AUTORIDADE CERTIFICADORA
prodemge
Tecnologia de Minas Gerais

ICP Brasil

Política de Certificado de Sigilo Tipo S3

da Autoridade Certificadora PRODEMGE

PC S3 da AC PRODEMGE

Versão 5.3 - 30/09/2016

ÍNDICE

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
5.2	**02/12/2015**	**Resolução 115, de 11.11.2015 (Versão 6.0)**	1.1.3, 1.1.7, 1.3.5.7, 6.1.1.1.1, 6.2.4.1, 7.1.2.3 e 7.1.2.8	Referência aos parágrafos referentes à Política de Certificado A CF-e-SAT
5.3	**30/09/2016**	**Resolução 116, de 09 de dezembro de 2015**	6.1.5.1, 7.1.3, 7.1.2.2	Referencia à autoridade certificadora Raiz V5 e suas cadeias subsequentes
		Resolução 118, de 09 de dezembro de 2015	7.1.2.2, 7.2.2.2	Aprova a retirada do campo AIA da LCR e define a obrigatoriedade de dois pontos de obtenção da LCR em novas cadeias de certificação digital ICP-Brasil
		Instrução Normativa 07, de 15 de julho de 2016	7.1.2.2, 7.1.2.3,9.2	Adequações exigidas pelo DOC-ICP-01.02: exclusão à referencia a certificados de equipamento e indicação de uso da AC para emissão de certificados de Assinatura Geral e Proteção de e-mail (S/MIME).

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 S3 da Autoridade Certificadora PRODEMGE na Infraestrutura de Chaves Públicas Brasileira.

1.1.2. 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 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 sigilo Tipo S3 da Autoridade Certificadora PRODEMGE" e referida como "PC S3 da AC PRODEMGE". Esta PC descreve os usos relacionados ao certificado de sigilo correspondente ao tipo S3 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.103.5.

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://wwws.prodemge.gov.br/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, 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. Não se aplica.

1.3.5.5. Os certificados emitidos pela AC PRODEMGE no âmbito desta PC podem ser utilizados apenas para aplicações de sigilo como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

1.3.5.6. Não se aplica.

1.3.5.7. 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
Nome:	Jacira dos Reis Xavier
Telefone:	(31) 3339-1245
Fax:	(31) 3339-1319
E-mail:	gor@prodemge.gov.br / goc@prodemge.gov.br

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**

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 CSP (Cryptographic Service Provider) existente na estação do solicitante apresentados pelo browser .

A geração do par de chaves criptográficas ocorre utilizando cartão inteligente ou token ambos com capacidade de geração de chave protegidos por senha.

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 deverão ser armazenadas em cartão inteligente ou token, ambos com capacidade de geração de chave, sendo ativados e protegidos por senha e/ou identificação biométrica.

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 é única e seu sigilo é suficientemente assegurado;

b) A chave privada 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 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 S3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
S3	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou hardware criptográfico homologado junto à ICP-Brasil.

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 seus(s) representante(s) legal(s), conforme especificado no Termo de Responsabilidade, no caso de certificados de pessoa jurídica 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 (para cadeia V2) e http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G4.p7c (para cadeia V5).

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 a hierarquia V1 e de 2048 bits para a hierarquia V2 e V5.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo S3 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 S3 desta PC, é realizada por hardware criptográfico aprovado pelo CG da ICP-Brasil.

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

Os certificados têm ativados os bits keyEncipherment e dataEncipherment.

6.2. Proteção da Chave Privada

6.2.1.Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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, isto é, não se permite que terceiros possam obter uma chave privada de sigilo 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 não mantém cópia de segurança de chave privada de titular de certificado de sigilo 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 sigilo 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

Não se aplica.

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 sigilo emitidos pela AC PRODEMGE permanecem armazenadas após a expiração dos correspondentes certificados, permanentemente, na forma da legislação em vigor .

6.3.2.Períodos de uso para as chaves pública e privada

6.3.2.1. Não se aplica.

6.3.2.2. As chaves privadas de sigilo 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 encriptações geradas durante o prazo de validade dos respectivos certificados.

6.3.2.3. O período máximo de validade admitido para certificados de sigilo Tipo S3 da AC PRODEMGE é de 5 (cinco) anos.

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 dos titulares de certificados possui conexão com o dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves.

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 os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. 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.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC PRODEMGE provêem 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

O módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado está em conformidade com o padrão de segurança FIPS 140-1 nível 2 (para a cadeia de certificação V0); ou FIPS 140-2 nível 2 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para a cadeia de certificação V1); ou FIPS 140-2 nível 3 (para cadeia de certificação V2) e no padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), utilizando o algoritmo RSA.

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 keyEncipherment e dataEncipherment estão ativados;

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

- O OID desta PC: 2.16.76.1.2.103.5;

- 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;

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/ACPRODEMGEG2/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGEG2/LatestCRL.crl

http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACPRODEMGEG2/LatestCRL.crl

Para certificados emitidos na G3:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGEG3/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGEG3/LatestCRL.crl

http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACPRODEMGEG3/LatestCRL.crl

Para certificados emitidos na G4:

http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGEG4/LatestCRL.crl

http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGEG4/LatestCRL.crl

e) **Authority Information Access**, não crítica: contém o endereço de acesso aos certificados da cadeia de certificação através do link:

Para certificados emitidos na G3:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G3.p7c

Para certificados emitidos na G4:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G4.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 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

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

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 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.

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 Titulo 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, 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 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 os demais certificados de Assinatura e/ou Proteção de e-mail: os propósitos "client authentication" (OID 1.3.6.1.5.5.7.3.2) e "E-mail protection" (OID 1.3.6.1.5.5.7.3.4) estão ativados.

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) na hierarquia 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 e 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:

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

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 aplicação, o identificador CN contém o 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 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 2.16.76.1.2.103.5.

Todo certificado emitido segundo essa PC, PC S3 AC PRODEMGE, contem 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).

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 criticalidade.

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 sequencial para cada LCR emitida pela AC PRODEMGE.

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 consequente 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_S3_AC_PRODEMGE_v5.3.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
[4]	REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS	DOC-ICP-01.02