Euroopan unionin
virallinen lehti

FI
L-sarja

2024/2981

4.12.2024

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2981,

annettu 28 päivänä marraskuuta 2024,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisten digitaalisen identiteetin lompakoiden sertifioinnin 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 c artiklan 6 kohdan,

sekä katsoo seuraavaa:

(1) Asetuksen (EU) N:o 910/2014 5 c artiklan mukaan eurooppalaiset digitaalisen identiteetin lompakot, jäljempänä 'lompakot', on sertifioitava toiminnallisuutta, kyberturvallisuutta ja tietosuojaa koskevien vaatimusten mukaisesti, jotta voidaan varmistaa korkea turvallisuustaso ja luottamus lompakoihin. Nämä sertifiointivaatimukset on yhdenmukaistettava kaikissa jäsenvaltioissa, jotta voidaan estää markkinoiden pirstoutuminen ja luoda vankka kehys.

(2) Tämän asetuksen mukaisiin henkilötietojen käsittelytoimiin sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 ([2]) ja tarvittaessa Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY ([3]).

(3) Komissio arvioi säännöllisesti uusia teknologioita, käytäntöjä, standardeja tai teknisiä eritelmiä. Jotta lompakoiden kehittämisessä ja sertifioinnissa voidaan varmistaa mahdollisimman suuri yhdenmukaistaminen jäsenvaltioiden kesken, tässä asetuksessa vahvistetut tekniset eritelmät perustuvat työhön, jota on tehty unionin yhteisestä välineistöstä eurooppalaista digitaalisen identiteetin kehystä koskevaa koordinoitua lähestymistapaa varten 3 päivänä kesäkuuta 2021 annetun komission suosituksen (EU) 2021/946 ([4]) perusteella, ja erityisesti siihen kuuluvaan arkkitehtuuriin ja viitekehykseen. Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1183 ([5]) johdanto-osan 75 kappaleen mukaan komission olisi tarkasteltava uudelleen ja tarvittaessa päivitettävä tätä täytäntöönpanoasetusta sen pitämiseksi maailmanlaajuisen kehityksen ja arkkitehtuurin ja viitekehyksen mukaisena sekä sisämarkkinoiden parhaiden käytäntöjen noudattamiseksi.

(4) Sertifiointikehykseen sisältyvien kyberturvallisuusvaatimusten noudattamisen osoittamiseksi lompakkoratkaisujen sertifioinnissa olisi viitattava Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 ([6]) nojalla perustettuihin eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin, siltä osin kuin niitä on saatavilla ja ne ovat merkityksellisiä. Jos tällaisia järjestelmiä ei ole tai ne kattavat kyberturvallisuusvaatimukset vain osittain, tässä asetuksessa vahvistetaan kansallisiin sertifiointijärjestelmiin sovellettavat yleiset vaatimukset, jotka kattavat toiminnallisuutta, kyberturvallisuutta ja tietosuojaa koskevat vaatimukset.

([1]) EUVL L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) 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).
([3]) 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).
([4]) EUVL L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/1183, annettu 11 päivänä huhtikuuta 2024, asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta (EUVL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Asetuksen (EU) N:o 910/2014 5 a artiklan 11 kohdan mukaan lompakot on sertifioitava asetuksessa (EU) N:o 910/2014 ja komission täytäntöönpanoasetuksessa (EU) 2015/1502 ([7]) vahvistetulla korkealla varmuustasolla. Tämä varmuustaso on saavutettava lompakon kokonaisratkaisulla. Tämän asetuksen nojalla jotkin lompakkoratkaisun osat voidaan sertifioida alemmalla varmuustasolla edellyttäen, että tämä on asianmukaisesti perusteltua eikä estä kokonaisratkaisua saavuttamasta korkeaa varmuustasoa.

(6) Kaikissa kansallisissa sertifiointijärjestelmissä olisi nimettävä järjestelmän omistaja, joka vastaa sertifiointijärjestelmän kehittämisestä ja ylläpidosta. Järjestelmän omistaja voi olla vaatimustenmukaisuuden arviointilaitos, valtiollinen elin tai viranomainen, toimialajärjestö, vaatimustenmukaisuuden arviointilaitosten ryhmä tai mikä tahansa asianmukainen elin, ja se voi olla eri kuin kansallisen sertifiointijärjestelmän toiminnasta vastaava elin.

(7) Sertifioinnin kohteena olisi oltava lompakkoratkaisun ohjelmistokomponentit, kuten lompakon ilmentymä. Lompakon suojattu salaussovellus, lompakon suojattu salauslaite ja alustat, joilla ohjelmistokomponentit toteutetaan, ovat osa käyttöympäristöä, mutta ne olisi sisällytettävä sertifioinnin kohteeseen vain, jos ne tarjoaa lompakkoratkaisu. Muissa tapauksissa ja erityisesti silloin, kun loppukäyttäjät tarjoavat nämä laitteet ja alustat, palveluntarjoajien olisi tehtävä oletuksia lompakkoratkaisun käyttöympäristöstä, myös näistä laitteista ja näistä alustoista, ja toteutettava toimenpiteitä sen varmistamiseksi, että nämä oletukset todennetaan käytännössä. Jotta kriittisten resurssien suojaaminen voidaan varmistaa lompakon suojatun salauslaitteen luomien, tallentamien tai käsittelemien salausavainten hallinnointiin ja suojaamiseen käytettävien laitteisto- ja järjestelmäohjelmistojen avulla, lompakon suojatun salauslaitteen on täytettävä korkeat sertifiointivaatimukset, jotka ilmenevät kansainvälisissä standardeissa, kuten komission täytäntöönpanoasetuksessa (EU) 2024/482 ([8]) vahvistetuissa yhteisissä kriteereissä ('EUCC'), tason EAL4 arvioinnissa ja kehittyneessä menetelmällisessä haavoittuvuusanalyysissa, joka on verrattavissa AVA_VAN-tasoon 5. Näitä sertifiointistandardeja olisi käytettävä viimeistään silloin, kun suoritetaan lompakoiden vaatimustenmukaisuuden sertifiointi asetuksen (EU) 2019/881 nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti.

(8) Täysin mobiileja, suojattuja ja käyttäjäystävällisiä lompakoita tukee se, että saatavilla on standardoituja ja sertifioituja luvattoman käytön estäviä ratkaisuja, kuten sulautettuja turvaelementtejä, älykorttien kaltaisia ulkoisia laitteita tai mobiililaitteisiin sulautettuja SIM-alustoja. On tärkeää varmistaa, että sulautettuja turvaelementtejä on hyvissä ajoin saatavilla kansallisia sähköisen tunnistamisen välineitä ja lompakoita varten, ja koordinoida jäsenvaltioiden toimia tällä alalla. Sen vuoksi asetuksen (EU) N:o 910/2014 46 e artiklan 1 kohdan nojalla perustetun eurooppalaisen digitaalisen identiteetin yhteistyöryhmän, jäljempänä 'yhteistyöryhmä', olisi perustettava tätä asiaa käsittelevä alaryhmä. Alaryhmän olisi kuultava asiaankuuluvia sidosryhmiä ja sovittava sulautettujen turvaelementtien saatavuutta koskevasta yhteisestä etenemissuunnitelmasta, jonka komissio ottaa huomioon asetusta (EU) N:o 910/2014 koskevassa tarkastelukertomuksessa. Lompakon käyttöönoton helpottamiseksi kansallisella tasolla komission olisi lisäksi yhteistyössä jäsenvaltioiden kanssa laadittava osana arkkitehtuuria ja viitekehystä käyttötapauksia koskeva käsikirja ja pidettävä se jatkuvasti ajan tasalla.

(9) Kansallisten sertifiointijärjestelmien sertifioinnin kohteena olisi oltava myös prosessit, joita käytetään lompakkoratkaisun tarjoamiseen ja toimintaan, vaikka näiden prosessien määrittely tai toteuttaminen olisi annettu kolmansien osapuolten tehtäväksi. Sen osoittamiseksi, että prosessit täyttävät järjestelmien vaatimukset, näyttönä voidaan käyttää varmennustietoja sillä edellytyksellä, että riippuvuusanalyysiä käytetään sen määrittämiseen, ovatko varmennustiedot riittäviä. Varmennustietoja voidaan esittää monissa eri muodoissa, kuten raporteissa ja vaatimustenmukaisuustodistuksissa, jotka voivat olla yksityisiä, kansallisia, eurooppalaisia tai kansainvälisiä, standardien tai teknisten eritelmien pohjalta. Riippuvuusanalyysin tavoitteena on arvioida lompakon komponenteista saatavilla olevien varmennustietojen laatua.

([7]) Komission täytäntöönpanoasetus (EU) 2015/1502, annettu 8 päivänä syyskuuta 2015, teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti (EUVL L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Komission täytäntöönpanoasetus (EU) 2024/482, annettu 31 päivänä tammikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä (EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Yhteistyöryhmän olisi voitava antaa lausuntoja ja suosituksia sille toimitetuista kansallisten sertifiointijärjestelmien luonnoksista tätä tarkoitusta varten perustettujen menettelyjen mukaisesti. Näiden kansallisten sertifiointijärjestelmien olisi oltava lompakkoarkkitehtuurikohtaisia, ja kutakin tuettua arkkitehtuuria varten olisi oltava erityiset profiilit.

(11) Jotta voidaan varmistaa yhteinen näkemys lompakoiden tarjontaan ja toimintaan mahdollisesti vaikuttavien kriittisimpien riskien arvioinnista ja yhdenmukainen lähestymistapa tähän arviointiin, olisi laadittava rekisteri riskeistä ja uhkista, jotka olisi otettava huomioon lompakkoratkaisuja suunniteltaessa niiden erityisestä arkkitehtuurista riippumatta. Asetuksessa (EU) N:o 910/2014 kuvatut kyberturvallisuustavoitteet, kuten lompakkoratkaisun luottamuksellisuus, eheys ja saatavuus sekä käyttäjien yksityisyys ja tietosuoja, olisi otettava huomioon määritettäessä, mitkä riskit olisi sisällytettävä rekisteriin. Tähän riskirekisteriin sisältyvien riskien ja uhkien asianmukaisen huomioon ottamisen olisi oltava osa kansallisten sertifiointijärjestelmien vaatimuksia. Jotta riskirekisteri pysyisi jatkuvasti kehittyvän uhkaympäristön tasalla, sitä olisi ylläpidettävä ja päivitettävä säännöllisesti yhteistyössä yhteistyöryhmän kanssa.

(12) Kun järjestelmien omistajat perustavat sertifiointijärjestelmiään, niiden olisi tehtävä riskinarviointi, jossa rekisterissä lueteltuja riskejä ja uhkia tarkennetaan ja täydennetään lompakkoratkaisun arkkitehtuuriin tai toteutukseen liittyvillä erityisillä riskeillä ja uhkilla. Riskinarvioinnissa olisi tarkasteltava, miten sovellettavia riskejä ja uhkia voidaan käsitellä asianmukaisesti. Lompakon tarjoajien olisi täydennettävä järjestelmän riskinarviointia, jotta voidaan tunnistaa niiden lompakoiden toteutukseen liittyvät erityiset riskit ja uhat ja ehdottaa asianmukaisia käsittelytoimenpiteitä sertifiointielimen arvioitavaksi.

(13) Sen osoittamiseksi, että lompakkoratkaisun arkkitehtuuri täyttää sovellettavat turvallisuusvaatimukset, kussakin arkkitehtuurikohtaisessa järjestelmässä tai profiilissa olisi oltava vähintään kuvaus lompakkoratkaisun arkkitehtuurista, luettelo lompakkoratkaisun arkkitehtuuriin sovellettavista turvallisuusvaatimuksista, arviointisuunnitelma sen vahvistamiseksi, että tähän arkkitehtuuriin perustuva lompakkoratkaisu täyttää kyseiset vaatimukset, sekä riskinarviointi. Kansallisissa sertifiointijärjestelmissä olisi edellytettävä, että lompakon tarjoajat osoittavat, miten niiden tarjoaman lompakkoratkaisun suunnittelu vastaa viitearkkitehtuuria ja tietyn lompakkoratkaisun turvatoimenpiteiden ja validointisuunnitelmien yksityiskohtia. Kansallisissa sertifiointijärjestelmissä olisi myös määriteltävä vaatimustenmukaisuuden arviointitoimi, jolla varmistetaan, että lompakon suunnittelu todella vastaa valitun profiilin viitearkkitehtuuria. Kansallisten sertifiointijärjestelmien olisi täytettävä asetuksen (EU) 2019/881 51 artiklassa vahvistetut vaatimukset, lukuun ottamatta sen lokitietoja koskevaa e ja f alakohtaa.

(14) Tuotteiden sertifioinnin osalta olisi sallittava yhteisiin kriteereihin perustuvan EU:n kyberturvallisuuden sertifiointijärjestelmän (EUCC) mukaisesti myönnettyjen vaatimustenmukaisuustodistusten sekä SOG-IS:n vastavuoroista tunnustamista koskevan sopimuksen puitteissa kansallisten sertifiointijärjestelmien mukaisesti myönnettyjen vaatimustenmukaisuustodistusten käyttö. Lisäksi vähemmän sensitiivisten tuotekomponenttien osalta olisi oltava sallittua käyttää muita kansallisia sertifiointijärjestelmiä, kuten määräajassa suoritettavan kyberturvallisuuden arvioinnin menetelmää koskevan standardin CEN EN 17640 mukaisesti vahvistettuja järjestelmiä.

(15) EU:n digitaalisen identiteetin lompakon luotettavuusmerkkiä, jäljempänä 'luotettavuusmerkki', olisi käytettävä osoittamaan selkeällä, yksinkertaisella ja tunnistettavalla tavalla, että lompakko on tarjottu asetuksen (EU) N:o 910/2014 mukaisesti. Sitä olisi sen vuoksi pidettävä vaatimustenmukaisuusmerkkinä kansallisten sertifiointijärjestelmien mukaisesti sertifioiduille lompakkoratkaisuille. Kansallisissa sertifiointijärjestelmissä ei pitäisi määritellä muita vaatimustenmukaisuusmerkkejä.

(16) Petosten ehkäisemiseksi kansallisissa sertifiointijärjestelmissä olisi määriteltävä toimet, jotka on toteutettava, jos esitetään vilpillisiä väitteitä järjestelmän mukaisesta sertifioinnista.

(17) Haavoittuvuusilmoitusten tehokkaan hallinnoinnin varmistamiseksi lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, tarjoajien olisi määriteltävä ja toteutettava prosessit haavoittuvuuksien vakavuuden ja mahdollisten vaikutusten arvioimiseksi. Kansallisissa sertifiointijärjestelmissä olisi vahvistettava kynnysarvo, jonka ylittyessä asiasta on ilmoitettava sertifiointielimelle. Tällainen ilmoitusvelvollisuus ei saisi vaikuttaa tietosuojalainsäädännössä vahvistettuihin ja jäsenvaltioiden tietosuojaviranomaisten asettamiin kriteereihin, jotka koskevat henkilötietojen tietoturvaloukkauksista ilmoittamista. Mahdollisia synergioita voitaisiin luoda lompakkoratkaisujen tietoturvaloukkauksia tai turvallisuuden vaarantumista koskevien pakollisten ilmoitusten ja asetuksen (EU) 2016/679 mukaisen henkilötietojen tietoturvaloukkauksista ilmoittamisen välillä. Sertifiointielimen arviointi haavoittuvuutta koskevasta vaikutusanalyysiraportista ei saisi vaikuttaa tietosuojaviranomaisen arvioon asetuksen (EU) 2016/679 35 ja 36 artiklan mukaisesta tietosuojaa koskevasta vaikutustenarvioinnista.

(18) Lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, tarjoajien olisi ilmoitettava järjestelmän omistajalle kaikista perusteista poikkeuksille, jotka koskevat lompakon suojatun salauslaitteen ja lompakon suojatun salaussovelluksen arvioinnissa edellytettyä haavoittuvuusarviointia, kuten liitteessä IV esitetään.

(19) Vaatimustenmukaisuustodistuksen peruuttamisella voi olla vakavia seurauksia, kuten kaikkien käyttöön otettujen lompakkoyksiköiden peruuttaminen. Sen vuoksi sertifiointielinten olisi harkittava peruuttamista vain, jos korjaamaton haavoittuvuus todennäköisesti vaikuttaa merkittävästi kyseessä olevan lompakkoratkaisun luotettavuuteen tai jonkin toisen lompakkoratkaisun luotettavuuteen.

(20) Kansallisten sertifiointijärjestelmien päivittämiseksi olisi otettava käyttöön erityinen prosessi, jolla hallitaan siirtymistä järjestelmien peräkkäisten versioiden välillä, erityisesti niiden toimien osalta, jotka sertifikaatin haltijan on toteutettava tulevien arviointien, ylläpidon, uudelleensertifioinnin ja erityisarviointien osalta.

(21) Läpinäkyvyyden lisäämiseksi lompakon tarjoajien olisi jaettava julkisesti lompakkoratkaisujaan koskevia turvatietoja.

(22) Jos kansallisissa sertifiointijärjestelmissä käytetään muista sertifiointijärjestelmistä tai lähteistä saatuja varmennustietoja, olisi tehtävä riippuvuusanalyysi sen todentamiseksi, että varmennusdokumentaatio, kuten varmennusraportit ja vaatimustenmukaisuustodistukset, on saatavilla ja riittävä lompakkoratkaisujen ja sen sähköisen tunnistamisen järjestelmän kannalta, jonka puitteissa niitä tarjotaan. Tämän riippuvuusanalyysin perustana olisi oltava riskinarviointi lompakkoratkaisuista ja sähköisen tunnistamisen järjestelmästä, jonka puitteissa niitä tarjotaan. Arvioinnissa olisi määritettävä, onko tietystä lompakkoratkaisusta ja sähköisen tunnistamisen järjestelmästä, jonka puitteissa sitä tarjotaan, saatavilla oleva varmennusdokumentaatio riittävä tavoiteltua arviointitasoa vastaavan varmuuden saavuttamiseksi. Arvioinnissa olisi myös päivitettävä riippuvuusanalyysi tai se olisi tarvittaessa tehtävä kokonaan uudelleen.

(23) Sertifiointielinten olisi myönnettävä vaatimustenmukaisuustodistuksia kansallisissa sertifiointijärjestelmissä yhdessä asetuksen (EU) N:o 910/2014 5 d artiklan 2 kohdan a alakohdassa tarkoitetun julkisesti saatavilla olevan sertifiointiraportin kanssa. Tähän liittyvä sertifioinnin arviointiraportti olisi asetettava yhteistyöryhmän saataville.

(24) Kansallisissa sertifiointijärjestelmissä olisi tehtävä vuosittainen valvonta-arviointi sen varmistamiseksi, että lompakoiden hallintaan ja ylläpitoon liittyvät prosessit toimivat tehokkaasti eli että ne toimivat prosessien määrittämisperiaatteissa määritellyllä tavalla. Joka toinen vuosi tehtävä haavoittuvuusarviointi on asetuksesta (EU) N:o 910/2014 johtuva vaatimus sen varmistamiseksi, että lompakkoratkaisu kattaa edelleen asianmukaisesti riskirekisterissä yksilöidyt kyberturvallisuusriskit ja -uhat, mukaan lukien uhkaympäristön mahdollinen kehitys. Valvonta-, uudelleensertifiointi- ja erityisarviointien käsitteiden olisi oltava standardin EN ISO/IEC 17021–1:2015 mukaisia.

(25) Sertifiointisykli päättyy vaatimustenmukaisuustodistuksen voimassaolon päättymiseen tai uuden vaatimustenmukaisuustodistuksen myöntämiseen onnistuneen uudelleensertifiointiarvioinnin jälkeen. Uudelleensertifiointiarviointiin olisi sisällyttävä sertifioinnin kohteen kaikkien osatekijöiden arviointi, mukaan lukien toimintatehokkuuden arviointi ja tarvittaessa haavoittuvuusarviointi. Uudelleensertifioinnin aikana olisi voitava käyttää uudelleen aiempien arviointien tuloksia niistä osatekijöistä, jotka eivät ole muuttuneet.

(26) Kun eurooppalainen kyberturvallisuuden sertifiointijärjestelmä hyväksytään, sertifiointien myöntäminen kansallisista sertifiointijärjestelmistä, joilla on sama soveltamisala, olisi lopetettava asetuksen (EU) 2019/881 57 artiklan 1 kohdassa määritellyn siirtymäkauden jälkeen.

(27) Kansallisissa sertifiointijärjestelmissä olisi hyödynnettävä olemassa olevia kehyksiä ja mahdollisuuksien mukaan käytettävä uudelleen näyttöä yhdenmukaisuuden ja yhteentoimivuuden varmistamiseksi. Jäsenvaltiot voivat tehdä sopimuksia sertifiointijärjestelmien tai niiden osien rajatylittävästä uudelleenkäytöstä. Euroopan komission ja ENISAn olisi yhteistyössä yhteistyöryhmän kanssa tuettava jäsenvaltioita niiden kansallisten sertifiointijärjestelmien kehittämisessä ja ylläpidossa, jotta voidaan varmistaa tietämyksen ja parhaiden käytäntöjen jakaminen.

(28) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([9]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 30 päivänä syyskuuta 2024.

(29) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) N:o 910/2014 48 artiklan 1 kohdassa tarkoitetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde ja soveltamisala

Tässä asetuksessa esitetään viitestandardit ja vahvistetaan eritelmät ja menettelyt sellaisen vankan kehyksen luomiseksi lompakoiden sertifiointia varten, jota päivitetään säännöllisesti teknologian ja standardien kehityksen sekä unionin yhteisestä välineistöstä eurooppalaista digitaalisen identiteetin kehystä koskevaa koordinoitua lähestymistapaa varten suosituksen (EU) 2021/946 mukaisesti tehdyn työn ja erityisesti siihen kuuluvan arkkitehtuurin ja viitekehyksen perusteella.

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) 'lompakkoratkaisulla' ohjelmistojen, laitteiden, palvelujen, asetusten ja konfiguraatioiden yhdistelmää, mukaan lukien lompakon ilmentymät, yksi tai useampi lompakon suojattu salaussovellus ja yksi tai useampi lompakon suojattu salauslaite;

2) 'järjestelmän omistajalla' organisaatiota, joka vastaa sertifiointijärjestelmän kehittämisestä ja ylläpidosta;

3) 'sertifioinnin kohteella' tuotteita, prosesseja ja palveluja tai niiden yhdistelmää, johon määriteltyjä vaatimuksia sovelletaan;

4) 'lompakon suojatulla salaussovelluksella' sovellusta, joka hallitsee kriittisiä resursseja linkittymällä lompakon suojatun salauslaitteen tarjoamiin salausteknisiin ja muihin toimintoihin ja käyttämällä näitä toimintoja;

5) 'lompakon ilmentymällä' sovellusta, joka on asennettu ja konfiguroitu lompakon käyttäjän laitteeseen tai ympäristöön ja on osa lompakkoyksikköä ja jota lompakon käyttäjä käyttää ollakseen vuorovaikutuksessa lompakkoyksikön kanssa;

([9]) 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).

6) ’lompakon suojatulla salauslaitteella’ väärinkäytöltä suojattua laitetta, joka tarjoaa lompakon suojattuun salaussovellukseen liitetyn ja sen käyttämän ympäristön kriittisten resurssien suojaamiseksi ja salaustoimintojen tarjoamiseksi kriittisten toimintojen turvallista suorittamista varten;

7) ’riskirekisterillä’ rekisteriä, joka sisältää sertifiointiprosessin kannalta merkityksellisiä tietoja tunnistetuista riskeistä;

8) ’lompakon tarjoajalla’ lompakkoratkaisuja tarjoavaa luonnollista henkilöä tai oikeushenkilöä;

9) ’sertifiointielimellä’ ulkopuolista vaatimustenmukaisuuden arviointilaitosta, joka vastaa sertifiointijärjestelmän toiminnasta;

10) ’lompakkoyksiköllä’ lompakkoratkaisun ainutlaatuista konfiguraatiota, johon kuuluvat lompakon ilmentymät, lompakon suojatut salaussovellukset ja lompakon suojatut salauslaitteet ja jonka lompakon tarjoaja tarjoaa yksittäiselle lompakon käyttäjälle;

11) ’kriittisillä resursseilla’ lompakkoyksikössä olevia tai siihen liittyviä resursseja, jotka ovat niin merkittäviä, että niiden saatavuuden, luottamuksellisuuden tai eheyden vaarantuminen erittäin vakavasti heikentäisi kykyä luottaa lompakkoyksikköön;

12) ’lompakon käyttäjällä’ käyttäjää, jonka hallinnassa lompakkoyksikkö on;

13) ’poikkeamalla’ Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 ([10]) 6 artiklan 6 alakohdassa määriteltyä poikkeamaa;

14) ’sisäänrakennetuilla tietojen luovuttamiskäytännöillä’ sääntöjä, jotka sähköisen attribuuttitodistuksen tarjoaja on sisällyttänyt sähköiseen attribuuttitodistukseen ja joissa asetetaan edellytykset lompakkoon luottavan osapuolen pääsylle sähköiseen attribuuttitodistukseen.

II LUKU

KANSALLISET SERTIFIOINTIJÄRJESTELMÄT

3 artikla

Kansallisten sertifiointijärjestelmien perustaminen

1. Jäsenvaltioiden on nimettävä järjestelmän omistaja kullekin kansalliselle sertifiointijärjestelmälle.

2. Kansallisessa sertifiointijärjestelmässä määriteltynä sertifioinnin kohteena on oltava lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmien, joiden puitteissa niitä tarjotaan, tarjonta ja toiminta.

3. Täytäntöönpanoasetuksen (EU) 2015/1502 mukaisesti sertifioinnin kohteeseen on kansallisissa sertifiointijärjestelmissä sisällyttävä seuraavat seikat:

a) ohjelmistokomponentit, mukaan lukien lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa lompakkoratkaisuja tarjotaan, asetukset ja konfiguraatiot;

b) laitteistokomponentit ja alustat, joilla b) kohdassa tarkoitetut ohjelmistokomponentit toimivat tai joihin ne tukeutuvat kriittisissä toiminnoissa, kun lompakkoratkaisu ja sähköisen tunnistamisen järjestelmä, jonka puitteissa sitä tarjotaan, tarjoaa ne suoraan tai välillisesti ja kun niiden on saavutettava kyseisten ohjelmistokomponenttien haluttu varmuustaso. Jos lompakon tarjoaja ei tarjoa laitteistokomponentteja ja alustoja, kansallisissa sertifiointijärjestelmissä on muotoiltava laitteistokomponenttien ja alustojen arviointia varten oletuksia, joiden perusteella voidaan täytäntöönpanoasetuksen (EU) 2015/1502 mukaisesti tarjota kykyä vastustaa hyökkäyksiä, joiden vakavuusaste on korkea, ja täsmennettävä arviointitoimet näiden oletusten vahvistamiseksi liitteessä IV tarkoitetulla tavalla;

([10]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) prosessit, jotka tukevat lompakkoratkaisun tarjoamista ja toimintaa, mukaan lukien asetuksen (EU) N:o 910/2014 5 a artiklassa tarkoitettu käyttösuhteen aloittamisprosessi, ja jotka kattavat ainakin rekisteröinnin, sähköisten menetelmien hallinnan ja organisoinnin täytäntöönpanoasetuksen (EU) 2015/1502 liitteessä I olevan 2.1, 2.2 ja 2.4 kohdan mukaisesti.

4. Kansallisiin sertifiointijärjestelmiin on sisällyttävä kuvaus lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, erityisestä arkkitehtuurista. Jos kansalliset sertifiointijärjestelmät kattavat useamman kuin yhden erityisen arkkitehtuurin, niissä on oltava profiili kutakin erityistä arkkitehtuuria varten.

5. Kansallisissa sertifiointijärjestelmissä on vahvistettava kunkin profiilin osalta vähintään seuraavat:

a) lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, erityinen arkkitehtuuri;

b) asetuksen (EU) N:o 910/2014 8 artiklassa vahvistettuihin varmuustasoihin liittyvät turvatoimenpiteet;

c) standardin EN ISO/IEC 17065:2012 kohdan 7.4.1 mukaisesti laadittu arviointisuunnitelma;

d) turvallisuusvaatimukset, jotka ovat tarpeen tämän asetuksen liitteessä I vahvistetussa riskirekisterissä lueteltujen kyberturvallisuusriskien ja -uhkien käsittelemiseksi vaadittuun varmuustasoon asti ja tarvittaessa asetuksen (EU) 2019/881 51 artiklassa määriteltyjen tavoitteiden saavuttamiseksi;

e) tämän kohdan b alakohdassa tarkoitettujen turvatoimenpiteiden sovittaminen arkkitehtuurin komponentteihin;

f) kuvaus siitä, miten b–c alakohdassa tarkoitetut turvatoimenpiteet, sovittaminen, turvallisuusvaatimukset ja arviointisuunnitelma antavat lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, tarjoajille mahdollisuuden puuttua riittävällä tavalla d alakohdassa tarkoitetussa riskirekisterissä yksilöityihin kyberturvallisuusriskeihin ja -uhkiin vaadittuun varmuustasoon asti sellaisen riskinarvioinnin perusteella, jossa rekisterissä lueteltuja riskejä ja uhkia tarkennetaan ja täydennetään lompakkoratkaisun arkkitehtuuriin liittyvillä erityisillä riskeillä ja uhkilla.

6. Edellä 5 kohdan c alakohdassa tarkoitetussa arviointisuunnitelmassa on lueteltava arviointitoimet, jotka on sisällytettävä lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, arviointiin.

7. Edellä 6 kohdassa tarkoitetussa arviointitoimessa on edellytettävä, että lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, tarjoajat antavat tiedot, jotka täyttävät liitteessä II luetellut vaatimukset.

4 artikla

Yleiset vaatimukset

1. Kansallisten sertifiointijärjestelmien on katettava toiminnallisuutta, kyberturvallisuutta ja tietosuojaa koskevat vaatimukset käyttämällä seuraavia sertifiointijärjestelmiä, jos ne ovat saatavilla ja sovellettavissa:

a) asetuksen (EU) 2019/881 nojalla perustetut eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät, mukaan lukien EUCC;

b) EUCC:n soveltamisalaan kuuluvat kansalliset kyberturvallisuuden sertifiointijärjestelmät täytäntöönpanoasetuksen (EU) 2024/482 49 artiklan mukaisesti.

2. Kansallisissa sertifiointijärjestelmissä voidaan lisäksi viitata seuraaviin, jos ne ovat saatavilla ja sovellettavissa:

a) muut merkitykselliset kansalliset sertifiointijärjestelmät;

b) kansainväliset, eurooppalaiset ja kansalliset standardit;

c) tekniset eritelmät, jotka täyttävät Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ([11]) liitteessä II vahvistetut vaatimukset.

3. Kansallisten sertifiointijärjestelmien on täytettävä seuraavat vaatimukset:

a) niissä on täsmennettävä standardin EN ISO/IEC 17067:2013 kohdassa 6.5 luetellut tekijät;

b) ne on toteutettava tyypin 6 järjestelminä standardin EN ISO/IEC 17067:2013 kohdan 5.3.8 mukaisesti.

4. Kansallisten sertifiointijärjestelmien on täytettävä seuraavat vaatimukset:

a) ainoastaan asetuksen (EU) N:o 910/2014 5 a artiklan 2 kohdassa tarkoitetut tarjoajat voivat saada sertifikaatteja kansallisissa sertifiointijärjestelmissä;

b) vaatimustenmukaisuusmerkkinä käytetään ainoastaan luotettavuusmerkkiä;

c) lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, tarjoajat viittaavat asetukseen (EU) N:o 910/2014 ja tähän asetukseen viitatessaan järjestelmään;

d) lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, tarjoajat täydentävät 3 artiklan 5 kohdan f alakohdassa tarkoitettua järjestelmän riskinarviointia, jotta voidaan tunnistaa niiden toteutukseen liittyvät erityiset riskit ja uhat ja ehdottaa asianmukaisia käsittelytoimenpiteitä kaikkien merkityksellisten riskien ja uhkien varalta;

e) vastuut ja oikeudelliset toimet on vahvistettu, ja niihin sisältyvät viittaukset sovellettavaan kansalliseen lainsäädäntöön, jossa määritellään vastuut ja mahdolliset oikeudelliset toimet, jos järjestelmän mukaista sertifiointia käytetään vilpillisesti.

5. Edellä 4 kohdan d alakohdassa tarkoitettu arviointi on toimitettava sertifiointielimelle arviointia varten.

5 artikla

Poikkeamien ja haavoittuvuuksien hallinta

1. Kansallisiin sertifiointijärjestelmiin on sisällyttävä poikkeamien ja haavoittuvuuksien hallintaa koskevia vaatimuksia 2–9 kohdan mukaisesti.

2. Lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, vaatimustenmukaisuustodistuksen haltijan on ilmoitettava sertifiointielimelleen ilman aiheetonta viivytystä kaikista lompakkoratkaisuun tai sähköisen tunnistamisen järjestelmään, jonka puitteissa sitä tarjotaan, kohdistuvista tietoturvaloukkauksista tai turvallisuuden vaarantumisista, jotka todennäköisesti vaikuttavat siihen, ovatko ne kansallisen sertifiointijärjestelmän vaatimusten mukaisia.

3. Vaatimustenmukaisuustodistuksen haltijan on laadittava haavoittuvuuksien hallintaa koskevat toimintaperiaatteet ja menettelyt, joissa otetaan huomioon voimassa olevissa eurooppalaisissa ja kansainvälisissä standardeissa, mukaan lukien EN ISO/IEC 30111:2019, esitetyt menettelyt, ja ylläpidettävä ja noudatettava niitä.

4. Vaatimustenmukaisuustodistuksen haltijan on ilmoitettava todistuksen myöntäneelle sertifiointielimelle lompakkoratkaisuun vaikuttavista haavoittuvuuksista ja muutoksista näiden haavoittuvuuksien ja muutosten vaikutusta koskevien määriteltyjen kriteerien perusteella.

5. Vaatimustenmukaisuustodistuksen haltijan on laadittava haavoittuvuutta koskeva vaikutusanalyysiraportti kaikista haavoittuvuuksista, jotka vaikuttavat lompakkoratkaisun ohjelmistokomponentteihin. Raportin on sisällettävä seuraavat tiedot:

a) haavoittuvuuden vaikutus sertifioituun lompakkoratkaisuun;

b) hyökkäyksen läheisyyteen tai todennäköisyyteen liittyvät mahdolliset riskit;

([11]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1025/2012, annettu 25 päivänä lokakuuta 2012, eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 98/34/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta (EUVL L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) voidaanko haavoittuvuus korjata käytettävissä olevin keinoin;

d) jos haavoittuvuus voidaan korjata käytettävissä olevin keinoin, mahdolliset keinot haavoittuvuuden korjaamiseksi.

6. Jos ilmoitusta edellytetään 4 kohdan mukaisesti, vaatimustenmukaisuustodistuksen haltijan on toimitettava 5 kohdassa tarkoitettu haavoittuvuutta koskeva vaikutusanalyysiraportti sertifiointielimelle ilman aiheetonta viivytystä.

7. Vaatimustenmukaisuustodistuksen haltijan on laadittava haavoittuvuuksien hallintaa koskevat toimintaperiaatteet, jotka täyttävät kyberkestävyyssäädöksen ([12]) liitteessä I vahvistetut vaatimukset, ja ylläpidettävä ja sovellettava niitä.

8. Kansallisissa sertifiointijärjestelmissä on vahvistettava sertifiointielimiin sovellettavat haavoittuvuuksien julkistamista koskevat vaatimukset.

9. Vaatimustenmukaisuustodistuksen haltijan on julkistettava ja rekisteröitävä lompakkoratkaisun julkisesti tiedossa olevat ja korjatut haavoittuvuudet jossakin liitteessä V tarkoitetuista verkkotietokannoista.

6 artikla

Kansallisten sertifiointijärjestelmien ylläpitäminen

1. Kansallisiin sertifiointijärjestelmiin on sisällyttävä prosessi, jossa niiden toimintaa tarkastellaan säännöllisesti. Prosessissa on pyrittävä vahvistamaan järjestelmien riittävyys ja tunnistamaan parannuksia edellyttävät näkökohdat ottaen huomioon sidosryhmiltä saatu palaute.

2. Kansallisiin sertifiointijärjestelmiin on sisällyttävä niiden ylläpitoa koskevia säännöksiä. Tähän prosessiin on sisällytettävä vähintään seuraavat vaatimukset:

a) kansallisten sertifiointijärjestelmien määrittelyn ja vaatimusten hallinnointia koskevat säännöt;

b) määräaikojen vahvistaminen sertifikaattien myöntämiselle kansallisten sertifiointijärjestelmien päivitettyjen versioiden hyväksymisen jälkeen sekä uusien että aiemmin myönnettyjen vaatimustenmukaisuustodistusten osalta;

c) kansallisten sertifiointijärjestelmien säännöllinen uudelleentarkastelu sen varmistamiseksi, että kansallisten sertifiointijärjestelmien vaatimuksia sovelletaan johdonmukaisesti, ottaen huomioon ainakin seuraavat näkökohdat:

— järjestelmän omistajalle osoitetut selvennyspyynnöt, jotka liittyvät kansallisen sertifiointijärjestelmän vaatimuksiin;

— sidosryhmiltä ja muilta asianomaisilta osapuolilta saatu palaute;

— kansallisen sertifiointijärjestelmän omistajan reagointi tietopyyntöihin;

d) kansallisten sertifiointijärjestelmien viiteversioiden kehittämiseen liittyvien viiteasiakirjojen ja -menettelyjen seurantaa koskevat säännöt, mukaan lukien vähintään siirtymäkaudet;

e) prosessi, jolla varmistetaan, että tämän asetuksen liitteessä I vahvistetussa riskirekisterissä luetellut viimeisimmät kyberturvallisuusriskit ja -uhat katetaan;

f) kansallisten sertifiointijärjestelmien muiden muutosten hallintaprosessi.

([12]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL L 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Kansallisiin sertifiointijärjestelmiin on sisällyttävä vaatimuksia, jotka koskevat arviointien suorittamista kulloinkin sertifioiduista tuotteista määrätyn ajan kuluessa järjestelmän tarkistamisesta tai sellaisten uusien eritelmien tai standardien tai niiden uusien versioiden julkistamisen jälkeen, joiden mukaisia lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, on oltava.

III LUKU

JÄRJESTELMÄN OMISTAJIA KOSKEVAT VAATIMUKSET

7 artikla

Yleiset vaatimukset

1. Järjestelmien omistajien on kehitettävä ja ylläpidettävä kansallisia sertifiointijärjestelmiä ja hallinnoitava niiden toimintaa.

2. Järjestelmän omistajat voivat antaa kaikki tai osan tehtävistään alihankintana kolmannelle osapuolelle. Kun järjestelmän omistaja antaa tehtäviä alihankintana yksityiselle osapuolelle, hänen on vahvistettava kaikkien osapuolten velvollisuudet ja vastuut sopimuksella. Järjestelmän omistajat ovat edelleen vastuussa kaikista alihankkijoidensa suorittamista alihankintana teetetyistä toimista.

3. Järjestelmän omistajien on tarvittaessa suoritettava seurantatoimensa vähintään seuraavien tietojen perusteella:

a) sertifiointielimiltä, kansallisilta akkreditointielimiltä ja asianomaisilta markkinavalvontaviranomaisilta saatavat tiedot;

b) tiedot, jotka perustuvat sen omiin tai toisen viranomaisen suorittamiin tarkastuksiin ja tutkimuksiin;

c) 15 artiklan mukaisesti vastaanotetut valitukset ja kantelut.

4. Järjestelmän omistajien on ilmoitettava yhteistyöryhmälle kansallisiin sertifiointijärjestelmiin tehdyistä tarkistuksista. Ilmoituksessa on annettava riittävät tiedot, jotta yhteistyöryhmä voi antaa suosituksia järjestelmän omistajille ja lausuntoja päivitetyistä kansallisista sertifiointijärjestelmistä.

IV LUKU

LOMPAKKORATKAISUJEN JA SÄHKÖISEN TUNNISTAMISEN JÄRJESTELMÄN, JONKA PUITTEISSA NIITÄ TARJOTAAN, TARJOAJIA KOSKEVAT VAATIMUKSET

8 artikla

Yleiset vaatimukset

1. Kansallisiin sertifiointijärjestelmiin on sisällyttävä kyberturvallisuusvaatimuksia, jotka perustuvat kustakin tuetusta erityisestä arkkitehtuurista tehtyyn riskinarviointiin. Näillä kyberturvallisuusvaatimuksilla on pyrittävä käsittelemään liitteessä I vahvistetussa riskirekisterissä yksilöityjä tunnistettuja kyberturvallisuusriskejä ja -uhkia.

2. Asetuksen (EU) N:o 910/2014 5 a artiklan 23 kohdan mukaisesti kansallisissa sertifiointijärjestelmissä on edellytettävä, että lompakkoratkaisut ja sähköisen tunnistamisen järjestelmät, joiden puitteissa niitä tarjotaan, pystyvät vastustamaan hyökkäyksiä, joiden vakavuusaste on korkea, komission täytäntöönpanoasetuksessa (EU) 2015/1502 tarkoitetulla korkealla varmuustasolla.

3. Kansallisissa sertifiointijärjestelmissä on vahvistettava turvallisuuskriteerit, joihin on sisällyttävä seuraavat vaatimukset:

a) tapauksen mukaan kyberkestävyyssäädös tai vaatimukset, jotka täyttävät asetuksen (EU) 2019/881 51 artiklassa vahvistetut turvallisuustavoitteet;

b) lompakkoratkaisun toimintaan liittyvien riskien hallintaa koskevien toimintaperiaatteiden ja menettelyjen laatiminen ja täytäntöönpano, mukaan lukien riskien tunnistaminen ja arviointi sekä tunnistettujen riskien vähentäminen;

c) muutosten hallintaan ja haavoittuvuuksien hallintaan liittyvien toimintaperiaatteiden ja menettelyjen laatiminen ja täytäntöönpano tämän asetuksen 5 artiklan mukaisesti;

d) henkilöstöhallinnon toimintaperiaatteiden ja menettelyjen laatiminen ja täytäntöönpano, mukaan lukien lompakkoratkaisun kehittämiseen tai toimintaan osallistuvan henkilöstön asiantuntemusta, luotettavuutta, kokemusta, turvallisuuskoulutusta ja pätevyyttä koskevat vaatimukset;

e) lompakkoratkaisun käyttöympäristöön liittyvät vaatimukset, myös oletukset niiden laitteiden ja alustojen turvallisuudesta, joilla lompakkoratkaisun ohjelmistokomponentit toimivat, mukaan lukien lompakon suojatut salauslaitteet, ja tapauksen ja merkityksellisyyden mukaan vaatimustenmukaisuuden arviointivaatimukset sen varmistamiseksi, että kyseiset oletukset todennetaan asianomaisilla laitteilla ja alustoilla;

f) kunkin sellaisen oletuksen osalta, jonka tueksi ei ole esitetty vaatimustenmukaisuustodistusta tai muita hyväksyttäviä varmennustietoja, kuvaus mekanismista, jota lompakon tarjoaja käyttää oletuksen seuraamiseksi, sekä perustelut sille, että mekanismi on riittävä sen varmistamiseksi, että oletus todennetaan;

g) sellaisten toimenpiteiden määrittely ja toteuttaminen, joilla varmistetaan lompakkoratkaisun kulloisenkin sertifioidun version käyttö.

4. Kansallisiin sertifiointijärjestelmiin on sisällyttävä toiminnallisia vaatimuksia, jotka liittyvät lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, jokaisen ohjelmistokomponentin päivitysmekanismeihin liitteessä III lueteltuja toimintojen osalta.

5. Kansallisissa sertifiointijärjestelmissä on edellytettävä, että sertifioinnin hakija toimittaa sertifiointielimelle tai asettaa muulla tavoin sen saataville seuraavat tiedot ja asiakirjat:

a) liitteessä IV olevassa 1 kohdassa tarkoitettuihin tietoihin liittyvä näyttö, mukaan lukien tarvittaessa lompakkoratkaisua ja sen lähdekoodia koskevat yksityiskohtaiset tiedot, mukaan lukien seuraavat:

   — *arkkitehtuuritiedot*: lompakkoratkaisun jokaisen komponentin (mukaan lukien tuote-, prosessi- ja palvelukomponentit) osalta kuvaus sen olennaisista turvallisuusominaisuuksista, myös sen ulkoisista riippuvuuksista;

   — *turvatoimenpiteet ja varmuustasot*: lompakkoratkaisun jokaisen turvatoimenpiteen osalta kuvaus toimenpiteestä ja vaaditusta varmuustasosta perustuen täytäntöönpanoasetuksen (EU) 2015/1502 liitteeseen, jossa esitetään useita teknisiä eritelmiä ja menettelyjä, joita sovelletaan sähköisen tunnistamisen menetelmissä toteutettuihin eri turvatoimenpiteisiin;

   — *turvatoimenpiteiden sovittaminen arkkitehtuurikomponentteihin*: kuvaus siitä, miten lompakon turvatoimenpiteet toteutetaan käyttäen lompakkoratkaisun eri komponentteja, ja perustelut, joissa selitetään, miksi tiettyä varmuustasoa vaaditaan ja miten turvatoimenpide toteutetaan siten, että kaikki vaaditut turvallisuusnäkökohdat ovat asianmukaisella tasolla;

   — *riskien kattamisen lähtökohdat ja perustelut*: perustelut sille, miten

      — turvatoimenpiteet sovitetaan komponentteihin,

      — ehdotettu arviointisuunnitelma soveltuu kattamaan asianmukaisesti kaikki turvatoimenpiteet,

      — turvatoimenpiteet kattavat asianmukaisella varmuustasolla riskirekisterissä yksilöidyt kyberturvallisuusriskit ja -uhkat, täydennettynä toteutukseen liittyviä erityisiä riskejä ja uhkia koskevilla turvatoimenpiteillä;

b) liitteessä V luetellut tiedot;

c) täydellinen luettelo arviointitoimien aikana näyttönä käytetyistä vaatimustenmukaisuustodistuksista ja muista varmennustiedoista;

d) muut arviointitoimien kannalta merkitykselliset tiedot.

V LUKU

SERTIFIOINTIELIMIÄ KOSKEVAT VAATIMUKSET

9 artikla

Yleiset vaatimukset

1. Sertifiointielinten on oltava Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 ([13]) nojalla nimitettyjen kansallisten akkreditointielinten standardin EN ISO/IEC 17065:2012 mukaisesti akkreditoimia edellyttäen, että ne täyttävät kansallisissa sertifiointijärjestelmissä 2 kohdan mukaisesti asetetut vaatimukset.

2. Akkreditointia varten sertifiointielinten on täytettävä kaikki seuraavat pätevyysvaatimukset:

a) yksityiskohtainen ja tekninen tietämys lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, asiaankuuluvista arkkitehtuureista sekä näiden arkkitehtuurien kannalta merkityksellisistä uhkista ja riskeistä;

b) tietämys käytettävissä olevista turvaratkaisuista ja niiden ominaisuuksista täytäntöönpanoasetuksen (EU) 2015/1502 liitteen mukaisesti;

c) tietämys niiden vaatimustenmukaisuustodistusten nojalla suoritetuista toimista, joita sovelletaan sertifioinnin kohteena olevan lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, komponentteihin;

d) yksityiskohtainen tietämys II luvun mukaisesti perustetusta sovellettavasta kansallisesta sertifiointijärjestelmästä.

3. Sertifiointielinten on suoritettava valvontatoimensa erityisesti seuraavien tietojen perusteella:

a) kansallisilta akkreditointielimiltä ja asianomaisilta markkinavalvontaviranomaisilta saatavat tiedot;

b) tiedot, jotka perustuvat niiden omiin tai toisen viranomaisen suorittamiin tarkastuksiin ja tutkimuksiin;

c) 15 artiklan mukaisesti vastaanotetut valitukset ja kantelut.

10 artikla

Alihankinta

Sertifiointielimet voivat antaa 13 artiklan mukaiset arviointitoimet alihankintana kolmansille osapuolille. Jos arviointitoimet teetetään alihankintana, kansallisissa sertifiointijärjestelmissä on vahvistettava seuraavat:

1) kaikkien sertifiointielimen alihankkijoiden, jotka suorittavat arviointitoimia, on soveltuvin osin ja suoritettavien toimien kannalta tarkoituksenmukaisella tavalla täytettävä yhdenmukaistettujen standardien vaatimukset, kuten EN ISO/IEC 17025:2017 testauksen osalta, EN ISO/IEC 17020:2012 tarkastusten osalta, EN ISO/IEC 17021–1:2015 auditoinnin osalta ja EN ISO/IEC 17029:2019 validoinnin ja todentamisen osalta;

2) sertifiointielinten on otettava vastuu kaikista muille elimille ulkoistetuista arviointitoimista ja osoitettava, että ne ovat toteuttaneet asianmukaiset toimenpiteet akkreditoinnin aikana, tarvittaessa myös käyttämällä alihankkijoidensa omaa akkreditointia;

3) missä määrin ennakkosuostumus ulkoistamiseen on saatava järjestelmän omistajilta tai asiakkaalta, jonka lompakkoratkaisua sertifiointijärjestelmässä sertifioidaan.

([13]) Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008, annettu 9 päivänä heinäkuuta 2008, tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (EUVL L 218, 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

11 artikla

Ilmoittaminen valvontaelimelle

Sertifiointielinten on ilmoitettava asetuksen (EU) N:o 910/2014 46 a artiklan 1 kohdassa tarkoitetulle valvontaelimelle lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, vaatimustenmukaisuustodistusten myöntämisestä, voimassaolon keskeyttämisestä ja peruuttamisesta.

12 artikla

Poikkeamien ja haavoittuvuuksien hallinta

1. Sertifiointielinten on ilman aiheetonta viivytystä keskeytettävä lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, vaatimustenmukaisuustodistuksen voimassaolo sen jälkeen, kun ne ovat vahvistaneet, että ilmoitettu tietoturvaloukkaus tai turvallisuuden vaarantuminen vaikuttaa siihen, onko lompakkoratkaisu tai sähköisen tunnistamisen järjestelmä, jonka puitteissa sitä tarjotaan, kansallisten sertifiointijärjestelmien vaatimusten mukainen.

2. Sertifiointielinten on peruutettava vaatimustenmukaisuustodistus, jonka voimassaolo on keskeytetty tietoturvaloukkauksen tai turvallisuuden vaarantumisen vuoksi, jos asiaa ei ole korjattu kohtuullisessa ajassa.

3. Sertifiointielinten on peruutettava vaatimustenmukaisuustodistus, jos havaittua haavoittuvuutta ei ole korjattu kohtuullisessa ajassa ja oikeasuhteisesti haavoittuvuuden vakavuuteen ja mahdolliseen vaikutukseen nähden asetuksen (EU) N:o 910/2014 5 c artiklan 4 kohdan ja 5 e artiklan 2 kohdan mukaisesti.

VI LUKU

VAATIMUSTENMUKAISUUDEN ARVIOINTITOIMET

13 artikla

Arviointitoimet

1. Kansallisiin sertifiointijärjestelmiin on sisällyttävä menetelmät ja menettelyt, joita vaatimustenmukaisuuden arviointilaitosten on käytettävä suorittaessaan arviointitoimiaan standardin EN ISO/IEC 17065:2012 mukaisesti ja joiden on katettava vähintään seuraavat näkökohdat:

a) arviointitoimien suorittamista koskevat menetelmät ja menettelyt, mukaan lukien lompakon suojattuun salauslaitteeseen liittyvät menetelmät ja menettelyt, siten kuin liitteessä IV esitetään;

b) lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, toteutuksen tarkastus riskirekisterin perusteella, siten kuin liitteessä I esitetään ja tarvittaessa täydennettynä toteutuskohtaisilla riskeillä;

c) toiminnalliset testaustoimet, jotka perustuvat teknisten eritelmien tai standardien mukaisesti määriteltyihin testisarjoihin, jos niitä on saatavilla ja ne ovat tarkoituksenmukaisia;

d) ylläpitoprosessien olemassaolon ja soveltuvuuden arviointi, mukaan lukien ainakin versioiden hallinta, päivitysten hallinta ja haavoittuvuuksien hallinta;

e) ylläpitoprosessien toimintatehokkuuden arviointi, mukaan lukien ainakin versioiden hallinta, päivitysten hallinta ja haavoittuvuuksien hallinta;

f) lompakon tarjoajan toimittama riippuvuusanalyysi, mukaan lukien menetelmät, joilla arvioidaan varmennustietojen hyväksyttävyyttä, johon on sisällyttävä liitteessä VI esitetyt tiedot;

g) haavoittuvuusarviointi asianmukaisella tasolla, mukaan lukien

— lompakkoratkaisun suunnittelun ja tarvittaessa sen lähdekoodin uudelleentarkastelu;

— sen testaaminen, että lompakkoratkaisu pystyy vastustamaan hyökkäyksiä, joiden vakavuusaste on korkea, täytäntöönpanoasetuksen (EU) 2015/1502 liitteessä olevan 2.2.1 kohdan mukaisella korkealla varmuustasolla;

h) arviointi uhkaympäristön kehityksestä ja sen vaikutuksesta siihen, miten lompakkoratkaisu kattaa riskit, jotta voidaan määrittää, mitä arviointitoimia lompakkoratkaisun eri komponenteille on tarpeellista tehdä.

2. Kansallisiin sertifiointijärjestelmiin on sisällyttävä arviointi sen määrittämiseksi, vastaako lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa kyseisiä lompakkoratkaisuja tarjotaan, toteutus 3 artiklan 5 kohdan a alakohdassa tarkoitettua arkkitehtuuria, sekä arviointi sen määrittämiseksi, vastaako yhdessä toteutuksen kanssa ehdotettu arviointisuunnitelma 3 artiklan 5 kohdan c alakohdassa tarkoitettua arviointisuunnitelmaa.

3. Kansallisissa sertifiointijärjestelmissä on vahvistettava otantasäännöt, jotta vältetään samanlaisten arviointitoimien toistaminen ja keskitytään tietylle muunnokselle ominaisiin toimiin. Otantasääntöjen on mahdollistettava toiminta- ja turvallisuustestien suorittaminen ainoastaan lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, kohdekomponentin muunnosten otokselle sekä kohdelaitteiden otokselle. Kansallisissa sertifiointijärjestelmissä on edellytettävä, että kaikki sertifiointielimet perustelevat otosten käytön.

4. Kansallisissa sertifiointijärjestelmissä on edellytettävä, että sertifiointielin arvioi lompakon suojatun salaussovelluksen liitteessä IV esitettyjen menetelmien ja menettelyjen mukaisesti.

14 artikla

Sertifiointitoimet

1. Kansallisissa sertifiointijärjestelmissä on vahvistettava vaatimustenmukaisuustodistuksen myöntämistä koskeva toimi standardin EN ISO/IEC 17067:2013 V jakson a kohdan taulukon 1 mukaisesti, mukaan lukien seuraavat näkökohdat:

a) vaatimustenmukaisuustodistuksen sisältö liitteen VII mukaisesti;

b) miten arvioinnin tulokset raportoidaan julkisessa sertifiointiraportissa, mukaan lukien vähintään tiivistelmä alustavasta tarkastus- ja validointisuunnitelmasta liitteen VIII mukaisesti;

c) sertifioinnin arviointiraportissa raportoitujen arviointitulosten sisältö, mukaan lukien liitteessä VIII esitetyt seikat.

2. Sertifioinnin arviointiraportti voidaan asettaa yhteistyöryhmän ja komission saataville.

15 artikla

Valitukset ja kantelut

Kansallisiin sertifiointijärjestelmiin on sisällyttävä menettelyt tai viittaukset sovellettavaan kansalliseen lainsäädäntöön, joissa määritellään mekanismi, jonka avulla voidaan tehokkaasti tehdä ja käsitellä sertifiointijärjestelmän toteuttamiseen tai myönnettyyn vaatimustenmukaisuustodistukseen liittyviä valituksia ja kanteluja. Näihin menettelyihin on sisällyttävä tietojen antaminen valituksen tekijälle menettelyn etenemisestä ja tehdystä päätöksestä sekä valituksen tekijälle tiedottaminen oikeudesta tehokkaisiin oikeussuojakeinoihin. Kansallisissa sertifiointijärjestelmissä on edellytettävä, että kaikki valitukset ja kantelut, joita sertifiointielin ei ole ratkaissut tai ei voi ratkaista, toimitetaan järjestelmän omistajalle arviointia ja ratkaisua varten.

16 artikla

Valvontatoimet

1. Kansallisissa sertifiointijärjestelmissä on edellytettävä, että sertifiointielimet toteuttavat valvontatoimia, joihin kuuluu prosessien valvonta-arviointi yhdistettynä satunnaistesteihin tai -tarkastuksiin.

2. Kansallisiin sertifiointijärjestelmiin on sisällyttävä järjestelmien omistajille asetettavia vaatimuksia valvoa, että sertifiointielimet noudattavat asetuksen (EU) N:o 910/2014 ja tarvittaessa kansallisten sertifiointijärjestelmien mukaisia velvoitteitaan.

3. Kansallisiin sertifiointijärjestelmiin on sisällyttävä vaatimuksia, joiden mukaan sertifiointielinten on seurattava, että

a) kansallisten sertifiointijärjestelmien mukaisesti myönnetyn vaatimustenmukaisuustodistuksen haltijat noudattavat sertifiointia koskevia velvoitteitaan asetuksen (EU) N:o 910/2014 ja kansallisten sertifiointijärjestelmien mukaisesti;

b) sertifioidut lompakkoratkaisut ovat kansallisten sertifiointijärjestelmien vaatimusten mukaisia.

17 artikla

Velvoitteiden noudattamatta jättämisen seuraukset

Kansallisissa sertifiointijärjestelmissä on esitettävä seuraukset, joita aiheutuu siitä, että sertifioitu lompakkoratkaisu ja sähköisen tunnistamisen järjestelmä, jonka puitteissa sitä tarjotaan, eivät ole tässä asetuksessa säädettyjen vaatimusten mukaisia. Näihin seurauksiin on sisällyttävä seuraavat näkökohdat:

1) sertifiointielimen velvollisuus ilmoittaa vaatimustenmukaisuustodistuksen haltijalle ja pyytää vaatimustenmukaisuustodistuksen haltijaa toteuttamaan korjaavia toimia;

2) sertifiointielimen velvollisuus ilmoittaa muille asiaankuuluville markkinavalvontaviranomaisille, jos vaatimustenvastaisuus koskee asiaa koskevaa unionin lainsäädäntöä;

3) edellytykset vaatimustenmukaisuustodistuksen haltijan korjaavien toimien toteuttamiselle;

4) edellytykset, jotka koskevat sertifiointielimen suorittamaa vaatimustenmukaisuustodistuksen voimassaolon keskeyttämistä ja vaatimustenmukaisuustodistuksen palauttamista sen jälkeen, kun vaatimustenvastaisuus on korjattu;

5) edellytykset, joiden täyttyessä sertifiointielin peruuttaa vaatimustenmukaisuustodistuksen;

6) seuraukset siitä, että sertifiointielin ei noudata kansallisen sertifiointijärjestelmän vaatimuksia.

VII LUKU

SERTIFIOINNIN ELINKAARI

18 artikla

Sertifioinnin elinkaari

1. Sertifiointielimen on arvioitava säännöllisesti kansallisten sertifiointijärjestelmien nojalla myönnettyjen vaatimustenmukaisuustodistusten voimassaoloa liitteessä IX vahvistettujen vaatimusten mukaisesti.

2. Kansallisiin sertifiointijärjestelmiin on sisällyttävä menettely lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmän, jonka puitteissa niitä tarjotaan, uudelleensertifioimiseksi vaatimustenmukaisuustodistuksen haltijan pyynnöstä ennen alkuperäisen vaatimustenmukaisuustodistuksen voimassaolon päättymistä. Uudelleensertifiointiprosessiin on sisällyttävä lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, täydellinen arviointi, mukaan lukien haavoittuvuusarviointi, liitteessä IX vahvistettujen periaatteiden mukaisesti.

3. Kansallisiin sertifiointijärjestelmiin on sisällyttävä lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, muutosten hallintaprosessi. Tähän prosessiin on sisällyttävä säännöt sen määrittämiseksi, onko muutoksesta tehtävä 4 kohdassa tarkoitettu erityisarviointi vai liitteessä IV tarkoitettu ylläpitoprosessien toimintatehokkuuden todentaminen.

4. Kansallisiin sertifiointijärjestelmiin on sisällyttävä prosessi standardin EN ISO/IEC 17065:2012 mukaisia erityisarviointeja varten. Tähän erityisarviointiprosessiin on sisällyttävä niiden toimien valinta, jotka on toteutettava erityisarvioinnin aiheuttaneeseen erityisongelmaan puuttumiseksi.

5. Kansallisissa sertifiointijärjestelmissä on vahvistettava vaatimustenmukaisuustodistuksen peruuttamista koskevat säännöt.

VIII LUKU

TIETOJEN SÄILYTTÄMINEN JA SUOJAAMINEN

19 artikla

Tietojen säilyttäminen

1. Kansallisiin sertifiointijärjestelmiin on sisällyttävä sertifiointielimille asetettavia vaatimuksia kirjanpitojärjestelmästä, joka sisältää kaikki niiden suorittamien vaatimustenmukaisuuden arviointitoimien yhteydessä tuotetut merkitykselliset tiedot, mukaan lukien lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmien, joiden puitteissa niitä tarjotaan, tarjoajien myöntämät ja vastaanottamat tiedot. Tällaiset tiedot on säilytettävä suojatusti. Tiedot voidaan säilyttää sähköisesti, ja niiden on oltava saatavilla niin kauan kuin unionin oikeudessa tai kansallisessa lainsäädännössä edellytetään ja vähintään viiden vuoden ajan kulloisenkin vaatimustenmukaisuustodistuksen peruuttamisen tai voimassaolon päättymisen jälkeen.

2. Kansallisissa sertifiointijärjestelmissä on vahvistettava vaatimukset, joiden mukaan vaatimustenmukaisuustodistuksen haltijan on säilytettävä suojatusti seuraavat tiedot tämän asetuksen soveltamiseksi tarvittavan ajan ja vähintään viiden vuoden ajan kulloisenkin vaatimustenmukaisuustodistuksen peruuttamisen tai voimassaolon päättymisen jälkeen:

a) sertifiointielimelle tai mille tahansa sen alihankkijalle sertifiointiprosessin aikana toimitetut tiedot;

b) näytekappaleet lompakkoratkaisun sertifioinnin soveltamisalaan sisällytetyistä laitteistokomponenteista.

3. Kansallisissa sertifiointijärjestelmissä on edellytettävä, että vaatimustenmukaisuustodistuksen haltija asettaa 1 kohdassa tarkoitetut tiedot pyynnöstä sertifiointielimen tai asetuksen (EU) N:o 910/2014 46 a artiklan 1 kohdassa tarkoitetun valvontaelimen saataville.

20 artikla

Tietojen suojaaminen

Kansallisissa sertifiointijärjestelmissä on edellytettävä, että kaikki henkilöt tai organisaatiot, joille myönnetään pääsy tietoihin kansallisen sertifiointijärjestelmän mukaisten toimien toteuttamisen yhteydessä, varmistavat liikesalaisuuksien ja muiden luottamuksellisten tietojen turvallisuuden ja suojaamisen sekä immateriaalioikeuksien säilyttämisen ja toteutettavat tarvittavat ja asianmukaiset tekniset ja organisatoriset toimenpiteet.

IX LUKU

LOPPUSÄÄNNÖKSET

21 artikla

Siirtyminen eurooppalaiseen kyberturvallisuuden sertifiointijärjestelmään

Tätä asetusta tarkastellaan uudelleen, kun lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmien, joiden puitteissa niitä tarjotaan, ensimmäinen eurooppalainen kyberturvallisuuden sertifiointijärjestelmä hyväksytään, jotta voidaan ottaa huomioon tällaisen eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän vaikutus lompakkoratkaisujen ja sähköisen tunnistamisen järjestelmien, joiden puitteissa niitä tarjotaan, yleiseen sertifiointiin.

22 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 28 päivänä marraskuuta 2024.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE I

EUROOPPALAISTEN DIGITAALISEN IDENTITEETIN LOMPAKOIDEN RISKIREKISTERI

Johdanto

Riskirekisterissä kuvataan tärkeimmät lompakoihin liittyvät tietoturva- ja yksityisyysriskit ja -uhat, joita on käsiteltävä riittävällä tavalla kaikissa lompakkoarkkitehtuureissa ja -toteutuksissa. **Korkean tason riskit** (I osa) liittyvät lompakoiden käyttöön käyttäjien ja luottavien osapuolten keskuudessa, ja ne ovat yhteydessä lompakoiden resursseihin kohdistuviin välittömiin uhkiin. Lisäksi määritellään joitakin lompakoihin liittyviä **järjestelmätason riskejä** (II osa), jotka yleensä johtuvat koko lompakkojärjestelmään kohdistuvien uhkien yhdistelmästä.

Riskityyppi	Riskin tunnus	Asiaan liittyvät riskinimikkeet
Lompakoihin kohdistuvat korkean tason riskit	R1	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö
	R2	Väärän sähköisen henkilöllisyyden luominen tai käyttö
	R3	Väärien attribuuttien luominen tai käyttö
	R4	Identiteettivarkaus
	R5	Tietovarkaus
	R6	Tietojen luovuttaminen
	R7	Tietojen manipulointi
	R8	Tietojen häviäminen
	R9	Luvaton tapahtuma
	R10	Tapahtuman manipulointi
	R11	Kiistäminen
	R12	Tapahtumatietojen julkistaminen
	R13	Palvelukeskeytys
	R14	Seuranta
Järjestelmään liittyvät riskit	SR1	Laaja-alainen seuranta
	SR2	Maineen vahingoittuminen
	SR3	Oikeudellisten velvoitteiden noudattamatta jättäminen

Rekisterissä yksilöidään myös lompakkoratkaisun toteutukseen kohdistuvat **tekniset uhat** (III osa). Nämä uhat ovat liittyvät korkean tason riskeille siinä mielessä, että kutakin niistä voitaisiin käyttää useiden korkean tason riskien realisoimiseen.

Uhkatyyppi	Uhkan tunnus	Asiaan liittyvät uhkanimikkeet	Uhkien alaluokat
Tekninen uhka	TT1	Fyysiset hyökkäykset	1.1 *Varkaus*
			1.2 *Tietovuoto*
			1.3 *Luvaton muuttaminen*
	TT2	Virheet ja väärät konfiguraatiot	2.1 *Tietotekniikkajärjestelmän hallinnoinnissa tehdyt virheet*
			2.2 *Sovellustason virheet tai käyttövirheet*
			2.3 *Kehittämisen aikana tehdyt virheet ja järjestelmän virheelliset konfiguraatiot*

Uhkatyyppi	Uhkan tunnus	Asiaan liittyvät uhkanimikkeet	Uhkien alaluokat
	TT3	Epäluotettavien resurssien käyttö	3.1 *Lompakon komponenttien virheellinen käyttö tai konfigurointi*
	TT4	Vikaantuminen ja toiminnan keskeytykset	4.1 *Laitteiden tai järjestelmien vika tai toimintahäiriö*
			4.2 *Resurssien menetys*
			4.3 *Tukipalvelujen menetys*
	TT5	Vihamieliset toimet	5.1 *Tietojen sieppaaminen*
			5.2 *Tietojen kalastelu ja toisena henkilönä esiintyminen*
			5.3 *Viestien toistaminen*
			5.4 *Väsytyshyökkäys*
			5.5 *Ohjelmistojen haavoittuvuudet*
			5.6 *Toimitusketjuhyökkäykset*
			5.7 *Haittaohjelmat*
			5.8 *Satunnaislukujen ennustaminen*

Rekisterissä on lisäksi luettelo **lompakoihin kohdistuvista välittömistä uhkista**, joista kukin liittyy (ei-tyhjentävään) valikoimaan riskejä (IV osa).

I OSA

Lompakoihin kohdistuvat korkean tason riskit

R1. Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö

Olemassa olevan sähköisen henkilöllisyyden luomisella tai käytöllä tarkoitetaan sellaisen sähköisen henkilöllisyyden luomista lompakkoon, joka on olemassa reaalimaailmassa ja joka on annettu toiselle käyttäjälle. Tämä riski johtaa luonteensa vuoksi identiteettivarkauden (R4) ja luvattomien tapahtumien (R9) riskiin.

R2. Väärän sähköisen henkilöllisyyden luominen tai käyttö

Väärän sähköisen henkilöllisyyden luomisella tai käytöllä tarkoitetaan sellaisen sähköisen henkilöllisyyden luomista lompakkoon, jota ei ole olemassa reaalimaailmassa.

R3. Väärien attribuuttien luominen tai käyttö

Väärien attribuuttien luomisella tai käytöllä tarkoitetaan sellaisten attribuuttien luomista tai käyttöä, joita ei voida validoida väitetyn tarjoajan myöntämiksi ja joihin ei voida luottaa.

R4. Identiteettivarkaus

Identiteettivarkaudella tarkoitetaan lompakkoyksikön luvatonta haltuunottoa tai todentamistekijöiden menetystä, joka mahdollistaa toisena henkilönä esiintymisen.

R5. Tietovarkaus

Tietovarkaudella tarkoitetaan tietojen luvatonta poimintaa. Tietovarkaus liittyy myös uhkiin, kuten tietojen sieppaamiseen (siirrettävän tiedon luvaton haltuunotto) ja salauksen purkamiseen (salattujen tietojen luvaton dekoodaus), jotka joissain tapauksissa todennäköisesti johtavat tietojen luovuttamiseen (R6).

R6. Tietojen luovuttaminen

Tietojen luovuttamisella tarkoitetaan henkilötietojen luvatonta paljastamista, mukaan lukien erityiset henkilötietojen ryhmät. Yksityisyyden loukkauksen riski on hyvin samankaltainen, kun asiaa tarkastellaan pikemminkin yksityisyyden kuin tietoturvan kannalta.

R7. Tietojen manipulointi

Tietojen manipuloinnilla tarkoitetaan tietojen luvatonta muuttamista.

R8. Tietojen häviäminen

Tietojen häviämisellä tarkoitetaan tilannetta, jossa lompakkoon tallennetut tiedot menetetään väärinkäytön tai vihamielisten toimien vuoksi. Tämä riski on usein tietojen manipulointiin (R7) tai palvelun keskeytymiseen (R13) liittyvä toissijainen riski, kun tietoja ei voida palauttaa kokonaan tai osittain.

R9. Luvaton tapahtuma

Luvattomilla tapahtumilla tarkoitetaan operatiivisia toimintoja, jotka toteutetaan ilman lompakon käyttäjän lupaa tai tämän tietämättä. Monissa tapauksissa luvaton tapahtuma voi johtaa identiteettivarkauksiin (R4) tai tietojen luovuttamiseen (R6). Se liittyy myös salausavainten väärinkäytön kaltaisiin luvattomiin tapahtumiin.

R10. Tapahtuman manipulointi

Tapahtuman manipuloinnilla tarkoitetaan lompakon toimintojen luvatonta muuttamista. Tapahtuman manipulointi on eheyteen kohdistuva hyökkäys ja liittyy tietojen eheyden loukkaamiseen.

R11. Kiistäminen

Kiistämisellä tarkoitetaan tilannetta, jossa osapuoli voi kieltää toteuttaneensa toimen tai osallistuneensa toimeen eikä muilla osapuolilla ole riittävää näyttöä tämän väitteen kumoamiseksi.

R12. Tapahtumatietojen julkistaminen

Tapahtumatietojen julkistamisella tarkoitetaan osapuolten välistä tapahtumaa koskevien tietojen julkistamista.

R13. Palvelukeskeytys

Palvelukeskeytyksellä tarkoitetaan lompakon normaalin toiminnan keskeytymistä tai heikkenemistä. Erityinen palvelukeskeytyksen muoto on käyttäjän sulkeminen palvelusta, millä tarkoitetaan sitä, että käyttäjä ei voi käyttää käyttäjätiliään tai lompakkoaan.

R14. Seuranta

Seurannalla tarkoitetaan lompakon käyttäjän toiminnan, viestinnän tai tietojen luvatonta jäljittämistä tai tarkkailua. Seuranta liittyy usein inferenssiin, millä tarkoitetaan arkaluonteisten tietojen tai henkilötietojen päättelemistä näennäisesti vaarattomista tiedoista.

II OSA

Järjestelmään liittyvät riskit

Näitä riskejä ei käytetä uhkien luettelossa, koska ne ovat yleensä seurausta useista uhista, jotka toistuvat koko järjestelmää uhkaavalla tavalla.

SR1. Laaja-alainen seuranta

Laaja-alaisella seurannalla tarkoitetaan useiden käyttäjien toiminnan jäljittämistä tai tarkkailua heidän lompakkojensa viestinnän tai tietojen avulla. Laaja-alainen seuranta liittyy usein seurantaan (R14) ja inferenssiin maailmanlaajuisessa mittakaavassa, jolloin useita käyttäjiä koskevat tiedot yhdistetään, jotta voidaan päätellä käyttäjiä koskevia arkaluonteisia tietoja tai henkilötietoja tai tunnistaa tilastollisia suuntauksia, joita voidaan käyttää uusien hyökkäysten suunnittelussa.

SR2. Maineen vahingoittuminen

Maineen vahingoittumisella tarkoitetaan organisaation tai valtion elimen maineelle aiheutuvaa haittaa. Maineen vahingoittuminen voi johtua myös muista riskeistä, kun tiedotusvälineet kertovat tietoturvaloukkauksesta tai turvapoikkeamasta ja kuvailevat organisaatiota epäsuotuisassa valossa. Maineen vahingoittuminen voi johtaa uusiin riskeihin, kuten luottamuksen menettämiseen, joka johtuu käyttäjän perustelluista epäilyistä, ja ekosysteemin menettämiseen, kun koko ekosysteemi romahtaa.

SR3. Oikeudellisten velvoitteiden noudattamatta jättäminen

Oikeudellisten velvoitteiden noudattamatta jättämisellä tarkoitetaan tilannetta, jossa asiaankuuluvia lakeja, määräyksiä tai standardeja ei voida noudattaa. Lompakon tapauksessa ratkaisun tietoturva ja yksityisyys ovat lakisääteisiä vaatimuksia, joten kaikki uhat voivat todennäköisesti johtaa jonkinlaiseen oikeudellisten velvoitteiden noudattamatta jättämiseen.

III OSA

Tekniset uhat

Kaikki tekniset uhat eivät liity tiettyihin lompakoihin kohdistuviin riskeihin, sillä monet niistä ovat keinoja, joita voitaisiin käyttää monia erilaisia riskejä vastaavien hyökkäysten toteuttamiseen.

TT1. Fyysiset hyökkäykset

1.1 *Varkaus*

Varkaudella tarkoitetaan sellaisten laitteiden varastamista, jotka voivat muuttaa lompakon asianmukaista toimintaa (jos laite varastetaan eikä lompakkoyksikköä ole suojattu riittävästi). Tämä voi olla osatekijänä monissa riskeissä, kuten identiteettivarkauksissa (R4), tietovarkauksissa (R5) ja luvattomissa tapahtumissa (R9).

1.2 *Tietovuoto*

Tietovuodolla tarkoitetaan luvatonta pääsyä tietoihin, tietojen altistumista tai tietojen jakamista sen jälkeen, kun lompakkoon on saatu fyysinen pääsy. Tämä voi olla osatekijänä erityisesti tietojen luovuttamisessa (R6) ja tietovarkauksissa (R5).

1.3 *Luvaton muuttaminen*

Luvattomalla muuttamisella tarkoitetaan lompakkoyksikön yhden tai useamman komponentin tai komponenttien, joihin lompakkoyksikkö tukeutuu, kuten käyttäjän laitteen tai sen käyttöjärjestelmän, eheyden rikkomista. Tämä voi olla osatekijänä erityisesti tietojen manipuloinnissa (R7), tietojen häviämisessä (R8) ja tapahtumien manipuloinnissa (R10). Kun luvaton muuttaminen kohdistuu ohjelmistokomponentteihin, se voi vaikuttaa moniin riskeihin.

TT2. Virheet ja väärät konfiguraatiot

2.1 *Tietotekniikkajärjestelmän hallinnoinnissa tehdyt virheet*

Tietotekniikkajärjestelmän hallinnoinnissa tehdyillä virheillä tarkoitetaan tietovuotoja, tietojen jakamista tai vahinkoja, jotka johtuvat siitä, että käyttäjät käyttävät väärin tietoteknisiä resursseja (sovelluksen ominaisuuksien puutteellinen tuntemus) tai tietotekniset resurssit on konfiguroitu tai niitä hallinnoidaan epäasianmukaisesti.

2.2 *Sovellustason virheet tai käyttövirheet*

Sovellustason virheillä tai käyttövirheillä tarkoitetaan sovelluksen toimintahäiriöitä, jotka johtuvat itse sovelluksessa olevasta virheestä tai jonkin käyttäjän (lompakon käyttäjän ja luottavan osapuolen) virheestä.

2.3 *Kehittämisen aikana tehdyt virheet ja järjestelmän virheelliset konfiguraatiot*

Kehittämisen aikana tehdyillä virheillä ja järjestelmän virheellisillä konfiguraatioilla tarkoitetaan toimintahäiriöitä tai haavoittuvuuksia, jotka johtuvat epäasianmukaisesti kehitetyistä tai konfiguroiduista tietoteknisistä resursseista tai liiketoimintaprosesseista (tietoteknisten tuotteiden riittämättömät eritelmät, puutteellinen käytettävyys, puutteellisesti suojatut rajapinnat, epäasianmukaiset toimintaperiaatteet ja menettelyt, suunnitteluvirheet).

TT3. Epäluotettavien resurssien käyttö

Epäluotettavien resurssien käytöllä tarkoitetaan toimintaa, joka johtaa tahattomiin vahinkoihin, jotka johtuvat puutteellisesti määritellyistä luottamussuhteista, kuten luottamisesta ulkopuoliseen palveluntarjoajaan ilman riittävää varmuutta.

3.1 *Lompakon komponenttien virheellinen käyttö tai konfigurointi*

Lompakon komponenttien virheellisellä käytöllä tai konfiguroinnilla tarkoitetaan lompakon komponenteille aiheutuneita tahattomia vahinkoja, jotka johtuvat lompakon käyttäjien tai puutteellisesti koulutettujen kehittäjien virheellisestä käytöstä tai konfiguroinnista tai siitä, että uhkaympäristön muutoksiin ei ole mukauduttu, tyypillisesti haavoittuvien kolmannen osapuolen komponenttien tai ajoalustojen käytön takia.

TT4. Vikaantuminen ja toiminnan keskeytykset

4.1 *Laitteiden tai järjestelmien vika tai toimintahäiriö*

Laitteiden vialla tai toimintahäiriöllä tarkoitetaan tietoteknisille resursseille aiheutuneita tahattomia vahinkoja, jotka johtuvat laitteen viasta tai toimintahäiriöstä, mukaan lukien palveluntarjoajan infrastruktuuri ja käyttäjien laitteet.

4.2 *Resurssien menetys*

Resurssien menetyksellä tarkoitetaan käyttökatkosta tai toimintahäiriötä, joka johtuu siitä, että tällaisia resursseja ei ole saatavilla, esimerkiksi huolto-osiksi.

4.3 *Tukipalvelujen menetys*

Tukipalvelujen menetyksellä tarkoitetaan käyttökatkosta tai toimintahäiriötä, joka johtuu siitä, että järjestelmän asianmukaisen toiminnan edellyttämät tukipalvelut, mukaan lukien palveluntarjoajan infrastruktuurin ja käyttäjien laitteiden verkkoyhteydet, eivät ole käytettävissä.

TT5. Vihamieliset toimet

5.1 *Tietojen sieppaaminen*

Tietojen sieppaamisella tarkoitetaan sellaisten tietojen kaappaamista, joita ei ole riittävästi suojattu siirron aikana, mukaan lukien väliintulohyökkäykset.

5.2 *Tietojen kalastelu ja toisena henkilönä esiintyminen*

Tietojen kalastelulla tarkoitetaan sellaisten tietojen sieppaamista, jotka käyttäjä on antanut vilpillisen vuorovaikutuksen seurauksena. Siihen liittyy usein toisena henkilönä esiintyminen laillisissa viestintävälineissä ja verkkosivustoilla. Nämä uhat kohdistuvat käyttäjään ja ovat tyypillisesti osatekijöinä identiteettivarkauksissa (R4) ja luvattomissa tapahtumissa (R9), usein tietovarkauksien (R5) tai tietojen luovuttamisen (R6) kautta.

5.3 *Viestien toistaminen*

Viestien toistamisella tarkoitetaan aiemmin siepattujen viestien uudelleenkäyttöä luvattomien tapahtumien suorittamiseksi, usein protokollatasolla. Tämä tekninen uhka liittyy pääasiassa luvattomiin tapahtumiin, jotka voivat tapahtumasta riippuen johtaa muihin riskeihin.

5.4 *Väsytyshyökkäys*

Väsytyshyökkäyksellä tarkoitetaan tietoturvaloukkausta, usein luottamuksellisuuden suojan rikkomista, joka tehdään toteuttamalla suuri joukko vuorovaikutustapahtumia, kunnes vastauksista saadaan arvokasta tietoa.

5.5 *Ohjelmistojen haavoittuvuudet*

Ohjelmistojen haavoittuvuuksiin liittyvä uhka on tietoturvaloukkaus, joka toteutetaan hyödyntämällä ohjelmiston haavoittuvuutta lompakon komponenteissa tai lompakon toteutuksessa käytetyissä ohjelmisto- ja laitteistokomponenteissa, mukaan lukien julkaistut haavoittuvuudet ja julkaisemattomat haavoittuvuudet (nollapäivähaavoittuvuudet).

5.6 *Toimitusketjuhyökkäykset*

Toimitusketjuhyökkäyksellä tarkoitetaan tietoturvaloukkausta, joka toteutetaan tekemällä hyökkäyksiä lompakon tarjoajan tai sen käyttäjän tavarantoimittajaan, mikä mahdollistaa uudet hyökkäykset itse lompakkoa vastaan.

5.7 *Haittaohjelmat*

Haittaohjelmalla tarkoitetaan tietoturvaloukkausta, joka tehdään käyttäen vihamielisiä sovelluksia, jotka toteuttavat ei-toivottuja ja laittomia toimia lompakossa.

5.8 *Satunnaislukujen ennustaminen*

Satunnaislukujen ennustamisella tarkoitetaan väsytyshyökkäysten mahdollistamista ennustamalla generoituja satunnaislukuja osittain tai kokonaan.

IV OSA

Lompakoihin kohdistuvat uhat

Tässä viimeisessä osassa esitetään joukko lompakoille tyypillisiä uhkaskenaarioita, jotka on sovitettu niihin liittyviin, edellä lueteltuihin keskeisiin korkean tason riskeihin. Luettelossa esitetään uhat, jotka on katettava. Luettelo ei ole kuitenkaan tyhjentävä, sillä se riippuisi suuressa määrin valitun lompakkoratkaisun arkkitehtuurista ja uhkaympäristön kehityksestä. Lisäksi lompakon tarjoaja voi riskinarvioinnin ja ehdotettujen toimenpiteiden osalta olla vastuussa ainoastaan sertifioinnin piiriin kuuluvista komponenteista (*).

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus (*)*	Riskin nimi *Uhkaan liittyvät riskit*
TR1	Hyökkääjä voi peruuttaa pseudonyymejä ilman perusteltua syytä.	Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR2	Hyökkääjä voi myöntää väärennettyjä sähköisiä henkilöllisyyksiä, joita ei ole olemassa.	Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR3	Hyökkääjä voi alkaa myöntää luvattomia henkilön tunnistetietoja.	Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR4	Hyökkääjä voi saada hallinnoijan merkitsemään väärän henkilön tunnistetietojen tarjoajan luotettujen tarjoajien luetteloon.	Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR5	Hyökkääjä voi ohittaa henkilöllisyyden todentamisen etäpalvelun.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR6	Hyökkääjä voi ohittaa fyysisen henkilöllisyyden todentamispalvelun.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR7	Hyökkääjä voi ohittaa (hyväksytyn) etävarmenteen käyttöön liittyvät henkilöllisyyden todentamispalvelut.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR8	Hyökkääjä voi saada pääsyn lompakkoon, joka ei ole sidoksissa henkilöön.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR9	Hyökkääjä voi estää tekniset ja menettelylliset tarkastukset luodakseen vääriä henkilön tunnistetietoja.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR10	Hyökkääjä voi aktivoida uuden lompakon epäkelvolla lompakon suojatulla salauslaitteella.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2)
TR11	Hyökkääjä voi ohittaa olemassa olevan sähköisen tunnistamisen menetelmän käyttöön liittyvät henkilöllisyyden todentamispalvelut.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Identiteettivarkaus (R4) / Luvaton tapahtuma (R9)
TR12	Hyökkääjä voi kiertää henkilön tunnistetietojen tarjoajan todennuksen siitä, että lompakko on käyttäjän hallinnassa, ja saada henkilön tunnistetietoja vaarantuneeseen lompakkoon, joka on hyökkääjän hallinnassa.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Identiteettivarkaus (R4) / Luvaton tapahtuma (R9)

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus* (*)	Riskin nimi *Uhkaan liittyvät riskit*
TR13	Hyökkääjä voi saada voimassa olevan henkilön tunnistetiedon lompakkoyksikköön, joka ei ole voimassa.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Identiteettivarkaus (R4) / Luvaton tapahtuma (R9)
TR14	Henkilön tunnistetietojen tarjoaja voi myöntää väärennettyjä henkilöllisyyksiä, joissa henkilöllisyys liittyy olemassa olevaan henkilöön.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Identiteettivarkaus (R4) / Luvaton tapahtuma (R9)
TR15	Hyökkääjä voi yhdistää henkilön tunnistetiedon väärään lompakkoon, koska henkilön tunnistetietojen tarjoaja ei pysty yhdistämään henkilön tunnistetietoa oikeaan lompakkoon.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Identiteettivarkaus (R4) / Luvaton tapahtuma (R9)
TR16	Hyökkääjä voi saada käyttäjän hyväksymään hyökkääjän hallinnassa olevan uuden lompakkoyksikön tai lompakon ilmentymän aktivoinnin, jolloin hyökkääjä saa hallintaansa myös todistukset.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Väärän sähköisen henkilöllisyyden luominen tai käyttö (R2) / Identiteettivarkaus (R4) / Luvaton tapahtuma (R9)
TR17	Hyökkääjä voi myöntää toisen valtion henkilön tunnistetietoja saadakseen pääsyn kohteena olevien kansalaisten dataan tai digitaalisiin resursseihin.	Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1) / Identiteettivarkaus (R4) / Luvaton tapahtuma (R9)
TR18	Hyökkääjä voi estää tekniset ja menettelylliset tarkastukset luodakseen vääriä (hyväksyttyjä) sähköisiä attribuuttitodistuksia.	Väärien attribuuttien luominen tai käyttö (R3)
TR19	Hyökkääjä voi esittää (hyväksyttyjä) sähköisiä attribuuttitodistuksia, joita ei ole validisti myönnetty tälle.	Väärien attribuuttien luominen tai käyttö (R3)
TR20	Hyökkääjä voi hyökätä lompakon salaustekniseen linkitysmekanismiin henkilön tunnistetietojen ja sellaisen (hyväksytyn) sähköisen attribuuttitodistuksen välillä, jota ei pitäisi myöntää hänelle.	Väärien attribuuttien luominen tai käyttö (R3)
TR21	Hyökkääjä voi käyttää lompakossa (hyväksyttyä) sähköistä attribuuttitodistusta, vaikka todistuksen fyysinen vastine on vanhentunut tai virheellinen.	Väärien attribuuttien luominen tai käyttö (R3)
TR22	Hyökkääjä voi kiertää (hyväksyttyjen) sähköisten attribuuttitodistusten tarjoajan todennuksen siitä, että lompakko on käyttäjän hallinnassa, ja saada (hyväksytyn) sähköisen attribuuttitodistuksen vaarantuneeseen lompakkoon, joka on hyökkääjän hallinnassa.	Väärien attribuuttien luominen tai käyttö (R3)
TR23	Hyökkääjä voi väärentää sähköisiä attribuuttitodistuksia.	Väärien attribuuttien luominen tai käyttö (R3)
TR24	Hyökkääjä voi syöttää lompakkoon väärennettyjä sähköisiä attribuuttitodistuksia.	Väärien attribuuttien luominen tai käyttö (R3)
TR25	Lompakko voi esittää attribuutteja luottavalle osapuolelle ilman käyttäjän suostumusta.	Tietojen luovuttaminen (R6)
TR26	Henkilön tunnistetiedot, (hyväksytyt) sähköiset attribuuttitodistukset tai pseudonyymit voidaan esittää väärälle luottavalle osapuolelle.	Tietojen luovuttaminen (R6)
TR27	Hyökkääjä voi käynnistää sähköisen attribuuttitodistuksen uusimisen vihamielisessä tarkoituksessa.	Tietojen luovuttaminen (R6)
TR28	Hyökkääjä voi saada käyttäjän hyväksymään virheellisesti sähköisiä attribuuttitodistuksia koskevan pyynnön (tietojen kalastelu tai muu).	Tietojen luovuttaminen (R6)

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus* (*)	Riskin nimi *Uhkaan liittyvät riskit*
TR29	Hyökkääjä voi vuotaa lompakosta attribuutteja ja tunnistaa lompakon käyttäjän, kun tunnistamista ei vaadita tai sallita.	Tietojen luovuttaminen (R6)
TR30	Hyökkääjä voi estää tekniset ja menettelylliset tarkastukset poimiakseen tietoja.	Tietojen luovuttaminen (R6)
TR31	Pyyntö voidaan vuotaa hyökkääjälle.	Tietojen luovuttaminen (R6)
TR32	Hyökkääjä voi saada tietoa attribuutteja koskevasta sisäänrakennetusta tietojen luovuttamiskäytännöstä ja esittää lompakkoyksikön kulloiseenkin pyyntöön sisältyviä attribuutteja.	Tietojen luovuttaminen (R6)
TR33	Hyökkääjä voi poimia lokitietoja tai niiden osia.	Tietojen luovuttaminen (R6)
TR34	Hyökkääjä voi tietää, onko lompakko asennettu samaan laitteeseen, jota hän käyttää, tai toiseen laitteeseen, ja saada siitä tietoa.	Tietojen luovuttaminen (R6)
TR35	Hyökkääjä voi saada haltuunsa tietotekijän, jota käytetään käyttäjän todentamiseen lompakon suojatulle salaussovellukselle.	Tietojen luovuttaminen (R6)
TR36	Henkilöä koskeva sähköinen attribuuttitodistus, joka esitetään useissa tapahtumissa luottavan osapuolen kanssa tai eri luottavien osapuolten välillä, mahdollistaa tahattomasti useiden tapahtumien yhdistämisen asianomaiseen henkilöön.	Tietojen luovuttaminen (R6)
TR37	Julkisessa todistuksen tai luottavan osapuolen peruutusluettelossa voi olla tietoa siitä, miten käyttäjä käyttää todistusta (esim. sijainti, IP-osoite jne.).	Tietojen luovuttaminen (R6)
TR38	Luottavat osapuolet eivät pysty osoittamaan käyttäjän suostumusta yhteisiin attribuutteihin, mikä voi vaikuttaa lokitietojen eheyteen.	Tietojen luovuttaminen (R6)
TR39	Hyökkääjä voi laittomasti jäljittää lompakon käyttäjän yksilöllisillä tai jäljitettävillä tunnisteilla.	Tietojen luovuttaminen (R6) / Seuranta (R14)
TR40	Luottava osapuoli, joka koostuu useista yksiköistä tai elimistä, joilla kullakin on eri kattavuus sen suhteen, mitä tietoja ne voivat pyytää tai käsitellä, voi pyytää ja käsitellä tietoja, joihin sillä ei ole laillisia perusteita.	Tietojen luovuttaminen (R6) / Luvaton tapahtuma (R9)
TR41	Hyökkääjä voi harhauttaa lompakon tekemät henkilön tunnistetietojen eheys- ja aitoustarkastukset siten, että ne antavat aina positiivisen tuloksen.	Tietojen manipulointi (R7)
TR42	Hyökkääjä voi ohittaa tai harhauttaa lompakon suorittamat tarkastukset, joilla todennetaan pyydettyjen attribuuttien eheys ja aitous, siten, että ne antavat aina positiivisen tuloksen.	Tietojen manipulointi (R7)
TR43	Hyökkääjä voi ohittaa tai harhauttaa lompakon suorittamat tarkastukset, joilla todennetaan, että kaikki pyydetyt attribuutit kuuluvat samalle käyttäjälle, siten, että ne antavat aina positiivisen tuloksen.	Tietojen manipulointi (R7)
TR44	Hyökkääjä voi ohittaa tai harhauttaa lompakon suorittamat tarkastukset, joilla todennetaan, että henkilön tunnistetieto on voimassa ja luotetun henkilön tunnistetietojen tarjoajan myöntämä, siten, että ne antavat aina positiivisen tuloksen.	Tietojen manipulointi (R7)

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus* (*)	Riskin nimi *Uhkaan liittyvät riskit*
TR45	Hyökkääjä voi ohittaa tai harhauttaa lompakon suorittamat tarkastukset, joilla todennetaan, että hyväksytty sähköinen attribuuttitodistus on voimassa ja sellaisen luotetun luottamuspalvelun tarjoajan myöntämä, joka on rekisteröity myöntämään hyväksyttyjä sähköisiä attribuuttitodistuksia, siten, että ne antavat aina positiivisen tuloksen.	Tietojen manipulointi (R7)
TR46	Hyökkääjä voi ohittaa tai harhauttaa lompakon suorittamat tarkastukset, joilla todennetaan, onko henkilön tunnistetietojen tarjoaja perunut henkilön tunnistetiedon, siten, että ne antavat aina positiivisen tuloksen.	Tietojen manipulointi (R7)
TR47	Hyökkääjä voi ohittaa tai harhauttaa lompakon suorittamat tarkastukset, joilla todennetaan, onko (hyväksyttyjen) sähköisten attribuuttitodistusten tarjoaja perunut (hyväksytyn) sähköisen attribuuttitodistuksen, siten, että ne antavat aina positiivisen tuloksen.	Tietojen manipulointi (R7)
TR48	Hyökkääjä voi muuttaa varmuuskopio- ja palautustietojen sisältöä, jonka olisi oltava yksinomaan käyttäjän hallinnassa.	Tietojen manipulointi (R7) / Tietojen häviäminen (R8)
TR49	Hyökkääjä voi muuttaa tietyn lompakon ilmentymän tapahtumahistoriaa toimintolokista.	Tietojen manipulointi (R7) / Tietojen häviäminen (R8)
TR50	Hyökkääjä voi salakuunnella yhteyttä lompakosta luottaviin osapuoliin.	Tietovarkaus (R5) / Tietojen luovuttaminen (R6)
TR51	Hyökkääjä voi vakuuttaa käyttäjän jakamaan henkilötietoja (esim. henkilön tunnistetietoja, sähköisiä attribuuttitodistuksia, sähköisiä allekirjoituksia, lokitietoja ja muita tietoja) hyökkääjän tai sellaisen kolmannen osapuolen kanssa, jonka kanssa käyttäjän ei ollut tarkoitus jakaa tietoja.	Tietovarkaus (R5) / Tietojen luovuttaminen (R6)
TR52	Hyökkääjä voi lukea tietyn lompakon ilmentymän tapahtumahistorian toimintolokista.	Tietovarkaus (R5) / Tietojen luovuttaminen (R6)
TR53	Hyökkääjä voi viedä tai poimia salausavainten aineistoa lompakon suojatun salauslaitteen ulkopuolella.	Tietovarkaus (R5) / Tietojen luovuttaminen (R6) / Luvaton tapahtuma (R9)
TR54	Hyökkääjä voi lukea varmuuskopio- ja palautustietojen sisällön, jonka olisi oltava yksinomaan käyttäjän hallinnassa.	Tietovarkaus (R5) / Tietojen luovuttaminen (R6)
TR55	Hyökkääjä voi ohittaa käyttäjän todentamismenetelmän käyttääkseen lompakkoyksikön luomaa pseudonyymiä.	Identiteettivarkaus (R4)
TR56	Hyökkääjä voi ehdottaa käyttäjille sovellusta, joka jäljittelee tiettyä laillista lompakkoa.	Identiteettivarkaus (R4)
TR57	Hyökkääjä voi viedä lompakon tietoja, mukaan lukien henkilön tunnistetiedot, (hyväksytyt) sähköiset attribuuttitodistukset tai lokitiedot.	Identiteettivarkaus (R4)
TR58	Hyökkääjä voi viedä salauksen sitomiseen liittyvää aineistoa.	Identiteettivarkaus (R4)
TR59	Hyökkääjä voi ottaa haltuun henkilöllisyyksiä lompakon salausavainten kautta.	Identiteettivarkaus (R4)
TR60	Hyökkääjä voi kopioida toisen käyttäjän henkilökohtaisen lompakkoyksikön omalle laitteelleen ja käyttää sitä.	Identiteettivarkaus (R4) / Olemassa olevan sähköisen henkilöllisyyden luominen tai käyttö (R1)

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus* (*)	Riskin nimi *Uhkaan liittyvät riskit*
TR61	Toisen valtion viranomaiset voivat pyytää käyttäjää näyttämään ja/tai jakamaan kaikki lompakon tiedot lähitilanteessa, esimerkiksi tämän ylittäessä kyseisen valtion rajan.	Identiteettivarkaus (R4) / Seuranta (R14)
TR62	Käyttäjät eivät voi siirtää tapahtumalokejaan käyttäjän laitteen toimintahäiriön jälkeen, mikä johtaa siihen, että aiempia tapahtumia ei voida jäljittää uudessa lompakossa.	Kiistäminen (R11)
TR63	Käyttäjät eivät voi palauttaa tapahtumalokejaan käyttäjän laitteen toimintahäiriön jälkeen, mikä johtaa siihen, että tapahtumia ei voida jäljittää uudessa lompakossa.	Kiistäminen (R11)
TR64	Luottavilla osapuolilla voi olla vaikeuksia todistaa suostumus sähköisiin etäallekirjoituksiin.	Kiistäminen (R11)
TR65	Hyökkääjä voi tukkia yhteydet luottaviin osapuoliin esittämällä liiallisen määrän pyyntöjä.	Palvelukeskeytys (R13)
TR66	Hyökkääjä voi tukkia tilantarjontapalvelun liiallisilla yhteyksillä luottaviin osapuoliin.	Palvelukeskeytys (R13)
TR67	Hyökkääjä voi saada attribuutin esittämisen vaikuttamaan kiistanalaiselta tai kielletyltä, vaikka attribuutin esitys näyttää attribuutin olevan voimassa.	Palvelukeskeytys (R13)
TR68	Hyökkääjä voi peruuttaa henkilön tunnistetiedon ilman perusteltua syytä.	Palvelukeskeytys (R13)
TR69	Hyökkääjä voi peruuttaa henkilön tunnistetiedon ilman käyttäjän suostumusta.	Palvelukeskeytys (R13)
TR70	Hyökkääjä voi peruuttaa (hyväksytyn) sähköisen attribuuttitodistuksen ilman perusteltua syytä.	Palvelukeskeytys (R13)
TR71	Hyökkääjä voi peruuttaa (hyväksytyn) sähköisen attribuuttitodistuksen ilman käyttäjän suostumusta.	Palvelukeskeytys (R13)
TR72	Hyökkääjä voi käynnistää useita tunnistamispyyntöjä ilman, että niiden havaitaan olevan tahallisia orpopyyntöjä.	Palvelukeskeytys (R13)
TR73	Hyökkääjä voi lähettää useita pyyntöjä ilman jatkotapahtumia.	Palvelukeskeytys (R13)
TR74	Hyökkääjä voi antaa luottavan osapuolen pyytää tunnistamista antamatta vastaavaa tunnistamista (vastausta) ja täyttä hallintaa.	Palvelukeskeytys (R13)
TR75	Hyökkääjä voi lähettää vastauksen pyyntöön sen aikakatkaisun jälkeen tai vastaavanlaiset tilanteet, jotka johtavat palvelun keskeytymiseen.	Palvelukeskeytys (R13)
TR76	Luottava osapuoli voi lähettää useita virheellisiä pyyntöjä.	Palvelukeskeytys (R13)
TR77	Hyökkääjä voi lähettää useita virheellisiä pyyntöjä lompakon tarjoajalle.	Palvelukeskeytys (R13)
TR78	Hyökkääjä voi estää jäsenvaltiota peruuttamasta ei-luotettua henkilön tunnistetietojen tarjoajaa henkilön tunnistetietojen tarjoajien luotetusta luettelosta.	Palvelukeskeytys (R13)
TR79	Hyökkääjä voi estää lompakon voimassaolon keskeyttämisen tai peruuttamisen.	Palvelukeskeytys (R13)

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus* (*)	Riskin nimi *Uhkaan liittyvät riskit*
TR80	Hyökkääjä voi estää luottavien osapuolten, käyttäjien ja/tai henkilön tunnistetietojen tarjoajien tapahtumat.	Palvelukeskeytys (R13)
TR81	Hyökkääjä voi estää lompakon suojatun salauslaitteen käytön.	Palvelukeskeytys (R13)
TR82	Hyökkääjä voi estää henkilön tunnistetietojen tarjoajaa peruuttamasta henkilön tunnistetietoja tai keskeyttämästä niiden voimassaoloa.	Palvelukeskeytys (R13) / Luvaton tapahtuma (R9)
TR83	Luottava osapuoli voi johtaa käyttäjästä enemmän henkilöllisyystietoja kuin ne, joita sen kanssa on jaettu.	Seuranta (R14)
TR84	Ryhmä yhdessä toimivia luottavia osapuolia tai henkilön tunnistetietojen tarjoajia voi johtaa käyttäjästä enemmän henkilöllisyystietoja kuin ne, joita niiden kanssa on jaettu.	Seuranta (R14)
TR85	Hyökkääjä voi seurata ja jäljittää käyttäjää käyttämällä tämän henkilön tunnistetietoja, kun käyttäjän tunnistamista ei vaadita.	Seuranta (R14)
TR86	Hyökkääjä voi koota (hyväksyttyjen) sähköisten attribuuttitodistusten yhdistelmien ”väärennetyn” esityksen.	Tapahtuman manipulointi (R10)
TR87	Hyökkääjä voi aktivoida lompakon tai ottaa sen haltuun etäyhteydellä (esim. pankkisovellus, johon sisältyy todentamis- tai todistuspyyntö) ilman käyttäjän nimenomaista suostumusta tai yksinomaista hallintaa tilanteissa, joissa käyttäjä ei ole tietoinen asiasta (esim. lepotila) tai ei pysty näkemään luottavaa osapuolta.	Tapahtuman manipulointi (R10)
TR88	Hyökkääjä voi muuttaa pyynnön metadataa (palvelun nimi, käyttötarkoitukset jne.).	Tapahtuman manipulointi (R10)
TR89	Hyökkääjä voi muuttaa vastauksen tietoja (palvelutila, nonce-luku jne.).	Tapahtuman manipulointi (R10)
TR90	Hyökkääjä voi muuttaa pyynnön attribuuttitietoja (ylikysyntä jne.).	Tapahtuman manipulointi (R10)
TR91	Luottava osapuoli voi toistaa aiemman istunnon elementtejä toisessa istunnossa.	Tapahtuman manipulointi (R10)
TR92	Hyökkääjä voi korvata henkilön tunnistetiedon tai muuttaa sitä, kun se siirretään henkilön tunnistetiedon tarjoajalta lompakkoyksikköön.	Tapahtuman manipulointi (R10)
TR93	Hyökkääjä voi korvata henkilön tunnistetiedon tai muuttaa sitä, kun se siirretään lompakkoyksiköstä verkossa olevalle luottavalle osapuolelle.	Tapahtuman manipulointi (R10)
TR94	Hyökkääjä voi korvata henkilön tunnistetiedon tai muuttaa sitä, kun se siirretään lompakkoyksiköstä verkon ulkopuolella olevalle luottavalle osapuolelle.	Tapahtuman manipulointi (R10)
TR95	Hyökkääjä voi myöntää henkilön tunnistetiedon ilman käyttäjän suostumusta.	Luvaton tapahtuma (R9)
TR96	Hyökkääjä voi käyttää peruutettuja tai voimassaolemattomia sisäänrakennettuja tietojen luovuttamiskäytäntöjä, mahdollisesti luottavien osapuolten tietämättä.	Luvaton tapahtuma (R9)
TR97	Hyökkääjä voi huijata lompakon todentamaan vääriä sähköisiä allekirjoituksia.	Luvaton tapahtuma (R9)
TR98	Hyökkääjä voi käyttää lompakkoa käyttäjän valvonnan ulkopuolella.	Luvaton tapahtuma (R9)

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus* (*)	Riskin nimi *Uhkaan liittyvät riskit*
TR99	Hyökkääjä voi saada käyttäjän todentamaan ja hyväksymään tapahtumia hyökkääjän tai luvattoman kolmannen osapuolen kanssa.	Luvaton tapahtuma (R9)
TR100	Hyökkääjä voi saada käyttäjän tekemään sähköisen allekirjoituksen esittämättä sisältöä käyttäjälle tai esitettyään väärän sisällön.	Luvaton tapahtuma (R9)
TR101	Hyökkääjä voi ohittaa lompakon tarjoajaan luodun käyttäjätilin pääsynvalvonnan.	Luvaton tapahtuma (R9)
TR102	Hyökkääjä voi esiintyä luottavana osapuolena luottaviin osapuoliin luodun yhteyden aikana.	Luvaton tapahtuma (R9) / Tietojen luovuttaminen (R6)
TR103	Luottavan osapuolen ja selaimen välisen yhteyden takana oleva käyttäjä voi olla eri kuin luottavan osapuolen ja lompakon välisen yhteyden takana oleva käyttäjä.	Luvaton tapahtuma (R9) / Tietojen luovuttaminen (R6) / Identiteettivarkaus (R4)
TR104	Hyökkääjä voi vakuuttaa käyttäjän peruuttamaan käyttäjän lompakon ilman syytä.	Luvaton tapahtuma (R9) / Palvelukeskeytys (R13)
TR105	Hyökkääjä voi tehdä väliintulohyökkäyksiä.	Luvaton tapahtuma (R9) / Tietojen luovuttaminen (R6) / Seuranta (R14)
TR106	Hyökkääjä voi esittää voimassa olemattomia tai peruutettuja attribuutteja lompakosta, joka ei ole säännöllisesti yhteydessä verkkoon.	Vaikuttaa useisiin riskeihin
TR107	Hyökkääjä voi varastaa käyttäjältä tietoja esiintymällä toisena henkilönä lompakolle.	Vaikuttaa useisiin riskeihin
TR108	Hyökkääjä voi esiintyä käyttäjänä toistamalla tietopyynnön tai jäljittelemällä tietopyyntöä (esim. todentaminen), joka vaikuttaisi olevan voimassa.	Vaikuttaa useisiin riskeihin
TR109	Hyökkääjä voi toistaa sisäänrakennetun tietojen luovuttamiskäytännön käyttäjälle jäljitelläkseen hyväksyttyä pyyntöä.	Vaikuttaa useisiin riskeihin
TR110	Hyökkääjä voi hyödyntää lompakon käyttäjien tiedonpuutetta tai tarpeettomia viivästyksiä tietoturvaloukkauksen tai vaarantumisen jälkeen.	Vaikuttaa useisiin riskeihin
TR111	Hyökkääjä voi muuttaa aiemmin asennettua laillista lompakon ilmentymää lisätäkseen siihen haitallisia ominaisuuksia.	Vaikuttaa useisiin riskeihin
TR112	Hyökkääjä voi muuttaa laillista lompakon ilmentymää ja ehdottaa sitä käyttäjille laillisena.	Vaikuttaa useisiin riskeihin
TR113	Hyökkääjä voi estää käyttäjän todentamismekanismin ohittaakseen lompakon käyttäjän todentamisen.	Vaikuttaa useisiin riskeihin
TR114	Hyökkääjä voi lisätä lompakon koodiin haitallisen koodin tai takaportteja, kun lompakko otetaan käyttöön käyttäjän laitteessa.	Vaikuttaa useisiin riskeihin
TR115	Hyökkääjä voi lisätä lompakon koodiin haitallisen koodin tai takaportteja lompakon kehittämisen aikana.	Vaikuttaa useisiin riskeihin
TR116	Hyökkääjä voi puuttua satunnaislukujen generointiin vähentääkseen niiden entropiaa niin paljon, että hyökkäykset mahdollistuvat.	Vaikuttaa useisiin riskeihin

ID *Tunniste*	Uhan kuvaus *Havaitun uhan kuvaus* (*)	Riskin nimi *Uhkaan liittyvät riskit*
TR117	Hyökkääjä voi puuttua käyttäjien laitteisiin toimitusketjussa ja sisällyttää niihin koodin tai konfiguraatioita, jotka eivät täytä lompakon käyttöehtoja.	Vaikuttaa useisiin riskeihin
TR118	Hyökkääjä voi aktivoida lompakkoyksikön esiintymällä toisena henkilönä lompakon suojatulle salauslaitteelle, joka on hyökkääjän hallinnassa.	Vaikuttaa useisiin riskeihin
TR119	Hyökkääjä voi lukea lompakon suojatulle salaussovellukselle ja/tai lompakon suojatulle salauslaitteelle lähetettyjä tietoja.	Vaikuttaa useisiin riskeihin
TR120	Hyökkääjä voi lähettää mielivaltaisia tietoja lompakon suojatulle salaussovellukselle.	Vaikuttaa useisiin riskeihin
TR121	Hyökkääjä voi varastaa tietoja sieppaamalla lompakon suojatun salaussovelluksen ja lompakon suojatun salauslaitteen välillä vaihdettuja tietoja.	Vaikuttaa useisiin riskeihin
TR122	Hyökkääjä voi lähettää mielivaltaisia tietoja lompakon suojatulle salauslaitteelle.	Vaikuttaa useisiin riskeihin
TR123	Hyökkääjä voi lähettää tietoja lompakon suojatulle salauslaitteelle ja kiertää lompakon suojatun salaussovelluksen.	Vaikuttaa useisiin riskeihin
TR124	Hyökkääjä voi käyttää tietojen kalastelua saadakseen käyttäjiä väärennetylle lompakolle ja henkilön tunnistetietojen hallinnan verkkosovellukselle.	Vaikuttaa useisiin riskeihin
TR125	Hyökkääjä voi korvata lompakon avaimet muilla avaimilla luodakseen viestejä, joita voidaan käyttää toisessa hyökkäyksessä.	Vaikuttaa useisiin riskeihin
TR126	Hyökkääjä voi muuttaa lompakon avaimia tai tuhota ne, mikä tekee joistakin lompakon toiminnoista käyttökelvottomia.	Vaikuttaa useisiin riskeihin
TR127	Hyökkääjä voi hallita haittaohjelmaa päästäkseen käsiksi lompakkoon tallennettuihin tietoihin.	Vaikuttaa useisiin riskeihin
TR128	Hyökkääjä voi päästä käsiksi lompakossa tuotettuihin todisteisiin.	Vaikuttaa useisiin riskeihin
TR129	Lompakon tarjoajat voivat päästä käsiksi lompakon objekteihin.	Vaikuttaa useisiin riskeihin
TR130	Lompakon tarjoajat voivat päästä käsiksi lompakossa tuotettuihin todisteisiin.	Vaikuttaa useisiin riskeihin
TR131	Hyökkääjä voi varastaa lukitsemattoman lompakkolaitteen.	Vaikuttaa useisiin riskeihin
TR132	Hyökkääjä voi manipuloida järjestelmää estääkseen tiettyjen tapahtumien kirjaamisen.	Vaikuttaa useisiin riskeihin
TR133	Hyökkääjä voi siepata lompakon ilmentymän ja lompakon suojatun salaussovelluksen välisiä viestejä tai toistaa tai jäljitellä käyttäjän toimintaa (esim. kaappaamalla todentamismekanismin).	Vaikuttaa useisiin riskeihin

LIITE II

VARMENNUSTIETOJEN HYVÄKSYTTÄVYYDEN ARVIOINTIPERUSTEET

Nimi	Kohde	Huomioitavat seikat
EUCC	TVT-tuotteet	Myöntäjästä: ei mitään (akkreditoidut sertifiointielimet) Kattavuudesta: — Tarkistetaan suojausprofiili ja turvatavoite — Tarkistetaan arvioinnin vakuuttavuustaso ja korotukset Varmennuksesta: — Tarkistetaan rajoitukset käyttäjädokumentaatiossa — Kokoonpanon osalta voi edellyttää, että tekninen arviointiraportti on saatavilla.
EUCS (jos saatavilla)	Pilvipalvelut	Myöntäjästä: ei mitään (akkreditoidut sertifiointielimet) Kattavuudesta: — Tarkistetaan pilvipalvelun kuvaus — Tarkistetaan arviointitaso ja laajennusprofiilit Varmennuksesta: — Tarkistetaan avoimuustiedot ja tarvittaessa kokoonpanoa koskevat tiedot
EU:ssa käytössä olevat yhteisiin kriteereihin perustuvat järjestelmät, mukaan lukien SOG-IS-järjestelmät	TVT-tuotteet	Myöntäjästä: ei mitään (jäsenvaltiot) Kattavuudesta: — Tarkistetaan suojausprofiili ja turvatavoite — Tarkistetaan arvioinnin vakuuttavuustaso ja korotukset Varmennuksesta: — Tarkistetaan rajoitukset käyttäjädokumentaatiossa — Kokoonpanon osalta voi edellyttää, että tekninen arviointiraportti on saatavilla.
EN 17640:2018 (FITCEM, mukaan lukien CSPN, BSZ, LINCE, BSZA)	TVT-tuotteet	Myöntäjästä: — Tarkistetaan järjestelmä ja sertifiointielimiä koskevat vaatimukset Kattavuudesta: — Tarkistetaan tuotteen kuvaus — Tarkistetaan turvaväitteet — Tarkistetaan varmuustaso Varmennuksesta: — Tarkistetaan suoritetut toimet ja raportissa esitetyt havainnot
Asetuksen (EU) N:o 910/2014 30 artiklan mukaiset hyväksyttyjen allekirjoitusten luontivälineiden sertifiointijärjestelmät	Hyväksytyt allekirjoitusten luontivälineet	Myöntäjästä: — Tarkistetaan järjestelmä ja sertifiointielimiä koskevat vaatimukset Kattavuudesta: — Tarkistetaan tuotteen kuvaus — Tarkistetaan turvaväitteet — Tarkistetaan varmuustaso Varmennuksesta: — Tarkistetaan suoritetut toimet

Nimi	Kohde	Huomioitavat seikat
EN ISO/IEC 27001:2022	Tietoturvan hallintajärjestelmä	Myöntäjästä: ei mitään (akkreditoidut sertifiointielimet) Kattavuudesta: — Tarkistetaan hallintajärjestelmän kuvaus — Tarkistetaan soveltuvuuslausunto Varmennuksesta: — Tarkistetaan suoritetut toimet
SOC2	Organisaatiot	Myöntäjästä: — Tarkistetaan tarkastajan asema Kattavuudesta: — Tarkistetaan johdon lausuma ja tarkastusten kuvaus — Tarkistetaan soveltuvuuslausunto Varmennuksesta: — Tarkistetaan raportissa esitetyt havainnot — Tarkistetaan tarvittaessa tarkastusraportin voimassaolon jatkuminen (bridge letters)
MDSCert (GSMA) (jos saatavilla)	Mobiililaitteet	Myöntäjästä: — Tarkistetaan sertifiointielimiä koskevat vaatimukset Kattavuudesta: — Tarkistetaan tietoturvan varmuustaso — Tarkistetaan järjestelmän vaatimukset Varmennuksesta: — Tarkistetaan suoritetut toimet ja raportissa esitetyt havainnot
Muut järjestelmät	Mikä tahansa komponentti	Järjestelmästä: — Tarkistetaan järjestelmän tarkoituksenmukaisuus ja sitä koskevat säännökset Myöntäjästä: — Tarkistetaan sertifiointielimiä koskevat vaatimukset Kattavuudesta: — Tarkistetaan järjestelmän vaatimukset — Tarkistetaan turvatavoite tai vastaava asiakirja, jossa kuvataan toiminnalliset turvallisuusvaatimukset ja turvallisuusvarmistusvaatimukset — Tarkistetaan tuotekuvaus ja valitut toiminnalliset turvallisuusvaatimukset Varmennuksesta: — Tarkistetaan suoritetut toimet ja raportissa esitetyt havainnot

LIITE III

LOMPAKKORATKAISUJA KOSKEVAT TOIMINNALLISET VAATIMUKSET

Asetuksen (EU) N:o 910/2014 5 a artiklan 4, 5, 8 ja 14 kohdan mukaan niihin toiminnallisiin kriteereihin, jotka sertifioidun lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, on täytettävä, on sisällyttävä toiminnalliset vaatimukset seuraavissa säädöksissä luetelluille toimille:

1) Komission täytäntöönpanoasetus (EU) 2024/2979 ([1]) Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisten digitaalisen identiteetin lompakoiden eheyden ja ydintoimintojen osalta;

2) Komission täytäntöönpanoasetus (EU) 2024/2982 ([2]) Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisen digitaalisen identiteetin kehyksen tukemien protokollien ja rajapintojen osalta;

3) Komission täytäntöönpanoasetus (EU) 2024/2977 ([3]) Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisille digitaalisen identiteetin lompakoille myönnettävien henkilön tunnistetietojen ja sähköisten attribuuttitodistusten osalta.

([1]) 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).

([2]) 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).

([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).

LIITE IV

ARVIOINTITOIMIA KOSKEVAT MENETELMÄT JA MENETTELYT

1. **Lompakkoratkaisun toteutuksen tarkastus**

Vaatimustenmukaisuuden arviointitoimeen kuuluu yksittäisten arviointitoimien valinta.

Kansallisissa sertifiointijärjestelmissä on määriteltävä arviointitoimi, jossa arvioidaan toimitetut tiedot ja joka kattaa ainakin seuraavat:

a) toimitettujen tietojen analysointi sen varmistamiseksi, että ne soveltuvat johonkin kansallisissa sertifiointijärjestelmissä määritellyistä arkkitehtuureista;

b) analyysi siitä, miten kuvatut turvatoimenpiteet kattavat liitteessä I olevassa riskirekisterissä yksilöidyt kyberturvallisuusriskit ja -uhat.

Edellä a ja b alakohdassa mainitun analyysin on perustuttava lompakon tarjoajan esittämiin periaatteisiin ja perusteluihin.

2. **Lompakon suojattuun salauslaitteeseen liittyvät arviointitoimet**

1) Kriittisiä toimintoja, kuten salauslaskentaa, ei tarvitse toteuttaa kokonaisuudessaan lompakon suojatussa salauslaitteessa. Lompakon suojatussa salauslaitteessa toteutetun osan, kun se toimii osana lompakkoratkaisua, on kuitenkin taattava sen toteuttamien kriittisten toimintojen suojaaminen hyökkäyksiltä, joiden vakavuusaste on korkea, komission täytäntöönpanoasetuksen (EU) 2015/1502 ([1]) mukaisesti.

2) Lompakon suojattu salauslaite tai sen osa voi kuulua sertifioinnin kohteeseen, jos sen tarjoaa sertifikaatin haltija tai hakija, tai olla sen soveltamisalan ulkopuolella, jos se on sisällytetty loppukäyttäjän tarjoamaan laitteeseen. Kansallisissa sertifiointijärjestelmissä on lisäksi täsmennettävä arviointitoimet lompakon suojatun salauslaitteen soveltuvuuden todentamiseksi seuraavissa kahdessa tapauksessa:

   a) jos lompakon suojattu salaussovellus on riippuvainen tietystä lompakon suojatusta salauslaitteesta (eli jos se on arvioitava lompakon suojattuun salauslaitteeseen perustuvana yhdistelmätuotteena), lompakon suojatun salaussovelluksen arviointi edellyttää pääsyä lompakon suojatun salauslaitteen sertifiointiin liittyviin lisätietoihin, mukaan lukien erityisesti sen tekninen arviointiraportti;

   b) jos järjestelmässä tarkasteltavassa arkkitehtuurissa käytetään useita lompakon suojattuja salauslaitteita tai jos osa kriittisiin resursseihin liittyvistä toimista toteutetaan lompakon suojatun salauslaitteen ulkopuolella, kansallisiin sertifiointijärjestelmiin on sisällyttävä arviointitoimia, joilla varmistetaan, että kokonaisratkaisu tarjoaa odotetun turvallisuustason.

3) Kansallisten sertifiointijärjestelmien mukaisen sertifioinnin edellytyksenä on, että lompakon suojattu salauslaite arvioidaan täytäntöönpanoasetuksessa (EU) 2015/1502 vahvistettujen korkeaa varmuustasoa koskevien vaatimusten perusteella.

   a) Kun 3 artiklan 3 kohdan b alakohdan edellytykset täyttyvät, lompakon suojatun salauslaitteen tai sen osan arviointiin on sisällyttävä standardissa EN ISO/IEC 15408–3:2022 esitetty haavoittuvuusarviointi AVA_VAN-tasolla 5 komission täytäntöönpanoasetuksen (EU) 2024/482 ([2]) liitteen I mukaisesti, paitsi jos sertifiointielimelle perustellaan asianmukaisesti, että lompakon suojatun salaussovelluksen turvaominaisuudet mahdollistavat alhaisemman arviointitason käytön ja säilyttävät samalla täytäntöönpanoasetuksessa (EU) 2015/1502 vahvistetun yleisen korkean varmuustason.

([1]) Komission täytäntöönpanoasetus (EU) 2015/1502, annettu 8 päivänä syyskuuta 2015, teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti (EUVL L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Komission täytäntöönpanoasetus (EU) 2024/482, annettu 31 päivänä tammikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä (EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4) Lisäksi kansallisissa sertifiointijärjestelmissä on kuhunkin yksittäiseen arkkitehtuuriin liittyvässä dokumentaatiossa muotoiltava lompakon suojatun salauslaitteen arviointia varten oletuksia, joiden perusteella voidaan täytäntöönpanoasetuksen (EU) 2015/1502 mukaisesti tarjota kyky vastustaa hyökkäyksiä, joiden vakavuusaste on korkea, ja täsmennettävä arviointitoimet, joilla vahvistetaan nämä oletukset ja vahvistetaan sertifikaatin myöntämisen jälkeen, että oletukset todennetaan edelleen. Kansallisissa järjestelmissä on myös edellytettävä, että sertifioinnin hakijat täsmentävät näitä oletuksia oman toteutuksensa osalta ja kuvailevat käytössä olevat toimenpiteet, joilla taataan, että oletukset todennetaan sertifioinnin koko elinkaaren ajan.

5) Kansallisiin sertifiointijärjestelmiin on kaikissa tapauksissa sisällyttävä arviointitoimi, jolla todennetaan, että lompakon suojattua salauslaitetta varten saatavilla olevat varmennustiedot soveltuvat lompakkoratkaisuun, analysoimalla varmennustietoja, kuten EUCC-sertifikaattien turvatavoitetta, mukaan lukien seuraavat toimet:

   a) sen todentaminen, että arvioinnin laajuus on sopiva, mikä tarkoittaa esimerkiksi EUCC-sertifikaattien osalta sen todentamista, että turvatavoite on jonkin EUCC-järjestelmässä suositellun suojausprofiilin mukainen;

   b) sen todentaminen, että toimintaympäristöä koskevat oletukset ovat yhteensopivia lompakkoratkaisun kanssa, mikä tarkoittaa esimerkiksi EUCC-sertifikaattien osalta, että nämä oletukset löytyvät turvatavoitteesta;

   c) sen todentaminen, että käyttöohjeissa tai dokumentaatiossa annetut suositukset ovat yhteensopivia niiden olosuhteiden kanssa, joissa lompakon suojattua salauslaitetta on tarkoitus käyttää lompakkoratkaisussa;

   d) sen todentaminen, että kansallisessa sertifiointijärjestelmässä lompakon suojatuista salauslaitteista tehdyt oletukset on todennettu ja varmennustiedot kattavat ne.

6) Tapauksissa, joissa joidenkin todentamisten tulos ei ole täysin yksiselitteinen, kansallisissa sertifiointijärjestelmissä on edellytettävä, että sertifiointielimet määrittävät lompakon suojatulle salaussovellukselle lompakon suojattuun salauslaitteeseen perustuvia korvaavia vaatimuksia, jotka sisällytetään lompakon suojatun salaussovelluksen arviointiin. Jos tämä ei ole mahdollista, kansallisten sertifiointijärjestelmien on pidettävä lompakon suojattua salauslaitetta soveltumattomana, mikä tarkoittaa, että lompakkoratkaisulle ei myönnetä vaatimustenmukaisuustodistusta.

3. **Lompakon suojattuun salaussovellukseen liittyvät arviointitoimet**

1) Kansallisissa sertifiointijärjestelmissä on edellytettävä, että lompakon suojattu salaussovellus arvioidaan osana lompakkoratkaisua vähintään täytäntöönpanoasetuksessa (EU) 2015/1502 vahvistettujen korkeaa varmuustasoa koskevien vaatimusten perusteella.

2) Tähän arviointiin on sisällyttävä standardissa EN ISO/IEC 15408–3:2022 esitetty haavoittuvuusarviointi AVA_VAN-tasolla 5 täytäntöönpanoasetuksen (EU) 2024/482 liitteen I mukaisesti, paitsi jos sertifiointielimelle perustellaan asianmukaisesti, että lompakon suojatun salaussovelluksen turvaominaisuudet mahdollistavat alhaisemman arviointitason käytön ja säilyttävät samalla täytäntöönpanoasetuksessa (EU) 2015/1502 vahvistetun yleisen korkean varmuustason.

3) Kun lompakon tarjoaja ei tarjoa lompakon suojattua salaussovellusta, kansallisissa sertifiointijärjestelmissä on muotoiltava lompakon suojatun salaussovelluksen arviointia varten oletuksia, joiden perusteella voidaan täytäntöönpanoasetuksen (EU) 2015/1502 mukaisesti tarjota kyky vastustaa hyökkäyksiä, joiden vakavuusaste on korkea, ja täsmennettävä arviointitoimet, joilla vahvistetaan nämä oletukset ja vahvistetaan sertifikaatin myöntämisen jälkeen, että oletukset todennetaan edelleen. Kansallisissa järjestelmissä on myös edellytettävä, että sertifioinnin hakijat täsmentävät näitä oletuksia oman toteutuksensa osalta ja kuvailevat käytössä olevat toimenpiteet, joilla taataan, että oletukset todennetaan sertifioinnin koko elinkaaren ajan.

4) Kansallisiin sertifiointijärjestelmiin on kaikissa tapauksissa sisällyttävä arviointitoimi, jolla todennetaan, että lompakon suojattua salaussovellusta varten saatavilla olevat varmennustiedot soveltuvat lompakkoratkaisuun, analysoimalla varmennustietoja, kuten EUCC-sertifikaattien turvatavoitetta, mukaan lukien seuraavat toimet:

   a) sen todentaminen, että arvioinnin laajuus on sopiva, mikä tarkoittaa esimerkiksi EUCC-sertifikaattien osalta sen todentamista, että turvatavoite on jonkin EUCC-järjestelmässä suositellun suojausprofiilin mukainen;

   b) sen todentaminen, että toimintaympäristöä koskevat oletukset ovat yhteensopivia lompakkoratkaisun kanssa, mikä tarkoittaa esimerkiksi EUCC-sertifikaattien osalta, että nämä oletukset löytyvät turvatavoitteesta;

c) sen todentaminen, että käyttöohjeissa tai dokumentaatiossa annetut suositukset ovat yhteensopivia niiden olosuhteiden kanssa, joissa lompakon suojattua salaussovellusta on tarkoitus käyttää lompakkoratkaisussa;

d) sen todentaminen, että kansallisessa sertifiointijärjestelmässä lompakon suojatuista salaussovelluksista tehdyt oletukset on todennettu ja varmennustiedot kattavat ne.

5) Kansallisissa sertifiointijärjestelmissä on edellytettävä, että lompakon suojatun salaussovelluksen arviointi kattaa kaikki kyseisen lompakon suojatun salaussovelluksen toteuttamat turvatoimenpiteet.

4. **Loppukäyttäjän laitteeseen liittyvät arviointitoimet**

Koska tämän asetuksen liitteessä I vahvistetussa riskirekisterissä yksilöidään loppukäyttäjän laitteen turvallisuuteen suoraan liittyvät riskit, kansallisissa sertifiointijärjestelmissä on määriteltävä loppukäyttäjien laitteita koskevat turvallisuusvaatimukset. Koska nämä laitteet kuitenkin tarjoaa loppukäyttäjä eikä lompakon tarjoaja, nämä vaatimukset on katettava olettamuksilla.

Lompakkoratkaisuun on sisällyttävä kunkin oletuksen osalta mekanismi, jolla todennetaan jokaisen lompakkoyksikön osalta, että loppukäyttäjän laite täyttää oletuksen. Tällaisia mekanismeja on pidettävä turvatoimenpiteinä ja ne on otettava huomioon arviointitoimissa niiden soveltuvuuden ja tehokkuuden osoittamiseksi asianmukaisella varmuustasolla.

Seuraavassa esitetään kaksi esimerkkiä:

a) Loppukäyttäjän laitteeseen voi sisältyä sertifioitu lompakon suojattu salauslaite, jolloin sertifiointi on osoitettava. Tämä tapahtuisi tyypillisesti käyttämällä salausmekanismia sen todentamiseen, että sertifioidussa lompakon suojatussa salauslaitteessa on kryptografinen salaisuus, joka on saatavilla ainoastaan sertifioidussa lompakon suojatussa salauslaitteessa. Tässä tapauksessa tätä kryptografista salaisuutta olisi pidettävä kriittisenä resurssina, ja sen olisi kuuluttava lompakon suojatun salauslaitteen ja/tai lompakon suojatun salaussovelluksen sertifioinnin piiriin.

b) Tyypillinen vaatimus loppukäyttäjän laitteille olisi se, että laitteiden on vastaanotettava tietoturvapäivityksiä. Koska tämä vaatimus liittyy lompakon ilmentymään, turvapäivitysten saatavuuden todentamiseen käytettävä mekanismi on katettava ainoastaan lompakon ilmentymään soveltuvalla varmuustasolla toteutettavilla arviointitoimilla, erityisesti koska se todennäköisesti integroidaan lompakon ilmentymään.

5. **Lompakon ilmentymään liittyvät arviointitoimet**

1) Lompakon ilmentymän arvioinnissa on tarkasteltava seuraavia kahta pääasiallista haastetta:

a) lompakon ilmentymä on todennäköisesti olemassa sarjana saman perussovelluksen muunnoksia, joista kukin on erikoistunut tiettyyn loppukäyttäjän laiteluokkaan;

b) lompakon ilmentymän eri muunnoksia on todennäköisesti päivitettävä usein niiden pitämiseksi perustana olevan turva-alustan kehityksen tasalla, esimerkiksi silloin, kun havaitaan haavoittuvuuksia, jotka edellyttävät muutoksia sovelluksiin.

2) Nämä erityiset haasteet on otettava huomioon lompakon ilmentymän arvioinnissa. Yksi välittömistä seurauksista on se, että yhteisten kriteerien kehys ei välttämättä sovellu kaikkiin tapauksiin. Sen vuoksi on tarvittaessa harkittava vaihtoehtoisia arviointimenetelmiä. Kansallisissa sertifiointijärjestelmissä on harkittava standardin EN 17640:2018 mukaisen menetelmän käyttöä seuraavissa tapauksissa:

a) osana itse järjestelmää;

b) menetelmään perustuvien kansallisten järjestelmien kautta;

c) sellaisten kansallisten järjestelmien kautta, jotka perustuvat samanlaisiin periaatteisiin mutta jotka on luotu ennen standardin EN 17640:2018 mukaisen menetelmän kehittämistä.

3) Lisäksi koska erillisen kattavan arvioinnin suorittaminen kustakin muunnoksesta saattaa tuoda vain vähän lisäarvoa, kansallisissa sertifiointijärjestelmissä on harkittava sellaisten kriteerien määrittämistä, jotka mahdollistavat otannan, jotta vältetään samanlaisten arviointitoimien toistaminen ja voidaan keskittyä tietylle muunnokselle ominaisiin toimiin. Kansallisissa sertifiointijärjestelmissä on edellytettävä, että kaikki sertifiointielimet perustelevat otosten käytön.

4) Kansallisten sertifiointijärjestelmien on katettava lompakon ilmentymän päivitykset osana lompakkoratkaisua varten määritettyä yleistä muutostenhallintaprosessia. Niissä on myös vahvistettava säännöt menettelyistä, jotka lompakon tarjoajan on suoritettava jokaisen päivityksen yhteydessä (esim. analyysin tekeminen muutosten vaikutuksesta turvatoimenpiteisiin), ja arviointitoimista, jotka sertifiointielimen on suoritettava päivitysten yhteydessä tietyin edellytyksin (esim. muutetun turvatoimenpiteen toimintatehokkuuden arviointi). Muutostenhallintaprosessi on yksi prosesseista, joiden toimintatehokkuus on tarkastettava vuosittain 18 artiklan 3 kohdan mukaisesti.

6. **Lompakkoratkaisun tarjoamisessa ja toiminnassa käytettäviin palveluihin ja prosesseihin liittyvät arviointitoimet**

1) Arviointiryhmän on kerättävä näyttöä sellaisten palvelujen ja prosessien arvioimiseksi, joilla on merkitystä lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, tarjoamisessa ja toiminnassa, suorittamalla arviointitoimia, joihin voi sisältyä auditointi-, tarkastus-, todentamis- ja validointitoimia.

2) Sertifiointielimen on vahvistettava, että näyttö on riittävää ja asianmukaista, jotta saadaan riittävä varmuus siitä, että palvelut ja prosessit täyttävät sertifiointivaatimukset, vahvistamalla seuraavat seikat:

   a) prosessien ja palvelujen kuvauksessa esitettyjen tietojen paikkansapitävyys;

   b) prosessien ja palvelujen suunnittelun ja valvonnan soveltuvuus arviointikriteerien täyttymiseen;

   c) näiden valvontatoimien toteutuksen toimintatehokkuus tietyn ajan ennen arviointia.

3) Kuvauksen paikkansapitävyyttä ja valvontatoimien toteutuksen toimintatehokkuutta voidaan pitää standardissa ISO/IEC 17000:2020 tarkoitettuina todentamistavoitteina lompakon tarjoajan vastaavien väitteiden osalta (eli jo tapahtuneiden tapahtumien tai jo saatujen tulosten paikkansapitävyyden vahvistaminen), kun taas prosessien ja palvelujen suunnittelun ja valvonnan soveltuvuutta arviointikriteerien täyttymiseen voidaan pitää standardissa ISO/IEC 17000:2020 tarkoitettuna validointitavoitteena lompakon tarjoajan vastaavien väitteiden osalta (eli varmistuminen aiotun tulevan käytön tai ennakoidun tuloksen uskottavuudesta).

4) Kun otetaan huomioon, että lompakkoratkaisu ei saa toimia ennen kuin se on sertifioitu, toimintatehokkuutta ei voida vahvistaa ratkaisun tosiasiallisen toiminnan perusteella. Se on sen vuoksi vahvistettava kokeiden tai pilottitoimien aikana kerätyn näytön perusteella.

5) Kansallisia sertifiointijärjestelmiä voi jo olla olemassa tiettyjä palveluja ja prosesseja varten, esimerkiksi käyttäjien käyttösuhteen aloittamista varten. Kansallisissa sertifiointijärjestelmissä on tarvittaessa harkittava tällaisten järjestelmien käyttöä.

7. **Lompakkoratkaisun tarjoamisessa ja toiminnassa käytettäviin tieto- ja viestintäteknisiin palveluihin liittyvät arviointitoimet**

1) Jotkin lompakkoarkkitehtuurit voivat tukeutua erityisiin tieto- ja viestintäteknisiin palveluihin, kuten pilvipalveluihin lompakkoratkaisun tarjoamista ja toteuttamista varten, ja näihin palveluihin voi sisältyä arkaluonteisia tietoja ja arkaluonteisia toimintoja. Tällaisissa tapauksissa kansallisissa sertifiointijärjestelmissä on määriteltävä näitä tieto- ja viestintäteknisiä palveluja koskevat tietoturvavaatimukset.

2) Tieto- ja viestintäteknisille palveluille, pilvipalveluille ja muille varmennustietojen lähteille on jo olemassa monia sertifiointijärjestelmiä, mukaan lukien liitteessä II luetellut järjestelmät. Kansallisten sertifiointijärjestelmien on perustuttava näihin olemassa oleviin mekanismeihin, jos niitä on saatavilla ja ne ovat sovellettavissa, käyttäen jotakin seuraavista mekanismeista:

   a) tehdään tietyn järjestelmän tai tiettyjen järjestelmien valikoiman käyttö pakolliseksi täsmentämällä edellytykset, joiden mukaisesti tieto- ja viestintäteknisiä palveluja tai pilvipalveluja on arvioitava näiden järjestelmien avulla;

   b) jätetään arvioinnin valinta lompakon tarjoajalle ja käytetään riippuvuusanalyysia näiden arviointien avulla saatujen varmennustietojen soveltuvuuden analysointiin.

3) Molemmissa tapauksissa kansallisissa sertifiointijärjestelmissä on täsmennettävä muita arviointitoimia, joita tarvitaan näiden järjestelmien kautta saatujen tietojen analysoimiseksi tai täydentämiseksi.

LIITE V

LUETTELO LOMPAKOISTA JULKISESTI SAATAVILLA OLEVISTA TIEDOISTA

1. Tämän asetuksen 8 artiklan 5 kohdan mukaisesti julkistettaviin tietoihin on sisällyttävä vähintään seuraavat:
   a) lompakkoratkaisun mahdolliset käyttörajoitukset;
   b) lompakon tarjoajan antamat ohjeet ja suositukset, jotka auttavat loppukäyttäjiä lompakoiden turvallisessa konfiguroinnissa, asentamisessa, käyttöönotossa, käytössä ja ylläpidossa;
   c) loppukäyttäjille tarjottavan turvallisuustuen kesto, erityisesti kyberturvallisuuteen liittyvien päivitysten saatavuuden osalta;
   d) valmistajan tai tarjoajan yhteystiedot ja hyväksytyt tavat, joilla loppukäyttäjät ja tietoturvatutkijat voivat toimittaa tietoa haavoittuvuuksista;
   e) viittaus verkkotietolähteisiin, joissa on luettelo lompakoihin liittyvistä julkisesti tiedossa olevista haavoittuvuuksista ja niihin liittyvää kyberturvallisuusneuvontaa.

2. Edellä 1 kohdassa tarkoitetut tiedot on asetettava selkeällä, kattavalla ja helppokäyttöisellä tavalla kaikkien sellaisten henkilöiden saataville, jotka haluavat käyttää lompakkoratkaisua.

LIITE VI

VARMENNUSTIETOJEN HYVÄKSYTTÄVYYDEN ARVIOINTIMENETELMÄ

1. **Varmennusdokumentaation saatavuuden arviointi**

Arvioijien on lueteltava lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, kustakin merkityksellisestä osasta saatavilla oleva varmennusdokumentaatio. Tämän jälkeen arvioijien on arvioitava varmennusdokumentaation kunkin osan yleinen merkityksellisyys riippuvuusarvioinnin kannalta.

Analyysissa on otettava huomioon seuraavat näkökohdat:

1) itse varmennusdokumentaation osalta:

   a) varmennusdokumentaation tyyppi, mukaan lukien kaikki vaaditut tiedot

      (esimerkkejä tällaisista asiakirjoista ovat standardin EN ISO/IEC 27001:2022 mukaiset vaatimustenmukaisuustodistukset tai ISAE-raporttien tyyppi 1 tai 2);

   b) raportointikausi tai voimassaoloaika

      (tätä ajanjaksoa voidaan jatkaa asiakirjalla, joka kattaa ajanjakson nykyisen ISAE-raportin raportointikauden päättymispäivän ja uuden ISAE-raportin julkistamisen välillä (ns. bridge letter), tai vastaavalla lausunnolla);

   c) sovellettava kehys (esim. voimassa oleva standardi);

   d) sisältyykö varmennusdokumentaatioon kartoitus suhteessa järjestelmän vaatimuksiin;

2) varmennusraportin laatijan ammatillisen pätevyyden ja puolueettomuuden osalta:

   a) sertifiointielimen nimi ja, jos saatavilla, pääarvioijan nimi;

   b) näyttö sertifiointielimen ja arvioijan pätevyydestä (esim. akkreditointi, henkilökohtainen sertifiointi jne.);

   c) näyttö sertifiointielimen ja arvioijan puolueettomuudesta (esim. akkreditointi).

2. **Yksittäisiin vaatimuksiin liittyvän varmuuden arviointi**

Arvioijien on todennettava, että lompakkoratkaisusta ja sähköisen tunnistamisen järjestelmästä, jonka puitteissa sitä tarjotaan, saatavilla oleva varmennusdokumentaatio on riittävä sen määrittämiseksi, että lompakkoratkaisu täyttää sertifiointijärjestelmän yksittäisiin vaatimuksiin liittyvät odotukset.

Tämä arviointi on tehtävä lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, kaikista merkityksellisistä komponenteista muotoilemalla lompakkoratkaisun turvatoimenpiteitä koskeva oletus.

Arviointiryhmän on määritettävä kunkin tällaisen oletuksen osalta, onko saatavilla olevan varmennusdokumentaation tarjoama varmuus riittävä vai ei.

Varmuuden riittävyyden määrittämisen on perustuttava seuraaviin seikkoihin:

1) vaaditut tiedot ovat saatavilla odotetulla varmuustasolla varmennusdokumentaatiossa;

2) varmennusdokumentaatiossa saatavilla olevat tiedot eivät kata koko vaatimuksen soveltamisalaa, mutta lompakkoratkaisussa tai sähköisen tunnistamisen järjestelmässä, jonka puitteissa sitä tarjotaan, toteutetut täydentävät tai korvaavat turvatoimenpiteet (eli sisäiset turvatoimenpiteet, jotka vähentävät turvatoimenpiteen olemassa olevan tai mahdollisen puutteen riskiä) mahdollistavat sen, että arvioijat katsovat tietojen olevan riittäviä;

3) varmennusdokumentaatiossa saatavilla olevat tiedot eivät tarjoa odotettua varmuustasoa, mutta lompakon tarjoajan arvioimiseksi ja seuraamiseksi toteutetut turvatoimenpiteet mahdollistavat sen, että arvioijat katsovat tietojen olevan riittäviä;

4) jos varmennusdokumentaatiossa mainitaan oletuksen täyttämiseksi käytettyjen turvatoimenpiteiden suunnitteluun tai toteutukseen liittyviä vaatimustenvastaisuuksia, lompakon tarjoajan ehdottamien ja toteuttamien ja arvioijien tarkistamien korjaavien toimien on oltava riittäviä sen takaamiseksi, että oletus todella täyttyy.

LIITE VII

VAATIMUSTENMUKAISUUSTODISTUKSEN SISÄLTÖ

1. Vaatimustenmukaisuustodistuksen myöntäneen sertifiointielimen antama yksilöllinen tunniste.

2. Tiedot sertifioidusta lompakkoratkaisusta ja sähköisen tunnistamisen järjestelmistä, joiden puitteissa sitä tarjotaan, sekä vaatimustenmukaisuustodistuksen haltijasta, mukaan lukien seuraavat:
   a) lompakkoratkaisun nimi;
   b) niiden sähköisen tunnistamisen järjestelmien nimi, joiden puitteissa lompakkoratkaisua tarjotaan;
   c) arvioitu lompakkoratkaisun versio;
   d) vaatimustenmukaisuustodistuksen haltijan nimi, osoite ja yhteystiedot;
   e) linkki vaatimustenmukaisuustodistuksen haltijan verkkosivustolle, joka sisältää tiedot, jotka on asetettava julkisesti saataville.

3. Tiedot, jotka liittyvät lompakkoratkaisun ja sähköisen tunnistamisen järjestelmien, joiden puitteissa sitä tarjotaan, arviointiin ja sertifiointiin, mukaan lukien seuraavat:
   a) vaatimustenmukaisuustodistuksen myöntäneen sertifiointielimen nimi, osoite ja yhteystiedot;
   b) arvioinnin suorittaneen vaatimustenmukaisuuden arviointilaitoksen nimi ja tiedot sen akkreditoinnista, jos se ei ole sama kuin sertifiointielin;
   c) järjestelmän omistajan nimi;
   d) viittaukset asetukseen (EU) N:o 910/2014 ja tähän asetukseen;
   e) viittaus vaatimustenmukaisuustodistukseen liittyvään sertifiointiraporttiin;
   f) viittaus vaatimustenmukaisuustodistukseen liittyvään sertifioinnin arviointiraporttiin;
   g) viittaus arvioinnissa käytettyihin standardeihin, mukaan lukien niiden versiot;
   h) vaatimustenmukaisuustodistuksen myöntämispäivä;
   i) vaatimustenmukaisuustodistuksen voimassaoloaika.

LIITE VIII

JULKISEN SERTIFIOINTIRAPORTIN JA SERTIFIOINNIN ARVIOINTIRAPORTIN SISÄLTÖ

1. Sertifiointiraportissa on oltava ainakin seuraavat tiedot:

   a) tiivistelmä;

   b) lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, tunnistetiedot;

   c) lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa sitä tarjotaan, kuvaus;

   d) liitteessä V kuvatut julkisesti saataville asetettavat turvallisuustiedot tai näiden tietojen viitetiedot;

   e) tiivistelmä alustavasta tarkastus- ja validointisuunnitelmasta;

   f) tiivistelmä tarkastelusta ja sertifiointipäätöksestä.

2. Sertifioinnin arviointiraportin on sisällettävä vähintään seuraavat:

   a) kuvaus lompakkoratkaisun suunnittelusta, tunnistusjärjestelmästä ja käyttösuhteen aloittamisprosessista sekä riskinarviointi ja erityinen validointisuunnitelma;

   b) kuvaus siitä, miten lompakkoratkaisu täyttää korkeaa varmuustasoa koskevat vaatimukset ja miten tämä osoitetaan tämän asetuksen mukaisesti tehdyn lompakkoratkaisun sertifiointiarvioinnin tuloksissa;

   c) kuvaus lompakkoratkaisun ja sähköisen tunnistamisen järjestelmän, jonka puitteissa vastaavia lompakkoyksiköitä tarjotaan, vaatimustenmukaisuuden arvioinnin tuloksista ja erityisesti seuraavien vaatimusten mukaisuudesta:

      — asetuksen (EU) N:o 910/2014 5 a artiklan 4, 5 ja 8 kohdassa säädetyt vaatimukset;

      — asetuksen (EU) N:o 910/2014 5 a artiklan 14 kohdassa säädetty loogista erillään pitoa koskeva vaatimus;

      — tarvittaessa asetuksen (EU) N:o 910/2014 5 a artiklan 24 kohdassa tarkoitetut standardit ja tekniset eritelmät, samalla kun kuvataan, miten nämä vaatimukset liittyvät kansallisissa sertifiointijärjestelmissä määriteltyihin vastaaviin normatiivisiin vaatimuksiin;

   d) tiivistelmä validointisuunnitelman toteutuksen tuloksista, mukaan lukien kaikki havaitut vaatimustenvastaisuudet.

LIITE IX

PAKOLLISTEN VALVONTA-ARVIOINTIEN AIKATAULU

1. Tämän asetuksen 18 artiklassa täsmennetään sertifioinnin elinkaarta ja erityisesti säännöllisten arviointitoimien suorittamista koskevat vaatimukset. Näihin toimiin on sisällyttävä vähintään seuraavat:

   a) vaatimustenmukaisuuden arvioinnin kohteen täydellinen arviointi ensimmäisessä arvioinnissa ja jokaisessa uudelleensertifiointiarvioinnissa, mukaan lukien tuotekomponentteja koskeva päivitystoiminto;

   b) ensimmäisessä arvioinnissa ja jokaisessa uudelleensertifiointiarvioinnissa ja vähintään joka toinen vuosi valvonta-arvioinnissa tehtävä haavoittuvuusarviointi, joka kattaa ainakin vaatimustenmukaisuuden arvioinnin kohteessa ja uhkaympäristössä viimeisimmän haavoittuvuusarvioinnin jälkeen tapahtuneet muutokset;

   c) lisätoimet, kuten tunkeutumistestaus, jos riskitaso on kohonnut tai esiin on tullut uusia uhkia;

   d) vähintään vuosittain valvonta- ja uudelleensertifiointiarvioinneissa tehtävä ylläpitoprosessien toimintatehokkuuden arviointi, joka kattaa ainakin versioiden, päivitysten ja haavoittuvuuksien hallintaa koskevat prosessit;

   e) ensimmäisen arvioinnin ja jokaisen uudelleensertifiointiarvioinnin jälkeen vaatimustenmukaisuustodistuksen myöntäminen läpäistyn tarkastuksen ja sertifiointipäätöksen jälkeen.

2. Taulukossa 1 esitetään neljän vuoden sykliin perustuva viiteaikataulu, jossa

   a) vuosi 1 alkaa, kun vaatimustenmukaisuustodistus myönnetään ensimmäisen kerran, ja

   b) kaikki arviointitoimet on suoritettava 12 kuukauden kuluessa edellisen vuoden arvioinnista.

3. Taulukossa 1 esitetty aikataulu on suositus, jolla varmistetaan viiveetön uudelleensertifiointi ja vältetään häiriöt lompakkoratkaisun tarjoamisessa. Muut aikataulut voivat olla mahdollisia, kunhan vaatimustenmukaisuustodistus on voimassa enintään viisi vuotta, kuten asetuksen (EU) N:o 910/2014 5 c artiklan 4 kohdassa säädetään.

4. Säännöllisten arviointien lisäksi sertifiointielimen tai vaatimustenmukaisuustodistuksen haltijan pyynnöstä voidaan käynnistää erityisarviointi sen jälkeen, kun sertifioinnin kohteessa tai uhkaympäristössä on tapahtunut merkittävä muutos.

5. Kaikki arvioinnit, mukaan lukien valvonta- ja erityisarvioinnit, voivat johtaa uuden vaatimustenmukaisuustodistuksen myöntämiseen, erityisesti jos sertifioinnin kohteessa tapahtuu merkittäviä muutoksia, mutta voimassaolon päättymispäivä pysyy samana kuin alkuperäisessä vaatimustenmukaisuustodistuksessa.

Taulukko 1

Täysi nelivuotinen arviointisykli

Ajankohta	Arvioinnin tyyppi	Toiminnot
Vuosi 0	Ensimmäinen	— Sertifioinnin kohteen täydellinen arviointi, mukaan lukien haavoittuvuusarviointi — Mukaan lukien toiminto, jolla tehdään kutakin ohjelmistokomponenttia koskevia päivityksiä. — Ylläpitoprosessien arviointi, lukuun ottamatta niiden toimintatehokkuutta — Vaatimustenmukaisuustodistuksen myöntäminen ja nelivuotisen syklin alkaminen
Vuosi 1	Valvonta	— Ylläpitoprosessien toimintatehokkuuden arviointi — Ainakin versioiden tarkistaminen, päivittäminen, haavoittuvuuksien hallinta — Tuotteen turvallisuuteen vaikuttavien muutosten arviointi

Ajankohta	Arvioinnin tyyppi	Toiminnot
Vuosi 2	Valvonta	— Koko ratkaisun haavoittuvuusarviointi — Ylläpitoprosessien toimintatehokkuuden arviointi — Ainakin versioiden hallinta, päivittäminen, haavoittuvuuksien hallinta — Tuotteen turvallisuuteen vaikuttavien muutosten arviointi
Vuosi 3	Valvonta	— Ylläpitoprosessien toimintatehokkuuden arviointi — Ainakin versioiden tarkistaminen, päivittäminen, haavoittuvuuksien hallinta — Tuotteen turvallisuuteen vaikuttavien muutosten arviointi
Vuosi 4	Uudelleensertifiointi	1) Sertifioinnin kohteen täydellinen arviointi, mukaan lukien haavoittuvuusarviointi 2) Yksinkertaistettu arviointi niistä ominaisuuksista/prosesseista, jotka eivät ole muuttuneet 3) Mukaan lukien toiminto, jolla tehdään kutakin ohjelmistokomponenttia koskevia päivityksiä. 4) Ylläpitoprosessien arviointi, mukaan lukien niiden toimintatehokkuus 5) Uuden vaatimustenmukaisuustodistuksen myöntäminen