BDOC
DIGITAALALLKIRJA VORMING

BDOC
Format for Digital Signatures

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESSÕNA

Käesolev Eesti standard:

- on standardi EVS 821:2003 "Digitaalallkirja kontrolli üldpõhimõtted. Sertifikaadi kehtivuskinnituse vorming ja protokollid" uustöötlus;
- on kinnitatud Eesti Standardikeskuse 20.04.2009 käskkirjaga nr 65;
- jõustub sellekohase teate avaldamisel EVS Teataja 2009 aasta maikuu numbris;
- asendab standardid EVS 821:2003 ja EVS 822:2003 "Ajatempliteenuse protokollid ja andmevormingud".

Standardi koostamisettepaneku esitas EVS/TK 4 "Infotehnoloogia", standardi koostamist toetas Majandus- ja Kommunikatsiooniministeerium.

Standardi ja selle tõlke inglise keelde koostas AS Sertifitseerimiskeskus, standardi on heaks kiitnud tehniline komitee EVS/TK 4 "Infotehnoloogia".

ICS 35.040 Märgistikud ja informatsiooni kodeerimine
Võtmesõnad: digitaalallkiri, kehtivuskinnitus, protokollid, infoturve
Hinnagrupp RN

FOREWORD

This Estonian standard:

— is a revision of EVS 821:2003 "General rules of validation of digital signature. Format and protocol of certificates";

— is implemented by decree of Estonian Centre for Standardisation 20.04.2009 no 65;

— becomes valid with notice in EVS Teataja, issue May 2009;

— replaces EVS 821:2003 and EVS 822:2003 "Protocols and formats of timestamp".

The proposal for drafting of standard submitted by EVS/TK 4 "Information technology", drafting of standard is supported by Ministry of Economic Affairs and Communications.

Standard and its translation into English language has been prepared by the Estonian Certification Centre (AS Sertifitseerimiskeskus), standard approved by technical committee EVS/TK 4 "Information technology".

ICS 35.040 Character sets and information coding
Descriptors: digital signature, validity confirmation, protocol, IT security
Price group RN

SISUKORD

TABLE OF CONTENT

SISSEJUHATUS

Euroopa direktiiv 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta defineerib elektroonilise allkirja kui “elektroonilised andmed, mis on lisatud muudele elektroonilistele andmetele või on nendega loogiliselt seotud ja mida kasutatakse ehtsuse tõendamiseks”.

Käesoleva dokumendi eesmärgiks on hõlmata elektroonilise allkirja kasutamine eritüübiliste transaktsioonide puhul, kaasa arvatud äritransaktsioonid (näiteks ostukorraldused, lepingud ja arved). Seega saab standardis esitatud spetsifikatsiooni kasutada igasuguse transaktsiooni puhul eraisiku ja firma vahel, kahe firma vahel, kodaniku ja riigiasutuse vahel jne. Käesolev spetsifikatsioon on keskkonna-neutraalne. Seda saab kasutada erinevate allkirjastamisvahendite puhul: näiteks kiipkaardid, GSM SIM kaardid, elektroonilise allkirjastamise spetsiaalprogrammid jne.

ETSI standard TS 101 903[1] (siin ja edaspidi: XAdES) defineerib formaadid täiustatud elektrooniliste allkirjade jaoks, mis omavad pikaajalist tõestusväärtust, on vastavuses Euroopa direktiiviga ja kaasavad kasulikku lisainformatsiooni tavapärasteks kasutusjuhtudeks (näiteks allkirjastaja rolli või resolutsiooni näitamine). XAdES on XML-põhine ning seega sobilik kaasaegses IKT-keskkonnas.

Käesolev standard:

- spetsifitseerib XAdES-e profiili kitsendades elementide ja väärtuste valikut standardis;
- defineerib XAdES-e elementide kogumi, mis annavad XAdES-allkirjale pikaajalise tõestusväärtuse;
- spetsifitseerib konteineri vormingu allkirjastatud failide ja allkirjade kapseldamiseks.

Edasises tekstis kasutame mõistet “BDOC“ tähistamaks nii XAdES-e profiili kui ka konteineri vormingut.

1 KÄSITLUSALA

Käesolev dokument defineerib XML vormingud täiustatud elektrooniliste allkirjade jaoks, mis omavad pikaajalist tõestusväärtust, on vastavuses Euroopa direktiiviga ning kaasavad kasulikku lisainformatsiooni tavapärasteks kasutusjuhtudeks. See lisainformatsioon sisaldab ka tõestusmaterjali allkirja kehtivusest, mis on kasutatav isegi siis, kui allkirjastaja või verifitseerija üritab hiljem eitada (salata) allkirja kehtivust.

Käesolev standard rajaneb järgmistel standarditel:

- ETSI TS 101 903 v1.3.2 – XML Advanced Electronic Signatures (XAdES) [1];
- ITU-T Recommendation X.509 [2];
- RFC 3161 – PKIX Time-Stamp protocol [3];
- RFC 2560 – Online Certificate Status Protocol [4];
- *Packaging conventions*, OpenDocument [5] standardi osa.

Jaotis 2 toob ära täieliku loetelu välistest allikatest.

Jaotis 5 defineerib BDOC vormingu põhiprofiili. Põhiprofiil sisaldab ainult signatuuri ilma mingi kehtivusinfota.

Jaotis 6 defineerib kaks BDOC profiili koos kehtivusinfoga, mis võimaldab neid käsitleda kui “käsitsi antud allkirja asendust”.

Jaotis 7 käsitleb ja defineerib meetodeid saavutamaks elektrooniliste allkirjade pikaajalist tõestusväärtust.

Jaotis 8 spetsifitseerib konteineri vormingu allkirjastatud failide ja allkirjade kapseldamiseks.

INTRODUCTION

The European Directive on a community framework for Electronic Signatures defines an electronic signature as: "data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication".

The present document is intended to cover electronic signatures for various types of transactions, including business transactions (e.g. purchase requisition, contract, and invoice applications). Thus the present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment. It can be used with different signature creation devices e.g. smart cards, GSM SIM cards, special programs for electronic signatures, etc.

The ETSI standard TS 101 903 [1] (hereinafter: XAdES) defines formats for advanced electronic signatures that remain valid over long periods, are compliant with the European Directive and incorporate additional useful information in common use cases (like indication of the role or resolution of the signatory). XAdES is XML-based and therefore suitable for the current ICT environment.

The present document:

- specifies profiles of XAdES by narrowing down choices of elements and value types in the standard;
- defines sets of XAdES elements for long-time validity of XAdES signature;
- specifies container format for embedding signed files and signatures.

For the further reference, term BDOC is used thorough the text to denote both XAdES profile and container format.

1 SCOPE

The present document defines XML formats for advanced electronic signatures that remain valid over long periods, are compliant with the European Directive and incorporate additional useful information in common uses cases. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature.

The present document builds on the following standards:

- ETSI TS 101 903 v1.3.2 – XML Advanced Electronic Signatures (XAdES) [1];
- ITU-T Recommendation X.509 [2];
- RFC 3161 – PKIX Time-Stamp protocol [3];
- RFC 2560 – Online Certificate Status Protocol [4];
- Packaging conventions, part of OpenDocument [5] standard.

For a complete list of references, see section 2.

Section 5 defines basic profile of the BDOC format. This profile contains just signature without any validation data.

Section 6 defines two profiles of the BDOC format with validation data providing for “replacement of handwritten signature”.

Section 7 discusses and defines means for achieving long-time validity of the electronic signatures.

Section 8 specifies container format for embedding signed files and signatures into one data unit.

2 NORMIVIITED

[1] ETSI 101 903 V1.3.2 – XML Advanced Electronic Signatures (XAdES)

[2] ITU-T Recommendation X.509: "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks"

[3] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp protocol"

[4] RFC 2560: “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”

[5] ISO/IEC 26300:2006 Information technology – Open Document Format for Office Applications (OpenDocument) v1.0

[6] IETF RFC 3275: “XML-Signature Syntax and Processing”

[7] ETSI TS 102 023 V1.2.1 – Policy requirements for time-stamping authorities