BDOC
Digitaalallkirja vorming

BDOC
Format for digital signatures

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— standardi EVS 821:2009 uustöötlus;

— jõustunud sellekohase teate avaldamisega EVS Teataja 2014. aasta juunikuu numbris.

Standardi koostamise ettepaneku on esitanud tehniline komitee EVS/TK 4 „Infotehnoloogia“, standardi koostamist on korraldanud Eesti Standardikeskus.

Standardi ja selle tõlke inglise keelde on koostanud AS Sertifitseerimiskeskus, standardi on heaks kiitnud EVS/TK 4.

Standardi uustöötluse peamine põhjus on ETSI hiljuti avaldatud uute standarditega harmoneerimine; samuti signeerimispoliitika kajastamine allkirjas ning kasutatavate krüptoalgoritmide ajakohastamine.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine

SISUKORD

SISSEJUHATUS

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

Selle dokumendi eesmärk on hõlmata elektroonilise allkirja kasutamine mitmesuguste tehingute puhul, kaasa arvatud äritehingud (näiteks ostukorraldused, lepingud ja arved). Seega saab seda spetsifikatsiooni kasutada igasuguse tehingu puhul eraisiku ja firma vahel, kahe firma vahel, kodaniku ja riigiasutuse vahel jne. See spetsifikatsioon on keskkonna-neutraalne. Seda saab kasutada mitmesuguste allkirjastamisvahendite puhul: kiipkaartide, GSM SIM-kaartide, elektroonilise allkirjastamise eriprogrammidega jne.

ETSI standard TS 101 903 [1] (edaspidi: XAdES) määratleb vormingud täiustatud elektrooniliste allkirjade jaoks, millel on pikaajaline tõestusväärtus, ja kaasab kasulikku lisainformatsiooni tavapärasteks kasutusjuhtudeks (näiteks allkirjastaja rolli või resolutsiooni näitamiseks). XAdES on XML-põhine ning seega sobib praegusesse IKT-keskkonda. ETSI standard TS 103 171 [4] profileerib standardit XAdES, ahendades valikuvõimalusi.

ETSI standard TS 102 918 [3] (edaspidi: ASiC) määratleb konteineri vormingu kapseldamaks allkirjastatud faile ja allkirju koos lisateabega. Nimetatud standardit profileerib ETSI TS 103 174 [5].

See BDOC-i standard on täielikult ühilduv ülalnimetatud ETSI standarditega.

See dokument spetsifitseerib:

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

Edasises tekstis tähistab „BDOC“ nii XAdES-profiili kui ka konteineri vormingut.

1 KÄSITLUSALA

See dokument määratleb XML-vormingud täiustatud elektrooniliste allkirjade jaoks, millel on pikaajaline tõestusväärtus, ja kaasab kasulikku lisateavet tavapärasteks kasutusjuhtudeks. See lisateave sisaldab ka tõestusmaterjali allkirja kehtivusest, mis on kasutatav isegi siis, kui allkirjastaja või verifitseerija üritab hiljem eitada (salata) allkirja kehtivust.

See dokument rajaneb järgmistel standarditel:

- ETSI TS 101 903 V1.4.2. XML Advanced Electronic Signatures (XAdES) [1]; ning selle baasprofiil ETSI TS 103 171 V2.1.1 [4];
- ITU-T Recommendation X.509 [11];
- IETF RFC 3161. PKIX Time-Stamp protocol [7];
- IETF RFC 6960. Online Certificate Status Protocol [10];
- ETSI TS 102 918 V1.2.1. Associated Signature Containers (ASiC) [3]; ning selle baasprofiil ETSI TS 103 174 V2.1.1 [5]. Viimane põhineb omakorda standardi OpenDocument [12] osal „OpenDocument V1.2 Part 3 – Packages“.

Peatükk 2 esitab väliste allikate täieliku loetelu.

Peatükk 5 määratleb BDOC-vormingu põhiprofiili. Põhiprofiil sisaldab ainult signatuuri ilma mingi kehtivusteabeta.

Peatükk 6 määratleb kaks BDOC-i profiili koos kehtivusteabega, mis võimaldab neid käsitleda kui „käsitsi antud allkirja asendust“.

Peatükk 7 käsitleb ja määratleb elektrooniliste allkirjade pikaajalise tõestusväärtuse saavutamise meetodeid.

Peatükk 8 spetsifitseerib konteineri vormingu allkirjastatud failide ja allkirjade kapseldamiseks.

2 NORMIVIITED

Alljärgnevalt nimetatud dokumendid on vajalikud selle standardi rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

[1] ETSI TS 101 903 V1.4.2 (2010-12). XML Advanced Electronic Signatures (XAdES)

[2] ETSI TS 102 023 V1.2.2 (2008-10). Policy requirements for time-stamping authorities

[3] ETSI TS 102 918 V1.2.1 (2012-02). Associated Signature Containers (ASiC)

[4] ETSI TS 103 171 V2.1.1 (2012-03). XAdES Baseline Profile

[5] ETSI TS 103 174 V2.1.1 (2012-03). ASiC Baseline Profile

[6] ETSI TS 102 176-1 V2.1.1 (2011-07). Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

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

[8] IETF RFC 3275. XML-Signature Syntax and Processing

[9] IETF RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[10] IETF RFC 6960. Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP)

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

[12] OASIS. Open Document Format for Office Applications (OpenDocument) Version 1.2. Part 3: Packages

3 MÄÄRATLUSED JA LÜHENDID

Standardi rakendamisel kasutatakse XAdES [1] peatükis 3 ja lisas A esitatud määratlusi ja lühendeid.

4 ÜLEVAADE

Kuigi XAdES on olnud kasutusel juba mitmeid aastaid ning seda standardit kasutavaid rakendusi on mitmeid, on need rakendused ikkagi kokkusobimatud. Põhjused on järgmised:

- XAdES sisaldab palju valikuid. Reeglina ei kasuta selle rakendused kõiki mittekohustuslikke ehitusplokke ja elemente ning tulemuseks on XAdES-allkirjade ühildumatus.
- XAdES-e profileerimise valikud sõltuvad olulisel määral rakendusele esitatavatest turvanõuetest ja PKI teenustest. Kuna need nõuded ja teenused varieeruvad, siis teevad seda ka vastavad XAdES-e profiilid.
- XAdES spetsifitseerib vaid signatuuri vormingu, mis ei määratle (allkirjastatavate) andmete asukohta muul viisil kui URI-mehhanismi kasutades. Praktikas on sagedaseks nõudeks algandmete ja allkirjade sidumine ühtseks andmekogumiks (konteineri või failina). Kuna rakenduste kirjutajatel on siin vaba voli, on tulemuseks digitaalselt allkirjastatud failide kokkusobimatus.

ETSI standardite rida on täienenud, profileerides XAdES-e baasprofiili [4] ning standardides allkirja konteineri [3] ning selle baasprofiili [5].

See spetsifikatsioon kasutab uusi alusstandardeid ja lahendab ülalmainitud probleemid, defineerides:

- alamhulga XAdES-e elementidest ja parameetritest – „BDOC-i profiili XAdES-est“;
- nõuete profiilid PKI, ajatembelduse ja kehtivusteabe teenustele ning vastavatele XAdES-e ehitusplokkidele;
- konteineri vormingu algandmete ja allkirjade kapseldamiseks – „BDOC-failivormingu“.

See dokument põhineb standardil XAdES [1] ja seetõttu ei ole üksinda käsitletav. Lugeja peab kasutama seda standardit põhjana ja jälgima viiteid ning profileerimismärkusi selles dokumendis. Nõuded muudest standarditest (XAdES-e baasprofiil [4], AsiC [3] ja selle baasprofiil [5]) on kaetud selle spetsifikatsiooniga, kuid nendega tutvumine võib lugejale anda lisainformatsiooni.

Lisa B sisaldab ülevaadet kasutatavatest XAdES-e elementidest BDOC-i eri variantides.

5 BDOC-I PÕHIPROFIIL

BDOC-i põhiprofiil on XML-struktuur, mis sisaldab üht krüptograafilist signatuuri üle defineeritud andmekogumi. See ei sisalda mingeid andmeid (ajatempleid ja/või kehtivuskinnitusi) signatuuri täielikuks valideerimiseks. BDOC-i põhiprofiil on aluseks teistele BDOC-i vormidele, mis on kirjeldatud järgmises peatükis.

BDOC-i põhiprofiil põhineb XAdES-EPES (*Explicit Policy Based Electronic Signature*) vormingul, mis on määratletud XAdES [1] jaotisega 4.4.2.

Nõudeid elementide kasutamisele tähistavad järgnevas tekstis märgised vastavalt tabelile 1.