DIÁRIO OFICIAL DA UNIÃO

Publicado em: 04/11/2024 | Edição: 213 | Seção: 1 | Página: 1

Órgão: Presidência da República/Casa Civil/Comitê Gestor da Infraestrutura de Chaves Públicas

RESOLUÇÃO CG ICP-BRASIL Nº 211, DE 31 DE OUTUBRO DE 2024

Dispõe sobre os tipos de certificados digitais emitidos no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

O COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6º, § 1º, inc. IV, da Resolução CG ICP-Brasil nº 190, de 18 de maio de 2021 (Regimento Interno), torna público que oCOMITÊ 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 reunião ordinária, realizada em sessão presencial em 31 de outubro de 2024, resolveu:

Art. 1º Esta Resolução dispõe sobre os tipos de certificados digitais emitidos no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Art. 2º Ficam criados os seguintes tipos de certificado digital no âmbito da ICP-Brasil:

I - certificado digital de selo eletrônico em software - SE-S;

II - certificado digital de selo eletrônico em hardware - SE-H;

III - certificado digital de aplicações específicas em software - AE-S; e

IV - certificado digital de aplicações específicas em hardware - AE-H.

Art. 3º Ficam extintos os seguintes tipos de certificado digital no âmbito da ICP-Brasil:

I - certificado de assinatura dos tipos A1 e A2; e

II - certificado de sigilo dos tipos S1, S2, S3 e S4.

Art. 4º Fica vedado o uso de certificado digital de selo eletrônico com propósito de assinatura como manifestação de vontade de pessoa jurídica.

Art. 5º Fica vedada a emissão de certificados digitais destinados à assinatura de código (*Code siging*) na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Parágrafo único. Certificados para assinatura de código emitidos até a data de publicação desta Resolução permanecem vigentes até a data de expiração.

Art. 6º Fica dispensada a aderência aos requisitos de princípios e critériosWebtrust *Baseline* - *Code Signing*e SSL/TLS, para suas respectivas cadeias de certificação.

Art. 7º Ficam extintos os seguintes OIDs (*Object Identifier*) da extensão "*Subject Alternative Name*" do certificado digital:

I - OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

II - OID = 2.16.76.1.3.9 e conteúdo = nas primeiras 11 (onze) posições, o número de Registro de Identidade Civil.

III - OID = 2.16.76.1.3.11 e conteúdo = nas primeiras 10 (dez) posições, o cadastro único do servidor público da ativa e militares da União constante no Sistema de Gestão de Pessoal (SIGEPE) mantido pelo Ministério do Planejamento ou nos sistemas correlatos, no âmbito da esfera estadual e do Distrito Federal, e nos Sistemas de Gestão de Pessoal das Forças Armadas.

IV - 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;

V - OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

Art. 8º Fica implementado o campo*serialNumber*(OID 2.5.4.5) no*Distinguished Name*do titular do certificado digital de pessoa física, contendo o CPF, e de selo eletrônico, contendo CNPJ, a fim de garantir a unicidade de nome.

Art. 9º O anexo da Resolução CG ICP-Brasil nº 178, de 20 de outubro de 2020, DOC-ICP-03, passa a vigorar com as seguintes alterações:

"2.2.2.1.2 a solicitação de credenciamento deve estar separada por propósito de uso de chave, quais sejam:

i. autenticação de aplicações específicas;

ii. assinatura de documentos e proteção de e-mail (S/MIME) e garantia de origem e integridade; e

iii.assinatura de carimbo do tempo (*TimeStamping*)." NR

Art. 10. O anexo da Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020, DOC-ICP-04, passa a vigorar com as seguintes alterações:

"1.1.5 São 10 (dez) os tipos de certificados digitais para usuários finais da ICP-Brasil:

A3

A4 SE-S SE-H T3 T4 AE-S AE-H

A CF-e-SAT OM-BR

1.1.6 Certificados do tipo A3 e A4 são certificados de assinatura e devem ser emitidos exclusivamente para pessoas físicas.

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.

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 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.

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.

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.

1.1.11 Certificados do tipo Objeto Metrológico - OM-BR devem ser emitidos apenas para equipamentos metrológicos regulados pelo Inmetro.

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.

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.

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

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
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

..... Usabilidade do Certificado

1.3.1 .....

.....

1.3.1.4 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.

1.3.1.5 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.

1.3.1.6 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.

1.3.1.7 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.

.....

1.3.2 .....

1.3.2.1 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).

1.3.2.2 É proibido o uso do certificado de selo eletrônico para assinatura digital com o propósito de manifestação de vontade.

1.3.2.3. Neste item devem ser relacionadas, quando cabível, outras aplicações para as quais existem restrições ou proibições para o uso desses certificados.

1.4 Política de Administração

.....

6.1.1.8 .....

Tabela 4 - Mídias Armazenadoras de Chaves Criptográficas

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.

.....6.3.2.3.....

Tabela 6 - Períodos de Validade dos Certificados

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

6.4 Dados de Ativação

.....

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.

7.1.2.2 Os campos*otherName*devem estar de acordo com as seguintes especificações:

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

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";

c) se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF;

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;

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;

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;

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) 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.

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.

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.

7.1.2.5 Todas as informações utilizadas para preenchimento dos campos do certificado devem ser verificadas.

7.1.3 .....

.....

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.

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

7.1.5 Restrições de nome

.....

7.2 Perfil de LCR

.....

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.

7.3 Perfil de OCSP

"NR .....

ANEXO I

Tabela de Perfis de Certificado e LCR

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. Númerode 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*Time*, 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.(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.
8.1.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Subject Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	

8.3.*Key Usage*	*digitalSignature*	O	crítica	
	keyEncipherment	P		
	nonRepudiation	P		
8.4.*Certificate Policies*	*PolicyIdentifier*especificando o OID da PC correspondente ao certificado	O	não-crítica	
	*Policyqualifiers*OID 1.3.6.1.5.5.7.2.1			
	cPSuri: URI do endereço web da DPC da AC emitente			
8.5.*Subject Alternative Name*	OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaa; 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*otherName 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 serial NUmber(OID*2.5.4.5) do campo DN do titular. Após 31/12/2028, fica opcional o uso desse*otherName.*
	OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado	P	não-crítica	Outros*otherNames*podem ser utilizados, conforme definido no ADE-ICP- 04.01.
8.6.*Basic Constraints*	cA = False	O	crítica	
8.7.*Extended Key Usage*	*Client authentication*OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	
	E-mail protection OID = 1.3.6.1.5.5.7.3.4	P		
8.8.*CRL Distribution Points*	*DistributionPointName*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		

8.9. Authority Information Access	*id-ad-calssuer*do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	*id-ad-ocsp*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 (*bit string*).	O		

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*Time*, conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil CN = <Razão Social>*serialNumber* = <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
8. Extensões X.509v3		-	-	Outros campos de extensão poderão ser utilizados na forma e propósitos definidos conforme RFC5280.
8.1.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Subject Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
8.3.*Key Usage*	*digitalSignature*	O	crítica	
	keyEncipherment	P		
	nonRepudiation	P		
8.4.*Certificate Policies*	*PolicyIdentifier*especificando o OID da PC correspondente ao certificado	O	não-crítica	
	*Policyqualifiers*OID 1.3.6.1.5.5.7.2.1			
	cPSuri: URI do endereço web da DPC da AC emitente			
8.5.*Subject Alternative Name*	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 other Name de forma provisória , até 31/12/2028, com propósito de possibilitar que todas a aplicações possam ser
				ajustadas para obtenção dessa informação pelo atributo serialNumber(OID
				=2.5.4.5) do campo DN do titular após 31/12/2028, fica opcional o uso desse otherName. Outros

				otherNames podem ser utilizados, conforme definido ADE-ICP-04.01
8.6.*Basic Constraints*	cA = False	O	crítica	
8.7.*Extended Key Usage*	*Client authentication*OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	
	E-mail protection OID = 1.3.6.1.5.5.7.3.4	P		
8.8.*CRLDistribution Points*	*DistributionPointName*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		
8.9. Authority Information Access	*id-ad-caIssuer*do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	o-crítica	
	*id-ad-ocsp*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 (*bit string*).	O		

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*Time*, 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	O	-	Ver DOC-ICP-01.01
	Defina os padrões e algoritmos criptográficos da ICP-Brasil			

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.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Key Usage*	*digitalSignature*	O	crítica	
	keyEncipherment	N		
	nonRepudiation	P		
8.3.*Certificate Policies*	*PolicyIdentifier*especificando o OID da PC correspondente ao certificado	O	não-crítica	
	Policyqualifiers OID 1.3.6.1.5.5.7.2.1			
	cPSuri: URI do endereço web da DPC da AC emitente			
8.4.*Subject Alternative Name*	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.*Basic Constraints*	cA = False	O	crítica	
8.6.*Extended Key Usage*	*KeyPurposeID*OID = 1.3.6.1.5.5.7.3.8	O	crítica	

8.7.*CRLDistribution Points*	*DistributionPointName*do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	
	reasons	N		
	cRLIssuer	N		
8.8. Authority Information Access	*id-ad-calssuer*do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
*id-ad-ocsp*do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P			
8.9.*Subject Key Identifier*	*Hash*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 (*bit string*).	O		

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*Time*, 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	O		Outros atributos poderão ser utilizados na forma e propósitos definidos conforme RFC5280.

	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 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.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Key Usage*	*digitalSignature*	O	crítica	
	keyEncipherment	P		
	nonRepudiation	N		
8.3.*Certificate Policies*	*PolicyIdentifier*especificando o OID da PC correspondente ao certificado	O	não-crítica	
	*Policyqualifiers*OID 1.3.6.1.5.5.7.2.1			
	cPSuri: URI do endereço web da DPC da AC emitente			
8.4.*Subject Alternative Name*	Campo dNSName, contendo um ou mais domínios pertencentes ou controlados pelo titular, conforme RFC5280	O	não-crítica	
8.5.*Basic Constraints*	cA =*False*	O	crítica	
8.6.*Extended Key Usage*	*id-kp-serverAuth*OID = 1.3.6.1.5.5.7.3.1	P*	crítica	* Ao menos um propósito deve estar ativado.
	*id-kp-clientAuth*OID = 1.3.6.1.5.5.7.3.2	P*		
8.7.*CRL Distribution Points*	*DistributionPointName*do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	
	reasons	N		
	cRLIssuer	N		
8.8. Authority Information Access	*id-ad-caIssuer*do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	*id-ad-ocsp*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 (*bit string*).	O		

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/inmet ro/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*Time*, conforme RFC5280
não depois	AAAAMMDDHHMMSSZ			
6. Titular	C = BR O = ICP-Brasil SERIAL NUMBER (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/inmet ro/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
8. Extensões X.509v3		-	-	
8.1.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Key Usage*	*digitalSignature*	O	crítica	
	keyEncipherment	O		
	nonRepudiation	O		
8.3.*Certificate Policies*	*PolicyIdentifier*especificando o OID da PC correspondente ao certificado	O	não-crítica	
	*Policyqualifiers*OID 1.3.6.1.5.5.7.2.1			
	cPSuri: URI do endereço web da DPC da AC emitente			
8.4.*Subject Alternative Name*	OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, idêntico ao	P	não-crítica	
	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 foruma 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).			
8.5.*Basic Constraints*	cA = False	O	crítica	
8.6.*Extended Key Usage*	*id-kp-clientAuth*OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	
8.7.*CRL Distribution Points*	*DistributionPointName*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. Authority Information Access	*id-ad-caIssuer*do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	*id-ad-ocsp*do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		
8.9.*Subject Key Identifier*	*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 (*bit string*).	O		

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. Períodode Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo*Time*, 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.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Key Usage*	*digitalSignature*	O	crítica	
	keyAgreement	P		
	nonRepudiation	O		
8.3.*Certificate Policies*	*PolicyIdentifier*especificando o OID da PC correspondente ao certificado	O	não-crítica	
	*Policyqualifiers*OID 1.3.6.1.5.5.7.2.1			
	cPSuri: URI do endereço web da DPC da AC emitente			
8.4.*Subject Alternative Name*	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	P	não-crítica	Outros*GeneralNames*podem ser utilizados conforme RFC5280.
	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; 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; 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			
8.5.*Basic Constraints*	cA = False	O	crítica	
8.6.*Extended Key Usage*	*id-kp-clientAuth*OID = 1.3.6.1.5.5.7.3.2	O	não-crítica	
8.7.*CRL Distribution Points*	*DistributionPointName*do tipo URI contendo HTTP URL do serviço de LCR da AC emissora desse certificado	O	não-crítica	
	reasons	N		
	cRLIssuer	N		
8.8. Authority Information Access	*id-ad-calssuer*do tipo URI contendo HTTP URL para recuperação da cadeia de certificação desse certificado	O	não-crítica	
	*id-ad-ocsp*do tipo URI contendo HTTP URL com o respectivo endereço do respondedor OCSP para esse certificado	P		

8.9.*Subject Key Identifier*	*Hash*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 (*bit string*).	O		

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*Time*, 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.
8.1.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Subject Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
8.3.*Key Usage*	*keyCertSign*	O	crítica	
	cRLSign	O		
8.4.*Certificate Policies*	*PolicyIdentifier*especificando o OID da DPC da AC titular	O	não-crítica	
8.5.*Basic Constraints*	cA = True	O	crítica	
8.6.*CRL Distribution Points*	*DistributionPointName*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 (*bit string*).	O		

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 = BRO = ICP-BrasilOU = Instituto Nacional de Tecnologia da Informacao - ITI CN = <Nome da AC Emitente>	O	-	
5. Período de Validade				
não antes	AAAAMMDDHHMMSSZ	O	-	Formato do tipo*Time*,
não depois	AAAAMMDDHHMMSSZ			conforme RFC5280
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 utlizados na forma e propósitos definidos conforme RFC5280
8.1.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que emite o certificado	O	não-crítica	
8.2.*Subject Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC titular do certificado	O	não-crítica	
8.3.*Key Usage*	*keyCertSign*	O	crítica	
	cRLSign	O		
8.4.*Certificate Policies*	*PolicyIdentifier*especificando o(s) OID(s) da(s) PC que a AC titular do certificado implementa	O	não-crítica	
	*Policyqualifiers*OID 1.3.6.1.5.5.7.2.1			
	cPSuri: URI do endereço web da DPC da AC emitente			
8.5.*Basic Constraints*	cA = True	O	crítica	
8.6.*CRL Distribution Points*	*DistributionPointName*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 (*bit string*).	O		

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*Time*, conforme RFC5280
próxima emissão	AAAAMMDDHHMMSSZ			
5. Extensões X.509v3		-	-	
5.1.*Authority Key Identifier*	*Hash*160 bits SHA-1 da chave pública da AC que assina a LCR	O	não-crítica	
5.2.*CRL Number*	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 (*bit string*).	O	-	

Legenda: O = Obrigatório, P = Permitido e N = Não permitido" (NR)

Art. 11. O anexo da Resolução CG ICP-Brasil nº 177, de 20 de outubro de 2020, DOC-ICP-05, passa a vigorar com as seguintes alterações:

"1.1.2 .....

1.1.3 A estrutura desta DPC está baseada na RFC 3647.

1.1.4 A AC responsável deverá manter todas as informações da sua DPC sempre atualizadas.

1.1.5 Este documento compõe o conjunto normativo da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.

1.2 .....

.....

1.2.2 As ACs emissoras de certificados para usuários finais devem ser exclusivas e separadas de acordo com os seguintes propósitos de uso de chaves:

a) autenticação de aplicações específicas;

b) assinatura de documento e proteção de e-mail (S/MIME) e garantia de origem e integridade; e

c) assinatura de carimbo do tempo (*TimeStamping*).

1.3 .....

.....

3.1.1.1 Neste item devem ser definidos os tipos de nomes admitidos para os titulares de certificados emitidos pela AC responsável pela DPC. Entre os tipos de nomes considerados, poderão estar o "*Distinguished Name*" do padrão ITU X.500.

.....

3.2.2.2 Documentos para efeitos de identificação de uma organização

a) .....

b) .....

i) .....

ii) prova de inscrição no Cadastro Nacional de Obras - CNO.

Nota 1: As confirmações de que trata o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório que essas validações constem no dossiê eletrônico do titular do certificado.

3.2.2.3 Responsabilidade decorrente do uso do certificado de uma organização

Os atos praticados com o certificado digital de titularidade de uma organização estão sujeitos ao regime de responsabilidade definido em lei.

3.2.3 .....

.....

3.2.3.1.8.1 No caso de AR ELETRÔNICA, a base oficial nacional, a ser definida por Instrução Normativa da AC Raiz, deverá ter como requisito técnico a garantia de individualização unívoca dos cidadãos, biométrica e biográfica, a nível nacional.

3.2.4 Informações não verificadas do titular do certificado

.....

3.2.7.1.5 Fica dispensada a observância do item 3.2.2.1.3, alíneas "b" e "c", para certificados cujo titular seja pessoa jurídica quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo A3 ou superior, cuja titularidade é da mesma pessoa física responsável legal da organização e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.2.7.2.1 Para certificados de aplicações específicas que utilizem URL na identificação do titular, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele endereço. Nesse caso, deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

3.2.7.2.2 Para emissão de certificados do tipo T3 ou T4, para equipamentos de ACT credenciadas na ICP-Brasil, a solicitação deve conter o nome de servidor e o número de série do equipamento. Esses dados devem ser validados comparando-os com aqueles publicados pelo ITI no Diário Oficial da União, quando do deferimento do credenciamento da ACT.

3.2.7.3 Autenticação de identificação de equipamento para certificado CF-e-SAT

3.2.7.3.1 Disposições gerais

3.2.7.3.1.1 Em se tratando de certificado emitido para equipamento SAT, o titular será representado pelo contribuinte identificado no certificado digital ICP-Brasil de pessoa jurídica que assina a solicitação, associada ao número de série do equipamento detentor da chave privada.

3.2.7.3.1.2 Para certificados do tipo A CF-e-SAT, a confirmação da identidade da organização e das pessoas físicas se dará conforme disposto no item 3.2.2 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

3.2.7.3.1.3 Para certificados do tipo A CF-e-SAT, por se tratar de certificado para equipamento fiscal específico para contribuinte já identificado quando da emissão do certificado digital ICP-Brasil de pessoa jurídica válido que assina a requisição do certificado A CF-e-SAT, a confirmação da identidade se dará exclusivamente na forma do disposto no item 3.2.3 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

3.2.7.4 Procedimentos para efeitos de identificação de um equipamento SAT

3.2.7.4.1 Para certificados de equipamento SAT, deve ser verificado se o CNPJ do contribuinte que assina digitalmente a solicitação desse certificado está vinculado ao número de série do referido equipamento, o qual deve estar registrado e autorizado pela unidade fiscal federada. Essas informações devem ser obtidas e confirmadas pela AC emissora do certificado.

3.2.7.5 Autenticação de identificação de equipamentos para certificado OM-BR 3.2.7.5.1 Disposições gerais

3.2.7.5.1.1 Em se tratando de certificado emitido para equipamento OM-BR, o titular será representado pelo fabricante identificado no certificado digital ICP-Brasil de pessoa jurídica que assina a solicitação, associada ao número de identificação do equipamento detentor da chave privada.

3.2.7.5.1.2 Para certificados do tipo OM-BR, a confirmação da identidade do fabricante se dará conforme disposto no item 3.2.7.1 e com a assinatura do TERMO DE TITULARIDADE

[4] específico de que trata o item 4.1.

3.2.7.5.1.3 Para certificados do tipo OM-BR, por se tratar de certificado para equipamento metrológico específico de fabricante autorizado já identificado quando da emissão do certificado digital ICP-Brasil de pessoa jurídica válido que assina a requisição do certificado OM-BR, a confirmação da identidade se dará exclusivamente na forma do disposto no item 3.2.7.1 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1

3.2.7.6 Procedimentos para efeitos de identificação de um equipamento metrológico

3.2.7.6.1 Para certificados de equipamento metrológico, deve ser verificado se o CNPJ do fabricante que assina digitalmente a solicitação desse certificado está vinculado aos controles regulatórios do referido equipamento, o qual deve estar registrado e autorizado pelo Inmetro. Essas informações devem ser obtidas e confirmadas pela AC emissora do certificado.

3.2.8 Procedimentos complementares

3.2.8.1 A AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro, bem como os Princípios e Critérios*WebTrust*.

.....

3.2.9.7 .....

a) o responsável pelo uso do certificado de selo eletrônico deverá ser autenticado através de batimento biométrico (1:1) em PSBio credenciado na ICP-Brasil, na base biométrica oficial do TSE ou em outra base biométrica oficial da União, dos Estados ou do Distrito Federal, com comprovação auditável desse processo de autenticação biométrica por parte da AC. Essa comprovação poderá ser pelo CPF ou outro indexador viável entre os sistemas;

.....

3.2.9.8 .....

a) a pessoa física titular do certificado deverá ter sido biometricamente identificada e individualizada na base biométrica do órgão responsável pela emissão da Carteira de Identidade (RG) ou da Carteira Nacional de Habilitação (CNH), conforme o caso, bem como ter dado consentimento expresso e específico para o compartilhamento com as entidades da ICP-Brasil dos dados biométricos e biográficos necessários para a identificação, cadastro e emissão do certificado digital. Essa individualização poderá ser pelo CPF ou outro indexador viável entre os sistemas;

.....

3.3.2 .....

a) .....

b) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP- Brasil válido, do tipo A3 ou superior, cujo certificado requisitado seja do mesmo nível de segurança ou inferior; ou

c) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

3.3.2.1 Para certificados de aplicações específicas que utilizem URL, a AC poderá implementar mecanismos automatizado de gerenciamento de certificado (ACME) de forma a preservar a posse ou propriedade da URL (domínio) e a identificação do solicitante, seja pessoa física ou jurídica. O processo automatizado implica as seguintes etapas:

a) .....

b) a requisição deverá ser acompanhada do certificado da URL solicitada, ainda válido, e o conjunto (requisição + certificado da URL) deve ser assinado com certificado ICP-Brasil, no mínimo do tipo A3, do responsável pelo domínio;

.....

4.1 .....

.....

c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico, e, ainda, quando emissão para servidor público da ativa e militar da União, Estados e Distrito Federal pela autoridade designada formalmente pelos órgãos competentes;

d) o disposto na alínea 'b' e a assinatura do termo de titularidade, no caso de AR ELETRÔNICA, por se tratar de procedimento automatizado, sem intervenção de agente de registro, serão regulamentados por Instrução Normativa da AC Raiz; e

e) que na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados de equipamento, aplicação, carimbo de tempo e outros que façam uso de CSR) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

4.1.1 .....

.....

4.9.1.4 . A DPC deve observar que todo certificado deverá ter a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado.

4.9.1.5 .....

.....

4.9.7.4 Caso sejam utilizadas frequências de emissão de LCR específicas para as PCs implementadas, as mesmas devem ser descritas nessas PCs, no item correspondente.

4.9.8 .....

.....

5.2.1.3 Todos os operadores do sistema de certificação da AC deverão receber treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso serão determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4.....

.....

5.4.1.1 A AC responsável pela DPC deverá registrar em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

.....

l) Operações de escrita nesse repositório, quando aplicável.

5.4.1.2 .....

.....

6.2.4.3 A AC não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.5 Arquivamento de chave privada

6.2.5.1 Não devem ser arquivadas chaves privadas de assinatura digital.

.....

6.3.2.1 .....

6.3.2.2 Cada PC implementada pela AC responsável deve definir o período máximo de validade do certificado que define, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.3 A validade admitida para certificados de AC é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

.....

7.1 Perfil do certificado

Todos os certificados emitidos pela AC responsável deverão estar em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8, de acordo com o perfil estabelecido na RFC 5280.

7.1.1 Número de versão

Todos os certificados emitidos pela AC responsável 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

A ICP-Brasil define como obrigatórias as extensões para certificados de AC conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I do DOC-ICP-04, aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.

7.1.3 .....

.....

7.1.4 Formatos de nome

7.1.4.1 O nome da AC titular de 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 do DOC-ICP-04, aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.

7.1.5 Restrições de nome

.....

7.2.2 Extensões de LCR e de suas entradas

Neste item, a DPC deve descrever todas as extensões de LCR utilizadas pela AC responsável e sua criticalidade, conforme especificado na Tabela de Perfis de Certificado e LCR, Anexo I do DOC-ICP-04, aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.

7.3 Perfil de OCSP

.....

9.3.3.3 A DPC deve informar que os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

9.4 Privacidade da informação

.....

9.6.1.6 Revogação

A AC irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos Princípios e Critérios*WebTrust*." NR

Art. 12. Ficam aprovadas:

I - a versão 7.2 do documento DOC-ICP-03 - Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil;

II - a versão 8.2 do documento DOC-ICP-04 - Requisitos Mínimos para as Políticas de Certificados na ICP- Brasil; e

III - a versão 6.5 do documento DOC-ICP-05 - Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.

Parágrafo único. A identificação da versão deverá ser atualizada no preâmbulo e incluída no controle de versões do anexo das respectivas Resoluções.

Regras de transição

Art. 13. Os certificados digitais dos tipos A1, A2, A3, A4, S1, S2, S3, S4, T3 e T4, com seus perfis e propósitos de uso estabelecidos nos regulamentos da ICP-Brasil anteriores à data de publicação desta Resolução, poderão ser emitidos e utilizados na cadeia de certificação V5 durante toda a sua vigência, até 02 de março de 2029.

Art. 14. Poderão ser emitidos certificados digitais dos tipos A1 e A3 na cadeia V10 da AC Raiz da ICP-Brasil até 31 de dezembro de 2026 para uso restrito em aplicações específicas.

Art. 15. As entidades com pedido de credenciamento protocolado junto à ICP-Brasil antes da data de publicação deste regulamento deverão estar aderentes a esta Resolução e terão o prazo de até cento e oitenta dias da data de publicação deste regulamento para efetuar os ajustes necessários no pedido de credenciamento, bem como atender ao item 2.2.2.2.1 do Anexo I da Resolução CG ICP-Brasil nº 178, de 20 de outubro de 2020.

Parágrafo único. As entidades com pedido de credenciamento deferido pelo ITI e que não tenham consumado o credenciamento na ICP-Brasil poderão optar pela emissão de certificados na cadeia V5 da AC Raiz da ICP-Brasil no prazo de até cento e oitenta dias da data de publicação deste regulamento.

Art. 16. As entidades credenciadas na ICP-Brasil que já emitem certificados de equipamentos e aplicações na cadeia V10 terão até cento e oitenta dias, a partir da data de publicação deste regulamento, para incluir as novas políticas de aplicações específicas mediante a realização de credenciamento simplificado a ser definido por instrução normativa do ITI.

§ 1º As entidades credenciadas na ICP-Brasil que já emitem certificados de equipamentos e aplicações na cadeia V5 que migrarem para a cadeia V10 em até cento e oitenta dias da data de publicação deste regulamento realizarão credenciamento simplificado nessa cadeia.

§ 2º Após o período de cento e oitenta dias da data de publicação deste regulamento, a migração estará sujeita a um novo credenciamento.

Art. 17. Esta Resolução entra em vigor na data de sua publicação.

ENYLSON FLAVIO MARTINEZ CAMOLESI