Sistema eletrônico de votação

Formatos dos arquivos de assinatura

Apresentação

Os sistemas informatizados da Justiça Eleitoral utilizam um formato próprio para um arquivo que contém a assinatura digital de outros arquivos. Esse formato é descrito no padrão Abstract Syntax Notation One (ASN.1)[1], utilizando o formato Basic Encoding Rules (BER)[2] para a sua representação na forma de arquivo binário. Tratam-se de padrões amplamente utilizados para a comunicação entre sistemas. Um dos exemplos mais proeminentes de uso desses formatos é o certificado digital (padrão X.509[3]).

A construção de um formato próprio foi uma decisão de projeto com vistas à simplicidade e otimização. Durante a sua especificação, o padrão PCKS#7[4] foi usado como referência.

Aplicações

Os arquivos de assinatura de descritos aqui são utilizados nos seguintes contextos:

1. **Assinatura dos dados que alimentam a urna**. Consiste na assinatura digital com a biblioteca fornecida pelo Cepesc/Abin dos arquivos de descrição do processo eleitoral, eleitores e candidatos, além de arquivos gerados pela própria urna. Essas assinaturas são geradas pelos sistemas responsáveis pela guarda original dos dados. Nesses casos os arquivos de assinatura possuem a extensão VSC.
2. **Assinatura do software**. Trata-se da assinatura digital com a biblioteca fornecida pelo Cepesc/Abin do software compilado durante a Cerimônia Pública de Lacração dos Sistemas Eleitorais. Essas assinaturas são geradas pelo titular da Secretaria de Tecnologia da Informação do TSE ou pessoa por ele designada. Nesses casos os arquivos possuem a extensão VST.
3. **Assinatura dos resultados da urna**. Consiste no conjunto de assinaturas digitais dos arquivos produzidos pela urna ao final da votação. Nesse caso, pode haver dois tipos de assinatura: gerada pela biblioteca fornecida pelo Cepesc/Abin e produzida pelo hardware de segurança das urnas (nos modelos que possuem esse hardware). Nesse caso os arquivos possuem a extensão VSCMR.

Os arquivos VSC e VST possuem o mesmo formato - estão descritos sobre a mesma especificação ASN.1 (`ModuloEnvelopeAssinatura::EntidadeAssinatura`). O arquivo VSCMR possui outra especificação (`ModuloAssinaturaResultado::EntidadeAssinaturaResultado`). Todos estão codificados em formato binário BER.

Especificações ASN.1

```
ModuloEnvelopeAssinatura DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

EntidadeAssinatura ::= SEQUENCE {
    dataHoraCriacao      DataHoraJE,
    versao               INTEGER(2..99999999),  -- Versão do formato do arquivo.
    autoAssinado         AutoAssinaturaDigital, -- Assinatura do conjunto de assinaturas presente no arquivo.
    conteudoAutoAssinado OCTET STRING,          -- Conteúdo serializado (BER) descrito em 'Assinatura'.
    certificadoDigital   OCTET STRING OPTIONAL  -- Quando assinado pelo hardware de segurança da urna, inclui o
                                                -- certificado digital da urna (X.509/DER).
}

DataHoraJE ::= GeneralString(SIZE(15)) -- Formato AAAAMMDDThhmmss
```

[1] https://en.wikipedia.org/wiki/Abstract_Syntax_Notation_One
[2] https://en.wikipedia.org/wiki/X.690
[3] https://en.wikipedia.org/wiki/X.509
[4] https://tools.ietf.org/html/rfc2315

```
Assinatura ::= SEQUENCE {
    arquivosAssinados SEQUENCE OF AssinaturaArquivo
}

AssinaturaDigital ::= SEQUENCE {
    tamanho    INTEGER,      -- Tamanho do arquivo em bytes.
    hash       OCTET STRING,
    assinatura OCTET STRING
}

AutoAssinaturaDigital ::= SEQUENCE {
    usuario             DescritorChave,
    algoritmoHash       AlgoritmoHashInfo,
    algoritmoAssinatura AlgoritmoAssinaturaInfo,
    assinatura          AssinaturaDigital
}

DescritorChave ::= SEQUENCE {
    nomeUsuario GeneralString, -- Nome do titular.
    serial INTEGER             -- Identificador do par.
}

AssinaturaArquivo ::= SEQUENCE {
    nomeArquivo GeneralString,
    assinatura  AssinaturaDigital
}

AlgoritmoHashInfo ::= SEQUENCE {
    algoritmo AlgoritmoHash
}

AlgoritmoHash ::= ENUMERATED {
    sha512(4)
}

AlgoritmoAssinaturaInfo ::= SEQUENCE {
    algoritmo AlgoritmoAssinatura,
    bits      INTEGER
}

AlgoritmoAssinatura ::= ENUMERATED {
    ecdsa(2),
    cepesc(3)
}

END

ModuloAssinaturaResultado DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS EntidadeAssinatura FROM ModuloEnvelopeAssinatura;

EntidadeAssinaturaResultado ::= SEQUENCE {
    modeloUrna      ModeloUrna,
    assinaturaSW    EntidadeAssinatura,
    assinaturaHW    EntidadeAssinatura OPTIONAL
}

ModeloUrna ::= ENUMERATED {
    ue2006(6),
    ue2008(8),
    ue2009(9),
    ue2010(10),
    ue2011(11),
    ue2013(13),
    ue2015(15)
}

END
```