Autor: Confederação Nacional de Dirigentes Lojistas - SPC Brasil
Edição: 28/12/2015
Versão: 1.1

1. INTRODUÇÃO

1.1 Visão Geral

1.1.1. Este documento descreve os requisitos mínimos para as Politica de Certificado (PC) obrigatoriamente observado pela Autoridade Certificadora Confederação Nacional de Dirigentes Lojistas – SPC Brasil para assinatura digital tipo A1, integrantes da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

1.1.2. A Estrutura desta PC de assinatura digital tipo A1 está baseada no documento Requisitos Mínimos para as Politicas de Certificados do Comitê Gestor da ICP-Brasil – (DOC-ICP-04).

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

1.1.4. Item não aplicável.

1.1.5. Esta PC refere-se exclusivamente a certificados de pessoa física e de pessoa jurídica tipo A1, emitidos pela AC CNDL RFB (a seguir designada simplesmente por "AC CNDL RFB").

1.1.6. Item não aplicável.

1.1.7. Item não aplicável.

1.2 Identificação

1.2.1. Esta PC é chamada de Politica de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora Confederação Nacional de Dirigentes Lojistas – SPC Brasil referida como PC A1 da AC CNDL RFB". O Object Identifier (OID) atribuído para a PC A1 da AC CNDL RFB é 2.16.76.1.2.1.52.

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridade Certificadora (AC)

1.3.1.1. Esta PC está relacionada à AC CNDL RFB (Confederação Nacional de Dirigentes Logistas, com sede na Rua Leôncio de Carvalho, 234 – 13º andar – Paraíso – SP – CEP 04003-010, CNPJ nº 34.173.682/0003-18). As práticas e procedimentos de certificação da AC CNDL RFB estão descritos na Declaração de Práticas de Certificação da AC CNDL RFB a seguir designada simplesmente por "DPC-AC CNDL RFB".

1.3.1.2. A AC CNDL RFB mantém as informações acima sempre atualizadas.

1.3.2 Autoridade de Registro (AR)

1.3.2.1. A AC CNDL RFB informa que 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 - AR.

As Autoridades de Registro vinculadas (ARV) à AC CNDL RFB estão relacionadas na página Web: https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital.
Os conteúdos relacionados na página Web https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital são:
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 respectivas datas de encerramento das atividades;
f) acordos operacionais celebrados pelas AR vinculada com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC CNDL RFB mantém as informações acima sempre atualizadas.

1.3.3 Prestador de Serviços de Suporte

1.3.3.1. Todos os Prestadores de Serviços de Suporte vinculados à AC CNDL RFB estão relacionados na página Web https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital.

1.3.3.2. PSS são entidades utilizadas pela AC CNDL 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 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 CNDL RFB mantém as informações acima sempre atualizadas.

1.3.4 Titulares de Certificado

Os Titulares do Certificado de Assinatura Digital tipo A1 da AC CNDL RFB podem ser pessoas físicas ou jurídicas, desde que não estejam na situação cadastral CANCELADA (pessoa física) ou INAPTA, CANCELADA ou SUSPENSA (pessoa jurídica) conforme os itens 1.3.4, 3.1.9, 3.1.10 e 3.1.11 da DPC-AC CNDL RFB.

No caso de certificado emitido para pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrada no CNPJ da RFB.

1.3.5 Aplicabilidade

1.3.5.1. Os certificados definidos por esta PC possui 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.

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 CNDL RFB considera-se o nível de segurança previsto para o tipo do certificado. Esse nível de segurança caracteriza-se pelos requisitos mínimos que são definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado.

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

1.3.5.5. Item não aplicável.

1.3.5.6. Item não aplicável.

1.4 Dados de Contato

Dúvidas decorrentes da leitura desta PC e que não sejam respondidas mediante a leitura da página https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital podem ser esclarecidas contatando:

Confederação Nacional de Dirigente Lojistas – SPC Brasil
Rua: Leôncio de Carvalho nº 234 – 5ª Andar
CEP: 04003-010
São Paulo, SP
Telefones: (55 11) 3549 – 6800
Contato: Marta Santos
e-Mail: certificacao.digial@spcbrasil.org.br / gestão_cd@spcbrasil.org.br

2. DISPOSIÇÕES GERAIS

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

2.1. Obrigações e direitos

2.1.1. Obrigações da AC CNDL RFB
2.1.2. Obrigações das ARs
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 CNDL RFB
2.2.2. Responsabilidades das ARs

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. Auditoria e fiscalização

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
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 CNDL 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 CNDL 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*)
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 CNDL 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 sequência 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 definas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC da AC CNDL RFB. São também definidos outros controles técnicos de segurança utilizados pela AC 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 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 do par de chaves criptográficas tipo A1 ocorre, no mínimo, utilizando CSP (*Cryptographic Service Provider*) existente na estação do solicitante apresentados pelo Navegador (*browser*) Microsoft e, quando da geração, a chave privada é armazenada no HD da estação.

A chave privada poderá ser exportada e armazenada (cópia de segurança) em mídia externa – token, cartão inteligente e/ou demais mídias homologadas, protegidas por senha de acesso.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é o RSA, ECC-Brainpool (conforme RFC 5639) conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

6.1.1.4. Após 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, 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 meio de armazenamento de 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 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. O tipo de certificado emitido pela AC CNDL RFB e descrito nesta PC é o A1.

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

6.1.1.8. A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento, é do titular do certificado, conforme especificado no Termo de Titularidade, no caso de certificados de pessoa física e jurídica.

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

A entrega da chave pública do solicitante do certificado AC CNDL RFB, 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 CNDL RFB disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP–Brasil, através:

a) No momento da disponibilização de um certificado para seu titular; usando formato PKCS conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

b) Página Web*:* https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital.

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.

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

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

6.1.7. Os parâmetros são verificados de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program)* do NIST (*National Institute of standards and technology).*

6.1.8. 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

6.2.1. Padrões para módulo criptográfico

Item não aplicável.

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 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 CNDL RFB não mantém cópia de segurança de chave privada de titular de certificado por ela emitido.

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

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 pela AC CNDL RFB 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

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

6.2.7. Método de ativação de chave privada

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 ativação da sua chave privada.

6.2.9. Método de destruição de chave privada

Cada entidade titular de certificado deve definir procedimentos necessários para a ativação 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 CNDL 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. Item não aplicável.

6.3.2.3. O período máximo de uso das chaves correspondentes aos certificados emitidos pela PC AC CNDL RFB A1 é de (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; e
c) definir senhas com caracteres numéricos e alfanuméricos.

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; e
c) definir senhas com caracteres numéricos e alfanuméricos.

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

Nos equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC CNDL 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 antispyware, 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 dois minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2. Classificação da segurança computacional

Item não aplicável.

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

Item não aplicável.

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.

7.1. Perfil do Certificado

Os certificados emitidos pela AC CNDL 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 CNDL RFB 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 e sua criticidade.

7.1.2.2. Extensões Obrigatórias

7.1.2.2.1 para Certificados emitidos pela AC CNDL RFB v2:

Os certificados emitidos pela AC CNDL 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 CNDL RFB;
b) "Key Usage", crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;
c) "Certificate Policies", não crítica: contém o OID2.16.76.1.2.1.52 desta PC e o endereço Web da DPC-AC CNDL RFB (https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital);
http://repositório.acspcbrasil.org.br/ac-spcbrasilrfb/lcr-ac-spcbrasilrfbv2.crl.
http://repositorio.acsafeweb.com.br/ac-safewebrfb/lcr-ac-safewebrfbv2.crl

d) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente: https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital.

e) "Authority Information Access", não crítica:

I. Contendo endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia: https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital.
Contendo endereço na Web onde se acessa o serviço OCSP correspondente: https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital.

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)

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 da pessoa física titular do certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o número de inscrição no Cadastro de Pessoa Física (CPF) da pessoa física titular do certificado; nas 11 (onze) posições subsequentes, o número de Identificação Social da pessoa física titular do certificado - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) da pessoa física titular do certificado; nas 10 (dez) posições subsequentes, 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.

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.

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

A.2) campo otherName, não obrigatório, contendo:
i. OID = 2.16.76.1.4.2.1.1 e conteúdo = nas primeiras 07 (sete) posições os dígitos alfanuméricos do Número de Inscrição junto a Seccional, e nas 2 (duas) posições subsequentes a sigla do Estado da Seccional.

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

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 subsequentes, o número de inscrição no Cadastro de Pessoa Física (CPF) do responsável pela Pessoa Jurídica perante o CNPJ; nas 11 (onze) posições subsequentes, o Número de Inscrição Social - NIS (PIS, PASEP ou CI) do responsável pela Pessoa Jurídica perante o CNPJ; nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do responsável

pela Pessoa Jurídica perante o CNPJ; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:
OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pela Pessoa Jurídica, perante o CNPJ.
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.
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.

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.

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 10 (dez) 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 PincipalName, 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 CNDL 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.

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 CNDL RFB implementa adicionalmente campo otherName com OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo UPN (*User Principal Name*) a identificação do endereço de login do titular do certificado no diretório ActiveDirect (AD) Microsoft.

a.4) Para certificados e-CPF para logon de rede, a AC CNDL 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).

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC CNDL RFB às entidades titulares de certificado são assinados com o uso do algoritmo RSA com SHA-512 como função hash (OID = 1.2.840.113549.1.1.13) nas hierarquias V2 e V3 conforme o padrão PKCS#1.

7.1.4. Formatos de nome

7.1.4.1 Certificado e-CPF

a) para Certificados emitidos pela AC CNDL RFB v2:

C = BR
O = ICP-Brasil
OU = Secretaria da Receita Federal do Brasil - RFB
OU = RFB e-CPF A1
OU = Identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for ser empregado
OU = Nome da AR responsável pela aprovação do certificado
CN = Nome da Pessoa Física: número de inscrição no CPF

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 o segundo "OU" Identificação da empresa ou fornecedor do certificado não seja utilizado, o mesmo será grafado com o texto "(EM BRANCO)".

7.1.4.2 Certificado e-CNPJ

a) para Certificados emitidos pela AC CNDL RFB v2:

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

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.

7.1.5. 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 CNDL 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)	Caractere	Código NBR9611 (hexadecimal)
Branco	20	+	2B
!	21	,	2C
"	22	-	2D
#	23	.	2E
$	24	/	2F
%	25	:	3A
&	26	;	3B
'	27	=	3D
(	28	?	3F
)	29	@	40
*	2A	\	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**.52**

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 Web (https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital) da DPC-AC CNDL RFB.

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 CNDL RFB 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 CNDL RFB e sua criticidade.

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

7.2.2.2.1. Para LCRs emitidos pela AC CNDL 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 sequencial para cada LCR emitida pela AC CNDL RFB;

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 https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital.

8.3. Procedimentos de aprovação

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC CNDL 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
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