
**5.1.3. Energia e ar condicionado nas instalações de AC**
**5.1.4. Exposição à água nas instalações de AC**
**5.1.5. Prevenção e proteção contra incêndio nas instalações de AC**
**5.1.6. Armazenamento de mídia nas instalações de AC**
**5.1.7. Destruição de lixo nas instalações de AC**
**5.1.8. Instalações de segurança (backup) externas (off-site) para AC**
**5.1.9. Instalações técnicas de AR**

**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 sequencia 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

## 6.1. Geração e Instalação do Par de Chaves

### 6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física. 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.

6.1.1.1.1. Não se aplica.

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando Cryptographic Service Provider (CSP) existente na estação do solicitante apresentados pelo browser e, quando da geração, a chave privada é armazenada no HD da estação.

A chave privada poderá ser exportada e armazenada (cópia de segurança) em mídia externa – pendrive, token ou cartão inteligente - e protegida por senha de acesso.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado A1.

6.1.1.5. A chave privada trafega 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. O meio de armazenamento da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

b) a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;

c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

O tipo de certificado emitido pela AC PRODEMGE SSL e descrito nesta PC é o A1.

| Tipo de Certificado | Mídia Armazenadora de Chave Criptográfica<br><br>(Requisitos Mínimos) |
|---|---|
| A1 | Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima. |

Nota: para certificados do tipo A CF-e-SAT, T3 e T4, a exigência de homologação das mídias para geração e armazenamento de chaves criptográficas fica suspensa até ulterior deliberação do Comitê Gestor da ICP-Brasil.

6.1.1.8. A responsabilidade pela adoção de controles de segurança para a garantia do sigilo,

integridade e disponibilidade da chave privada gerada no equipamento é do titular do certificado, conforme especificado no Termo de Titularidade, no caso de certificados de pessoa física, e da pessoa responsável, indicada por seu(s) representante(s) legal(s), conforme especificado no Termo de Responsabilidade, no caso de certificados de pessoa jurídica, de aplicações.

### 6.1.2. Entrega da chave privada à entidade titular do certificado

Não se aplica.

### 6.1.3. Entrega da chave pública para emissor de certificado

A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura Secure Socket Layer (SSL).

### 6.1.4. Disponibilização de chave pública da AC para usuários

A AC PRODEMGE SSL disponibiliza o seu certificado e todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através endereços *web*: http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl.p7c e https://www.prodemge.gov.br/certificacaodigital.

### 6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC PRODEMGE SSL é de 2048 bits para a cadeia de certificação V5.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A1 da ICP-Brasil está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

### 6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

### 6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

### 6.1.8. Geração de chave por hardware ou software

A geração das chaves criptográficas do Certificado Tipo A1 desta PC, é realizada por software.

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

Os certificados têm ativados apenas o bit *digitalSignature*.

Os pares de chaves correspondentes aos certificados emitidos pela AC PRODEMGE SSL podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

## 6.2. Proteção da Chave Privada

### 6.2.1. Padrões para módulo criptográfico

Não se aplica.

### 6.2.2. Controle “n de m” para chave privada

Não se aplica.

### 6.2.3. Recuperação (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura sem o consentimento do titular do certificado.

### 6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. Com exceção das chaves privadas vinculadas a certificados do tipo A CF-e-SAT, T3 e T4, que não podem possuir cópia de segurança, qualquer titular de certificado dos demais tipos poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC PRODEMGE SSL não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

### 6.2.5. Arquivamento de chave privada

6.2.5.1. A AC PRODEMGE SSL não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados.

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

Os Titulares de Certificados poderão optar por utilizar um hardware criptográfico, cartão inteligente ou token, para armazenar sua chave privada após a aceitação do certificado.

### 6.2.7. Método de ativação de chave privada

O titular do certificado pode definir procedimentos necessários para a ativação de sua chave privada.

### 6.2.8. Método de desativação de chave privada

O titular de certificado pode definir procedimentos necessários para a desativação de sua chave privada.

### 6.2.9. Método de destruição de chave privada

O titular de certificado pode definir procedimentos necessários para a destruição de sua chave privada.

## 6.3. Outros Aspectos do Gerenciamento do Par de Chaves

### 6.3.1. Arquivamento de chave pública

As chaves públicas dos titulares de certificados de assinatura digital emitidos pela AC PRODEMGE SSL permanecem armazenadas após a expiração dos correspondentes certificados, permanentemente, na forma da legislação em vigor, 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. As chaves privadas de assinatura dos respectivos titulares de certificados emitidos pela AC PRODEMGE SSL são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação das assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. O período máximo de validade admitido para certificados de assinatura digital Tipo A1 da AC PRODEMGE SSL é de 1 (um) ano.

**6.4. Dados de Ativação**

**6.4.1. Geração e instalação dos dados de ativação**

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

**6.4.2. Proteção dos dados de ativação**

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

**6.4.3. Outros aspectos dos dados de ativação**

Não se aplica.

**6.5. Controles de Segurança Computacional**

**6.5.1. Requisitos técnicos específicos de segurança computacional**

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, com proteção anti-vírus e criptografia 3DES para a chave privada, armazenada no HD.

**6.5.2. Classificação da segurança computacional**

Não se aplica.

**6.6. Controles Técnicos do Ciclo de Vida**

A AC PRODEMGE SSL desenvolve sistemas apenas com finalidade relacionada à operação de suas AR vinculadas.

**6.6.1.Controles de desenvolvimento de sistema**

6.6.1.1. A AC PRODEMGE SSL utiliza o Processo de Software Prodemge fundamentado nos modelos de referências: Unified Process – UP e Melhoria do Processo de Software Brasileiro – MPS.BR. Contém as abordagens: tradicional e ágil e utiliza os padrões de engenharia de software aplicáveis ao contexto da Prodemge. É iterativo, incremental, adaptativo, configurável e com foco na qualidade de software, possibilitando o desenvolvimento e a manutenção de software em diferentes plataformas tecnológicas.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC PRODEMGE SSL provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC PRODEMGE SSL.

### 6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC PRODEMGE SSL verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. A AC PRODEMGE SSL utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

### 6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

## 6.7. Controles de Segurança de Rede

Não se aplica.

## 6.8. Controles de Engenharia do Módulo Criptográfico

Não se aplica.

# 7. PERFIS DE CERTIFICADO E LCR

## 7.1. Perfil do Certificado

Todos os certificados emitidos pela AC PRODEMGE SSL estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

### 7.1.1. Número de versão

Os certificados emitidos pela AC PRODEMGE SSL implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

### 7.1.2. Extensões de certificado

7.1.2.1. Neste item, a PC descreve todas as extensões de certificado utilizadas pela AC PRODEMGE SSL e sua criticalidade.

7.1.2.2. Extensões Obrigatórias:
Os certificados emitidos pela AC PRODEMGE SSL obedecem a ICP-Brasil, que define como obrigatórias as seguintes extensões:

a) ***"Authority Key Identifier"*, não crítica**: o campo *keyIdentifier* contém o hash SHA-1 da chave pública da AC PRODEMGE SSL;

b) ***"Key Usage"*, crítica**: somente os bits *digitalSignature, nonRepudiation e keyEncipherment* estão ativados;

c) ***"Certificate Policies"*, não crítica:** contém:

- O OID desta PC: 2.16.76.1.2.1.95;
- Os campos *policyQualifiers* contém o endereço *web* da DPC AC PRODEMGE SSL: http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_ssl/dpc_ac_prodemge_ssl.pdf;

d) ***"CRL Distribution Points"*, não crítica:** contém os endereços *web* onde se obtém a LCR da AC PRODEMGE SSL:

Para certificados emitidos na V1:
http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_ssl/lcr_ac_prodemge_ssl.crl
http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_ssl/lcr_ac_prodemge_ssl.crl

e) ***"Authority Information Access"*, não crítica:**
contém o endereço de acesso aos certificados da cadeia de certificação através do link: http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl.p7c;
e o endereço de acesso ao serviço de Consulta On-Line de Situação de Certificado (Online Certificate Status Protocol - OCSP) no link: http://ocsp.ac-prodemge-ssl.ac.prodemge.gov.br;

f) ***"basicConstraints",* não crítica**: contém o campo cA=False.

7.1.2.3. Os certificados emitidos pela AC PRODEMGE SSL possuem 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 nesta ordem:

i· 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 subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social – NIS (PIS,PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG)

do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;

ii· 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;

iii· 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 subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

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

i. rfc822Name contendo o endereço e-mail do titular do certificado;

ii. OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo = Nome Principal que contém o domínio de login em estações de trabalho (UPN)

b) Para certificado de pessoa jurídica:

b.1) 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 ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva Unidade da Federação;

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 = nas 14 (quatorze) posições o número do 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 Específico do INSS (CEI) da pessoa jurídica titular do certificado.

b.2) campos *otherName*, não obrigatórios, contendo:

i. rfc822Name contendo o endereço e-mail do titular do certificado;

ii. OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo = Nome Principal que contém o domínio de login em estações de trabalho (UPN)

c) Para certificado de aplicação:

c.1) 4 (quatro) campos *otherName*, obrigatórios, contendo, nesta ordem:

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

ii. OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do 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 ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

7.1.2.4. Os campos *otherName*, definidos como obrigatórios, estão de acordo com as seguintes especificações:

a) o conjunto de informações definido em cada campo *otherName* é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING, com exceção do campo UPN que possui uma cadeia de caracteres do tipo ASN.1 UTF8 STRING;

b) quando os números de NIS (PIS, PASEP ou CI), RG, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes são integralmente preenchidos com caracteres “zero”;

c) se o número do RG não estiver disponível, não é preenchido o campo de órgão emissor/UF. O mesmo ocorre para o campo do município e UF se não houver número de inscrição do Título de Eleitor;

d) não se aplica;

e) todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidos com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível;

f) as 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, sendo utilizados 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, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais, com exceção do campo UPN que utiliza caracteres especiais

7.1.2.5. Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos pela AC PRODEMGE SSL, podem ser utilizados com OID atribuídos ou aprovados pela AC-Raiz.

Campos *otherName* não obrigatórios quando não utilizados não terão seus OID incluído no certificado.

7.1.2.6. Os outros campos que compõem a extensão "*Subject Alternative Name*" podem ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.7. Não se aplica.

7.1.2.8. Não se aplica.

7.1.2.9. A AC PRODEMGE SSL implementa a extensão ***"Extended Key Usage"*, não critica**:

a) Para certificados de assinatura de resposta OCSP: somente o propósito “*OCSP Signing*” (OID 1.3.6.1.5.5.7.3.9) está ativado;

b) Para certificado de Autenticação de Servidor: deve conter o propósito “*server authentication*” (OID 1.3.6.1.5.5.7.3.1) ativado e pode conter o propósito “*client authentication*” (OID 1.3.6.1.5.5.7.3.2) ativado.

### 7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC PRODEMGE SSL são assinados com o uso do algoritmo RSA com SHA-256 como função de hash (OID 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função de hash (OID = 1.2.840.113549.1.1.13) na cadeia de certificação V5 conforme o padrão PKCS#1.

### 7.1.4. Formatos de nome

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

i. Nos formatos abaixo, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres “<” e “>” não devem ser incluídos.
ii. Os dados necessários para preenchimento do DN deverão ser os informados na AUTORIZAÇÃO citada no item 3.1.9.1 ou 3.1.10.2 da DPC.
iii. Todos os campos do DN são obrigatórios e devem ser preenchidos.
iv. O tamanho máximo de cada componente do DN (C,CN,O,OU,etc) é de 64 caracteres.

Para certificado na hierarquia da Autoridade Certificadora Raiz Brasileira V5:
C = BR
O = ICP-Brasil
OU = Autenticado por <AR Autenticadora>
OU = Assinatura Tipo A1
CN = < URL correspondente ao equipamento ou nome da aplicação >

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

O campo E (endereço e-mail do titular do certificado) deixou de compor o "Distinguished Name" (DN) a partir da implementação da cadeia V5.

### 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. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC PRODEMGE SSL são as seguintes:

a) Não são admitidos sinais de acentuação, trema ou cedilhas;
   i. Caracteres acentuados devem ser substituídos por seu correspondente sem acento;
   ii. O cedilha deve ser substituído pelo caractere 'c'.

b) - Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

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

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

O OID desta PC é 2.16.76.1.2.1.95.

Todo certificado emitido segundo essa PC (PC A1 da AC PRODEMGE SSL) contém o valor desse OID presente na extensão Certificate Policies.

### 7.1.7. Uso da extensão "Policy Constraints"

Não se aplica.

### 7.1.8. Sintaxe e semântica dos qualificadores de política

Os campos "*policyQualifiers*" da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC PRODEMGE SSL (http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_ssl/dpc_ac_prodemge_ssl.pdf).

### 7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

## 7.2. Perfil de LCR

### 7.2.1. Número(s) de versão

As LCR geradas pela AC PRODEMGE SSL implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

### 7.2.2.Extensões de LCR e de suas entradas

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC PRODEMGE SSL e sua criticalidade.

7.2.2.2. As LCR da AC PRODEMGE SSL obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

a) ***Authority Key Identifier*, não crítica**: contém o hash SHA-1 da chave pública da AC PRODEMGE SSL;
b) ***CRL Number*, não crítica**: contém um número sequencial para cada LCR emitida pela AC PRODEMGE SSL.

# 8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

## 8.1. Procedimentos de mudança de especificação

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC PRODEMGE SSL. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

## 8.2. Políticas de publicação e notificação

A AC PRODEMGE SSL mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço *web* http://icp-brasil.ac.prodemge.gov.br /repositorio/dpc/ac_prodemge_ssl/pc_a1_ac_prodemge_ssl_v1.0.pdf.

## 8.3. Procedimentos de aprovação

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC PRODEMGE SSL, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

## 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 |
|---|---|---|
| [1] | REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL | DOC-ICP-04 |
| [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 |
|---|---|---|
| [2] | PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL | DOC-ICP-01.01 |