SUMÁRIO

1 OBJETIVO

Esta norma estabelece o formato da assinatura digital produzida por Certificados Digitais para Objetos Metrológicos (OM-BR).

2 CAMPO DE APLICAÇÃO

Esta norma se aplica, compulsoriamente, 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	Requisitos para a elaboração e revisão da documentação do SGQI
DOC-ICP-15 – V.4.0	Visão Geral Sobre Assinaturas Digitais na ICP-Brasil
Portaria nº 559, de 15 de dezembro de 2016.	Regulamento Técnico Metrológico (RTM) que estabelece as condições técnicas e metrológicas mínimas e de segurança de software e hardware a que devem atender as bombas medidoras de combustíveis líquidos utilizadas nas medições de volume.

5 DOCUMENTOS COMPLEMENTARES

NIT-Sinst-020	Protocolo de Comunicação Serial para Verificação de Integridade de Software em Instrumentos de Medição.
Request for Comments (RFC) 2315	*PKCS #7: Cryptographic Message Syntax Version 1.5. IETF,* mar. 1998. Disponível em: http://www.ietf.org/rfc/rfc2315.txt.
Request for Comments (RFC) 5652	*Cryptographic Message Syntax (CMS).* IETF, sept. 2009. Disponível em: http://www.ietf.org/rfc/rfc5652.txt.

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
ASCII	*American Standard Code for Information Interchange* (Código Padrão Americano para o Intercâmbio de Informação)
CMS	*Cryptographic Message Syntax* (Sintaxe de Mensagens Criptográficas
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira)
IETF	*Internet Engineering Task Force* (Força-Tarefa de Engenharia da Internet
OM	Objeto Metrológico)
PKCS	*Public Key Cryptography Standards* (Padrões de Criptografia de Chave Pública
RFC	*Request for Comments* Solicitação de Comentários)
RTM	Regulamento Técnico Metrológico
TI	Tecnologia da Informação
W3C	*World Wide Web Consortium* (Consórcio *World Wide Web*)

7 TERMOS E DEFINIÇÕES

7.1 Assinatura digital ICP-Brasil

É a assinatura eletrônica que:

a) esteja associada inequivocamente a um par de chaves criptográficas que permita identificar o signatário;
b) seja produzida por dispositivo seguro de criação de assinatura;
c) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer alteração subsequente neste seja plenamente detectável; e
d) esteja baseada em um certificado ICP-Brasil, válido à época da sua aposição.

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 serão utilizados exclusivamente em equipamentos metrológicos regulamentados pelo Inmetro, como bombas de combustível, balanças, taxímetros, dispositivos de controle de velocidade, medidores de consumo de água, energia e gás, entre outros. Para certificados do tipo OM-BR, o titular do certificado será o fabricante, que fará a solicitação do certificado OM-BR com uso de certificado digital ICP-Brasil de pessoa jurídica válido, do fabricante autorizado pelo Inmetro.

8 FORMATO DE ASSINATURAS DIGITAIS PARA CERTIFICADOS DIGITAIS OM-BR

8.1 Motivação

8.1.1 A AC-Inmetro é responsável por estabelecer regras e políticas que permitem a emissão e o gerenciamento de certificados digitais de objetos metrológicos OM-BR com segurança.

8.1.2 A utilização de formatos padronizados de assinatura digital criada por objeto metrológico para o qual um certificado digital OM-BR foi emitido é essencial para a confiabilidade e credibilidade do processo de criação e validação da assinatura. A utilização dos formatos propostos favorece a interoperabilidade e minimiza riscos associados à utilização de formatos de assinatura inadequados para o tipo de documento ou para o tipo de compromisso que está sendo selado com aquela assinatura.

8.1.3 Para propiciar a larga utilização de assinaturas digitais é necessário definir as diretrizes técnicas a serem adotadas para que os processos de geração e verificação de assinaturas digitais sejam realizados de forma padronizada e com requisitos de segurança suficientes para garantir, a médio e longo prazo, a recuperação das assinaturas e documentos eletrônicos, bem como a determinação de sua autoria e integridade.

8.1.4 Nesse contexto, portanto, a definição de formatos sobre assinatura digital criada por objeto metrológico para o qual um certificado digital OM-BR foi emitido apresenta as seguintes motivações:

a) auxiliar entidades na adoção de normas e condutas técnicas comuns que possam ser utilizadas em sistemas de assinatura digital;
b) consolidar e popularizar o uso seguro da assinatura digital;
c) desenvolver a interoperabilidade entre sistemas que utilizam a assinatura digital para agilizar seus processos e aplicações;
d) uniformizar os esforços na definição dos requisitos técnicos de segurança e interoperabilidade para assinaturas digitais, possibilitando maior pragmatismo e concentração de esforços na implementação dos sistemas de assinatura digital;
e) aprimorar a relação custo/benefício em processos e aplicações de TI; e
f) melhorar a competência técnica de entidades na utilização de assinaturas digitais.

8.1.5 É recomendado que as assinaturas digitais sejam criadas com características apropriadas à finalidade e longevidade esperada. Uma assinatura digital pode incorporar elementos que permitam uma validação confiável a longo prazo, o que, em contrapartida, aumenta o tamanho do arquivo e o tempo gasto na geração da assinatura.

8.1.6 O padrão CMS dispõe de ampla documentação e de variada gama de bibliotecas de *software* disponíveis. É o padrão mais utilizado, atualmente, nas aplicações em nível mundial.

8.2 Padrões para assinatura digital

8.2.1 A AC-Inmetro estabelece o formato CMS (descrito pela RFC 5652) para representação de assinatura digital criada por objeto metrológico para o qual um certificado digital OM-BR foi emitido.

8.3 CMS (*Cryptographic Message Syntax*)

8.3.1 O padrão CMS é uma evolução do padrão PKCS#7. A versão CMS utilizada como referência neste documento é a descrita na RFC 5652. O padrão CMS descreve uma estrutura para armazenamento de conteúdos (dados) assinados digitalmente, conteúdos cifrados, conteúdos autenticados e conteúdos com resumos criptográficos. Este documento trata especificamente do tipo de conteúdo *Signed-data*, relevante para o contexto de assinatura digital.

8.3.2 As aplicações de interesse do tipo de conteúdo *signed-data* são a assinatura digital sobre o tipo de conteúdo "data" e a disseminação de certificados.

8.3.3 Quando usado para representar o conteúdo digital assinado, a inclusão do conteúdo digital propriamente dito é opcional e, por este motivo, permite a existência de duas representações diferentes:

a) estrutura assinada com conteúdo digital anexado (*attached*): neste caso, o pacote de dados está incluído na estrutura CMS; e
b) estrutura assinada com conteúdo digital separado (*detached*): neste caso, o pacote de dados não está incluído na estrutura CMS.

8.3.4 Além dos atributos assinados (ou seja, que fazem parte do cálculo do resumo criptográfico, sobre o qual a assinatura será gerada), o CMS permite adicionar atributos não assinados, bem como gerar assinaturas em paralelo e assinaturas em série. O CMS não permite, todavia, assinar partes de um documento, somente o documento como um todo.

8.3.5 Para aderência ao padrão CMS, todos os campos não opcionais do tipo de conteúdo *Signed-data* da RFC 5652 devem estar contidos na representação da assinatura digital.

8.4 Exemplo de como gerar as assinaturas digitais no formato CMS é apresentados no Anexos A.

Nota 1 – É recomendada a estrutura assinada com conteúdo digital separado (*detached*) no padrão CMS para aderência à NIT-Sinst-020.

Nota 2 – É recomendado que os arquivos com assinaturas digitais ICP-Brasil sejam gerados com as extensões p7s e xml.

9 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
01	Jun/2023	▪ Remoção do item 8.4 (XMLDSig) e Anexo B (EXEMPLO: GERAÇÃO DE ASSINATURA DIGITAL XMLDSIG (DETACHED) COM JAVA)

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

/ANEXO A

ANEXO A – EXEMPLO: ASSINATURA DIGITAL CMS DETACHED COM A OPENSSL POR LINHA DE COMANDO

A-1 COMANDO PARA ASSINAR

A-1.1 A utilização do comando seguinte permite a criação de um arquivo assinado de tamanho reduzido, desejável considerando a aplicação em objetos metrológicos.

openssl cms -sign -nocerts -nosmimecap -keyid -noattr -binary -in $filein -out $fileout -signer $cert -inkey $privatekey -outform der

A-1.2 flags:

a) -sign. Assina o arquivo de entrada utilizando a chave privada e o certificado fornecidos;
b) -nocerts. Não inclui o certificado no arquivo de saída;
c) -nosmimecap. Exclui a lista de algoritmos suportados dos atributos que são assinados;
d) -keyid. Utiliza o *subject key identifier* para identificar o assinante;
e)-noattr. Não inclui atributos assinados no arquivo de saída;
f) -binary. Trata o arquivo entrada como dados binários
g) -in. Arquivo entrada a ser assinado;
h) -out. Arquivo saída contendo a assinatura digital;
i) -signer. Arquivo entrada contendo o certificado digital associado à chave privada usada;
j) -inkey. Arquivo entrada contendo a chave privada usada; e
k) -outform der. Estabelece o formato DER para o arquivo CMS que é criado.

A-2 COMANDO PARA VERIFICAR

openssl cms -verify -certfile $cert -inform der -binary -in $infile -content $originalfile -noverify

A-2.1 flags:

a) -verify. Verifica a assinatura digital com base no certificado e arquivos fornecidos;
b) -certfile. Certificado digital a ser utilizado para verificar a assinatura digital;
c) -inform der. Formato da assinatura digital;
d) -binary. Trata o arquivo entrada ($originalfile acima) como dados binários;
g) -in. Arquivo entrada contendo a assinatura digital;
d) -content. Arquivo entrada o qual foi assinado;
e)-noverify. Não verifica o certificado digital;