DIÁRIO OFICIAL DA UNIÃO

Publicado em: 09/03/2021 | Edição: 45 | Seção: 1 | Página: 82

Órgão: Ministério da Economia/Instituto Nacional de Metrologia, Qualidade e Tecnologia

PORTARIA 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.

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO, no exercício da competência que lhe foi outorgada pelos artigos 4º, § 2º, da Lei nº 5.966, de 11 de dezembro de 1973, e 3º, incisos I e IV , da Lei nº 9.933, de 20 de dezembro de 1999, combinado com o disposto nos artigos 18, inciso V , do Anexo I ao Decreto nº 6.275, de 28 de novembro de 2007, e 105, inciso V , do Anexo à Portaria nº 2, de 4 de janeiro de 2017, do então Ministério da Indústria, Comércio Exterior e Serviços;

Considerando a necessidade da implantação da Autoridade Certificadora do Inmetro, e da vinculação de Autoridades Certificadoras de Segundo nível;

Considerando o que consta no Processo SEI nº 0052600.002119/2021-94, resolve:

Art. 1º O processo de certificação digital para Objetos Metrológicos, e da habilitação de Autoridades Certificadoras de Segundo Nível observará o disposto nesta Portaria.

CAPÍTULO I

DO LEIAUTE DOS CERTIFICADOS DIGITAIS DA AC INMETRO

Art. 2º Fica aprovado o Leiaute dos Certificados Digitais da Autoridade Certificadora Inmetro Versão 1.0, segundo anexo I desta portaria.

CAPÍTULO II

DAS AUTORIDADES CERTIFICADORAS HABILITADAS

Art. 3º O INMETRO habilitará as Autoridades Certificadoras que emitirão os certificados digitais para objetos metrológicos (OM-BR), por intermédio da AC-INMETRO, no âmbito da ICP-Brasil.

Art. 4º Poderá ser autorizada a emitir os certificados digitais OM-BR, na condição de Autoridade Certificadora Habilitada pela AC-INMETRO, a pessoa jurídica que:

I - atender a todos os requisitos estabelecidos para o credenciamento de Autoridades Certificadoras no âmbito da ICP-Brasil.

Parágrafo único. Para fins do disposto neste artigo, a pessoa jurídica deverá protocolar no Inmetro a documentação comprobatória do atendimento das condições para credenciamento junto à ICP-Brasil e habilitação junto ao INMETRO.

Art. 5º São atribuições da Autoridade Certificadora Habilitada:

I - emitir e revogar certificados digitais de objetos metrológicos;

II - adotar as medidas necessárias para garantir a confidencialidade de sua chave privativa e solicitar, imediatamente, à AC-INMETRO a revogação de seu certificado caso constatado comprometimento da segurança deste;

III - manter, na Internet, de forma permanente e para acesso público, lista dos certificados digitais OM-BR revogados;

IV - disponibilizar para a AC-INMETRO, com atualização diária, lista dos certificados digitais emitidos e sua respectiva situação;

V - disponibilizar, na Internet, sua Declaração de Práticas de Certificação (DPC) e a Política de Certificados (PC) para OM-BR implementada, aprovadas pelo Inmetro, observada a legislação aplicável;

VI - contratar auditoria independente com a finalidade de verificar, a cada 12 (doze) meses, o correto exercício das atividades de Autoridade Certificadora Habilitada; e

VII - informar, imediatamente, ao INMETRO todas as revogações de certificados digitais efetuadas.

§ 1º O resultado da auditoria prevista no inciso VI do caput deverá ser encaminhado ao Inmetro.

§ 2º A habilitação da Autoridade Certificadora será cancelada pelo Inmetro em caso de descumprimento de obrigação prevista neste artigo.

Art. 6º A Autoridade Certificadora responderá pelas perdas e danos sofridos pelos usuários ou por terceiros em consequência do descumprimento de obrigação prevista e pelos prejuízos decorrentes da emissão ou revogação indevidas de certificado digital, ou ainda da ausência de revogação deste em prazo hábil.

Art. 7º Em caso de encerramento das atividades ou de cancelamento da habilitação da Autoridade Certificadora:

I - todos os certificados por ela emitidos perderão sua validade e não serão mais aceitos; e

II - toda a documentação referente ao processo de emissão de certificados digitais OM-BR deverá ser imediatamente entregue ao INMETRO.

Parágrafo único. O INMETRO poderá autorizar nova emissão dos certificados referidos no inciso II por outra Autoridade Certificadora Habilitada, à qual deverá ser transferida toda a documentação a eles referente.

CAPÍTULO III

DA AUTORIDADE CERTIFICADORA DO INMETRO

Art. 8º O Inmetro atuará como AC-INMETRO por intermédio da Divisão de Metrologia em Tecnologia da Informação e Telecomunicações (DMTIC), à qual compete:

I - gerenciar o processo de emissão e uso dos certificados digitais do Inmetro;

II - analisar as solicitações de credenciamento e habilitação;

III - autorizar a Autoridade Certificadora a assinar os certificados digitais OM-BR por ela emitidos, no âmbito da ICP Brasil;

IV - emitir certificados para as Autoridades Certificadoras credenciadas pela ICP-Brasil e habilitadas pelo Inmetro;

V - revogar os certificados das Autoridades Certificadoras referidas no inciso IV que deixarem de cumprir os requisitos estabelecidos;

VI - manter, na Internet, de forma permanente e para acesso público, lista assinada e atualizada dos certificados emitidos e revogados de Autoridades Certificadoras Habilitadas;

VII - elaborar toda a documentação técnica necessária à operação da AC-INMETRO;

VIII - auditar, periodicamente, as atividades das Autoridades Certificadoras Habilitadas;

IX - analisar os relatórios de auditorias executadas por empresas de auditoria independente nas Autoridades Certificadoras Habilitadas;

X - notificar, com antecedência mínima de 13 (treze) meses, o vencimento dos certificados das Autoridades Certificadoras referidas no inciso IV;

XI - identificar e registrar todas as ações executadas pela AC-INMETRO;

XII - publicar os certificados emitidos para as Autoridades Certificadoras Habilitadas no Diário Oficial da União; e

XIII - arquivar toda a documentação referente ao processo de credenciamento e habilitação das Autoridades Certificadoras, bem como as solicitações de emissão e revogação de certificados digitais.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 9º Esta Portaria entrará em vigor na data de sua publicação no Diário Oficial da União.

MARCOS HELENO GUERSON DE OLIVEIRA JUNIOR

ANEXO I

LEIAUTE DOS CERTIFICADOS DIGITAIS DA AUTORIDADE CERTIFICADORA INMETRO VERSÃO 1.0

1. LEIAUTE DO CERTIFICADO DA AUTORIDADE CERTIFICADORA

1.1 Requisitos de Certificado

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

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.

1.1.1 Número de Versão

Os certificados digitais implementam a versão 3 de certificados definida no padrão ITU-TX.509 de acordo com o perfil estabelecido na RFC 5280 (Request for Comments - Internet X509 Public Key Infrastructure).

1.1.2 Campo Issuer

Todo certificado possui neste campo o nome X.500 da Autoridade Certificadora do Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro.

1.1.3 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).

Tamanho de Chave	Processo de Geração de Chave Criptográfica
448	Hardware

1.1.4 Algoritmo de Assinatura Digital

Os certificados deverão ser assinados com uso do algoritmo conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01).

1.1.5 Limite de Tamanho

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

1.1.6 Chave Pública do Titular do Certificado

Conforme definido na RFC 5280.

1.1.7 Identificação do Sistema Criptográfico Utilizado

Conforme definido na RFC 5280.

1.1.8 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 abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere 'c'.

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21
"	22
	#23

$	24
%	25
&	26
'	27
(	28
))	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

1.1.9 Identificação e Assinatura Digital da Autoridade Certificadora do INMETRO

Conforme definido na RFC 5280.

1.1.10 Número de Série Exclusivo do Certificado

Conforme definido na RFC 5280.

1.1.11 Validade do Certificado Digital

Conforme definido na Política de Certificação com validade igual ou inferior a validade do certificado da AC-INMETRO.

1.1.12 Composição do Distinguished Name (DN) do certificado

CN=<Nome da Autoridade Certificadora Habilitada>

OU= Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO

O=ICP-Brasil

C=BR

Onde:

O Common Name (CN) é o nome da Autoridade Certificadora definido na Declaração de Práticas da Certificação (DPC) aprovada pelo ITI.

O campo Organizational Unit (OU) com conteúdo fixo "Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO".

O campo Organization Name (O) com conteúdo fixo igual a "ICP-Brasil".

O campo Country Name (C) om conteúdo fixo igual a "BR".

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

Exemplo:

CN= AUTORIDADE CERTIFICADORA <vinculada à AC-INMETRO>

OU= Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro

O=ICP-Brasil

C=BR

1.2 Extensões Obrigatórias.

1.2.1 AuthorityKeyIdentifier

Não crítica

O campo keyIdentifier deve conter o hash SHA-1 da chave pública da AC-INMETRO.

1.2.2 SubjectKeyIdentifier

Não critica

O campo SubjectKeyIdentifier deve conter o hash SHA-1 da chave pública da AC titular do certificado.

1.2.3 KeyUsage

Crítica

Somente os seguintes bits devem estar ativados:

KeyCertSign; e

CRLSign.

1.2.4 Certificate Policies

Não crítica

- o campo policyIdentifier contém o OID da Política de Certificação (PC) que a AC titular do certificado implementa;

- 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.

1.2.5 CRL Distribution Points

Não crítica

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

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

1.2.6 Basic Constraints

Crítica

Obrigatório, deve conter;

- Subject Type=CA; e

- Path Lenght Constraint=0 (zero).

2. LEIAUTE DO CERTIFICADO OM-BR

2.1. Requisitos de Certificado

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.

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.

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.

Os certificados OM-BR atendem os seguintes requisitos:

2.1.1. 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).

2.1.2. Campo Issuer

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

2.1.3. 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 [1] (Elliptic Curve Digital Signature Algorithm), com o seguinte requisito:

Tipo	Tamanho de Chave [2] (bits)	Processo de Geração de Chave Criptográfica
OM-BR	256 ou 448 ou 521	Hardware

2.1.4. Algoritmo de Assinatura Digital

Os certificados OM-BR deverão ser assinados conforme curva utilizada.

2.1.5. Limite de Tamanho

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

2.1.6. Chave Pública do Titular do Certificado

Conforme definido na RFC 5280.

2.1.7. Identificação do Sistema Criptográfico Utilizado

Conforme definido na RFC 5280.

2.1.8. 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 abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere 'c'.

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

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

2.1.9. Identificação e Assinatura Digital da Autoridade Certificadora Emitente

Conforme definido na RFC 5280.

2.1.10. Número de Série Exclusivo do Certificado

Conforme definido na RFC 5280.

2.1.11. 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.

2.1.12. Composição do Distinguished Name (DN) do certificado OM-BR

CN=<Nome do Objeto Metrológico>

OU= <Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO>

OU=<OM-BR >

OU= <Autoridade Certificadora habilitada pela AC-INMETRO>

OU= <CNPJ da AR emissora>

O=ICP-Brasil

C=BR

Onde:

O Common Name (CN) é composto do nome do objeto metrológico, obtido por meio de consulta a portaria do INMETRO, com cumprimento máximo de 52 (cinquenta e dois) caracteres.

São quatro os campos Organizational Unit (OU) definidos no certificado, assim constituídos:

Primeiro "OU" com conteúdo fixo "Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO";

Segundo "OU" com conteúdo fixo "OM-BR";

Terceiro "OU" contendo o nome da Autoridade Certificadora habilitada pelo INMETRO

Quarto "OU" com informando o CNPJ da AR responsável pelo módulo eletrônico de identificação do equipamento e fabricante;

O campo Organization Name (O) com conteúdo fixo igual a "ICP-Brasil".

O campo Country Name (C) com conteúdo fixo igual a "BR".

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

Exemplo:

CN=RTM 556/2016 Bomba Medidora de combustível

OU=OM-BR

OU= Instituto Nacional de Metrologia, Qualidade e Tecnologia - INMETRO

OU=AC XXXXXXXX OM-BR

OU= xxxxxxxxxxxxxx(CNPJ DA AR)

O=ICP-Brasil C=BR

2.2. Extensões Obrigatórias.

2.2.1. 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.

2.2.2. Key Usage

Crítica

Somente os seguintes bits devem estar ativados:

DigitalSignature;

NonRepudiation; e

keyEncipherment.

2.2.3. Extended-Key-Usage

Não crítica

Somente o propósito client authentication OID = 1.3.6.1.5.5.7.3.2 deve estar presente;

2.2.4. Certificate Policies

Não crítica

O campo policyIdentifier contém o OID da Política de Certificação (PC) correspondente;

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.

2.2.5. CRL Distribution Points

Não crítica

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

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

2.2.6. Subject Alternative Name

Não crítica

Para certificado de equipamento OM-BR, 3 (três) campos otherName, obrigatórios, contendo, nesta ordem:

Campos Obrigatórios

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;

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 (modelo e número de série)

Campos Opcionais

Não permitido

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.

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.

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.

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.

2.2.7. Basic Constraints

Não crítica

Opcional,

- Subject Type= End Entity; e

- Path Length Constraint-None.

2.2.8. Authority Information Access

Não crítica

Obrigatório

Com os seguintes campos:

- Endereço de acesso ao protocolo de OCSP (On-line Certificate Status Protocol), conforme definido na RFC 5280;

- Endereço na web onde se obtêm o arquivo p7b com os certificados da cadeia da Autoridade Certificadora, conforme definido na RFC 3280.

[1] Algoritmos definidos para certificado do tipo OM-BR: ECC-Brainpool ou Curve25519 ou Ed25519 ou Ed448-Goldilocks ou E-521, conforme PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL DOC-ICP-01.01 da ICP-Brasil.

[2] Tamanho de chaves conforme algoritmo utilizado: brainpoolP256r1 ou Curve25519 (256 bits) ou Ed25519 (256 bits) ou Ed448 (448 bits) ou E-521 (521 bits) PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL DOC-ICP-01.01 da ICP-Brasil.