

Política de Certificado de Assinatura Tipo A3

PC A3 - AC SAFEWEB RFB

Versão 2.0
Outubro 2017

SUMÁRIO

1.1	VISÃO GERAL.....	06
1.2	IDENTIFICAÇÃO	06
1.3	COMUNIDADE E APLICABILIDADE	06
1.3.1	AUTORIDADE CERTIFICADORA - AC.....	06
1.3.2	AUTORIDADE DE REGISTRO (AR).....	07
1.3.3	PRESTADOR DE SERVIÇOS DE SUPORTE	08
1.3.4	TITULARES DE CERTIFICADO	08
1.3.5	APLICABILIDADE	09
1.4	DADOS DE CONTATO	09
2	DISPOSIÇÕES GERAIS.....	10
2.1	OBRIGAÇÕES E DIREITOS.....	10
2.2	RESPONSABILIDADES.....	10
2.3	RESPONSABILIDADE FINANCEIRA.....	10
2.4	INTERPRETAÇÃO E EXECUÇÃO.....	10
2.5	TARIFAS DE SERVIÇO	10
2.6	PUBLICAÇÃO E REPOSITÓRIO.....	11
2.7	FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE.....	11
2.8	SIGILO	11
2.9	DIREITOS DE PROPRIEDADE INTELECTUAL	11
3	IDENTIFICAÇÃO E AUTENTICAÇÃO	11
3.1	REGISTRO INICIAL.....	11
3.2	GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL.....	12
3.3	GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO	12
3.4	SOLICITAÇÃO DE REVOGAÇÃO.....	12
4	REQUISITOS OPERACIONAIS	12
4.1	SOLICITAÇÃO DE CERTIFICADO	13
4.2	EMISSÃO DE CERTIFICADO	13
4.3	ACEITAÇÃO DE CERTIFICADO	13
4.4	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	13
4.5	PROCEDIMENTO DE AUDITORIA DE SEGURANÇA.....	13
4.6	ARQUIVAMENTO DE REGISTROS.....	14
4.7	TROCA DE CHAVE	14
4.8	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	14
4.9	EXTINÇÃO DOS SERVIÇOS DE AC, AR ou PSS	14
5	CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL	14
5.1	CONTROLES FÍSICOS.....	15
5.2	CONTROLES PROCEDIMENTAIS.....	15
5.3	CONTROLE DE PESSOAL.....	15
6	CONTROLES TÉCNICOS DE SEGURANÇA.....	16
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	16

6.1.1	GERAÇÃO DO PAR DE CHAVES.....	16
6.1.2	ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR.....	17
6.1.3	ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO.....	17
6.1.4	DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC SAFEWEB RFB PARA USUÁRIOS.....	17
6.1.5	TAMANHOS DE CHAVE.....	18
6.1.6	GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS.....	18
6.1.7	VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS.....	18
6.1.8	GERAÇÃO DE CHAVE POR HARDWARE OU SOFTWARE.....	18
6.1.9	PROPÓSITO DE USO DE CHAVE (conforme o campo "key usage" na X.509 v3).....	18
6.2	PROTEÇÃO DE CHAVE PRIVADA.....	19
6.2.1	PADRÕES PARA MÓDULO CRIPTOGRÁFICO.....	19
6.2.2	CONTROLE "N de M" PARA CHAVE PRIVADA.....	19
6.2.3	CUSTÓDIA (escrow) DE CHAVE PRIVADA.....	19
6.2.4	CÓPIA DE SEGURANÇA (backup) DE CHAVE PRIVADA.....	19
6.2.5	ARQUIVAMENTO DE CHAVE PRIVADA.....	20
6.2.6	INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO.....	20
6.2.7	MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA.....	20
6.2.8	MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA.....	20
6.2.9	MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA.....	20
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES.....	20
6.3.1	ARQUIVAMENTO DE CHAVE PÚBLICA.....	20
6.3.2	PERÍODOS DE USO PARA AS CHAVES PÚBLICAS E PRIVADAS.....	21
6.4	DADOS DE ATIVAÇÃO.....	21
6.4.1	GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO.....	21
6.4.2	PROTEÇÃO DOS DADOS DE ATIVAÇÃO.....	21
6.4.3	OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO.....	21
6.5	CONTROLES DE SEGURANÇA COMPUTACIONAL.....	21
6.5.1	REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL.....	22
6.5.2	CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL.....	22
6.6	CONTROLES TÉCNICOS DO CICLO DE VIDA.....	22
6.6.1	CONTROLES DE DESENVOLVIMENTO DO SISTEMA.....	22
6.6.2	CONTROLES DE GERENCIAMENTO DE SEGURANÇA.....	22
6.6.3	CLASSIFICAÇÃO DE SEGURANÇA DE CICLO DE VIDA.....	22
6.7	CONTROLES DE SEGURANÇA DE REDE.....	22
6.8	CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO.....	23
7	PERFIS DE CERTIFICADO E LCR.....	23
7.1	PERFIL DO CERTIFICADO.....	23
7.1.1	NÚMERO (s) DE VERSÃO.....	23
7.1.2	EXTENSÕES DE CERTIFICADO.....	23
7.1.3	IDENTIFICADORES DE ALGORITMO.....	27
7.1.4	FORMATOS DE NOME.....	28
7.1.5	RESTRIÇÕES DE NOME.....	29
7.1.6	OID (Object Identifier) DE POLÍTICA DE CERTIFICADO.....	30
7.1.7	USO DA EXTENSÃO "Policy Constraints".....	30
7.1.8	SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA.....	30
7.1.9	SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS.....	30
7.2	PERFIL DE LCR.....	30

7.2.1	NÚMERO (s) DE VERSÃO.....	30
7.2.2	EXTENSÕES DE LCR E DE SUAS ENTRADAS	30
8	ADMINISTRAÇÃO DE ESPECIFICAÇÃO	31
8.1	PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO.....	31
8.2	POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO	31
8.3	PROCEDIMENTO DE APROVAÇÃO	31
9	DOCUMENTOS REFERENCIADOS.....	31
9.1	RESOLUÇÕES DO COMITÊ-GESTOR DA ICP BRASIL.....	31
9.2	INSTRUÇÕES NORMATIVAS DA AC RAIZ.....	32
10	LISTA DE ACRÔNIMOS	33

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou alteração	Item alterado
1.0	10/12/2014	N/A	N/A
1.1	01/06/2015	N/A	7.1.2.2 "c.2", 7.1.2.2 "d.1" "d.2" "d.3", 7.1.2.2 "f", 7.1.8, 7.2.2.2 "c", capa
2.0	24/10/2017	DOC-ICP-04	1.1, 1.3.4, 1.3.5, 6.1.4, 6.1.9, 6.2.4, 7.1.2.4, 7.1.2.6, 7.1.2.7, 7.1.2.8, 7.1.4.1, 7.1.4.2
		Resolução 116, de 2015	6.1.5, 7.1.2.2, 7.1.3
		Resolução 118, de 2015	7.1.2.2, 7.1.2.3
		Instrução Normativa nº 07, de 2016	
		DOC-ICP-05 e DOC-ICP-01.02	1.3.2.1, 1.3.3.1, 1.4, 6.1.4 "c", 7.1.2.2.1, 7.1.2.2.2, 7.1.2.4 "e", 8.2

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 - ACs integrantes da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PCs.

1.1.2 Esta Política de Certificado de Assinatura Digital tipo A3 da AC Safeweb RFB (a seguir designada simplesmente por "PC A3 da AC Safeweb RFB") adota a mesma estrutura empregada naquele documento.

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

1.1.4 Não se aplica.

1.1.5 Esta PC refere-se exclusivamente a Certificados de Pessoa Física, Pessoa Jurídica, Tipo A3 emitidos pela AC Safeweb RFB.

1.1.6 Não se aplica.

1.1.7 Não se aplica.

1.1.8 Não se aplica.

1.2 IDENTIFICAÇÃO

1.2.1 A PC A3 da AC Safeweb RFB descreve os procedimentos e práticas da AC Safeweb RFB e os usos relacionados ao Certificado de Assinatura Digital Tipo A3.

1.2.2 O *Object Identifier* - OID da PC A3 da AC Safeweb RFB, atribuído para esta PC, após processo de credenciamento da AC junto à ICP-Brasil, é **2.16.76.1.2.3.48**.

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 Safeweb RFB, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-

Brasil, sob a hierarquia da Autoridade Certificadora RFB, que por sua vez esta subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira – AC Raiz.

As práticas e procedimentos de certificação da AC Safeweb RFB estão descritos na Declaração de Práticas de Certificação da AC Safeweb RFB – DPC - AC Safeweb RFB.

1.3.1.2 ATUALIZAÇÃO DE DADOS

A AC Safeweb RFB mantém as informações acima sempre atualizadas.

1.3.2 AUTORIDADE DE REGISTRO (AR)

1.3.2.1 DADOS DAS AUTORIDADES DE REGISTROS

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 Safeweb RFB (ARs Vinculadas) estão relacionados na página <https://safeweb.com.br/ac/autoridades-registro> que contém:

- a) Relação de todas as ARs 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 ATUALIZAÇÃO DE DADOS

A AC Safeweb RFB mantém as informações acima sempre atualizadas.

1.3.3 PRESTADOR DE SERVIÇOS DE SUPORTE

1.3.3.1 DADOS DOS PSS

Os Prestadores de Serviços de Suporte vinculados à AC Safeweb RFB estão relacionados na página www.safeweb.com.br

1.3.3.2 PSS

PSS são entidades utilizados pela AC Safeweb RFB ou pelas ARs 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 ATUALIZAÇÃO DE DADOS

A AC Safeweb RFB mantém as informações acima sempre atualizadas.

1.3.4 TITULARES DE CERTIFICADO

1.3.4.1 Podem ser titulares de certificados emitidos segundo esta PC:

- a) Para certificados **e-CPF** - pessoas físicas inscritas no CPF, desde que não enquadradas na situação cadastral de CANCELADA OU NULA, conforme o disposto nos incisos I e II do art. 6º da Instrução Normativa RFB nº 222, de 11 de Outubro de 2002;
- b) Para certificados **e-CNPJ** - Pessoas jurídicas inscritas no CNPJ, desde que não enquadradas na condição de INAPTA, SUSPENSA, BAIXADA, NULA ou CANCELADA, conforme o disposto nos incisos I e II do art. 6º da Instrução Normativa RFB nº 222, de 11 de Outubro de 2002.

1.3.4.2. A validação do nome e da situação cadastral do titular do certificado (e do responsável, quando for o caso), é realizada por intermédio do sistema Consulta Prévia, disponibilizado pela RFB às Autoridades Certificadoras Habilitadas.

1.3.4.3 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 cadastrado no CNPJ da RFB.

1.3.5 APLICABILIDADE

1.3.5.1 Os certificados definidos por esta PC têm sua utilização vinculada à assinatura digital, não repúdio, garantia de integridade da informação, autenticação de seu titular.

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

1.3.5.3 Na definição das aplicações para o certificado definido pela PC, a AC Safeweb 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 São as seguintes as aplicações dos certificados emitidos por esta PC:

a) Os certificados **e-CPF** e **e-CNPJ** são utilizados para assinatura digital e autenticação do seu titular em sistemas e aplicações;

1.3.5.5 Não se aplica.

1.3.5.6 Não se aplica.

1.3.5.7 Não se aplica.

1.4 DADOS DE CONTATO

Dúvidas decorrentes da leitura desta PC e que não sejam respondidas mediante a leitura da página www.safeweb.com.br podem ser esclarecidas contatando:

Setor de Compliance

Telefone: (51) 3018-0300

E-mail: compliance@safeweb.com.br

Safeweb Segurança da Informação Ltda.

Endereço: Av. Princesa Isabel, 828 – Porto Alegre/RS – CEP 90620-000

2 DISPOSIÇÕES GERAIS

Os itens seguintes estão referidos nos correspondentes itens DPC-AC Safeweb 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

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 Safeweb 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 Safeweb 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 PROCEDIMENTO 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 Safeweb 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)
- 5.1.9 Instalações técnicas de AR

5.2 CONTROLES PROCEDIMENTAIS

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

5.3 CONTROLE 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, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São também definidos outros controles técnicos de segurança utilizados pela AC e pelas ARs vinculadas 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 [2].

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.

6.1.1.1.1. Não se aplica.

6.1.1.2 O processo de geração de chaves do tipo A3, 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 o RSA, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

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 [2], 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 e atende ao disposto na tabela a seguir:

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou hardware criptográfico homologado junto à ICP-Brasil

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR

A AC Safeweb 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, entrega sua chave pública à AC Safeweb RFB ou à correspondente AR vinculada, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [2].

6.1.4 DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC SAFEWEB RFB PARA USUÁRIOS

As formas para a disponibilização do certificado da AC Safeweb RFB, e de todos os certificados da cadeia V2 e da cadeia V5 de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

- a) Formato PKCS#7, que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- b) Diretório;
- c) Página Web da AC Safeweb RFB www.safeweb.com.br;
- d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil.

6.1.5 TAMANHOS DE CHAVE

6.1.5.1 Os certificados emitidos de acordo com esta PC situam-se sob a cadeia da Autoridade Certificadora Raiz V2 ou V5. O tamanho mínimo admitido para chaves criptográficas é de 2048 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 [2].

6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS

Os parâmetros de geração de chaves assimétricas dos titulares de certificado atendem ao estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [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 [2].

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 hardware.

6.1.9 PROPÓSITO DE USO DE CHAVE (conforme o campo "key usage" na X.509 v3)

Os pares de chaves correspondentes aos certificados emitidos pela AC Safeweb RFB podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

6.2 PROTEÇÃO DE 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

O módulo criptográfico de geração e armazenamento de chaves assimétricas de usuário final atende ao padrão FIPS 140-1 ou FIPS 140-2 e é homologado na ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

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 Safeweb 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 [2], 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 realizar 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

A chave privada é ativada, mediante senha solicitada pelo software de proteção da chave privada. A senha deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo. O Titular de certificado deverá adotar senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 3 meses.

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 Safeweb RFB, dos titulares de certificados de assinatura digital e as LCRs 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 PÚBLICAS E PRIVADAS

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 A3 da AC Safeweb RFB é de 5 (cinco) anos.

6.4 DADOS DE ATIVAÇÃO

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Os certificados de tipo A3 se utilizam, para armazenamento do par de chaves e certificado, de repositório protegido por senha e/ou identificação biométrica e cifrado por software.

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 Safeweb RFB, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

- a) Controle de acesso lógico ao sistema operacional;
- b) Exigência de uso de senhas fortes;
- c) Diretivas de senha e de bloqueio de conta;
- d) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;
- e) *Firewall* pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- f) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.);
- g) Proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 CLASSIFICAÇÃO DE 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 DO SISTEMA

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.6.3 CLASSIFICAÇÃO 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 [2].

7 PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCRs 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 Safeweb 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 Safeweb 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 Os certificados emitidos pela AC Safeweb RFB 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 Safeweb RFB;
- b) "**Key Usage**", crítica: somente os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment* estão ativados;

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

c.1) O campo *policyIdentifier* contém o OID desta PC 2.16.76.1.2.3.48;

c.2) O campo *PolicyQualifiers* contém o endereço Web onde se obtém a DPC da AC Safeweb RFB:
<http://repositorio.acsafeweb.com.br/ac-safewebrfb/dpc-acsafewebrfb.pdf>;

d) "**CRL Distribution Points**", não crítica: contém o endereço na Web onde se obtém a LCR correspondente:

Raiz V2:

d.1) <http://repositorio.acsafeweb.com.br/ac-safewebrfb/lcr-ac-safewebrfbv2.crl>

d.2) <http://repositorio2.acsafeweb.com.br/ac-safewebrfb/lcr-ac-safewebrfbv2.crl>

Raiz V5:

d.3) <http://repositorio.acsafeweb.com.br/ac-safewebrfb/lcr-ac-safewebrfbv5.crl>

d.4) <http://repositorio2.acsafeweb.com.br/ac-safewebrfb/lcr-ac-safewebrfbv5.crl>

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

Raiz V2:

e.1) <http://repositorio.acsafeweb.com.br/ac-safewebrfb/ac-safewebrfbv2.p7b>

Raiz V5:

e.1) <http://repositorio.acsafeweb.com.br/ac-safewebrfb/ac-safewebrfbv5.p7b>

7.1.2.2.2 A segunda entrada pode conter o método de acesso *id-ad-ocsp*, com o respectivo endereço do respondedor OCSP, quando aplicável.

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:

l) 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 Específico do INSS (CEI) da pessoa física titular do certificado.

III) OID = 2.16.76.1.3.5 e conteúdo: nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor 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.

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.

a.2) Não se aplica

a.3) Não se aplica

b) para Certificados de Pessoa Jurídica – e-CNPJ

b.1) 4 (quatro) campos *otherName*, obrigatórios, contendo, nesta ordem:

I) OID = 2.16.76.1.3.4 e conteúdo: nas primeiras 8 (oito) posições, a data de nascimento do responsável 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.

II) OID = 2.16.76.1.3.2 e conteúdo: nome do responsável pela Pessoa Jurídica, perante o CNPJ.

III) OID = 2.16.76.1.3.3 e conteúdo: nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

IV) OID = 2.16.76.1.3.7 e conteúdo: nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da Pessoa Jurídica titular do certificado.

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) Não se aplica;

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

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;

7.1.2.5 Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC Safeweb 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*" são utilizados, na forma e com os propósitos definidos na RFC 5280:

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 Safeweb RFB implementa adicionalmente campo *otherName* com OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo *User Principal Name - UPN* 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 Safeweb 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).

7.1.2.7 Não se aplica.

7.1.2.8 Não se aplica.

7.1.3 IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC Safeweb RFB às entidades titulares de certificado são assinados com o uso do algoritmo RSA com SHA-256 como função de hash (OID 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função de hash (OID 1.2.840.113549.1.1.13) na hierarquia V2 e V5 conforme o padrão PKCS#1.

7.1.4 FORMATOS DE NOME

7.1.4.1 O nome do titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594:

a) CERTIFICADO e-CPF

C = BR

O = ICP-Brasil

OU = Secretaria da Receita Federal do Brasil - RFB

OU = RFB e-CPF A3

OU = Identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for seu 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 "OU" Identificação da empresa ou fornecedor do certificado não seja utilizado, o mesmo será grafado com o texto "(EM BRANCO)".

b) CERTIFICADO e-CNPJ

C = BR

O = ICP-Brasil

ST = Sigla da Unidade da Federação

L = Cidade

OU = Secretaria da Receita Federal do Brasil - RFB

OU = RFB e-CNPJ A3

OU = Nome da AR responsável pela aprovação do certificado

CN = Nome Empresarial: número de inscrição no CNPJ

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.

7.1.4.2 Não se aplica.

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 Safeweb 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

7.1.6 OID (*OBJECT IDENTIFIER*) DE POLÍTICA DE CERTIFICADO

O OID (Object Identifier) desta PC é 2.16.76.1.2.3.48.

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 da DPC AC Safeweb RFB:

<http://repositorio.acsafeweb.com.br/ac-safewebrfb/dpc-acsafewebrfb.pdf>

7.1.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 PERFIL DE LCR

7.2.1 NÚMERO (S) DE VERSÃO

As LCR geradas pela AC Safeweb 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 Safeweb RFB e sua criticidade.

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

- a) "**Authority Key Identifier**", não crítica: contém o hash SHA-1 da chave pública da AC que assina a LCR;
- b) "**CRL Number**", não crítica: contém um número sequencial para cada LCR emitida pela AC Safeweb RFB;

c) "**Authority Information Access**", não crítica, contendo endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia:

<http://repositorio.acsafeweb.com.br/ac-safeweb/brfb/ac-safeweb/brfbv5.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 www.safeweb.com.br.

8.3 PROCEDIMENTO DE APROVAÇÃO

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC Safeweb RFB, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

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	DOC-ICP-04

	ICP-BRASIL	
[3]	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 site <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[2]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA 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
CMM-SEI	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
COBIT	<i>Control Objectives for Information and related Technology</i>
COSO	<i>Comitee of Sponsoring Organizations</i>
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
IDS	Sistemas de Detecção de Intrusão
IEC	<i>International Electrotechnical Commission</i>
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	<i>National Institute of Standards and Technology</i>
OCSP	<i>On-line Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PIS	Programa de Integração Social
POP	<i>Proof of Possession</i>
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
SNMP	<i>Simple Network Management Protocol</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
TSDM	<i>Trusted Software Development Methodology</i>
URL	<i>Uniform Resource Location</i>