Euroopan unionin virallisen lehden allekirjoituspolitiikka

Versio 4

(1.3.171.4.1.1.4)

Voimassa lokakuun 1 päivästä 2023

Sisällysluettelo

1 Johdanto

Tässä asiakirjassa määritellään Euroopan unionin virallisen lehden allekirjoitukseen, jäljempänä ’EUVL-allekirjoitus’, ja Euroopan unionin virallisen lehden leimaan, jäljempänä ’EUVL-leimaan’, sovellettava allekirjoituspolitiikka. Politiikan avulla todennetaan Euroopan unionin virallisen lehden, jäljempänä ’EUVL’, sähköinen versio Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen (EU) N:o 216/2013[1] mukaisesti.

Allekirjoituspolitiikka muodostuu yhden tai useamman toisiinsa liittyvän sähköisen allekirjoituksen ja/tai leiman luomista, validointia ja uusimista koskevasta sääntökokonaisuudesta. Siinä määritellään sähköisen allekirjoituksen ja/tai leiman luomista, validointia ja pitkäaikaista hallintaa koskevat tekniset ja menettelylliset vaatimukset, joiden avulla pyritään täyttämään tietyt toiminnalliset tarpeet ja määrittämään, milloin allekirjoitus on pätevä. Allekirjoituspolitiikan avulla voidaan tehdä kukin allekirjoitus- tai leimausprosessi läpinäkyväksi kaikkien osapuolten (allekirjoittajat, vastaanottajat ja välittäjät) näkökulmasta siten, että politiikan noudattaminen sähköisissä allekirjoituksissa ja leimoissa lisää luottamusta niiden pätevyyttä ja hyväksyttävyyttä kohtaan.

Allekirjoituspolitiikkaan kuuluvat käsitteet selitetään yksityiskohtaisesti asiakirjassa [ETSI 2015], jossa esitettyihin suuntaviivoihin myös tämän asiakirjan rakenne perustuu. Tässä asiakirjassa käytetyt avainsanat ON / ON TEHTÄVÄ / TEKEE / TEHDÄÄN [”MUST”, ”SHALL”], EI (tule tehdä) [”MUST NOT”, ”SHALL NOT”] ja PAKOLLINEN [”REQUIRED”], OLISI (oltava/tehtävä) [”SHOULD”], EI PITÄISI [”SHOULD NOT”], SUOSITELTAVA [”RECOMMENDED”], VOI/VOIDAAN [”MAY”] ja VAPAAEHTOINEN/VALINNAINEN [”OPTIONAL”] on tulkittava asiakirjassa RFC 2911 [Bradner 1997] kuvatulla tavalla.

EUVL:ää julkaisee Euroopan unionin julkaisutoimisto, jäljempänä ’OP’, EUR-Lex-sivustolla (ks. kohta 1.2.4), joka on ainoa todistusvoimainen EU:n lainsäädännön lähde. EUVL:ää julkaistaan maanantaista perjantaihin, ja tarvittaessa myös viikonloppuisin, kaikilla Euroopan unionin (EU) virallisilla kielillä. *Lyhenteellä ’EUVL’ tarkoitetaan jäljempänä yhteisesti tätä kokonaisuutta.*

1.1 Yleistä

EUVL-allekirjoituspolitiikassa esitetään formaalissa muodossa sähköisen allekirjoituksen ja sähköisen leiman luomiseen, validointiin ja pitkäaikaiseen säilytykseen liittyvien keskeisten vaiheiden toteutuskäytäntö, kun sitä käytetään EU:n julkaisutoimiston julkaisemien EUVL:n numeroiden todentamiseen.
Politiikka koostuu seuraavista osista:

- johdanto, joka käsittää muun muassa allekirjoituspolitiikan nimen tai tunnisteen, tiedot politiikan vahvistajasta ja hallinnoinnista, määritelmät ja lyhenteet
- allekirjoitussovelluskäytäntöjä koskevat lausumat, joissa määritellään sovellukseen liittyvät toimintapoliittiset ja oikeudelliset vaatimukset sekä sovellettavat turvallisuusnäkökohdat

[1] Ks. EUVL L 69, 13.3.2013, s. 1.

- toiminnan määrittelyn parametrit, joissa esitetään yksityiskohtaisesti niiden sähköisten allekirjoitusten ja leimojen tuottamiseen liittyvät prosessit, joilla EU:n julkaisutoimiston julkaisemat EUVL:n numerot todennetaan
- teknisten mekanismien ja standardien toteutusta koskevat vaatimukset ja lausumat sekä liitteet.

1.2 Toiminnan ala

1.2.1 Allekirjoituspolitiikan soveltamisala ja rajat

EUVL-allekirjoituspolitiikka kattaa sellaiset sähköiset allekirjoitukset ja leimat, joita valtuutetut EUVL:n allekirjoittajat luovat Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen mukaisesti kunkin allekirjoitettavan numeron onnistuneen validoinnin yhteydessä.

1.2.2 Sovellusten ala

EUVL-allekirjoituspolitiikan piiriin kuuluvat ainoastaan kohdassa 3.1 kuvatut sähköiset allekirjoitukset ja leimat.

1.2.3 Tapahtumakonteksti

Ei sovelleta.

1.3 Allekirjoituspolitiikan nimi, tunniste ja vaatimustenmukaisuussäännöt

1.3.1 Allekirjoituspolitiikan nimi

EUVL-allekirjoituspolitiikasta käytetään seuraavaa nimeä:

Euroopan unionin virallisen lehden allekirjoituspolitiikka

1.3.2 Allekirjoituspolitiikan tunniste

Koska on olemassa vain yksi Euroopan unionin virallinen lehti ja sen julkaiseminen on tunnettu Euroopan unionin prosessi, mikä tahansa taho pystyy epäsuorasti tunnistamaan EUVL-allekirjoituspolitiikan. Allekirjoituspolitiikan yleinen toimintaprosessi kuvaillaan kohdassa 3.1.1.1.

Politiikan nimenomaista osoittamista varten kuhunkin EUVL-allekirjoitukseen ja -leimaan *VOIDAAN* sisällyttää [ETSI 2022-XAdES]:n kohdassa 5.2.9 esitetyn määritelmän mukainen eksplisiittinen viittaus allekirjoituspolitiikkaan. Jos allekirjoituspolitiikkaan viitataan nimenomaisesti, viittauksessa ON ILMOITETTAVA objektitunniste 1.3.171.4.1.1.4 käyttäen [ETSI 2022-XAdES]:n kohdassa 5.2.9 ja [Mealling 2010]:ssa esitettyjä koodaussääntöjä.

Globaali objektitunniste 1.3.171.4.1.1.4 yksilöi yksiselitteisesti allekirjoituspolitiikan tämän version. Tarkennin 1.3.171.4 on rekisteröity OID-kannaksi *EU:n julkaisutoimiston allekirjoituspolitiikoille ja muille käyttökohteille* (ks. http://www.oid-info.com/get/1.3.171.4). Tarkennin 1.1.4 yksilöi EUVL-allekirjoituspolitiikan tämän version, ja sen ASN.1-merkintä nimineen ON {oj(1) signature-policy(1) version(4)}. Tämä versio korvaa allekirjoituspolitiikan version 1.1.3.

1.3.3 Allekirjoituspolitiikan vaatimustenmukaisuussäännöt

Tämän allekirjoituspolitiikan ei esitetä olevan minkään muun allekirjoituspolitiikan mukainen.

1.3.4 Allekirjoituspolitiikan jakelupisteet

EUVL-allekirjoituspolitiikkaa koskeva asiakirja julkaistaan EUR-Lex-sivustolla. Asiakirja löytyy julkaisutoimiston sivuston (https://eur-lex.europa.eu/) kautta.

1.3.5 Allekirjoituspolitiikan voimassaoloaika

Tämä allekirjoituspolitiikan versio tulee voimaan 1 päivänä tammikuuta 2023.

1.3.6 Allekirjoituspolitiikan soveltamisala

Tätä allekirjoituspolitiikkaa sovelletaan kaikkiin EUVL:n numeroihin, jotka julkaistaan ja allekirjoitetaan sähköisesti Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen voimaantulopäivänä tai sen jälkeen. Tätä allekirjoituspolitiikkaa ei sovelleta Euroopan unionin virallisen lehden täydennysosaan (’S-sarja’, ’Euroopan unionin virallinen lehti S’ tai ’EUVL S’).

HUOM. Tämän politiikan kukin versio on voimassa kussakin versiossa määritellyn ajan. Yhdessä eri versiot kattavat kaikki EUVL:n numerot.

1.4 Allekirjoituspolitiikan asiakirjojen hallinnointi

EUVL-allekirjoituspolitiikan vahvistajana toimii Euroopan unionin julkaisutoimisto hyväksyttyään tämän asiakirjan ja julkaistuaan sen EUR-Lex-sivustolla.

EUVL-allekirjoituspolitiikka ON automaattisesti oikeudellisesti pätevä sellaisena kuin se on julkaistu, ja sitä SOVELLETAAN EUVL-allekirjoitusten ja -leimojen luomiseen, tarkastukseen ja pitkäaikaiseen hallintaan.

EUVL-allekirjoituspolitiikan vahvistaja vastaa

- EUVL-allekirjoituspolitiikan määrittelystä ja hyväksymisestä
- EUVL-allekirjoituspolitiikan tarkistusmenettelyn määrittelystä
- arviointiperusteiden ja -prosessin määrittelystä sen varmistamiseksi, että EUVL-allekirjoituspolitiikka on Euroopan unionin virallisen lehden sähköisestä julkaisemisesta 7 päivänä maaliskuuta 2013 annetun neuvoston asetuksen (EU) N:o 216/2013 sekä Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun asetuksen (EU) N:o 216/2013 muuttamisesta 6 päivänä joulukuuta 2018 annetun neuvoston asetuksen (EU) 2018/2056 mukainen
- arviointiperusteiden ja -prosessin määrittelystä sen varmistamiseksi, että sovellukset, joiden ilmoitetaan noudattavan EUVL-allekirjoituspolitiikkaa, ovat todella niitä koskevien voimassa olevien sääntöjen mukaiset
- EUVL-allekirjoituspolitiikan ja sen tarkistettujen versioiden julkaisemisesta EUR-Lex-sivustolla.

1.4.1 Allekirjoituspolitiikkaa hallinnoiva viranomainen

EUVL-allekirjoituspolitiikkaa hallinnoi Euroopan unionin julkaisutoimisto.

1.4.2 Yhteyshenkilö

Tämän allekirjoituspolitiikan vahvistajaan voidaan ottaa yhteyttä seuraavassa osoitteessa:

Yhteyshenkilö:	The Head of Unit Official Journal and Case Law
Postiosoite:	2, rue Mercier, L-2985 Luxembourg
Puhelinnumero:	(+352) 29291
Faksinumero:	(+352) 292 944 620
Sähköpostiosoite:	OP-JO-AUTHENTIQUE-HELPDESK@publications.europa.eu

1.4.3 Hyväksymismenettelyt

Allekirjoituspolitiikan hyväksyntäviranomainen Euroopan unionin julkaisutoimistossa on Euroopan unionin julkaisutoimiston pääjohtaja.

1.4.4 Allekirjoituspolitiikan versiot

Allekirjoituspolitiikan alkuperäisessä ja muutetussa versiossa *VOIDAAN* ILMOITTAA päivä, jona se viimeistään tulee voimaan. Kun allekirjoituspolitiikan uusi versio julkaistaan, se TULEE voimaan viimeistään jonakin seuraavista kolmesta päivämäärästä:

1. päivänä, jona se viimeistään tulee voimaan, jos tämä päivä on ilmoitettu asianomaisessa versiossa
2. sitä päivää seuraavana päivänä, jota sen EUVL-numeron, jossa allekirjoituspolitiikan versio julkaistaan, EUVL-allekirjoituksen tai -leiman varhaisin aikaleima osoittaa, Luxemburgin paikallisen ajan mukaisesti
3. allekirjoituspolitiikan version julkaisupäivää seuraavana päivänä.

Allekirjoituspolitiikan muutetun version voimassaolo PÄÄTTYY ilman eri toimenpiteitä, kun seuraava muutettu versio tulee voimaan. Sen lisäksi seuraavassa muutetussa versiossa OLISI mainittava versio, jonka se korvaa.

Edellä esitetyillä säännöillä pyritään kehäpäätelmien estämiseksi varmistamaan, että allekirjoituspolitiikan tietyn version allekirjoitukseen ei suoraan tai välillisesti sovelleta allekirjoituspolitiikan samaa versiota. Lisäksi vanhentunut versio on suositeltavaa säilyttää valinnaisella tavalla.

1.5 Määritelmät ja lyhenteet

Tässä asiakirjassa käytetyt määritelmät ja lyhenteet luetellaan taulukossa 1.

Lyhenne	**Määritelmä (FI)**
CA	Varmenneviranomainen
DTBS	Allekirjoitettava data
LTV	Pitkäkestoisuus
OID	Objektitunniste
EUVL	Euroopan unionin virallinen lehti
PIN	Henkilökohtainen tunnusluku
OP	Euroopan unionin julkaisutoimisto
QC	Hyväksytty varmenne
QESig	Hyväksytty sähköinen allekirjoitus
QESeal	Hyväksytty sähköinen leima
QSCD	Hyväksytty allekirjoituksen/leiman luontiväline
SAA	Allekirjoituksen täydentämissovellus
SCA	Allekirjoituksen luomissovellus
SSCD	Turvallinen allekirjoituksen luontiväline
SVA	Allekirjoituksen validointisovellus
TSP	Luottamuspalvelun tarjoaja
QTSP	Hyväksytty luottamuspalvelun tarjoaja
WIPIWIS	Periaate, jonka mukaan asiakirja julkaistaan sellaisena kuin se on allekirjoitettu

Taulukko 1: Määritelmät ja lyhenteet

2 Allekirjoitussovelluskäytäntöjä koskevat lausumat

2.1 Asiaan liittyvät toimintapoliittiset vaatimukset

EUVL:n numeroihin sovelletaan Euroopan unionin virallisen lehden julkaisemisesta annetun neuvoston asetuksen 1 ja 2 artiklaa, joissa säädetään muun muassa siitä, että virallisen lehden sähköisessä versiossa ON Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 mukaisesti määritelty hyväksytty sähköinen allekirjoitus tai asetuksen (EU) N:o 910/2014 mukaisesti määritelty hyväksytty sähköinen leima.

Euroopan komissio antoi 30 päivänä marraskuuta 2009 asiakirjan IMPLEMENTING RULES FOR THE DECISION 2002/47/EC, ECSC, EURATOM ON DOCUMENT MANAGEMENT AND FOR THE DECISION 2004/563/EC, EURATOM ON ELECTRONIC AND DIGITISED DOCUMENTS, jäljempänä ’päätöksen 2002/47/EY ja päätöksen 2004/563/EY täytäntöönpanosäännöt’[2]. EUVL:n numeroiden sähköiseen allekirjoittamiseen ja leimaamiseen sovelletaan näiden täytäntöönpanosääntöjen III.2.1 artiklassa ilmaistua periaatetta, jonka mukaan allekirjoituksen toteuttaminen on merkityksellinen muodollisuus. Tämän lisäksi EUVL:n sähköisessä allekirjoittamisessa on mainitun päätöksen mukaisesti käytettävä [eIDAS]-asetuksen määritelmän mukaista hyväksyttyä sähköistä allekirjoitusta.

PÄÄTÖKSEN 2002/47/EY JA PÄÄTÖKSEN 2004/563/EY[2] TÄYTÄNTÖÖNPANOSÄÄNTÖJEN III.2.3 artiklan mukaan allekirjoittavan viranomaisen suorittama tarkastus on EUVL:n SCA:n vastuulla, kun OP:n virkamiehiä valtuutetaan allekirjoittamaan EUVL:n numeroita sähköisesti tai kun OP oikeushenkilönä valtuutetaan leimaamaan EUVL:n numeroita sähköisesti.

Vaikka sähköisessä muodossa olevilla EUVL:n numeroilla ei voi olla oikeudellisia vaikutuksia, ellei niitä ole allekirjoitettu tai leimattu, EUVL-allekirjoituspolitiikassa edellytetään lisäksi, että EUVL:n SCA TAKAA, että ainoastaan valtuutetut EUVL:n allekirjoittajat voivat kiistää EUVL:n numeroiden aitouden, jotta voidaan tehokkaasti ehkäistä EUVL:n julkaisuprosessiin kohdistuvia hyökkäyksiä.

Koska EUVL:n valtuutetut allekirjoittajat toimivat OP:n puolesta, OP:n pääjohtajan vastuulla on taata (delegoinnin kautta), että EUVL:n allekirjoittamiseen vaadittavat QC:t on hyväksytty asianmukaisesti. Tätä varten EUVL:n allekirjoittamiseen tarvittavien QC:iden valtuutukset

- *MÄÄRITETÄÄN* oikein EUVL:n SCA:n käyttäjäoikeuksien hallinnassa
- *OLISI* rajoitettava (ammatillisiin) organisaatiovarmenteisiin, joilla taataan käyttäjän yhteys OP:hen[3]
- *JULKISTETAAN* julkaisemalla QC:t EUR-Lex-sivustolla Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen 2 artiklan mukaisesti.

2.2 Asiaan liittyvät oikeudelliset vaatimukset

EUVL-allekirjoituspolitiikan kattamaan sähköisten allekirjoitusten ja sähköisten leimojen toteutukseen SOVELLETAAN seuraavia säädöksiä:

- Neuvoston asetus (EU) N:o 216/2013, annettu 7 päivänä maaliskuuta 2013, Euroopan unionin virallisen lehden sähköisestä julkaisemisesta

[2] Ks. SEC(2009) 1643.

[3] Organisaatiotodistus takaa käyttäjän yhteyden tiettyyn organisaatioon. Tämä lisää turvallisuutta, koska todistuksen myöntävä QTSP valvoo sitä, että todistuksen haltijalla on siihen oikeus.

- Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014[4], annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta
- 2009/767/EY: Komission päätös, tehty 16 päivänä lokakuuta 2009, toimenpiteistä sähköisten menettelyjen käytön edistämiseksi keskitettyjä asiointipisteitä käyttäen palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY mukaisesti[5]
- Euroopan parlamentin ja neuvoston asetus (EU) 2016/679[6], annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
- Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY[7], annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi)
- Euroopan parlamentin ja neuvoston direktiivi 2009/136/EY[8], annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta
- 2010/425/EU: Komission päätös, annettu 28 päivänä heinäkuuta 2010, päätöksen 2009/767/EY muuttamisesta jäsenvaltioiden valvomia/akkreditoimia varmennepalvelujen tarjoajia koskevien luotettavien luetteloiden laatimisen, ylläpitämisen ja julkaisun osalta[9]
- 2009/496/EY, Euratom: Euroopan parlamentin, neuvoston, komission, yhteisöjen tuomioistuimen, tilintarkastustuomioistuimen, Euroopan talous- ja sosiaalikomitean ja alueiden komitean päätös, tehty 26 päivänä kesäkuuta 2009, Euroopan unionin julkaisutoimiston organisaatiosta ja toiminnasta[10]
- 2011/130/EU: Komission päätös, annettu 25 päivänä helmikuuta 2011, palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY nojalla toimivaltaisten viranomaisten sähköisesti allekirjoittamien asiakirjojen maiden rajat ylittävää käsittelyä koskevista vähimmäisvaatimuksista[3].

2.3 Tekniset turvallisuusnäkökohdat

EUVL-allekirjoitusten ja -leimojen toteutuksessa käytettäviksi hyväksytyt salausvälineet TÄYTTÄVÄT [eIDAS]-asetuksessa [ETSI 2016]:ssa määritellyt hyväksyttyä sähköistä allekirjoitusta koskevat vaatimukset sekä asianmukaisten uusimpien käytäntöjen asettamat vaatimukset.

[4] Ks. EUVL L 257, 28.8.2014, s. 73.

[5] Ks. EUVL L 274, 20.10.2009, s. 36.

[6] Ks. EUVL L 119, 4.5.2016, s. 1.

[7] Ks. EYVL L 201, 31.7.2002, s. 37.

[8] Ks. EUVL L 337, 18.12.2009, s. 11.

[9] Ks. EUVL L 199, 31.7.2010, s. 30.

[10] Ks. EUVL L 168, 30.6.2009, s. 41.

2.4 Oikeudelliset lausunnot

EUVL:n numeroihin liitetyt sähköiset allekirjoitukset ja leimat generoidaan julkaisutoimiston puolesta Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen mukaisesti.

3 Toiminnan määrittelyn parametrit (business scoping parameters, BSP)

3.1 Lähinnä asianomaiseen sovellukseen/toimintaprosessiin liittyvät BSP-parametrit

3.1.1 BSP a): Allekirjoitusprosessi (järjestys ja ajoitus)

3.1.1.1 Toimintaprosessin yleinen kuvaus

OP julkaisee EUVL:ää maanantaista perjantaihin ja tarvittaessa viikonloppuisin. Julkaistava EUVL voi olla EUVL:n tai säädöskohtaisen EUVL:n numero. Kukin EUVL:n numero on yhdestä tai useammasta asiakirjasta koostuva monikielinen julkaisu. Kukin kieliversio koostuu kaikki asiakirjat yhteen asiakirjaan kokoavasta tekstistä. Säädöskohtaisen EUVL:n numero sisältää yhden ainoan erikseen julkaistavan asiakirjan kaikki kieliversiot. Säädöskohtaisen EUVL:n kukin kieliversio sisältää kyseisen asiakirjan koko tekstin yhteen asiakirjaan koottuna.

EUVL:n ja säädöskohtaisen EUVL:n numerot julkaistaan eri sarjoissa. Sarjan tunnus on EUVL:n numerointijärjestelmän keskeinen osa. Tässä asiakirjassa tarkoitetun soveltamisalan kannalta merkityksellisiä sarjoja on kaksi, L-sarja (lainsäädäntö) ja C-sarja (tiedonannot ja ilmoitukset). Sarjalla voi olla erilaisia alasarjoja tai luokitusjärjestelmiä. Sivuilla http://publications.europa.eu/code/fi/fi-10000.htm esitellään yksityiskohtaisemmin soveltamisalaa ja asiakirjojen rakennetta ja annetaan täydentäviä taustatietoja.

EUVL:ää julkaistaan L- ja C-sarjojen lisäksi myös liittyvien maiden tai uusien jäsenvaltioiden kielisinä, EU:n sekundäärilainsäädäntöä sisältävinä erityispainoksina. Allekirjoituspolitiikkaa sovelletaan myös näihin erityispainoksiin.

Kun EUVL:n tai säädöskohtaisen EUVL:n numero on valmis julkaistavaksi (eli kaikki EUVL:n tai säädöskohtaisen EUVL:n numeron kieliversiot ovat saatavilla PDF/A-tiedostona), prosessi jatkuu joko sähköisellä leimausprosessilla (ks. kohta 3.1.1.2) tai sähköisellä allekirjoitusprosessilla (ks. kohta 3.1.1.3). Sähköisen leimauksen yhteydessä hyväksytty sähköinen leima luodaan automaattisesti OP:lle Euroopan komission yksikkönä myönnetyn hyväksytyn sähköisen leimausvarmenteen avulla. Sähköisen allekirjoituksen yhteydessä hyväksytyn sähköisen allekirjoituksen luo valtuutettu henkilö hyväksytyn sähköisen allekirjoitusvarmenteen avulla.

Sähköinen leimaus on SCA:n oletusarvoisesti valitsema prosessi, eli valmiisiin EUVL:n tai säädöskohtaisen EUVL:n numeroihin sovelletaan automaattista leimausprosessia paitsi jos leimausprosessi ei ole käytettävissä. Siinä tapauksessa käytetään allekirjoitusprosessia.

Koska kunkin numeron allekirjoittamiseen käytetään Manifest-elementillä, jäljempänä ’manifesti’, varustettua erillistä XAdES-allekirjoitusta tai -leimaa (ks. [Bartel 2008], [ETSI 2022-XAdES] ja palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY[11] nojalla toimivaltaisten viranomaisten sähköisesti allekirjoittamien asiakirjojen maiden rajat ylittävää käsittelyä koskevista vähimmäisvaatimuksista 25 päivänä helmikuuta 2011 annettu komission päätös (2011/130/EU)), EUVL:n tai säädöskohtaisen EUVL:n allekirjoitusta tai leimaa tarkastettaessa on validoitava [ETSI 2022-XAdES] -validoinnin yhteydessä XML-allekirjoituksen ytimen (ks. [Bartel 2008]) lisäksi myös manifesti, jotta EUVL:n tai säädöskohtaisen EUVL:n allekirjoitus tai leima voidaan todeta tarkastetuksi.

Seuraavissa alakohdissa kuvataan korkean tason leimaus- ja allekirjoitusprosessit sellaisina kuin ne on toteutettu EUVL:n SCA:ssa, SAA:ssa ja SVA:ssa (ks. [ETSI 2016]).

[11] EUVL L 53, 26.2.2011, s. 66.

3.1.1.2 EUVL:n tai säädöskohtaisen EUVL:n leiman luominen

1. Havaitaan kokonainen leimattava EUVL:n tai säädöskohtaisen EUVL:n numero.
2. SCA tarkastaa alustavasti toimitetut tiedostot:
    a. Se tarkistaa, onko EUVL:n tai säädöskohtaisen EUVL:n numeron eri kieliversioiden kokojen välillä epäjohdonmukaisuutta ja sijoittuvatko ne konfiguroitavissa olevan koon vaihteluväliin.
    b. Se tarkistaa, oliko kaikki toimitetut kieliversiot ilmoitettu julkaistavaksi.
3. Jos tarkastus epäonnistuu, leimausprosessi keskeytyy. Leimausprosessin jatkaminen edellyttää OP:n valtuutetun henkilöstön manuaalisesti suorittamia toimia.
4. Kun SCA on onnistuneesti suorittanut validoinnin, luodaan manifesti, jossa viitataan koko numeron kuhunkin erikieliseen versioon. Lisäksi kukin kieliversio vastaa manifestissa yhtä EU:n virallista kieltä ja esitetään PDF/A-asiakirjana, jota käsitellään laskettaessa sanomatiivistettä binäärisenä oktettivirtana.
5. SCA suorittaa todennuksen Euroopan komission keskitetyssä sähköisessä allekirjoitusportaalissa ja siirtää luodun manifestin automaattista leimausta varten.
6. Sähköinen allekirjoitusportaali leimaa toimitetun manifestin akkreditoidun eurooppalaisen QTSP:n myöntämän hyväksytyn leimausvarmenteen avulla (ks. [eIDAS]-asetus). Tähän leimausvarmenteeseen liittyvä yksityinen avain tallennetaan QSCD:lle, joka on yhdistetty sähköiseen allekirjoitusportaaliin.
7. Tällä tavalla luotu XAdES-allekirjoitus (ks. [ETSI 2022-XAdES]) lähetetään takaisin SCA:lle, joka tarkastaa muun muassa algoritmien validiteetin sekä sen, että kyseisen leiman leimausvarmenne on valtuutettu ja sen omistaa oikeushenkilö, joka on todennettu valtuutetuksi allekirjoittajaksi.
8. Kun tarkastus on suoritettu, sähköinen leima täydennetään liittämällä siihen akkreditoidun QTSP:n antama aikaleima (ks. [eIDAS]-asetus).
9. Edellisen käsittelyvaiheen aikana täydennetty sähköinen leima siirretään julkaistavaksi EUR-Lex-sivustolla. Samalla SCA säilyttää leiman identtisen kopion.
10. Kun edellisessä käsittelyvaiheessa luodun leiman pakollinen 24 tunnin odotusaika on päättynyt, leima täydennetään pysyvässä muodossa akkreditoidun eurooppalaisen QTSP:n luotettavan aikaleiman avulla, jotta allekirjoitus on voimassa pitkän aikaa (ks. [eIDAS]-asetus).
11. Edellisessä käsittelyvaiheessa täydennetty leima siirretään julkaistavaksi EUR-Lex-sivustolla. Sillä korvataan vaiheessa 9 luotu leima, jota ei ole vielä täydennetty pysyvässä muodossa.
12. Sen lisäksi, että EUVL:n tai säädöskohtaisen EUVL:n numeroon sisältyvät asiakirjat julkaistaan EUR-Lex-sivustolla, niiden identtiset kopiot ja niitä koskeva pysyvä leima siirretään OP:n hallinnoimaan EU:n toimielinten virallisten asiakirjojen sähköiseen arkistointijärjestelmään pitkäaikaista säilytystä varten. Tässä allekirjoituspolitiikassa EI puututa pitkäaikaisen säilytyksen täytäntöönpanoon liittyviin näkökohtiin.

3.1.1.3 EUVL:n tai säädöskohtaisen EUVL:n allekirjoituksen luominen

1. Havaitaan kokonainen allekirjoitettava EUVL:n tai säädöskohtaisen EUVL:n numero.
2. Luodaan manifesti, jossa viitataan koko numeron kuhunkin erikieliseen versioon. Lisäksi kukin kieliversio vastaa manifestissa yhtä EU:n virallista kieltä ja esitetään

PDF/A-asiakirjana, jota käsitellään laskettaessa sanomatiivistettä binäärisenä oktettivirtana.

SCA hallinnoi ja lukitsee yksinomaisesti kokonaisia EUVL:n numeroita manifestin generoinnin aikana varmistaakseen, että tiiviste lasketaan yhdenmukaisesti, mikä on koko prosessin kannalta kriittistä.

3. Kun SCA on onnistuneesti suorittanut todennuksen, valtuutettu allekirjoittaja voi valita allekirjoitettavaksi koko numeron edellyttäen, että edellisen vaiheen aikana on luotu tarvittava manifesti.
4. Kun allekirjoitettava numero on valittu, valtuutettu allekirjoittaja aloittaa sitä koskevan allekirjoitusprosessin:
    a. WIPIWIS-periaatteen noudattamiseksi valtuutetun allekirjoittajan on ennen numeron allekirjoittamista tarkastettava vähintään kolme eri kieliversiota käyttäen standardinmukaista PDF/A-lukijaa. Jos EUVL:n tai säädöskohtaisen EUVL:n painos koostuu yhdestä tai kahdesta kieliversiosta, valtuutetun allekirjoittajan on tarkastettava ainoa tai kumpikin kieliversio.

        SCA sallii allekirjoittajan tarkastaa minkä tahansa allekirjoitettavassa numerossa olevan kieliversion. Allekirjoittaja VOI näin ollen halutessaan tarkastaa koko allekirjoitettavan sisällön.

    b. Valtuutettu allekirjoittaja voi tarkoituksellisesti joko hylätä numeron, jolloin allekirjoitusprosessi keskeytyy, tai allekirjoittaa sen valitsemalla Sign-vaihtoehdon.
    c. Kun valitaan Sign-vaihtoehto:
        i. SCA luo allekirjoituspyynnön Euroopan komission keskitetylle sähköiselle allekirjoitusportaalille, toimittaa manifestin allekirjoitettavaksi ja ohjaa valtuutetun allekirjoittajan edelleen portaaliin.
        ii. Valtuutettu allekirjoittaja todentautuu sähköiseen allekirjoitusportaaliin ja saa manifestin allekirjoitettavaksi WIPIWIS-periaatteiden mukaisesti.
        iii. Sähköinen allekirjoitusportaali luo yhteyden valtuutetun allekirjoittajan työasemalle asennettuun välitysohjelmistoon ja noutaa allekirjoittajan hyväksytyn allekirjoitusvarmenteen, jonka on myöntänyt akkreditoitu eurooppalainen QTSP (ks. [eIDAS]-asetus). Varmenne esitetään valtuutetulle allekirjoittajalle, ja tämän jälkeen allekirjoittaja päättää allekirjoitusprosessin kirjoittamalla QSCD:tä suojaavan PIN-tunnuksen, jolla hän valtuuttaa QSCD:n luomaan allekirjoituksen valittua allekirjoitusvarmennetta vastaavan yksityisen avaimen avulla.
    d. Välitysohjelmisto lähettää luodun allekirjoitusarvon sähköiseen allekirjoitusportaaliin, joka puolestaan luo vastaavan XAdES-allekirjoituksen (ks. [ETSI 2022-XAdES]).
5. XAdES-allekirjoitus lähetetään takaisin SCA:lle, joka tarkastaa – sähköisen allekirjoitusportaalin kautta – muun muassa algoritmien validiteetin sekä sen, että kyseisen allekirjoituksen allekirjoitusvarmenne on valtuutettu ja sen omistaa henkilö, joka on todennettu valtuutetuksi allekirjoittajaksi.
6. Kun tarkastus on suoritettu, allekirjoitus täydennetään – sähköisen allekirjoitusportaalin kautta – liittämällä siihen akkreditoidun QTSP:n antama aikaleima (vrt. [eIDAS]).

7. Edellisen käsittelyvaiheen aikana uusittu allekirjoitus siirretään julkaistavaksi EUR-Lex-sivustolla. Samalla SCA säilyttää allekirjoituksen identtisen kopion.
8. Kun edellisessä käsittelyvaiheessa luodun allekirjoituksen pakollinen 24 tunnin odotusaika on päättynyt, allekirjoitus täydennetään pysyvässä muodossa akkreditoidun eurooppalaisen QTSP:n luotettavan aikaleiman avulla, jotta allekirjoitus on voimassa pitkän aikaa (ks. [eIDAS]-asetus).
9. Edellisessä käsittelyvaiheessa uusittu allekirjoitus siirretään julkaistavaksi EUR-Lex-sivustolla. Sillä korvataan vaiheessa 7 luotu allekirjoitus, jota ei ole vielä täydennetty pysyvässä muodossa.
10. Sen lisäksi, että EUVL:n tai säädöskohtaisen EUVL:n numeroon sisältyvät asiakirjat julkaistaan EUR-Lex-sivustolla, niiden identtiset kopiot ja niitä koskeva pysyvä allekirjoitus siirretään OP:n hallinnoimaan EU:n toimielinten virallisten asiakirjojen sähköiseen arkistointijärjestelmään pitkäaikaista säilytystä varten. Tässä allekirjoituspolitiikassa EI puututa pitkäaikaisen säilytyksen täytäntöönpanoon liittyviin näkökohtiin.

3.1.1.4 Hätätilanteet

Jos EUVL:n tai säädöskohtaisen EUVL:n leimaa tai allekirjoitusta ei voida luoda kohdassa 3.1.1.2 tai 3.1.1.3 kuvatulla tavalla, koska EUVL:n SCA ei ole saatavilla odottamattomasta ja poikkeuksellisesta syystä, julkaisutoimisto laittaa QESeal:n tai QESig:n jokaiseen EUVL:n tai säädöskohtaisen EUVL:n numeron eri kieliversion sisältävään PDF/A-asiakirjaan. Kaikki leimatut/allekirjoitetut PDF/A-asiakirjat siirretään julkaistavaksi EUR-Lex-sivustolla.

3.1.2 BSP b): Allekirjoitettava data

- EUVL:n tai säädöskohtaisen EUVL:n allekirjoitukset ja leimat perustuvat XML-manifestiin (ks. [Bartel 2008] ja [ETSI 2022-XAdES]), joka kattaa kerralla kaikki tiettyyn EUVL:n tai säädöskohtaisen EUVL:n numeroon kuuluvat, PDF/A-muodossa saatavilla olevat kieliversiot samalla allekirjoituksella. Sen on täytettävä seuraavat edellytykset: Kullakin EUVL:n tai säädöskohtaisen EUVL:n numeroon loogisesti liittyvällä kieliversiolla *ON OLTAVA* oma tiivistearvo.
- Kaikki EUVL:n tai säädöskohtaisen EUVL:n numeroon loogisesti liittyvät kieliversiot *ON ESITETTÄVÄ* allekirjoittajalle tarkastettavaksi allekirjoituksen luomisen aikana. Näin allekirjoittaja voi WIPIWIS-periaatteen noudattamiseksi tarkastaa allekirjoituksen sisällön kohdassa 3.1.1.3 kuvatulla tavalla.
- Asianmukainen visualisointi *ON VARMISTETTAVA* käyttämällä PDF/A-yhteensopivaa lukijaa.
- Allekirjoittajalle ESITETÄÄN allekirjoitusprosessin aikana ainoastaan allekirjoitettavaan numeroon kuuluvat kieliversiot.
- Kaikkien EUVL:n tai säädöskohtaisen EUVL:n numeroon loogisesti liittyvien kieliversioiden tekniset ominaisuudet *ON TARKISTETTAVA* leiman ja allekirjoituksen luomisen yhteydessä johdonmukaisuuden varmistamiseksi.

Edellä kohdassa 3.1.1.4 kuvatuissa hätätilanteissa sovelletaan seuraavia vaatimuksia:

- Kullakin EUVL:n tai säädöskohtaiseen EUVL:n numeron kieliversiolla *ON OLTAVA* oma QESeal tai QESig.
- Allekirjoittajan *ON TARKASTETTAVA* kaikki EUVL:n tai säädöskohtaisen EUVL:n numeroon loogisesti liittyvät kieliversiot allekirjoituksen luomisen aikana. Näin allekirjoittaja voi WIPIWIS-periaatteen mukaisesti tarkastaa allekirjoituksen sisällön.

- Asianmukainen visualisointi *ON VARMISTETTAVA* käyttämällä PDF/A-yhteensopivaa lukijaa.

3.1.3 BSP c): Allekirjoitetun datan sekä allekirjoituksen/allekirjoitusten ja leiman/leimojen välinen suhde

EUVL:n tai säädöskohtaisen EUVL:n allekirjoitus tai leima kattaa kaikki tiettyyn EUVL:n tai säädöskohtaisen EUVL:n numeroon sisältyvät, PDF/A-muodossa olevat kieliversiot.

EUVL:n tai säädöskohtaisen EUVL:n allekirjoituksen tai leiman luomisen yhteydessä allekirjoitettavan/leimattavan asiakirjan digitaalinen sisältö tiivistetään binääriseksi oktettijonoksi vahvimmalla [ETSI 2022-Crypto]:n kohdan 7.3 mukaisella tuetulla tiivistealgoritmilla.

Yksittäisten asiakirjojen tiivistearvot liitetään alkuperäisten tiedostonimien URI-osoitteiden kanssa XML-manifestiksi. Muita muutoksia ei tehdä (ks. [Bartel 2008]).

Manifesti ja allekirjoitettavat attribuutit allekirjoitetaan tai leimataan käyttäen XAdESia (ks. [ETSI 2022-XAdES]) 25 päivänä helmikuuta 2013 annetussa komission päätöksessä 2011/130/EU määritellyn profiilin osalta.

Kun kyseessä on edellä kohdassa 3.1.1.4 kuvattu hätätilanne, kukin EUVL:n tai säädöskohtaisen EUVL:n numeron eri kieliversion sisältävä PDF/A-asiakirja allekirjoitetaan tai leimataan käyttäen PAdESia (ks. [ETSI 2016-PAdES] [eIDAS]).

3.1.4 BSP d): Kohdeyhteisö

Kohdeyhteisö on mikä tahansa luottava osapuoli, jonka on voitava varmistaa EUVL:n todistusvoimaisuus, sekä kaikki osapuolet, jotka vastaavat SCA:n ja SAA:n käyttöönotosta. SCA:ta ja SAA:ta käytetään sähköisten allekirjoitusten ja sähköisten leimojen luomiseen ja niiden täydentämiseen EUVL:n tai säädöskohtaisen EUVL:n numeroa varten.

3.1.5 BSP e): Allekirjoituksen validointia ja täydentämistä koskeva vastuunjako

3.1.5.1 EUVL:n tai säädöskohtaisen EUVL:n allekirjoituksen ja leiman tarkastus

Mikä tahansa luottava osapuoli, esimerkiksi kuka tahansa unionin kansalainen, voi ladata EUR-Lex-sivustolla julkaistun EUVL:n tai säädöskohtaisen EUVL:n sekä sitä koskevan erillisen XAdES-allekirjoituksen tai leiman (ks. [ETSI 2022-XAdES]) tarkastusta varten.

Koska allekirjoituksen ja leiman luomisessa käytetään yhteentoimivaa eurooppalaista allekirjoitusstandardia ja akkreditoidun eurooppalaisen QTSP:n palveluja (ks.[eIDAS]-asetus), tarkastamiseen voidaan käyttää mitä tahansa kolmannen osapuolen tarkastuspalvelua, joka noudattaa tätä standardia, edellyttäen että manifesti voidaan validoida EUVL-allekirjoituspolitiikan mukaisesti.

Kun kyseessä on edellä kohdassa 3.1.1.4 kuvattu hätätilanne, kukin EUVL:n tai säädöskohtaisen EUVL:n numeron eri kieliversion sisältävä PDF/A-asiakirja allekirjoitetaan tai leimataan käyttäen PAdESia (ks. [ETSI 2016-PAdES]). Tarkastamiseen voidaan käyttää mitä tahansa kolmannen osapuolen tarkastuspalvelua, joka noudattaa tätä standardia.

3.1.5.1.1 Palvelinpuolen tarkastus

Allekirjoituksen ja leiman tarkastamisen helpottamiseksi julkaisutoimisto VOI tarjota ilmaiseksi EUVL:n palvelinpuolen SVA:ta. Tarkastaminen etenee tällöin seuraavasti:

1. Tarkastuksen pyytäjä tallentaa palvelimelle tarkastettavan PDF/A-tiedoston sekä siihen liittyvän allekirjoitus- tai leimaustiedoston SVA:n tallennustoiminnolla.
2. SVA laskee tallennetun PDF/A-tiedoston tiivisteen ja tarkastaa, että tiiviste sisältyy tallennetun allekirjoituksen manifestiosaan.

3. Kun tiiviste on onnistuneesti tarkastettu, suoritetaan tallennetun tarkastettavan allekirjoituksen tai leiman tavanomainen XAdES-tarkastus edellyttäen, että allekirjoitusvarmenteessa on ilmoitettu valtuutettu EUVL:n allekirjoittaja allekirjoituksen aikaleiman osoittamaksi ajaksi. SVA tarkastaa myös, että allekirjoittajalla oli allekirjoitusvaltuudet allekirjoituksen aikaleiman osoittamana allekirjoituksen luontiajankohtana.
4. Tarkastus on onnistunut, kun kaikki edellä kuvatut vaiheet on läpäisty. Muussa tapauksessa tarkastus on epäonnistunut. Tarkastuksen pyytäjä saa kuitenkin myös tässä tapauksessa selkeän raportin tarkastusprosessin kulusta.

3.1.5.1.2 Asiakaspuolen tarkastus

Allekirjoituksen ja leiman tarkastamisen helpottamiseksi julkaisutoimisto VOI tarjota ilmaiseksi EUVL:n asiakaspuolen SVA:ta. Tarkastaminen etenee tällöin seuraavasti:

1. Tarkastuksen pyytäjä käynnistää lataamansa SVA:n, ajoympäristö tarkastaa automaattisesti sen koodin allekirjoituksen, ja tarkastuksen onnistuttua käyttäjä valtuuttaa sovelluksen ajon.
2. Tarkastuksen pyytäjä valitsee tarkastettavan PDF/A-tiedoston tiettynä kieliversiona sekä siihen liittyvän tarkastettavan allekirjoitus- tai leimaustiedoston koneellaan käyttäen SVA:n tiedostonvalintaikkunaa.
3. SVA laskee valitun asiakirjan tiivisteen ja tarkastaa, sisältyykö tiiviste valitun tarkastettavan allekirjoituksen tai leiman manifestiin.
4. Kun tiiviste on tarkastettu onnistuneesti, suoritetaan valitun tarkastettavan allekirjoituksen tai leiman tavanomainen XAdES-tarkastus.
5. Tarkastusprosessi on onnistunut, kun kaikki edellä kuvatut vaiheet on läpäisty ja kun allekirjoitus- tai leimausvarmenteessa on ilmoitettu valtuutettu EUVL:n allekirjoittaja allekirjoituksen aikaleiman osoittamaksi ajaksi.

   Valtuutetun allekirjoittajan tiedot VOIVAT OLLA SVA:n hallussa (oletus)määritysten perusteella. SVA:n tuloksesta käy kuitenkin ilmi myös allekirjoitus- tai leimavarmenteen tiiviste, jota todentaja voi erikseen verrata allekirjoituksen tai leiman luomisvaiheeseen liittyviin, laillista allekirjoittajaa koskeviin julkisiin tietoihin, jotka myös sisältyvät SVA:n tulokseen.

3.2 BSP-parametrit, joihin vaikuttavat pääasiassa asianomaiseen sovellukseen/toimintaprosessiin liittyvät oikeudelliset ja sääntelyä koskevat säännökset

3.2.1 BSP f): Allekirjoitusten oikeudelliset lajit

EUVL:n tai säädöskohtaisen EUVL:n sähköiset allekirjoitukset ja leimat OVAT QESig:ejä ja QESeal:eja [eIDAS]-asetuksessa tarkoitetussa mielessä.

Tätä edellytetään erityisesti neuvoston asetuksessa Euroopan unionin virallisen lehden sähköisestä julkaisemisesta (ks. kohta 2.2).

Voidakseen käyttää allekirjoitusjärjestelmää jokaisen allekirjoittajan on hankittava QC.

Vaaditun QESig:n ja QESeal:n eri elementit TÄYTTÄVÄT seuraavat laatuvaatimukset:

- Allekirjoitus- ja leimausväline: [eIDAS]-asetuksen liitteen II mukaiset QSCD:t
- Varmenteen myöntäminen: [eIDAS]:n liitteen I mukainen QC

- Varmenteen myöntäjän riippumaton varmistus: QC:n myöntäjän on oltava jossakin [eIDAS]:n soveltamisalaan kuuluvassa valtiossa akkreditoitu valvottu tai akkreditoitu QCSP-varmennepalvelu.
- allekirjoituksen salausjärjestelmä: käytetään ainoastaan [ETSI 2022-Crypto]:n kohdassa 7.3 lueteltuja allekirjoitusjärjestelmiä;
- LTV-ratkaisut: EUVL:n tai säädöskohtaisen EUVL:n XAdES-allekirjoitusten (ks. [ETSI 2022-XAdES]) muoto TÄYDENNETÄÄN LTA-muotoon, joka kattaa arkisto- tai muiden aikaleimojen uusimisen (ulkopuolisia turvallisia arkistointimekanismeja VOIDAAN pitää vaihtoehtona arkistoaikaleiman uusimiselle edellyttäen, että ne ovat laadultaan vastaavia tai parempia).
- Allekirjoituksen luomissovellus: EUVL:n SCA:n laadun ON TÄYTETTÄVÄ Euroopan komission toimintapolitiikkojen mukaiset laatuvaatimukset sekä Euroopan unionin virallisesta lehdestä annetussa neuvoston asetuksessa asetetut vaatimukset.

3.2.2 BSP g): Allekirjoittajan tekemä sitoumus

EUVL:n tai säädöskohtaisen EUVL:n numeroihin liitetyt sähköiset allekirjoitukset ja leimat GENEROIDAAN julkaisutoimiston puolesta Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen mukaisesti.

Valtuutetun EUVL:n allekirjoittajan tekemä sitoumus ilmaisee sen, että allekirjoitettu data edustaa todistusvoimaista, soveltamisalaan liittyviä sääntöjä noudattaen asianmukaisesti validoitua EUVL:n tai säädöskohtaisen EUVL:n numeroa (ks. kohta 3.1.1), jonka OP on julkaissut EU:n lainsäädännön aitona lähteenä Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen mukaisesti.

EUVL:n allekirjoitukseen EI SISÄLLY mitään nimenomaista viittausta sitoumustyyppiin (ks. [ETSI 2022-XAdES]), kohta 5.2.3).

3.2.3 BSP h): Aikaa koskevan näytön varmuustaso

EUVL:n tai säädöskohtaisen EUVL:n allekirjoitukseen tai -leimaan ON LISÄTTÄVÄ kohdassa 3.1.1.2 tai 3.1.1.3 kuvatulla tavalla luotu aikaleima EUVL:n tai säädöskohtaisen EUVL:n numeron julkaisupäivänä (Luxemburgin paikallisen ajan mukaisesti), jotta voidaan varmentaa, että allekirjoitusta tai leimaa ei ole luotu julkaisupäivän jälkeen. Näin varmistetaan, että julkaisupäivänä valtuutetut allekirjoittajat ovat valtuutettuja myös kyseisen allekirjoituksen osalta.

EUVL:n SCA VARMISTAA, että kaikki generoidut XAdES-B-T-allekirjoitukset täyttävät tämän edellytyksen.

XAdES-B-T-allekirjoitusten aikaleiman luomiseen KÄYTETÄÄN ainoastaan hyväksyttyjä aikaleimoja.

PAdES-allekirjoitukset VOIDAAN luoda ilman allekirjoituksen aikaleimaa kohdassa 3.1.1.4 kuvatuissa hätätilanteissa.

Jos kohdassa 3.1.1.4 kuvatussa hätätilanteessa PAdES-allekirjoitukseen liitetään aikaleima, sen OLISI oltava hyväksytty aikaleima, joka lisätään EUVL:n tai säädöskohtaisen EUVL:n numeron julkaisupäivänä (Luxemburgin paikallisen ajan mukaisesti), jotta voidaan varmentaa, että allekirjoitusta tai leimaa ei ole luotu julkaisupäivän jälkeen.

HUOM. Hätätilanteessa allekirjoitukseen liitettävän aikaleiman ei siis tarvitse olla hyväksytty aikaleima.

Kaikkien muiden aikaleimojen, kuten mahdollisten arkistointi- ja sisältöaikaleimojen, OLISI kuitenkin oltava hyväksyttyjä aikaleimoja.

3.2.4 BSP i): Allekirjoittamiseen liittyvät muodollisuudet

EUVL:n SCA:n allekirjoittajan käyttöliittymä toteutetaan siten, että allekirjoitus- ja leimausympäristö on oikeudellisesti mahdollisimman pätevä. Käyttöliittymän on

- sisällettävä asianmukaista neuvontaa ja informaatiota sovelluksen allekirjoitus- ja leimausprosessista
- varmistettava allekirjoituksen ja leiman luomis- ja tarkastustietojen käytön, allekirjoituksen ja leiman luontivälineiden, allekirjoitettavan datan sekä allekirjoituksen (tai allekirjoitus- tai leimaustapahtuman) odotetun laajuuden ja tarkoituksen keskinäinen johdonmukaisuus
- mahdollistettava ja osoitettava selkeä allekirjoittamista koskeva tahdonilmaisu, josta ilmenee myös käyttäjän aikomus sitoutua allekirjoitukseen tai leimaan
- mahdollistettava ja esitettävä tietoinen suostumus.

EUVL:n SVA MAHDOLLISTAA luottaville osapuolille (mukaan lukien allekirjoittaja) tarvittavat menettelyt sähköisten allekirjoitus-, leimaus- ja tarkastustietojen tarkastamista ja arkistointia varten.

3.2.5 BSP j): Pitkäaikaisuus ja pysyvyys

Allekirjoitetut EUVL:n tai säädöskohtaisen EUVL:n numerot ja niiden allekirjoitukset ON SÄILYTETTÄVÄ toistaiseksi. EUVL:n tai säädöskohtaisen EUVL:n allekirjoitusten voimassaolon jatkuminen ON VARMISTETTAVA täksi ajaksi (ks. Euroopan unionin virallisen lehden sähköisestä julkaisemisesta annetun neuvoston asetuksen 2 artikla).

3.2.6 BSP (k): Arkistointi

Ei sovelleta.

3.3 Lähinnä allekirjoitusten luomiseen/täydentämiseen/validointiin osallistuviin toimijoihin liittyvät BSP-parametrit

3.3.1 BSP l): Allekirjoittajien henkilöllisyys (ja roolit/attribuutit)

3.3.1.1 Allekirjoittajaa ja tunnistamista koskeva sääntöehdotus

EUVL:n tai säädöskohtaisen EUVL:n allekirjoittajat OVAT valtuutettuja allekirjoittajia, ja erityisesti he OVAT julkaisutoimiston virkamiehiä, joilla on tarvittava asiantuntemus EUVL:n tai säädöskohtaisen EUVL:n numeroiden validoimiseksi tämän asiakirjan soveltamisalaan liittyvien sääntöjen mukaisesti (ks. kohta 3.1.1.3). EUVL:n tai säädöskohtaisen EUVL:n leimojen osalta valtuutettu allekirjoittaja ON itse julkaisutoimisto Euroopan komission yksikkönä.

Valtuutetut allekirjoittajat OVAT tietoisia vastuustaan, ja he TOIMIVAT vilpittömässä mielessä todentaessaan EU:n oikeuteen kuuluvia säädöstekstejä.

Näiden allekirjoittajina toimivien luonnollisten henkilöiden ja heidän allekirjoitustensa tarkastustietojen välinen yhteys OSOITETAAN QC:ssä [eIDAS]-asetuksessa tarkoitetulla tavalla vahvistamalla heidän henkilöllisyytensä ja sidonnaisuutensa OP:hen.

EUVL:n allekirjoittajan valtuutuksen MYÖNTÄÄ OP:n pääjohtaja (mahdollisesti delegoimalla).

3.3.1.2 Allekirjoittajan roolit ja attribuutit

Allekirjoittajan ja OP:n välistä sidonnaisuutta lukuun ottamatta mitkään muut roolit, tehtävät tai pätevyysattribuutit EIVÄT EDELLYTÄ varmentamista allekirjoittajan QC:ssä.

EUVL:n SCA HUOLEHTII asianmukaisesta käyttöoikeuksien hallinnasta ja allekirjoittajan valtuuttamisesta ennen EUVLT-allekirjoitustoimintojen käyttöoikeuksien myöntämistä allekirjoittajille.

Käyttöoikeuksien hallinnassa ja allekirjoittajan valtuuttamisessa KÄYTETÄÄN SCA:ssa toteutettavaa vahvaa todentamismenetelmää sekä käyttöoikeuksia, jotka on rekisteröity SCA:n käyttöoikeustietokantaan valtuutettuja allekirjoittajia koskevien julkisen avaimen varmenteiden kanssa.

Luottavat osapuolet *VOIVAT* käyttää EUVL:n allekirjoittajien julkaistuja varmenteita heidän laillisten oikeuksiensa tarkastamiseksi.

3.3.1.3 Asiaan liittyvä toimivaltuustodistus

Ei muita määräyksiä kohdan 3.3.1.2 lisäksi.

3.3.2 BSP m): Allekirjoittajan todentamisen edellyttämä varmuustaso

Allekirjoittajan todentamisen edellyttämä varmuustaso taataan käyttämällä hyväksyttyä varmennetta ja sen mukaista allekirjoituksen luontivälinettä, jonka ON oltava [eIDAS]-asetuksessa vahvistetun määritelmän mukainen hyväksytty allekirjoituksen/leiman luontiväline.

3.4 Muut BSP-parametrit

3.4.1 BSP o): Muut allekirjoitukseen tai leimaan liitettävät tiedot

3.4.1.1 Valtuutetut EUVL:n allekirjoittajat ja aikaleimaajat

Allekirjoittajien valtuutuksen tarkastaminen on EUVLT:n luotettavuuden keskeinen edellytys.

Valtuutus TEHDÄÄN näkyväksi julkaisemalla kaikkien valtuutettujen allekirjoittajien sähköiset varmenteet tiivisteiden heksadesimaalisarja SCA:sta/SVA:sta erillisellä luotettavana pidetyllä tavalla.

Valtuutettujen EUVL:n allekirjoittajien julkaisemisen yhteydessä ILMOITETAAN, että allekirjoitusvarmenteiden valvontastatus taataan meneillään olevan EUVL tai säädöskohtaisen EUVL:n allekirjoituskauden ajaksi.

Valtuutettujen EUVL:n allekirjoittajien ja aikaleimaajien nimiä EI tule julkaista EUVL:ssä, koska tämä johtaisi erityisesti pitkäaikaista validointia koskeviin kehäpäätelmäongelmiin.

Kun valtuutetut allekirjoittajat tai aikaleimaajat vaihtuvat ajan mittaan, tiedot edellisestä allekirjoittajajoukosta JULKAISTAAN vanhoina luotettavuutta koskevina tietoina. Tämä on tarpeen, jotta voidaan tarkastaa näiden allekirjoittajien allekirjoittamat EUVL:n tai säädöskohtaisen EUVL:n numerot.

Valtuutettuja allekirjoittajia julkistettaessa TÄSMENNETÄÄN ajanjakso, jonka osalta luettelossa olevilla allekirjoittajilla oli tai on valtuutus tämän allekirjoituspolitiikan version aikarajoitusten puitteissa.

3.4.1.2 Sähköisen allekirjoituksen ja leiman attribuutteja, soveltamisalaa ja tarkoitusta koskevat säännöt

Allekirjoituksen ja leiman luomisprosesseissa HYÖDYNNETÄÄN asianmukaisesti seuraavia edellytyksiä noudattaen allekirjoitettuja attribuutteja, erityisesti sellaisia sähköistä allekirjoitusta/leimaa tukevia tietoja, joita, samoin kuin DTBS:ää, allekirjoitus/leima koskee:

- KÄYTETÄÄN allekirjoitusvarmenteen tunnistetta. Tämän varmenteen tunniste tai viittaus tähän tunnisteeseen sisältää allekirjoituksen tai leiman tarkastustiedot, jotka vastaavat allekirjoittajan sähköistä allekirjoitusta tai leimaa luodessaan käyttämiä luomistietoja.

- Viittausta allekirjoituspolitiikkaan VOIDAAN käyttää (ks. kohta 1.2.2).
- KÄYTETÄÄN ilmoitettua allekirjoittamisajankohtaa. Se on ajankohta, jona allekirjoittaja ilmoittaa luoneensa allekirjoituksen tai leiman.

  Tämä ajankohta vastaa allekirjoittajan työaseman järjestelmäaikaa. Se EI ole luotettu aika.

  EUVL:n SCA:n omistaja (OP:n pääjohtajan delegoimana) HUOLEHTII, että kaikkien allekirjoittajien työasemien järjestelmäajat täsmäävät.

Tähän päästään käyttämällä NTP-protokollaa ja sopivaa aikalähdettä (ks. [Mills 2010]).

- Viittausta sitoumustyyppiin EI KÄYTETÄ.
- Muita allekirjoitettuja attribuutteja VOIDAAN käyttää.

Allekirjoitusattribuutteja käytettäessä ON NOUDATETTAVA [ETSI 2010]:ä ja 25 päivänä helmikuuta 2013 annettua komission päätöstä 2011/130/EU.

3.4.2 BSP p): Salausjärjestelmät

Katso kohta 3.2.1.

4 Teknisten mekanismien ja standardien täytäntöönpanoa koskevat vaatimukset ja lausumat

4.1 Luotettua aikaleimaa koskevat säännöt

XAdES-LTA-allekirjoitus (ks. [ETSI 2022-XAdES]) edellyttää useita aikaleimoja, jotka HANKITAAN jäsenvaltiossa tai ETA-maassa akkreditoidulta hyväksytyltä aikaleimapalvelulta.

EUVL:n SCA:n omistaja HUOLEHTII (OP:n pääjohtajan delegoimana), että SCA on määritetty käyttämään sopivia salausalgoritmeja.

4.2 Pitkäaikaista voimassaoloa koskevat vaatimukset

EUVL:n tai säädöskohtaisen EUVL:n allekirjoitusten voimassaolon jatkuminen oletettuna säilytysaikana varmistetaan XAdES-B-LTA-muodon toteutuksella (ks. [ETSI 2022-XAdES]) ja lisäämällä sen jälkeen allekirjoitukseen uusi hyväksytty arkistointiaikaleima sen voimassaolon jatkamiseksi tarvittaessa tai käyttämällä sopivaa arkistoratkaisua, joka takaa allekirjoituksen voimassaolon.

4.3 Muita toiminnallisia ja oikeudellisia näkökohtia

Koska EUVL julkaistaan tiistaista perjantaihin ja tarvittaessa viikonloppuisin, EUVL:n SCA:n omistajan ON HUOLEHDITTAVA (OP:n pääjohtajan delegoimana) siitä, että SCA on jatkuvasti toimintakunnossa.

Tätä varten OLISI tehtävä asianmukaiset palvelutasosopimukset.

Vaikka EUVL:n tai säädöskohtaisen EUVL:n allekirjoitukset ja leimat voi tarkastaa millä tahansa EUVL-allekirjoituspolitiikassa vahvistettuja standardeja ja sääntöjä, joiden mukaan myös manifesti on validoitava, noudattavalla SVA:lla, OP VOI asettaa SVA:n yleisön saataville EUR-Lex-sivustolla antaakseen luottaville osapuolille, erityisesti Euroopan kansalaisille, mahdollisuuden tarkastaa EUVL:n tai säädöskohtaisen EUVL:n allekirjoitukset joutumatta turvautumaan kolmannen osapuolen palveluun.

Vaihtoehtoisesti OP VOI asettaa SVA:n käyttöön yleisesti verkosta ladattavana ohjelmana, joka toimii tarvittaessa itsenäisesti käyttäjän koneella. Tämä edellyttää ainoastaan sitä, että tarkastuksen pyytäjä luottaa ohjelmaan tukeutuessaan sen tuottamiin tuloksiin.

5 Liite

[Bartel 2008]	Bartel M., Boyer J., Fox B., LaMacchia B., Simon E. *XML Signature Syntax and Processing (Second Edition)* W3C Recommendation, 2008
[Bradner 1997]	Bradner S. *Key words for use in RFCs to indicate requirement levels* RFC 2119, Network Working Group, 1997
[Mealling 2010]	Mealling M. *A URN Namespace of Object Identifiers* RFC 3061, Network Working Group, 2001
[Mills 2010]	Mills D., Delaware U., Martin J., ISC Ed., Burbank J., Kasch W. *Network Time Protocol Version 4: Protocol and Algorithms Specification* RFC 5905, IETF, 2010
[eIDAS]-asetus	*Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta* EUVL L 257
[ETSI 2015]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents* TS 119 172-1, v1.1.1, ETSI, 2015
[ETSI 2016]	ETSI-ESI *Electronic Signatures and Infrastructures (ESI);* *Policy and security requirements for applications for signature creation and signature validation* TS 119 101, v1.1.1, ETSI, 2016
[ETSI 2016-PAdES]	ETSI-ESI PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures ETSI EN 319 142-1 V1.1.1 (2016-04)
[ETSI 2022-XAdES]	ETSI-ESI XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures ETSI EN 319 132-1 V1.2.1 (2022-02)
[ETSI 2022-Crypto]	ETSI-ESI Cryptographic Suites ETSI TS 119 312 V1.4.2 (2022-02)