Euroopan unionin
virallinen lehti

FI
L-sarja

2026/1731

22.7.2026

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2026/1731,

annettu 15 päivänä heinäkuuta 2026,

täytäntöönpanoasetusten (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 ja (EU) 2024/2982 muuttamisesta sovellettavien standardien ja eritelmien osalta

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta 23 päivänä heinäkuuta 2014 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([1]) ja erityisesti sen 5 a artiklan 23 kohdan,

sekä katsoo seuraavaa:

(1) Jotta eurooppalaisten digitaalisen identiteetin lompakoiden kehittämisessä voidaan varmistaa mahdollisimman suuri yhdenmukaistaminen jäsenvaltioiden kesken, lompakoita koskevat tekniset eritelmät perustuvat työhön, jota on tehty komission suosituksen (EU) 2021/946 ([2]) perusteella, ja erityisesti siihen kuuluvaan arkkitehtuuriin ja viitekehykseen. Koska arkkitehtuuri ja viitekehys ovat kehittyneet merkittävästi komission täytäntöönpanoasetusten (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) ja (EU) 2024/2982 ([6]) antamisen jälkeen, kyseisiä täytäntöönpanoasetuksia olisi nyt muutettava niiden saattamiseksi uusien standardien, eritelmien ja menettelyjen mukaisiksi.

Asetuksen (EU) N:o 910/2014 tavoitteiden mukaisesti näiden erityisvaatimusten täyttämiseksi on valittu joukko standardeja. Näiden standardien olisi heijastettava vakiintuneita käytäntöjä, ja niiden olisi oltava laajasti tunnustettuja kyseessä olevilla aloilla. Koska esimerkiksi W3C VCDM -muotoa käytetään todistusten viitemuotona erityisesti koulutusalalla, eurooppalaisten digitaalisen identiteetin lompakkojen olisi tuettava tätä muotoa myös sitten, kun W3C VCDM -muodon uudet profiilit ovat saatavilla. Näitä standardeja olisi tarvittaessa mukautettava tai täydennettävä, jotta varmistetaan eurooppalaisten digitaalisen identiteetin lompakoiden turvallisuus ja luotettavuus, samalla kun helpotetaan rajat ylittävää yhteentoimivuutta ja sisämarkkinoiden tehokasta toimintaa.

(2) Kaikessa lompakon käytössä, joka edellyttää lompakon käyttäjän kasvokuvan esittämistä, lompakkoratkaisujen on tuettava valikoivan luovuttamisen toiminnallisuutta ja luovuttamisen on oltava täysin käyttäjän päätösvallassa. Jotta voitaisiin suojella kykyä päättää luovuttamisesta ja kasvokuva voitaisiin suojata tahattoman tai luvattoman luovuttamispyynnön varalta, eurooppalaisten digitaalisen identiteetin lompakoiden arkkitehtuurin suunnitteluun olisi sisällyttävä varoitusmekanismeja ja kaikkien kasvokuvan käyttöön liittyvien tapahtumien kirjaaminen lokitietoihin. Sen varmistamiseksi, että lompakon käyttäjä on tietoinen biometristen tietojen jakamisesta, varoituksissa olisi mainittava, että pyyntöön liittyy biometristen tietojen jakamista, ja erityisesti olisi edellytettävä,

([1]) EUVL L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Komission suositus (EU) 2021/946, annettu 3 päivänä kesäkuuta 2021, unionin yhteisestä välineistöstä eurooppalaista digitaalisen identiteetin kehystä koskevaa koordinoitua lähestymistapaa varten (EUVL L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Komission täytäntöönpanoasetus (EU) 2024/2977, annettu 28 päivänä marraskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisille digitaalisen identiteetin lompakoille myönnettävien henkilön tunnistetietojen ja sähköisten attribuuttitodistusten osalta (EUVL L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([4]) Komission täytäntöönpanoasetus (EU) 2024/2979, annettu 28 päivänä marraskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisten digitaalisen identiteetin lompakoiden eheyden ja ydintoimintojen osalta (EUVL L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([5]) Komission täytäntöönpanoasetus (EU) 2024/2980, annettu 28 päivänä marraskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisten digitaalisen identiteetin lompakoiden ekosysteemistä komissiolle tehtävien ilmoitusten osalta (EUVL L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

([6]) Komission täytäntöönpanoasetus (EU) 2024/2982, annettu 28 päivänä marraskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisen digitaalisen identiteetin kehyksen tukemien protokollien ja rajapintojen osalta (EUVL L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

että käyttäjä vahvistaa luovuttamisen. Jos luottava osapuoli käsittelee kasvokuvaa luonnollisen henkilön yksiselitteistä tunnistamista tai kyseisen henkilön ilmoitetun henkilöllisyyden vahvistamista varten, sovelletaan Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 ([7]) 6 ja 9 artiklaa sekä kaikkia muita mainitun asetuksen vaatimuksia, mukaan lukien sitä, että luottavien osapuolten suorittama kasvokuvan käsittely olisi rajoitettava siihen, mikä on tarpeen aiottua käyttötarkoitusta varten. Aiottu käyttötarkoitus olisi ilmoitettava lompakon käyttäjälle yhdessä luovutuspyynnön kanssa selkeällä ja ymmärrettävällä kielellä. Jotta biometristen tietojen arkaluonteisuus voitaisiin ottaa asianmukaisesti huomioon, lompakon käyttäjän olisi nimenomaisesti ja erityisesti vahvistettava kasvokuvan luovuttaminen. Vastaamattomuutta tai valmiiksi rastitettuja ruutuja ei tulisi pitää lompakon käyttäjän vahvistuksena. Lompakon käyttäjän nimenomaisen vahvistuksen olisi oltava tekninen suojatoimi, eikä se saisi itsessään tarjota oikeusperustaa käsittelylle. Asetuksen (EU) 2016/679 9 artiklan 4 kohdan mukaisesti jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön lisäehtoja, mukaan lukien rajoituksia, jotka koskevat geneettisten tietojen, biometristen tietojen tai terveystietojen käsittelyä.

(3) Jotta jäsenvaltioilla olisi riittävästi aikaa mukauttaa kansallisia menettelyjään, lompakon käyttäjän kasvokuva voi olla osa luonnollisen henkilön pakollisia tunnistetietoja vasta 11 päivästä elokuuta 2028. Jos nämä kuvat hankitaan olemassa olevista henkilöllisyystodistuksista, kuten henkilökorteista tai passeista, sovelletaan neuvoston asetuksissa (EU) 2025/1208 ([8]) tai (EY) N:o 2252/2004 ([9]) säädettyjä asiaankuuluvia vaatimuksia.

(4) Asetuksen (EU) N:o 910/2014 mukaan lompakoissa on voitava esittää EU:n digitaalisen identiteetin lompakon luotettavuusmerkki tarkastettavissa olevana, yksinkertaisena ja tunnistettavana osoituksena siitä, että lompakko on tarjottu asetuksen mukaisesti. Tällaisen luotettavuusmerkin käyttö tukee sisämarkkinoiden tehokasta toimintaa, takaa reilun kilpailun ja suojaa kuluttajien etuja. Tällaisen luotettavuusmerkin käytön mahdollistamiseksi olisi vahvistettava luotettavuusmerkin visuaaliset ja tekniset ominaisuudet.

(5) Kuten asetuksen (EU) N:o 910/2014 12 b artiklassa säädetään, portinvartijoiden on mahdollistettava eurooppalaisten digitaalisen identiteetin lompakoiden tarjoajien ja ilmoitettujen sähköisen tunnistamisen menetelmien myöntäjien tehokas yhteentoimivuus samojen käyttöjärjestelmä-, laitteisto- tai ohjelmisto-ominaisuuksien kanssa ja pääsy niihin yhteentoimivuuden varmistamiseksi. Tällainen tehokas yhteentoimivuus ja pääsy on sallittava maksutta riippumatta siitä, ovatko kyseiset laitteisto- tai ohjelmisto-ominaisuudet osa käyttöjärjestelmää, ovatko ne kyseisen portinvartijan saatavilla tai käyttääkö portinvartija niitä tarjotessaan tällaisia palveluja. Koska kaikkien lompakkoratkaisujen olisi tuettava yhteisiä protokollia ja rajapintoja käytettävyyden, tietoturvan ja yhteentoimivuuden varmistamiseksi kaikissa jäsenvaltioissa, portinvartijoiden olisi mahdollistettava käyttöjärjestelmä-, laitteisto- tai ohjelmisto-ominaisuudet, jotka ovat tarpeen tämän asetuksen liitteessä XII vahvistettujen protokollien ja rajapintojen toteuttamiseksi. Tässä yhteydessä portinvartijoiden olisi suosittava verkossa tapahtuvissa laitteiden välisissä tietovirroissa sekä kahden laitteen fyysisen läheisyyden tarkistamisen että näiden laitteiden välisen tiedonsiirron osalta CTAP-protokollan (Client To Authenticator Protocol) eritelmän version 2.3 ([10]) mahdollistamaa paikallista viestintäkanavaa CTAP:n hybriditunnelipalvelujen käytön sijaan.

(6) Jotta jäsenvaltioilla, lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajilla ja lompakon tarjoajilla olisi riittävästi aikaa mahdollistaa se, että lompakkoyksiköt voivat todentaa ja validoida lompakkoon luottavan osapuolen rekisteröintivarmenteet, tätä vaatimusta olisi sovellettava vasta 11 päivästä elokuuta 2028 alkaen.

(7) Kaikkiin tämän asetuksen mukaisiin henkilötietojen käsittelytoimiin sovelletaan asetusta (EU) 2016/679 ja tarvittaessa Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY ([11]).

([7]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Neuvoston asetus (EU) 2025/1208, annettu 12 päivänä kesäkuuta 2025, unionin kansalaisten henkilökorttien sekä oikeuttaan vapaaseen liikkuvuuteen käyttäville unionin kansalaisille ja heidän perheenjäsenilleen myönnettävien oleskeluasiakirjojen turvallisuuden lisäämisestä (EUVL L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Neuvoston asetus (EY) N:o 2252/2004, annettu 13 päivänä joulukuuta 2004, jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista (EUVL L 385, 29.12.2004, s. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Fido Alliancen ehdottama standardi, Client to Authenticator Protocol (CTAP), 26. helmikuuta 2026.

([11]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([12]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 17 päivänä huhtikuuta 2026 ([13]).

(9) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) N:o 910/2014 48 artiklalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Täytäntöönpanoasetuksen (EU) 2024/2977 muuttaminen

Muutetaan täytäntöönpanoasetus (EU) 2024/2977 seuraavasti:

1) Lisätään 3 a artikla seuraavasti:

"*3 a artikla*

Kasvokuvan suojaaminen

1) Asetuksen (EU) 2016/679 mukaisten tietovaatimusten lisäksi lompakon tarjoajien on varmistettava, että niiden tarjoamat lompakkoratkaisut, jos lompakkoon luottavat osapuolet pyytävät kasvokuvan luovuttamista, antavat lompakon käyttäjille varoituksia, joissa ilmoitetaan, että pyyntöön liittyy biometristen tietojen jakamista ja että se edellyttää vahvistusta kasvokuvan valikoivaa luovuttamista varten.

2) Jotta kasvokuva voidaan luovuttaa valikoivasti lompakkoon luottavalle osapuolelle, lompakon tarjoajien on varmistettava, että lompakkoratkaisut edellyttävät, että lompakon käyttäjä vahvistaa nimenomaisesti ja erityisesti kasvokuvan esittämisen.

3) Lompakkoon luottavat osapuolet eivät saa säilyttää kasvokuvaa, paitsi jos sen käsittely on tarpeen tunnistamista ja todentamista varten unionin tietosuojalainsäädännön mukaisesti tai jos siitä säädetään unionin tai kansallisessa lainsäädännössä. Kasvokuvaa ei saa siirtää kolmansille maille tai kansainvälisille järjestöille, ellei sitä sallitaan unionin tietosuojalainsäädännössä."

2) Korvataan 4 artiklan 1 kohta seuraavasti:

"1. Lompakkoyksiköille myönnettävien sähköisten attribuuttitodistusten on oltava vähintään yhden täytäntöönpanoasetuksen (EU) 2024/2979 liitteessä II esitetyn standardin mukaisia."

3) Korvataan 5 artiklan 4 kohdan b alakohta seuraavasti:

"b) kun sen lompakkoyksikön lompakkoyksikkötodistus, jolle henkilön tunnistetiedot on myönnetty, on peruutettu;"

4) Korvataan liite tämän asetuksen liitteessä I olevalla tekstillä.

([12]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | European Data Protection Supervisor.

2 artikla

Täytäntöönpanoasetuksen (EU) 2024/2979 muuttaminen

Muutetaan täytäntöönpanoasetus (EU) 2024/2979 seuraavasti:

1) Kumotaan 3 artiklan 2 kohta.

2) Korvataan 5 artiklan 1 kohdan a alakohta seuraavasti:

”a) suorittavat sellaisiin kriittisiin resursseihin liittyviä lompakon salaustoimintoja, jotka on tallennettu lompakon suojattuun salauslaitteeseen mutta joita ei tarvita lompakon käyttäjän todentamiseen, ainoastaan tapauksissa, joissa kyseiset sovellukset ovat onnistuneesti todentaneet lompakon käyttäjät;”

3) Lisätään 5 a artikla seuraavasti:

”*5 a artikla*

Salausmekanismit

Sovellettaessa 4 artiklan 2 kohtaa lompakon tarjoajien on käytettävä ainoastaan liitteessä I a tarkoitettuja salausmekanismeja.”

4) Muutetaan 6 artikla seuraavasti:

a) Korvataan 1 kohta seuraavasti:

”1. Lompakon tarjoajien on myönnettävä lompakkoyksikkötodistuksia kullekin lompakkoyksikölle. Lompakon tarjoajien on allekirjoitettava tai leimattava lompakkoyksikkötodistukset siten, että allekirjoitukset tai leimat voidaan validoida täytäntöönpanoasetuksen (EU) 2024/2980 liitteessä II olevan 2 jakson 1 kohdan h alakohdan mukaisesti luetellulla varmenteella.”

b) Korvataan 2 kohta seuraavasti:

”2. Lompakon tarjoajien on varmistettava, että 1 kohdassa tarkoitetut lompakkoyksikkötodistukset ovat liitteessä I b esitettyjen teknisten eritelmien mukaisia.”

c) Korvataan 3 kohdan b alakohta seuraavasti:

”b) tarjottava lompakon käyttäjille turvallisia tunnistamis- ja todentamismekanismeja, jotka ovat lompakkoyksiköistä riippumattomia;”

5) Korvataan 9 artiklan 2 kohdan b alakohta seuraavasti:

”b) asianomaisen lompakkoon luottavan osapuolen nimi, yhteystiedot ja yksilöllinen tunniste sekä jäsenvaltio, johon lompakkoon luottava osapuoli on sijoittautunut;”.

6) Korvataan 10 artiklan 1 kohta seuraavasti:

”1. Lompakon tarjoajien on varmistettava, että niiden tarjoamat lompakkoyksiköt voivat käsitellä sähköisiä attribuuttitodistuksia, jotka on myönnetty liitteessä III vahvistettuihin yhteisiin sisäänrakennettuihin tietojen luovuttamiskäytäntöihin sovellettavien teknisten eritelmien mukaisesti.”

7) Muutetaan 12 artikla seuraavasti:

a) Korvataan 2 kohdan c alakohta seuraavasti:

”c) allekirjoitusten tai leimojen luominen vähintään liitteessä IV tarkoitetussa pakollisessa allekirjoitus- tai leimamuodossa;”

b) Korvataan 3 kohta seuraavasti:

”3. Allekirjoituksen luontisovellukset voivat olla joko lompakon ilmentymiin integroituja tai niiden ulkopuolisia.”

c) Lisätään kohta seuraavasti:

”4. Lompakkoyksiköiden käyttämien allekirjoituksen luontisovellusten on tuettava vähintään liitteessä IV tarkoitettua sovellusrajapintaa.”

8) Kumotaan 14 artiklan 1 kohta.

9) Lisätään 14 a artikla seuraavasti:

"*14 a artikla*

EU:n digitaalisen identiteetin lompakon luotettavuusmerkki

1) Lompakon tarjoajien on varmistettava, että lompakkoyksiköt esittävät EU:n digitaalisen identiteetin lompakon luotettavuusmerkin. EU:n digitaalisen identiteetin lompakon luotettavuusmerkin on oltava liitteissä VI ja VII esitetyssä muodossa.

2) Lompakon tarjoajien on varmistettava, että lompakkoyksiköt antavat lompakon käyttäjille mahdollisuuden saada tiedot, joiden avulla he voivat tarkistaa lompakkoratkaisun sertifiointitilan. Tätä varten lompakon tarjoajien on varmistettava, että lompakkoratkaisun rekisteröinnin jälkeen asianomaiset lompakkoyksiköt sisältävät Euroopan komission tällaista tarkistamista varten tarjoamat URL-osoitteet. Lompakon tarjoajien on varmistettava, että niiden lompakkoyksiköillä on pääsy EU:n digitaalisen identiteetin lompakon luotettavuusmerkkiä koskeviin tietoihin, jotka ovat liitteessä VIII esitettyjen teknisten eritelmien mukaiset.

3) EU:n digitaalisen identiteetin lompakon luotettavuusmerkin viitevärit ovat Pantone nro 661 ja 116 tai sininen (100 % syaani + 67 % magenta + 0 % keltainen + 40 % musta) ja keltainen (0 % syaani + 20 % magenta + 100 % keltainen + 0 % musta), kun käytetään neliväripainatusta; RGB-värejä käytettäessä viitevärit ovat sininen (0 punainen + 51 vihreä + 153 sininen) ja keltainen (255 punainen + 204 vihreä + 0 sininen).

4) EU:n digitaalisen identiteetin lompakon luotettavuusmerkki voidaan esittää mustavalkoisena liitteen VII mukaisesti ainoastaan silloin, jos värien käyttö ei ole käytännössä mahdollista.

5) Jos EU:n digitaalisen identiteetin lompakon luotettavuusmerkki esitetään tummalla pohjalla, se voidaan esittää negatiivina käyttäen samaa pohjaväriä. Jos EU:n digitaalisen identiteetin lompakon luotettavuusmerkki esitetään värillisenä värillisellä pohjalla, joka vaikeuttaa sen havaitsemista, EU:n digitaalisen identiteetin lompakon luotettavuusmerkin ympärillä voidaan käyttää ääriviivoja, jotta se erottuu paremmin pohjaväreistä.

6) EU:n digitaalisen identiteetin lompakon luotettavuusmerkin koon on oltava vähintään 64 × 85 pikseliä resoluutiolla 150 dpi.

7) Lompakon tarjoajien on varmistettava, että EU:n digitaalisen identiteetin lompakon luotettavuusmerkkiä käytetään tavalla, joka mahdollistaa sen lompakkoyksikön, johon EU:n digitaalisen identiteetin lompakon luotettavuusmerkki liittyy, selkeän ilmaisemisen. EU:n digitaalisen identiteetin lompakon luotettavuusmerkkiin voidaan liittää graafisia elementtejä tai tekstielementtejä, joista käy selvästi ilmi lompakkoyksikkö, jota varten merkkiä käytetään, sillä edellytyksellä, että ne eivät vaikuta sen tunnistettavuuteen EU:n digitaalisen identiteetin lompakon luotettavuusmerkkinä taikka yhdistämiseen asetuksen (EU) N:o 910/2014 5 d artiklassa tarkoitettuun sertifioitujen eurooppalaisten digitaalisen identiteetin lompakoiden luetteloon.

8) Kun lompakon tarjoajat ovat peruuttaneet lompakkoyksikkötodistuksen, niiden on varmistettava, että asianomainen lompakkoyksikkö ei enää esitä EU:n digitaalisen identiteetin lompakon luotettavuusmerkkiä."

10) Lisätään liitteet I a ja I b tämän asetuksen liitteiden II ja III mukaisesti.

11) Korvataan liite II tämän asetuksen liitteellä IV.

12) Korvataan liite III tämän asetuksen liitteellä V.

13) Muutetaan liite IV tämän asetuksen liitteen VI mukaisesti.

14) Kumotaan liite V.

15) Lisätään tämän asetuksen liitteessä VII oleva teksti liitteeksi VI.

16) Lisätään tämän asetuksen liitteessä VIII oleva teksti liitteeksi VII.

17) Lisätään tämän asetuksen liitteessä IX oleva teksti liitteeksi VIII.

3 artikla

Täytäntöönpanoasetuksen (EU) 2024/2980 muuttaminen

Muutetaan täytäntöönpanoasetus (EU) 2024/2980 seuraavasti:

1) Korvataan 5 artiklan 2 kohta seuraavasti:

”2. Komissio laatii, ylläpitää ja julkaisee tarvittaessa luettelon, johon kootaan liitteessä II olevassa 2, 3, 4 ja 5 jaksossa tarkoitetut jäsenvaltioiden ilmoittamat tiedot lompakon tarjoajista, henkilön tunnistetietojen tarjoajista, lompakkoon luottavan osapuolen pääsyvarmenteiden tarjoajista ja lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajista.”

2) Muutetaan täytäntöönpanoasetuksen (EU) 2024/2980 liite II tämän asetuksen liitteen X mukaisesti.

4 artikla

Täytäntöönpanoasetuksen (EU) 2024/2982 muuttaminen

Muutetaan täytäntöönpanoasetus (EU) 2024/2982 seuraavasti:

1) Korvataan 1 artiklan 2 kohta seuraavasti:

”2) henkilön tunnistetietojen ja sähköisten attribuuttitodistusten attribuuttien esittäminen lompakkoon luottaville osapuolille;”

2) Muutetaan 3 artikla seuraavasti:

a) Korvataan 1 kohta seuraavasti:

”1) todentavat ja validoivat lompakkoon luottavan osapuolen pääsyvarmenteet, kun lompakkoyksiköt ovat vuorovaikutuksessa lompakkoon luottavien osapuolten kanssa, siirtämättä näiden prosessien suorittamista käyttöjärjestelmän selaimen tai muun välityssovelluksen tehtäväksi;”

b) Kumotaan 2 kohta.

c) Korvataan 3 kohta seuraavasti:

”3) todentavat ja validoivat pyynnöt, jotka on tehty lompakkoon luottavan osapuolen pääsyvarmenteita käyttäen;”

d) Korvataan 4 kohta seuraavasti:

”4) todentavat ja validoivat lompakkoon luottavan osapuolen rekisteröintivarmenteet;”

e) Korvataan 5 kohta seuraavasti:

”5) näyttävät lompakon käyttäjille lompakkoon luottavan osapuolen pääsyvarmenteisiin sisältyvät tiedot;”

f) Kumotaan 8 kohta.

g) Korvataan 9 kohta seuraavasti:

”9) eivät esitä mitään pyydettyjä attribuutteja lompakkoon luottaville osapuolille ennen kuin seuraavat vaiheet on suoritettu:

a) sen varmistaminen, että sisäänrakennettuja tietojen luovuttamiskäytäntöjä on käsitelty lompakkoyksikössä täytäntöönpanoasetuksen (EU) 2024/2979 10 artiklan mukaisesti;

b) sen varmistaminen, että lompakon käyttäjät ovat hyväksyneet esittämisen osittain tai kokonaan;”

3) Korvataan 4 artiklan 1 kohta seuraavasti:

”1. Lompakon tarjoajien on varmistettava, että lompakkoratkaisut tukevat liitteessä I esitettyjä protokollia ja rajapintoja, jotka mahdollistavat henkilön tunnistetietojen ja sähköisten attribuuttitodistusten myöntämisen lompakkoyksiköille.”

4) Muutetaan 5 artikla seuraavasti:

   a) Korvataan 1 ja 2 kohta seuraavasti:

      ”1. Lompakon tarjoajien on varmistettava, että lompakkoratkaisut tukevat protokollia ja rajapintoja, jotka mahdollistavat attribuuttien esittämisen lompakkoon luottaville osapuolille etäyhteyden välityksellä ja tarvittaessa lähiyhteyden avulla liitteessä II esitettyjen teknisten eritelmien mukaisesti.

      2. Lompakon tarjoajien on varmistettava, että lompakkoyksiköt vastaavat käyttäjien pyynnöstä 3 artiklassa tarkoitettuihin lompakkoon luottavien osapuolten onnistuneesti todennettuihin ja validoituihin pyyntöihin liitteessä II esitettyjen teknisten eritelmien mukaisesti.”

   b) Kumotaan 5 kohta.

5) Korvataan 8 artikla seuraavasti:

   ”*8 artikla*

   Voimaantulo

   Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

   Sen 3 artiklan 4 kohtaa sovelletaan 11 päivästä elokuuta 2028.

   Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.”.

6) Kumotaan liite.

7) Lisätään tämän asetuksen liitteessä XI oleva teksti liitteeksi I.

8) Lisätään tämän asetuksen liitteessä XII oleva teksti liitteeksi II.

5 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 15 päivänä heinäkuuta 2026.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE I

”LIITE

3 artiklan 3 kohdassa tarkoitetut henkilön tunnistetietoja koskevat tekniset eritelmät

1) 1 jakso: Luonnollisen henkilön tunnistetiedot

Taulukko 1

Luonnollisen henkilön pakolliset tunnistetiedot valikoivaa luovuttamista varten

Tunniste	Määritelmä
`family_name`	Sen käyttäjän nykyinen sukunimi (sukunimet), johon henkilön tunnistetiedot liittyvät
`given_name`	Sen käyttäjän nykyinen etunimi (etunimet), mukaan lukien toinen nimi (toiset nimet), johon henkilön tunnistetiedot liittyvät
`birth_date`	Päivä, kuukausi ja vuosi, jona käyttäjä, johon henkilön tunnistetiedot liittyvät, on syntynyt
`birth_place`	Maa ISO 3166-1 -standardin mukaisena alpha-2-maakoodina tai osavaltio, provinssi, hallintopiiri tai alue taikka kunta, kaupunki tai kylä, jossa käyttäjä, johon henkilön tunnistetiedot liittyvät, on syntynyt
`nationality`	Yksi tai useampi ISO 3166-1 -standardin mukainen alpha-2-maakoodi, joka edustaa sen käyttäjän kansalaisuutta, johon henkilön tunnistetiedot liittyvät
`portrait`	Tarvittaessa lukuun ottamatta tapauksia, joissa käyttäjä nimenomaisesti päättää olla sisällyttämättä kasvokuvaa, ISO/IEC 39794-5 -standardin, tai aiempaa yhteensopivuutta varten ISO/IEC 19794-5 -standardin, kohdissa 8.2, 8.3 ja 8.4 vahvistettujen kokokasvokuvia koskevien laatuvaatimusten mukainen kasvokuva käyttäjästä, johon henkilön tunnistetiedot liittyvät, kun kasvokuva esitetään koodattuna kuvatietona ilman ISO/IEC 19794-5 -standardin kohdassa 5 määriteltyjä otsikoita tai jaksoja, lukuun ottamatta itse kuvatietoja (JPEG); sovelletaan 11 päivästä elokuuta 2028.

— Jäsenvaltiot voivat säätää, että käyttäjällä on mahdollisuus kieltäytyä kasvokuvan sisällyttämisestä henkilön tunnistetietoihin.

— Jäsenvaltioiden on varmistettava, että valikoivaa luovuttamista sovelletaan jokaiseen tunnisteeseen, myös kasvokuvaan.

— Jos luonnollisen henkilön syntymäaika ei ole tiedossa, jäsenvaltioiden on valittava sopivat arvot, jotka ovat tässä liitteessä olevassa 4.1 tai 4.2 kohdassa (tapauksen mukaan) esitettyjen eritelmien mukaiset.

— Jos luonnollisen henkilön kansalaisuus ei ole tiedossa, jäsenvaltioiden on käytettävä arvoa ’QU’.

— Jos luonnollisella henkilöllä ei ole kansalaisuutta, jäsenvaltioiden on käytettävä arvoa ’QS’.

— Jos käyttäjä päättää olla sisällyttämättä kasvokuvaa, jäsenvaltioiden on asetettava arvo tyhjäksi.

Taulukko 2

Luonnollisen henkilön valinnaiset tunnistetiedot valikoivaa luovuttamista varten

Tunniste	Määritelmä
resident_address	Sen paikan täydellinen osoite, jossa käyttäjä, johon henkilön tunnistetiedot liittyvät, asuu tällä hetkellä tai jossa häneen voidaan olla yhteydessä (katuosoite, talon numero, postitoimipaikka jne.)
resident_country	Maa, jossa käyttäjä, johon henkilön tunnistetiedot liittyvät, asuu tällä hetkellä, ISO 3166-1 -standardin mukaisena alpha-2-maakoodina
resident_state	Osavaltio, provinssi, hallintopiiri tai alue, jossa käyttäjä, johon henkilön tunnistetiedot liittyvät, asuu tällä hetkellä
resident_city	Kunta, kaupunki tai kylä, jossa käyttäjä, johon henkilön tunnistetiedot liittyvät, asuu tällä hetkellä
resident_postal_code	Sen paikan postinumero, jossa käyttäjä, johon henkilön tunnistetiedot liittyvät, asuu tällä hetkellä
resident_street	Sen kadun nimi, jolla käyttäjä, johon henkilön tunnistetiedot liittyvät, asuu tällä hetkellä, mukaan lukien talon numero ja sen mahdolliset etu- tai jälkiliitteet
personal_administrative_-number	Sille käyttäjälle, johon henkilön tunnistetiedot liittyvät, annettu arvo, joka on yksilöllinen kaikkien henkilön tunnistetietojen tarjoajan myöntämien henkilökohtaisten hallinnollisten numeroiden joukossa. Jos jäsenvaltiot päättävät käyttää tätä attribuuttia, niiden on kuvattava sähköisen tunnistamisen järjestelmissään, joiden mukaisesti henkilön tunnistetiedot myönnetään, toimintaperiaatteet, joita ne soveltavat tämän attribuutin arvoihin, mukaan lukien tarvittaessa kyseisen arvon käsittelyä koskevat erityisehdot.
family_name_birth	Sen käyttäjän sukunimi (sukunimet) syntymähetkellä, johon henkilön tunnistetiedot liittyvät.
given_name_birth	Sen käyttäjän etunimi (etunimet), mukaan lukien toinen nimi (toiset nimet), syntymähetkellä, johon henkilön tunnistetiedot liittyvät
sex	Arvon on oltava yksi seuraavista: 0 = ei tiedossa 1 = mies 2 = nainen 3 = muu 4 = intersukupuolinen 5 = monisukupuolinen 6 = avoin 9 = ei sovelleta Arvoihin 0, 1, 2 ja 9 sovelletaan standardia ISO/IEC 5218.
email_address	Sen käyttäjän sähköpostiosoite, johon henkilön tunnistetiedot liittyvät [RFC 5322:n ([1]) mukaisesti].

Tunniste	Määritelmä
`mobile_phone_number`	Sen käyttäjän matkapuhelinnumero, johon henkilön tunnistetiedot liittyvät, alkaen ulkomaantunnuksesta '+' ja maatunnuksesta, joita seuraavat ainoastaan numerot

([1]) Resnick, P., toim., "Internet Message Format", RFC 5322, lokakuu 2008.

2) 2 jakso: Oikeushenkilön tunnistetiedot

Taulukko 3

Oikeushenkilön pakolliset tunnistetiedot

Tunniste
Nykyinen virallinen nimi
Yksilöllinen tunniste, jonka lähettävä jäsenvaltio on luonut teknisten eritelmien mukaisesti rajat ylittävää tunnistamista varten ja joka on mahdollisimman pitkäkestoinen

— Jos tunnistetta ei tunneta henkilöstä tai sitä ei voida muutoin myöntää osana henkilön tunnistetietoja, jäsenvaltioiden on käytettävä sen sijaan tilanteeseen soveltuvaa attribuuttiarvoa.

Taulukko 4

Oikeushenkilön valinnaiset tunnistetiedot

Tunniste
Nykyinen osoite
Arvonlisäverotunniste
Verorekisterinumero
Euroopan parlamentin ja neuvoston direktiivissä (EU) 2017/1132 ([1]) tarkoitettu eurooppalainen yksilöivä tunniste
Komission täytäntöönpanoasetuksessa (EU) 2022/1860 ([2]) tarkoitettu oikeushenkilötunnus (LEI)
Komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013 ([3]) tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero)
Neuvoston asetuksen (EU) N:o 389/2012 ([4]) 2 artiklan 12 alakohdassa tarkoitettu valmisteveronumero

([1]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2017/1132, annettu 14 päivänä kesäkuuta 2017, tietyistä yhtiöoikeuden osa-alueista(kodifikaatio) (EUVL L 169, 30.6.2017, s. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Komission täytäntöönpanoasetus (EU) 2022/1860, annettu 10 päivänä kesäkuuta 2022, teknisistä täytäntöönpanostandardeista Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 soveltamiseksi ilmoitettavia tietoja koskevien vaatimusten ja muotojen, ilmoitusten antamistiheyden sekä ilmoittamista koskevien menetelmien ja järjestelyjen osalta (EUVL L 262, 7.10.2022, s. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Komission täytäntöönpanoasetus (EU) N:o 1352/2013, annettu 4 päivänä joulukuuta 2013, teollis- ja tekijänoikeuksien tullivalvonnasta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 608/2013 säädettyjen lomakkeiden vahvistamisesta (EUVL L 341, 18.12.2013, s. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Neuvoston asetus (EU) N:o 389/2012, annettu 2 päivänä toukokuuta 2012, hallinnollisesta yhteistyöstä valmisteverotuksen alalla ja asetuksen (EY) N:o 2073/2004 kumoamisesta (EUVL L 121, 8.5.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3) 3 jakso: Henkilön tunnistetietoja koskevat metatiedot

Taulukko 5

Henkilön tunnistetietoja koskevat metatiedot

Tunniste	Määritelmä	Käyttö
`issuing_authority`	Henkilön tunnistetiedot myöntäneen hallintoviranomaisen nimi tai asianomaisen jäsenvaltion ISO 3166 -standardin mukainen alpha-2-maakoodi, jos ei ole erillistä viranomaista, jolla on valtuudet myöntää henkilön tunnistetietoja	Pakollinen
`issuing_country`	Henkilön tunnistetietojen tarjoajan maan tai alueen ISO 3166-1 -standardin mukainen alpha-2-maakoodi	Pakollinen
`expiry_date`	Päivämäärä (ja jos mahdollista, kellonaika), jolloin henkilön tunnistetietojen hallinnollinen voimassaoloaika päättyy	Valinnainen
`document_number`	Henkilön tunnistetietojen tarjoajan antama henkilön tunnistetietojen numero	Valinnainen
`issuing_jurisdiction`	Henkilön tunnistetiedot myöntäneen lainkäyttöalueen maakoodin alajaottelu standardin ISO 3166-2:2020 kohdan 8 mukaisesti. Koodin ensimmäisen osan on oltava sama kuin myöntävän maan arvo.	Valinnainen
`issuance_date`	Päivämäärä ja, jos mahdollista, kellonaika, jolloin henkilön tunnistetietojen hallinnollinen voimassaoloaika alkoi	Valinnainen

4) 4 jakso: Luonnollisen henkilön tunnistetietojen attribuuttien koodaus

— Luonnollisen henkilön tunnistetiedot on myönnettävä täytäntöönpanoasetuksen (EU) 2024/2979 liitteessä II esitetyn standardin 5 kohdan (SD-JWT VC -muoto) ja 6 kohdan (ISO/IEC-mdoc-muoto) mukaisesti siltä osin kuin niitä sovelletaan sähköisiin attribuuttitodistuksiin. Kohtia 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3, 6.2.4 ja 6.2.5 ei sovelleta.

— Luonnollisen henkilön tunnistetietojen koodauksen on oltava tässä liitteessä olevassa 4.1 ja 4.2 kohdassa esitettyjen teknisten eritelmien mukainen.

4.1 Luonnollisen henkilön tunnistetietojen koodaus ISO/IEC-mdoc-muodossa

— Henkilön tunnistetietojen ISO/IEC-mdoc-muotoisen todistustyypin on oltava ’eu.europa.ec.eudi.pid.1’. Tässä liitteessä esitettyjen henkilön tunnistetietojen attribuuttien nimitilan tunnisteen on oltava ’eu.europa.ec.eudi.pid.1’.

— Jos henkilön tunnistetiedot sisältävät tietoja, joiden tunnisteita ei vahvisteta tässä liitteessä, nämä tiedot on määriteltävä kansallisessa henkilön tunnistetietojen nimitilassa, jossa käytetään yleistä muotoa eu.europa.ec.eudi.pid.[ISO 3166-1 -standardin mukainen alpha-2-maakoodi tai ISO 3166-2 -standardin mukainen aluekoodi], jonka jälkeen voidaan lisätä valinnaisesti piste ja versionumero.

— Jos käytetään kansallista nimitilaa, sen järjestelmä, mukaan lukien kaikki tunnisteet, niiden määritelmät, käyttö ja koodausmuodot, on julkaistava komission täytäntöönpanoasetuksen (EU) 2025/1569 ([1]) 8 artiklan mukaisesti.

— Henkilön tunnistetiedot ja niiden metatiedot, jotka vahvistetaan tässä liitteessä olevissa 1 ja 3 jaksossa, on sisällytettävä ISO/IEC-mdoc-muotoa koskevissa eritelmissä tarkoitettuihin henkilön tunnistetietojen elementteihin.

— MobileSecurityObject-tyypin ilmentymän deviceKeyInfo-jäsenessä olevan deviceKey-jäsenen on sisällettävä julkinen avain.

— Julkisen avaimen on vastattava yksityistä avainta, joka on tallennettu lompakon käyttäjän lompakon suojattuun salauslaitteeseen ('WSCD').

— Sen digitaalisen CB-AdES-allekirjoituksen suojatun otsikon, jolla allekirjoitetaan ISO/IEC-mdoc-muotoiset henkilön tunnistetiedot, on sisällettävä x5u- ja x5t-otsikkoparametrit, jotka on määritelty RFC 9360:ssä ([2]).

— x5t-otsikkoparametrissa käytettävän tiivistealgoritmin on oltava SHA-256.

— Henkilön tunnistetietojen koodausta ISO/IEC-mdoc-muodossa koskevat vaatimukset esitetään taulukossa 6:

Taulukko 6

Henkilön tunnistetietojen koodausta ISO/IEC-mdoc-muodossa koskevat vaatimukset

Tunniste	Attribuutin tunniste	Koodausmuoto
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Komission täytäntöönpanoasetus (EU) 2025/1569, annettu 29 päivänä heinäkuuta 2025, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä hyväksyttyjen sähköisten attribuuttitodistusten ja virallisesta lähteestä vastaavan julkisen sektorin elimen myöntämien tai sen puolesta myönnettyjen sähköisten attribuuttitodistusten osalta (EUVL L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([2]) Schaad, J., "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates" (https://datatracker.ietf.org/doc/rfc9360/).

Tunniste	Attribuutin tunniste	Koodausmuoto
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate tai full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate tai full-date

— Taulukossa 6 esitetyn attribuuttien koodausmuodon notaatiossa on käytettävä RFC 8610:n ([3]) mukaisia esitystyyppejä ja noudatettava seuraavia lisävaatimuksia:

a) tstr on koodattava UTF-8-muodossa;

b) tstr:n on tuettava koko Unicode-aluetta;

c) tstr saa olla enintään 150 merkkiä pitkä;

d) päivämäärä on koodattava RFC 8943:n ([4]) mukaisesti;

e) full-date on tulkittava #6.1004(tstr):ksi, jossa tunniste 1004 on RFC 8943:n mukainen;

f) tdate-attribuutin on sisällettävä RFC 3339:n ([5]) mukainen päivämäärä-kellonaikamerkkijono.

g) full-date-attribuutin on sisällettävä RFC 3339:n mukainen full-date-merkkijono (päivämäärä-merkkijono) RFC 8943:n mukaisesti;

h) jollei toisin ilmoiteta, attribuuteissa olevassa päivämäärän esityksessä

— ei saa ilmoittaa sekunnin murto-osia;

— ei saa ilmoittaa paikallista poikkeamaa UTC:stä, ja RFC 3339:n mukaiseksi aikapoikkeamaksi on asetettava 'Z';

i) kokonaisluvun, jonka tärkeimmät tyypit ovat 0 ja 1, on oltava mahdollisimman pieni RFC 8949:n ([6]) kohdan 4.2 mukaisesti.

j) place_of_birth-attribuutissa on oltava vähintään yksi seuraavista avainarvopareista: 'country', 'region' tai 'locality';

k) bstr:n, tstr:n, taulukon tai hakurakenteen on oltava mahdollisimman lyhyt RFC 8949:n kohdan 4.2 mukaisesti;

([3]) C. Vigano and H. Birkholz, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures," RFC 8610, kesäkuu 2019.
([4]) M. Jones, A. Nadalin and J. Richter, "Concise Binary Object Representation (CBOR) Tags for Date," RFC 8943, marraskuu 2020.
([5]) G. Klyne and C. Newman, "Date and Time on the Internet: Timestamps," RFC 3339, heinäkuu 2002.
([6]) C. Bormann and P. Hoffman, "Concise Binary Object Representation (CBOR)," RFC 8949, joulukuu 2020.

l) nationality-attribuutti on koodattava standardin ISO 3166-1 mukaisista alpha-2-maakoodeista koostuvana taulukkona. Jos käytetään RFC 8610:n mukaista CDDL-notaatiota, tämän attribuutin koodauksen on oltava seuraava:

— nationalities = [+ CountryCode];

— CountryCode = tstr; standardin ISO 3166-1 mukainen alpha-2-maakoodi;

— jos lompakon käyttäjällä, johon henkilön tunnistetiedot liittyvät, on useita kansalaisuuksia ja henkilön tunnistetietojen tarjoaja vahvistaa nämä useat kansalaisuudet, henkilön tunnistetietojen tarjoaja voi sisällyttää kaikki kansalaisuudet henkilön tunnistetietoihin;

— place_of_birth-attribuutti on koodattava tyyppinä place_of_birth. Jos käytetään RFC 8610:n mukaista CDDL-notaatiota, tämän attribuutin koodauksen on oltava seuraava:

place_of_birth =

{'

? country': tstr; yksi standardin ISO 3166-1 mukainen alpha-2-maakoodi

? 'region': tstr; osavaltion, provinssin, hallintopiirin tai alueen nimi

? 'locality': tstr; kunnan, kaupungin tai kylän nimi

}

4.2 Henkilön tunnistetietojen koodausta SD-JWT VC -muodossa koskevat vaatimukset

— Tässä kohdassa esitetyt henkilön tunnistetiedot ja niiden metatiedot on sisällytettävä henkilön tunnistetietoihin SD-JWT VC -muotoa koskevissa eritelmissä tarkoitettuina väitteinä.

— Kaikki edellisessä luetelmakohdassa tarkoitettujen myönnettyjen henkilön tunnistetietojen sisältämät väitteet on voitava luovuttaa erikseen valikoivasti, lukuun ottamatta väitteitä, jotka on määritelty väitteiksi, joita ei saa luovuttaa valikoivasti SD-JWT VC -muodossa.

— Taulukossa 7 esitetään julkisten väitteiden nimien koodaus.

— Taulukossa 8 esitetään yksityisten väitteiden nimien koodaus.

— JSON-merkkijono, jota käytetään SD-JWT VC -muodossa koodatuissa henkilön tunnistetiedoissa, on koodattava UTF-8-muodossa, ja sen on tuettava koko Unicode-aluetta, jollei jäljempänä taulukossa 8 tai siinä mainituissa viittauksissa nimenomaisesti toisin mainita.

— SD-JWT VC -muodon mukaisten henkilön tunnistetietojen tekninen voimassaoloaika on ilmaistava RFC 7519:ssä ([7]) määritellyillä JWT-väitteillä nbf ja exp.

([7]) J. Jones, et al., "JSON Web Token (JWT)", RFC 7519, toukokuu 2015.

— Henkilön tunnistetietojen on sisällettävä RFC 7800:ssa ([8]) määritelty cnf-väite, jonka on oltava julkinen avain, joka on luotu lompakon käyttäjän lompakkoyksikön WSCD:een tallennetusta yksityisestä avaimesta.

— Sen digitaalisen allekirjoituksen suojatun otsikon, jolla allekirjoitetaan SD-JWT VC -muotoiset henkilön tunnistetiedot, on sisällettävä RFC 7515:n ([9]) mukaiset otsikkoparametrit x5u ja x5t#S256.

Taulukko 7

Vaatimukset, jotka koskevat henkilön tunnistetietojen koodausta SD-JWT VC -muodossa julkisilla nimillä

Tunniste	Attribuutin tunniste	Koodausmuoto
family_name	family_name	merkkijono
given_name	given_name	merkkijono
birth_date	birthdate	merkkijono, ISO 8601-1, VVVV-KK-PP-muoto
birth_place	place_of_birth	JSON-rakenne
nationality	nationalities	merkkijonotaulukko
resident_address	address.formatted	merkkijono
resident_country	address.country	merkkijono
resident_state	address.region	merkkijono
resident_city	address.locality	merkkijono
resident_postal_code	address.postal_code	merkkijono
resident_street	address.street_address	merkkijono
family_name_birth	birth_family_name	merkkijono
given_name_birth	birth_given_name	merkkijono
email_address	email	merkkijono
mobile_phone_number	phone_number	merkkijono
portrait	picture	merkkijono; data-URL, joka sisältää base64-koodatun kasvokuvan JPEG-muodossa

([8]) M. Jones, et al., "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, huhtikuu 2016.
([9]) M. Jones, et al., "JSON Web Signature (JWS)", RFC 7515, toukokuu 2015.

Taulukko 8

Vaatimukset, jotka koskevat henkilön tunnistetietojen koodausta SD-JWT VC -muodossa yksityisillä nimillä

Tunniste	Attribuutin tunniste	Koodausmuoto
`expiry_date`	`date_of_expiry`	merkkijono, ISO 8601-1, VVVV-KK-PP-muoto
`issuance_date`	`date_of_issuance`	merkkijono, ISO 8601-1, VVVV-KK-PP-muoto
`personal_administrative_number`	`personal_administrative_number`	merkkijono
`sex`	`sex`	numero
`issuing_authority`	`issuing_authority`	merkkijono
`issuing_country`	`issuing_country`	merkkijono
`document_number`	`document_number`	merkkijono
`issuing_jurisdiction`	`issuing_jurisdiction`	merkkijono

— Henkilön tunnistetietojen perustyypin on oltava ’urn:eudi:pid:1’, joka sisällytetään vct-väitteeseen. Kaikissa henkilön tunnistetiedoissa on käytettävä tyyppejä nimitilassa ’urn:eudi:pid:’.

— Jos henkilön tunnistetietoihin sisältyy attribuutteja, joita ei mainita tässä liitteessä, nämä attribuutit on määriteltävä kansallisessa tyypissä.

— Jos käytetään kansallista tyyppiä, sen järjestelmä, mukaan lukien kaikki tunnisteet, niiden määritelmät, käyttö ja koodausmuodot, on määriteltävä järjestelmässä, joka julkaistava täytäntöönpanoasetuksen (EU) 2025/1569 8 artiklan mukaisesti.

5) 5 jakso: Luottamusinfrastruktuuria koskevat tiedot

Komission täytäntöönpanoasetuksen (EU) 2024/2980 mukaisesti saataville asettama henkilön tunnistetietojen tarjoajien luettelo mahdollistaa henkilön tunnistetietojen todentamisen.”

LIITE II

”LIITE I a

5 a artiklassa tarkoitetut salausmekanismit

Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: Euroopan kyberturvallisuusviraston (ENISA) julkaisema asiakirja ’Agreed Cryptographic Mechanisms’ ([1]).”

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en?prefLang=fi.

LIITE III

”LIITE I b

6 artiklan 2 a kohdassa tarkoitetut lompakkoyksikkötodistuksia koskevat tekniset eritelmät

1) Lompakkoyksikkötodistuksessa on oltava yksi tai useampi lompakon ilmentymää koskeva todistus ja yksi tai useampi avaintodistus.

2) Lompakon ilmentymää koskevien todistusten ja avaintodistusten on täytettävä seuraavat vaatimukset:

a) Muotovaatimukset

— FR-WIA-1: Lompakon ilmentymää koskevan todistuksen on oltava RFC 7519:n ([1]) mukainen JSON Web Token (JWT), jonka lompakon tarjoaja allekirjoittaa tai leimaa Compact JAdES Baseline B -allekirjoituksella.

— FR-WIA-1.1: Lompakon ilmentymää koskevan todistuksen on oltava lompakkotodistus, joka määritellään ”OpenID for Verifiable Credential Issuance v1.0” -julkaisun ([2]) (’OID4VCI’), lisäyksessä E ja jota laajennetaan jäljempänä olevien C-WIA-1 ja C-WIA-2 kohdan mukaisesti.

— FR-KA-1: Avaintodistuksen on oltava RFC 7519:n mukainen JWT, jonka lompakon tarjoaja allekirjoittaa tai leimaa Compact JAdES Baseline B -allekirjoituksella.

— FR_KA_1.1: Avaintodistuksen on oltava OID4VCI:n lisäyksessä D määritelty avaintodistus, jota laajennetaan jäljempänä olevien C_KA-1 ja C_KA-2 kohdan mukaisesti.

b) Kuljetusta koskevat vaatimukset

— TR-WIA-1: Lompakkoyksikön on käytettävä lompakon ilmentymää koskevaa todistusta henkilön tunnistetietojen, hyväksyttyjen tai ei-hyväksyttyjen sähköisten attribuuttitodistusten tai virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamien tai sen puolesta tarjottujen sähköisten attribuuttitodistusten myöntämisen aikana.

— TR-WIA-2: Lompakon tarjoajan on tarkistettava lompakon ilmentymän eheys ja allekirjoitettava tai leimattava lompakon ilmentymää koskeva todistus.

— TR-WIA-2.1: Kun lompakon tarjoaja myöntää lompakon ilmentymää koskevan todistuksen, ajan, jolloin lompakon tarjoaja on tarkistanut lompakon ilmentymän eheyden, ja ajan, jonka lompakon tarjoaja merkitsee myönnetyn lompakon ilmentymää koskevan todistuksen ’exp’-otsikkoparametriin, välisen eron on oltava alle 24 tuntia.

— TR-WIA-2.2: Lompakon tarjoajan on varmistettava, että lompakkoyksikkö sisältää lompakon ilmentymää koskevat todistukset, jotka tarvitaan henkilön tunnistetietojen ja sähköisten attribuuttitodistusten myöntämiseksi.

— TR-WIA-3: Myöntämisen aikana lompakkoyksikön on lähetettävä lompakon ilmentymää koskeva todistus valtuutuspalvelimelle suorassa valtuutuspyynnössä ja token-pyynnössä OID4VCI:n mukaisesti.

— TR-WIA-3.1: Lompakkoyksikön on lähetettävä lompakon ilmentymää koskeva todistus yhdessä hallussapitotodistuksen (Proof-of-Possession, ’PoP’) kanssa OID4VCI:n lisäyksen E mukaisesti.

— TR-WIA-3.2: Lompakkoyksikkö saa lähettää saman lompakon ilmentymää koskevan todistuksen ainoastaan yhdelle valtuutuspalvelimelle.

([1]) RFC 7519: JSON Web Token (JWT), toukokuu 2015.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Jos lompakon tarjoaja käyttää jäljempänä R_WIA_1 kohdassa määriteltyä ’per-issuer reuse’ -vaihtoehtoa, lompakkoyksikkö voi lähettää lompakon ilmentymää koskevan todistuksen samalle valtuutuspalvelimelle useita kertoja.

— TR-WIA-3.2.2: Jos lompakon tarjoaja ei käytä ’per-issuer reuse’ -vaihtoehtoa, lompakkoyksikkö saa käyttää lompakon ilmentymää koskevaa todistusta enintään yhdessä myöntämisprosessissa.

— TR-WIA-4: Kun valtuutuspalvelin saa lompakon ilmentymää koskevan todistuksen, sen on tarkistettava lompakon ilmentymää koskevan todistuksen allekirjoitus käyttäen kyseisen todistuksen JOSE-otsikon ’x5c’-parametriin sisältyvän allekirjoitusvarmenteen julkista avainta.

— TR-WIA-4.1: Valtuutuspalvelimen on myös tarkistettava, että tämä allekirjoitusvarmenne voidaan tarkistaa täytäntöönpanoasetuksen (EU) 2024/2980 5 artiklassa tarkoitetussa lompakon tarjoajien luettelossa olevalla luottamusankkurilla käyttäen mahdollisesti x5c-parametriin sisältyviä välivarmenteita.

— TR-WIA-4.2: Valtuutuspalvelimen on tarkistettava, ettei lompakon ilmentymää koskevan todistuksen voimassaoloaika ole päättynyt.

— TR-WIA-4.3: Valtuutuspalvelimen on tarkistettava PoP:n allekirjoitus ’cnf’-väitteessä esitetyllä julkisella avaimella.

— TR_KA-1: Lompakkoyksikön on käytettävä avaintodistusta henkilön tunnistetietojen myöntämisen aikana ja laitesidonnaisten hyväksyttyjen tai ei-hyväksyttyjen sähköisten attribuuttitodistusten taikka virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamien tai sen puolesta tarjottujen sähköisten attribuuttitodistusten myöntämisen aikana.

— TR_KA-1.1: Lompakkoyksikkö ei saa käyttää avaintodistusta muiden kuin laitesidonnaisten hyväksyttyjen tai ei-hyväksyttyjen sähköisten attribuuttitodistusten taikka virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamien tai sen puolesta tarjottujen sähköisten attribuuttitodistusten myöntämisen aikana.

— TR_KA-2: Lompakon tarjoajan on annettava lompakkoyksikölle eri avaintodistukset lompakkoyksikön WSCD:n ja kunkin avainsäilön osalta.

— TR_KA-2.1: Lompakon tarjoajan on allekirjoitettava tai leimattava avaintodistus sen jälkeen, kun se on tarkistanut, että avaintodistuksessa oikeaksi todistetut avaimet on tallennettu avaintodistuksessa kuvattuun lompakkoyksikön WSCD:een tai avainsäilöön.

— TR_KA-2.2: Avaintodistuksen on sisällettävä vähintään yksi oikeaksi todistettu julkinen avain. Valtuustietojen myöntäjälle lähetetyssä avaintodistuksessa olevien avainten määrä ei saa ylittää kyseisen valtuustietojen myöntäjän metatiedoissaan (Credential Issuer Metadata) määrittämää enimmäismäärää. Ks. ETSI TS 119 472-3 ([3]), parametri ’credential_configurations_supported.credential_metadata.credential_reuse_policy.options.batch_size’.

— TR_KA-2.3: Lompakon tarjoaja saa sisällyttää julkisen avaimen (joka vastaa lompakkoyksikön WSCD:een tai avainsäilöön tallennettua yksityistä avainta) enintään yhteen avaintodistukseen.

— TR_KA-2.4: Lompakkoyksikkö saa käyttää avaintodistusta enintään yhden valtuustietojen myöntämistä tai uudelleenmyöntämistä koskevan prosessin aikana.

— TR_KA-2.5: Lompakon tarjoajan on varmistettava, että lompakkoyksiköllä on hallussaan avaintodistukset, joita tarvitaan henkilön tunnistetietojen ja laitesidonnaisten sähköisten attribuuttitodistusten myöntämiseksi.

([3]) ETSI, ”Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles”, ETSI TS 119 472-3, V1.1.1, maaliskuu 2026.

— TR_KA-3: Lompakkoyksikön on sisällytettävä avaintodistus valtuustietojen myöntäjälle lähetetyn valtuustietopyynnön kenttään 'proofs' OID4VCIn mukaisesti joko 'jwt'-tyypin todistuksena tai 'attestation'-tyypin todistuksena, jos tämä on tarpeen myöntämisen aikana.

— TR_KA_3.1: Jos lompakkoyksikkö sisällyttää avaintodistuksen 'jwt'-elementtiin, sen on allekirjoitettava avaintodistus yksityisellä avaimella, joka vastaa 'key_attestation'-objektin 'attested_keys'-taulukon indeksissä 0 olevaa julkista avainta.

— TR_KA-4: Jos valtuustietojen myöntäjä myöntää laitesidonnaisia valtuustietoja, sen on ilmoitettava OID4VCI:n kohdan 12.2.4 mukaisessa metatietojensa 'proof_types_supported'-parametrissa, että se tukee sekä 'jwt'-todistustyyppiä että 'attestation'-todistustyyppiä avaintodistusten osalta, joiden sisällettävä 'key_attestation_required'-objekti.

— TR_KA-4.1: Jos valtuustietojen myöntäjä myöntää muita kuin laitesidonnaisia valtuustietoja, sen on jätettävä parametrit 'proof_types_supported' ja 'cryptographic_binding_methods_supported' pois metatiedoistaan.

— TR_KA-5: Jos valtuustietojen myöntäjä saa avaintodistuksen 'jwt'- tai 'attestation'-todistustyyppinä, sen on tarkistettava avaintodistuksen allekirjoitus avaintodistuksen JOSE-otsikon 'x5c'-parametriin sisältyvässä allekirjoitusvarmenteessa olevalla julkisella avaimella sekä tämä allekirjoitusvarmenne täytäntöönpanoasetuksen (EU) 2024/2980 5 artiklassa tarkoitetussa lompakon tarjoajien luettelossa olevalla luottamusankkurilla, mahdollisesti käyttämällä 'x5c'-parametriin sisältyviä välivarmenteita.

— TR_KA-6: Jos valtuustietojen myöntäjä saa avaintodistuksen 'jwt'-todistustyyppinä, sen on tarkistettava 'jwt'-elementin allekirjoitus 'jwt'-elementtiin sisältyvän 'key_attestation'-objektin 'attested_keys'-taulukon indeksissä 0 olevalla avaimella.

— TR_KA-6.1: Valtuustietojen myöntäjän on tarkistettava, että 'jwt'-elementin 'nonce'-kentässä on OID4VCI:n mukainen kelvollinen 'c_nonce'-arvo sen 'nonce_endpoint'-parametrista.

— TR_KA-7: Kun valtuustietojen myöntäjä saa avaintodistuksen 'attestation'-todistustyyppinä, sen on tarkistettava, että 'key_attestation'-objekti sisältää kelvollisen 'c_nonce'-arvon sen 'nonce_endpoint'-parametrista.

— TR_KA-8: Henkilön tunnistetietojen tarjoajan on varmistettava, että henkilön tunnistetiedot sidotaan julkiseen avaimeen, joka on peräisin avaintodistuksesta, jossa mainitaan WSCD.

c) Sisältövaatimukset

— C_WIA-1: Lompakon ilmentymää koskevan todistuksen on sisällettävä seuraavat tiedot:

— OID4VCI:n lisäyksen E mukainen 'wallet_name'-väite, jonka arvo on täytäntöönpanoasetuksen (EU) 2024/2980 5 artiklassa tarkoitetussa lompakon tarjoajien luettelossa mainitun lompakkoratkaisun tunniste;

— 'wallet_version'-väite ([4]), joka on merkkijono, jonka arvo on lompakkoratkaisun versio;

— 'wallet_solution_certification_information'-väite, joka on JSON-objekti, joka sisältää tiedot lompakkoratkaisun sertifioineesta vaatimustenmukaisuuden arviointilaitoksesta, tarvittaessa sertifiointinumeron sekä muita sertifiointi koskevia merkityksellisiä tietoja;

([4]) Tämä väite määritellään tässä täytäntöönpanoasetuksessa, koska se ei ole osa OID4VCI-eritelmää.

— ’client_status’-väite, joka sisältää kaksi alakenttää:

— ’status’: OID4VCI:n lisäyksen E mukainen statusluetteloviittaus, joka edustaa lompakon ilmentymän peruutusstatusta. Katso lisätietoja jäljempänä olevasta e alakohdasta;

— ’exp’: RFC 7519:n mukainen NumericDate, joka kuvaa aikaa, johon asti lompakon tarjoaja säilyttää peruutusstatuksen kohdassa ’status’ viitatussa statusluetteloindeksissä.

— OID4VCI:n lisäyksen E mukainen ’exp’-väite.

— *HUOMAUTUS:* ’client_status.status’-väite lompakon ilmentymää koskevassa todistuksessa edustaa lompakon ilmentymän peruutusstatusta, ei itse todistuksen peruutusstatusta. Kuten jäljempänä R_WIA-1 kohdassa kuvataan, lompakon tarjoaja voi päättää rajata kunkin lompakon ilmentymää koskevan todistuksen tiettyyn valtuutuspalvelimeen sen perusteella, että kaikki kyseiselle palvelimelle lähetetyt todistukset sisältävät saman indeksiarvon ’client_status.status’-merkinnässä.

— *HUOMAUTUS:* ’Status’-väitteen ’idx’-arvoa voidaan käyttää lompakon ilmentymän ja lompakkoyksikön (parittaisena) yksilöllisenä tunnisteena.

— C_WIA-2: Lompakon ilmentymää koskevan todistuksen olisi sisällettävä myös OID4VCI:n lisäyksen E mukainen ’wallet_link’-väite, ja tämän väitteen arvon on oltava URI-osoite, jossa kyseisestä lompakkoratkaisusta voidaan saada lisätietoa.

— C_WIA-3: Valtuutuspalvelin ei saa tulkita lompakon ilmentymää koskevan todistuksen ylimmän tason ’exp’-parametria lompakon ilmentymän peruutusstatuksen säilyttämisajan päättymiseksi.

— *HUOMAUTUS:* Lompakon ilmentymää koskevan todistuksen ylimmän tason ’exp’-parametri osoittaa, milloin itse todistuksen voimassaoloaika päättyy.

— C_KA-1: Avaintodistuksen on sisällettävä seuraavat tiedot:

— OID4VCI:n lisäyksen D mukaiset ’key_storage’- ja ’user_authentication’-väitteet;

— ’Key_storage’- ja ’user_authentication’-attribuuttien arvon on oltava ’iso_18045_high’, jos avaintodistuksessa mainitaan lompakon suojattu salauslaite.

— OID4VCI:n lisäyksen D mukainen ’certification’-väite, joka sisältää URL-osoitteen, josta voidaan saada tietoa WSCD:n tai avainsäilön saamasta sertifioinnista, esimerkiksi yhteisten kriteerien tai GlobalPlatformin kaltaisesta järjestelmästä, arvioiduista vaatimuksista, kuten sovellettavasta suojausprofiilista, sekä arviointitasosta;

— Näistä tiedoista on voitava päätellä, onko avainten säilytyspaikka WSCD.

— ’key_storage_status’-väite, joka sisältää kaksi alakenttää:

— ’status’: OID4VCI:n lisäyksen D.1 mukainen statusluetteloviite. Arvo edustaa joko oikeaksi todistettujen avainten säilyttämiseen käytetyn WSCD:n tai avainsäilön peruutusstatusta tai – käytettäessä ’per-key-attestation index’ -vaihtoehtoa – yksittäisen lompakkoyksikön WSCD:n tai avainsäilön peruutusstatusta. Katso käytettävissä olevat indeksin määritysvaihtoehdot jäljempänä olevasta R_KA_1 kohdasta;

— ’exp’: RFC 7519:n mukainen NumericDate, joka kuvaa aikaa, johon asti lompakon tarjoaja säilyttää peruutusstatuksen kohdassa ’status’ viitatussa statusluetteloindeksissä.

— OID4VCI:n lisäyksen D mukainen ’exp’-väite.

— *HUOMAUTUS:* 'idx'-arvosta avaintodistuksen 'key_storage_status.status'-väitteessä: Jos lompakon tarjoaja käyttää 'type-shared index' -vaihtoehtoa (ks. R_KA_1 kohta jäljempänä), kaikissa samaan WSCD:n tai avainsäilön tyyppiin liittyvissä avaintodistuksissa on sama statusluetteloindeksi. Näin ollen 'idx'-arvo ei ole lompakkoyksikkökohtainen. Sitä vastoin, kun lompakon tarjoaja käyttää 'per-key-attestation index' -vaihtoehtoa, 'idx'-arvo on lompakkoyksikkökohtainen (tai parittaisesti yksilöllinen valtuustietojen myöntäjälle). Valtuustietojen myöntäjä ei kuitenkaan saa missään tapauksessa käyttää avaintodistuksen 'idx'-arvoa lompakkoyksikön tunnisteena, vaan sen on käytettävä sen sijaan lompakon ilmentymää koskevan todistuksen 'idx'-arvoa.

— C_KA-2: Jos avaintodistus lähetetään 'attestation'-todistustyyppinä, siihen on sisällyttävä myös OID4VCI:n lisäyksen F.3 mukainen kelvollinen 'c_nonce'.

— C_KA-3: Valtuustietojen myöntäjä ei saa tulkita avaintodistuksen ylimmän tason 'exp'-parametria WSCD:n tai avainsäilön peruutusstatuksen säilyttämisajan päättymiseksi.

— *HUOMAUTUS:* Avaintodistuksen ylimmän tason 'exp'-parametri osoittaa, milloin itse avaintodistuksen voimassaolo päättyy.

d) Elinkaarivaatimukset

— Tässä liitteessä käsitellään seuraavia valtuustietojen myöntäjän metatietoparametreja:

— 'preferred_client_status_period': OPTIONAL. Kokonaisluku, joka osoittaa sekunteina ensisijaisen jäljellä olevan ajan, jonka ajan lompakkoyksikön myöntämisen aikana esitettävän lompakon ilmentymää koskevan todistuksen statusta säilytetään. Jäljellä oleva statuksen säilyttämisaika määritellään siten, että todistuksen 'client_status.exp'-arvosta vähennetään todistuksen vastaanottoaika;

— 'preferred_key_storage_status_period': OPTIONAL. Kokonaisluku, joka osoittaa sekunteina ensisijaisen jäljellä olevan ajan, jonka ajan lompakkoyksikön myöntämisen aikana esitettävän avaintodistuksen statusta säilytetään. Jäljellä oleva statuksen säilyttämisaika määritellään siten, että todistuksen 'key_storage_status.exp'-arvosta vähennetään todistuksen vastaanottoaika.

— LC_WIA-1: Valtuutuspalvelin voi ilmoittaa ensisijaiset jäljellä olevat statuksen säilyttämisajat lompakon ilmentymää koskevissa todistuksissa sisällyttämällä 'preferred_client_status_period'-metatietoparametrin valtuustietojen myöntäjän metatietojensa päätepisteeseen (endpoint) OID4VCI:n kohdan 12.2.2 mukaisesti.

— LC_WIA-1.1: Tämä kenttä on sijoitettava valtuustietojen myöntäjän metatietojen ylimmälle tasolle.

— LC_WIA_2: Valtuutuspalvelin ei saa tulkita lompakon ilmentymää koskevan todistuksen ylimmän tason 'exp'-parametria lompakon ilmentymän peruutusstatuksen säilyttämisajan päättymiseksi.

— LC_WIA_3: Kun lompakon tarjoaja allekirjoittaa tai leimaa lompakon ilmentymää koskevan todistuksen, sen on säilytettävä kyseisen lompakon ilmentymän peruutusstatus, kunnes kyseisessä lompakon ilmentymää koskevassa todistuksessa mainittu 'wallet_instance_status.exp'-aika on umpeutunut.

— LC_KA-1: Jos tarvitaan avaintodistusta, valtuustietojen myöntäjä voi ilmoittaa ensisijaiset jäljellä olevat statuksen säilyttämisajat avaintodistuksissa sisällyttämällä edellä kuvatun 'preferred_key_storage_status_period'-metatietoparametrin metatietojensa päätepisteeseen (endpoint) OID4VCI:n kohdan 12.2.2 mukaisesti.

— LC_KA-1.1: Tämä kenttä on sijoitettava OID4VCI:n kohdan 12.2.4 mukaisiin 'key_attestations_required'-objekteihin.

— LC_KA-2: Lompakon tarjoajan on päätettävä myöntämiensä avaintodistusten tekninen voimassaoloaika.

— LC_KA-3: Jos lompakon tarjoaja allekirjoittaa tai leimaa avaintodistuksen, sen on säilytettävä kyseisen WSCD:n tai avainsäilön peruutusstatus, kunnes kyseisessä avaintodistuksessa mainittu 'key_storage_status.exp'-aika on umpeutunut.

— LC_GEN-1: Lompakon tarjoajan on varmistettava, että lompakkoyksikkö voi esittää aina lompakkoyksikkötodistuksen ja avaintodistuksen, jonka 'client_status.exp' ja vastaavasti 'key_storage_status.exp' ovat aina 31 päivän päässä tulevaisuudessa siitä hetkestä katsottuna, kun todistukset esitetään valtuutuspalvelimelle tai valtuustietojen myöntäjälle.

— *HUOMAUTUS:* Näin taataan, että henkilön tunnistetietojen tarjoajat voivat turvautua peruutusketjutukseen joutumatta myöntämään lyhytaikaisia henkilön tunnistetietoja.

— LC_GEN-2: Lompakon tarjoajan on varmistettava, että lompakkoyksikkö hakee valtuustietojen myöntäjän metatiedot myöntämisen aikana.

  — LC_GEN_2.1: Jos näihin metatietoihin sisältyy 'preferred_key_storage_status_duration'-kenttä, lompakkoyksikön on lähetettävä avaintodistus, jossa on mahdollisimman pieni muttei negatiivinen ('key_storage_status.exp' – nykyinen aika) – 'preferred_key_storage_status_duration'. Jos lompakkoyksikön saatavilla ei ole tällaista avaintodistusta, sen on hankittava lompakon tarjoajalta uusi avaintodistus, joka täyttää ehdon 'key_storage_status.exp' – nykyinen aika ≥ 'preferred_key_storage_status_duration'.

  — LC_GEN_2.2: Jos näihin metatietoihin sisältyy 'preferred_client_status_duration'-kenttä, lompakkoyksikön on lähetettävä lompakon ilmentymää koskeva todistus, jossa on mahdollisimman pieni muttei negatiivinen ('client_status.exp' – nykyinen aika) – 'preferred_client_status_duration'. Jos lompakkoyksikön saatavilla ei ole tällaista lompakon ilmentymää koskevaa todistusta, sen on pyydettävä lompakon tarjoajalta uusi lompakon ilmentymää koskeva todistus, joka täyttää ehdon 'client_status.exp' – nykyinen aika ≥ 'preferred_client_status_duration'.

— LC_GEN-3: Henkilön tunnistetietojen teknisen voimassaoloajan on päätyttävä ennen myöntämisprosessissa henkilön tunnistetietojen tarjoajalle lähetetyn lompakon ilmentymää koskevan todistuksen 'client_status.exp'-aikaa että myöntämisprosessissa henkilön tunnistetietojen tarjoajalle lähetetyn avaintodistuksen 'key_storage_status.exp'-aikaa.

— LC_GEN-4: Sellaisten henkilön tunnistetietojen tarjoajan, joiden tekninen voimassaoloaika on yli 24 tuntia, on tarkistettava myöntämisen aikana saatujen lompakon ilmentymää koskevan todistuksen ja avaintodistuksen peruutusstatus vähintään kerran vuorokaudessa henkilön tunnistetietojen teknisen voimassaoloajan aikana. Jos jompikumpi todistus peruutetaan, tarjoajan on peruutettava henkilön tunnistetiedot.

e) Peruuttamista koskevat vaatimukset

— R_GEN-1: Lompakon tarjoajan on käytettävä Token Status Lists -luetteloja (token-statusluetteloja) (jotka on määritetty IETF Token Status List -eritelmässä) sekä avaintodistusten että lompakon ilmentymää koskevien todistusten peruutusmekanismina OID4VCI:n lisäysten D ja E mukaisesti.

— *HUOMAUTUS:* Lompakon tarjoaja voi käyttää seuraavia optimointitapoja parantaakseen statusluetteloidensa skaalattavuutta:

  — statusluettelon jakaminen useisiin osiin, kun lompakon tarjoajilla on huomattava määrä käyttäjiä ja myönnettyjä todistuksia. On olemassa useita jaottelustrategioita, jotka perustuvat esimerkiksi määräkokoon tai ajanjaksoon. Lompakon toimittaja voi itse päättää jaottelustrategiastaan. Huomioitavia asioita voivat olla ladattavan statusluettelon koko ja käyttäjän yksityisyys;

  — useat statusluettelot;

  — statusluettelon pakkaaminen sen koon pienentämiseksi.

— R_WIA-1: Lompakon tarjoaja voi antaa saman arvon ’client_status.status’-väitteen ’idx’-väitteelle kaikissa lompakon ilmentymää koskevissa todistuksissa, jotka tietty lompakkoyksikkö esittää samalle valtuutuspalvelimelle. Tätä kutsutaan ’per-issuer reuse’ -vaihtoehdoksi. Jos tätä vaihtoehtoa käytetään

  — R_WIA-1.1: lompakkoyksikön on säilytettävä tila, jossa se on käyttänyt indeksiarvoa kunkin sellaisen valtuutuspalvelimen osalta, jonka kanssa se on ollut aiemmin vuorovaikutuksessa, ja pyydettävä lompakon ilmentymää koskeva todistus, joka sisältää saman indeksiarvon, ollessaan uudestaan vuorovaikutuksessa saman valtuutuspalvelimen kanssa;

  — R_WIA-1.2: jos lompakon tarjoaja saa pyynnön antaa lompakon ilmentymää koskeva todistus, joka sisältää tietyn indeksiarvon, sen on varmistettava, että pyytävä lompakkoyksikkö on saanut kyseisen indeksiarvon aiemmin, ennen kuin se antaa uuden lompakon ilmentymää koskevan todistuksen, joka sisältää kyseisen indeksiarvon;

  — R_WIA-1.3: lompakkoyksikkö ei saa käyttää samaa indeksiarvoa uudelleen ollessaan vuorovaikutuksessa eri valtuutuspalvelimien kanssa.

— *HUOMAUTUS:* Jos käytetään ’per-issuer reuse’ -vaihtoehtoa, lompakon tarjoaja pystyy määrittämään, kuinka monen valtuutuspalvelimen kanssa lompakkoyksikkö on ollut vuorovaikutuksessa ja kuinka usein se on vuorovaikutuksessa kunkin niistä kanssa.

— R_WIA-2: Lompakon tarjoajan on ilmoitettava tietosuojaselosteessaan, käyttääkö se ’per-issuer reuse’ -vaihtoehtoa lompakon ilmentymän peruuttamiseksi.

— R_WIA-3: Jos lompakon tarjoaja ei käytä ’per-issuer reuse’ -vaihtoehtoa, sen on määritettävä jokaiselle myöntämälleen lompakon ilmentymää koskevalle todistukselle uusi, linkittämätön indeksiarvo.

— R_WIA-4: Jos lompakkoyksikkö on peruutettava, lompakon tarjoajan on peruutettava kaikkien kyseiseen lompakkoyksikköön liittyvien lompakon ilmentymää koskevien todistusten ’client_status.status’-väitteen indeksiarvot.

— R_WIA-5: Määrittäessään lompakon ilmentymää koskevien todistusten statusluetteloiden kokoa lompakon tarjoajan on otettava huomioon statusluetteloiden käyttöönoton laajuus ja niiden perustana oleva arkkitehtuuri ja varmistettava, että statusluettelot ovat riittävän suuria korrelaation estämiseksi ja käyttäjien yksityisyyden suojaamiseksi. Statusluettelon on mahdollisuuksien mukaan liityttävä vähintään 10 000 todistukseen.

— R_KA_1: Lompakon tarjoajan on valittava avaintodistuksessa olevalle ’key_storage_status.status’-väitteelle jokin seuraavista indeksinmääritysvaihtoehdoista:

  — vaihtoehto 1 eli ’type-shared index’, jossa kaikki avaintodistukset, jotka todistavat oikeiksi saman tyypin WSCD:een tai avainsäiliöön tallennetut avaimet, sisältävät saman indeksiarvon ’key_storage_status.status’-parametrissa;

  — vaihtoehto 2 eli ’per-key-attestion index’, jossa avaintodistus, joka todistaa oikeiksi yhteen yksittäiseen WSCD:een tai avainsäiliöön tallennetut avaimet, sisältää (parittaisesti) yksilöllisen indeksiarvon ’key_storage_status.status’-parametrissa.

— *HUOMAUTUS:* Jos lompakon tarjoaja käyttää vaihtoehtoa 1, yksi peruuttamistoimenpide mitätöi kaikki kyseisen tyypin avaintodistukset kaikissa lompakkoyksiköissä. Lisäksi koska kaikilla saman tyypin WSCD:een tai avainsäiliöön liittyvillä avaintodistuksilla on sama statusluetteloindeksi, avaintodistusten statusluettelon merkintöjen määrä heijastaa lompakon tarjoajan tukemien WSCD- tai avainsäiliötyyppien määrää, ei käyttöön otettujen lompakkoyksiköiden määrää. Yksityisyysnäkökohdat, jotka vaikuttavat lompakon ilmentymien statusluetteloiden vähimmäiskokoon, eivät näin ollen koske avaintodistusten statusluetteloja vaihtoehdossa 1, edellyttäen, että saman tyypin WSCD:ta tai avainsäiliöä käyttäviä lompakkoyksiköitä on riittävän monta.

— *HUOMAUTUS:* Jos lompakon tarjoaja käyttää vaihtoehtoa 2, kukin indeksi edustaa kyseisessä avaintodistuksessa oikeaksi todistetun WSCD:n tai avainsäilön peruutusstatusta.

— *HUOMAUTUS:* Jos lompakon tarjoaja käyttää vaihtoehtoa 2, tietty WSCD tai avainsäilö voidaan peruuttaa myös käyttäjän pyynnöstä.

— R_KA-2: Jos lompakon tarjoaja käyttää vaihtoehtoa 2, se voi halutessaan käyttää R_WIA-1 kohdassa kuvattua ’per-issuer reuse’ -vaihtoehtoa. Jos lompakon tarjoaja käyttää tätä vaihtoehtoa, sovelletaan soveltuvin osin vaatimuksia R_WIA-1 – R_WIA-3.

— R_KA-3: Jos lompakon tarjoaja käyttää vaihtoehtoa 2, sen on määrittäessään avaintodistusten statusluetteloiden kokoa otettava huomioon statusluetteloiden käyttöönoton laajuus ja niiden perustana oleva arkkitehtuuri ja varmistettava, että statusluettelot ovat riittävän suuria korrelaation estämiseksi ja käyttäjien yksityisyyden suojaamiseksi. Statusluettelon on mahdollisuuksien mukaan liityttävä vähintään 10 000 avaintodistukseen.

— R_KA-4: Jos lompakon tarjoaja käyttää vaihtoehtoa 1 (type-shared index), lompakon tarjoaja saa peruuttaa ’key_storage_status.status’-merkinnän vain, jos WSCD- tai avainsäilötyypin tietoturvassa on haavoittuvuus.

f) Allekirjoitusalgoritmeja koskevat vaatimukset

— SA-1: Lompakon ilmentymää koskevien todistusten, avaintodistusten, niihin liittyvien hallussapitotodistusten ja token-statusluetteloiden allekirjoittamista varten on käytettävä jotakin seuraavista algoritmeista:

— ES256 (ECDSA, SHA-256 ja P-256);

— ES384 (ECDSA, SHA-384 ja P-384);

— ES512 (ECDSA, SHA-512 ja P-521);

— SA-2: Lompakon tarjoajan on valittava, mitä SA-1 kohdassa mainituista algoritmeista se käyttää.

— SA-3: Valtuutuspalvelimen tai valtuustietojen myöntäjän (jotka määritellään OID4VCI:ssä) on tuettava kaikkia SA-1 kohdassa mainittuja algoritmeja.”

LIITE IV

”LIITE II

8 artiklassa tarkoitettu luettelo standardeista

Sovelletaan standardin ETSI TS 119 472-1 V1.2.1 (2026-02) kohdissa 2–6 esitettyjä teknisiä eritelmiä. Niitä koskevat seuraavat mukautukset:

1) 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): ”Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures”.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): ”Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers”.

— [25] IETF Token Status List (TSL), draft-ietf-oauth-status-list-20: ”Token Status List”, 20. huhtikuuta 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: Kun henkilön tunnistetiedoissa, hyväksytyissä sähköisissä attribuuttitodistuksissa tai virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamissa tai sen puolesta tarjotuissa sähköisissä attribuuttitodistuksissa käytetään statuselementtiä, sen on osoitettava ainoastaan, onko todistus peruutettu vai ei, eikä se saa tukea muita statusarvoja, kuten ”peruutettu väliaikaisesti” -arvoa.

— EAA-4.2.11.1-06.1: Jos todistus peruutetaan, se on peruutettava pysyvästi.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: Lyhytaikaisia sähköisiä attribuuttitodistuksia, joiden voimassaoloaika on enintään 24 tuntia, ei tarvitse peruuttaa.

4) 4.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

— PuB-EAA-4.6.2-03: tyhjä.

— PuB-EAA-4.6.2-04: tyhjä.

— PuB-EAA-4.6.3-03: Virallisesta lähteestä vastaavan julkisen elimen myöntämän tai sen puolesta myönnetyn sähköisen attribuuttitodistuksen (’PuB-EAA’) digitaalisen allekirjoituksen olisi sisällettävä PuB-EAA:n digitaalista allekirjoitusta tukeva hyväksytty varmenne.

— PuB-EAA-4.6.3-04: PuB-EAA:n digitaalista allekirjoitusta tukevan hyväksytyn varmenteen on täytettävä standardin ETSI TS 119 412-6 v1.1.1 lausekkeen 8 vaatimukset, ja sen on sisällettävä standardissa ETSI EN 319 412-5 v2.5.1 määritelty ’QcType QcStatement’, jonka arvo ’id-etsi-qct-eidaspsbeaa’ määritellään seuraavasti:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- 45 f artiklan 1 kohdan b alakohdassa tarkoitettu varmenne, joka tukee asetuksen (EU) N:o 910/2014 3 artiklan 46 alakohdassa tarkoitettua julkisen sektorin elimen hyväksyttyä sähköistä allekirjoitusta tai hyväksyttyä sähköistä leimaa.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: tyhjä.

— EAA-5.2.10.1-05: tyhjä.

— EAA-5.2.10.1-06: Statusjäsen voi sisältää IETF draft-ietf-oauth-status-list-20:n [25] kohdassa 6.2 määritellyn status_list-jäsenen.

— EAA-5.2.10.1-07: tyhjä.

— EAA-5.2.10.1-08: tyhjä.

— EAA-5.2.10.1-09: tyhjä.

— EAA-5.2.10.1-10: tyhjä.

— EAA-5.2.10.1-11: tyhjä.

— EAA-5.2.10.1-12: tyhjä.

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: Jos ISO/IEC-mdoc-muodon mukaisessa sähköisessä attribuuttitodistuksessa käytetään EAA-6.2.10.1-02.2:n mukaista todistusten statusluetteloa koskevaa mekanismia tai EAA-6.2.10.1-02.3:n mukaista todistusten sulkulistaa koskevaa mekanismia, kyseisen todistuksen mobiiliturvallisuusobjektin (Mobile Security Object, MSO) on sisällettävä EAA-6.2.10.1-17:n mukainen statusrakenne, joka sisältää MSO:n peruuttamistiedot.

— EAA-6.2.10.1-01.1: Toteutettaessa tunnisteluettelomekanismia statuselementin on sisällettävä EAA-6.2.10.1-11:n mukainen 'identifier_list'-elementti.

— EAA-6.2.10.1-01.2: Toteutettaessa statusluettelomekanismia statuselementin on sisällettävä EAA-6.2.10.1-13: n mukainen 'status_list'-elementti.

— *HUOMAUTUS:*

  — Statusrakenne sisältää viittauksen MSO:n sulkulistaan.

  — MSO:n sulkulista on 'COSE_Sign1'-rakenne, joka ilmaisee, onko tietty MSO peruutettu vai ei.

  — Statusrakenne sisältää kaikki tiedot, jotka lompakkoon luottava osapuoli tarvitsee määrittääkseen, onko MSO:n sulkulista oikeellinen.

— EAA-6.2.10.1-02: Henkilön tunnistetietojen tarjoajan, hyväksyttyjen sähköisten attribuuttitodistusten tarjoajan tai virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamien tai sen puolesta tarjottujen sähköisten attribuuttitodistusten tarjoajan on käytettävä jotakin seuraavista menetelmistä henkilön tunnistetietojen, hyväksyttyjen sähköisten attribuuttitodistusten tai virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamien tai sen puolesta tarjottujen sähköisten attribuuttitodistusten peruuttamiseen:

— EAA-6.2.10.1-02.1: Jos ne myöntävät lyhytaikaisia sähköisiä attribuuttitodistuksia, joiden voimassaoloaika on enintään 24 tuntia, peruuttaminen ei ole tarpeen.

— EAA-6.2.10.1-02.2: Peruuttamistiedot koodataan statusluetteloksi käyttämällä todistusten statusluetteloa koskevaa mekanismia.

— EAA-6.2.10.1-02.2.1: Statusluetteloa koskeva mekanismi peruuttaa MSO:n sen perusteella, onko myöntäjän määrittämän bittipaikan bitti MSO:ssa määritetty todeksi statusluettelossa.

— EAA-6.2.10.1-02.2.2: Statusluetteloa koskeva mekanismi määritellään token-statusluetteloa (draft-ietf-oauth-status-list-20) koskevassa eritelmässä.

— EAA-6.2.10.1-02.3: Peruuttamistiedot koodataan tunnisteluetteloksi käyttämällä todistusten sulkulistaa koskevaa mekanismia.

— EAA-6.2.10.1-02.3.1: Tunnisteluetteloa koskeva mekanismi peruuttaa MSO:n sen perusteella, onko myöntäjän määrittämä MSO:ssa oleva tunniste tunnisteluettelossa.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 ja EAA-6.2.10.1-11 kohdissa kuvataan tunnisteluetteloa koskeva mekanismi, joka perustuu token-statusluetteloa koskevan eritelmän vaatimuksiin, mukaan lukien statusluetteloa koskevan mekanismin ja tunnisteluetteloa koskevan mekanismin yhteneväisyydet.

— EAA-6.2.10.1-03: Kun statuselementtiä käytetään henkilön tunnistetiedoissa, hyväksytyissä sähköisissä attribuuttitodistuksissa tai virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamissa tai sen puolesta tarjotuissa sähköisissä attribuuttitodistuksissa, on käytettävä ainoastaan statusta 'revoked'.

— EAA-6.2.10.1-03.1: Statusluettelon osalta tämä tarkoittaa, että ainoastaan token-statusluetteloa koskevan eritelmän mukaisten arvojen 'valid' tai 'invalid' käyttö on sallittua.

— EAA-6.2.10.1-03.2: Tunnisteluetteloon voidaan sisällyttää ainoastaan peruutetut MSO:t, toisin kuin väliaikaisesti peruutetut MSO:t.

— EAA-6.2.10.1-04: Jos MSO peruutetaan, se on peruutettava pysyvästi.

— EAA-6.2.10.1-05: Lompakkoon luottava osapuoli voi halutessaan tarkistaa MSO:n sulkulistan, ja mahdollisen tarkistamisen on oltava EAA-6.2.10.1-01 kohdassa esitetyssä token-statusluetteloa koskevassa eritelmässä ja statusrakennetta koskevassa eritelmässä määriteltyjen tarkistusvaatimusten mukainen.

— EAA-6.2.10.1-05.1: Jos lompakkoon luottavan osapuolen on voitava tarkistaa henkilön tunnistetietojen tai sähköisten attribuuttitodistusten peruutusstatus, sen on tuettava sekä todistusten statusluetteloa koskevaa mekanismia että todistusten sulkulistaa koskevaa mekanismia, jotka määritetään EAA-6.2.10.1-02 kohdassa.

— EAA-6.2.10.1-06: MSO:ssa olevat 'identifier_list' ja 'status_list' voivat sisältää varmenne-elementin.

— EAA-6.2.10.1-06.1: Jos käytetään varmenne-elementtiä, siinä on oltava sellaisen julkisen avaimen sisältävä varmenne, jolla allekirjoitettiin tai leimattiin ylimmän tason varmenne x5chain-elementissä MSO:n sulkulistarakenteessa.

— EAA-6.2.10.1-06.1.1: Lompakkoon luottavan osapuolen ilmentymän on käytettävä kyseistä varmennetta luottamusankkurina MSO:n sulkulistarakenteen x5chain-elementin tarkistamiseksi.

— EAA-6.2.10.1-06.2: Jos varmenne-elementtiä ei ole, MSO:n sulkulistarakenteen x5chain-elementin ylimmän tason varmenne on allekirjoitettava tai leimattava varmenteella, jota käytetään MSO:n x5chain-elementissä olevan varmenteen allekirjoittamiseen.

— EAA-6.2.10.1-06.2.1: Lompakkoon luottavan osapuolen ilmentymän on käytettävä kyseistä varmennetta luottamusankkurina MSO:n sulkulistarakenteen x5chain-elementin tarkistamiseksi.

— EAA-6.2.10.1-07: MSO:n sulkulista on toteutettava token-statusluetteloa koskevan eritelmän mukaisesti statusluettelo-tokenina CWT-muodossa.

— EAA-6.2.10.1-08: Tunnisteluetteloa ja statusluetteloa koskevaa mekanismiin liittyvään MSO:n sulkulistaan sovelletaan seuraavia vaatimuksia:

  — On käytettävä exp-väitettä.

  — On käytettävä ttl-väitettä.

  — IdentifierList- tai StatusList-väitteessä voidaan käyttää aggregation_uri-väitettä, ja henkilön tunnistetietojen tarjoaja, hyväksyttyjen sähköisten attribuuttitodistusten tarjoaja tai virallisesta lähteestä

vastaavan julkisen sektorin elimen tarjoamien tai sen puolesta tarjottujen sähköisten attribuuttitodistusten tarjoaja voi käyttää aggregation_uri-väitettä token-statusluetteloa koskevan eritelmän mukaisen koontimekanismin tukemisen osoittamiseksi.

— CWT:n on oltava COSE_Sign1-objekti, jossa käytetään jotakin seuraavista allekirjoitusalgoritmeista allekirjoituksen laskemiseen:

a) 'ES256' (ECDSA ja käyrä NIST P-256 ja SHA-256);

b) 'ES384' (ECDSA ja käyrä NIST P-384 ja SHA-384);

c) 'ES512' (ECDSA ja käyrä NIST P-521 ja SHA-512);

d) 'ESB256' (ECDSA ja käyrä brainpoolP256r1 ja SHA-256);

e) 'ESB384' (ECDSA ja käyrä brainpoolP384r1 ja SHA-384);

f) 'ESB512' (ECDSA ja käyrä brainpoolP512r1 ja SHA-512);

— CWT:n on sisällettävä 'x5chain' suojatussa otsikossa, joka sisältää varmenteen tai varmenneketjun MSO:n sulkulistan allekirjoituksen varmentamiseksi.

— Token-statusluetteloa koskevan eritelmän mukaisen objektitunnisteen avaimen laajennettua käyttöä voidaan hyödyntää statusluettelon ja tunnisteluettelon allekirjoitusvarmenteessa, ja lompakkoon luottavan osapuolen ilmentymät voivat tukea token-statusluetteloa koskevan eritelmän mukaisten objektitunnisteiden avaimen laajennettua käyttöä, ja hyväksyttyjen sähköisten attribuuttitodistusten tarjoaja tai virallisesta lähteestä vastaavan julkisen sektorin elimen tarjoamien tai sen puolesta tarjottujen sähköisten attribuuttitodistusten tarjoaja ei saa tehdä avaimen laajennettua käyttöä koskevasta kentästä kriittistä hyödynnettäessä token-statusluetteloa koskevan eritelmän mukaista avaimen laajennetun käytön objektitunnistetta.

— EAA-6.2.10.1-09: Token-statusluetteloa koskevan eritelmän vaatimuksista poiketen tunnisteluetteloa koskevaan mekanismiin sovelletaan seuraavia vaatimuksia:

— tyyppiväitteen arvon on oltava 'application/identifierlist+cwt';

— CWT-väitteet eivät saa sisältää StatusList-väitettä;

— EAA-6.2.10.1-11 kohdassa määritellyn IdentifierList-rakenteen on sisällyttävä väitteenä CWT-väitteisiin, jotka on määritetty käyttäen avainta 65530.

— EAA-6.2.10.1-10: IdentifierList-rakenteen on oltava CBOR-rakenne, jossa käytetään seuraavaa CDDL:ää:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: Jos käytetään IdentifierList-rakenteen tunnistetta, MSO, joka sisältää tunnisteen statuselementissä, peruutetaan.

— EAA-6.2.10.1-10.2: Aggregation_uri-väite on määritelty token-statusluetteloa koskevan eritelmän kohdassa 9.2.

— EAA-6.2.10.1-10.3: Tunnisteluettelon sisältötyypin (content-type) on oltava 'application/identifierlist+cwt', joka esitetään token-statusluetteloa kokevan eritelmän kohdan 8.2 vaatimuksissa.

— EAA-6.2.10.1-11: MSO:n identifier_list-elementtiin sovelletaan seuraavia vaatimuksia (ks. EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: identifier_list-elementti on CBOR-rakenne, jossa käytetään seuraavaa CDDL:ää:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Jotta tunnistetta ei käytettäisi korrelatiivisesti eri esityksissä, sen on oltava MSO-kohtainen.

— EAA-6.2.10.1-12: Statusluetteloon sovelletaan seuraavia vaatimuksia:

  — EAA-6.2.10.1-12.1: StatusList-rakenteen bittielementin on oltava 1.

— EAA-6.2.10.1-13: MSO:n status_list-elementtiin sovelletaan seuraavia vaatimuksia (ks. EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Status_list-elementin on täytettävä StatusListInfo-rakennetta koskevat vaatimukset, sellaisina kuin ne on määritelty token-statusluetteloa koskevassa eritelmässä, ja siihen lisätään EAA-6.2.10.1-06 kohdassa määritelty valinnainen varmenne-elementti.

  — EAA-6.2.10.1-13.2: Jotta statusindeksi ei korreloisi eri esitysten välillä, statusindeksin ja URI:n yhdistelmän on oltava MSO-kohtainen.

— EAA-6.2.10.1-14: Lompakon tarjoajan on käytettävä toista (EAA-6.2.10.1-02.2) tai kolmatta (EAA-6.2.10.1-02.3) EAA-6.2.10.1-02 kohdan mukaisista menetelmistä lompakon ilmentymää koskevan todistuksen (WIA) ja avaintodistuksen (KA) peruuttamiseen.

— EAA-6.2.10.1-15: Lompakon tarjoajan on toteuttava lompakkoratkaisussaan EAA-6.2.10.1-02 kohdan mukaiset todistuksen peruuttamista koskevat mekanismit.

— EAA-6.2.10.1-16: Henkilön tunnistetietojen tarjoajan ja sähköisten attribuuttitodistusten tarjoajan on tuettava sekä todistusten statusluetteloa koskevaa mekanismia että todistusten sulkulistaa koskevaa mekanismia, jotka kuvataan vaatimuksessa EAA-6.2.10.1-02, lompakon ilmentymää koskevan todistuksen (WIA) ja avaintodistuksen (KA) peruutusstatuksen tarkistamista varten.

— EAA-6.2.10.1-17: MSO:n statusrakenteen on oltava CBOR-rakenne, jossa käytetään seuraavaa CDDL:ää:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list' : StatusListInfo,

* tstr => RFU

}”

LIITE V

”LIITE III

10 artiklassa tarkoitetut tekniset eritelmät

— Tekniset eritelmät:

  — standardin ETSI TS 119 472-3 V1.1.1 (2026-03) kohta 4.2.5.”

LIITE VI

Muutetaan täytäntöönpanoasetuksen (EU) 2024/2979 liite IV seuraavasti:

1) Korvataan 1 kohta seuraavasti:

”1. Allekirjoituksen tai leiman pakollinen muoto:

a) PAdES (PDF Advanced Electronic Signature), sellaisena kuin se on määritelty standardissa ETSI EN 319 142-1 V1.2.1 (2024-01) ”Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures”.”

2) Korvataan 3 kohta seuraavasti:

”3. Sovellusrajapinta:
standardin ETSI TS 119 432 v1.3.1 (2026-03) kohdat 6.4.3, A.6, A.7 ja A.8.”

LIITE VII

”LIITE VI

EU:n digitaalisen identiteetin lompakon luotettavuusmerkki värillisenä



”

LIITE VIII

”LIITE VII

EU:n digitaalisen identiteetin lompakon luotettavuusmerkki mustavalkoisena



”

LIITE IX

”LIITE VIII

EU:n digitaalisen identiteetin lompakon luotettavuusmerkin tiedot

Tieto	Kuvaus	Koodaus	Tiedon pakollisuus
TrustMarkResourceURL	EU:n digitaalisen identiteetin lompakon luotettavuusmerkin graafisia elementtejä ja käyttötietoja koskevien resurssien URL-osoite lompakon käyttöliittymässä.	URL-osoite	Pakollinen
ListOfCertifiedWalletsURL	Komission täytäntöönpanoasetuksessa (EU) 2025/849 ([1]) vahvistetun EU:ssa saatavilla olevien sertifioitujen lompakkoratkaisujen julkisen luettelon URL-osoite.	URL-osoite	Pakollinen
ListOfCertifiedWalletsQRCode	QR-koodi, joka sisältää ListOfCertifiedWalletsURL:n tiedot	ISO-8859-1-merkistön mukainen QR-koodi	Valinnainen
WalletSolutionInfoPageURL	URL-osoite sertifioidun lompakkoratkaisun tietosivulle, joka on sertifioitujen lompakkoratkaisujen luetteloa koskevalla sivulla URL-osoitteessa ListOfCertifiedWalletsURL, johon on liitetty ’?’ ja lompakkoratkaisun WalletSolutionID-tunniste.	URL-osoite	Pakollinen
WalletSolutionInfoPageQRCode	QR-koodi, joka sisältää WalletSolutionInfoPageURL-osoitteen tiedot	ISO-8859-1-merkistön mukainen QR-koodi	Valinnainen
WalletVerifierToolURL*	URL-osoite, joka viittaa lompakoiden tarkistustyökalun */.well-known/openid-credential-issuer*-päätepisteeseen, jota käytetään todistusten tarjoajan metatietojen hakemiseen.	URL-osoite	Valinnainen

([1]) Komission täytäntöönpanoasetus (EU) 2025/849, annettu 6 päivänä toukokuuta 2025, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä siltä osin kuin on kyse tietojen toimittamisesta komissiolle ja yhteistyöryhmälle sertifioitujen eurooppalaisten digitaalisen identiteetin lompakoiden luetteloa varten (EUVL L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).”

LIITE X

Muutetaan täytäntöönpanoasetuksen (EU) 2024/2980 liite II seuraavasti:

1) Korvataan liitteessä II olevan 1 jakson 1 kohdan i alakohta seuraavasti:

”i) yksi tai useampi standardin ETSI EN 319 412-2 V2.4.1 (2025-06) tai standardin ETSI EN 319 412-3 V1.3.1 (2023-09) mukainen varmenne, jota voidaan käyttää rekisterinpitäjän rekisterin tietoihin luoman allekirjoituksen tai leiman todentamiseen ja jonka osalta varmennettuihin henkilöllisyystietoihin sisältyvät rekisterinpitäjän nimi ja tarvittaessa rekisterinpitäjän rekisterinumero, kuten c ja d alakohdassa esitetään;”.

2) Korvataan liitteessä II olevan 2 jakson 1 kohdan h alakohta seuraavasti:

”h) yksi tai useampi standardin ETSI EN 319 412-2 V2.4.1 (2025-06) tai standardin ETSI EN 319 412-3 V1.3.1 (2023-09) mukainen varmenne, jota voidaan käyttää lompakon tarjoajan myöntämien lompakkoyksikkötodistusten todentamiseen ja validointiin ja jonka osalta varmennettuihin henkilöllisyystietoihin sisältyvät lompakon tarjoajan nimi ja tarvittaessa rekisterinumero, kuten a ja b alakohdassa esitetään;”.

3) Korvataan liitteessä II olevan 3 jakson 1 kohdan h alakohta seuraavasti:

”h) yksi tai useampi standardin ETSI EN 319 412-2 V2.4.1 (2025-06) tai standardin ETSI EN 319 412-3 V1.3.1 (2023-09) mukainen varmenne, jota voidaan käyttää henkilön tunnistetietojen tarjoajan tarjoamiinsa henkilön tunnistetietoihin luoman allekirjoituksen tai leiman todentamiseen ja jonka osalta varmennettuihin henkilöllisyystietoihin sisältyvät henkilön tunnistetietojen tarjoajan nimi ja tarvittaessa rekisterinumero, kuten a ja b alakohdassa esitetään.”

4) Korvataan liitteessä II olevan 4 jakson 1 kohdan g alakohta seuraavasti:

”g) yksi tai useampi standardin ETSI EN 319 412-2 V2.4.1 (2025-06) tai standardin ETSI EN 319 412-3 V1.3.1 (2023-09) mukainen varmenne, jota voidaan käyttää lompakkoon luottavan osapuolen pääsyvarmenteiden tarjoajan lompakkoon luottaville osapuolille tarjoamiin pääsyvarmenteisiin luoman allekirjoituksen tai leiman todentamiseen, sekä tarvittaessa tiedot, joita tarvitaan lompakkoon luottavan osapuolen pääsyvarmenteiden erottamiseksi muista varmenteista.”

5) Lisätään liitteessä II oleva 5 jakso seuraavasti:

”5. Lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajia koskevien tietojen ilmoittaminen

1. Jäsenvaltioiden on toimitettava komissiolle lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajista seuraavat tiedot:

a) lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajan nimi;

b) tarvittaessa lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajan rekisterinumero;

c) jäsenvaltio, johon lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoaja on sijoittautunut;

d) lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajan sähköpostiosoite ja puhelinnumero asioissa, jotka liittyvät sen lompakkoon luottaville osapuolille tarjoamiin rekisteröintivarmenteisiin;

e) tarvittaessa lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajan verkkosivuston URL-osoite, joka sisältää lisätietoja tarjoajasta ja sen lompakkoon luottaville osapuolille tarjoamista rekisteröintivarmenteista;

f) sen verkkosivuston URL-osoite, joka sisältää lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajan lompakkoon luottaville osapuolille tarjoamien rekisteröintivarmenteiden tarjoamiseen ja käyttöön sovellettavat toimintaperiaatteet, ehdot ja edellytykset;

g) yksi tai useampi standardin ETSI EN 319 412-2 V2.4.1 (2025-06) tai standardin ETSI EN 319 412-3 V1.3.1 (2023-09) mukainen varmenne, jota voidaan käyttää lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajan lompakkoon luottaville osapuolille tarjoamiin rekisteröintivarmenteisiin luoman allekirjoituksen tai leiman todentamiseen, sekä tarvittaessa tiedot, joita tarvitaan lompakkoon luottavan osapuolen rekisteröintivarmenteiden erottamiseksi muista varmenteista.

2. Edellä 1 kohdassa tarkoitetut tiedot on toimitettava kustakin lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoajasta.”

LIITE XI

”LIITE I

4 artiklassa tarkoitetut protokollat ja rajapinnat

Sovelletaan teknistä eritelmää ETSI TS 119 472-3 V1.1.1 (2026-03) seuraavin mukautuksin:

1) 4.1 General requirements

— GEN-REQ-4.1-05: Tyhjä

— *HUOMAUTUS:* Tyhjä

2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: Yhden issuer_info-taulukkoparametrin elementeistä on sisällettävä henkilön tunnistetietojen (PID) / sähköisten attribuuttitodistusten (EAA) tarjoajan rekisteröintivarmenne.

— ISS-MDATA-REG_CERT-4.2.3-07: tyhjä

— ISS-MDATA-REG_CERT-4.2.3-08: tyhjä

— ISS-MDATA-REG_CERT-4.2.3-09: tyhjä

— ISS-MDATA-REG_CERT-4.2.3-10: tyhjä

— ISS-MDATA-REG_CERT-4.2.3-11: tyhjä

— ISS-MDATA-REG_CERT-4.2.3-12: tyhjä

— ISS-MDATA-REG_CERT-4.2.3-13: tyhjä

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Jos id-jäsenen arvo on ’arf_annex_ii’ ja nimiöön ’details’ yhdistetty taulukko sisältää arvon ’once_only’ tai arvon ’per-relying-party’, JSON-objektin, joka sisältää tämän nimiöön ’details’ yhdistetyn taulukon, on sisällettävä myös nimiöön ’reissue_trigger_unused’ yhdistetty JSON-numero.

4) Liitettä A ei sovelleta.”

LIITE XII

”LIITE II

5 artiklassa tarkoitetut tekniset eritelmät

Sovelletaan standardin ISO/IEC 18013-7:2025 liitteessä C olevaa teknistä eritelmää.

Sovelletaan standardin ETSI TS 119 472-2 V1.2.1 (2026-03) kohdissa 4.1, 4.2, 5 ja 6 olevia teknisiä eritelmiä seuraavin mukautuksin, mukaan lukien uuden kohdan 4.3 lisääminen:

1) 1 Scope

— Tässä asiakirjassa määritetään kaksi protokollaprofiilia, joiden avulla luottavat osapuolet (jäljempänä RP) voivat pyytää eurooppalaiselta digitaalisen identiteetin lompakolta sähköisten attribuuttitodistusten esityksiä (Electronic Attestation of Attributes Presentation, EAAP) tai henkilön tunnistetietoja (jäljempänä PID) ja eurooppalainen digitaalisen identiteetin lompakko voi lähettää pyydetyt EAAP:t tai PID:t RP:lle. Kumpikin profiileista tukee seuraavaa kahta siirtomekanismia eli API-välitteistä mekanismia ja muuta kuin API-välitteistä mekanismia, jotka kuvataan alla:

a) Profiili perustuu seuraaviin:

— standardi ISO/IEC 18013-5 [10] ainoastaan muun kuin API-välitteisen siirtomekanismin osalta ja

— standardin ISO/IEC 18013-7 [16] liite C API-välitteisen siirtomekanismin osalta.

Profiili on nimetty ISO/IEC-mdoc-profiiliksi, ja se määritellään tämän asiakirjan 5 kohdassa.

b) Profiili perustuu seuraavaan:

OpenID4VC-HAIP [11] sekä API-välitteisen siirtomekanismin että muun kuin API-välitteisen siirtomekanismin osalta seuraavasti:

— eritelmän [11] kohdat 5, 5.1, 5.3, 7 ja 8 uudelleenohjausten (Redirects) kautta tapahtuvan siirron tai muun kuin API-välitteisen siirtomekanismin osalta ja

— eritelmän [11] kohdat 5, 5.2, 5.3, 7 ja 8 API-välitteisen siirtomekanismin osalta.

Tämän profiili on nimetty OpenID4VC-HAIP-profiiliksi, ja se määritellään tämän asiakirjan 6 kohdassa.

2) 2.1 Normative references

— [15] ISO 639: ”Language code”.

— [16] ISO/IEC 18013-7:2025 ”Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions”.

3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: tyhjä.

4) 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: tyhjä.

— *Note2:* tyhjä.

— EAAP-ISO/IEC-mdoc-02: tyhjä.

5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: Eurooppalaisen digitaalisen identiteetin lompakon on tuettava välittäjä-API:a, joka tukee sekä eritelmän [11] kohdassa 5.2 että standardin [16] liitteessä C määriteltyä protokollaa.

— *HUOMAUTUS:* Jos laite, johon eurooppalainen digitaalisen identiteetin lompakko on asennettu, ei tue molempia protokollia, tätä vaatimusta ei voida täyttää ja se aiheuttaa vaatimustenvastaisuuden johtuen siitä, että taustalla olevissa käyttöjärjestelmissä ja selaimissa ei ole toteutettu tarvittavia yhteentoimivuusominaisuuksia.

— EAAP-API-GEN-02: Eurooppalaisen digitaalisen identiteetin lompakon on tuettava välittäjä-API:a ainakin täytäntöönpanoasetuksessa (EU) 2025/1569 määriteltyyn järjestelmien luetteloon rekisteröityjen PID- ja EAA-tyyppien osalta ja vähintään kaikissa täytäntöönpanoasetuksen (EU) 2024/2979 liitteessä II määritellyissä muodoissa.

— *HUOMAUTUS 1:* Tätä vaatimusta ei voida täyttää, jos taustalla oleva käyttöjärjestelmä, selain, välittäjä-API tai mikä tahansa muu tekninen kerros, joka ei ole eurooppalaisen digitaalisen identiteetin lompakon hallittavissa, rajoittaa, suodattaa, esivalitsee tai muulla tavoin rajoittaa valtuustietojen muotoja ja järjestelmien luetteloon rekisteröityjä PID- ja EAA-tyyppejä. Jos tällainen rajoitus estää eurooppalaista digitaalisen identiteetin lompakkoa tukemasta rekisteröityä valtuustietotyyppiä tai -muotoa, tästä seuraavan vaatimustenvastaisuuden voidaan katsoa johtuvan siitä, että kyseiset taustalla olevat käyttöjärjestelmät, selaimet, välittäjä-API:t tai muut asiaankuuluvat tekniset kerrokset eivät pysty tarjoamaan tarvittavia yhteentoimivuusominaisuuksia.

6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: Eurooppalaisen digitaalisen identiteetin lompakon on validoitava pyynnössä vastaanotettu lompakkoon luottavan osapuolen rekisteröintivarmenne ennen pyydetyn PID:n tai sähköisen attribuuttitodistuksen esittämistä lompakon käyttäjälle hyväksyntää varten.

— WRP-VALIDATION-02: Jos lompakkoon luottavan osapuolen rekisteröintivarmenteen validointi epäonnistuu, myös silloin, kun varmenteen voimassaolo on päättynyt tai se on peruutettu, sitä ei ole myöntänyt pätevä luotettu lompakkoon luottavan osapuolen rekisteröintivarmenteiden tarjoaja tai se on virheellinen tai sitä ei voida salausteknisesti todentaa, eurooppalaisen digitaalisen identiteetin lompakon on varoitettava lompakon käyttäjää siitä, että lompakkoon luottavaa osapuolta ei voitu validoida, eikä se saa esittää pyyntöä onnistuneesti validoituna. Lompakon käyttäjän on nimenomaisesti hyväksyttävä luottavan osapuolen pyyntö. Vastaamattomuus tai valmiiksi rastitetut ruudut eivät riitä nimenomaiseen hyväksyntään.

— WRP-VALIDATION-03: Lompakon tarjoajan on määritettävä riskianalyysinsä ja turvallisuuspolitiikkansa perusteella, voiko lompakon käyttäjä ohittaa tietyt epäonnistuneet validointitarkastukset ja millä edellytyksillä.

— WRP-OVERASKING-01: Eurooppalaisen digitaalisen identiteetin lompakon on verrattava lompakkoon luottavan osapuolen pyytämiä todistuksia ja attribuutteja lompakkoon luottavan osapuolen rekisteröintivarmenteessa oleviin rekisteröityihin todistuksiin ja attribuutteihin.

— WRP-OVERASKING-02: Jos lompakkoon luottava osapuoli pyytää PID:tä tai sähköisiä attribuuttitodistuksia tai väitteitä, jotka eivät kuulu lompakkoon luottavan osapuolen rekisteröintivarmenteen piiriin, eurooppalaisen digitaalisen identiteetin lompakon on selkeästi varoitettava lompakon käyttäjää ennen tietojen luovuttamista. Varoituksessa on yksilöitävä, että lompakkoon luottava osapuoli pyytää enemmän tietoja kuin se on rekisteröinyt. Lompakon käyttäjän on nimenomaisesti hyväksyttävä luottavan osapuolen pyyntö. Vastaamattomuus tai valmiiksi rastitetut ruudut eivät riitä nimenomaiseen hyväksyntään.

— WRP-OVERASKING-03: Lompakon tarjoajan on määritettävä riskianalyysinsä, turvallisuuspolitiikkansa ja sovellettavan lainsäädännön perusteella, voiko lompakon käyttäjä jatkaa varoituksesta huolimatta, voidaanko luovuttaa ainoastaan rekisteröintivarmenteen kattama pyydettyjen tietojen osajoukko vai onko pyyntö hylättävä.

7) 5.1 Introduction

— Kohdassa 5 ja sen alakohdissa määritellään profiili protokollalle, jonka avulla RP voi pyytää eurooppalaiselta digitaalisen identiteetin lompakolta EAAP:itä tai PID:itä ja eurooppalainen digitaalisen identiteetin lompakko voi lähettää pyydetyt EAAP:t tai PID:t RP:lle käyttäen joko muuta kuin API-välitteistä siirtomekanismia, joka perustuu standardiin ISO/IEC 18013-5 [10], tai API-välitteistä siirtomekanismia, joka perustuu standardin ISO/IEC 18013-7 [16] liitteeseen C, standardissa ISO/IEC 18013-5 [10] määriteltyjen tietorakenteiden siirtämiseksi asianmukaisesti kapseloituna.

— Kohdan 5 muut osat on järjestetty seuraavasti:

— kohdassa 5.2 määritellään vaatimukset, jotka koskevat sitä, miten RP:ien ja eurooppalaisen digitaalisen identiteetin lompakon on tuettava profiilia ja siirtomekanismeja.

— kohdassa 5.3 määritetään vaatimukset, jotka koskevat muuta kuin API-välitteistä siirtomekanismia.

— kohdassa 5.4 ja sen alakohdissa määritetään vaatimukset, jotka koskevat API-välitteistä siirtomekanismia.

8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Lompakkoyksiköt, PID:ien tarjoajat, todistusten tarjoajat, lompakon tarjoajat ja luottavat osapuolet eivät saa tukea standardin ISO/IEC 18013-5 [10] mukaisia palvelimelta suoritettavia noutoja PID:ien tai attribuuttitodistusten pyytämistä ja esittämistä varten.

— ISO/IEC 18013-SUPPORT-02: Eurooppalaisen digitaalisen identiteetin lompakon on täytettävä tämän asiakirjan 5.3 ja 5.4 kohdassa määritellyt vaatimukset.

— ISO/IEC 18013-SUPPORT-04: Luottavan osapuolen olisi toteutettava tämän asiakirjan 5.4 kohdassa määritelty profiili.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Eurooppalaisille digitaalisen identiteetin lompakoille lähetettävien laitepyyntöjen on sisällettävä standardin [10] kohdan 8.3.2.1.2.1 mukainen 'requestInfo'-avain-arvopari. Tämän parin arvon on oltava tyyppiä RequestInfo.

— ISO/IEC 18013-5-REQ-05: RequestInfo-tyypin on seuraavan CDDL:ää koskevan määritelmän mukainen.

RequestInfo = {

'euWrprc': bstr ; sisältää rekisteröintivarmenteen (ks. vaatimukset jäljempänä)

}

— ISO/IEC 18013-5-REQ-06: Mainitun requestInfon-jäsenen on sisällettävä jäsen, jossa on nimiö 'euWrprc'.

— ISO/IEC 18013-5-REQ-07: 'euWrprc':n arvon on oltava CBOR-koodattu rekisteröintivarmenne.

— ISO/IEC 18013-5-REQ-08: tyhjä.

— *HUOMAUTUS 3:* tyhjä.

— ISO/IEC 18013-5-REQ-09: tyhjä.

— ISO/IEC 18013-5-REQ-10: tyhjä.

— ISO/IEC 18013-5-REQ-11: tyhjä.

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— Tässä kohdassa määritellään DeviceResponse-viestityyppiä koskevat vaatimukset, jotka koskevat molempia siirtomekanismityyppejä (API-välitteinen ja muu kuin API-välitteinen).

— *HUOMAUTUS 1:* Jos käytetään ISO/IEC 18013-5 [10] -standardiin perustuvaa muuta kuin API-välitteistä mekanismia, EAAP-vastaus on kaikilta osin tässä kohdassa kuvattu DeviceResponsen ilmentymä. Jos käytetään ISO/IEC 18013-7 [16] -standardin liitteeseen C perustuvaa API-välitteistä mekanismia, DeviceRequestin ilmentymä kapseloidaan standardin [16] liitteen C mukaisesti.

— ISO/IEC 18013-5-RESP-02: Henkilön tunnistetietojen ja sähköisten attribuuttitodistusten tarjoaja ei saa sisällyttää tietoelementtejä myöntämiensä henkilön tunnistetietojen ja sähköisten attribuuttitodistusten mobiiliturvallisuusobjektin KeyAuthorizations-hakurakenteeseen, lukuun ottamatta tietoelementtejä, jotka lompakkoon luottava osapuoli on toimittanut sen mdoc-pyynnön transaktiotiedoissa, jonka lompakkoyksikön on allekirjoitettava tai leimattava käyttäen henkilön tunnistetietojen tai sähköisten attribuuttitodistusten yksityistä avainta.

— *HUOMAUTUS 2:* Lompakkoyksiköt eivät näin ollen voi esittää laiteallekirjoitettuja tietoelementtejä lompakkoon luottaville osapuolille, paitsi lompakkoon luottavan osapuolen toimittamien tietojen allekirjoittamista varten esimerkiksi käyttäjien turvallista todentamista koskevissa käyttötapauksissa.

— *HUOMAUTUS 3:* Standardissa ISO/IEC 18013-5:2021 ei täsmennetä, miten lompakkoon luottavat osapuolet voivat sisällyttää transaktiotietoja mdoc-pyyntöön. Transaktiotiedot on sisällytettävä mdoc-pyyntöön uusien laadittavien teknisten eritelmien mukaisesti.

— ISO/IEC 18013-5-RESP-03: Henkilön tunnistetietojen tarjoajat eivät saa mahdollistaa sitä, että henkilön tunnistetietojen yksityisellä avaimella voidaan allekirjoittaa tietoelementtejä, jotka lompakkoon luottava osapuoli on toimittanut mdoc-pyynnön transaktiotiedoissa.

11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

Tässä kohdassa määritellään API-välitteistä siirtomekanismia koskevat vaatimukset, jotka liittyvät standardin [16] liitteessä C määriteltyihin vaatimuksiin.

— ISO/IEC 18013-7-API-01: API-välitteisiä esityksiä tukevan profiilin on täytettävä standardin ISO/IEC 18013-7 [16] liitteen C vaatimukset, joita täsmennetään tämän asiakirjan 5.3 ja 5.4 kohdassa.

— ISO/IEC 18013-7-API-02: Kaikkia standardin [16] liitteessä C määriteltyjä pakollisia vaatimuksia sovelletaan sellaisina, kuin niitä täsmennetään tämän asiakirjan 5.3 ja 5.4 kohdassa.

— ISO/IEC 18013-7-API-03: Kaikki standardin [16] liitteessä C määritellyt valinnaiset vaatimukset pysyvät valinnaisina, ellei tässä asiakirjassa toisin mainita.

12) 5.4.2 Additional requirements

— Tässä kohdassa täsmennetään API-välitteistä siirtomekanismia koskevat lisävaatimukset.

— ISO/IEC 18013-ADD-API-01: Eurooppalaisen digitaalisen identiteetin lompakon on oletusarvoisesti ilmoitettava kaikkien tallennettujen sähköisten attribuuttitodistusten tyyppien käytöstä välittäjä-API:lle, joka toimii standardin [16] liitteen C mukaisesti, mutta se ei saa luovuttaa attribuutteja ja niiden arvoja näissä sähköisissä attribuuttitodistuksissa.

— *HUOMAUTUS 1:* Attribuuttien arvoja koskevaa rajoitusta sovelletaan, vaikka tällainen luovuttaminen parantaisi käyttöjärjestelmän eurooppalaiselle digitaalisen identiteetin lompakolle tarjoamia palveluja, esimerkiksi todistusten valintaa välittäjä-API:n yhteydessä.

— Toteuttajat eivät voi vaikuttaa kaikkiin käyttöjärjestelmiä ja selaimia koskeviin näkökohtiin, mikä voidaan ottaa huomioon seuraavien huomautusten 2–4 mukaisesti:

— *HUOMAUTUS 2:* Selain ja/tai käyttöjärjestelmä voi käsitellä standardin [16] liitettä C tukevan luottavan osapuolen esityspyyntöä saatavilla olevien EAA:ien hakemista varten käyttäjään kohdistuvien petosten estämiseksi tai vianetsintää varten.

— *HUOMAUTUS 3:* Selaimen ja/tai käyttöjärjestelmän odotetaan käsittelevän standardin [16] liitettä C tukevan luottavan osapuolen esityspyyntöä käyttöturvallisuussyistä.

— *HUOMAUTUS 4:* Selaimen ja/tai käyttöjärjestelmän odotetaan olevan käsittelemättä standardin [16] liitettä C tukevan luottavan osapuolen esityspyyntöä markkina-analyysejä varten (myöskään toissijaisena tarkoituksena) tai selaimen ja/tai käyttöjärjestelmän sisäisiä tarkoituksia varten.

— ISO/IEC 18013-ADD-API-02: Jos eurooppalainen digitaalisen identiteetin lompakko poistaa käyttäjän pyynnöstä PID:n tai EAA:n, jotka on aiemmin luovutettu standardin [16] liitteen C mukaisesti toimivalle välittäjä-API:lle, eurooppalaisen digitaalisen identiteetin lompakon on ilmoitettava välittäjä-API:lle, että se ei enää säilytä tätä PID:tä tai EAA:ta.

— ISO/IEC 18013-ADD-API-03: Jos käyttäjä poistaa eurooppalaisen digitaalisen identiteetin lompakkonsa asennuksen, eurooppalaisen digitaalisen identiteetin lompakon on ilmoitettava standardin [16] liitteen C mukaisesti toimivalle välittäjä-API:lle, että se ei enää säilytä aiemmin luovutettuja PID:itä tai EAA:ita.

— ISO/IEC 18013-ADD-API-04: Eurooppalaisen digitaalisen identiteetin lompakon on tarjottava yleinen käyttöasetus, jolla voidaan estää tallennettujen EAA:ien luovuttaminen standardin ISO/IEC 18013-ADD-API-01 mukaisesti toimivan välittäjä-API:n kautta. Kun tämä asetus on käytössä, eurooppalainen digitaalisen identiteetin lompakko ei saa ilmoittaa API-välitteisistä esitys- tai myöntämispyynnöistä eikä vastata niihin.

— ISO/IEC 18013-ADD-API-05: Eurooppalaisen digitaalisen identiteetin lompakoiden on välittäjä-API:a käyttäen todennettava laitteiden välisissä tietovirroissa, että vuorovaikutuksessa oleva laite on fyysisesti lähellä eurooppalaisen digitaalisen identiteetin lompakkoa, käyttäen fyysisen läheisyyden tarkistamiseen suojattua, suoraa ja käyttäjän välittämää paikallista viestintäkanavaa, kuten lyhyen kantaman langatonta viestintäteknologiaa.

— *HUOMAUTUS:* CTAP 2.3 mahdollistaa BLE:n käytön fyysisen läheisyyden tarkistamiseen, ja molempien laitteiden toteuttamana se mahdollistaa myös datan siirtämisen laitteiden välillä lyhyen kantaman tiedonsiirtoteknologioiden avulla. CTAP 2.3:n mahdollistamaa paikallista viestintäkanavaa käyttäen suoritettavaa fyysisen läheisyyden tarkistusta ja tiedonsiirtoa näiden kahden laitteen välillä olisi suosittava taustalla olevissa käyttöjärjestelmissä, selaimissa, välittäjä-API:ssa tai missä tahansa muussa teknisessä kerroksessa, joka ei ole eurooppalaisen digitaalisen identiteetin lompakon hallittavissa, CTAP:n hybriditunnelipalvelujen käytön sijaan.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: Eurooppalaisen digitaalisen identiteetin lompakon on täytettävä tässä liitteessä olevassa 6.5 kohdassa esitetyt vaatimukset.

— OIDFVP-HAIP-SUPPORT-03: Eurooppalainen digitaalisen identiteetin lompakko ei saisi tukea 6.4 kohdan mukaista uudelleenohjaukseen perustuvaa mekanismia laitteiden välisiä esityskulkuja varten.

— *HUOMAUTUS 3:* Tämän mekanismin käyttö on altis hyökkäyksille, kuten istuntojen ennaltamääräämiselle. Tällaisten hyökkäysten ehkäiseminen on luottavien osapuolten tehtävä. Tämän mekanismin täytäntöönpano ei saisi johtaa vaatimusten noudattamatta jättämiseen.

— OIDFVP-HAIP-SUPPORT-05: Luottavan osapuolen on täytettävä tässä liitteessä olevassa 6.5 kohdassa esitetyt vaatimukset.

— *HUOMAUTUS 5:* tyhjä.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: Sovelletaan kaikkia HAIP:n [11] kohdissa 5, 5.3, 7 ja 8 esitettyjä pakollisia vaatimuksia.

— *HUOMAUTUS 1:* ”HAIP:n [11] kohdassa 5 esitetyillä vaatimuksilla” tarkoitetaan ainoastaan vaatimuksia, jotka esitetään suoraan kohdan 5 otsikon alapuolella. Tähän eivät sisälly kohdat 5.1, 5.2 ja 5.3.

— OIDFVP-HAIP-GEN-03: Jos tässä liitteessä muutetaan OpenID4VC-HAIP:ssä [11] esitettyä vaatimusta, sovelletaan tämän liitteen mukaista muutettua vaatimusta.

— *HUOMAUTUS 2:* Tämä mahdollistaisi esimerkiksi OpenID4VC-HAIP:n [11] valinnaisen vaatimuksen muuttamisen pakolliseksi tai pakollisten vaatimusten laajentamisen.

— OIDFVP-HAIP-GEN-04: Jos pyydetyn todistuksen muoto on standardin [10] mukainen, luottavien osapuolten ja eurooppalaisten digitaalisen identiteetin lompakoiden on noudatettava standardin [11] kohdassa 6 esitettyä ”ISO mdocs” -profiilia.

— *HUOMAUTUS 3:* Selkeyden vuoksi: HAIP:ssä esitetyllä ”ISO mdocs -profiililla” tarkoitetaan, että luottavien osapuolten ja eurooppalaisten digitaalisen identiteetin lompakoiden on noudatettava standardin [7] liitteessä B.2 esitettyjä sovellettavia vaatimuksia.

— OIDFVP-HAIP-GEN-05: Jos pyydetyn todistuksen muoto on standardin [2] mukainen, luottavien osapuolten ja eurooppalaisten digitaalisen identiteetin lompakoiden on noudatettava standardin [11] kohdassa 6 esitettyä ”IETF SD-JWT VCs” -profiilia.

— *HUOMAUTUS 4:* Selkeyden vuoksi: ”IETF SD-JWT VCs -profiililla” tarkoitetaan, että luottavien osapuolten ja eurooppalaisten digitaalisen identiteetin lompakoiden on noudatettava standardin [7] liitteessä B.3 esitettyjä vaatimuksia sekä standardin [11] kohdassa 6.1 esitettyjä vaatimuksia.

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: tyhjä

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-03: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-04: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-05: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-06: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-07: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-08: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-09: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-10: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-11: tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-12: tyhjä

— *Huomautus 2:* tyhjä

— OIDFVP-HAIP-COMMON-REQ-RO-13: Yhden verifier_info-parametrin elementeistä on sisällettävä rekisteröintivarmenne.

— OIDFVP-HAIP-COMMON-REQ-RO-23: OpenID4VP:n kohdassa 5.9.3 mainitun lehtivarmenteen, jota käytetään x509_hash Client Identifier Prefix:n kanssa, on oltava standardin ETSI TS 119 475 [14] mukainen RP:n pääsyvarmenne.

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: tyhjä.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: tyhjä.

— *HUOMAUTUS:* tyhjä.

19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: Eurooppalaisen digitaalisen identiteetin lompakon on oletusarvoisesti ilmoitettava kaikkien tallennettujen EAA-tyyppien käytöstä välittäjä-API:lle, joka toimii standardin [11] kohdan 5.2 mukaisesti, mutta se ei saa luovuttaa attribuutteja ja niiden arvoja näissä EAA:issa.

— OIDFVP-HAIP-ADD-API-04: Jos eurooppalainen digitaalisen identiteetin lompakko tukee OIDFVP-HAIP-ADD-API-01:n mukaisesti toimivaa välittäjä-API:a, sen on tarjottava yleinen käyttöasetus, jolla estetään tallennettujen EAA:ien luovuttaminen välittäjä-API:n kautta. Kun tämä asetus on otettu käyttöön luovuttamisen estämiseksi, eurooppalaisen digitaalisen identiteetin lompakon olisi seuraavaksi mahdollistettava se, että käyttäjä voi valita yksittäisiä todistuksia luovutettavaksi välittäjä-API:lle.

— OIDFVP-HAIP-ADD-API-05: Eurooppalaisen digitaalisen identiteetin lompakoiden on välittäjä-API:a käyttäen todennettava laitteiden välisissä tietovirroissa, että vuorovaikutuksessa oleva laite on fyysisesti lähellä eurooppalaisen digitaalisen identiteetin lompakkoa, käyttäen fyysisen läheisyyden tarkistamiseen suojattua, suoraa ja käyttäjän välittämää paikallista viestintäkanavaa, kuten lyhyen kantaman langatonta viestintäteknologiaa.

— *HUOMAUTUS 5:* CTAP 2.3 mahdollistaa BLE:n käytön fyysisen läheisyyden tarkistamiseen, ja molempien laitteiden toteuttamana se mahdollistaa myös datan siirtämisen laitteiden välillä lyhyen kantaman tiedonsiirtoteknologioiden avulla. CTAP 2.3:n mahdollistamaa paikallista viestintäkanavaa käyttäen suoritettavaa fyysisen läheisyyden tarkistusta ja tiedonsiirtoa näiden kahden laitteen välillä olisi suosittava taustalla olevissa käyttöjärjestelmissä, selaimissa, välittäjä-API:ssa tai missä tahansa muussa teknisessä kerroksessa, joka ei ole eurooppalaisen digitaalisen identiteetin lompakon hallittavissa, CTAP:n hybriditunnelipalvelujen käytön sijaan.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Kaikkia tässä asiakirjassa vahvistettuja vaatimuksia, joita sovelletaan standardin ISO/IEC 18013-5 mukaisiin laitepyyntö- ja laitevastausrakenteisiin (”Device Request” ja ”Device Response”), sovelletaan myös silloin, kun eurooppalainen digitaalisen identiteetin lompakko saa ISO/IEC-mdoc-esitystä koskevan pyynnön standardin [16] kohdan C.1 mukaisen API-välitteisen mekanismin kautta.”