

	Tipo de Documento:	Código:
	<b>PROCEDIMENTO</b>	<b>NPS-DIREX-006</b>

Título do Documento:		Homologação:
NORMA DE CERTIFICAÇÃO DIGITAL – PC AC PRODEST RFB A1		
Número total de página 17	Vigorar a partir de: 21/10/2011	Revisão atual: Versão: 2.0

## 1. INTRODUÇÃO

### 1.1 Visão Geral

1.1.1 O documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras - AC integrantes da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2 Esta Política de Certificado de Assinatura Digital tipo A1 da AC PRODEST RFB (a seguir designada simplesmente por "PC AC PRODEST RFB A1") adota a mesma estrutura empregada neste documento.

1.1.3. O tipo de certificado emitido sob esta PC é o Tipo A1.

1.1.4. Não se aplica.

1.1.5. Esta PC refere-se exclusivamente a Certificados de Pessoa Física, de Pessoa Jurídica, de Equipamento Servidor e Assinatura de Código Tipo A1 emitidos pela AC PRODEST RFB (a seguir designada simplesmente por "AC PRODEST RFB").

1.1.6. Não se aplica.

1.1.7. Não se aplica.

### 1.2 Identificação

1.2.1. A PC AC PRODEST RFB A1 descreve os procedimentos e práticas da AC PRODEST RFB e os usos relacionados ao Certificado de Assinatura Digital Tipo A1.

1.2.2. O OID (Object Identifier) da PC AC PRODEST RFB A1 é 2.16.76.1.2.1.35.

### 1.3 Comunidade e Aplicabilidade

#### 1.3.1 Autoridade Certificadora (AC)

##### 1.3.1.1. Dados da Autoridade Certificadora

Esta PC se refere à AC PRODEST RFB (PRODEST - INSTITUTO DE TECNOLOGIA DA INFORMACAO E COMUNICACAO DO ESTADO DO ESPIRITO SANTO, com sede na Avenida João Batista Parra, 465 , Praia do Suá, Vitória, ES, CEP: 29050-925, CNPJ: 28.162.790/0001-20).

As práticas e procedimentos de certificação da AC PRODEST RFB estão descritos na Declaração de Práticas de Certificação da AC PRODEST RFB (a seguir designada simplesmente por "DPC-AC PRODEST RFB").

##### 1.3.1.2. Atualização de Dados

A AC PRODEST RFB mantém as informações acima sempre atualizadas.

#### 1.3.2 Autoridade de Registro (AR)

##### 1.3.2.1. Dados das Autoridades Registradoras

Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência das Autoridades de Registro. As Autoridades de Registro vinculadas à AC PRODEST RFB (AR Vinculadas) estão relacionados na página <http://loja.certificadodigital.com.br/prodest/Autoridades>.

A página <http://loja.certificadodigital.com.br/prodest/Autoridades> contém:

- relação de todas as AR credenciadas, com informações sobre as PC que implementam;
- para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

	<p>Tipo de Documento:</p> <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	<p>Código:</p> <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

- 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 respectivas datas do descredenciamento;
- e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectivas datas 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. Atualização de Dados

A AC PRODEST RFB mantém as informações acima sempre atualizadas.

### 1.3.3 Prestador de Serviços de Suporte

#### 1.3.3.1. Dados das PSS

Os Prestadores de Serviços de Suporte vinculados à AC PRODEST RFB estão relacionados na página <http://loja.certificadodigital.com.br/prodest/PSS>.

#### 1.3.3.2. PSS

PSS são entidades utilizados pela AC PRODEST RFB ou pelas AR Vinculadas para desempenhar atividade descrita nesta PC e se classificam em três categorias, conforme o tipo de atividade prestada:

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

#### 1.3.3.3. Atualização de Dados

A AC PRODEST RFB mantém as informações acima sempre atualizadas.

### 1.3.4 Titulares de Certificado

Os Titulares de Certificado de Assinatura Digital tipo A1 da AC PRODEST RFB podem ser pessoas físicas ou jurídicas, observados os itens 1.3.4, 3.1.9, 3.1.10 e 3.1.11 da DPC-AC PRODEST RFB.

### 1.3.5 Aplicabilidade

1.3.5.1. Os certificados definidos por esta PC têm sua utilização vinculada à assinatura digital, assinatura de código de software, não repúdio, garantia de integridade da informação, autenticação de seu Titular e de aplicações e identificação de equipamentos.

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

1.3.5.3. Na definição das aplicações para o certificado definido pela PC, a AC PRODEST RFB leva em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado.

1.3.5.4. Não se aplica.

1.3.5.5. Não se aplica.

1.3.5.6. Não se aplica.

1.3.5.7. Os certificados emitidos sob esta PC AC PRODEST RFB A1 são apropriados ao uso, por exemplo, nas aplicações apresentadas abaixo:

- Assinatura digital em correio eletrônico;
- Assinatura de código de software;
- Acesso a aplicações disponibilizadas pela Receita Federal do Brasil, ou por qualquer outro órgão da Administração Pública Direta ou Indireta, que aceitem este certificado;
- Software de assinatura elaborado em parceria com outros órgãos, entidades ou empresas;
- Confirmação de identidade na Web;

	Tipo de Documento:  <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	Código:  <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

- Transações eletrônicas e transações on-line;
- Redes privadas virtuais (VPN);
- Cifração de chaves de sessão.

#### 1.4 Dados de Contato

Dúvidas decorrentes da leitura desta PC e que não sejam respondidas mediante a leitura da página <http://loja.certificadodigital.com.br/prodest/ProdestRFB> podem ser esclarecidas contatando:

PRODEST - INSTITUTO DE TECNOLOGIA DA INFORMACAO E COMUNICACAO DO ESTADO DO ESPIRITO SANTO

Avenida João Batista Parra, 465

CEP: 29050-925

Praia do Suá, Vitória, ES,

Telefones: (55 27) 3636-7220

Fax: (55 27) 3636- 7155

Pessoa para contato: Helton Lopes de Moraes (e-mail: [helton.moraes@prodest.es.gov.br](mailto:helton.moraes@prodest.es.gov.br))

## 2. DISPOSIÇÕES GERAIS

Os itens seguintes estão referidos nos correspondentes itens DPC-AC PRODEST RFB.

### 2.1. Obrigações e direitos

- 2.1.1. Obrigações da AC
- 2.1.2. Obrigações das AR
- 2.1.3. Obrigações do Titular do Certificado
- 2.1.4. Direitos da terceira parte (*Relying Party*)
- 2.1.5. Obrigações do Repositório

### 2.2. Responsabilidades

- 2.2.1. Responsabilidades da AC
- 2.2.2. Responsabilidades das AR vinculadas

### 2.3. Responsabilidade Financeira

- 2.3.1. Indenizações devidas pela terceira parte (*Relying Party*)
- 2.3.2. Relações Fiduciárias
- 2.3.3. Processos Administrativos

### 2.4. Interpretação e Execução

- 2.4.1. Legislação
- 2.4.2. Forma de interpretação e notificação
- 2.4.3. Procedimentos de solução de disputa

### 2.5. Tarifas de Serviço

- 2.5.1. Tarifas de emissão e renovação de certificados
- 2.5.2. Tarifas de acesso a certificados
- 2.5.3. Tarifas de revogação ou de acesso à informação de status
- 2.5.4. Tarifas para outros serviços
- 2.5.5. Política de reembolso

### 2.6. Publicação e Repositório

- 2.6.1. Publicação de informação da AC
- 2.6.2. Frequência de publicação
- 2.6.3. Controles de acesso
- 2.6.4. Repositórios

### 2.7. Fiscalização e Auditoria de Conformidade

#### 2.8. Sigilo

- 2.8.1. Tipos de informações sigilosas
- 2.8.2. Tipos de informações não sigilosas
- 2.8.3. Divulgação de informação de revogação e de suspensão de certificado
- 2.8.4. Quebra de sigilo por motivos legais

	<p>Tipo de Documento:</p> <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	<p>Código:</p> <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

- 2.8.5. Informações a terceiros
- 2.8.6. Divulgação por solicitação do titular
- 2.8.7. Outras circunstâncias de divulgação de informação

2.9. Direitos de Propriedade Intelectual

### **3. IDENTIFICAÇÃO E AUTENTICAÇÃO**

Os itens seguintes estão referidos nos correspondentes itens da DPC-AC PRODEST RFB.

- 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**

Os itens seguintes estão referidos nos correspondentes itens da DPC-AC PRODEST RFB.

- 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*)

	Tipo de Documento:  <h2 style="text-align: center;">PROCEDIMENTO</h2>	Código:  <h3 style="text-align: center;">NPS-DIREX-006</h3>
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------	-------------------------------------------------------------------

- 4.5.3. Período de retenção para registros (*logs*) de auditoria
- 4.5.4. Proteção de registro (*log*) de auditoria
- 4.5.5. Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria
- 4.5.6. Sistema de coleta de dados de auditoria
- 4.5.7. Notificação de agentes causadores de eventos
- 4.5.8. Avaliações de vulnerabilidade

#### 4.6. Arquivamento de Registros

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

#### 4.7. Troca de chave

#### 4.8. Comprometimento e Recuperação de Desastre

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

#### 4.9. Extinção dos serviços de AC, AR ou PSS

## 5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os itens seguintes estão referidos nos correspondentes itens da DPC-AC PRODEST RFB.

#### 5.1. Controles Físicos

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

#### 5.2. Controles Procedimentais

- 5.2.1. Perfis qualificados
- 5.2.2. Número de pessoas necessário por tarefa
- 5.2.3. Identificação e autenticação para cada perfil

#### 5.3. Controles de Pessoal

- 5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade
- 5.3.2. Procedimentos de verificação de antecedentes
- 5.3.3. Requisitos de treinamento
- 5.3.4. Frequência e requisitos para reciclagem técnica
- 5.3.5. Frequência e seqüência de rodízio de cargos
- 5.3.6. Sanções para ações não autorizadas
- 5.3.7. Requisitos para contratação de pessoal
- 5.3.8. Documentação fornecida ao pessoal

## 6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC.

	Tipo de Documento:  <h2 style="text-align: center;">PROCEDIMENTO</h2>	Código:  <h3 style="text-align: center;">NPS-DIREX-006</h3>
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------	-------------------------------------------------------------------

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

#### 6.1. Geração e Instalação do Par de Chaves

Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, publicando nova versão do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

##### 6.1.1. Geração do par de chaves

6.1.1.1. Quando o titular de certificado é uma pessoa física, esta é a responsável pela geração dos pares de chaves criptográficas.

Quando o titular de certificado é uma pessoa jurídica, esta indica 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. O processo de geração de chaves do tipo A1, contemplada nesta PC, exige:

- a) a instalação de software relacionado ao repositório armazenador do certificado selecionado pelo cliente;
- b) o par de chaves será gerado em repositório protegido por senha e/ou identificação biométrica e cifrado por software;
- c) o responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado deve executar pessoalmente a geração dos pares de chaves criptográficas.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

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 ICP-BRASIL [3], em repositório protegido por senha e/ou identificação biométrica e cifrado por software.

6.1.1.5. A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e o repositório utilizado para o seu armazenamento.

6.1.1.6. O processo de geração do par de chaves 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 é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) a chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

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

A AC PRODEST RFB não acessa a chave privada da entidade titular do certificado. Assim, não se configura a entrega da chave privada à entidade titular.

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

A entidade titular do certificado, através de seu software de acionamento, disponibiliza para a entrega de sua chave pública à AC PRODEST RFB, à solicitante ou a correspondente AR vinculada, a chave pública em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3].

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

As formas para a disponibilização do certificado da AC PRODEST RFB, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

- a) Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- b) Diretório;
- c) Página Web da AC PRODEST RFB (<http://loja.certificadodigital.com.br/prodest/ProdestRFB>);

	Tipo de Documento:  <h2 style="text-align: center;">PROCEDIMENTO</h2>	Código:  <h3 style="text-align: center;">NPS-DIREX-006</h3>
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------	-------------------------------------------------------------------

d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil.

### 6.1.5. Tamanhos de chave

6.1.5.1. Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V2 o tamanho mínimo admitido para chaves criptográficas é de 2048 bits.

Para certificados emitidos sob as demais cadeias da Autoridade Certificadora Raiz Brasileira o tamanho mínimo admitido para chaves criptográficas é de 1024 bits.

6.1.5.2. Os algoritmos e os tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3].

### 6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas das entidades titulares de certificados adotarão o padrão FIPS 140-2.

### 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 das entidades titulares de certificados é feito em 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.

## 6.2. Proteção da Chave Privada

O repositório de armazenamento da chave privada 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 é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) a chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

### 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. Custódia (escrow) de chave privada

Não é permitido, no âmbito da ICP-Brasil, a custódia (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

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

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

6.2.4.2. A AC PRODEST RFB não pode manter cópia de segurança de chave privada de titular de certificado por ela emitido.

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3], como 3-DES, IDEA, SAFER+ e protegida com um nível de segurança não inferior àquele definido para a chave principal.

	<p>Tipo de Documento:</p> <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	<p>Código:</p> <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

6.2.4.4. Através das tecnologias atualmente disponíveis, a entidade titular de certificado deve realiza a geração de cópia de segurança da chave privada.

### **6.2.5. Arquivamento de chave privada**

6.2.5.1. As chaves privadas das entidades titulares de certificados emitidos por esta PC não são arquivadas.

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**

Cada entidade titular de certificado deve definir procedimentos necessários para a ativação da sua chave privada.

### **6.2.8. Método de desativação de chave privada**

Cada entidade titular de certificado deve definir procedimentos necessários para a desativação da sua chave privada.

### **6.2.9. Método de destruição de chave privada**

Cada entidade titular de certificado deve definir procedimentos necessários para a destruição da sua chave privada.

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

### **6.3.1. Arquivamento de chave pública**

As chaves públicas da AC PRODEST RFB, dos titulares de certificados de assinatura digital e as LCR por ela emitidas permanecem armazenadas 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 podem 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. O período máximo de uso das chaves correspondentes aos certificados emitidos pela PC AC PRODEST RFB A1 é de 1 (um) ano.

## **6.4. Dados de Ativação**

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

Os certificados de tipo A1 se utilizam, para armazenamento do par de chaves e certificado, de repositório protegido por senha e/ou identificação biométrica e cifrado por software.

No caso de ativação por senha, recomenda-se que as mesmas sejam criadas de forma aleatória, respeitando-se procedimentos básicos de segurança, tais como:

- a) nunca fornecer senha a terceiros;
- b) escolher senhas de 8 ou mais caracteres;
- c) definir senhas com caracteres numéricos e alfanuméricos;
- d) memorizar a senha e
- e) não escrevê-la.

	Tipo de Documento:  <h2 style="text-align: center;">PROCEDIMENTO</h2>	Código:  <h3 style="text-align: center;">NPS-DIREX-006</h3>
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------	-------------------------------------------------------------------

#### 6.4.2. Proteção dos dados de ativação

Para a proteção dos dados de ativação da chave privada da entidade titular do certificado, no caso de ativação por senha, recomenda-se:

- a) nunca fornecer senha a terceiros;
- b) escolher senhas de 8 ou mais caracteres;
- c) definir senhas com caracteres numéricos e alfanuméricos;
- d) memorizar a senha e
- e) não escrevê-la.

#### 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

Nos equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC PRODEST RFB, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

- a) senha de bios ativada;
- b) controle de acesso lógico ao sistema operacional;
- c) exigência de uso de senhas fortes;
- d) diretivas de senha e de bloqueio de conta;
- e) antivírus, antitrojan e antispysware, instalados, atualizados e habilitados;
- f) firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- g) sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
- h) proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

#### 6.5.2. Classificação da segurança computacional

Não se aplica.

### 6.6. Controles Técnicos do Ciclo de Vida

Os itens abaixo não se aplicam a esta PC.

#### 6.6.1. Controles de desenvolvimento de sistema

#### 6.6.2. Controles de gerenciamento de segurança

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

### 6.7. Controles de Segurança de Rede

Não se aplica.

### 6.8. Controles de Engenharia do Módulo Criptográfico

Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado devem obedecer aos padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3].

## 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. Os requisitos mínimos estabelecidos nos itens seguintes são atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

	<p>Tipo de Documento:</p> <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	<p>Código:</p> <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

### 7.1. Perfil do Certificado

Os certificados emitidos pela AC PRODEST RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

#### 7.1.1. Número(s) de versão

Os certificados emitidos pela AC PRODEST RFB implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

#### 7.1.2. Extensões de certificado

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

##### 7.1.2.2. Extensões Obrigatórias

7.1.2.2.1. Os certificados emitidos pela AC PRODEST RFB V2 obedecem a ICP-Brasil e ao anexo I da Portaria RFB/Cotec no. 061, de 04 de setembro de 2008, que definem como obrigatórias as seguintes extensões:

- a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC PRODEST RFB V2;
- b) "Key Usage", crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados; "Certificate Policies", não crítica: contém o OID desta PC e o endereço Web da DPC-AC PRODEST RFB V2 (<http://www.certificadodigital.com.br/repositorio/prodest/dpc>);
- c) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente: <http://www.certificadodigital.com.br/repositorio/lcr/PRODESTrfbv2.crl>, <http://lcr.certificados.com.br/repositorio/lcr/PRODESTrfbv2.crl> e <http://repositorio.icpbrasil.gov.br/lcr/PRODEST/repositorio/lcr/PRODESTrfbv2.crl>.
- d) "Authority Information Access", não crítica:
  - i. contendo endereço na Web onde se obtém o arquivo p7b com os certificados da cadeia: <http://www.certificadodigital.com.br/cadeias/PRODESTrfbv2.p7b>;
  - ii. contendo endereço na Web onde se acessa o serviço OCSP correspondente: <http://ocsp.certificadodigital.com.br/PRODESTrfbv2>.

7.1.2.2.2. Os certificados emitidos pela AC PRODEST RFB v1 obedecem a ICP-Brasil e ao anexo I da Portaria RFB/Cotec no. 061, de 04 de setembro de 2008, que definem como obrigatórias as seguintes extensões:

- a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC PRODEST RFB;
- b) "Key Usage", crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados; "Certificate Policies", não crítica: contém o OID desta PC e o endereço Web da DPC-AC PRODEST RFB (<http://www.certificadodigital.com.br/repositorio/prodest/dpc>);
- c) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente: <http://www.certificadodigital.com.br/repositorio/lcr/PRODESTrfbv1.crl>, <http://lcr.certificados.com.br/repositorio/lcr/PRODESTrfbv1.crl> e <http://repositorio.icpbrasil.gov.br/lcr/PRODEST/repositorio/lcr/PRODESTrfbv1.crl>.
- d) "Authority Information Access", não crítica:
  - iii. contendo endereço na Web onde se obtém o arquivo p7b com os certificados da cadeia: <http://www.certificadodigital.com.br/cadeias/PRODESTrfbv1.p7b>;
  - iv. contendo endereço na Web onde se acessa o serviço OCSP correspondente: <http://ocsp.certificadodigital.com.br/PRODESTrfbv1>.

##### 7.1.2.3. Subject Alternative Name

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

a) para Certificados de Pessoa Física (e-CPF)

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 da pessoa física titular do certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o número de inscrição no Cadastro de Pessoa Física (CPF) da pessoa física titular do certificado; nas 11 (onze) posições subseqüentes, o número de Identificação Social da pessoa física titular do certificado - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) da pessoa física titular do certificado; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.

	Tipo de Documento:  <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	Código:  <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

- ii. OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor da pessoa física titular do certificado; nas 3 (três) posições subseqüentes, o número correspondente a Zona Eleitoral; nas 4 (quatro) posições seguintes, o número correspondente a Seção; nas 22 (vinte e duas) posições subseqüentes, o nome do município e a UF do Título de Eleitor.
- iii. 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.

O preenchimento dos campos abaixo, referentes à pessoa física titular do certificado, é obrigatório:

- Nome;
- Número de inscrição no CPF;
- Data de nascimento;
- E-mail.

b) para Certificados de Pessoa Jurídica (e-CNPJ)

4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

- i. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pela Pessoa Jurídica, perante o CNPJ.
- ii. 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.
- iii. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pela Pessoa Jurídica perante o CNPJ, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o número de inscrição no Cadastro de Pessoa Física (CPF) do responsável pela Pessoa Jurídica perante o CNPJ; nas 11 (onze) posições subseqüentes, o Número de Inscrição Social - NIS (PIS, PASEP ou CI) do responsável pela Pessoa Jurídica perante o CNPJ; nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável pela Pessoa Jurídica perante o CNPJ; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.
- 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.

O preenchimento dos campos abaixo é obrigatório:

- Número de inscrição no CNPJ da Pessoa Jurídica titular do certificado;
- Nome empresarial da Pessoa Jurídica titular do certificado;
- Nome do responsável pela Pessoa Jurídica perante o CNPJ;
- Número de inscrição no CPF do responsável pela Pessoa Jurídica perante o CNPJ;
- Data de nascimento do responsável pela Pessoa Jurídica perante o CNPJ;
- E-mail do responsável pela Pessoa Jurídica perante o CNPJ.

c) para Certificados de Equipamento (e-Servidor)

4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

- i. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado.
- ii. 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.
- iii. 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 número de inscrição no Cadastro de Pessoa Física (CPF) do responsável pelo certificado; nas 11 (onze) posições subseqüentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI) do responsável pelo certificado; nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável pelo certificado; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.
- iv. OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado, sem abreviações.

O preenchimento dos campos abaixo é obrigatório:

- Número de inscrição no CNPJ da Pessoa Jurídica titular do certificado;
- Nome empresarial da Pessoa Jurídica titular do certificado;
- Nome DNS do servidor;
- Nome do responsável pelo certificado;
- Número de inscrição no CPF do responsável pelo certificado;
- Data de nascimento do responsável pelo certificado;
- E-mail do responsável pelo certificado.

	Tipo de Documento:  <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	Código:  <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

d) para Certificados de Assinatura de Código (e-Código)

4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

- i. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo Certificado.
- ii. 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.
- iii. 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 número de inscrição no Cadastro de Pessoa Física (CPF) do responsável pelo certificado; nas 11 (onze) posições subseqüentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI) do responsável pelo certificado; nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável pelo certificado; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.
- iv. OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado, sem abreviações.

O preenchimento dos campos abaixo é obrigatório:

- Número de inscrição no CNPJ da Pessoa Jurídica titular do certificado;
- Nome empresarial da Pessoa Jurídica titular do certificado;
- Nome do responsável pelo certificado;
- Número de inscrição no CPF do responsável pelo certificado;
- Data de nascimento do responsável pelo certificado;
- E-mail do responsável pelo certificado.

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

a) O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING, com exceção do campo PrincipalName cuja cadeia de caracteres é do tipo UTF-8 string;

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

c) Se o número do RG ou o número de inscrição do Título de Eleitor não estiver disponível, não se deve preencher o campo de órgão emissor e UF ou os campos Zona Eleitoral, Sessão, Município e UF, respectivamente;

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

e) As 6 (seis) posições das informações sobre órgão expedidor 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;

f) Para todos os campos OtherName, com exceção do campo PrincipalName, 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;

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

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

Para o preenchimento do campo PrincipalName serão permitidos os caracteres de "A" a "Z", de "0" a "9" além dos caracteres "." (ponto), "-" (hífen) e "@" (arroba), necessários à formação do endereço de e-mail do responsável pelo uso do certificado. Outros caracteres especiais, símbolos, espaços ou acentuação não são permitidos.

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

	<p>Tipo de Documento:</p> <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	<p>Código:</p> <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

#### 7.1.2.7. Extensões Não-Obrigatórias pela ICP-Brasil

a) para Certificados de Pessoa Física (e-CPF)

a.1) sub-extensão "rfc822Name", parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do titular do certificado deverá estar presente.

a.2) extensão "Extended Key Usage", não crítica, contendo o valor:

- i. "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2) e
- ii. "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4).

a.3) Para certificados e-CPF para logon de rede, a AC PRODEST RFB implementa adicionalmente o valor "Smart Card Logon" (OID 1.3.6.1.4.1.311.20.2.2).

b) para Certificados de Pessoa Jurídica (e-CNPJ)

b.1) sub-extensão "rfc822Name", parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do responsável, perante o CNPJ, pela Pessoa Jurídica titular do certificado deverá estar presente.

b.2) extensão "Extended Key Usage", não crítica, contendo o valor:

- i. "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2) e
- ii. "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4).

c) para Certificados de Equipamento (e-Servidor)

c.1) sub-extensão "rfc822Name", parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do responsável pelo certificado deverá estar presente.

c.2) extensão "Extended Key Usage", não crítica, contendo o valor "server authentication" (id-kp-serverAuth) (OID 1.3.6.1.5.5.7.3.1).

d) para Certificados de Assinatura de Código (e-Código)

d.1) sub-extensão "rfc822Name", parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do responsável pelo certificado deverá estar presente.

d.2) extensão "Extended Key Usage", não crítica, contendo o valor "code signing" (id\_kp\_codeSigning) (OID 1.3.6.1.5.5.7.3.3).

#### 7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC PRODEST RFB às entidades titulares de certificado 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, e 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 hash (OID = 1.2.840.113549.1.1.13) nas hierarquias V2

#### 7.1.4. Formatos de nome

##### 7.1.4.1 Certificado e-CPF

CN = Nome da Pessoa Física: número de inscrição no CPF

OU = Nome da AR responsável pela aprovação do certificado

OU = Identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for ser empregado

OU = RFB e-CPF A1

OU = Secretaria da Receita Federal do Brasil - RFB

O = ICP-Brasil

C = BR

Onde:

- i. Nome da Pessoa Física é obtido do Cadastro de Pessoas Físicas da RFB, com comprimento máximo de 52 caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da pessoa física do titular neste cadastro, composto por 11 (onze) caracteres.

**NOTA1:** Caso os "OU" não sejam utilizados, os mesmos serão grafados com o texto "(EM BRANCO)".

	Tipo de Documento:  <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	Código:  <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

#### 7.1.4.2 Certificado e-CNPJ

CN = Nome Empresarial:número de inscrição no CNPJ  
OU = Nome da AR responsável pela aprovação do certificado  
OU = RFB e-CNPJ A1  
OU = Secretaria da Receita Federal do Brasil - RFB  
L = Cidade  
ST = sigla da Unidade da Federação  
O = ICP-Brasil  
C = BR

Onde:

- i. O Nome Empresarial da pessoa Jurídica é obtido do Cadastro Nacional de Pessoa Jurídica da RFB, com comprimento máximo de 49 caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.
- ii. O campo locality "L=" representa o nome completo, por extenso, sem acentos e nem abreviaturas da cidade onde se localiza a Pessoa Jurídica.
- iii. O campo state or province name"ST=" representa a sigla da Unidade da Federação onde se localiza a Pessoa Jurídica.

#### 7.1.4.3 Certificado de e-Servidor

CN = Nome do DNS (Domain Name Service) oficial do equipamento  
OU = Nome da AR responsável pela aprovação do certificado  
OU = RFB e-Servidor A1  
OU = Secretaria da Receita Federal do Brasil - RFB  
O = ICP-Brasil  
C = BR

**NOTA1:** Será escrita o DNS até o limite de 64 caracteres, vedada a abreviatura.

**NOTA2:** Caso os "OU" não sejam utilizados, os mesmos serão grafados com o texto "(EM BRANCO)".

#### 7.1.4.4 Certificado de e-Código

CN = Nome empresarial:número de inscrição no CNPJ  
OU = Nome da AR responsável pela aprovação do certificado  
OU = RFB e-Código A1  
OU = Secretaria da Receita Federal do Brasil - RFB  
O = ICP-Brasil  
C = BR

Onde:

- i. O Nome Empresarial da pessoa Jurídica é obtido do Cadastro Nacional de Pessoa Jurídica da RFB, com comprimento máximo de 49 caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.

	Tipo de Documento:  <h2 style="text-align: center;">PROCEDIMENTO</h2>	Código:  <h3 style="text-align: center;">NPS-DIREX-006</h3>
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------	-------------------------------------------------------------------

### 7.1.5. Restrições de nome

7.1.5.1. Neste item estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC PRODEST RFB são as seguintes:

- a) Os acentos não devem ser utilizados e devem ser substituídos pelo caractere não acentuado;
- b) o cedilha deve ser substituído pelo caractere 'c';
- c) além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
\$	24
%	25
&	26
'	27
(	28
)	29
*	2A

Caractere	Código NBR9611 (hexadecimal)
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

**Tabela 1 - Caracteres especiais admitidos em nomes**

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

O OID (Object Identifier) desta PC é 2.16.76.1.2.1.35.

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

Não se aplica.

### 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 Web (<http://www.certificadodigital.com.br/repositorio/prodest/dpc>) da DPC-AC PRODEST RFB.

### 7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 3280.

## 7.2. Perfil de LCR

### 7.2.1. Número(s) de versão

As LCR geradas pela AC PRODEST RFB implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

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

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC PRODEST RFB e sua criticidade.

	Tipo de Documento:  <h2 style="text-align: center;">PROCEDIMENTO</h2>	Código:  <h3 style="text-align: center;">NPS-DIREX-006</h3>
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------	-------------------------------------------------------------------

7.2.2.2. As LCRs da AC PRODEST RFB V2 obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

7.2.2.2.1. Para as LCRs da AC PRODEST RFB V2:

- a) "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC que assina a LCR;
- b) "CRL Number", não crítica: contém um número seqüencial para cada LCR emitida pela AC PRODEST RFB V2;
- c) "Authority Information Access", não crítica, contendo endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia: <http://www.certificadodigital.com.br/cadeias/PRODESTrfbv2.p7b>.

7.2.2.2.2. Para as LCRs da AC PRODEST RFB V1:

- a) "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC que assina a LCR;
- b) "CRL Number", não crítica: contém um número seqüencial para cada LCR emitida pela AC PRODEST RFB V1;
- c) "Authority Information Access", não crítica, contendo endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia: <http://www.certificadodigital.com.br/cadeias/PRODESTrfbv1.p7b>.

## 8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

### 8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta PC é submetida à aprovação do CG da ICP-Brasil.

### 8.2. Políticas de publicação e notificação

Esta PC está disponível para a comunidade no endereço web <http://loja.certificadodigital.com.br/prodest/ProdestRFB>.

### 8.3. Procedimentos de aprovação

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC PRODEST RFB, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

## 9. DOCUMENTOS REFERENCIADOS

### 9.1 Resoluções do Comitê-Gestor da ICP-Brasil

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

Ref.	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

### 9.2 Instruções Normativas da AC Raiz

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
[3]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

## 10. LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora

AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil

AR - Autoridades de Registro

	Tipo de Documento:  <p style="text-align: center;"><b>PROCEDIMENTO</b></p>	Código:  <p style="text-align: center;"><b>NPS-DIREX-006</b></p>
-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------	------------------------------------------------------------------------

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