INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA Nº 02, DE 09 DE JANEIRO DE 2009.

Aprova a versão 1.0 do PERFIL PARA ASSINATURAS DIGITAIS NA ICP-BRASILL.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso I, do art. 1º, do anexo I, do Decreto nº 4.689, de 7 de maio de 2003, e pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004;

R E S O L V E :

Art. 1º Fica aprovada a versão 1.0 do documento PERFIL PARA ASSINATURAS DIGITAIS NA ICP-BRASIL (DOC-ICP-15.02), em anexo.

Art. 2º Esta Instrução Normativa entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI

ANEXO

PERFIL DE USO GERAL PARA ASSINATURAS DIGITAIS NA ICP-BRASIL

DOC-ICP-15.02

Versão 1.0

1. INTRODUÇÃO

1.1. Este documento define um perfil para assinatura digital ICP-Brasil que contêm um sub-conjunto dos atributos/propriedades definidos nos padrões CadES [1] e XadES [2]. Tal perfil foi criado com o objetivo de minimizar as diferenças entre implementações e maximizar a interoperabilidade das aplicações para geração e verificação de assinaturas digitais.

1.2 Este documento está associado a um conjunto de normativos criados para regulamentar a geração e verificação de assinaturas digitais no âmbito da Infra-estrutura de Chaves Públicas

Brasileira - ICP-Brasil. Tal conjunto se compõe de:

a) VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15 [9];

b) REQUISITOS MÍNIMOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15.01 [10];

c) PERFIL PARA ASSINATURAS DIGITAIS NA ICP-BRASIL – USO GERAL – DOC-ICP-15.02 (este documento);

d) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE ASSINATURA NA ICP-BRASIL – DOC-ICP-15.03 [11].

1.3 Recomenda-se a leitura prévia dos documentos listados nos itens 1.2.a) e 1.2.b) para melhor compreensão do contexto deste normativo.

1.4 As diretrizes aqui constantes DEVEM ser observadas por todas as entidades da ICP-Brasil, em especial pelos desenvolvedores de aplicações para geração/verificação de assinatura digital.

1.5 Este documento adota como referência, além das normas da ICP-Brasil, os padrões internacionais relacionados no item 5 – BIBLIOGRAFIA.

2. TERMINOLOGIA

Os termos abaixo, quando encontrados ao longo deste documento grafados em **maiúsculas**, DEVEM ser interpretados conforme descrito neste item:

2.1 **DEVE (D)** - Esta palavra, ou os termos "**EXIGIDO**" ou "**OBRIGATÓRIO**, significa que a definição é um requisito absoluto da especificação.

2.2 **NÃO DEVE (ND)** - Esta expressão significa que a definição é uma proibição absoluta na especificação.

2.3 **É RECOMENDADO (R)** - Esta expressão, ou o adjetivo "**RECOMENDADO**", significa que podem existir razões válidas, em circunstâncias particulares, para ignorar um ponto específico, mas as implicações completas precisam ser entendidas e ponderadas cuidadosamente antes de escolher um caminho diferente.

2.4 **NÃO É RECOMENDADO (NR)** - Esta expressão significa que podem existir razões válidas, em circunstâncias particulares, em que o comportamento possa ser aceitável ou mesmo útil, mas as implicações completas devem ser entendidas e ponderadas cuidadosamente, antes de se realizar qualquer comportamento descrito com este rótulo.

2.5 **PODE (P)** - Esta palavra, ou o adjetivo **"OPCIONAL",** significa que é um item verdadeiramente opcional. Um implementador pode optar por incluir o item, enquanto outro pode omitir o mesmo item. Uma aplicação que não inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que inclui aquela opção, embora talvez com funcionalidade reduzida. No mesmo espírito, uma aplicação que inclui uma determinada opção DEVE estar preparada para interoperar com outra aplicação que não a inclui (exceto, é claro, para o recurso que a opção oferece.)

3. PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES CMS / CAdES

3.1. Atributos assinados

Atributo	Ref [1]	Obrigatoriedade	Requisitos adicionais / Observações
id-aa-ets-commitmentType	5.11.1	P	O tipo de comprometimento empregado DEVE ser reconhecido pelas partes geradora e verificadora de modo que ambas as partes estejam cientes das implicações associadas ao seu uso, ou DEVE ser um dos tipos registrados conforme Anexo 1 do DOC-ICP-15.01 [10]
id-aa-ets-contentTimestamp	5.11.4	P	Os carimbos do tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [8].
id-aa-ets-signerAttr	5.11.3	P	
id-aa-ets-signerLocation	5.11.2	P	Nos processos de assinatura digital, caso o signatário deseje informar o local físico onde a assinatura digital foi gerada, esse DEVE ser expresso, no mínimo, pela combinação de dois elementos: a) Identificador do país, como especificado no padrão internacional ISO 3166. No caso do Brasil, esse valor é **76** (setenta e seis) b) Localidade: Nome do Município-UF
id-signingTime	5.9.1	P	
id-contentType	5.7.1	D	
id-messageDigest	5.7.2	D	
id-aa-signingCertificate ou id-aa-signingCertificateV2	5.7.3	D	DEVE-se migrar para o uso do atributo *ESS signing-certificate v2* em detrimento do atributo *ESS signing-certificate* dada a estimativa de tempo de vida do algoritmo *SHA-1*. Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [4].
id-aa-ets-sigPolicyId	5.7.3	D	

3.2 Atributos não assinados

Atributo	Ref. [1]	Obrigatoriedade	Requisitos adicionais / Observações
id-countersignature	5.9.2	P	Contra-assinaturas são empregadas quando a ordem de aplicação das assinaturas é relevante, ou seja, quando a função da segunda assinatura é, no mínimo, atestar o recebimento do documento com a primeira assinatura já presente. O uso de contra-assinaturas DEVE ser previamente acordado entre as partes geradora e verificadora, de modo que o verificador esteja ciente da presença, número, e significado da contra-assinatura.
id-aa-signatureTimeStampToken	6.1.1	P	Os carimbos de tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [8].
id-aa-ets-certificateRefs	6.2.1	P	Certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [6].
id-aa-ets-revocationRefs	6.2.2	P	Listas de Certificados Revogados empregadas DEVEM atender ao perfil definido no documento DOC-ICP-04 [6].
id-aa-ets-attrCertificateRefs	6.2.3	P	
id-aa-ets-attrRevocationRefs	6.2.4	P	
id-aa-ets-escTimeStamp	6.3.5	P	Os carimbos de tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [8].
id-aa-ets-certValues	6.3.3	P	Certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [6]. Conforme especificado no documento DOC-ICP-05 [7], cláusula 4.6.2, os certificados de assinatura digital são retidos permanentemente pelas ACs da ICP-Brasil para fins de consulta histórica.
id-aa-ets-revocationValues	6.3.4	P	Conforme especificado no documento DOC-ICP-05 [7], cláusula 4.6.2, as LCRs são retidas permanentemente pelas ACs da ICP-Brasil para fins de consulta histórica.
id-aa-ets-archiveTimestamp	6.4.1	P	Carimbos do tempo empregados

			DEVEM atender ao perfil definido no documento DOC-ICP-12 [8].

4 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES XMLdSIG / XAdES

4.1 Propriedades Assinadas

Propriedade	Ref [2]	Obrigatoriedade	Requisitos adicionais / Observações
CommitmentTypeIndication	7.2.6	P	O tipo de comprometimento empregado DEVE ser reconhecido pelas partes geradora e verificadora de modo que ambas as partes estejam cientes das implicações associadas ao seu uso, ou DEVE ser um dos tipos registrados conforme Anexo 1 do DOC-ICP-15.01 [10].
SignatureProductionPlace	7.2.7	P	Nos processos de assinatura digital, caso o signatário deseje informar o local físico onde a assinatura digital foi gerada, esse DEVE ser expresso, no mínimo, pela combinação de dois elementos: c) Identificador do país, como especificado no padrão internacional ISO 3166. No caso do Brasil, esse valor é **76** (setenta e seis) d) Localidade: Nome do Município-UF
SignerRole	7.2.8	P	
SigningTime	7.2.1	P	
AllDataObjectsTimeStamp	7.2.9	P	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [8].
IndividualDataObjectsTimeStamp	7.2.10	P	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [8].
DataObjectFormat	7.2.5	X	
SigningCertificate	7.2.2	D	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [6].
SignaturePolicyIdentifier	7.2.3	D	

Obs.: ***X*** *significa que a presença da propriedade é OBRIGATÓRIA para assinaturas do tipo detached. Para assinaturas do tipo enveloping e enveloped a propriedade é OPCIONAL.*

4.2 Propriedades Não-assinadas

Propriedade	Ref. [2]	Obrigatoriedade	Requisitos adicionais / Observações
CounterSignature	7.2.4	P	Contra-assinaturas são empregadas quando a ordem de aplicação das assinaturas é relevante, ou seja, quando a função da segunda assinatura é, no mínimo, atestar o recebimento do documento com a primeira assinatura presente. O uso de contra-assinaturas DEVE ser previamente acordado entre as partes geradora e verificadora, de modo que o verificador esteja ciente da presença, número e significado da assinatura paralela.
SignatureTimeStamp	7.3	P	Os carimbos do tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [8].
CompleteCertificateRefs	7.4.1	P	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [6].
CompleteRevocationRefs	7.4.2	P	As LCRs empregadas DEVEM atender ao perfil definido no documento DOC-ICP-04 [6].
AttributeCertificateRefs	7.4.3	P	
AttributeRevocationRefs	7.4.4	P	
SigAndRefsTimeStamp	7.5.1	P	Os carimbos do tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [8].
CertificateValues	7.6.1	P	Conforme especificado no documento DOC-ICP-05, cláusula 4.6.2, os certificados de assinatura digital são retidos permanentemente pelas ACs da ICP-Brasil para fins de consulta histórica. Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [6].
RevocationValues	7.6.2	P	Conforme especificado no documento DOC-ICP-05, cláusula 4.6.2, as LCRs são retidas

			permanentemente pelas ACs da ICP-Brasil para fins de consulta histórica. As LCRs empregadas DEVEM atender ao perfil definido no documento DOC-ICP-04 [6].
AttrAuthoritiesCertValues	7.6.3	P	
AttributeRevocationValues	7.6.4	P	
ArchiveTimeStamp	7.7	P	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [8].

5 BIBLIOGRAFIA

[1] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Electronic Signatures and Infrastructures (ESI): CMS Advanced Electronic Signatures (CAdES). Technical Specification. ETSI TS 101 733 v 1.7.3, Jan. 2007.

[2] ETSI. XML Advanced Electronic Signatures (XAdES); ETSI TS 101 903 (2006-03); European Telecomunications Standards Institute, 2006.

[3] HOUSLEY, R. Cryptographic Message Syntax (CMS). Internet Engineering Task Force (IETF). Jul. 2004.

[4] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Electronic Signatures and Infrastructures: Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES). Technical Specification. ETSI TS 101 734 v1.1.1. Feb. 2007.

[5] ETSI. Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES); ETSI TS 102 904 (2007-02); European Telecomunications Standards Institute, 2007.

[6] ITI. REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL DOC-ICP-04 - Instituto Nacional de Tecnologia da Informação. Versão 2.0; Brasília: ICP-Brasil, 2006.

[7] ITI. REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL DOC-ICP-05 - Instituto Nacional de Tecnologia da Informação. Versão 2.1; Brasília: ICP-Brasil, 2007.

[8] ITI. REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL DOC-ICP-12 - V 1.0

[9] ITI. VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15 - Instituto Nacional de Tecnologia da Informação. Versão - V 1.0

[10] ITI. REQUISITOS MÍNIMOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15.01 - Instituto Nacional de Tecnologia da Informação. Versão - V 1.0

[11] ITI. REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE ASSINATURA NA ICP-BRASIL – DOC-ICP-15.03 - Instituto Nacional de Tecnologia da Informação. Versão - V 1.0

6. DOCUMENTOS REFERÊNCIADOS

Os documentos abaixo são aprovados por Resolução do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Código	Nome do Documento
DOC-ICP-04	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL
DOC-ICP-05	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL
DOC-ICP-12	MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL
DOC-ICP-15	VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL
DOC-ICP-15.01	REQUISITOS MÍNIMOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL
DOC-ICP-15.03	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE ASSINATURA NA ICP-BRASIL