

RESOLUÇÃO CG ICP-BRASIL Nº 179, DE 20 DE OUTUBRO DE 2020

Aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil – DOC-ICP-04.

O COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6º, §1º, inc. IV, do Regimento Interno, torna público que o COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício das competências previstas no art. 4º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, em plenária por videoconferência realizada em 20 de outubro de 2020,

CONSIDERANDO a determinação estabelecida pelo Decreto nº 10.139, de 28 de novembro de 2019, para revisão e consolidação dos atos normativos inferiores a decreto, editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional,

RESOLVEU:

Art. 1º Esta Resolução aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil.

Art. 2º Fica aprovada a versão 8.1 do documento DOC-ICP-04 – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil, anexa a esta Resolução. ([Redação dada pela Resolução CG ICP-Brasil nº 197, de 2021](#))

Art. 3º Ficam revogadas:

- I - a [Resolução nº 169, de 17 de abril de 2020](#);
- II - a [Resolução nº 150, de 07 de novembro de 2018](#);
- III - a [Resolução nº 138, de 02 de abril de 2018](#);
- IV - a [Resolução nº 103, de 29 de abril de 2014](#);
- V - a [Resolução nº 95, de 27 de setembro de 2012](#);
- VI - a [Resolução nº 91, de 05 de julho de 2012](#);
- VII - a [Resolução nº 87, de 19 de abril de 2012](#);
- VIII - a [Resolução nº 77, de 31 de março de 2010](#);
- IX - a [Resolução nº 53, de 28 de novembro de 2008](#); e
- X - a [Resolução nº 41, de 18 de abril de 2006](#).

Art. 4º Esta Resolução entra em vigor em 03 de novembro de 2020.

THIAGO MEIRELLES FERNANDES PEREIRA



Infraestrutura de Chaves Públicas Brasileira

ANEXO

REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL

DOC-ICP-04

Versão 8.2

(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)

31 de outubro de 2024

(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)



Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

CONTROLE DE ALTERAÇÕES	3
1 INTRODUÇÃO	7
1.1 VISÃO GERAL	7
1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO	8
1.3 PARTICIPANTES DA ICP-BRASIL	9
1.4 USABILIDADE DO CERTIFICADO	9
1.5 POLÍTICA DE ADMINISTRAÇÃO	11
1.6 DEFINIÇÕES E ACRÔNIMOS	11
2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	12
3 IDENTIFICAÇÃO E AUTENTICAÇÃO	13
4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	13
5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES	16
6 CONTROLES TÉCNICOS DE SEGURANÇA	17
6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	17
6.2 PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO	20
6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	22
6.4 DADOS DE ATIVAÇÃO	22
6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL	23
6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA	23
6.7 CONTROLES DE SEGURANÇA DE REDE	24
6.8 CARIMBO DO TEMPO	24
7 PERFIS DE CERTIFICADO, LCR E OCSP	24
7.1 PERFIL DO CERTIFICADO	24
7.2 PERFIL DE LCR	27
7.3 PERFIL DE OCSP	27
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	27
9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS	28
10 DOCUMENTOS REFERENCIADOS	31
11 REFERÊNCIAS BIBLIOGRÁFICAS	31
ANEXO I - TABELA DE PERFIS DE CERTIFICADO E LCR	32



Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 211, de 31.10.2024 Versão 8.2	1.1.5 a 1.1.12, 1.2.1, 1.2.2, 1.4.1.4 a 1.4.1.7, 1.4.2.1 a 1.4.2.3, 6.1.1.8 (tabela), 6.3.2.3 (tabela), 7.1.2, 7.1.4.1, 7.1.4.2 e 7.2.2	Pauta modernizante. Alteração dos tipos de certificados digitais e seus perfis. Inclusão do Anexo I - Tabela de Perfis de Certificado e LCR.
Resolução nº 197, de 16.11.2021 Versão 8.1	7.1.4.1	Regulamentação dos procedimentos e requisitos técnicos para a operacionalização de Autoridade de Registro Eletrônica na ICP-Brasil.
Resolução nº 196, de 16.11.2021 Versão 8.1	6.3.2.4, 6.3.2.5 e 7.1.2.3 c)	Atualização dos requisitos Webtrust
Resolução 179, de 20.09.2020 Versão 8.0		Revisão e consolidação do DOC-ICP-04, conforme Decreto nº 10.139, de 28 de novembro de 2019. Ajustes para emissão por meio de videoconferência.
Resolução 169, de 17.04.2020 Versão 7.2	7.1.4.1	Inclui no certificado digital a informação de como foi realizada a identificação do titular.
Resolução 156, de 07.02.2020 Versão 7.1	7.1.2.3.a.2), 7.1.2.4.d	Alteração nos procedimentos para emissão de certificados digitais pelos conselhos de classes profissionais instituídos por lei.
Resolução 151, de 30.05.2019 Versão 7.0		Aprova a versão 7.0 do DOC-ICP-04.
Resolução 150, de 07.11.2018 Versão 6.7	7.1.4.1,	Inclui no certificado digital o CNPJ da Autoridade de Registro onde ocorreu a identificação presencial.
Resolução 141, de 03.07.2018 Versão 6.6	7.1.2.3-a	Incluir os servidores públicos dos estados e do Distrito Federal nos procedimentos específicos de emissão de certificados digitais.



Infraestrutura de Chaves Públicas Brasileira

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 139, de 03.07.2018 Versão 6.6	1.1.3, 1.1.7A, 1.1.8, 1.2.2, 1.3.5.8, 6.1.1.1.2, 6.1.1.7, 6.1.8, 6.2.4.1, 6.3.2.3, 7.1.2.3, Tabela do Anexo I	Criação da Política de Certificado para Objetos Metrológicos – OM-BR no âmbito da ICP-Brasil.
Resolução 138, de 02.04.2018 Versão 6.5	7.1.2.3 e 7.1.2.4	Alteração da extensão " <i>subject alternative name</i> " para certificados de equipamento A CF-e-SAT.
Resolução 132, de 10.11.2017 Versão 6.4	1.3.3A, 6.2.4.2	Institui o Prestador de Serviço de Confiança.
Resolução 128, de 13.09.2017 Versão 6.3	7.1.2.3.c	Obriga certificados do tipo SSL/TLS a incluírem o Campo <i>dNSName</i> da extensão <i>Subject Alternative Name</i> .
Resolução 124, de 13.09.2017 Versão 6.3	7.1.2.8	Retira a proibição de certificados A CF-e-SAT de implementar a extensão <i>Extended Key Usage</i> .
Resolução 119, 121 e 123, de 06.07.2017 Versão 6.2	7.1.2.2.e, 7.1.2.3.a.4 e 6.1.1 Tabela 4 e Anexo I	Obrigações de resposta OCSP para certificados de autenticação de servidor (SSL/TLS). Inclui a previsão para certificados para servidor público federal e militar. Atualiza tabela de mídias armazenadoras de chaves criptográficas e tabela Comparativa de Requisitos Mínimos por Tipo de Certificado.
Resolução 118, de 09.12.2015 Versão 6.1	7.1.2.2 7.2.2.2.c	Previsão de dois pontos para obtenção da LCR. Retirada do campo AIA da LCR.
Resolução 115, de 11.11.2015 Versão 6.0	1.1.3, 1.1.7, 1.1.8, tabela 3, 1.3.5.7, 6.1.1.1.1, tabela 4, tabela 5, 6.2.4.1, tabela 6, 7.1.2.3, 7.1.2.8 e anexo I.	Cria nova política de certificado A CF-e-SAT.



Infraestrutura de Chaves Públicas Brasileira

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 103, de 29.04.2014 Versão 5.3	7.1.2.2-e; 7.1.2.7; 7.1.2.3-a.a1.i; 7.1.2.3-b.i; 7.1.2.4-f.	Esclarece uso da extensão ExtendedKeyUsage nos certificados de usuário final e ajusta o campo de RG na extensão “Subject Alternative Name”.
Resolução 99, de 09.10.2013 Versão 5.2	Tabela 6 item 6.3.2.3; Tabela do Anexo I.	Amplia prazo de validade de certificados das hierarquias da ICP-Brasil que implementam exclusivamente algoritmos de curvas elípticas.
Resolução 95, de 27.09.2012 Versão 5.1	Tabela 4 do item 6.1.1.7; Tabela do Anexo I.	Adequação das exigências vinculadas aos equipamentos, para certificados do tipo T3 e T4.
Resolução 91, de 05.07.2012 Versão 5.0	Tabela 6 do item 6.3.2.3; Tabela do Anexo I; alíneas “iii” do subitem “b” e “ii” do subitem “c”, do item 7.1.2.3	Alteração do Período máximo de Validade dos Certificados A3, S3, T3 para 5 anos e do Tamanho (bits) da Chave Criptográfica. Inclusão das 14 pos. no CNPJ para o OID 2.16.76.1.3.3.
Resolução 87, de 17.04.2010 Versão 4.0	7.1.2.3-a; Tabela 4 do item 6.1.1.7; Tabela 6 do item 6.3.2.3; Tabela do Anexo I.	Ajuste em redação para campos otherName e alteração de validade de certificados de tipo A4, S4 e T4 para 6 anos, com restrição de armazenamento em hardware criptográfico.
Resolução 84, de 18.11.2010 Versão 3.2	7.1.2.3-a	Inclusão de campo <i>otherName</i> , obrigatório para certificado vinculado ao RIC.
Resolução 77, de 31.03.2010 Versão 3.1	7.1.2.2-e, 7.1.2.2-f, 7.2.2.2-c	Inclusão do campo de extensão de Authority Information Access.
Resolução 53, de 19.11.2008 Versão 3.0	1.1.3, 1.1.6, 1.2.2, 1.3.5.6, 6.1.1.7, 6.1.8, 6.2.4.1, 6.3.2.3, 7.1.2.2, 7.1.4.2, Anexo I	Inclusão de referências a Carimbo do Tempo.
	7.1.2.4	Inclusão do formato PRINTABLE STRING como alternativa ao formato OCTET STRING para



Infraestrutura de Chaves Públicas Brasileira

Ato que aprovou a alteração	Item alterado	Descrição da alteração
		armazenamento das informações definidas nos campos otherName.
Resolução 41, de 18.04.2006 Versão 2.0	Diversos	Consolidação de documentos anteriores.
Resolução 07, de 12.12.2001 Versão 1.0	Diversos	Criação do DOC-ICP-04.



Infraestrutura de Chaves Públicas Brasileira

1 INTRODUÇÃO

1.1 Visão Geral

- 1.1.1 Este documento estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras – AC integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de suas Políticas de Certificado (PC).
- 1.1.2 Toda PC elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.
- 1.1.3 A estrutura desta PC está baseada na RFC 3647.
- 1.1.4 Este documento compõe o conjunto da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.
- 1.1.5 São 10 (dez) os tipos de certificados digitais para usuários finais da ICP-Brasil: [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - A3 [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - A4 [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - SE-S [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - SE-H [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - T3 [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - T4 [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - AE-S [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - AE-H [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - A CF-e-SAT [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
 - OM-BR [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.1.6 Certificados do tipo A3 e A4 são certificados de assinatura e devem ser emitidos exclusivamente para pessoas físicas. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.1.7 Certificados do tipo SE-S e SE-H são certificados de selo eletrônico, respectivamente em software e em hardware, e devem ser emitidos apenas para pessoas jurídicas. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.1.8 Certificados do tipo T3 e T4 somente devem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo - ACTs credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4



Infraestrutura de Chaves Públicas Brasileira

estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

- 1.1.9 Certificados do tipo AE-S e AE-H são certificados de aplicações específicas, respectivamente em software e em hardware, e devem ser emitidos pelas ACs para equipamentos, servidores, aplicações e dispositivos IOT. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.1.10 Certificados do tipo A CF-e-SAT devem ser emitidos apenas para equipamentos integrantes do Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico - SAT-CF-e, seguindo a regulamentação do CONFAZ. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.1.11 Certificados do tipo Objeto Metrológico - OM-BR devem ser emitidos apenas para equipamentos metrológicos regulados pelo Inmetro. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.1.12 Outros tipos de certificado, além dos anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescidas aos tipos de certificados aceitos pela ICP-Brasil. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

1.2 Nome do documento e identificação

- 1.2.1 Neste item deve ser identificada a PC e indicado, no mínimo, o tipo de certificado a que está associada. Exemplo: “Política de Certificado de Assinatura Digital, tipo A3, do(a) <nome da instituição>”. O OID (*Object Identifier*) da PC deve também ser incluído neste item. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.2.2 No âmbito da ICP-Brasil, os OIDs das PCs serão atribuídos na conclusão do processo de credenciamento da AC, conforme a Tabela 3 a seguir:

Tabela 3 - OID de PC na ICP-Brasil

(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)

Tipo de Certificado	OID
A3	2.16.76.1.2.3.n
A4	2.16.76.1.2.4.n
SE-S	2.16.76.1.2.201.n
SE-H	2.16.76.1.2.202.n
T3	2.16.76.1.2.303.n
T4	2.16.76.1.2.304.n



Infraestrutura de Chaves Públicas Brasileira

AE-S	2.16.76.1.2.401.n
AE-H	2.16.76.1.2.402.n
A CF-e-SAT	2.16.76.1.2.500.n
OM-BR	2.16.76.1.2.550.n

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

1.3.1.1 Neste item deve ser identificada a AC integrante da ICP-Brasil que implementa a PC.

1.3.1.2 Deve também ser identificado o documento Declaração de Práticas de Certificação (DPC) dessa AC, onde estarão descritas suas práticas e procedimentos de certificação.

1.3.2 Autoridades de Registro

1.3.2.1 Neste item deve ser identificado o endereço da página web (URL) onde estão publicados os dados a seguir, referentes às Autoridades de Registro (AR) utilizadas pela AC para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

- relação de todas as ARs credenciadas;
- relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3 Titulares do Certificado

Neste item devem ser caracterizadas as entidades (pessoas físicas ou jurídicas, equipamentos ou aplicações) que poderão ser titulares dos certificados emitidos segundo a PC.

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

Neste item deve ser identificado o endereço da página web (URL) onde está publicada a relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC, vinculados à AC responsável.

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

1.4.1.1 Neste item devem ser relacionadas as aplicações para as quais os certificados definidos pela PC são adequados.



Infraestrutura de Chaves Públicas Brasileira

- 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 Na definição das aplicações para o certificado definido pela PC, a AC responsável deve 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 do tipo A3 e A4 serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.4.1.5 Certificados do tipo SE-S e SE-H serão utilizados para garantir origem e integridade de um documento eletrônico, servindo de prova da emissão do documento por uma pessoa jurídica. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.4.1.6 Certificados do tipo T3 e T4 serão utilizados em aplicações mantidas por Autoridades de Carimbo do Tempo credenciadas na ICP-Brasil para assinatura de carimbos do tempo. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.4.1.7 Certificados de tipo A CF-e-SAT serão utilizados exclusivamente em equipamentos para assinatura de Cupom Fiscal Eletrônico – CF-e por meio do Sistema de Autenticação e Transmissão de Cupom Fiscal Eletrônico – SAT-CF-e.
- 1.4.1.8 Certificados do tipo OM-BR serão utilizados exclusivamente em equipamentos metrológicos regulamentados pelo Inmetro
- 1.4.1.9 Certificados do tipo AE-S e AE-H serão utilizados em equipamentos, servidores, aplicações e dispositivos IOT, entre entidades dentro de um ecossistema fechado, onde as autenticações são mútuas e limitadas aos intervenientes conhecidos. [\(Incluído pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

1.4.2 Uso proibitivo do certificado

- 1.4.2.1 É proibido o uso do certificado de aplicações específicas com a finalidade de autenticação de servidor (SSL/TLS) destinado ao reconhecimento confiável pelos navegadores de internet (browsers). [\(Incluído pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.4.2.2 É proibido o uso do certificado de selo eletrônico para assinatura digital com o propósito de manifestação de vontade. [\(Incluído pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 1.4.2.3 Neste item devem ser relacionadas, quando cabível, outras aplicações para as quais existem restrições ou proibições para o uso desses certificados. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)



Infraestrutura de Chaves Públicas Brasileira

1.5 Política de Administração

Neste item devem ser incluídos nome, endereço e outras informações da AC responsável pela PC. Devem ser também informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC.

1.5.2 Contatos

Endereço:

Telefone:

Fax:

Página web:

E-mail:

Outros:

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome:

Telefone:

E-mail:

Outros:

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 ICP-Brasil.

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CMM-SEI	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>
CN	<i>Common Name</i>



Infraestrutura de Chaves Públicas Brasileira

SIGLA	DESCRIÇÃO
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	<i>Code Signing</i>
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
EV	<i>Extended Validation</i>
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	<i>International Electrotechnical Commission</i>
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	<i>International Organization for Standardization</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	<i>Online Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OM-BR	Objetos Metrológicos ICP-Brasil
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SSL	<i>Secure Socket Layer</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Locator</i>

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

- **2.1 Repositórios**
- **2.2 Publicação de informações dos certificados**
- **2.3 Tempo ou Frequência de Publicação**
- **2.4 Controle de Acesso aos Repositórios**



Infraestrutura de Chaves Públicas Brasileira

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

- **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**
- **3.2.4 Autenticação da identidade de um indivíduo**
- **3.2.5 Informações não verificadas do titular do certificado**
- **3.2.6 Validação das autoridades**
- **3.2.7 Critérios para interoperação**
- **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

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

- **4.1 Solicitação do certificado**
- **4.1.1 Quem pode submeter uma solicitação de certificado**
- **4.1.2 Processo de registro e responsabilidades**
- **4.2 Processamento de Solicitação de Certificado**
- **4.2.1 Execução das funções de identificação e autenticação**



Infraestrutura de Chaves Públicas Brasileira

- 4.2.2 Aprovação ou rejeição de pedidos de certificado
- 4.2.3 Tempo para processar a solicitação de certificado
- 4.3 Emissão de Certificado
- 4.3.1 Ações da AC durante a emissão de um certificado
- 4.3.2 Notificações para o titular do certificado pela AC na emissão do certificado
- 4.4 Aceitação de Certificado
- 4.4.1 Conduta sobre a aceitação do certificado
- 4.4.2 Publicação do certificado pela AC
- 4.4.3 Notificação de emissão do certificado pela AC Raiz para outras entidades
- 4.5 Usabilidade do par de chaves e do certificado
- 4.5.1 Usabilidade da Chave privada e do certificado do titular
- 4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis
- 4.6 Renovação de Certificados
- 4.6.1 Circunstâncias para renovação de certificados
- 4.6.2 Quem pode solicitar a renovação
- 4.6.3 Processamento de requisição para renovação de certificados
- 4.6.4 Notificação para nova emissão de certificado para o titular
- 4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado
- 4.6.6 Publicação de uma renovação de um certificado pela AC
- 4.6.7 Notificação de emissão de certificado pela AC para outras entidades
- 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
- 4.8.3 Processamento de requisição de modificação de certificado



Infraestrutura de Chaves Públicas Brasileira

- **4.8.4 Notificação de emissão de novo certificado para o titular**
- **4.8.5 Conduta constituindo a aceitação de uma modificação de certificado**
- **4.8.6 Publicação de uma modificação de certificado pela AC**
- **4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades**
- **4.9 Suspensão e Revogação de Certificado**
- **4.9.1 Circunstâncias para revogação**
- **4.9.2 Quem pode solicitar revogação**
- **4.9.3 Procedimento para solicitação de revogação**
- **4.9.4 Prazo para solicitação de revogação**
- **4.9.5 Tempo em que a AC deve processar o pedido de revogação**
- **4.9.6 Requisitos de verificação de revogação para as partes confiáveis**
- **4.9.7 Frequência de emissão de LCR**
- **4.9.8 Latência máxima para a LCR**
- **4.9.9 Disponibilidade para revogação/verificação de status on-line**
- **4.9.10 Requisitos para verificação de revogação on-line**
- **4.9.11 Outras formas disponíveis para divulgação de revogação**
- **4.9.12 Requisitos especiais para o caso de comprometimento de chave**
- **4.9.13 Circunstâncias para suspensão**
- **4.9.14 Quem pode solicitar suspensão**
- **4.9.15 Procedimento para solicitação de suspensão**
- **4.9.16 Limites no período de suspensão**
- **4.10 Serviços de status de certificado**
- **4.10.1 Características operacionais**
- **4.10.2 Disponibilidade dos serviços**
- **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**



Infraestrutura de Chaves Públicas Brasileira

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

- **5.1 Controles físicos**
- **5.1.1 Construção e localização das instalações de AC**
- **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) para AC**
- **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**
- **5.2.4 Funções que requerem separação de deveres**
- **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**
- **5.4 Procedimentos de Log de Auditoria**
- **5.4.1 Tipos de eventos registrados**
- **5.4.2 Frequência de auditoria de registros**
- **5.4.3 Período de retenção para registros de auditoria**
- **5.4.4 Proteção de registros de auditoria**



Infraestrutura de Chaves Públicas Brasileira

- 5.4.5 Procedimentos para cópia de segurança (Backup) de registros de auditoria
- 5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)
- 5.4.7 Notificação de agentes causadores de eventos
- 5.4.8 Avaliações de vulnerabilidade
- 5.5 Arquivamento de Registros
- 5.5.1 Tipos de registros arquivados
- 5.5.2 Período de retenção para arquivo
- 5.5.3 Proteção de arquivo
- 5.5.4 Procedimentos de cópia de arquivo
- 5.5.5 Requisitos para datação de registros
- 5.5.6 Sistema de coleta de dados de arquivo (interno e externo)
- 5.5.7 Procedimentos para obter e verificar informação de arquivo
- 5.6 Troca de chave
- 5.7 Comprometimento e Recuperação de Desastre
- 5.7.1 Procedimentos gerenciamento de incidente e comprometimento
- 5.7.2 Recursos computacionais, software, e/ou dados corrompidos
- 5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade
- 5.7.4 Capacidade de continuidade de negócio após desastre
- 5.8 Extinção da AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC deve definir as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC. Devem também ser 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

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.



Infraestrutura de Chaves Públicas Brasileira

- 6.1.1.1.1 Para certificados do tipo A CF-e-SAT, o titular do certificado será o contribuinte, que fará a solicitação do certificado A CF-e-SAT com uso de certificado digital ICP-Brasil de pessoa jurídica válido e correspondente ao mesmo CNPJ para o qual está autorizado pela unidade fiscal federada, associado ao número de série do equipamento SAT.
- 6.1.1.1.2 Para certificados do tipo OM-BR, o titular do certificado será o fabricante, que fará a solicitação do certificado OM-BR com uso de certificado digital ICP-Brasil de pessoa jurídica válido, do fabricante autorizado pelo Inmetro.
- 6.1.1.2 Neste item, a PC deve descrever todos os requisitos e procedimentos referentes ao processo de geração de chaves aplicável ao certificado que define.
- 6.1.1.3 Neste item, a PC deve indicar o algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.
- 6.1.1.4 Ao ser gerada, a chave privada da entidade titular deverá ser gravada cifrada, por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme a Tabela 4 a seguir.
- 6.1.1.5 A chave privada deverá trafegar 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 deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.
- 6.1.1.8 O armazenamento de chaves privadas por terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos dos REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL[1], 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.



Infraestrutura de Chaves Públicas Brasileira

Tabela 4 – Mídias Armazenadoras de Chaves Criptográficas

(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
SE-S e AE-S	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima.
A3, A4, SE-H, T3, T4, AE-H e OM-BR	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: para certificados do tipo A CF-e-SAT, T3 e T4, a exigência de homologação ou certificação das mídias para geração e armazenamento de chaves criptográficas fica suspensa até ulterior deliberação do Comitê Gestor da ICP-Brasil.

6.1.2 Entrega da chave privada à entidade

Item não aplicável.

6.1.3 Entrega da chave pública para emissor de certificado

A PC deve detalhar os procedimentos utilizados para a entrega da chave pública de titular de certificado à AC responsável. Nos casos em que houver solicitação de certificado pelo seu titular ou por AR vinculada, deverá ser adotado formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.4 Entrega de chave pública da AC às terceiras partes

Neste item, a PC deve definir as formas para a disponibilização do certificado da AC responsável, e de todos os certificados de sua cadeia de certificação, para os usuários da ICP-Brasil, formas essas que poderão compreender, entre outras:

- no momento da disponibilização de um certificado para seu titular; usando formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil;
- diretório;
- página web da AC; e
- outros meios seguros aprovados pelo CG ICP-Brasil.

6.1.5 Tamanhos de chave



Infraestrutura de Chaves Públicas Brasileira

- 6.1.5.1 Este item deve definir o tamanho das chaves criptográficas associadas aos certificados emitidos segundo a PC.
- 6.1.5.2 Os algoritmos e os tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros

A PC deve prever que os parâmetros de geração e verificação de chaves assimétricas das entidades titulares de certificados adotarão o padrão estabelecido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

Neste item, a PC deve especificar os propósitos para os quais poderão ser utilizadas as chaves criptográficas dos titulares de certificados, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes (item 1.4).

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

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

6.2.1 Padrões e controle para módulo criptográfico

- 6.2.1.1 Neste item, quando cabíveis, devem ser especificados os padrões requeridos para os módulos de geração de chaves criptográficas, observados os padrões definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.
- 6.2.1.2 Este item da PC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado. Poderão ser indicados padrões de referência, observados os padrões definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2 Controle “n de m” para chave privada

Item não aplicável.

6.2.3 Custódia (*escrow*) de chave privada

Neste item a PC deve identificar quem é o agente de recuperação (*escrow*), qual forma que a chave é recuperada (por exemplo, inclui o texto em claro, encriptado, por divisão de chaves) e quais são os controles de segurança do sistema de recuperação.

6.2.4 Cópia de segurança de chave privada



Infraestrutura de Chaves Públicas Brasileira

- 6.2.4.1 Com exceção das chaves privadas vinculadas a certificados do tipo A CF-e-SAT, OM-BR, T3 e T4, que não podem possuir cópia de segurança, qualquer titular de certificado dos demais tipos poderá, a seu critério, manter cópia de segurança de sua própria chave privada.
- 6.2.4.2 A AC responsável pela PC não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.
- 6.2.4.3 Em qualquer caso, a cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil e protegida com um nível de segurança não inferior àquele definido para a chave original.
- 6.2.4.4 Além das observações acima, a PC deve descrever todos os requisitos e procedimentos aplicáveis ao processo de geração de uma cópia de segurança.

6.2.5 Arquivamento de chave privada

- 6.2.5.1 Neste item de uma PC que defina certificados de sigilo, devem ser descritos, quando cabíveis, os requisitos para arquivamento de chaves privadas. Não devem ser arquivadas chaves privadas de assinatura digital.
- 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

Neste item, quando aplicáveis, devem ser definidos os requisitos para inserção da chave privada de titular em módulo criptográfico.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8 Método de ativação de chave privada

Neste item da PC devem ser descritos os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular. Devem ser definidos os agentes autorizados a ativar essa chave, o método de confirmação da identidade desses agentes (senhas, tokens ou biometria) e as ações necessárias para a ativação.

6.2.9 Método de desativação de chave privada

Neste item da PC devem ser descritos os requisitos e os procedimentos necessários para desativação da chave privada de entidade titular. Devem ser definidos os agentes autorizados, o método de confirmação da identidade desses agentes e as ações necessárias.

6.2.10 Método de destruição de chave privada

Neste item da PC devem ser descritos os requisitos e os procedimentos necessários para destruição da chave privada de titular e de suas cópias de segurança. Devem ser definidos os agentes autorizados,



Infraestrutura de Chaves Públicas Brasileira

o método de confirmação da identidade desses agentes e as ações necessárias, tais como destruição física, sobrescrita ou apagamento das mídias de armazenamento.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A PC deve prever que as chaves públicas de titulares dos certificados de assinatura digital e as LCR serão armazenadas pela AC emissora, 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 Caso a PC se refira a certificados de assinatura digital, ela deve prever que as chaves privadas dos respectivos titulares deverão ser utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Caso a PC se refira a certificados de sigilo, ela deve definir os períodos de uso das chaves correspondentes.

6.3.2.3 A Tabela 6, a seguir, define os períodos máximos de validade admitidos para cada tipo de certificado previsto pela ICP-Brasil:

Tabela 6 – Períodos de Validade dos Certificados
(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)

Tipo de Certificado	Período Máximo de Validade do Certificado (em anos)
SE-S e AE-S	1
A3, SE-H, AE-H e T3	5
A4 e T4	11 (para cadeias hierárquicas completas em Curvas Elípticas)
	6 (para as demais hierarquias)
A CF-e-SAT	5
OM-BR	10

6.4 Dados de Ativação

Nos itens seguintes da PC devem ser descritos os requisitos 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.



Infraestrutura de Chaves Públicas Brasileira

6.4.1 Geração e instalação dos dados de ativação

A PC deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão únicos e aleatórios.

6.4.2 Proteção dos dados de ativação

A PC deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão protegidos contra uso não autorizado.

6.4.3 Outros aspectos dos dados de ativação

Neste item, quando for o caso, devem ser definidos outros aspectos referentes aos dados de ativação. Entre esses outros aspectos podem ser considerados alguns daqueles tratados, em relação às chaves, nos itens de 6.1 a 6.3.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

A PC deve descrever os requisitos de segurança computacional do equipamento onde serão gerados os pares de chaves criptográficas dos titulares de certificados, observados os requisitos gerais previstos na DPC.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

Caso a AC responsável exija um software específico para a utilização dos certificados emitidos segundo a PC, nos itens seguintes devem ser descritos os controles implementados no desenvolvimento e no gerenciamento de segurança referentes a esse software.

6.6.1 Controles de desenvolvimento de sistema

Neste item da PC devem ser abordados aspectos tais como: segurança do ambiente e do pessoal de desenvolvimento, práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros.

6.6.2 Controles de gerenciamento de segurança

Neste item devem ser descritos os procedimentos e as ferramentas empregados para garantir que o software e seu ambiente operacional implementem os níveis configurados de segurança.

6.6.3 Controles de segurança de ciclo de vida

Neste item deve ser informado, quando disponível, o nível de maturidade atribuído ao ciclo de vida do software, com base em critérios como: *Trusted Software Development Methodology* (TSDM) ou o *Capability Maturity Model do Software Engineering Institute* (CMM-SEI).



Infraestrutura de Chaves Públicas Brasileira

6.6.4 Controles na Geração de LCR

Antes de publicadas, todas as LCRs geradas pela AC devem ser 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

Caso o ambiente de utilização do certificado definido pela PC exija controles específicos de segurança de rede, esses controles devem ser descritos neste item da PC, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

6.8 Carimbo do Tempo

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL[2].

7 PERFIS DE CERTIFICADO, LCR E OCSP

Os itens seguintes devem especificar os formatos dos certificados e das LCR/OCSP gerados segundo a PC. Devem ser incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes deverão ser 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 responsável, segundo a PC, deverão estar 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 responsável, segundo a PC, deverão implementar a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

7.1.2.1 Neste item, a PC deve descrever todas as extensões de certificado utilizadas e sua criticalidade, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I deste documento. ([Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024](#))

7.1.2.2 Os campos otherName devem estar de acordo com as seguintes especificações: ([Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024](#))



Infraestrutura de Chaves Públicas Brasileira

- 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; (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)
- b) quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CNO ou CAEPF não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero"; (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)
- c) se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF; (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)
- d) quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional; (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)
- e) 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; (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)
- 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; (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)
- 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; (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)
- h) quando o número da inscrição estadual e o número da inscrição municipal da pessoa jurídica emissora do CF-e-SAT não estiverem disponíveis não precisam ser preenchidos. (Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024)

7.1.2.3 Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

7.1.2.4 Os outros campos que compõem a extensão "*Subject Alternative Name*" poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

7.1.2.5 Todas as informações utilizadas para preenchimento dos campos do certificado devem ser verificadas. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

7.1.3 Identificadores de algoritmo

Neste item da PC deve ser indicado o OID (*Object Identifier*) do algoritmo criptográfico utilizado para assinatura do certificado, observados os algoritmos admitidos no âmbito da ICP-Brasil conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.



Infraestrutura de Chaves Públicas Brasileira

7.1.4 Formatos de nome

- 7.1.4.1 O nome do titular do certificado, constante do campo “*Subject*”, deverá adotar o “*Distinguished Name*” (DN) do padrão ITU X.500/ISO 9594, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I deste documento. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)
- 7.1.4.2 Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

7.1.5 Restrições de nome

- 7.1.5.1 Neste item da PC, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados.
- 7.1.5.2 A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:
- não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e
 - além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

Tabela 7 - Caracteres especiais admitidos em nomes

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



Infraestrutura de Chaves Públicas Brasileira

7.1.6 OID (*Object Identifier*) da PC

Neste item, deve ser informado o OID atribuído à PC. Todo certificado emitido segundo a PC deverá conter, na extensão “*Certificate Policies*”, o OID correspondente.

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 a PC, o campo *policyQualifiers* da extensão “*Certificate Policies*” deverá conter o endereço *Web* (URL) da DPC da AC responsável.

7.1.9 Semântica de processamento para as extensões críticas de PC

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela AC responsável, segundo a PC, deverão implementar 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 Neste item, a PC deve descrever todas as extensões de LCR utilizadas e sua criticalidade, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I deste documento. [\(Redação dada pela Resolução CG ICP-Brasil nº 211, de 2024\)](#)

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

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

7.3.2 Extensões de OCSP

Se implementado, deve estar em conformidade com a RFC 6960.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPC da AC responsável, ou detalhados aspectos específicos para a PC, se houver.

- **8.1 Frequência e circunstâncias das avaliações**
- **8.2 Identificação/Qualificação do avaliador**



Infraestrutura de Chaves Públicas Brasileira

- **8.3 Relação do avaliador com a entidade avaliada**
- **8.4 Tópicos cobertos pela avaliação**
- **8.5 Ações tomadas como resultado de uma deficiência**
- **8.6 Comunicação dos resultados**

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens correspondentes à lista abaixo devem ser referidos os itens correspondentes da DPC da AC responsável, ou detalhados aspectos específicos para a PC, se houver. Os itens seguintes com requisitos especificados devem ser atendidos.

- **9.1 Tarifas**
 - **9.1.1 Tarifas de emissão e renovação de certificados**
 - **9.1.2 Tarifas de acesso ao certificado**
 - **9.1.3 Tarifas de revogação ou de acesso à informação de status**
 - **9.1.4 Tarifas para outros serviços**
 - **9.1.5 Política de reembolso**
- **9.2 Responsabilidade Financeira**
 - **9.2.1 Cobertura do seguro**
 - **9.2.2 Outros ativos**
 - **9.2.3 Cobertura de seguros ou garantia para entidades finais**
- **9.3 Confidencialidade da informação do negócio**
 - **9.3.1 Escopo de informações confidenciais**
 - **9.3.2 Informações fora do escopo de informações confidenciais**
 - **9.3.3 Responsabilidade em proteger a informação confidencial**
- **9.4 Privacidade da informação pessoal**
 - **9.4.1 Plano de privacidade**
 - **9.4.2 Tratamento de informação como privadas**
 - **9.4.3 Informações não consideradas privadas**
 - **9.4.4 Responsabilidade para proteger a informação privadas**
 - **9.4.5 Aviso e consentimento para usar informações privadas**
 - **9.4.6 Divulgação em processo judicial ou administrativo**
 - **9.4.7 Outras circunstâncias de divulgação de informação**
- **9.5 Direitos de Propriedade Intelectual**
- **9.6 Declarações e Garantias**



Infraestrutura de Chaves Públicas Brasileira

- **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**
- **9.12.3 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**
- **9.16.2 Cessão**
- **9.16.3 Independência de disposições**
- **9.16.4 Execução (honorários dos advogados e renúncia de direitos)**

9.12.1 Procedimento para emendas

Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na PC. Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2 Mecanismo de notificação e períodos

Neste item devem ser descritos os mecanismos empregados para a distribuição da PC à comunidade envolvida.

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 ICP-Brasil, prevalecerá sempre a última editada.



Infraestrutura de Chaves Públicas Brasileira

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 responsável.



Infraestrutura de Chaves Públicas Brasileira

10 DOCUMENTOS REFERENCIADOS

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.it.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 DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL Aprovado pela Resolução nº 132, de 10 de novembro de 2017	DOC-ICP-17
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	DOC-ICP-12
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03

11 REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3647, IETF - *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, november 2003.

RFC 5280, IETF - *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, may 2008.

RFC 2818, IETF - *HTTP Over TLS*, may 2000.

RFC 6960, IETF - *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, june 2003.



Infraestrutura de Chaves Públicas Brasileira

ANEXO I - TABELA DE PERFIS DE CERTIFICADO E LCR

(Incluído pela Resolução CG ICP-Brasil nº 211, de 2024)

1. Detalhamento dos campos e extensões dos Certificados de Assinatura Digital para Pessoa Física

Campo	Valor	Presença	Criticalidade	Comentário
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos	O	-	
3. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil CN = <Nome Civil> serialNumber = <número CPF>	O	-	Outros atributos poderão ser utilizados na forma e propósitos definidos conforme RFC5280. OID 2.5.4.5 – serialNumber , conforme ETSI EN 319 412-2 V2.3.1 (2023-09).
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
8. Extensões X.509v3		-	-	Outros campos de extensão poderão ser utilizados na forma e propósitos definidos conforme RFC5280.
8.1. <i>Authority Key Identifier</i>	<i>Hash</i> 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2. <i>Subject Key Identifier</i>	<i>Hash</i> 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
8.3. <i>Key Usage</i>	<i>digitalSignature</i>	O	crítica	
	<i>keyEncipherment</i>	P		
	<i>nonRepudiation</i>	P		
8.4. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o OID da PC correspondente ao certificado	O	não-crítica	
	<i>Policyqualifiers</i> OID 1.3.6.1.5.5.7.2.1			
	<i>cPSuri</i> : URI do endereço web da DPC da AC emitente			
8.5. <i>Subject Alternative Name</i>	OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF	O*	não-crítica	(*) A obrigatoriedade com restrição implica recomendação de manutenção desse <i>otherName</i> de forma provisória, até 31/12/2028, com o propósito de possibilitar que todas as aplicações possam ser ajustadas para obtenção dessa informação pelo atributo <i>serialNumber</i> (OID 2.5.4.5), do campo DN do titular. Após 31/12/2028, fica opcional o uso desse <i>otherName</i> .
	OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do	P	não-crítica	Outros <i>otherNames</i> podem ser utilizados, conforme definido no



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
	Cadastro Específico do INSS (CEI) da pessoa física titular do certificado			ADE-ICP-04.01.
8.6. <i>Basic Constraints</i>	cA = False	O	crítica	
8.7. <i>Extended Key Usage</i>	<i>Client authentication</i> OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	
	<i>E-mail protection</i> OID = 1.3.6.1.5.5.7.3.4	P		
8.8. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	Deve conter mais de uma entrada para endereços onde se obtém a LCR.
	<i>reasons</i>	N		
	<i>cRLIssuer</i>	N		
8.9. <i>Authority Information Access</i>	<i>id-ad-caIssuer</i> do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	<i>id-ad-ocsp</i> do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

2. Detalhamento dos campos e extensões dos Certificados de Selo Eletrônico para Pessoa Jurídica

Campo	Valor	Presença	Criticalidade	Comentário/Referência
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos.	O	-	
3. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.	O	-	DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil CN = <Razão Social> <i>serialNumber</i> = <número CNPJ>	O	-	Outros atributos poderão ser utilizados na forma e propósitos definidos conforme RFC5280. ETSI EN 319 412-3 V1.3.1 (2023-09).
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário/Referência
8. Extensões X.509v3		-	-	Outros campos de extensão poderão ser utilizados na forma e propósitos definidos conforme RFC5280.
8.1. <i>Authority Key Identifier</i>	<i>Hash</i> 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2. <i>Subject Key Identifier</i>	<i>Hash</i> 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
8.3. <i>Key Usage</i>	<i>digitalSignature</i>	O	crítica	
	<i>keyEncipherment</i>	P		
	<i>nonRepudiation</i>	P		
8.4. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o OID da PC correspondente ao certificado	O	não-crítica	
	<i>Policyqualifiers</i> OID 1.3.6.1.5.5.7.2.1			
	<i>cPSuri</i> : URI do endereço web da DPC da AC emitente			
8.5. <i>Subject Alternative Name</i>	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	O*	não-crítica	(*) A obrigatoriedade com restrição implica recomendação de manutenção desse <i>otherName</i> de forma provisória, até 31/12/2028, com o propósito de possibilitar que todas as aplicações possam ser ajustadas para obtenção dessa informação pelo atributo <i>serialNumber</i> (OID 2.5.4.5), do campo DN do titular. Após 31/12/2028, fica opcional o uso desse <i>otherName</i> . Outros <i>otherNames</i> podem ser utilizados, conforme definido no ADE-ICP-04.01.



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário/Referência
8.6. <i>Basic Constraints</i>	cA = False	O	crítica	
8.7. <i>Extended Key Usage</i>	<i>Client authentication</i> OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	
	<i>E-mail protection</i> OID = 1.3.6.1.5.5.7.3.4	P		
8.8. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	Deve conter mais de uma entrada para endereços onde se obtém a LCR.
	<i>reasons</i>	N		
	<i>cRLIssuer</i>	N		
8.9. <i>Authority Information Access</i>	<i>id-ad-caIssuer</i> do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	<i>id-ad-ocsp</i> do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil– DOC-ICP-01.01	O	-	DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

3. Certificado de Equipamento de Carimbo do Tempo

Campo	Valor	Presença	Criticalidade	Comentário
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos	O	-	
3. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil OU = <Nome da Autoridade de Carimbo do Tempo> CN = <Nome do Servidor de Carimbo do Tempo (incluindo o serial do SCT)>	O	-	
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
8. Extensões X.509v3		-	-	

Campo	Valor	Presença	Criticalidade	Comentário
8.1. <i>Authority Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2. <i>Key Usage</i>	<i>digitalSignature</i>	O	crítica	
	<i>keyEncipherment</i>	N		
	<i>nonRepudiation</i>	P		
8.3. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o OID da PC correspondente ao certificado	O	não-crítica	
	<i>Policyqualifiers</i> OID 1.3.6.1.5.5.7.2.1			
	<i>cPSuri</i> : URI do endereço web da DPC da AC emitente			
8.4. <i>Subject Alternative Name</i>	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	P	não-crítica	
8.5. <i>Basic Constraints</i>	<i>cA</i> = False	O	crítica	
8.6. <i>Extended Key Usage</i>	<i>KeyPurposeID</i> OID = 1.3.6.1.5.5.7.3.8	O	crítica	
8.7. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	
	<i>reasons</i>	N		
	<i>cRLIssuer</i>	N		
8.8. <i>Authority Information Access</i>	<i>id-ad-caIssuer</i> do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	<i>id-ad-ocsp</i> do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		
8.9. <i>Subject Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

4. Certificado de Aplicações Específicas

Campo	Valor	Presença	Criticalidade	Comentário
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos	O	-	
3. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	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) ST = 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” SERIALNUMBER (OID 2.5.4.5) = CPF ou CNPJ, conforme o tipo de pessoa Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR CN = se presente, este campo deve conter um único nome de domínio	O	-	Outros atributos poderão ser utilizados na forma e propósitos definidos conforme RFC5280.



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
	pertencente ou controlado pelo titular			
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
8. Extensões X.509v3		-	-	Outros campos de extensão poderão ser utilizados na forma e propósitos definidos conforme RFC5280.
8.1. <i>Authority Key Identifier</i>	<i>Hash</i> 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2. <i>Key Usage</i>	<i>digitalSignature</i>	O	crítica	
	<i>keyEncipherment</i>	P		
	<i>nonRepudiation</i>	N		
8.3. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o OID da PC correspondente ao certificado	O	não-crítica	
	<i>Policyqualifiers</i> OID 1.3.6.1.5.5.7.2.1			
	<i>cPSuri</i> : URI do endereço web da DPC da AC emitente			
8.4. <i>Subject Alternative Name</i>	Campo <i>dNSName</i> , contendo um ou mais domínios pertencentes ou controlados pelo titular, conforme RFC5280	O	não-crítica	
8.5. <i>Basic Constraints</i>	<i>cA = False</i>	O	crítica	
8.6. <i>Extended Key Usage</i>	<i>id-kp-serverAuth</i> OID = 1.3.6.1.5.5.7.3.1	P*	crítica	* Ao menos um propósito deve estar ativado.
	<i>id-kp-clientAuth</i> OID = 1.3.6.1.5.5.7.3.2	P*		



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
8.7. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	
	<i>reasons</i>	N		
	<i>cRLIssuer</i>	N		
8.8. <i>Authority Information Access</i>	<i>id-ad-caIssuer</i> do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	<i>id-ad-ocsp</i> do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

5. Certificado de Equipamento OM-BR – Perfil meramente exemplificativo, visto que o regulamento é dado pelo Inmetro (NIT-Dmtic-008)

Campo	Valor	Presença	Criticalidade	Comentário
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos	O	-	
3. Algoritmo de Assinatura	Conforme regulamento dado pelo Inmetro.	O	-	Ver NIT-DMTIC-008: disponível em https://www.gov.br/inmetro/pt-br/assuntos/certificacao-digital/NITDmtic008.pdf
4. Emissor	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil SERIALNUMBER (OID 2.5.4.5) = número de identificação do equipamento OMBR CN = <Razão Social> OU = <número CNPJ> Conforme regulamento dado pelo Inmetro.	O	-	Ver NIT-DMTIC-008: disponível em https://www.gov.br/inmetro/pt-br/assuntos/certificacao-digital/NITDmtic008.pdf
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
8. Extensões X.509v3		-	-	
8.1. <i>Authority Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2. <i>Key Usage</i>	<i>digitalSignature</i>	O	crítica	
	<i>keyEncipherment</i>	O		
	<i>nonRepudiation</i>	O		
8.3. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o OID da PC correspondente ao certificado	O	não-crítica	
	<i>Policyqualifiers</i> OID 1.3.6.1.5.5.7.2.1			
	<i>cPSuri</i> : URI do endereço web da DPC da AC emitente			
8.4. <i>Subject Alternative Name</i>	OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, idêntico ao constante no certificado digital de pessoa jurídica requisitante deste; OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) idêntico ao constante no certificado digital de pessoa jurídica requisitante deste certificado ou quando o requisitante for uma Secretaria Estadual da Fazenda, o CNPJ do contribuinte a quem foi atribuído o certificado; OID = 2.16.76.1.3.12 e conteúdo = nas primeiras 8 (oito) posições, a data de fabricação do equipamento, no formato ddmmaaaa; nas posições subsequentes os dados de identificação do equipamento (código do produto e número de série).	P	não-crítica	
8.5. <i>Basic Constraints</i>	cA = False	O	crítica	
8.6. <i>Extended Key Usage</i>	<i>id-kp-clientAuth</i> OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
8.7. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	Deve conter mais de uma entrada para endereços onde se obtém a LCR.
	reasons	N		
	cRLIssuer	N		
8.8. <i>Authority Information Access</i>	<i>id-ad-calssuer</i> do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	<i>id-ad-ocsp</i> do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		
8.9. <i>Subject Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
9. Algoritmo de Assinatura	Conforme regulamento dado pelo Inmetro.	O	-	Ver NIT-DMTIC-008: disponível em https://www.gov.br/inmetro/pt-br/assuntos/certificacao-digital/NITDmtic008.pdf
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

6. Certificado de Equipamento SAT

Campo	Valor	Presença	Criticalidade	Comentário
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos	O	-	
3. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil SERIALNUMBER (OID 2.5.4.5) = número de identificação do equipamento CF-e-SAT CN = <Razão Social>:<:>número CNPJ>	O	-	Outros atributos poderão ser utilizados na forma e propósitos definidos conforme RFC5280.
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
8. Extensões X.509v3		-	-	
8.1. <i>Authority Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
8.2. <i>Key Usage</i>	<i>digitalSignature</i>	O	crítica	
	<i>keyAgreement</i>	P		
	<i>nonRepudiation</i>	O		
8.3. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o OID da PC correspondente ao certificado	O	não-crítica	
	<i>Policyqualifiers</i> OID 1.3.6.1.5.5.7.2.1			
	<i>cPSuri</i> : URI do endereço web da DPC da AC emitente			
8.4. <i>Subject Alternative Name</i>	<p>OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, idêntico ao constante no certificado digital de pessoa jurídica requisitante deste ou quando o requisitante for uma Secretaria Estadual da Fazenda, o CNPJ do contribuinte a quem foi atribuído o certificado;</p> <p>OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), idêntico ao constante no certificado digital de pessoa jurídica requisitante deste ou quando o requisitante for uma Secretaria Estadual da Fazenda, o CNPJ do contribuinte a quem foi atribuído o certificado;</p> <p>OID = 2.16.76.1.3.10 e conteúdo = nas primeiras 10 (dez) posições, número de série do equipamento emissor de CF-e-SAT; nas 14 (quatorze) posições subsequentes, o número da inscrição estadual da pessoa jurídica emissora do CF-e-SAT; nas 14 (quatorze) posições subsequentes, o número da inscrição municipal da pessoa jurídica emissora do CF-e-SAT.</p>	P	não-crítica	Outros <i>GeneralNames</i> podem ser utilizados conforme RFC5280.
8.5. <i>Basic</i>	<i>cA</i> = False	O	crítica	



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário
<i>Constraints</i>				
8.6. <i>Extended Key Usage</i>	<i>id-kp-clientAuth</i> OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	
8.7. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	
	reasons	N		
	cRLIssuer	N		
8.8. <i>Authority Information Access</i>	<i>id-ad-caIssuer</i> do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	<i>id-ad-ocsp</i> do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		
8.9. <i>Subject Key Identifier</i>	<i>Hash</i> 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	Ver DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

7. Detalhamento dos campos e extensões dos Certificados de Autoridade Certificadora (AC) que emite certificado para outras AC

Campo	Valor	Presença	Criticalidade	Comentário/Referência
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos.	O	-	
3. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.	O	-	DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil OU = Instituto Nacional de Tecnologia da Informacao - ITI CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Titular>	O	-	ETSI EN 319 412-3 V1.3.1 (2023-09)
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
8. Extensões X.509v3		-	-	Outros campos de extensão poderão ser utilizados na forma e propósitos definidos conforme RFC5280.



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário/Referência
8.1. <i>Authority Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2. <i>Subject Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
8.3. <i>Key Usage</i>	<i>keyCertSign</i>	O	crítica	
	<i>cRLSign</i>	O		
8.4. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o OID da DPC da AC titular	O	não-crítica	
8.5. <i>Basic Constraints</i>	<i>cA</i> = True	O	crítica	
8.6. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	Deve conter uma entrada para endereço onde se obtém a LCR.
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil– DOC-ICP-01.01	O	-	DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

8. Detalhamento dos campos e extensões dos Certificados de Autoridade Certificadora (AC) que emite certificado para usuário final

Campo	Valor	Presença	Criticalidade	Comentário/Referência
1. Versão	3 (0x2)	O	-	
2. Número de Série	Número inteiro, longo, positivo, único para cada AC, não sequencial, não podendo exceder a 20 octetos.	O	-	
3. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.	O	-	DOC-ICP-01.01
4. Emissor	C = BR O = ICP-Brasil OU = Instituto Nacional de Tecnologia da Informacao - ITI CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Titular>	O	-	ETSI EN 319 412-3 V1.3.1 (2023-09).
7. Informações da Chave Pública do Titular			-	
7.1. Algoritmo	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
7.2. Chave Pública	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil	O	-	DOC-ICP-01.01
8. Extensões X.509v3		-	-	Outros campos de extensão poderão ser utilizados na forma e propósitos definidos conforme RFC5280.



Infraestrutura de Chaves Públicas Brasileira

Campo	Valor	Presença	Criticalidade	Comentário/Referência
8.1. <i>Authority Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2. <i>Subject Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
8.3. <i>Key Usage</i>	<i>keyCertSign</i>	O	crítica	
	<i>cRLSign</i>	O		
8.4. <i>Certificate Policies</i>	<i>PolicyIdentifier</i> especificando o(s) OID(s) da(s) PC que a AC titular do certificado implementa	O	não-crítica	
	<i>Policyqualifiers</i> OID 1.3.6.1.5.5.7.2.1			
	<i>cPSuri</i> : URI do endereço web da DPC da AC emitente			
8.5. <i>Basic Constraints</i>	<i>cA</i> = True	O	crítica	
8.6. <i>CRL Distribution Points</i>	<i>DistributionPointName</i> do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	Deve conter uma entrada para endereço onde se obtém a LCR.
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil– DOC-ICP-01.01	O	-	DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O		



Infraestrutura de Chaves Públicas Brasileira

9. Detalhamento dos campos e extensões das Listas de Certificados Revogados (LCR)

Campo	Valor	Presença	Criticalidade	Comentário/Referência
1. Versão	2 (0x1)	O	-	
2. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.	O	-	DOC-ICP-01.01
3. Emissor	C = BR O = ICP-Brasil OU = <CN da cadeia vinculada à emissora> CN = <Nome da AC Emissora>	O	-	
4. Período de Validade				
esta emissão	AAAAMMDDHHMMSSZ	O	-	Formato do tipo <i>Time</i> , conforme RFC5280
próxima emissão	AAAAMMDDHHMMSSZ			
5. Extensões X.509v3		-	-	
5.1. <i>Authority Key Identifier</i>	Hash 160 bits SHA-1 da chave pública da AC que assina a LCR	O	não-crítica	
5.2. <i>CRL Number</i>	Número sequencial para cada LCR emitida pela AC	O	não-crítica	
6. Certificados Revogados	Número de série do certificado	O	-	
	AAAAMMDDHHMMSSZ (data da revogação)			
9. Algoritmo de Assinatura	Conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil– DOC-ICP-01.01	O	-	DOC-ICP-01.01
10. Valor da Assinatura	Cálculo da assinatura digital dos campos básicos do certificado (<i>bit string</i>).	O	-	

Legenda: O = Obrigatório, P = Permitido e N = Não permitido