PERFIL PARA ASSINATURAS CADES

NA ICP-BRASIL

DOC-ICP-15.01

Versão 1.0

Sumário

1. INTRODUÇÃO

1.1. Este documento define um perfil, ou seja, um sub-conjunto dos atributos definidos no padrão CADES, com o objetivo de minimizar as diferenças entre implementações e maximizar a interoperabilidade das aplicações que utilizam aquele padrão para geração e verificação de assinaturas digitais.

1.2 Ele 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) ASSINATURAS DIGITAIS NA ICP-BRASIL – DOC-ICP-15

b) PERFIL PARA ASSINATURAS CADES ICP-BRASIL – DOC-ICP-15.01

c) REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE ASSINATURA NA ICP-BRASIL – DOC-ICP-15.03

c) POLÍTICA DE ASSINATURA ICP-BRASIL PADRÃO CADES – DOC-ICP-15.04

1.3 Recomenda-se a leitura prévia do documento listado no item 1.2.a) 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 4 – BILBIOGRAFIA.

2. ATRIBUTOS CADES RECONHECIDOS PELA ICP-BRASIL

2.1. Atributos assinados

Atributo	Referência CADES [2]	Requisitos adicionais / Observações
id-aa-contentHint	5.10.3	
id-aa-contentIdentifier	5.10.2	
id-aa-contentReference	5.10.1	
id-aa-ets-commitmentType	5.11.1	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.
id-aa-ets-contentTimestamp	5.11.4	Os carimbos do tempo utilizados devem seguir o perfil definido no documento DOC-ICP-12.
id-aa-ets-signerAttr	5.11.3	
id-aa-ets-signerLocation	5.11.2	Nos processos de assinatura digital, o local físico onde aparentemente a assinatura digital foi gerada deve ser expresso, no mínimo, mas não limitado à combinação de dois elementos: ▪ Identificador do país, como especificado no padrão internacional ISO 3166. No caso do Brasil, esse valor é **76** (setenta e seis) ▪ Código postal. No caso do Brasil, usar o CEP, definido pelos Correios
id-signingTime	5.9.1	
id-contentType	5.7.1	
id-messageDigest	5.7.2	
id-aa-signingCertificate ou id-aa-signingCertificateV2	5.7.3	Desenvolvedores devem 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.
id-aa-sigPolicyId	5.7.3	

2.2.Atributos não assinados

Atributo	Referência CADES [2]	Requisitos adicionais / Observações
id-countersignature	5.9.2	Contra-assinaturas devem ser 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	Os carimbos de tempo utilizados devem seguir o perfil definido no documento DOC-ICP-12.
id-aa-ets-certificateRefs	6.2.1	Certificados digitais empregados devem atender ao perfil definido no documento DOC-ICP-04.
id-aa-ets-revocationRefs	6.2.2	Listas de Certificados Revogados empregadas devem atender ao perfil definido no documento DOC-ICP-04.
id-aa-ets-attrCertificateRefs	6.2.3	
id-aa-ets-attrRevocationRefs	6.2.4	
id-aa-ets-escTimeStamp	6.3.5	Os carimbos de tempo utilizados devem seguir o perfil definido no documento DOC-ICP-12.
id-aa-ets-certValues	6.3.3	Certificados digitais empregados devem atender ao perfil definido no documento DOC-ICP-04. Conforme especificado no documento DOC-ICP-05, cláusula 4.6.2, os certificados de assinatura digital são retidos permanentemente pelas AC da ICP-Brasil para fins de consulta histórica.
id-aa-ets-revocationValues	6.3.4	Conforme especificado no documento DOC-ICP-05, cláusula 4.6.2, as LCR são retidas permanentemente pelas AC da ICP-Brasil para fins de consulta histórica.
id-aa-ets-archiveTimestamp	6.4.1	Carimbos do tempo empregados devem atender ao perfil definido no documento DOC-ICP-12.

3. FORMATOS ICP-BRASIL CADES

Atributo	EPES	EPES-T	EPES-CX	EPES-A
id-aa-contentHint	O	O	O	O
id-aa-contentIdentifier	O	O	O	O
id-aa-contentReference	O	O	O	O
id-aa-ets-commitmentType	O	O	O	O
id-aa-ets-contentTimestamp	O	O	O	O
id-aa-ets-signerAttr	O	O	O	O
id-aa-ets-signerLocation	O	O	O	O
id-countersignature	O	O	O	O
id-signingTime	M	M	M	M
id-contentType	M	M	M	M
id-messageDigest	M	M	M	M
id-aa-signingCertificate ou id-aa-signingCertificateV2	M	M	M	M
id-aa-sigPolicyId	M	M	M	M
id-aa-signatureTimeStampToken	-	M	M	M
id-aa-ets-certificateRefs	-	-	M	O
id-aa-ets-revocationRefs	-	-	M	O
id-aa-ets-attrCertificateRefs	-	-	C	O
id-aa-ets-attrRevocationRefs	-	-	C	O
id-aa-ets-escTimeStamp	-	-	M	O
id-aa-ets-certValues	-	-	-	M
id-aa-ets-revocationValues	-	-	-	M
id-aa-ets-archiveTimestamp	-	-	-	M

Definições

M	significa que a presença do atributo é MANDATÓRIO, ou seja, obrigatório.
O	significa que a presença do atributo é OPCIONAL. Entretanto, ele deve estar previsto nos softwares para ser utilizado pelos usuários, caso desejado.
C	significa que a presença do atributo é CONDICIONAL. Ele deve estar presente caso sejam utilizados certificados de atributo.

Observação

O formato EPES-A torna alguns atributos, anteriormente mandatórios, opcionais, por provê-los de um modo mais completo. Por exemplo, o atributo *id-aa-ets-certificateRefs* não precisa ser utilizado, pois o atributo *id-aa-ets-certValues* conterá todos os certificados utilizados, dispensando-se a referência a eles.

4.BIBLIOGRAFIA

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

[2] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI). Electronic Signatures and Infrastructures (ESI): CMS Advanced Electronic Signatures (CAdES). Technical Specification. ETSI TS 101 733 v1.7.3, Jan. 2007.

[3] 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 v1.1.1. Feb. 2007.

[4] 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.

[5] 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.

[6] ITI. REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL DOC-ICP-12 - V 1.0 – **Documento em elaboração**