Infraestrutura de Chaves Públicas Brasileira

PERFIL DE USO GERAL PARA ASSINATURAS DIGITAIS NA ICP-BRASIL

DOC-ICP-15.02

Versão 2.0

05 de abril de 2010

SUMÁRIO

1 INTRODUÇÃO

1.1 Este documento define um perfil para assinatura digital na Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) que contém um sub-conjunto dos atributos/propriedades definidos nos padrões CMS *Advanced Electronic Signatures* (CAdES) [1] e XML-DSig *Advanced Electronic Signatures* (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 ICP-Brasil. Tal conjunto se compõe de:

a) Visão Geral sobre Assinaturas Digitais na ICP-Brasil (DOC-ICP-15) [3];
b) Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil (DOC-ICP-15.01) [4];
c) Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil (DOC-ICP-15.02) (este documento);
d) Requisitos das Políticas de Assinatura na ICP-Brasil (DOC-ICP-15.03) [5].

1.3 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 O restante deste documento esta organizado da seguinte forma. O capítulo 2 apresenta o perfil de assinatura digital com base no CAdES e o capítulo 3 o perfil de assinatura digital com base no XAdES.

2 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES CMS / CADES

2.1 ATRIBUTOS ASSINADOS

A Tabela 2.1 apresenta os atributos assinados para assinaturas no formato CAdES. A coluna **Ref** aponta a seção no documento ETSI TS 101 733 [1] em que o atributo está especificado.

2.2 ATRIBUTOS NÃO ASSINADOS

A Tabela 2.2 apresenta os atributos não assinados para assinaturas no formato CAdES. A coluna **Ref** aponta a seção no documento ETSI TS 101 733 em que o atributo está especificado.

Atributo	Ref [1]	Requisitos adicionais / Observações
id-aa-ets-contentTimestamp	5.11.4	Os carimbos do tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [6].
id-aa-ets-signerAttr	5.11.3	
id-aa-ets-signerLocation	5.11.2	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	
id-contentType	5.7.1	
id-messageDigest	5.7.2	
id-aa-signingCertificate	5.7.3	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
id-aa-ets-sigPolicyId	5.7.3	

Tabela 2.1: Atributos assinados para assinaturas no formato CAdES

Atributo	Ref [1]	Requisitos adicionais / Observações
id-countersignature	5.9.2	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	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 [8], cláusula 4.6.2, os certificados de assinatura digital são retidos permanentemente pelas Autoridades Certificadoras (ACs) 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 LCRs são retidas permanentemente pelas ACs 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.

Tabela 2.2: Atributos não assinados para assinaturas no formato CAdES

3 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES XML-DSIG / XADES

3.1 PROPRIEDADES ASSINADAS

A Tabela 3.1 apresenta as propriedades assinadas para assinaturas em formato XAdES. A coluna **Ref** aponta a seção no documento ETSI TS 101 903 [2] em que a propriedade está especificada.

3.2 PROPRIEDADES NÃO ASSINADAS

A Tabela 3.2 apresenta as propriedades não assinadas para assinaturas no formato XAdES. A coluna **Ref** aponta a seção no documento ETSI TS 101 903 em que a propriedade está especificada.

Propriedade	Ref[2]	Requisitos adicionais / Observações
SignatureProductionPlace	7.2.7	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
SignerRole	7.2.8	
SigningTime	7.2.1	
AllDataObjectsTimeStamp	7.2.9	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12.
IndividualDataObjectsTimeStamp	7.2.10	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12.
DataObjectFormat	7.2.5	
SigningCertificate	7.2.2	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04.
SignaturePolicyIdentifier	7.2.3	

Tabela 3.1: Propriedades assinadas para assinaturas em formato XAdES.

Propriedade	Ref [2]	Requisitos adicionais / Observações
CounterSignature	7.2.4	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	Os carimbos do tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12.
CompleteCertificateRefs	7.4.1	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04.
CompleteRevocationRefs	7.4.2	As Listas de Certifificados Revogados (LCR) e respostas de *Online Certificate Status Protocol* (OCSP) empregadas DEVEM atender ao perfil definido no documento DOC-ICP-04.
AttributeCertificateRefs	7.4.3	
AttributeRevocationRefs	7.4.4	
SigAndRefsTimeStamp	7.5.1	Os carimbos do tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12.
CertificateValues	7.6.1	Conforme especificado no documento DOC-ICP-05, cláusula 4.6.2, os certificados de assinatura digital são retidos permanentemente pelas Autoridades Certificadoras da ICP-Brasil para fins de consulta histórica. Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04.
RevocationValues	7.6.2	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.
AttrAuthoritiesCertValues	7.6.3	
AttributeRevocationValues	7.6.4	
ArchiveTimeStamp	7.7	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12.

Tabela 3.2: Propriedades não assinadas para assinaturas no formato XAdES.

BIBLIOGRAFIA

[1] ETSI. *CMS Advanced Electronic Signatures (CAdES)*. 1.7.4. ed. [S.l.], 2008. Acesso em: 23/02/2009.

[2] ETSI. *XML Advanced Electronic Signatures (XAdES)*. 1.3.2. ed. [S.l.], 2006. Acesso em: 23/02/2009.

[3] ITI. *Visão Geral Sobre Assinaturas Digitais na ICP-Brasil*. v.1.0. Brasília. DOC-ICP-15.

[4] ITI. *Requisitos Mínimos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil*. v.1.0. Brasília. DOC-ICP-15.01.

[5] ITI. *Requisitos Mínimos para Políticas de Assinatura Digital na ICP-Brasil*. v.1.0. Brasília. DOC-ICP-15.03.

[6] ITI. *Requisitos Mínimos para as Declaracões de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil*. v.1.0. Brasília, Dezembro 2008. DOC-ICP-12.

[7] ITI. *Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil*. v.3.0. Brasília, Dezembro 2008. DOC-ICP-04.

[8] ITI. *Requisitos Mínimos para as Declaracões de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil*. v.3.1. Brasília, Junho 2009. DOC-ICP-05.