Política de Certificação
da
Autoridade Certificadora
PRODERJ

Certificados A3

(PC AC PRODERJ A3)

Versão 3.3 de Janeiro de 2019

GOVERNO DO
Rio de Janeiro

SUMÁRIO

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
ACT – Autoridade de Carimbo do Tempo
AR - Autoridades de Registro
CEI - Cadastro Específico do INSS
CF-e – Cupom Fiscal Eletrônico
CG - Comitê Gestor
CMM-SEI - *Capability Maturity Model* do *Software Engineering Institute*
CMVP - *Cryptographic Module Validation Program*
CN - Common Name
CNE - Carteira Nacional de Estrangeiro
COBIT - *Control Objectives for Information and related Technology*
COSO - *Comitee of Sponsoring Organizations*
CPF - Cadastro de Pessoas Físicas
DMZ - Zona Desmilitarizada
DN - *Distinguished Name*
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira
IDS - Sistemas de Detecção de Intrusão
IEC - *International Electrotechnical Commission*
ISO – *International Organization for Standardization*
ITSEC - *European Information Technology Security Evaluation Criteria*
ITU - *International Telecommunications Union*
LCR - Lista de Certificados Revogados
NBR - Norma Brasileira
NIS - Número de Identificação Social
NIST - *National Institute of Standards and Technology*
OCSP - *On-line Certificate Status Protocol*
OID - *Object Identifier*
OU - *Organization Unit*
PASEP - Programa de Formação do Patrimônio do Servidor Público
PC - Políticas de Certificado
PCN - Plano de Continuidade de Negócio
PIS - Programa de Integração Social
POP - *Proof of Possession*
PS – Política de Segurança
PRODERJ – Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro
PSS - Prestadores de Serviço de Suporte
RFC – *Request For Comments*
RG - Registro Geral
SAT – Sistema de Autenticação e Transmissão
SNMP - *Simple Network Management Protocol*
TCSEC - *Trusted System Evaluation Criteria*
TSDM - *Trusted Software Development Methodology*
UF - Unidade de Federação
URL - Uniform Resource Location

1. INTRODUÇÃO

1.1. VISÃO GERAL

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

1.1.2 A PC AC PRODERJ A3 elaborada no âmbito da ICP-Brasil adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04).

1.1.3 O tipo de certificado emitido sob esta PC é o Tipo A3.

1.1.4 Os tipos de certificados de A1 a A4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

1.1.5 Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6 Item não aplicável.

1.1.7 Item não aplicável

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

1.2. IDENTIFICAÇÃO

1.2.1 Esta PC obedece às recomendações da ICP-Brasil para a emissão de certificados de assinatura do tipo A3.

1.2.2 Após o processo de credenciamento do AC PRODERJ foi atribuído a esta Política de Certificação no âmbito da ICP-Brasil o seguinte OID:

TIPO DE CERTIFICADO	OID
A3	2.16.76.1.2.3.29

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. Autoridades Certificadoras

1.3.1.1 A Autoridade Certificadora do PRODERJ (AC PRODERJ) integra a Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora do SERPRO (ACSERPRO) e da Autoridade Certificadora Raiz Brasileira.

1.3.1.2 Esta PC segue a Declaração de Práticas de Certificação (DPC) da AC PPRODERJ, onde estão descritas suas práticas e procedimentos de certificação.

1.3.2. Autoridades de Registro

1.3.2.1 A AC PRODERJ mantém página web (**https://certificados.serpro.gov.br/acproderj)** onde estão publicados os seguintes dados; referentes às Autoridade de Registro – AR utilizadas pela AC PRODERJ para os processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

a) relação de todas as AR credenciadas, com informações sobre as PC que implementam;

b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;

d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;

f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC PRODERJ mantém as informações acima sempre atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A AC PRODERJ utiliza o Serviço Federal de Processamento de Dados(SERPRO) como PSS com endereço identificado na URL https://certificados.serpro.gov.br/acproderj

1.3.3.2PSS são entidades utilizadas pela AC ou pela AR para desempenhar as atividades descritas abaixo:

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 PRODERJ mantém as informações acima atualizadas.

1.3.3A Prestadores de Serviço de Confiança

1.3.3A.1 Não se aplica.

1.3.3A.2. Os Prestadores de Serviço de Confiança podem ser entidades utilizadas pela AC PPRODERJ, ou a própria AC, nesta PC se classificam em três categorias, conforme o tipo de atividade prestada:

a) armazenamento de chaves privadas dos usuários finais; ou
b) serviço de assinatura digital, verificação da assinatura digital; ou
c) ambos.

1.3.4. Titulares de Certificado

Os Titulares de Certificados desta PC ac PRODERJ A3 são Pessoas Físicas e Pessoas Jurídicas autorizadas pela AR vinculada a receber um certificado digital emitido pela AC PRODERJ, para sua própria utilização.
Em sendo o Titular do Certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.5. Aplicabilidade

1.3.5.1 Esses certificados se destinam exclusivamente à utilização em assinatura digital, não repúdio, garantia de integridade de informação e autenticação de seu titular.

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

1.3.5.3 Os certificados emitidos sob esta PC pela AC PRODERJ são apropriados ao uso apenas nas aplicações apresentadas na tabela descrita a seguir.

Política de Certificado	**Aplicações Apropriadas**
PC AC PRODERJ A3	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas seguintes aplicações; • Confirmação de Identidade na web; • Correio eletrônico; • Transações On-Line; • Redes privadas virtuais (VPN); • Transações eletrônicas; • Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.4 Certificados de tipo A3 são 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

Esta PC é administrada pelo PRODERJ, localizado no seguinte endereço:

Rua da Glória, 178 -11° andar

Bairro: Glória
CEP. 20.241-180
Rio de Janeiro – RJ.

Pessoas de Contato.

Raphael Carvalho Monetto
Tel: (21) 2333-0300

E-mail de Contato.

asi@proderj.rj.gov.br

2. DISPOSIÇÕES GERAIS

Os itens seguintes estão descritos na DPC PRODERJ.

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

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

Os itens seguintes estão descritos na DPC PRODERJ.

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. Freqüência 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*

5.3.3. Requisitos de treinamento

5.3.4. Freqüência e requisitos para reciclagem técnica

5.3.5. Freqüência e seqüência de rodízio de cargos

5.3.6. Sanções para ações não autorizadas

5.3.7. Requisitos para contratação de pessoal

5.3.8. Documentação fornecida ao pessoal

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC AC PRODERJ A3.

São definidos também outros controles técnicos de segurança utilizados pela AC PRODERJ e pelas AR vinculadas na execução de suas funções operacionais.

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1. Geração do par de chaves

6.1.1.1 Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is) a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1 Item não aplicável

6.1.1.2 O par de chaves criptográficas é gerado pelo Titular do Certificado, utilizando para isto a mídia inteligente autorizada pelo PRODERJ, com capacidade de geração de chave e protegida por senha (token ou Smart Card), na qual será armazenado o certificado

O Titular do certificado deverá acessar a página web do PRODERJ, escolher a opção de “solicitação de certificado” e preencher os dados solicitados, após o preenchimento o Titular deverá selecionar a mídia para a geração do par de chaves.

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 da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL[1], no meio de armazenamento definido para cada tipo de certificado A3 previsto pela ICP-Brasil.

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

a) a chave privada é única e seu sigilo é suficientemente assegurado;

b) a chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica
A3	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

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC PRODERJ por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC PRODERJ.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4. Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC PRODERJ, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1];
b) Página *web* da AC PRODERJ (**https://certificados.serpro.gov.br/acproderj**);
c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Os tamanhos das chaves criptográficas associadas aos certificados emitidos pela AC PRODERJ são os seguintes:

6.1.5.1.1. Para os certificados emitidos pela v2 e **v3** o tamanho das chaves criptográficas é de, no mínimo, 2048 (dois mil e quarenta e oito) bits;

6.1.5.1.2. Para os certificados emitidos pela AC PRODERJ o tamanho das chaves criptográficas é de 1024 (mil e vinte e quatro) bits.

NOTA: O tamanho de 1024 bits será utilizado somente até o dia 31/12/2011.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos Titulares de certificado adotam no mínimo, o padrão FIPS 140-1 ou equivalente estabelecido pelo CG da ICP-Brasil.

6.1.7 Verificação da qualidade dos parâmetros

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

6.1.8 Geração de chave por *hardware ou software*

O processo de geração do par de chaves dos Titulares do Certificado é feito por hardware criptográfico autorizado pelo PRODERJ.

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

Os certificados emitidos nesta PC tem ativado os bits digitalSignature, nonRepudiation e keyEncipherment.

6.2. Proteção da Chave Privada

Neste item são definidos os requisitos de proteção das chaves privadas de certificados emitidos, segundo a PC PRODERJ.

6.2.1. Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que, os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1], são observados para geração das chaves criptográficas.

6.2.2. Controle "n de m" para chave privada

Item não aplicável.

6.2.3. Custódia (*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 legalmente obter uma chave privada sem o

consentimento de seu titular.

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

6.2.4.1 A mídia utilizada para a geração e armazenamento das chaves criptográficas não permitem, manter cópia de segurança.

6.2.4.2 A AC PRODERJ responsável pela PC não mantém cópia de segurança de chave privada de titular.

6.2.4.3 Não se aplica.

6.2.4.4 Não se aplica.

6.2.5 Arquivamento de chave privada

6.2.5.1 Item não aplicável, uma vez que a ICP-Brasil não admite o arquivamento de chaves privadas de Assinatura Digital.

6.2.5.2 Defini-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

O Item não aplicável uma vez que a chave é gerada dentro do próprio módulo.

6.2.7. Método de ativação de chave privada

A chave privada é ativada mediante senha solicitada pelo CSP (*Cryptographic Service Provider*) existente nas estações. A senha deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo.

Os Titulares de Certificados devem alterar suas senhas a qualquer momento, sendo recomendável que o façam no mínimo a cada 3 meses.

6.2.8. Método de desativação de chave privada

A desativação da chave privada ocorre na retirada do dispositivo de armazenamento da chave da leitora ou da porta USB e fechando a sessão do Browser.

6.2.9 Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado deve ser feita através de software disponibilizado pelo fabricante da mídia, que permite apagar todas as informações nela contida, utilizando para isso a senha de acesso do titular do certificado à mídia armazenadora.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública

A AC PRODERJ prevê que as chaves públicas de titulares dos certificados de assinatura

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

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas dos respectivos Titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

6.3.2.3 Certificados do tipo A3 previstos nesta PC tem validade de até 5 anos.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Item não aplicável.

6.4.2 Proteção dos dados de ativação

Item não aplicável.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

Os equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados devem dispor de mecanismos mínimos que garantam a segurança computacional, como, proteção do equipamento com Senha, instalação do CSP correspondente ao cartão criptográfico.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6. Controles Técnicos do Ciclo de Vida

Item não aplicável.

6.6.1. Controles de desenvolvimento de sistema

Item não aplicável.

6.6.2 Controles de gerenciamento de segurança

Item não aplicável.

6.6.3 Classificações de segurança de ciclo de vida

Item não aplicável.

6.7. Controles de Segurança de Rede

Item não aplicável.

6.8 Controles de Engenharia do Módulo Criptográfico

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (*Federal Information Processing Standards*) 140-1 – requerido pelo PRODERJ para os certificados emitidos sob esta PC.

Poderão ser indicados padrões de referência, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

7. PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCR gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC PRODERJ, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão

Todos os certificados emitidos pela AC PRODERJ, segundo esta PC, implementam a versão 3 de certificado definida no 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 e sua criticalidade.

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

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

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

c) **"*Certificate Policies*", não crítica:** o campo ***policyIdentifier*** contém o OID 2.16.76.1.2.3.29 desta PC e o campo ***policyQualifiers*** contém o endereço *URL* da página *Web* **http://repositorio.serpro.gov.br/docs/dpcacproderj.pdf**

d) da AC PRODERJ com a DPC da AC PRODERJ;

e) **"CRL Distribution Points", não crítica**: contém o endereço URL da página Web onde se obtém a LCR da AC PRODERJ:

- Para os certificados emitidos pela AC PRODERJ v3:

http://repositorio.serpro.gov.br/lcr/acproderjv3.crl
http://certificados2.serpro.gov.br/lcr/acproderjv3.crl

- Para os certificados emitidos pela AC PRODERJ v2: http://ccd.serpro.gov.br/lcr/acproderjv2.crl, http://ccd2.serpro.gov.br/lcr/acproderjv2.crl e http://www.iti.gov.br/serpro/acproderjv2.crl; e
- Para os certificados emitidos pela AC PRODERJ v1: http://ccd.serpro.gov.br/lcr/acproderj.crl.

f) **"*Authority Information Access*", não critica**, contendo o método de acesso **id-ad-caIssuer**, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação no seguinte endereço:

- Para certificados emitidos pela AC PRODERJ v3:
http://repositorio.serpro.gov.br/cadeias/acproderjv3.p7b

- Para os certificados emitidos pela AC PRODERJ v2: http://ccd.serpro.gov.br/cadeias/acproderjv2.p7b
- OID=1.3.6.1.5.5.7.1.1.

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

a) Para **certificado de pessoa física:**
Três campos otherName, obrigatórios, contendo:

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 UF.

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

do certificado.

iii. **OID = 2.16.76.1.3.5 e conteúdo** = nas primeiras 12 (onze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subseqüentes,a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subseqüentes, o município e a UF do Título de Eleitor.

b) Para certificado de pessoa jurídica:
Quatro campos otherName, obrigatórios, contendo:

i. OID =2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11(onze) posições subseqüentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 10 (dez) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;
ii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;
iii. OID =2.16.76.1.3.3 e conteúdo = 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 Especifico do INSS (CEI) da pessoa jurídica titular do certificado.

7.1.2.4. Os campos “Other Name” definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

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

b) O preenchimento dos campos CPF e Data de Nascimento é obrigatório;

c) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

d) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;

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

f) Todas informações de tamanho variável referente a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

g)As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

h)Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

7.1.2.5. Campos "OtherName" adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

7.1.2.6. A AC PRODERJ implementa as seguintes extensões, definidas como opcional pela ICP-Brasil:

a) "***SubjectAlternativeName***", **não critica**, com o seguinte OtherName:
Certificados de Pessoa Fisica e Pessoa Jurídica:

- O campo "*rfc822Name*" contendo o endereço de email do titular do certificado.
- Campo "autenticação" OID = 1.3.6.1.4.1.311.20.2.3, que contém o domínio de login em estações de trabalho (UDN).

b) "***Extended-key-usage***", **não critica**, contendo os seguintes valores;
Certificados de Pessoa Fisica e Pessoa Jurídica:

- "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);

Certificados Pessoa Física, inclui-se:

- "SmartCardLogon" (OID = 1.3.6.1.4.1.311.20.2.2);

7.1.2.7. Não se aplica.

7.1.3 Identificadores de algoritmo

7.1.3.1.1 Os certificados emitidos pela AC PRODERJ v2 e v3 são assinados com o uso do algoritmo criptográfico SHA-256 com função de hash (OID = 1.2.840.113549.1.1.11).
7.1.3.1.2 Os certificados emitidos pela AC PRODERJ v2 são assinados com o uso do algoritmo criptográfico SHA-1 com função de hash (OID = 1.2.840.113549.1.1.5).

NOTA: O padrão SHA-1 com RSA será utilizado somente até o dia 31/12/2011.

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, para os certificados Pessoa Física:

C = BR
O = ICP-Brasil
OU = Autoridade Certificadora AC PRODERJ
OU = Nome da AR responsável pela aprovação do certificado
OU = CNPJ da AR onde ocorreu a identificação presencial
OU = Pessoa Fisica A3
OU = <*Órgão de lotação*>
CN = <N*ome do titular do certificado*> *<:>*<#######>

No formato acima, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres "<" e ">" não devem ser incluídos.

Os caracteres "#" representam os 7 dígitos da matrícula funcional do titular. Todos os outros caracteres devem ser interpretados literalmente;

Os últimos sete caracteres do campo CN (Common Name) devem ser o número de matrícula do titular no órgão de lotação, completado com caracteres brancos à direita, caso possua tamanho menor do que 7 caracteres;

O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.

No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite do tamanho do campo disponível, vedada a abreviatura.

Para os certificados de Pessoa Jurídica, o nome empresarial 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 = Autoridade Certificadora AC PRODERJ
OU = CNPJ da AR onde ocorreu a identificação presencial
OU = Nome da AR responsável pela aprovação do certificado
OU = Pessoa Juridica A3
L = Cidade
S = Estado (UF)
CN = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica)

7.1.5. Restrições de nome

7.1.5.1. Não se aplica.

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

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

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

Tabela 3 - Caracteres especiais admitidos em nomes

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

O OID atribuído à esta Política de Certificado é: 2.16.76.1.2.3.29.

7.1.7 Uso da extensão *"Policy Constraints"*

Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo **policyQualifiers** da extensão "*Certificate Policies*" contém o endereço da página *Web* (URL) com a DPC da AC PRODERJ.

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 de versão

As LCR geradas pela AC PRODERJ segundo a PC, implementam a versão 2 de LCR definida no 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 A AC PRODERJ adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) **"*Authority Key Identifier*", não crítica**: contém o *hash* SHA-1 da chave pública da AC PRODERJ;
b) **"*CRL Number*", não crítica:** contém número seqüencial para cada LCR emitida.
c) **"*Authority Information Access"*, não crítica:** contendo o endereço Web onde se obtêm o arquivo p7b com os certificados da cadeia da AC PRODERJ, a saber;

- AC PRODERJ
  - http://ccd.serpro.gov.br/cadeias/acproderj.p7b
- AC PRODERJ v2
  - http://ccd.serpro.gov.br/cadeias/acproderjv2.p7b
- AC PRODERJ v3
  - **http://repositorio.serpro.gov.br/cadeias/acproderjv3.p7b**

`

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes definem como é mantida e administrada a PC.

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

As alterações nas especificações desta PC são realizadas pelA AC PRODERJ. Quaisquer modificações são submetidas à aprovação da ACSERPRO que as submeterá ao CG da ICP-Brasil.

8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

A cada nova versão, esta PC é publicada na página web da AC PRODERJ

8.3 PROCEDIMENTOS DE APROVAÇÃO

Esta PC foi submetida à aprovação da AC PRODERJ, que por sua vez submeteu ao CG da

ICP-Brasil, durante o processo de credenciamento da AC PRODERJ, conforme o estabelecido no documento "Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil". Como parte desse processo, além da conformidade com os documentos definidos pela ICP-Brasil, foi verificada a compatibilidade entre esta PC e a DPC da AC PRODERJ.

9. DOCUMENTOS REFERENCIADOS

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

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

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

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.0