SUMÁRIO

1 OBJETIVO

Esta Norma estabelece o Leiaute dos Certificados Digitais da Autoridade Certificadora Inmetro, bem como o Leiaute dos Certificados Digitais para Objetos Metrológicos (OM-BR), emitidos para equipamentos regulados pelo Inmetro.

2 CAMPO DE APLICAÇÃO

Esta norma se aplica, compulsoriamente, à Autoridade Certificadora de primeiro nível AC-INMETRO e às Autoridades Certificadoras de Segundo Nível credenciadas para a cadeia de certificados OM-BR.

3 RESPONSABILIDADE

A responsabilidade pela revisão e cancelamento desta Norma é da Dmtic.

4 DOCUMENTOS DE REFERÊNCIA

NIE-Dimci-016	Controle de Registros Técnicos e da Qualidade.
NIG-Gabin-040	Apresentação, Elaboração, Aprovação, Cancelamento e Arquivamento de Norma do Inmetro.
Portaria Inmetro Nº 103, de 8 de março de 2021	Dispõe o processo de certificação digital, critérios para credenciamento na Autoridade Certificadora do Inmetro e descrição do leiaute dos certificados digitais.

5 DOCUMENTOS COMPLEMENTARES

DOC-ICP-01	Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil.
DOC-ICP-01.01	Padrões e Algoritmos Criptográficos da ICP-Brasil.
DOC-ICP-04	Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil
NBR 9611 de 02/1991	Tecnologia da Informação - Código Brasileiro para Intercâmbio de Informação - Padronização.
RESOLUÇÃO Nº 139, DE 3 DE JULHO DE 2018 do Comitê Gestor da ICP-Brasil	Aprova a Criação da Política de Certificado para Objetos Metrológicos - OM-BR no âmbito da ICP-Brasil.
Request for Comments (RFC) 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

6 SIGLAS

As siglas das UP/UO do Inmetro podem ser acessadas em: http://www.inmetro.gov.br/inmetro/pdf/regimento-interno.pdf

AC	Autoridade Certificadora
ASN.1	*Abstract Syntax Notation One*
C	*Country Name*
CG	Comitê Gestor
CN	*Common Name*
CNPJ	Cadastro Nacional de Pessoa Jurídica
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EdDSA	*Edwards-curve Digital Signature Algorithm*
ICP	Infraestrutura de Chaves Públicas
IoT	*Internet of Things*
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados
NBR	Norma Técnica Brasileira
O	*Organization Name*
OCSP	*On-line Certificate Status Protocol*
OID	*Object IDentifier*
OM	Objeto Metrológico

OU	*Organization Unit name*
PC	Política de Certificação
RFC	*Request for Comments*
URL	*Uniform Resource Locator*
UTF	*Unicode Transformation Format*

7 TERMOS E DEFINIÇÕES

7.1 *Abstract Syntax Notation One* (ASN.1)

É uma linguagem de descrição de interface padrão para definir estruturas de dados que podem ser serializadas e desserializadas em uma plataforma cruzada. É amplamente utilizado em telecomunicações, redes de computadores e, especialmente, em criptografia. A vantagem é que a descrição ASN.1 da codificação de dados é independente de um determinado computador ou linguagem de programação. Como o ASN.1 é legível por humanos e por máquina, um compilador ASN.1 pode compilar módulos em bibliotecas de código, codecs, que decodificam ou codificam as estruturas de dados.

7.2 Autoridade Certificadora Inmetro (AC Inmetro)

Autoridade Certificadora (AC) de 1º Nível na Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil). Como autoridade certificadora, o Inmetro não deverá fornecer certificados digitais para os objetos metrológicos, mas credenciar outras entidades para emissão dos certificados OM-BR.

7.3 Certificado tipo OM-BR (Certificados do tipo Objeto Metrológico)

Certificados do tipo OM-BR só podem ser emitidos para equipamentos metrológicos regulados pelo Inmetro, como bombas de combustível, balanças, taxímetros, dispositivos de controle de velocidade, medidores de consumo de água, energia e gás, entre outros.

7.4 Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira

O CG ICP-Brasil, instituído pela Medida Provisória no 2.200-2, de 24 de agosto de 2001, e regulamentado pelo Decreto nº. 6.605, de 14 de outubro de 2008, exerce a função de autoridade gestora de políticas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

7.5 EdDSA (*Edwards-curve Digital Signature Algorithm*)

É um algoritmo de assinatura digital moderno e seguro baseado em curvas elípticas com desempenho otimizado, como a curva de 255 bits Curve25519 e a curva de 448 bits Curve448-Goldilocks.

7.6 ITU-T X.509

Na criptografia, X.509 é um padrão ITU-T para infraestruturas de chaves públicas (ICP). A X.509 especifica, entre várias outras coisas, o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública, permitindo autenticação forte. Faz parte das séries X.500 de

recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Na ICP-Brasil utilizam--se certificados no padrão X-.509 V3.

7.7 NBR 9611 de 02/1991 - Tecnologia de informação - Código Brasileiro para Intercâmbio de Informação - Padronização

Esta Norma padroniza o código brasileiro de caracteres a ser usado em sistemas de processamento de dados, sistemas de comunicação e equipamentos associados, para intercâmbio de informação.

7.8 RFC 5280 (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile*)

Traça o perfil do certificado X.509 v3, a lista de revogação de certificados X.509 v2 e descreve um algoritmo para validação do caminho do certificado X.509.

7.9 UTF-8 (8-bit *Unicode Transformation Format*)

É um tipo de codificação binária (Unicode) de comprimento variável. Pode representar qualquer caractere universal padrão do Unicode, sendo também compatível com o ASCII. Por esta razão, está sendo lentamente adaptado como tipo de codificação padrão para e-mail, páginas web, e outros locais onde os caracteres são armazenados.

8 LEIAUTE DO CERTIFICADO DA AUTORIDADE CERTIFICADORA

8.1 Requisitos de certificado

8.1.1 Os certificados emitidos pela Autoridade Certificadora do INMETRO (AC INMETRO) obedecem às Resoluções do Comitê Gestor da ICP-Brasil.

8.1.2 Os certificados da Autoridade Certificadora do INMETRO são destinados a Autoridades Certificadoras credenciadas pelo ICP-Brasil e habilitadas pelo INMETRO a emitir certificados para objetos metrológicos conforme Resolução n. 139/2018 do Comitê Gestor da ICP-Brasil.

8.1.3 Elementos do leiaute do certificado

8.1.3.1 Número de Versão: Os certificados digitais implementam a versão 3 de certificados definida no padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 5280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

8.1.3.2 Campo *Issuer*: Todo certificado possui neste campo o nome X.500 da Autoridade Certificadora do Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro.

8.1.3.3 Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave: O algoritmo utilizado para a geração das chaves dos certificados de Autoridade Certificadora é o EdDSA (Ed448-*Goldilocks*).

Tabela 1 – Tamanho e processo de geração de chave

Tamanho da Chave (bits)	Processo de Geração da Chave Criptográfica
448	Hardware

Fonte: Doc-ICP-01.01

8.1.3.4 Algoritmo de Assinatura Digital: Os certificados deverão ser assinados com uso do algoritmo conforme documento DOC ICP-01.01.

8.1.3.5 Limite de Tamanho: O tamanho máximo de cada componente do DN (CN, OU, O e C) é de 64 caracteres.

8.1.3.6 Chave Pública do Titular do Certificado: Conforme definido na RFC 5280.

8.1.3.7 Identificação do Sistema Criptográfico Utilizado: Conforme definido na RFC 5280.

8.1.3.8 Conjunto de Caracteres: Todas as sequências de caracteres nos certificados, inclusive as dos DN (*Distinguished Name*) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela 2. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere ‘c’.

Tabela 2 – Caracteres especiais admitidos em nomes

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21
“	22
#	23
$	24
%	25
&	26
‘	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D

(continua)

.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

Fonte: Doc-ICP-04

8.1.3.9 Identificação e Assinatura Digital da Autoridade Certificadora do INMETRO: Conforme definido na RFC 5280.

8.1.3.10 Número de Série Exclusivo do Certificado: Conforme definido na RFC 5280.

8.1.3.11 Validade do Certificado Digital: Conforme definido na Política de Certificação com validade igual ou inferior a validade do certificado da AC-INMETRO.

8.1.3.12 Composição do *Distinguished Name* (DN) do certificado:

a) CN=<Nome da Autoridade Certificadora Habilitada>;
b) OU=Instituto Nacional de Metrologia Qualidade e Tecnologia INMETRO;
c) O=ICP-Brasil; e
d) C=BR.

8.1.3.12.1 Os elementos do *Distinguished Name* (DN) do certificado são definidos como:

a) O *Common Name* (CN) é o nome da Autoridade Certificadora definido na Declaração de Práticas da Certificação (DPC) aprovada pelo ITI;
b) O campo *Organizational Unit* (OU) com conteúdo fixo "Instituto Nacional de Metrologia Qualidade e Tecnologia INMETRO";
c) O campo *Organization Name* (O) com conteúdo fixo igual a "ICP-Brasil"; e
d) O campo *Country Name* (C) com conteúdo fixo igual a "BR".

8.1.3.12.2 No formato, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado. Por exemplo:

a) CN=AUTORIDADE CERTIFICADORA <vinculada à AC-INMETRO>;
b) OU=Instituto Nacional de Metrologia Qualidade e Tecnologia INMETRO;
c) O=ICP-Brasil; e
d) C=BR.

8.2 Extensões obrigatórias

8.2.1 *AuthorityKeyIdentifier*: Não crítica. O campo *AuthoritykeyIdentifier* deve conter o hash SHA-1 da chave pública da AC-INMETRO.

8.2.2 *SubjectKeyIdentifier*: Não crítica. O campo *SubjectKeyIdentifier* deve conter o hash SHA-1 da chave pública da AC titular do certificado.

8.2.3 *KeyUsage*: Crítica. Somente os seguintes bits devem estar ativados:

a) *KeyCertSign*; e
b) *CRLSign*.

8.2.4 *Certificate Policies*: Não crítica.

8.2.4.1 O campo *policyIdentifier* contém o OID da Política de Certificação (PC) que a AC titular do certificado implementa.

8.2.4.2 O campo *policyQualifiers* contém o endereço URL da página Web da AC-INMETRO, onde se obtém a Declaração de Práticas de Certificação (DPC) da AC-INMETRO.

8.2.5 *CRL Distribution Points*: Não crítica.

8.2.5.1 Deve conter o endereço na Web onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC-INMETRO que gerou este certificado.

8.2.5.2 Deve conter dois (2) endereços web diferentes para busca da LCR.

8.2.6 *Basic Constraints*: Crítica. Campo obrigatório, deve conter:

a) *Subject Type*=CA; e
b) *Path Length Constraint*=0 (zero).

9 LEIAUTE DO CERTIFICADO OM-BR

9.1 Requisitos do certificado

9.1.1 Os certificados do tipo Objeto Metrológico - OM-BR só podem ser emitidos para equipamentos regulados pelo Inmetro, obedecendo às Resoluções do Comitê Gestor da ICP-Brasil.

9.1.2 Os certificados OM-BR são utilizados para assinatura digital e autenticação unívoca do seu titular em sistemas e aplicações definidos em Regulamentos Técnicos de Metrologia (RTM) e/ou outros regulamentos do INMETRO.

9.1.3 Admite-se a emissão de certificados OM-BR para outros objetos caracterizados como "IoT – *Internet of Things*", desde que atendam a requisitos técnicos estabelecidos pelo INMETRO.

9.1.4 Os certificados OM-BR atendem os seguintes requisitos:

9.1.4.1 Número de versão: Os certificados digitais OM-BR implementam a versão 3 de certificados definida no padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 5280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

9.1.4.2 Campo *Issuer*: Todo certificado OM-BR possui neste campo o nome X.500 da Autoridade Certificadora habilitada pela AC-INMETRO.

9.1.4.3 Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave: O algoritmo utilizado para a geração das chaves dos certificados OM-BR é o ECDSA (brainpoolP256r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits)), definido em regulamento editado por instrução normativa da AC Raiz que define os "Padrões e Algoritmos Criptográficos da ICP-Brasil", com o seguinte requisito:

Tabela 3 – Tamanho e processo de geração de chave

Tipo	Tamanho de Chave (bits)	Processo de Geração de Chave Criptográfica
OM-BR	256 ou 448 ou 521	Hardware

Fonte:Doc-ICP-01.01

9.1.4.4 Algoritmo de Assinatura Digital: Os certificados OM-BR deverão ser assinados conforme curva utilizada.

9.1.4.5 Limite de Tamanho: O tamanho máximo de cada componente do *Distinguished Name* (DN), CN, OU, O e C, é de 64 caracteres.

9.1.4.6 Chave Pública do Titular do Certificado: Conforme definido na RFC 5280.

9.1.4.7 Identificação do Sistema Criptográfico Utilizado: Conforme definido na RFC 5280.

9.1.4.8 Conjunto de Caracteres: Todas as sequências de caracteres nos certificados, inclusive as dos *Distinguished Name* (DN) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela 2. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere 'c'.

9.1.4.9 Identificação e Assinatura Digital da Autoridade Certificadora Emitente: Conforme definido na RFC 5280.

9.1.4.10 Número de Série Exclusivo do Certificado: Conforme definido na RFC 5280.

9.1.4.11 Validade do Certificado Digital: Conforme definido na Política de Certificação OM-BR, sendo o prazo máximo limitado até 10 (dez) anos, conforme estabelecido nos regulamentos da ICP-Brasil.

9.1.4.12 Composição do *Distinguished Name* (DN) do certificado OM-BR:

a) CN=<Nome do Objeto Metrológico>;
b) OU=<Instituto Nacional de Metrologia Qualidade e Tecnologia INMETRO>;
c) OU=<OM-BR >;
d) OU=<Autoridade Certificadora habilitada pela AC-INMETRO>;
e) OU=<CNPJ da AR emissora>;
f) O=ICP-Brasil; e
g) C=BR.

9.1.4.12.1 Os elementos do *Distinguished Name* (DN) do certificado são definidos como:

a) O *Common Name* (CN) é composto do nome do objeto metrológico, obtido por meio de consulta a portaria do INMETRO, com comprimento máximo de 52 (cinquenta e dois) caracteres;
b) São quatro os campos *Organizational Unit* (OU) definidos no certificado, assim constituídos:
b.1) Primeiro "OU" com conteúdo fixo "Instituto Nacional de Metrologia Qualidade e Tecnologia INMETRO";
b.2) Segundo "OU" com conteúdo fixo "OM-BR";
b.3) Terceiro "OU" contendo o nome da Autoridade Certificadora habilitada pelo INMETRO; e
b.4) Quarto "OU" informando o CNPJ da AR responsável pelo módulo eletrônico de identificação do equipamento e fabricante;
c) O campo *Organization Name* (O) com conteúdo fixo igual a "ICP-Brasil"; e
d) O campo *Country Name* (C) com conteúdo fixo igual a "BR".

9.1.4.12.2 No formato, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado. Por exemplo:

a) CN=RTM 556/2016 Bomba Medidora de combustível;
b) OU=OM-BR;
c) OU=Instituto Nacional de Metrologia Qualidade e Tecnologia INMETRO;
d) OU=AC XXXXXXXX OM-BR;
e) OU=xxxxxxxxxxxxxx(CNPJ DA AR);
f) O=ICP-Brasil; e
g) C=BR.

9.2 Extensões obrigatórias

9.2.1 *Authority Key Identifier*: Não crítica. O campo *Key Identifier* deve conter o hash SHA-1 da chave pública da AC Habilitada que emitiu o certificado.

9.2.2 *Key Usage*: Crítica. Somente os seguintes bits devem estar ativados:

a) *DigitalSignature*;
b) *NonRepudiation*; e
c) *keyEncipherment*.

9.2.3 *Extended-Key-Usage*: Não crítica. Somente o propósito *client authentication* OID = 1.3.6.1.5.5.7.3.2 deve estar presente.

9.2.4 *Certificate Policies*: Não crítica.

9.2.4.1 O campo *policyIdentifier* contém o OID da Política de Certificação (PC) correspondente.

9.2.4.2 O campo *policyQualifiers* contém o endereço URL da página Web onde se obtém a Declaração de Práticas de Certificação (DPC) da AC Habilitada que emitiu o certificado.

9.2.5 *CRL Distribution Points*: Não crítica.

9.2.5.1 Deve conter os endereços na Web onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC Habilitada que assinou o certificado.

9.2.5.2 Deve conter dois (2) endereços web diferentes para busca da LCR.

9.2.6 *Subject Alternative Name*: Não crítica. Para certificado de equipamento OM-BR, deve conter 3 (três) campos *otherName*, obrigatórios, apresentando, nesta ordem:

9.2.6.1 Campos obrigatórios

9.2.6.1.1 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;

9.2.6.1.2 OID = 2.16.76.1.3.3 e conteúdo = o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), idêntico ao constante no certificado digital de pessoa jurídica requisitante deste, nas 14 (quatorze) posições;

9.2.6.1.3 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)

9.2.6.2 Campos Opcionais: Não permitido.

9.2.6.2.1 O conjunto de informações definido em cada campo *OtherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING, com exceção do campo *Principal Name* cuja cadeia de caracteres é do tipo UTF-8 String.

9.2.6.2.2 Para todos os campos *OtherName*, com exceção do campo *Principal Name*, apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

9.2.6.2.3 Para o preenchimento do campo *Principal Name* serão permitidos os caracteres de "A" a "Z", de "0" a "9" além dos caracteres "." (ponto), "-" (hífen) e "@" (arroba), necessários à formação do endereço de login do titular do certificado. Outros caracteres especiais, símbolos, espaços ou acentuação não são permitidos.

9.2.6.2.4 O campo *rfc822Name*, parte da extensão obrigatória *Subject Alternative Name*, contendo o endereço e-mail do titular do certificado (fabricante do objeto metrológico) também deverá estar presente.

9.2.7 ***Basic Constraints*****:** Não crítica.

9.2.7.1 Opcional,

a) *Subject Type=End Entity*; e
b) *Path Length Constraint-None*.

9.2.8 ***Authority Information Access*****:** Não crítica.

9.2.8.1 Obrigatório, com os seguintes campos:

a) Endereço de acesso ao protocolo de OCSP (*On-line Certificate Status Protocol*), conforme definido na RFC 5280; e
b) Endereço na web onde se obtêm o arquivo p7b com os certificados da cadeia da Autoridade Certificadora, conforme definido na RFC 3280.

10 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
00	Mai/2022	▪ Emissão Inicial.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Flávia Paiva Agostini	Pesquisador-Tecnologista em Metrologia e Qualidade
Verificado por:	Rodolfo Saboia Lima de Souza	Pesquisador-Tecnologista em Metrologia e Qualidade
Aprovado por:	Rodolfo Saboia Lima de Souza	Pesquisador-Tecnologista em Metrologia e Qualidade