Laboratório de Sistemas Integráveis Tecnológico

PROJETO SREI

Sistema de Registro Eletrônico Imobiliário

Recomendação para assinatura digital.

Título	PROJETO SREI: Recomendação para assinatura digital.
Versão	Versão 1.1 release 5
Data da liberação	20/01/2012
Classificação	LSI-TEC:Restrito
Autores	Volnys Bernal
Propriedade	LSI-TEC
Restrições de acesso	LSI-TEC, CNJ e ARISP

Sumário

1 Introdução

Este documento apresenta a recomendação para formato, estrutura de atributos da assinatura, certificados de atributo e demais objetos eletrônicos da assinatura digital no contexto do SREI.

A recomendação para assinatura digital no contexto do SREI busca a segurança, a interoperabilidade e a preservação a longo prazo do documento eletrônico assinado.

2 Direcionamentos

Os requisitos relacionados à assinatura digital foram concebidos levando em consideração os seguintes direcionamentos:

- Aderência a padrões internacionais;
- Aderência às normalizações da ICP-Brasil;
- Presença de elementos que possibilite a validação no futuro;
- Presença de características para favorecer a preservação à longo prazo;
- Segurança: restrição de uso de componentes mutáveis de acordo com o contexto;
- Coerção: conteúdo e assinatura no mesmo container;
- Possibilidade de representação de dados estruturados, para possibilitar a obtenção automática de dados por programas. Este requisito é relevante para os registros eletrônicos e certidões eletrônicas;
- Possibilidade de validação do poder do signatário de forma segura, padronizada e automática.

3 Formatos de assinatura digital

Na geração de uma assinatura digital, o sistema SREI DEVE fazer uso de um dos formatos de assinatura digital relacionados no Quadro 1.

Quadro 1 – Formatos de assinatura digital para SREI.

Documento eletrônico	Estruturação do conteúdo	Formato do conteúdo	Formato do conteúdo com assinatura digital
Representante digital	Não estruturado	Imagem (PNG, TIFF)	HTML + XML Dsig.
			XML + XML Dsig. Deve ser utilizado somente para documentos de uso interno devido a dificuldades de visualização.
			PDF/A-2 + assinatura PDF *PAdES Long Term*
Natodigital	Não estruturado	Texto	PDF/A-2 + assinatura PDF *PAdES Long Term*
			XML Digital Signture (XML DSig) com assinatura envelopada (*enveloped signature*).
		Imagem (PNG, TIFF)	HTML + XML Dsig
			PDF/A-2 + assinatura PDF *PAdES Long Term*
			XML Digital Signture (XML DSig) com assinatura envelopada (*enveloped signature*). Deve ser utilizado somente para documentos de uso interno, devido a possíveis dificuldades de visualização.
	Estruturado	XML	*Documento final: XML Digital Signture (XML DSig)* com assinatura envelopada (*enveloped signature*)
			Protótipo de documento: XML Digital Signture (XML DSig) com assinatura envelopada (*enveloped signature*) ou assinatura separada (*signature detached*) sobre partes do documento.

4 Perfil SREI dos atributos de assinatura digital

O sistema SREI, na geração de uma assinatura digital, DEVE utilizar os perfis de atributos de assinatura digital relacionados no Quadro 2.

Quadro 2 – Perfis de atributos na geração de assinatura digital.

Formato de assinatura digital	Perfil	Descrição
XML DSIG	SREI XAdES	Aderente ao perfil de atributos ICP-Brasil AD-RC do perfil XAdES, com a obrigatoriedade de inclusão de outros atributos, opcionais no perfil ICP-Brasil AD-RC ou no perfil XAdES. Os atributos obrigatórios estão relacionados no quadro Quadro 3. A política de assinatura a ser utilizada na assinatura é AD-RC. Para preservação a longo prazo, quando necessário, DEVE ser incluído o atributo ArchiveTimeStamp sobre as assinaturas.
PDF	SREI PAdES	Aderente ao perfil de atributos ICP-Brasil AD-RC do perfil *PAdES Long Term.* (observação: este formato ainda não está normalizado pela ICP-Brasil).

O Quadro 3 apresenta a relação de atributos obrigatórios quando for utilizado o perfil SREI XAdES e a Figura 1 a ilustração da composição destes atributos .

Quadro 3 – Obrigatoriedade de atributos (propriedades) do perfil SREI XAdES.

Atributo (propriedade)	Perfil SREI XAdES
SigningTime	O
SigningCertificate	O
SignaturePolicyIdentifier	O
CounterSignature	Permitido
DataObjectFormat	R
CommitmentTypeIndication	O
SignatureProductionPlace	R
SignerRole	OC
AllDataObjectsTimeStamp	F
IndividualDataObjectsTimeStamp	F
SignatureTimeStamp	O
CompleteCertificateRefs	O
CompleteRevocationRefs	O
AttributeCertificateRefs	OC
AttributeRevocationRefs	OC
SigAndRefsTimeStamp	O
RefsOnlyTimeStamp	F
CertificateValues	O
RevocationValues	O

Código	Obrigatoriedade
O	Obrigatório
OC	Obrigatório condicional
R	Recomendado
RC	Recomendado condicional
F	Facultativo
P	Proibido
NA	Não se aplica

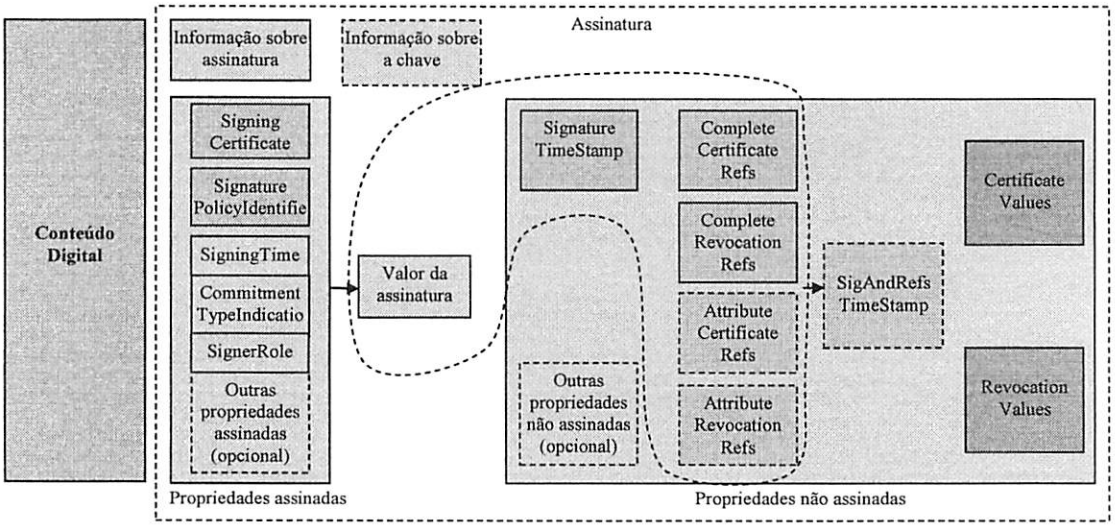

Figura 1 – Ilustração do perfil SREI XAdES.

Quadro 4 – Classificação da obrigatoriedade do atendimento dos atributos.

Código	Obrigatoriedade do atendimento do requisito
O	Obrigatório
OC	Obrigatório condicional
R	Recomendado
RC	Recomendado condicional
F	Facultativo
P	Proibido
NA	Não se aplica

5 Certificado de atributo

O certificado de atributo é utilizado para permitir automatizar o processo da verificação da assinatura, permitindo verificar de forma segura se o signatário possui autoridade para assinatura do documento.

O certificado de atributo é um recurso definido inicialmente na especificação x509 (a mesma que definiu o certificado digital), sendo o perfil definido na RFC 3281 o mais utilizado atualmente.

No contexto do SREI, o certificado de atributo é utilizado para verificar a autoridade do signatário dos documentos emitidos pelo cartório (certidões, notas de exigência, etc) e dos documentos presentes nos livros eletrônicos.

O Judiciário DEVE emitir, para cada Oficial Registrador um certificado de atributo. Este certificado de atributo é gerado pela Autoridade de Atributo.

O certificado de atributo DEVE informar:

- Nome do oficial registrador;
- Privilégio "Oficial de Registro de Imóveis";
- Identificação do cartório;
- Possibilidade de delegação deste privilégio uma única vez.

Este certificado DEVE possuir validade de três anos, com possibilidade de revogação.

O Oficial pode, a seu critério, delegar este privilégio para seus prepostos, gerando certificados de atributos para eles Isto é realizado pelo Oficial, com o auxílio de um programa, emitindo e assinado o certificado de atributo de seu preposto utilizando a chave privada associada a seu certificado digital. O certificado de atributo dos prepostos NÃO DEVE possuir revogação. Por este motivo, DEVE possuir validade curta (por exemplo, um dia ou uma semana).

Uma pessoa que esteja verificando, por exemplo, a assinatura de uma certidão, após a verificação da assinatura, deve verificar a autoridade do signatário. Para isso,

deve já ter estabelecido seu contexto de segurança: os certificados raiz da ICP-Brasil e as fontes de autoridade dos privilégios, neste caso o Poder Judiciário para o privilégio de Oficial de Registro de Imóveis.

6 Algoritmos criptográficos

Os algoritmos que devem ser utilizados nos processos de assinatura são aqueles definidos pela ICP-Brasil, exceto o algoritmo hash SHA-1.

7 Referências

ETSI. **ETSI TS 101 903 v1.4.1. Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).**

ETSI. **ETSI TS 102 778-1 v1.1.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 1: PAdES Overview: a framework document for PAdES.** ETSI. 20p. July, 2009.

ETSI. **ETSI TS 102 778-3 v1.1.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles**. ETSI. 20p. July, 2009.

ETSI. **ETSI TS 102 778-4 v1.1.1. Electronic signatures and infrastrutctures (ESI) – PDF advanced electronic signature profiles – Part 4: PAdES Long Term – PAdES-LTV Profile.** ETSI. 20p. July, 2009.

EASTLAKE 3rd, D.; REAGLE, J.; SOLO, D. **RFC 3275. (Extensible Markup Language) XML-Signature Syntax and Processing**. IETF, mar. 2002.

BARTEL, M; et. al. **XML Signature Syntax and Processing. Second edition**. World Wide Web Consortium (W3C). June, 2008.

ISO. **ISO 32000-1:2008 – Document management: portable document format (PDF 1.7)**. 748p. 2008.

ADOBE. **The AdES family of standards: CAdES, XAdES and PAdES: implementation guidance for using electronic signatures in the European Union**. Adobe Systems Inc. 2009.

ITU-T. **ITU-T Recommendation X.690, Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).** ITU-T. 2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>. Acesso em: 19 mar. 2010.

ICP-Brasil. **DOC-ICP-15: Visão geral sobre assinaturas digitais na ICP-Brasil**. ICP-Brasil. Versão 2.0. Abril. 2010.

FARRELL, S; HOUSLEY, R.; **RFC 3281: an Internet attribute certificate profile for authorization**. Internet Engineering Task Force (IETF). April, 2002.