BDOC – DIGITAALALLKIRJA VORMING

Versioon 2.1.2:2014

OID: 1.3.6.1.4.1.10015.1000.3.2.3

Sisukord

Sisukord 2
Sissejuhatus 3
1. Käsitlusala 4
2. Viited 5
3. Definitsioonid ja lühendid 6
4. Ülevaade 7
5. BDOC põhiprofiil 8
5.1. Krüptograafiliste algoritmide kasutamine 8
5.2. BDOC põhiprofiili definitsioon 9
6. Kvalifitseeritud BDOC-allkirjad 12
6.1. BDOC ajamärkidega 14
6.2. BDOC ajatemplitega 14
7. Pikaajalise tõestusväärtuse tagamine 16
7.1. Logimine 16
7.2. Arhivaalne ajatembeldamine 17
8. Konteineri vorming 18
Lisa 1: BDOC-faili näidis 19
Lisa 2: BDOC allkirja profiilid 22

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

ETSI standard TS 101 903[1] (edaspidi: XAdES) defineerib 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[8] profileerib standardit XAdES, ahendades valikuvõimalusi.

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

Käesolev BDOC standard on täielikult ühilduv ülalnimetatud ETSI standarditega.

Käesolev dokument:

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

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

1. Käsitlusala

Käesolev dokument defineerib 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.

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 6960 – 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 esitab väliste allikate täieliku loetelu.

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

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

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

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 6960: “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] ETSI TS 102 176-1 V2.1.1 (2011-07) - Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

[12] RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”

3. Definitsioonid ja lühendid

Käesoleva dokumendi otstarbeks kehtivad definitsioonid ja lühendid XAdES [1] peatükist 4 ja alljärgnevad.

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

Käesolev 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[8], ASiC[9] ja selle baasprofiil[10]) on kaetud käesoleva spetsifikatsiooniga, kuid nendega tutvumine võib lugejale anda täiendavat informatsiooni.

Lisa 2 sisaldab ülevaadet kasutatavatest XAdES-e elementidest BDOC eri variantides.

5. BDOC põhiprofiil

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

BDOC põhiprofiil põhineb XAdES-EPES (*Explicit Policy based Electronic Signature*) vormingul ja on määratletud XAdES[1] sättega 4.4.2.

Nõudeid elementide kasutamisele tähistavad järgnevas tekstis märgised vastavalt tabelile

Tabel 1. Elementide kasutamise märgised

Märgis	***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 nüüdisaegsetest rahvusvahelistest hinnangutest. Headeks allikateks on vastav ETSI standard[11] ja www.keylength.com. Alltoodud valikud on käesoleva standardi koostamise ajal kehtinud soovitused, kuid BDOC spetsifikatsioon ei keela teistsuguste krüptoalgoritmide ja võtmepikkuste kasutamist.

Räsialgoritmid.
BDOC dokumentide moodustamisel soovitatakse tungivalt kasutada SHA-256 või sellest tugevamat räsialgoritmi. Siiski pole tehniliste piirangute tõttu mõnikord võimalik kasutada midagi muud peale SHA-1. Seetõttu peab BDOC-ühilduv rakendus verifitseerimisel suutma käsitleda algoritme SHA-1, SHA-224, SHA-256, SHA-384 ja SHA-512 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 määrab BDOC-dokumendi moodustamisel kasutatava krüptograafilise vahendi võimekus. Soovitatav 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 järgmistest osadest:

- `ds:SignedInfo` -- plokk, mis sisaldab viiteid (koos räsiväärtustega) allkirjastatud andmeobjektidele
- `ds:SignatureValue` -- element, mis sisaldab signatuuri
- `ds:KeyInfo` -- struktuur, mis sisaldab signeerija sertifikaati
- `xades:QualifyingProperties` -- selles plokis sisalduvad lisaandmed XAdES-EPES tasemeni

Ploki `ds:SignedInfo` plki elementide kohta kehtivad järgmised piirangud.

Tabel 2. Piirangud plokis `ds:SignedInfo`

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

`Plokk ds:SignedInfo` sisaldab kaht või enamat `ds:Reference`-struktuuri, mis viitavad signeeritavatele andmeobjektidele.

- Üks viide igale erinevale signeeritavale konteineris sisalduvale 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 peavad 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 täpsema teavetjaotises 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.

`Element ds:KeyInfo` peab sisaldama allkirjastaja sertifikaati. Seega kasutatakse alamelemente `ds:X509Data` ja `ds:X509Certificate` vastavalt XMLDSIG [6] sättele 4.4.

XAdES[1] defineerib mehhanismi täiendavate parameetrite kaasamiseks allkirja meetodiga `ds:Object`. Plokis `ds:SignedInfo` viidatud element `SignedProperties` kapseldatakse plokki `ds:Object` nii, nagu kirjeldab XAdES[1] säte 6.2.1. Kasutatakse otsest (direct) kapseldamist vastavalt XAdES jaotisele 6.3, s.t. element QualifyingPropertiesReference ei ole toetatud.

Järgnev profileerib elementide kasutamise `QualifyingProperties`-plokis BDOC põhiprofiili jaoks.

Tabel 3. Parameetrid plokis `QualifyingProperties`, BDOC põhiprofiili puhul

Element		***XAdES klausel***	***Kommentaar***
QualifyingProperties	M	6.2	Peab olema parameeter `Target`, mis viitab elemendile `ds:Signature` (näiteks "`#S0`")
SignedProperties	M	6.2.1	Peab olema parameeter `Id` (näiteks "`S0-SignedProperties`")
SignedSignatureProperties	M	6.2.3	
SigningTime	M	7.2.1	Kasutatakse ajavööndit "Zulu"
SigningCertificate	M	7.2.2	Sisaldab ainult allkirjastaja sertifikaati; parameetrit `URI` ei kasutata.

SignaturePolicyIdentifier	M või N/A	7.2.3	Viitab käesolevale dokumendile. Kasutatakse ainult ajamärkidega BDOC-i puhul (vt p. 6.1).
SignaturePolicyId	M	7.2.3	
SigPolicyId	M	7.1.2	Kasutatakse meetodit OIDAsURN, OID väärtus on 1.3.6.1.4.1.10015.1000.3.2.3
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-viide käesolevale dokumendile
SignatureProductionPlace	C	7.2.7	
SignerRole	C	7.2.8	Lubatav 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 elemendis `Reference` kasutatud Id väärtusele.
CommitmentTypeIndication	N/A	7.2.6	Rolli, resolutsiooni või lubaduse väljendamiseks vaba tekstina kasutada elementi `ClaimedRoles`
AllDataObjectsTimeStamp	N/A	7.2.9	
IndividualDataObjectsTimeStamp	N/A	7.2.10	
UnsignedProperties	M	6.2.2	Vt. jaotis 6
UnsignedSignatureProperties	M	6.2.5	Vt. jaotis 6
CounterSignature	N/A	7.2.4	

6. Kvalifitseeritud BDOC-allkirjad

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

Sertifikaadi kehtivusteave tuleb hankida niipea kui võimalik peale XADES-BES signatuuri tekitamist. Selleks on kaks erinevat stsenaariumi:

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

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

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

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

Tabel 4. Elemendid 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. OCSP vastus peab olema väärtusega „good“.
AttrAuthoritiesCertValues	N/A	7.6.3	
AttributeRevocationValues	N/A	7.6.4	
Xadesv141: TimeStampValidationData		8.1	Vt jaotis 7.2 allpool
xadesv141: ArchiveTimeStamp		8.2	Vt jaotis 7 allpool
UnsignedDataObjectProperties	N/A	6.2.6	

6.1. BDOC ajamärkidega

XAdES-e spetsifikatsioon defineerib ajamärgi järgmiselt: “usaldatud teenuse väljastatud ajamärgil on samasugune toime kui ajatemplil, kuid sellisel juhul ei lisata seda elektroonilisele allkirjale ning teenuseandja on kohustatud on esitama nõudmisel tõendi ajamärgi kohta”.

Käesolev BDOC spetsifikatsioon defineerib ajamärkide mehhanismi, mis kasutab OCSP[4] protokolli. Kohe pärast signatuuri loomist peab allkirjastamise rakendus võtma kehtivuskinnituse, kasutades OCSP-protokolli. OCSP päringu väljal “nonce” peab olem signatuuri räsi binaarne väärtus ning räsialgoritrmini identifikaator. OCSP responder peab tagastama selle nonce-välja signeeritud vastuses. Nonce-välja sisu peab olema DER-kodeeritud vastavalt järgmisele ASN.1 struktuurile:

```
TBSDocumentDigest ::= SEQUENCE {
      algorithm AlgorithmIdentifier,
      digest OCTET STRING
}
```

Element `digest` on signatuuri räsiväärtus binaarsel kujul ning element `algorithm` määrab kasutatud räsialgoritmi vastavalt RFC5280[12]jaotisele 4.1.1.2.
Selline mehhanism lahendab ühekorraga ajatembelduse ja sertifikaadi kehtivuse omavahelise suhte keerukuse, ühendades 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 ajatempel vajalik ja elementi `SignatureTimeStamp` ei kasutata.

OCSP teenus peab olema reaalajateenus, mis peegeldab võimalikult värsket tõendusmaterjali sertifikaadi kehtivuse kohta. See tähendab, et OCSP vastuse väljade `thisUpdate` ja `producedAt` vahe peab olema mõõdetav sekundites. Teenus peab täitma ETSI standardis “*Policy requirements for time-stamping authorities*” [7] esitatud nõuded.

Nimetatud meetod ei kaitse allkirja moodustamiseks kasutatud räsifunktsiooni kollisioonikindluse kao vastu.

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 kehtivusteabe aja fikseerimiseks.

See saavutatakse ajatempli elemendi `SignatureTimeStamp` kaasamise teel allkirja struktuuri. Ajatempel võetakse niipea kui võimalik pärast signatuuri loomist.

Käesolev spetsifikatsioon ei sea nõudeid verifitseerimispõhimõtetele, mis puudutavad aktsepteeritavaid ajavahemikke allkirja elementide vahel. Siiski - aeg elemendis `SignatureTimeStamp` peab olema varasem kui aeg OSCP kehtivuskinnituses `ProducedAt` väljal.

Element `SignatureTimeStamp` on defineeritud XAdES[1] jaotises 7.3. Selle elemendi tüüp on `XAdESTimeStampType` vastavalt jaotisele 7.1.4.3. Käesolev BDOC spetsifikatsioon profileerib seda elementi järgmiselt:

- toetatud on ainult IETF standardile RFC3161 vastavad ajatemplid (st toetatud on ainult element `EncapsulatedTimeStamp`),
- atribuut `Id` on kohustuslik.

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 praktiliselt murdumatud, võtmepikkused piisavad ja teenuseandja (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 teenuseandja teenusevõtmed paljastatakse (s.t. satuvad võõrastesse kätesse).

Kirjeldatud ohtude vastaseks kaitseks on vajalikud täiendavad meetmed. Käesolev dokument kirjeldab kaht mehhanismi elektrooniliste allkirjade pikaajalise tõestusväärtuse tagamiseks; need on

- **logimine:** teenuseandja, kes kinnitab sertifikaadi kehtivust allkirjastamise ajal, peab logi väljaantud kinnituste kohta;
- **arhivaalne ajatempel:** kogu allkirja materjali ajatembeldatakse perioodiliselt üle.

Esimene võimalus ei nõua lõppkasutajalt eraldi tegevusi ega BDOC-ühilduvalt süsteemilt lisafunktsioone ning on seetõttu eelistatav meetod. Teisalt seab logimine täiendavaid nõudeid teenuseandjale, mida see ei pruugi täita. Et anda lõppkasutajale täielik kindlus ning teatav sõltumatus teenuseandjast, peaks arhivaalse 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, peavad vastavad teenused logima kõiki väljastatud vastuseid:

- ajamärgenduse puhul teeb seda (jaotis 6.1) OCSP teenus,
- ajatembelduse puhul (jaotis 6.2) ajatembeldusteenus ja OCSP teenus.

Logikirje tuleb tekitada **enne** vastuse väljastamist. Kui logikirje loomine ebaõnnestub, tuleb vastuseks väljastada veateade. See põhimõte tagab logikirje olemasolu iga väljastatud vastuse kohta.

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

Logimismehhanismi kindlustamiseks võivad kasutusel olla täiendavad turvameetmed:

- krüptograafiline sidumine: iga logikirje sõltub eelmisest. Seda saab teha räsiahelaga, mis muudab iga logikirje sõltuvaks kõikidest eelnevatest. Selline sidumine hoiab ära logi võltsimise – logikirjete kustutamise või võltskirje vahelepistmise;
- viimase logikirje avaldamine ajakirjanduses. See mehhanism loob teenuseandjale teatava salgamistõrjemeetme – see võtab teenuseandjalt kõik võimalused logi võltsimiseks, kuna avaldatud logikirje esindab kogu logi. Loomulikult on see meetod rakendatav ainult juhul, kui kasutatakse krüptograafilist linkimist.

Logi adekvaatse haldusele ja varundamisele tuleb pöörata piisavat tähelepanu.

Kirjeldatud meetod ei kaitse BDOC allkirju juhul, kui kaob signatuuri moodustamisel kasutatud räsifunktsiooni kollisioonikindlus.

7.2. Arhivaalne ajatembeldamine

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

Tuleb silmas pidada, et ajatembeldamine on enamasti kasutaja algatatud toiming. Juhul, kui digitaalselt allkirjastatud failid on kasutajate arvutites (või isegi välistel andmekandjatel) laiali, võib olla väga keeruline (kui mitte võimatu) tagada seda, et dokumendid saaksid õigel ajal üle-ajatembeldatud. Sellegi poolest võib üle-ajatembeldamine osutuda kasutamiskõlbulikuks juhul, kui digitaalselt allkirjastatud faile hoitakse mõnes keskses hoidlas.

BDOC arhivaalne ajatembeldamine vastab XAdES[1] jaotises 8.2 toodule. Toetatud on “mittehajus juht”, mida kirjeldab jaotis 8.2.1. Elementi `xadesv141:TimeStampValidationData` (jaotis 8.1) kasutatakse juhul, kui muudes BDOC elementides ei sisaldu vajalikke andmeid ajatempli verifitseerimiseks. Sarnaselt elemendiga `SignatureTimeStamp` on toetatud ainult `EncapsulatedTimeStamp` ning element `Id` on kohustuslik.

8. Konteineri vorming

See jaotis kirjeldab originaalfailide ja allkirjade pakkimise konteineri vormingut, , st defineerib selle, “mis on digitaalselt allkirjastatud fail”.

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

BDOC pakendus on ASiC BP[10] standardile vastav ASiC-E XAdES-tüüpi (vt [10] jaotis 8.3) ZIP-konteiner, kus on täidetud järgmised nõuded.

1. **MIME-tüübi fail**. Fail nimega ”mimetype” peab olema olemas ning pakendatud tihendamata kujul nii, nagu on kirjeldatud ASiC[9] standardi jaotises 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 on kirjeldatud OpenDocument[5] standardi jaotises 3.2. Loetelu ei sisalda faili „mimetype“ ega kataloogis „META-INF/“ olevaid faile, st allkirjafaile.

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

Allkirjad salvestatakse tavaliselt 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>`. Peab olema toetatud ka juht, kus ühes allkirjafailis on mitu allkirja.

Reeglina on kõik BDOC konteineris sisalduvad failid signeeritud, peale faili „mimetype“ ja failide META-INF/ kataloogis. Sellegipoolest on signeeritud objektidele otseselt viidatud allkirjas sisalduvate `<Reference>` elementidega, mistõttu BDOC-ühilduvad rakendused peavad allkirjastatud failide kuvamisel lähtuma sellest. Kõik allkirjad ühes BDOC konteineris peavad viitama samadele andmeobjektidele.

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

Lisa 1: BDOC-faili näidis

Järgnev näidisfail sisaldab üht kapseldatud originaalfaili ja üht allkirja ning on loodud ajamärgendiga.

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"?>
<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: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"
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
```

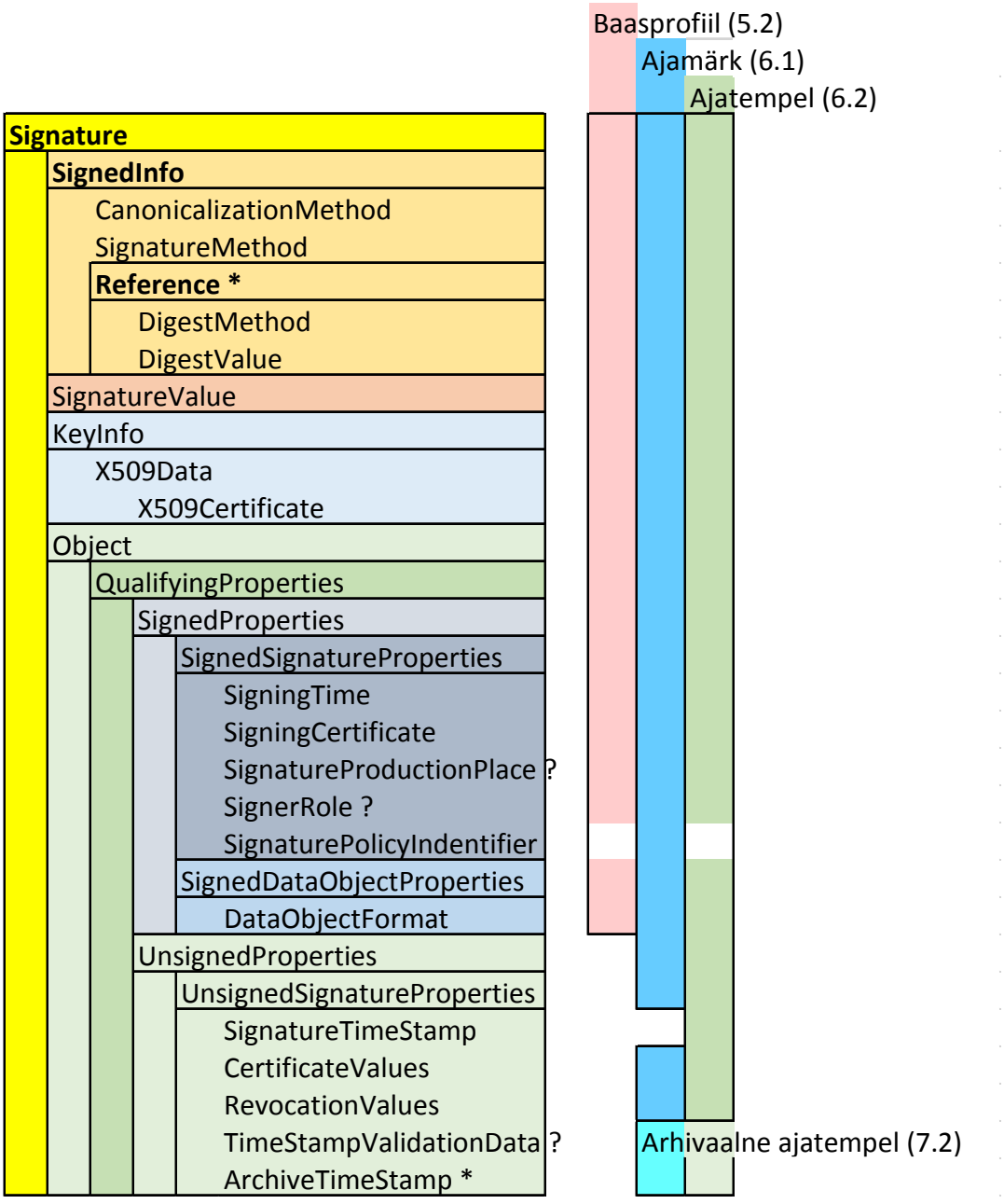
```
eq/OoSDlXVGi0H++27nI3xAl7P7Iz84xaji1aquZQVl5iOtWD8k=
    </ds:SignatureValue>
     <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
MIIEnDCCA4SgAwIBAgIQfybdp3nKOMhPqk9YDxgaTTANBgkqhkiG9w0BAQU...
x3CqdYNWwQhU2bMirW4=
       </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
    <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/w41P63VzQEXRkxsT/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:1.3.6.1.4.1.10015.1000.3.2.3</xades:Identifier>
                </xades:SigPolicyId>
                <xades:SigPolicyHash>
                  <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>*** SIIN ON KÄESOLEVA DOKUMENDI RÄSIVÄÄRTUS
BASE64 KODEERINGUS ***
</ds:DigestValue>
                </xades:SigPolicyHash>
                <xades:SigPolicyQualifiers>
                  <xades:SigPolicyQualifier>
                    <xades:SPURI>https://www.sk.ee/repository/bdoc-
spec212.pdf</xades:SPURI>
                  </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>application/msword</xades:MimeType>
            </xades:DataObjectFormat>
          </xades:SignedDataObjectProperties>
        </xades:SignedProperties>
   <xades:UnsignedProperties>
    <xades:UnsignedSignatureProperties>
     <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>
```

Lisa 2: BDOC allkirja profiilid

Järgnev joonis illustreerib XAdES elementide kasutamist erinevates BDOC profiilides.



Joonis 1. XAdES elementide kasutamine erinevates BDOC profiilides.