BDOC – DIGITAALALLKIRJA VORMING

Versioon 2.0~~1.9.9~~:201~~3~~2

OID: 1.3.6.1.4.1.10015.1000.3.1.1~~2.10.10~~

Sisukord

Sisukord

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 käesolevat 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] (edaspidi: XAdES) defineerib formaadid täiustatud elektrooniliste allkirjade jaoks, mis omavad pikaajalist tõestusväärtust ja kaasab kasulikku lisainformatsiooni tavapärasteks kasutusjuhtudeks (näiteks allkirjastaja rolli või resolutsiooni näitamine). XAdES on XML-põhine ning seega sobilik kaasaegses IKT-keskkonnas. ETSI standard TS 103 171[8] profileerib XAdES-t, ahendades valikuvõimalusi.

ETSI standard TS 102 918[9] (edaspidi: ASiC) defineerib ära konteineri vormingu kapseldamaks allkirjastatud faile ja allkirju koos lisainfoga. Nimetatud standardit profileerib ETSI TS 103 174[10].

Käesolev BDOC standard on täielikult ühilduv ülalnimetatud ETSI standarditega.

Käesolev dokument:

- spetsifitseerib XAdES-e profiili kitsendades elementide ja väärtuste valikut standardis;
- defineerib XAdES-e elementide kogumi, mis annavad XAdES-allkirjale pikaajalise tõestusväärtuse;
- spetsifitseerib ASiC-ul põhineva 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 ja kaasab 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 dokument rajaneb järgmistel standarditel:

- ETSI TS 101 903 v1.4.2 – XML Advanced Electronic Signatures (XAdES) [1] ning selle baasprofiil ETSI TS 103 171[8];
- ITU-T Recommendation X.509 [2];
- RFC 3161 – PKIX Time-Stamp protocol [3];
- RFC 2560 – Online Certificate Status Protocol [4];
- ETSI TS 102 918 v1.2.1 - Associated Signature Containers (ASiC) [9] ning selle baasprofiil ETSI TS 103 174[10]. Viimane põhineb omakorda standardi OpenDocument [5] osal *OpenDocument-v1.2-part3 – Packages*..

Peatükk 2 toob ära täieliku loetelu välistest allikatest.

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

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

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

Peatükk 8 spetsifitseerib konteineri vormingu allkirjastatud failide ja allkirjade kapseldamiseks.

2. Viited

[1] ETSI TS 101 903 V1.4.2 (2010-12) - 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] OASIS "Open Document Format for Office Applications (OpenDocument) Version 1.2 Part 3: Packages"

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

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

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

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

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

~~[11] W3C: XML Signature Syntax and Processing Version 2.0 (http://www.w3.org/TR/xmldsig-core2/)~~

~~[12]~~[11] ETSI TS 102 176-1 V2.1.1 (2011-07) - Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

3. Definitsioonid ja lühendid

Põhilised definitsioonid ja lühendid on toodud XAdES[1] peatükis 4.

BDOC – XAdES-e profiil ja konteineri pakendamise reeglid.
Signatuur – turvalise allkirja andmise vahendiga loodud krüptogramm
Allkiri, digitaalallkiri – Digitaalallkirja Seaduse nõuetele vastav digitaalallkiri

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 XAdES-e rakendused ei kasuta kõiki mitte-kohustuslikke ehitusplokke ja elemente, mille 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 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 („konteiner“ või „fail“). Kuna rakenduste kirjutajatel on siin vaba voli, siis tulemuseks on *digitaalselt allkirjastatud failide* ühtesobimatus.

ETSI standardite rida on täienenud, profileerides XAdES-e baasprofiili[8] ning standardides allkirja konteineri[9] ning selle baasprofiili[10].

Käesolev spetsifikatsioon kasutab uusi alusstandardeid ja lahendab ülalmainitud probleemid:

- defineerides alamahulga XAdES-e elementidest ja parameetritest – „BDOC profiil XAdES-est“;
- defineerides nõuete profiilid PKI, ajatembelduse ja kehtivusinfo teenustele ning vastavatele XAdES-e ehitusplokkidele;
- defineerides konteineri vormingu algandmete ja allkirjade kapseldamiseks – „BDOC failivorming“.

Ülejäänud dokument põhineb XAdES[1] ja selle baasprofiili[8] standardil ja seetõttu ei ole üksinda käsitletav. Lugeja peab kasutama neid standardeid põhjana ja jälgima viiteid ning profileerimismärkusi selles dokumendis. Standard ASiC[9] ja selle baasprofiil[10] on aluseks konteineri pakkimisreeglitele, mis on defineeritud selle dokumendi 8. peatükis.

5. BDOC põhiprofiil

BDOC põhiprofiil on XML struktuur, mis sisaldab ühte krüptograafilist signatuuri üle hästi-defineeritud andmekogumi. See ei sisalda mingeid täiendavaid andmeid (ajatemplid ja/või kehtivuskinnitused) signatuuri täielikuks valideerimiseks. BDOC põhiprofiil on aluseks teistele BDOC vormidele, mis on kirjeldatud järgmises peatükis.

BDOC põhiprofiil põhineb XAdES-BES (*Basic Electronic Signature*) vormingul ja on määratletud XAdES[1] klausliga 4.4.1.

Edaspidises tekstis on kasutatud järgnevat notatsiooni tähistamaks nõudeid elementide kasutamisele:

Notatsioon	***Allkirjastamisrakendus***	***Valideerimisrakendus***
M (Mandatory)	Peab looma selle elemendi	Peab töötlema seda elementi
C (*Critical*)	Võib luua selle elemendi	Peab töötlema seda elementi, kui see on olemas
O (*Optional*)	Võib luua selle elemendi	Võib töödelda seda elementi, kui see on olemas
N/A	Element ei ole kasutusel	Element ei ole kasutusel

5.1. Krüptograafiliste algoritmide kasutamine

Krüptograafiliste algoritmide ja võtmepikkuste valikul tuleb lähtuda kaasaegsetest rahvusvahelistest hinnangutest. Headeks allikateks on vastav ETSI standard[11][11][12] ja www.keylength.com. Alltoodud valikud on käesoleva standardi koostamise ajal kehtivad soovitused, BDOC spetsifikatsioon ei keela teistsuguste krüptoalgoritmide ja võtmepikkuste kasutamist.

Räsialgoritmid.
BDOC dokumentide moodustamisel soovitatakse tungivalt kasutada SHA-256 või tugevamat räsialgoritmi. Siiski pole tehniliste piirangute tõttu mõnikord võimalik kasutada midagi muud peale SHA-1. Sellest tulenevalt peab BDOC-sobilik rakendus verifitseerimisel suutma käsitleda SHA-1, SHA-224, SHA-256, SHA-384 ja SHA-512 algoritme ning digitaalallkirja moodustamisel andma endast parima selleks, et kasutada SHA-256 või tugevamat räsialgoritmi. Lubatud URI väärtused elementides `DigestMethod` parameetril `Algorithm` on seega:

```
http://www.w3.org/2000/09/xmldsig#sha1
http://www.w3.org/2001/04/xmldsig-more#sha224
http://www.w3.org/2001/04/xmlenc#sha256
http://www.w3.org/2001/04/xmldsig-more#sha384
http://www.w3.org/2001/04/xmlenc#sha512
```

Asümmeetrilised krüptoalgoritmid
Algoritmi ja võtmepikkuse BDOC dokumendi moodustamisel määrab üheselt ära kasutatava krüptograafilise vahendi võimekus. Soovitus on kasutada vähemalt 2048-bitist võtmepikkust RSA puhul ning vähemalt 224-bitist võtmepikkust elliptiliste kõverate (ECDSA) puhul. Lubatud `URI` väärtused elemendis `SignatureMethod` on seega:

```
http://www.w3.org/2000/09/xmldsig#rsa-sha1
http://www.w3.org/2001/04/xmldsig-more#rsa-sha224
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
http://www.w3.org/2001/04/xmldsig-more#rsa-sha384
http://www.w3.org/2001/04/xmldsig-more#rsa-sha512


http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha1
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha224
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384
http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512
```

5.2. BDOC põhiprofiili definitsioon

BDOC põhiprofiili struktuur koosneb:

- `ds:SignedInfo` plokist, mis sisaldab viiteid (koos räsiväärtustega) allkirjastatud andmeobjektidele
- `ds:SignatureValue` elemendist, mis sisaldab signatuuri
- `ds:KeyInfo` struktuuri, mis sisaldab signeerija sertifikaati
- `xades:QualifyingProperties` plokis sisalduvaid lisaandmeid XAdES-EPES tasemeni.

Järgnevad piirangud kehtivad `ds:SignedInfo` ploki elementide kohta:

Element		***Parameeter***	***Kommentaar***
Signature	M	Id	Näiteks “S0”
SignedInfo	M		
CanonicalizationMethod	M	Algorithm="http://www.w3.org/2006/12/xml-c14n11"	
SignatureMethod	M	Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"	Vt.5.1.
Reference	M	Id	Vt. allpool

`ds:SignedInfo` plokk sisaldab kahte või enamat `ds:Reference` struktuuri, mis viitavad signeeritavatele andmeobjektidele:

- Üks viide igale erinevale signeeritavale konteineris sisalduvale signeeritud failile. Sellisel juhul peab elemendil `ds:Reference` olema parameeter `URI`, mis viitab vastavale andmeobjektile (näiteks “`doc.txt`”).

- Ainult üks viide allpool kirjeldatud plokile `SignedProperties`. Sellisel juhul peab elemendil `ds:Reference` olema parameetrid `Type=`http://uri.etsi.org/01903/#SignedProperties ja `URI`, mis viitab plokile `SignedProperties` (näiteks "`#S0-SignedProperties`")

Kui `ds:Reference` struktuuris sisaldub element `Transforms`, siis tuleb valideerimisrakenduses seda käsitleda. Signatuuri loomisel peab alamelemendil `ds:DigestMethod` olema väärtus:
`http://www.w3.org/2001/04/xmlenc#sha256`
Räsialgoritmidest on täpsemalt juttu jaotises 5.1.

Käesolev spetsifikatsioon ei nõua eraldi `ds:Reference` elementi `ds:KeyInfo` jaoks kuna element `SigningCertificate` on selle spetsifikatsiooni järgi kohustuslik ning seetõttu on allkirjastaja sertifikaat signatuuriga turvatud.

`ds:KeyInfo` element peab sisaldama allkirjastaja ~~avalikku võtit ja~~ sertifikaati. Seega kasutatakse alamelemente `ds:X509Data` ja `ds:X509Certificate`~~Järgnev profileerib RSA algoritmi kasutuse puhul elemendi `ds:KeyInfo` kasutuse, mis põhineb~~ vastavalt XMLDSIG [6] klauslile 4.4~~:~~.

Formatted: Techno Char, English (United States)

Formatted: Techno Char, English (United States)

~~`KeyInfo`~~
~~`  KeyValue`~~
~~`    RSAKeyValue`~~
~~`      Modulus` — RSA mooduluse väärtus~~
~~`      Exponent` — RSA eksponendi väärtus~~
~~`  X509Data`~~
~~`    X509Certificate` — sertifikaat BASE64 kodeeringus~~

~~ECDSA algoritmi kasutamisel tuleb lähtuda XML-DSIG2 [11] jaotises 7.2.3 toodust.~~

XAdES[1] defineerib mehhanismi täiendavate parameetrite kaasamiseks allkirja kasutades `ds:Object` meetodit. Plokis `ds:SignedInfo` viidatud `SignedProperties` element kapsuleeritakse `ds:Object` plokki nii, nagu kirjeldab XAdES[1] klausel 6.2.1.

Järgnev profileerib elementide kasutamise `QualifiedProperties` plokis BDOC põhiprofiili jaoks:

Element		***XAdES klausel***	***Kommentaar***
QualifyingProperties	M	6.2	Peab olema parameeter `Target` mis viitab `ds:Signature` elemendile (näiteks "`#S0`")
SignedProperties	M	6.2.1	Peab olema parameeter `Id` (näiteks "`S0-SignedProperties`")
SignedSignatureProperties	M	6.2.3	

SigningTime	~~O~~M	7.2.1	Kasutatakse “Zulu” ajavööndit
SigningCertificate	M	7.2.2	Sisaldab ainult allkirjastaja sertifikaati; parameetrit `URI` ei kasutata.
SignaturePolicyIdentifier	M	7.2.3	Viitab käesolevale dokumendile ning määrab ära signatuuri räsi arvutamise algoritmi (vt p. 6.1)
SignaturePolicyId	M	7.2.3	
SigPolicyId	M	7.1.2	Kasutatakse meetodit OIDAsURN, OID väärtus on 1.3.6.1.4.1.10015.1000.3.1.1~~1.3.6.1.4.1.10015.1000.3.1.1~~1.3.6.1.4.1.10015.1000.2.10.10
SigPolicyHash	M	7.2.3	Käesoleva dokumendi räsi; allkirja verifitseerimisel ei ole kohustuslik seda kontrollida
SigPolicyQualifiers	M	7.2.3	
SigPolicyQualifier SPURI	M	7.2.3.1	URL käesolevale dokumendile
SigPolicyQualifier NonceAlgorithm	M		"http://www.w3.org/2001/04/xmlenc#sha256", kasutatakse ainult ajamärkide puhul, vt ~~ka~~ p.6.1
SignatureProductionPlace	C	7.2.7	
SignerRole	C	7.2.8	Lubatud on element `ClaimedRoles`; elementi `CertifiedRoles` ei toetata.
SignedDataObjectProperties	M	6.2.4	
DataObjectFormat	M	7.2.5	Kohustuslik igale signeeritud andmeobjektile v.a. element `SignedProperties`
MimeType	M	7.2.5	MIME tüüp
ObjectReference	M	7.2.5	Viide `Reference` elemendis kasutatud Id väärtusele.
CommitmentTypeIndication	N/A	7.2.6	Rolli, resolutsiooni või lubaduse väljendamiseks vaba tekstina kasutage `ClaimedRoles` elementi
AllDataObjectsTimeStamp	N/A	7.2.9	
IndividualDataObjectsTimeStamp	N/A	7.2.10	
UnsignedProperties	M	6.2.2	Vt. paragrahv 6
UnsignedSignatureProperties	M	6.2.5	Vt. paragrahv 6
CounterSignature	N/A	7.2.4	

6. Kvalifitseeritud BDOC allkirjad

BDOC põhiprofiil ei sisalda andmeid, mis võimaldaks kontrollida allkirjastaja sertifikaadi kehtivust (väidetaval) allkirjastamise ajahetkel. BDOC põhiprofiili vormingut võib kasutada sisesüsteemides, kus tegeletakse allkirjastaja sertifikaadi kehtivuse probleemidega mingisugusel teisel (dokumenteerimata) moel.

Sertifikaadi kehtivusinfo tuleb hankida nii pea kui võimalik peale XADES-BES signatuuri tekitamist. Selle jaoks on kaks erinevat stsenaariumi:

- lõppkasutaja arvutis – allkirjastamisrakendus peab hankima kehtivuskinnituse ja vajadusel ajatempli(d) nii pea kui võimalik peale signatuuri loomist;
- veebikeskkonnas – serverirakendus peab hankima kehtivuskinnituse ja vajadusel ajatempli(d) nii pea kui võimalik peale signatuuri loomist;

Kuna signatuuri loomine on tegu, mis tehakse vallasrežiimis, siis ei ole usaldusväärselt selle aega määratleda. See spetsifikatsioon rajaneb põhimõttel, et ”allkirjastamise aeg” tuletatakse väliste kehtivus- ja/või ajatempliteenuste ajainfost. Teiste sõnadega – signatuuri ei saa pidada *täielikuks* või *kehtivaks* ilma kehtivusinfota välistelt teenustelt.

Käesolev BDOC spetsifikatsioon defineerib kaks meetodit selliste elektrooniliste allkirjade loomiseks, mis on võrdväärsed käsitsi kirjutatud allkirjaga. Mõlemad profiilid on ühilduvad XAdES LT-taseme(vt. XAdES BP[8] osa 8) nõuetega ning kaasavad allkirjaga sertifikaatide kehtivusinfot ja ajainfot:

- **ajamärgendus** (*time-marking*): selle stsenaariumi kohasel peab OCSP teenus järgima teatud nõudeid, mis on kirjeldatud jaotises 6.1. Antud juhul ei ole vajalik täiendav ajatembeldusteenus
- **ajatembeldus** (*time-stamping*): kasutatakse juhtudel, kui lisaks OCSP vastusele on vajalikud täiendavad ajatemplid välisest ajatempliteenusest. Vt. XAdES klausel 4.4.3.1.

Rakendused, mis ühilduvad käesoleva BDOC spetsifiktsiooniga, peavad toetama mõlemat ülalnimetatud meetodit.

Mõlemad toetatud vormingud kasutavad elemente XAdES-e plokkidest „T“ ja ”L”.

Element		***XAdES klausel***	***Kommentaar***
SignatureTimeStamp		7.3	Vt. jaotised 6.1 ja 6.2 allpool
CompleteCertificateRefs	N/A	7.4.1	
CompleteRevocationRefs	N/A	7.4.2	
AttributeCertificateRefs	N/A	7.4.3	
AttributeRevocationRefs	N/A	7.4.4	
SigAndRefsTimeStamp	N/A	7.5.1	
RefsOnlyTimeStamp	N/A	7.5.2	
CertificateValues	M	7.6.1	Toetatud on ainult `EncapsulatedX509Certificate`. Peab sisaldama OCSP responderi sertifikaati ja allkirjastaja CA sertifikaati. Juhul, kui kasutatakse ajatembeldamist (vt jaotis 6.2), siis peab siin olema ka ajatempli teenuse sertifikaat.
RevocationValues	M	7.6.2	Toetatud on ainult `OCSPValues` ja `EncapsulatedOCSPValue` elemendid
AttrAuthoritiesCertValues	N/A	7.6.3	
AttributeRevocationValues	N/A	7.6.4	
ArchiveTimeStamp		7.7	Vt paragrahv 7 allpool
UnsignedDataObjectProperties	N/A	6.2.6	

6.1. BDOC ajamärkidega

XAdES spetsifikatsioon defineerib ajamärgi järgmiselt: “usaldatud teenuse poolt antud ajamärgil on samasugune efekt kui ajatemplil kuid sellisel juhul ei lisata seda elektroonilisele allkirjale ning teenuseseosutaja kohustus on esitada nõudmisel tõend ajamärgi kohta”.

Käesolev BDOC spetsifikatsioon defineerib ajamärgenduse mehhanismi kasutades OCSP[4] protokolli. Koheselt peale signatuuri loomist peab allkirjastamise rakendus võtma kehtivuskinnituse kasutades OCSP protokolli. Signatuuri räsi väärtus peab olema OCSP päringu “nonce” väljal. OCSP responder peab tagastama selle “nonce” välja signeeritud vastuses.

Signatuuri räsi arvutamise algoritm määratakse ära elemendis `NonceAlgorithm`, vt.jaotis 5.2.

Selline mehhanism lahendab ühekorraga ajatembelduse ja sertifikaadi kehtivuse omavahelise suhte keerukuse kombineerides need ühte teenusesse. Ülalkirjeldatud OCSP vastust tuleb käsitleda kui kehtivuskinnitust, mis ütleb: “hetkel, kui ma seda signatuuri nägin, oli vastav sertifikaat kehtiv” ning see on digitaalselt signeeritud. Tulemusena ei ole ~~täiendavad~~ ajatempel~~id~~ vajalik~~ud~~ ja element~~ei~~ `SignatureTimeStamp` ~~ja~~ ~~`SigAndRefsTimeStamp`~~ ei kasutata.

OCSP teenus peab olema ”reaal-aja” teenus ja peegeldama sertifikaatide hetkeolekut (mitte põhinema tühistusnimekirjal). Teenus peab täitma ETSI standardis “*Policy requirements for time-stamping authorities*” [7] toodud nõudeid.

Allkirja andmise ajaks tuleb lugeda OCSP kehtivuskinnituse vastuses sisalduva välja `ProducedAt` väärtust.

6.2. BDOC ajatemplitega

BDOC profiili ajatemplitega kasutatakse juhul, kui OCSP teenus ei vasta jaotises 6.1. toodud nõuetele. Sellisel juhul on vajalikud täiendavad ajatemplid sertifikaadi kehtivusinfo aja fikseerimiseks.

See saavutatakse ajatempli elemendi `SignatureTimeStamp` kaasamise teel allkirja struktuuri. Ajatempel võetakse nii pea kui võimalik peale signatuuri loomist.

Käesolev spetsifikatsioon ei sea nõudeid verifitseerimispõhimõtetele, mis puudutab aktsepteeritavaid ajaintervalle erinevate allkirja elementide vahe (väidetav signeerimisaeg elemendis `SigningTime`, aeg ajatemplis `SignatureTimeStamp`, aeg OSCP kehtivuskinnituses `ProducedAt` väljal).

Ajatempli vormingud on defineeritud XAdES[1] klauslis 7.1.4 ja näevad ette ülimalt paindlikke võimalusi. Käesolev BDOC spetsifikatsioon profileerib ajatemplid järgmiselt:

- Toetatud on ainult IETF standardile RFC3161 vastavad ajatemplid (s.t. toetatud on ainult element `EncapsulatedTimeStamp`)
- Ajatembeldus peab tembeldavatele andmeobjektidele viitamiseks kasutama *explicit* mehhanismi kasutades `Include` meetodit nii nagu on kirjeldatud XAdES[1] klauslis 7.1.4.3.1. See tähendab, et `ReferenceInfo` meetod ei ole toetatud.
- Elemendis `Include` on toetatud URI element, `referencedData` ei ole toetatud.
- Atribuut `Id` on kohustuslik

Formatted: Techno Char, English (United States)

Need reeglid kehtivad kõikidele käesolevas spetsifikatsioonis kasutatud ajatemplite kohta.

Allkirja andmise ajaks tuleb lugeda aja väärtust elemendis `SignatureTimeStamp`.

7. Pikaajalise tõestusväärtuse tagamine

Eelmises peatükis spetsifitseeritud BDOC allkirjad on piisavalt turvalised juhul, kui kasutatud krüptoalgoritmid on murdmatud, võtmepikkused piisavad ja teenusepakkuja (CA ja OSCP) privaatvõtmed jäävad tema kontrolli alla.

Arvutusjõudluse kiire ja pidev kasv viitab sellele, et võtmepikkused ja algoritmid, mis täna tunduvad turvalised, ei ole seda tulevikus enam mitte. Alati on olemas ka (teoreetiline) võimalus, et teenusepakkuja teenusevõtmed korrumpeeruvad (s.t. satuvad võõrastesse kätesse).

Kirjeldatud ohtude vastaseks kaitseks on vajalikud täiendavad meetmed. Käesolev dokument kirjeldab kahte mehhanismi elektrooniliste allkirjade pikaajalise tõestusväärtuse tagamiseks:

- **Logimine:** teenusepakkuja, kes kinnitab sertifikaadi kehtivust allkirjastamise ajal, peab logi väljaantud kinnituste kohta
- **Üle-ajatembeldamine:** kogu allkirja materjali ajatembeldatakse perioodiliselt üle

Esimene võimalus ei nõua lõpp-kasutajalt eraldi tegevusi ega BDOC-sobivalt süsteemilt täiendavat funktsionaalsust ning on seetõttu eelistatud meetod. Teisalt seab logimine täiendavaid nõudeid teenusepakkujale, mida viimane ei pruugi täita. Selleks, et anda lõppkasutajale täielik kindlus ning teatav sõltumatus teenusepakkujast, peaks üle-ajatembeldamise mehhanism olema samuti toetatud.

7.1. Logimine

See mehhanism rajaneb põhimõttel säilitada pikaks ajaks tõendusmaterjali selle kohta, et "allkirjastaja sertifikaat oli kehtiv allkirja andmise ajal".

Olenevalt kvalifitseeritud BDOC allkirja meetodist, peab logi kõikidest väljastatud vastustest tekitama:

- ajamärgenduse puhul (jaotis 6.1) OCSP teenus
- ajatembelduse puhul (jaotis 6.2) ajatembeldusteenus ja OCSP teenus

Logikirje tuleb tekitada **ennem** vastuse väljastamist. Kui logikirje loomine ebaõnnestub, siis tuleb vastuseks väljastada veateade. See põhimõte tagab logikirje olemasolu igale väljastatud vastusele.

Teenusepakkuja peab pakkuma avalikku liidest, mis võimaldab kontrollida kindla logikirje olemasolu tema logis.

Logimismehhanismi edasiseks kindlustamiseks võivad kasutuses olla täiendavad turvameetmed:

- Krüptograafiline linkimine: iga logikirje on sõltuv eelmisest. Seda saab saavutada räsiahela loomisega, mis muudab iga logikirje sõltuvaks kõikidest eelnevatest. Selline linkimine hoiab ära logi võltsimise – logikirjete kustutamise või võltskirje vahele sokutamise
- Viimase logikirje publitseerimine ajakirjanduses. See mehhanism annab teenusepakkujale teatava salgamise vääramise meetme – see võtab ära teenusepakkujalt kõik võimalused logi võltsimiseks kuna publitseeritud logikirje esindab kogu logi. Loomulikult on see meetod kohaldatav ainult juhul, kui kasutatakse krüpteerimist linkimist.

Logi adekvaatse halduse ja varundamise peale tuleb pöörata olulist tähelepanu.

7.2. Üle-ajatembeldamine

See mehhanism rajaneb põhimõttel "kindlustame seda, mis võib olla nõrk". Järjestikkused ajatemplid kaitsevad kogu materjali nõrkade räsialgoritmide ning krüptograafilise materjali ja algoritmide murdmise eest.

Peab märkima, et ajatembeldamine on üldjuhul kasutaja poolt algatatud tegu. Juhul, kui digitaalselt allkirjastatud failid on kasutajate arvutis (või isegi välistel andmekandjatel) laiali, siis võib olla väga keeruline (kui mitte võimatu) tagada seda, et dokumendid saaksid õigel ajal üle-ajatembeldatud. Sellegi poolest võib üle-ajatembeldamine osutada kasutamiskõlbulikuks juhul, kui digitaalselt allkirjastatud faile hoitakse mõnes keskses repositooriumis.

BDOC üle-ajatembeldamine vastab XAdES[1]~~[1]~~ klauslis 8.2 toodule. Toetatud on "mittehajutatud juht", mida kirjeldab klausel 8.2.1. Element `xadesv141:ArchiveTimeStamp` profileeritakse käesoleva spetsifikatsioonis jaotises 6.2 toodud reeglite kohaselt.

8. Konteineri vorming

See peatükk kirjeldab konteineri vormingut, kuhu pakitakse originaalfailid ja allkirjad. Teisesõnutsi defineerib see, “mis on digitaalselt allkirjastatud fail”.

BDOC faili vorming põhineb standardil ASiC[9], mida omakorda profileerib ASiC BP [10]~~, mis~~. Viimane näeb ette ODF-stiilis pakendust, mis on omakorda spetsifitseeritud OASIS-e standardis OpenPackaging[5].

BDOC pakendus on ASiC BP[10]~~on~~ standardile vastav ASiC-E XAdES-tüüpi (vt [10] klausel 8.3) ZIP konteiner, kus on ~~järgitud~~ täidetud järgmis~~i~~ed nõude~~i~~d:

1. **MIME-tüübi fail**. Fail nimega ”mimetype” peab olema olemas ning pakendatud kompressimata kujul nii nagu kirjeldatud ASiC[9] standardi klauslis A.1. Faili sisu peab olema:

   ```
   application/vnd.etsi.asic-e+zip
   ```

2. **Manifesti fail.** Fail nimega “manifest.xml” peab olema kataloogis META-INF/ ja peab sisaldama loetelu kõikidest konteineris sisalduvatest kataloogidest ja failidest nii nagu kirjeldatud OpenDocument[5]~~[5]~~ standardi klauslis 3.2. Loetelu ei sisalda faili „mimetype“ ega kataloogis „META-INF/“ olevaid faile, s.h. allkirjafailid.

Faili juurelement peab olema sama tüüpi kui „mimetype“ failis.

Allkirjad salvestatakse üldjuhul eraldi failidena META-INF/ kataloogi nii, et igas failis on täpselt üks allkiri. Nende failide nimed peavad sisaldama stringi „signatures“. Iga allkirjafaili juurelement peab olema `<asic:XAdESSignatures>`. Juht, kus ühes allkirjafailis on mitu allkirja, peab olema toetatud.

Reeglina on kõik BDOC konteineris sisalduvad failid signeeritud peale „mimetype“ faili ja failide META-INF/ kataloogis. Sellegi poolest on signeeritud objektid otseselt viidatud allkirjas sisalduvate `<Reference>` elementidega, mistõttu BDOC-ühilduvad rakendused peavad allkirjastatud failide kuvamisel lähtuma sellest.

~~Fail manifest.xml peab olema signeeritud[1],~~

BDOC faili laiend on “.bdoc”, rakendused võivad toetada ka faililaiendeid „.asice“ ja „.sce“. MIME tüüp on “ application/vnd.etsi.asic-e+zip”.

~~[1] See nõue võib kaduda standardi ETSI TS 103 174 V2.1.1 (2012-03) - ASiC Baseline Profile uue versiooniga. Tuleb lähtuda nimetatud standardi viimasest versioonist, vt p.8.3.2.~~

Lisa: Näidis BDOC

Järgnev näidisfail sisaldab üht kapseldatud originaalfaili, üht allkirja ja see on koos ajatemplitega.

1. BDOC faili struktuur

```
document.doc
mimetype
META-INF/manifest.xml
META-INF/signatures1.xml
```

2. Faili “mimetype” sisu

```
application/vnd.etsi.asic-e+zip
```

3. Faili “META-INF/manifest.xml” sisu

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE manifest:manifest PUBLIC " //OpenOffice.org//DTD Manifest 1.0//EN"
"Manifest.dtd">
<manifest:manifest
xmlns:manifest="urn:oasis:names:tc:opendocument:xmlns:manifest:1.0">
<manifest:file-entry manifest:media-type="application/vnd.etsi.asic-e+zip"
manifest:full-path="/" />
<manifest:file-entry manifest:media-type="application/msword"
       manifest:full-path="document.doc" />
</manifest:manifest>
```

4. Faili “META-INF/signatures1.xml” sisu

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<asic:XAdESSignatures xmlns:asic="http://uri.etsi.org/02918/v1.2.1#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:nonce="http://www.sk.ee/repository/NonceAlgorithm"
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#">

  <ds:Signature Id="S0">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-
c14n11"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha224"/>
      <ds:Reference Id="S0-RefId0" URI="document.doc">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>5UyKB9ht94y6CZNvLdO1C7Z3MXaYc2Qol3Dt3Qp4Ajg=
</ds:DigestValue>
      </ds:Reference>
      <ds:Reference Id="S0-RefId1" URI="META-INF/manifest.xml">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>DHaQsCfAX9oB6aDOukkNlsKOMAH2FuCr4cuudh+xppg=
</ds:DigestValue>
      </ds:Reference>
      <ds:Reference Id="S0-RefId12"
Type="http://uri.etsi.org/01903#SignedProperties" URI="#S0-SignedProperties">
```

```
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>YGDmd4GaWLgV4/hrEVV6/DvQ6uLhfnTSI0CQJX612KM=
</ds:DigestValue>
       </ds:Reference>
     </ds:SignedInfo>
     <ds:SignatureValue Id="S0-SIG">
YQs06u9ekMnZd2Jy+Won5VK0kIC9y5e2JPfraUItZOqwxd4rc4g3fiUnDkrf
iHIdD2xOGyszCZA/JAicqDPiFkmXbjkgpYYF8gY3NB/xFwoKv/zaWu7HEi+T
eq/OoSDlXVGi0H++27nI3xAl7P7Iz84xajilaquZQVl5iOtWD8k=
     </ds:SignatureValue>
      <ds:KeyInfo>
       <ds:KeyValue>
        <ds:RSAKeyValue>
         <ds:Modulus>
w5pn8hDi92l5E58b3ITgw7q5yfc9BECte8ot9B5ZqEikoP1y3U1Xu4XNAM6F
2ktClO9kNx1RQFoiW4FIRuBLr/Q1mpVQpROx0Oie5348DlNlfgxjIgFOTdtY
zEJFaq+CJQd3BeOZqyn2rhMyjf3hlYwNDUssn6ltJTqvx6Ierjs=
         </ds:Modulus>
         <ds:Exponent>Smya6Q==</ds:Exponent>
        </ds:RSAKeyValue>
       </ds:KeyValue>
       <ds:X509Data>
         <ds:X509Certificate>
MIIEnDCCA4SgAwIBAgIQfybdp3nKOMhPqk9YDxgaTTANBgkqhkiG9w0BAQU...
x3CqdYNWwQhU2bMirW4=
        </ds:X509Certificate>
       </ds:X509Data>
     </ds:KeyInfo>
     <ds:Object>
       <xades:QualifyingProperties Target="#S0">
         <xades:SignedProperties Id="S0-SignedProperties">
           <xades:SignedSignatureProperties>
             <xades:SigningTime>2012-12-09T15:49:32Z</xades:SigningTime>
             <xades:SigningCertificate>
               <xades:Cert>
                 <xades:CertDigest>
                   <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                   <ds:DigestValue>z/CsSIOu/w4lP63VzQEXRkxsT/oht2ggvA6rMxDQvoA=
</ds:DigestValue>
                 </xades:CertDigest>
                 <xades:IssuerSerial>
                   <ds:X509IssuerName>emailAddress=pki@sk.ee,CN=TEST of ESTEID-
SK 2011,O=AS Sertifitseerimiskeskus,C=EE</ds:X509IssuerName>
<ds:X509SerialNumber>169013758426626343561532977746185558605</ds:X509SerialNumb
er>
                 </xades:IssuerSerial>
               </xades:Cert>
             </xades:SigningCertificate>
             <xades:SignaturePolicyIdentifier>
               <xades:SignaturePolicyId>
                 <xades:SigPolicyId>
                   <xades:Identifier
Qualifier="OIDAsURN">urn:oid:1.3.6.1.4.1.10015.1000.3.1.11.3.6.1.4.1.10015.1000
.3.1.11.3.6.1.4.1.10015.1000.2.10.10</xades:Identifier>
                 </xades:SigPolicyId>
                 <xades:SigPolicyHash>
                   <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>FN9y5GRujvlIdPGXS+uTA6L1XBZDep2v9qFgk7zif9w=*** SIIN ON
KÄESOLEVA DOKUMENDI RÄSIVÄÄRTUS BASE64 KODEERINGUS ***
</ds:DigestValue>
```

Formatted: Font: (Default) Courier New, 9 pt

Formatted: Font: (Default) Courier New, 9 pt

```
                </xades:SigPolicyHash>
                <xades:SigPolicyQualifiers>
                  <xades:SigPolicyQualifier>
                    <xades:SPURI>https://www.sk.ee/repository/bdoc-
spec20.pdf</xades:SPURI>
                  </xades:SigPolicyQualifier>
                  <xades:SigPolicyQualifier>
<nonce:NonceAlgorithm>http://www.w3.org/2001/04/xmlenc#sha256</nonce:NonceAlgor
ithm>
                  </xades:SigPolicyQualifier>
                </xades:SigPolicyQualifiers>
              </xades:SignaturePolicyId>
            </xades:SignaturePolicyIdentifier>
            <xades:SignatureProductionPlace>
             <xades:City>Tallinn</xades:City>
             <xades:StateOrProvince>Harju</xades:StateOrProvince>
             <xades:PostalCode>10122</xades:PostalCode>
             <xades:CountryName>Estonia</xades:CountryName>
            <xades:/SignatureProductionPlace>
            <xades:SignerRole>
             <xades:ClaimedRoles>
              <xades:ClaimedRole>Agreed</xades:ClaimedRole>
             </xades:ClaimedRoles>
           </xades:SignerRole>
          </xades:SignedSignatureProperties>
          <xades:SignedDataObjectProperties>
            <xades:DataObjectFormat ObjectReference="#S0-RefId0">
              <xades:MimeType>text/plainapplication/msword</xades:MimeType>
            </xades:DataObjectFormat>
            <xades:DataObjectFormat ObjectReference="#S0-RefId1">
              <xades:MimeType>application/xml</xades:MimeType>
            </xades:DataObjectFormat>
          </xades:SignedDataObjectProperties>
        </xades:SignedProperties>
   <xades:UnsignedProperties>
    <xades:UnsignedSignatureProperties>
     <xades:SignatureTimeStamp Id="S0-T0">
      <xades:Include URI="#S0-SIG"></xades:Include>
      <xades:EncapsulatedTimeStamp>
MIIMYzADAgEAMIIMWgYJKoZIhvcNAQcCoIIMSzCCDEcCAQMxCzAJBgUrDgMCGgUA
       ...
       ZSQAy4ewaA==
      </xades:EncapsulatedTimeStamp>
     </xades:SignatureTimeStamp>
     <xades:CertificateValues>
      <xades:EncapsulatedX509Certificate Id="S0-CA-CERT">
MIIDPDCCAiSgAwIBAgIEQi2iwTANBgkqhkiG9w0BAQUFADB8MRgwFgYJKoZIhvcN
       ...
       EWyMVkNnZooWHIjLpNucQA==
      </xades:EncapsulatedX509Certificate>
      <xades:EncapsulatedX509Certificate Id="S0-RESPONDER_CERT">
MIIEITCCAwmgAwIBAgIBDDANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSUUx
       ...
       EWyMVkNnZooWHIjLpNucQA==
      </xades:EncapsulatedX509Certificate>
     </xades:CertificateValues>
     <xades:RevocationValues>
      <xades:OCSPValues>
       <xades:EncapsulatedOCSPValue Id="N0">
MIIBtgoBAKCCAa8wggGrBgkrBgEFBQcwAQEEggGcMIIBmDCCAQGhcTBvMQswCQYD
        ...
        knf8XDhdklVD0w==
        </xades:EncapsulatedOCSPValue>
```

```
        </xades:OCSPValues>
       </xades:RevocationValues>
      </xades:UnsignedSignatureProperties>
     </xades:UnsignedProperties>
    </xades:QualifyingProperties>
   </xades:Object>
  </xades:Signature>
</asic:XAdESSignatures>
```