www.serpro.gov.br

Política de Certificação
da
Autoridade Certificadora
do
SERPRO RFB SSL A1

Autenticação de Servidor(SSL/TSL)

(PC AC SERPRO RFB SSL A1)

Versão 2.0 de Outubro 2019

Sumário

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos a serem obrigatoriamente observados pela AC SERPRO RFB SSL integrante da infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2. A PC SERPRO RFB SSL A1 elaborada no âmbito da ICP-Brasil adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO na ICP-BRASIL (DOC-ICP-04).

1.1.3. São 12 (doze) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 8 (oito) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme descrito a seguir:

a) Tipos de Certificados de Assinatura Digital:

- A1
- A2
- A3
- A4
- T3
- T4
- A CF-e-SAT
- OM-BR

b) Tipos de Certificados de Sigilo:

- S1
- S2
- S3
- S4

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

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

1.1.5. O certificado do tipo A1 pode ser emitidos para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.1.8. Não se aplica.

1.1.9. Não se aplica.

1.1.10. Não se aplica.

1.2. Nome do Documento e Identificação

1.2.1. Política de Certificado de Assinatura Digital, tipo A1, da AC SERPRO RFB SSL, OID **2.16.76.1.2.1.91.**

1.2.2. No âmbito da ICP-Brasil, os OIDs das PCs serão atribuídos na conclusão do processo de credenciamento da AC

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

1.3.1.1. A Autoridade Certificadora do SERPRO RFB SSL(AC SERPRO RFB SSL) integra a infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora da RFB (AC RFB) e da Autoridade Certificadora Raiz Brasileira, cuja PC é implementada nesse documento.

1.3.1.2. A DPC dessa AC encontra-se publicada em sua página *Web* no seguinte endereço: https://certificados.serpro.gov.br/acserprorfbssl/

1.3.2. Autoridades de Registro

1.3.2.1. O endereço da página *web* (*URL*) da AC SERPRO RFB SSL é https://certificados.serpro.gov.br/acserprorfbssl/ onde estão publicados os dados abaixo referentes as Autoridades de Registro, responsáveis pelos processos de recebimento, identificação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

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

b) relação de AR que tenham sido descredenciadas da cadeia da AC, com a respectiva data do descredenciamento;

1.3.3. Titulares do Certificado

Titulares de Certificados são as entidades – pessoas físicas ou jurídicas, autorizados pela AR responsável a receber um certificado digital emitido pela AC, para utilização em equipamentos ou aplicações.

1.3.4. Partes Confiáveis

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil.

1.3.5. Outros Participantes

A AC utiliza o Serviço Federal de Processamento de dados (SERPRO) como Prestador de Serviço de Suporte – PSS, Prestador de Serviço Biométrico – PSBio e Prestador de Serviço de Confiança - PSC conforme disponibilizado no endereço: https://certificados.serpro.gov.br/acserprorfbssl/

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

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

Política de Certificado	Aplicações Apropriadas
PC SERPRO RFB SSL A1	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas seguintes aplicações: • Confirmação de Identidade na *web*; • Correio eletrônico; • Transações On-Line; • Redes privadas virtuais (VPN); • Transações eletrônicas; • Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.2. 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.

1.4.1.3. As aplicações para o certificado definido nesta PC, devem levar 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.

1.4.1.4. Certificados de tipo A1 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5. Não se aplica.

1.4.1.6. Não se aplica.

1.4.1.7. Não se aplica

1.4.1.8. Não se aplica.

1.4.2. Uso proibitivo do certificado

Não há restrições de aplicações identificadas.

1.5. Política de Administração

Esta PC é administrada pelo Centro de Certificação Digital do SERPRO(CCD-SERPRO).

1.5.1. Organização administrativa do documento

Autoridade Certificadora do Serpro Final – **AC SERPRO RFB SSL**

1.5.2. Contatos

Administrativo:

Nome: Pedro Moacir Rigo Motta

Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

E-mail: certificados@serpro.gov.br

Telefone: (61) 2021-7957

Suporte:

Nome: Central de Serviços SERPRO

Página Web: http://www.serpro.gov.br/menu/suporte/css

E-mail: css.serpro@serpro.gov.br

Telefone: 0800 7282323

1.5.3. Pessoa que determina a adequabilidade da DPC com a PC

Nome: Pedro Moacir Rigo Motta

Telefone: (61) 2021-7957

E-mail: certificados@serpro.gov.br

1.5.4. Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.

Os procedimentos de aprovação da PC da AC são estabelecidos a critério do CG da ICP-Brasil.

1.6. Definições e Acrônimos

Sigla	Definição
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
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	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
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	*Online 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

PSC	Prestador Servidor de Confiança
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 Locator*

2. Responsabilidades de publicação e repositórios

Os itens seguintes estão descritos da DPC da AC.

2.1. Repositórios

2.2. Publicação de informações dos certificados

2.3. Tempo ou Frequência de Publicação

2.4. Controle de Acesso aos Repositórios

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão descritos da DPC AC SERPRO RFB SSL.

3.1. Nomeação

3.1.1. Tipos de nomes

3.1.2. Necessidade dos nomes serem significativos

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

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

3.2. Validação inicial de identidade

3.2.1. Método para comprovar a posse de chave privada

3.2.2. Autenticação da identificação da organização

3.2.3. Autenticação da identidade de equipamento ou aplicação

Item 3.2.7. da DPC.

3.2.4. Autenticação da identidade de um indivíduo

Item 3.2.3. da DPC.

3.2.5. Informações não verificadas do titular do certificado

Item 3.2.4. da DPC.

3.2.6. Validação das autoridades

Item 3.2.5. da DPC.

3.2.7. Critérios para interoperação

Iem 3.2.6. da DPC.

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. Identificação e autenticação para rotina de novas chaves

3.3.2. Identificação e autenticação para novas chaves após a revogação

3.4. Identificação e Autenticação para solicitação de revogação

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Os itens seguintes estão descritos na DPC da AC.

4.7. Nova chave de certificado

4.7.1. Circunstâncias para nova chave de certificado

4.7.2. Quem pode requisitar a certificação de uma nova chave pública

4.7.3. Processamento de requisição de novas chaves de certificado

4.7.4. Notificação de emissão de novo certificado para o titular

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

4.7.6. Publicação de uma nova chave certificada pela AC

4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades

4.8. Modificação de certificado

4.8.1. Circunstâncias para modificação de certificado

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.10.3. Funcionalidades operacionais

4.11. Encerramento de atividades

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES

Os itens seguintes estão descritos na DPC da AC.

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC SERPRO RFB SSL A1.

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

6.1.1.1.1. Não se aplica.

6.1.1.1.2. Não se aplica.

6.1.1.2. O Titular do Certificado gera a chave utilizando aplicativos com esta finalidade. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficos e pelo uso do certificado. 6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1.].

6.1.1.4. Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICPBRASIL[1] e armazenada em repositório protegido por senha e/ou identificação biométrica, cifrado por software, conforme Tabela 1 a seguir para certificado do Tipo A1.

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

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

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

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

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

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

6.1.1.8. O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17 [4], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em *HSM* de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

Tabela 1 - Mídias Armazenadoras de Chaves Criptográficas

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A1 e S1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima
A2 e S2	Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica
A3 e S3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A4 e S4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
T3 e T4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A CF-e-SAT	Hardware criptográfico.
OM-BR	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

Nota: Não se aplica.

6.1.2. Entrega da chave privada à entidade titular

Não se aplica. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

6.1.3. Entrega da chave pública para o emissor de certificado

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

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

6.1.4. Disponibilização de chave pública da AC para usuários

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

a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL[1];

b) Não se aplica;

c) Página *web* da AC: https://certificados.serpro.gov.br/acserprorfbssl/

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

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC é de, no mínimo, 2048 (dois mil e quarenta e oito) bits;

6.1.5.2. Os algoritmos e o tamanho das chaves utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL [1].

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração e verificação de chaves assimétricas do usuário final adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

Os certificados emitidos pela AC têm no campo “Key usage” (**2.5.29.15**) ativado os bits *digitalSignature, nonRepudiation e keyEncipherment.*

Os certificados emitidos sob esta PC pela AC, são apropriados ao uso apenas nas aplicações apresentadas a seguir:

a) Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas seguintes aplicações;

b) Confirmação de Identidade na web;

c) Correio eletrônico;

d) Transações On-Line;

e) Redes privadas virtuais (VPN);

f) Transações eletrônicas;

g) Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Os certificados de tipo A1 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

Nos itens seguintes, são definidos os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos segundo esta PC.

6.2.1. Padrão e controle para módulo criptográfico

6.2.1.1. Não se aplica.

6.2.1.2. 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 se aplica.

6.2.4. Cópia de segurança (backup) de chave privada

6.2.4.1. Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3. Não se aplica.

6.2.4.4. Não se aplica.

6.2.5. Arquivamento de chave privada

6.2.5.1 Não se aplica.

6.2.5.2. Não se aplica.

6.2.6. Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A chave privada do usuário final 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(três) meses.

6.2.9. Método de desativação de chave privada

A desativação da chave privada ocorre no fechamento do “browser” utilizado para estabelecer uma conexão segura.

6.2.10. Método de destruição de chave privada

A destruição da chave privada do certificado deve ser feita pelo próprio usuário final, por meio da eliminação do arquivo que à contém.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

A AC armazena as chaves públicas da própria AC e dos titulares de certificados, bem como as LCR emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada

6.3.2.1. A chave privada da AC e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. Certificados do tipo A1, previsto nesta PC, tem validade de até 1 ano.

6.3.2.4. Não se aplica.

6.3.2.5. O período máximo de validade dos Certificados SSL/TLS será de até 825 (oitocentos e vinte cinco) dias, conforme documento *WebTrust Principles and Criteria for Certification Authorities*[7].

6.4. Dados de Ativação

Nos itens seguintes, estão descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Cada PC implementada deve descrever os requisitos específicos aplicáveis.

6.4.1. Geração e instalação dos dados de ativação

Os dados de ativação da chave privada da AC são únicos e aleatórios.

6.4.2. Proteção dos dados de ativação

Os dados de ativação da AC são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha e são armazenados em ambiente de nível 6 de segurança.

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

O Titular do Certificado gera a chave utilizando a página de instalação de certificados disponibilizado pela AC e a chave privada é armazenada no HD da estação.

Nos equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados emitidos pela AC SERPRO RFB, recomenda-se o uso de mecanismos que garantam a segurança computacional, tais como:

a) Senha de bios ativada;

b) Controle de acesso lógico ao sistema operacional;

c) Existência de uso de senhas fortes;

d) Diretivas de senha e de bloqueio de contas;

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); e

h) Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

A AC recomenda ainda:

a) que seja feito backup da chave privada, evitando assim perda do certificado; e

b) a remoção do certificado do browser da estação, após sua utilização, caso o equipamento seja compartilhado com outros usuários.

6.5.2 Classificação da segurança computacional

Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

A AC não exige um software específico para utilização dos certificados emitidos segundo esta PC.

6.6.1. Controles de desenvolvimento de sistema

Não se aplica.

6.6.2. Controles de gerenciamento de segurança

Não se aplica.

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Todas as LCR geradas pela AC são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7. Controles de Segurança de Rede

Os mesmos controles admitidos no item 6.7 da DPC.

6.8. Carimbo de Tempo

Não se aplica.

7. Perfis de Certificado, LCR e OCSP

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 obrigatoriamente atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1. Perfil do Certificado

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

7.1.1. Número de versão

Todos os certificados emitidos pela AC implementa 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 SERPRO RFB SSL A1 descreve todas as extensões de certificado utilizadas e sua criticalidade.

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

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

b) ***"Key Usage"*, crítica**: configurados conforme disposto no item 7.1.2.7 deste documento;

c) ***"Certificate Policies"*, não crítica**: o campo o OID 2.16.76.1.2.1.89 e o endereço URL da página Web https://certificados.serpro.gov.br/acserprorfbssl com a DPC da AC.

Certificados de autenticação de servidor (SSL/TLS) devem conter ainda o OID da política de certificado e identificação dos requisitos do CA/B Forum Guidelines (2.23.140.1.1, se EV SSL; 2.23.140.1.2.2, se OV SSL; 2.23.140.1.3, se EV Code Signing; e 2.23.140.1.4.1, se Baseline Requirement Code Signing);

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

http://certificados2.serpro.gov.br/lcr/acserprorfbssl.crl

http://repositorio.serpro.gov.br/lcr/acserprorfbssl.crl

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

http://repositorio.serpro.gov.br/cadeias/acserprorfbssl.p7b

A segunda entrada contém o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP - http://ocsp.serpro.gov.br/acserprorfbssl- utilizando o protocolo de acesso, HTTP.

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

a) Para certificado de Pessoa Física

Não se aplica.

b) Para certificados de Pessoa Jurídica

Não se aplica.

c) Para certificado de equipamento ou aplicação:

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

OID = 2.16.76.1.3.8. e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;

OID = 2.16.76.1.3.3. e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;

OID = 2.16.76.1.3.2. e conteúdo = nome do responsável pelo certificado;

OID = 2.16.76.1.3.4.e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS,PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

c.2) Para certificados do tipo SSL/TLS, Campo *dNSName*, obrigatório, contendo um ou mais domínios pertencentes ou controlados pelo titular, seguindo as regras definidas na RFC 5280 e RFC 2818, em conformidade com o documento *WebTrust Principles and Criteria for Certification Authorities[7]*.

d) Não se aplica;

e) Não se aplica.

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

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

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

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

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

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

g) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;

h) Não se aplica.

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

a) **“*SubjectAlternativeName*”, não critica,** com o seguinte *OtherName*:

- O campo “rfc822Name” contendo o endereço de email do titular do certificado;
- O campo “DNSName” contendo lista de URLs alternativas indicadas pelo solicitante do certificado, habilitando o certificado para uso com múltiplos domínios. Esta extensão contem pelo menos uma entrada. Cada entrada é uma DNSName contendo o nome de domínio qualificado ou o endereço IP de um servidor. A AC confirma que o requerente controla o nome de domínio ou o endereço IP. FQDNs curinga são permitidos. Não são permitidos neste campo Nome Interno ou IP Reservado;

b) **“*Extended-key-usage*”**, **não critica** contendo os seguintes valores:

“*server authentication*” **(OID = 1.3.6.1.5.5.7.3.1);**

"*client authentication*" **(OID = 1.3.6.1.5.5.7.3.2);**

c)"SignedCertificateTimestampList", (**OID = 1.3.6.1.4.1.11129.2.4.2**) não critica, conteúdo = uma lista SCT (Signed Certificate Timestamp) obtida de servidores confiáveis. Esse mecanismo visa tornar pública a emissão de certificados SSL aos donos de domínios, ACs e usuários por meio do registro da emissão de certificados em Logs que são serviços de rede criptografados e auditáveis.

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 5280.

7.1.2.7. A AC implementa as seguintes extensões, definidas como obrigatórias pela ICP-Brasil.

a) Não se aplica.

b) Para certificados de Autenticação de Servidor(SSL/TLS):

***"Key Usage"*, crítica**: somente os bits digitalSignature, keyEncipherment ou keyAgreement podem estar ativado;

"Extended Key Usage", não crítica: deve conter o propósito *server authentication* **OID = 1.3.6.1.5.5.7.3.1.** Pode conter o propósito *client authentication* **OID = 1.3.6.1.5.5.7.3.2.**

c) Não se aplica.

d) Não se aplica.

e) Não se aplica.

f) Não se aplica.

g) Não se aplica.

7.1.3. Identificadores de algoritmo

Os algoritmos criptográficos utilizados para assinatura dos certificados pela AC são os admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL [1]. Os certificados emitidos pela AC são assinados com o uso do algoritmo criptográfico SHA-256 com função de *hash* (**OID = 1.2.840.113549.1.1.11.**);

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, da seguinte forma:

. Para o certificado de equipamento, o identificador CN conterá o DNS oficial do equipamento:

C = BR

O = ICP-Brasil

OU= Autoridade Certificadora SERPRORFB SSL

OU = Nome da AR responsável pela aprovação do certificado

OU=CNPJ da AR onde ocorreu a identificação presencial

OU = Equipamento A1

CN = nome DNS oficial do equipamento (para servidores WWW)

. Para o certificado de aplicação, o identificador CN conterá o nome da aplicação:

C = BR

O = ICP-Brasil

OU= Autoridade Certificadora SERPRORFB SSL

OU = Nome da AR responsável pela aprovação do certificado

OU=CNPJ da AR onde ocorreu a identificação presencial

OU = Aplicacao A1

CN = nome da aplicação

Para todos os certificados o conteúdo do campo Domínio do Certificado será a identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for seu empregado, funcionário ou servidor.

NOTA: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. O certificado digital emitido para autenticação de servidor(SSL/TLS) deverá adotar o “Distinguished Name”(DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular

S = unidade da federação do endereço físico do titular do certificado

L = cidade do endereço físico do titular

Business Category (OID 2.5.4.15) = tipo de categoria comercial, devendo conter:

“Private Organization” ou “Government Entity” ou “Business Entity” ou “Non-

Commercial Entity”

7.1.5. Restrições de nome

7.1.5.1. Não se aplica.

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

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

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

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

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

O OID **2.16.76.1.2.1.91** foi atribuído a Política de Certificado. Todo certificado emitido segundo esta PC deverá conter, na extensão “*Certificate Policies*”, o OID correspondente.

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 da página *Web* com a DPC da AC a saber:

http://repositorio.serpro.gov.br/docs/dpcacserprorfbssl.pdf http://certificados2.serpro.gov.br/docs/dpcacserprorfbssl.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 de versão

As LCR geradas pela AC segundo a PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. A AC adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

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

b) ***"CRL Number"*, não crítica**: contém número sequencial para cada LCR emitida.

7.2.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

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

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

c) ***"Certificate Policies"*, não crítica**: o campo policyIdentifier contém o **OID 2.16.76.1.2.1.89,** o campo policyQualifiers contém o endereço URL da página *Web* e http://repositorio.serpro.gov.br/docs/dpcserproacfssl.pdf com a DPC da AC;

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

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

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

http://repositorio.serpro.gov.br/cadeias/acserproacfssl.p7b

A segunda entrada contém o método de acesso *id-ad-ocsp*, com o respectivo endereço http://ocsp.serpro.gov.br/acserproacfssl do respondedor OCSP, utilizando o protocolo de acesso, *HTTP*.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Serviços de respostas OCSP implementam a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP

O campo ***"Authority Information Access"*, não critica**, contém o método de acesso id-ad-caIssuer,que utiliza o protocolo de acesso HTTP para a recuperação da cadeia do certificado;

A segunda entrada desse campo contém o método de acesso *id-ad-ocsp*, com o respectivo endereço http://ocsp.serpro.gov.br/acserprorfbssl do respondedor OCSP, utilizando o protocolo de acesso, HTTP e **OID: 1.3.6.1.5.5.7.48.1.**

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC.

9.5. Direitos de Propriedade Intelectual

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

9.6.2. Declarações e Garantias da AR

9.6.3. Declarações e garantias do titular

9.6.4. Declarações e garantias das terceiras partes

9.6.5. Representações e garantias de outros participantes

9.7. Isenção de garantias

9.8. Limitações de responsabilidades

9.9. Indenizações

9.10. Prazo e Rescisão

9.10.1. Prazo

9.10.2. Término

9.10.3. Efeito da rescisão e sobrevivência

9.11. Avisos individuais e comunicações com os participantes

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

Mudança nesta PC será publicado no site da AC.

9.12.3. Circunstâncias na qual o OID deve ser alterado

9.13. Solução de conflitos

9.14. Lei aplicável

9.15. Conformidade com a Lei aplicável

9.16. Disposições Diversas

9.16.1. Acordo completo

Esta PC representa as obrigações e deveres aplicáveis à AC e AR e outras entidades citadas. Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2. Cessão

9.16.3. Independência de disposições

9.16.4. Execução (honorários dos advogados e renúncia de direitos)

9.17. Outras provisões

Toda PC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com este documento, deverá ser verificada a compatibilidade entre a PC e a DPC da AC.

10. DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-03**
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DEPRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇADA ICP-BRASIL	**DOC-ICP-17**
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	**DOC-ICP-12**

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

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	**DOC-ICP-01.01**
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	**DOC-ICP-04.01**

10.3. O documento abaixo se encontra no site da Webtrust: http://webtrust.org que mantém a responsabilidade por sua aprovação/atualização.

Ref.	Nome do documento	Versão
[6]	WebTrust Principles and Criteria for Registration Authorities	**1.0**
[7]	WebTrust Principles and Criteria for Certification Authorities	**2.2**