

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

**PC A1 da AC PRODEMGE**

**Versão 5.1 - 05/12/2014**

## ÍNDICE

<b>1. INTRODUÇÃO .....</b>	<b>6</b>
1.1.VISÃO GERAL.....	6
1.2.IDENTIFICAÇÃO .....	6
1.3.COMUNIDADE E APLICABILIDADE .....	6
1.3.1.Autoridades Certificadoras .....	6
1.3.2.Autoridades de Registro .....	6
1.3.3. Prestador de Serviço de Suporte .....	7
1.3.4.Titulares de Certificado.....	7
1.3.5.Aplicabilidade.....	7
1.4.DADOS DE CONTATO.....	7
<b>2. DISPOSIÇÕES GERAIS .....</b>	<b>8</b>
2.1. OBRIGAÇÕES E DIREITOS .....	8
2.1.1. Obrigações da AC PRODEMGE.....	8
2.1.2. Obrigações das AR.....	8
2.1.3. Obrigações do Titular do Certificado .....	8
2.1.4. Direitos da Terceira Parte (Relying Party).....	8
2.1.5. Obrigações do Repositório.....	8
2.2. RESPONSABILIDADES .....	8
2.2.1. Responsabilidades da AC PRODEMGE.....	8
2.2.2. Responsabilidades das AR.....	8
2.3. RESPONSABILIDADE FINANCEIRA.....	8
2.3.1. Indenizações devidas pela terceira parte(Relying Party).....	8
2.3.2. Relações Fiduciárias .....	8
2.3.3. Processos Administrativos.....	8
2.4. INTERPRETAÇÃO E EXECUÇÃO .....	8
2.4.1. Legislação.....	8
2.4.2. Forma de interpretação e notificação .....	8
2.4.3. Procedimentos da solução de disputa .....	8
2.5. TARIFAS DE SERVIÇO .....	8
2.5.1. Tarifas de emissão e renovação de certificados .....	8
2.5.2. Tarifas de acesso ao certificado .....	8
2.5.3. Tarifas de revogação ou de acesso à informação de status .....	8
2.5.4. Tarifas para outros serviços.....	8
2.5.5. Política de reembolso .....	8
2.6. PUBLICAÇÃO E REPOSITÓRIO .....	8
2.6.1. Publicação de informação da AC PRODEMGE .....	8
2.6.2. Frequência de publicação .....	8
2.6.3. Controles de acesso .....	8
2.6.4. Repositórios.....	8
2.7. FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE.....	8
2.8. SIGILO .....	8
2.8.1. Disposições gerais.....	8
2.8.2. Tipos de informações sigilosas.....	8
2.8.3. Tipos de informações não-sigilosas.....	8
2.8.4. Divulgação de informação de revogação ou suspensão de certificado.....	8
2.8.5. Quebra de sigilo por motivos legais.....	8
2.8.6. Informações a terceiros.....	8
2.8.7. Divulgação por solicitação do Titular.....	8
2.8.8. Outras circunstâncias de divulgação de informação .....	8
2.9. DIREITOS DE PROPRIEDADE INTELECTUAL.....	8
<b>3. IDENTIFICAÇÃO E AUTENTICAÇÃO .....</b>	<b>9</b>
3.1. REGISTRO INICIAL .....	9

3.1.1.	<i>Disposições Gerais</i> .....	9
3.1.2.	<i>Tipos de nomes</i> .....	9
3.1.3.	<i>Necessidade de nomes significativos</i> .....	9
3.1.4.	<i>Regras para interpretação de vários tipos de nomes</i> .....	9
3.1.5.	<i>Unicidade de nomes</i> .....	9
3.1.6.	<i>Procedimento para resolver disputa de nomes</i> .....	9
3.1.7.	<i>Reconhecimento, autenticação e papel de marcas registradas</i> .....	9
3.1.8.	<i>Método para comprovar a posse de chave privada</i> .....	9
3.1.9.	<i>Autenticação da identidade de um indivíduo</i> .....	9
3.1.9.1.	<i>Documentos para efeitos de identificação de um indivíduo</i> .....	9
3.1.9.2.	<i>Informações contidas no certificado emitido para um indivíduo</i> .....	9
3.1.10.	<i>Autenticação da identidade de uma organização</i> .....	9
3.1.10.1.	<i>Disposições Gerais</i> .....	9
3.1.10.2.	<i>Documentos para efeitos de identificação de uma organização</i> .....	9
3.1.10.3.	<i>Informações contidas no certificado emitido para uma organização</i> .....	9
3.1.11.	<i>Autenticação da identidade de equipamento ou aplicação</i> .....	9
3.1.11.1.	<i>Disposições Gerais</i> .....	9
3.1.11.2.	<i>Procedimentos para efeitos de identificação de um equipamento ou aplicação</i> .....	9
3.1.11.3.	<i>Informações contidas no certificado emitido para um equipamento ou aplicação</i> .....	9
3.2.	<b>GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL</b> .....	9
3.3.	<b>GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO</b> .....	9
3.4.	<b>SOLICITAÇÃO DE REVOGAÇÃO</b> .....	9
<b>4.</b>	<b>REQUISITOS OPERACIONAIS</b> .....	<b>9</b>
4.1.	<b>SOLICITAÇÃO DE CERTIFICADO</b> .....	9
4.2.	<b>EMISSÃO DE CERTIFICADO</b> .....	9
4.3.	<b>ACEITAÇÃO DE CERTIFICADO</b> .....	9
4.4.	<b>SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO</b> .....	10
4.4.1.	<i>Circunstâncias para revogação</i> .....	10
4.4.2.	<i>Quem pode solicitar revogação</i> .....	10
4.4.3.	<i>Procedimento para solicitação de revogação</i> .....	10
4.4.4.	<i>Prazo para solicitação de revogação</i> .....	10
4.4.5.	<i>Circunstâncias para suspensão</i> .....	10
4.4.6.	<i>Quem pode solicitar suspensão</i> .....	10
4.4.7.	<i>Procedimento para solicitação de suspensão</i> .....	10
4.4.8.	<i>Limites no período de suspensão</i> .....	10
4.4.9.	<i>Frequência de emissão de LCR</i> .....	10
4.4.10.	<i>Requisitos para verificação de LCR</i> .....	10
4.4.11.	<i>Disponibilidade para revogação ou verificação de status on-line</i> .....	10
4.4.12.	<i>Requisitos para verificação de revogação on-line</i> .....	10
4.4.13.	<i>Outras formas disponíveis para divulgação de revogação</i> .....	10
4.4.14.	<i>Requisitos para verificação de outras formas de divulgação de revogação</i> .....	10
4.4.15.	<i>Requisitos especiais para o caso de comprometimento de chave</i> .....	10
4.5.	<b>PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA</b> .....	10
4.5.1.	<i>Tipos de eventos registrados</i> .....	10
4.5.2.	<i>Frequência de auditoria de registros (logs)</i> .....	10
4.5.3.	<i>Período de retenção para registros (logs) de auditoria</i> .....	10
4.5.4.	<i>Proteção de registro (log) de auditoria</i> .....	10
4.5.5.	<i>Procedimentos para cópia de segurança (backup) de registro (log) de auditoria</i> .....	10
4.5.6.	<i>Sistema de coleta de dados de auditoria</i> .....	10
4.5.7.	<i>Notificação de agentes causadores de eventos</i> .....	10
4.5.8.	<i>Avaliações de vulnerabilidade</i> .....	10
4.6.	<b>ARQUIVAMENTO DE REGISTROS</b> .....	10
4.6.1.	<i>Tipos de registros arquivados</i> .....	10
4.6.2.	<i>Período de retenção para arquivo</i> .....	10
4.6.3.	<i>Proteção de arquivo</i> .....	10
4.6.4.	<i>Procedimentos para cópia de segurança (backup) de arquivo</i> .....	10

4.6.5.	Requisitos para datação (time-stamping) de registros .....	10
4.6.6.	Sistema de coleta de dados de arquivo .....	10
4.6.7.	Procedimentos para obter e verificar informação de arquivo .....	10
4.7.	TROCA DE CHAVE .....	10
4.8.	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE .....	10
4.8.1.	Recursos computacionais, software, e dados corrompidos .....	10
4.8.2.	Certificado de entidade é revogado .....	10
4.8.3.	Chave da entidade é comprometida .....	10
4.8.4.	Segurança dos recursos após desastre natural ou de outra natureza .....	10
4.8.5.	Atividades das Autoridades de Registro .....	10
4.9.	EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS .....	10
<b>5.</b>	<b>CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL .....</b>	<b>11</b>
5.1.	CONTROLES FÍSICOS .....	11
5.1.1.	Construção e localização das instalações .....	11
5.1.2.	Acesso físico nas instalações de AC .....	11
5.1.2.1.	Níveis de acesso .....	11
5.1.2.2.	Sistemas físicos de detecção .....	11
5.1.2.3.	Sistema de controle de acesso .....	11
5.1.2.4.	Mecanismos de emergência .....	11
5.1.3.	Energia e ar condicionado nas instalações de AC .....	11
5.1.4.	Exposição à água nas instalações de AC .....	11
5.1.5.	Prevenção e proteção contra incêndio nas instalações de AC .....	11
5.1.6.	Armazenamento de mídia nas instalações de AC .....	11
5.1.7.	Destruição de lixo nas instalações de AC .....	11
5.1.8.	Instalações de segurança (backup) externas (off-site) para AC .....	11
5.1.9.	Instalações técnicas de AR .....	11
5.2.	CONTROLES PROCEDIMENTAIS .....	11
5.2.1.	Perfis qualificados .....	11
5.2.2.	Número de pessoas necessário por tarefa .....	11
5.2.3.	Identificação e autenticação para cada perfil .....	11
5.3.	CONTROLES DE PESSOAL .....	11
5.3.1.	Antecedentes, qualificação, experiência e requisitos de idoneidade .....	11
5.3.2.	Procedimentos de verificação de antecedentes .....	11
5.3.3.	Requisitos de treinamento .....	11
5.3.4.	Frequência e requisitos para reciclagem técnica .....	11
5.3.5.	Frequência e seqüência de rodízio de cargos .....	11
5.3.6.	Sanções para ações não autorizadas .....	11
5.3.7.	Requisitos para contratação de pessoal .....	11
5.3.8.	Documentação fornecida ao pessoal .....	11
<b>6.</b>	<b>CONTROLES TÉCNICOS DE SEGURANÇA .....</b>	<b>12</b>
6.1.	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES .....	12
6.1.1.	Geração do par de chaves .....	12
6.1.2.	Entrega da chave privada à entidade titular do certificado .....	13
6.1.3.	Entrega da chave pública para emissor de certificado .....	13
6.1.4.	Disponibilização de chave pública da AC para usuários .....	13
6.1.5.	Tamanhos de chave .....	13
6.1.6.	Geração de parâmetros de chaves assimétricas .....	13
6.1.7.	Verificação da qualidade dos parâmetros .....	13
6.1.8.	Geração de chave por hardware ou software .....	13
6.1.9.	Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3) .....	13
6.2.	PROTEÇÃO DA CHAVE PRIVADA .....	13
6.2.1.	Padrões para módulo criptográfico .....	13
6.2.2.	Controle "n de m" para chave privada .....	13
6.2.3.	Recuperação (escrow) de chave privada .....	13
6.2.4.	Cópia de segurança (backup) de chave privada .....	14

6.2.5.Arquivamento de chave privada .....	14
6.2.6.Inserção de chave privada em módulo criptográfico .....	14
6.2.7.Método de ativação de chave privada .....	14
6.2.8.Método de desativação de chave privada.....	14
6.2.9.Método de destruição de chave privada.....	14
6.3.OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES .....	14
6.3.1.Arquivamento de chave pública.....	14
6.3.2.Períodos de uso para as chaves pública e privada.....	14
6.4.DADOS DE ATIVAÇÃO .....	15
6.4.1.Geração e instalação dos dados de ativação .....	15
6.4.2.Proteção dos dados de ativação.....	15
6.4.3.Outros aspectos dos dados de ativação.....	15
6.5.CONTROLES DE SEGURANÇA COMPUTACIONAL .....	15
6.5.1.Requisitos técnicos específicos de segurança computacional .....	15
6.5.2.Classificação da segurança computacional .....	15
6.6.CONTROLES TÉCNICOS DO CICLO DE VIDA .....	15
6.6.1.Controles de desenvolvimento de sistema .....	15
6.6.2.Controles de gerenciamento de segurança.....	15
6.6.3.Classificações de segurança de ciclo de vida.....	15
6.7.CONTROLES DE SEGURANÇA DE REDE .....	15
6.8.CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO .....	16
<b>7. PERFIS DE CERTIFICADO E LCR.....</b>	<b>16</b>
7.1.PERFIL DO CERTIFICADO .....	16
7.1.1.Número de versão.....	16
7.1.2.Extensões de certificado .....	16
7.1.3.Identificadores de algoritmo .....	19
7.1.4.Formatos de nome .....	19
7.1.5.Restrições de nome .....	20
7.1.6.OID (Object Identifier) de Política de Certificado.....	20
7.1.7.Uso da extensão “Policy Constraints” .....	20
7.1.8.Sintaxe e semântica dos qualificadores de política .....	20
7.1.9.Semântica de processamento para extensões críticas .....	20
7.2.PERFIL DE LCR .....	21
7.2.1.Número(s) de versão.....	21
7.2.2.Extensões de LCR e de suas entradas.....	21
<b>8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO.....</b>	<b>21</b>
8.1.PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO .....	21
8.2.POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO .....	21
8.3.PROCEDIMENTOS DE APROVAÇÃO .....	21
<b>9. DOCUMENTOS REFERENCIADOS.....</b>	<b>21</b>

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

### **1. INTRODUÇÃO**

#### **1.1. Visão Geral**

1.1.1. Esta "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE na Infraestrutura de Chaves Públicas Brasileira.

A estrutura desta PC está baseada no DOC-ICP-04 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC 2527 (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework).

1.1.2. Não se aplica.

1.1.3. Não se aplica.

1.1.4. Não se aplica.

1.1.5. Não se aplica.

1.1.6. Não se aplica.

#### **1.2. Identificação**

1.2.1. Esta PC é chamada "Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE" e referida como "PC A1 da AC PRODEMGE". Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A1 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.1.15.

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 no âmbito da ICP-Brasil.

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

##### **1.3.2. Autoridades de Registro**

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC PRODEMGE 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 serviço de diretório e/ou em página web da AC PRODEMGE (<https://www.prodemge.gov.br/certificacaodigital/atendimento-ao-cliente/contato/sub-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, 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 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 e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC PRODEMGE (<http://icp-brasil.certisign.com.br/repositorio/ac-prodemge/index.htm>).

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; ou
- c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. A AC PRODEMGE 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 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 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.

### **1.4. Dados de Contato**

Nome:	Companhia de Tecnologia da Informação do Estado de Minas Gerais - PRODEMGE
Endereço:	Rua da Bahia 2277 – Bairro de Lourdes – Belo Horizonte - MG
Telefone:	(31) 3339-1111
Fax:	
Nome:	Jacira dos Reis Xavier
Telefone:	(31) 3339-1245
Fax:	(31) 3339-1319
E-mail:	<a href="mailto:gor@prodemge.gov.br">gor@prodemge.gov.br</a>
E-mail:	<a href="mailto:goc@prodemge.gov.br">goc@prodemge.gov.br</a>



## **2. DISPOSIÇÕES GERAIS**

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

- 2.1. Obrigações e Direitos**
  - 2.1.1. Obrigações da AC PRODEMGE**
  - 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 PRODEMGE**
  - 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 PRODEMGE**
  - 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.

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

- 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.

### **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 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

### 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.

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) 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 –disquete, 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 [1].

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 [1]. 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; e

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 e descrito nesta PC é o A1.

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

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 seus(s) representante(s) legal(s), conforme especificado no Termo de Responsabilidade, no caso de certificados de pessoa jurídica, de equipamentos e 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 SSL - Secure Socket Layer.

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

A AC PRODEMGE disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web: [http://icp-brasil.certisign.com.br/repositorio/certificados/AC\\_PRODEMGE\\_G3.p7c](http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G3.p7c).

### **6.1.5. Tamanhos de chave**

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC PRODEMGE é de 1024 bits para as hierarquias V0 e V1 e de 2048 bits para as hierarquias V2.

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 [1].

### **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 [1].

### **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 [1].

### **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 os bits digitalSignature, nonRepudiation e keyEncipherment.

Os pares de chaves correspondentes aos certificados emitidos pela AC PRODEMGE 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. Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua chave privada.

6.2.4.2.A AC PRODEMGE 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 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 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 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 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 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 utiliza um modelo clássico espiral no desenvolvimento dos sistemas. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC PRODEMGE utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos informais.

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

### **6.6.2.Controles de gerenciamento de segurança**

6.6.2.1. A AC PRODEMGE 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 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 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 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 e sua criticalidade.

7.1.2.2. Extensões Obrigatórias:

Os certificados emitidos pela AC PRODEMGE 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;
- b) **Key Usage**, crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;
- c) **Certificate Policies**, não crítica contém:
  - O OID desta PC: 2.16.76.1.2.1.15;
  - Os campos policyQualifiers contém o endereço Web da DPC AC PRODEMGE: ([http://icp-brasil.certisign.com.br/repositorio/dpc/AC\\_PRODEMGE/DPC\\_AC\\_PRODEMGE.pdf](http://icp-brasil.certisign.com.br/repositorio/dpc/AC_PRODEMGE/DPC_AC_PRODEMGE.pdf));
- d) **CRL Distribution Points**, não crítica: contém os endereços Web onde se obtém a LCR da AC PRODEMGE:

Para certificados emitidos na G2:

  - <http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGE2/LatestCRL.crl>
  - <http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGE2/LatestCRL.crl>
  - <http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACPRODEMGE2/LatestCRL.crl>

Para certificados emitidos na G3:

  - <http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGE3/LatestCRL.crl>
  - <http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGE3/LatestCRL.crl>
  - <http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACPRODEMGE3/LatestCRL.crl>
- e) **Authority Information Access**, não crítica: contém o endereço de acesso aos certificados da cadeia de certificação através do link: [http://icp-brasil.certisign.com.br/repositorio/certificados/AC\\_PRODEMGE\\_G3.p7c](http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G3.p7c);
- f) **basicConstraints**, não crítica: contém o campo cA=False.

7.1.2.3. Os certificados emitidos pela AC PRODEMGE 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 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 10 (dez) posições subseqüentes, 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 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. 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 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 Registro Geral (RG) do responsável; nas 10 (dez) posições subseqüentes, 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 equipamento ou 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 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 = 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.

c.2) Quando certificados de equipamento forem emitidos para servidores de Domain Controller, adicionalmente irão conter os seguintes campos otherName:

- i. OID = 1.3.6.1.4.1.311.25.1 contendo o identificador (Globally Unique Identifier - GUID) do Domain Controller;
- ii. DNS Name, contendo o nome do domínio;
- iii. rfc822Name contendo o endereço e-mail do responsável pelo certificado ou da pessoa jurídica, em caso de email corporativo.

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;
- h) O campo UPN é opcional, caso não seja usado o OID não é incluído no certificado .

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

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. A AC PRODEMGE implementa a extensão "Extended Key Usage", não crítica, contendo o valor "server authentication" (OID 1.3.6.1.5.5.7.3.1), e podendo conter os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2) e/ou "Netscape SGC" (OID 2.16.840.1.113730.4.1) e/ou "Microsoft SGC" (OID 1.3.6.1.4.1.311.10.3.3) para certificados de equipamento, o valor "client authentication" (OID 1.3.6.1.5.5.7.3.2) e podendo conter os valores "code signing" (OID 1.3.6.1.5.5.7.3.3) e/ou "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4) e/ou "OCSPSigning" (OID 1.3.6.1.5.5.7.3.9) para certificados de aplicação e os valores "client authentication" (OID 1.3.6.1.5.5.7.3.2), "E-mail protection" (OID 1.3.6.1.5.5.7.3.4) e podendo conter o valor "Smart Card Logon" (OID 1.3.6.1.4.1.311.20.2.2), quando for utilizado o campo "UPN" na extensão "Subject Alternative Name", para certificados de pessoa jurídica e pessoa física.

### **7.1.3. Identificadores de algoritmo**

Os certificados emitidos pela AC PRODEMGE são assinados com o uso do algoritmo RSA com SHA-1 como função de hash (OID = 1.2.840.113549.1.1.5) nas hierarquias V0 e V1, 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 hierarquia V2 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:

C = BR

O = ICP-Brasil

OU = identificador (indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou seqüência alfanumérica)

CN = nome do titular do certificado

E = endereço e-mail do titular do certificado ou do responsável pela pessoa jurídica titular do certificado.

Onde:

O "Distinguished Name" (DN) pode apresentar até sete campos "OU". Caso qualquer um dos campos OU não seja utilizado, o mesmo terá grafado o texto "(em branco)" ou não será apresentado no DN.

Em um certificado de pessoa jurídica, o identificador CN contém a denominação da razão social correspondente.

Em um certificado de equipamento ou aplicação, o identificador CN contém o URL correspondente ou o nome da aplicação, e não contém o campo E.

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

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
"	22
#	23
'	27
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D

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

O OID desta PC é: 2.16.76.1.2.1.15.

Todo certificado emitido segundo essa PC, PC A1 AC PRODEMGE, 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

([http://icp-brasil.certisign.com.br/repositorio/dpc/AC\\_PRODEMGE/DPC\\_AC\\_PRODEMGE.pdf](http://icp-brasil.certisign.com.br/repositorio/dpc/AC_PRODEMGE/DPC_AC_PRODEMGE.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 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 e sua criticidade.

7.2.2.2. As LCR da AC PRODEMGE 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;
- b) **CRL Number**, não crítica: contém um número seqüencial para cada LCR emitida pela AC PRODEMGE;
- c) **Authority Information Access**, não crítica: contém o endereço de acesso aos certificados da cadeia de certificação através do link: [http://icp-brasil.certisign.com.br/repositorio/certificados/AC PRODEMGE G3.p7c](http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G3.p7c).

## 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. A aprovação e conseqüente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

### 8.2. Políticas de publicação e notificação

A AC PRODEMGE mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web: ([http://icp-brasil.certisign.com.br/repositorio/pc/AC PRODEMGE/PC A1 AC PRODEMGE v5.1.pdf](http://icp-brasil.certisign.com.br/repositorio/pc/AC_PRODEMGE/PC_A1_AC_PRODEMGE_v5.1.pdf)).

### 8.3. Procedimentos de aprovação

Esta PC da AC PRODEMGE foi submetida à aprovação, durante o processo de credenciamento da AC PRODEMGE, 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
[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 DA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01