

M72 valmistelumuistio 2021

Tunnistusmenetelmän turvallisuus, PSD2-vertailu. SSI-lausunnot.

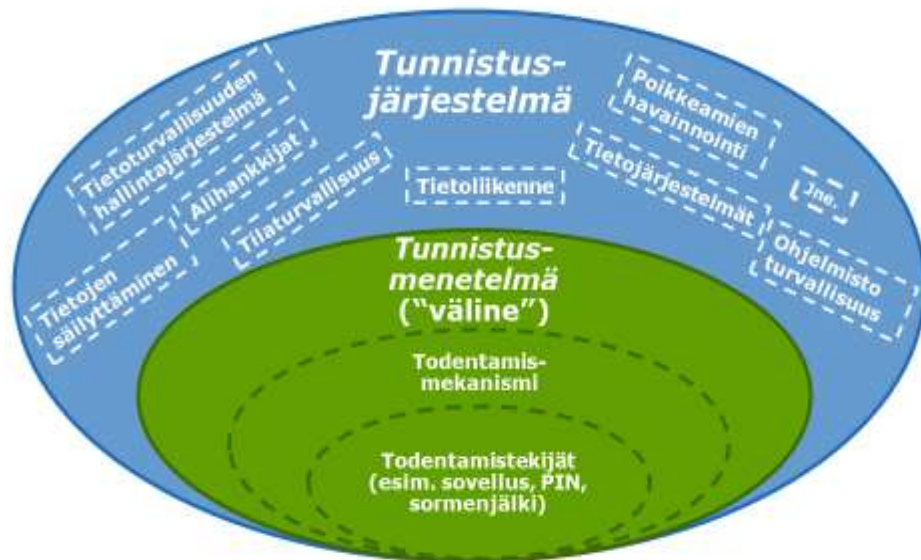
Contents

1	Kuva	3
2	Säännös ja perustelut (voimassa olevat).....	3
2.1	Säännös 6 § tunnistusmenetelmän tietoturva-vaatimukset.....	3
2.1.1	Perustelumuistio (voimassa oleva)	3
3	Lähteet vaikutusarviointiin	5
3.1	Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat	5
3.2	Lähteet, referenssit, standardit.....	5
3.3	Tunnistustilain ja maksupalvelusääntelyn vertailu (eIDAS vrt. PSD2)	6
3.3.1	Arvio sääntelyjen yhteensopivuudesta	7
3.3.2	Säädökset ja muut lähteet	7
3.3.3	Hallussapitoon perustuvat todentamistekijät yleisesti	8
3.3.4	Tunnuslukulista.....	9
3.3.5	SMS OTP (kertakäyttösalausana tekstiviestillä).....	9
3.3.6	Mobiilisovellus	10
3.3.7	Tunnuslukulaitteet	11
3.3.8	Tietoon perustuva todentamistekijä.....	12
3.3.9	Biometrinen todentamistekijä	14
3.3.10	Istunnon tunnistus, dynaaminen todentaminen/tunnistamiskoodi	15
3.3.11	Todentamistekijöiden riippumattomuus vrt. tunnistusmenetelmän ominaispiirteet ja todentamismekanismien hyökkäyksen sieto	19
3.3.12	Tietoliikenneturvallisuus tunnistuspalvelun yhteyksillä käyttäjään ja asiantuntijapalveluun.....	25
3.3.13	Tietoliikenteen osapuolten varmentaminen.....	28
3.3.1	Dynaaminen linkitys	28
3.3.2	Muut PSD2-asiat	29
3.4	Yleistä blockchain ja self sovereign identity	29
3.5	Toimialakysely 2020 muutostarpeista	30
3.5.1	Kysymys tietoturva-uhkista	30
3.5.2	Kysymys todentamistekijöistä.....	30
3.5.3	Kysymykset PSD2	30
3.5.4	Kysymykset blockchainista ja SSI:stä	33
4	2021 muutosvaihtoehdot ja vaikutusarviointi	37
4.1	Säännöksen alustava muutosehdotus	37
4.2	Todentamistekijöiden turvallisuuden sääntelytapa.....	37
4.2.1	Alustava sääntelyehdotus.....	38
4.2.2	Riskiarviomalli	38
4.2.3	Muut ohjauskeinot.....	40

4.3	Todentamistekijöiden uhkat ja turvaominaisuudet.....	40
4.3.1	Alustava sääntelyehdotus.....	40
4.3.2	Hallussapitoon perustuva todentamistekijä.....	41
4.3.3	Tietoon perustuva todentamistekijä.....	42
4.3.4	Biometriset todentamistekijät.....	43
4.3.5	Tunnistuspalveluiden kehitys.....	44
4.3.6	Taloudelliset vaikutukset.....	45
4.4	Riippumattomuus ja turvallisuus.....	45
4.4.1	Alustava sääntelyehdotus.....	45
4.4.2	Turvallisuusvaikutukset.....	46
4.5	Todentamismekanismin turvallisuus.....	46
4.5.1	Alustava sääntelyehdotus.....	46
4.5.2	Perustelut, lähteet.....	46
4.6	Blockchain ja SSI.....	47
4.6.1	Linjaus.....	47
4.6.2	Muut ohjauskeinot.....	47
5	Säädäntö	47
5.1	Määräyksen antamisen perusta	47
5.2	Arvio määräystoimivallasta	Error! Bookmark not defined.
5.3	Asiaan liittyvät säännökset.....	49
5.4	Muu sääntely.....	49

1 Kuva

Tunnistusjärjestelmä ja tunnistusmenetelmä



2 Säännös ja perustelut (voimassa olevat)

2.1 Säännös 6 § tunnistusmenetelmän tietoturvavaatimukset

6 § tunnistusmenetelmän tietoturvavaatimukset

Tunnistusvälinettä ei saa yhdistää hakijaan ennen hakijan ensitunnistamista tai tunnistusvälineen myöntämisprosessissa on muutoin varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen on tehty.

Palveluntarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.

Palveluntarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

2.1.1 Perustelumuistio (voimassa oleva)

Pykälän vaatimuksilla tarkennetaan eräitä tunnistusvälineen luomiseen ja myöntämiseen liittyviä yksityiskohtia, joihin on liittynyt soveltamiskysymyksiä. Ne koskevat yksittäisiä, lähinnä tunnistusvälineen myöntämiseen liittyviä menettelyjä, joilla turvataan sitä, että väline on ainoastaan sen oikean haltijan käytettävissä. Tunnistusmenetelmän ja -järjestelmän turvallisuudesta säädetään laajemmin tunnistus- ja luottamuspalvelulain 8 ja 8 a §:issä.

Vastaavat vaatimukset ovat muutoin olleet voimassa myös aikaisemmassa määräyksessä 8, mutta 1 momentin vaatimusta on joustavoitettu aikaisempaan nähdessä, että se sallii erilaiset prosessit tunnistusvälineen myöntämisessä.

Pykälän 2 momentin mukaan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu palveluntarjoajan henkilöstölle missään tilanteessa. Vaatimus on ollut aikaisemmassa määräyksessä ja säilytetään myös tässä määräyksessä, koska myöntämiskäytännössä on edelleen tullut vastaan tilanteita, joissa salaiset tiedot kuten PIN-koodi voivat myöntämisprosessissa tulla palveluntarjoajan henkilökunnan tietoon.

Pykälän 3 momentin vaatimuksella turvataan sitä, että salaiset tiedot ovat ainoastaan tunnistusvälineen hakijan (haltijan) tiedossa tai käytettävissä. Tällä varmistetaan se, ettei kukaan muu voi käyttää tunnistusvälinettä.

Soveltaminen

Pykälän 1 momentin vaatimus tarkoittaa sitä, että tunnistusvälineitä ei voida lähtökohtaisesti luoda ikään kuin varastoon odottamaan mahdollisia asiakkaita siten, että henkilötiedot on liitetty tunnistusvälineeseen. Ensitunnistaminen täytyy siis lähtökohtaisesti tehdä ennen kuin henkilötiedot yhdistetään tunnistusvälineeseen.

1 momentissa mahdollistetaan myös sellainen prosessi, jossa henkilötiedot yhdistetään haettuun välineeseen jos ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen tehdään. Tälle voi olla tarvetta esimerkiksi, jos ensitunnistaminen tehdään henkilökohtaisella käynnillä ja halutaan järjestää myöntämisprosessi yhdellä käynnillä. Tällaisia tarpeita on perustellusti esimerkiksi Väestörekisterikeskuksen ulkomailla oleville henkilöille myöntämien tunnistusvarmenteiden tuottamisessa.

Jos henkilötiedot yhdistetään tunnistusvälineeseen ennen ensitunnistamista, on muussa haku- ja myöntämisprosessissa käytettävä sellaisia järjestelyjä, että riski virheellisesti luoduista (väärillä henkilötiedoilla tai ilman aikomusta hakea tunnistusvälinettä) tunnistusvälineistä ja riski tunnistusvälineen päätymisestä käyttöön ennen ensitunnistamista on huomioitu. Näitä riskejä voi vähentää esimerkiksi tekemällä VTJ-tarkistuksen ennen henkilötietojen yhdistämistä välineeseen, estämällä teknisesti tunnistusvälineiden käytön ennen ensitunnistamista ja tarkistamalla, että haetut ja tilatut tunnistusvälineet vastaavat toimitettuja tunnistusvälineitä.

Viestintävirasto suosittelee ensisijaisena suojakeinona sitä, että estetään tunnistusvälineen käyttö teknisesti esimerkiksi sulkulistan avulla, kunnes sen myöntämisen ja toimittamisen edellytykset on kokonaan täytetty. Peruutettua varmennetta ei saa säädännön perusteella palauttaa käyttöön, mutta tämä kielto ei estä järjestelyä, jossa vasta vireillä oleva varmenteen käyttö on teknisesti estetty ja varmenne aktivoidaan käyttöön hakijan ensitunnistamisen jälkeen.

Tunnistusvälineen luovuttamisesta hakijalle säädetään tarkemmin tunnistus- ja luottamuspalvelulain 21 §:ssä. EU:n varmuustasoasetuksen kohdan 2.2.2. mukaan korkean varmuustason tunnistusvälineiltä edellytetään lisäksi erillistä aktivointiprosessia.

Lisäksi prosessissa täytyy luonnollisesti pitää huolta siitä, että ensitunnistaminen liittyy tunnistusvälineen myöntämiseen ja käyttäjä on tästä tietoinen. Samassa yhteydessä voidaan toki tarjota muitakin palveluita kuten matkaviestinliittymä ja tunnistaa henkilö myös niitä varten.

Pykälän 2 momentissa tarkoitettuja salaisia tietoja ovat ainakin tunnistusvälineeseen liittyvä yksityinen avain ja sen käyttöön tarvittava PIN-koodi.

Pykälän 3 momentin vaatimus tarkoittaa käytännössä sitä, että esimerkiksi tunnistusvälineeseen liittyvä PIN-koodi ei saa paljastua missään vaiheessa rekisteröintipisteen henkilöstölle, eikä sitä voi välittää sellaisten tietojärjestelmien kautta, joihin siitä jää kopio, kuten sähköpostitse.

3 Lähteet vaikutusarviointiin

3.1 Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat

Ei linjauksia erityisesti 6 §:stä.

3.2 Lähteet, referenssit, standardit

- BSI IT-Grundschutz catalogues, safeguard S 2.11 "Provisions governing the use of passwords"
- NIST 800-63-2 Appendix A Single token authentication & Password entropy of
- ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security"
- ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation".
 - o Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.
- ISO 29115
- Liikenne- ja viestintäviraston kysely 4.8.2020 tunnistus- ja luottamuspalvelumääräyksen 72 ja muun teknisen ohjauksen muutostarpeista - <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom%20kysely%204082020%20tunnistus-%20ja%20luottamuspalvelum%2072%20muutostarpeista.pdf>
- Biometrinen viitteet [täydennetään tarvittaessa]
- Tunnuslukulaitteet [täydennetään tarvittaessa]
- (EU) 2015/1502 komission varmuustasoasetus (eIDAS-varmuustasoasetus)
- eIDAS LOA Guidance 2016, eIDAS yhteistyöverkoston soveltamisohje
 - o EN: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents>
 - o Suomenkielinen käännös https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf
- eIDAS cooperation network opinions
 - o <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Opinions+of+the+Cooperation+Network>
- Overview of pre-notified and notified eID schemes under eIDAS
 - o <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS>

- (EU) 2018/389 komission delegoitu asetus direktiivin (EU) 2015/2366 (PSD2) täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla (RTS SCA & CSC)
 - o (EU) 2018/389 <https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32018R0389&from=EN>
- Euroopan pankkiviranomaisen (EBA) kannanotot ja tulkinnat Opinion RTS SCA & CSC:n tulkinnasta - EBA-Op-2018-04 RTS SCA & CSC:n tulkinnasta
 - o <https://eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018Op-04%29.pdf>
- EBA-Op-2019-06 Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2
 - o <https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf>
- EBA PSD2 Q&A prosessin mukaisia vastauksia, jotka koskevat RTS SCA & CSC sääntelyä. Työkalussa oli 25.5.2020 nähtävissä 79 tulkintavastausta
 - o https://eba.europa.eu/single-rule-book-qa/search?field_legal_act%5B%5D=517&field_legal_act_topic%5B%5D=676&field_qa_com%5B%5D=927&items_per_page=20
- SSI eIDAS Legal Report (How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market), Dr. Ignacio Alamillo Domingo April – 2020
 - o https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf
- European Blockchain Partnership (EBP) and cooperate in the establishment of a European Blockchain Services Infrastructure (EBSI)
 - o <https://ec.europa.eu/digital-single-market/en/news/european-countries-joinblockchain-partnership>

3.3 Tunnistuslain ja maksupalvelusääntelyn vertailu (eIDAS vrt. PSD2)

Tähän kohtaan on koottu sähköisen tunnistamisen sääntelyn yksityiskohtia, joiden vertailu voi olla tarpeellista yleisen toimialariippumattoman tunnistamisen (eIDAS) ja maksupalvelualan (PSD2) sääntelyjen erojen tunnistamiseksi ja erojen vaikutusten arvioimiseksi.

eIDAS-asetuksen ja tunnistuslain sääntely on

neutraalia sen suhteen, millä toimialalla ja missä palvelussa tunnistusta käytetään. Monia tunnistuslain mukaan rekisteröityjä vahvoja sähköisiä tunnistusmenetelmiä käytetään Suomessa myös maksupalvelusääntelyn mukaisena vahvana tunnistamisena.

3.3.1 Arvio sääntelyjen yhteensopivuudesta

2018

Traficom (tuolloin Viestintävirasto) ja Finanssivalvonta tarkastelivat 2018 sääntelyjen teknistä yhteensopivuutta ja pysyivät arviosta lausuntoja toimialalta Fivan PSD2-yhteistyöryhmältä ja Traficomin eIDAS-työryhmältä.

Arvion ja lausuntojen perusteella saman tunnistusmenetelmän käyttämiselle molempien sääntelyjen puitteissa ei havaittu esteitä, kunhan yksittäisistä vaatimuksista noudatetaan aina tiukempaa tai tarkempaa.

2021

Vuoden 2018 yhteistarkastelun jälkeen Fiva on linjannut, että painetut tunnuslukulistat eivät täytä maksupalvelusääntelyn vaatimuksia ilman jotain lisävahvistustekijää. Maksupalveluissa tunnistusmenetelmiin, joissa on yhtenä todentamistekijänä painettu tunnuslukulista, on lisättävä jokin tekijä tunnuslukulistan (ja haltijan tietoon tai ominaisuuteen perustuvan tekijän) lisäksi. Tyypillisesti pankit käyttävät tunnuslukulistan lisävahvistuksena tekstiviestiä eli käyttäjän on osoitettava sekä tunnuslukulistan että puhelinliittymän hallussapito.

Traficom ei ole toistaiseksi arvioinut tunnistuslain valvonnassa, että painetut tunnuslukulistat eivät kelpaisi hallussapitoon perustuvana todentamistekijänä. Tunnistuslain mukaisessa tunnistusmenetelmässä yhdistelmä tunnuslukulista + tieto tai tunnuslukulista + ominaisuus -yhdistelmä on toistaiseksi riittänyt täyttämään korotetun varmuustason vaatimukset.

Asiaa on kuitenkin ajankohtaista tarkastella uudestaan nyt määräysmuutoksen yhteydessä.

3.3.2 Säädökset ja muut lähteet

eIDAS-sääntelystä tähän on koottu poimintoja etupäässä komission varmuustasoasetuksesta (EU) 2015/1502 (eIDAS-varmuustasoasetus) ja siihen liittyvästä eIDAS Cooperation networkin laatimasta soveltamisohjeesta vuodelta 2016 (LOA Guidance 2016).

PSD2-sääntelyssä toimialakohtaiset vahvan tunnistamisen vaatimukset säädetään komission delegoidussa asetuksessa (EU) 2018/389 Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla (RTS SCA & CSC).

Kesäkuussa 2018 Euroopan pankkiviranomainen EBA julkaisi kannanoton (EBA-Op-2018-04) Opinion RTS SCA & CSC:n tulkinnasta.

Kesäkuussa 2019 EBA julkaisi kannanoton (EBA-Op-2019-06) Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2

EBA on myös julkaissut PSD2 Q&A prosessin mukaisia vastauksia, jotka koskevat RTS SCA & CSC sääntelyä. Työkalussa oli 25.5.2020 nähtävissä 79 tulkintavastausta.

3.3.3 Hallussapitoon perustuvat todentamistekijät yleisesti

LOA Guidance 2016

(FI) Hallussapitoon perustuvan todentamistekijän (esimerkiksi tunnistevälineen) olennaisena turvaominaisuutena on se, että se on yksinomaan omistajansa hallinnassa. Tämä edellyttää, että todentamistekijän jäljentäminen on kolmannelle osapuolelle niin vaikeaa ja epätoennäköistä, että tällainen vaara on merkityksetön. Varmuustasoon vaikuttaa jäljentämisyritysten sietokyky. Esimerkkejä: epäsymmetriset (yksityiset) salausavaimet, erityiseen laitteeseen (esimerkiksi älykortille) tallennetut yksityiset avaimet, ohjelmistotunnisteet, yksilöivät tunnisteet (esimerkiksi matkapuhelimen SIM-kortti) tai kertakäytöstä salasanaa (esimerkiksi RSA-tunnistetta tai paperikortilla olevaa salasanaa) käyttävät laitteet.

Tyypillisiä hallussapitoon perustuviin todentamistekijöihin kohdistuvia hyökkäyksiä ovat varkaus, toisintaminen tai väärentäminen (muuttaminen) sekä hallussapitoa koskeviin todisteisiin kohdistuvat hyökkäykset todentamishetkellä.

(EN) The relevant security characteristic of a possession-based authentication factor (e.g. token) is the sole control of it by the owner. This implies that it is important that reproduction of it by a third party is so difficult and unlikely that the risk of this is negligible. The Level of Assurance depends on the level of resistance against reproduction. For example: asymmetric cryptographic (private) keys, the private keys may be stored on dedicated hardware devices (e.g. smartcards), or software token, uniquely identifiable token (e.g. the SIM card of a cell phone) or devices with one-time-passwords (e.g. "RSA-Token" or printed cards).

Typical attacks on possession-based authentication factors are theft, duplication or tampering (manipulation), as well as attacks on the proof-of-possession during authentication.

Ks. EBA-Op-2019-06

30. Table 2 summarises the views expressed above on what does or does not constitute a possession element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.

- *Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP) - Yes**
- *Possession of a device evidenced by a signature generated by a device (hardware or software token) - Yes**
- *Card or device evidenced through a QR code (or photo TAN) scanned from an external device - Yes**
- *App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device - Yes**

- *Card evidenced by a card reader - Yes**
- *Card with possession evidenced by a dynamic card security code - Yes**

**Compliance with SCA requirements is dependent on the specific approaches used in the implementation of the elements.*

3.3.4 Tunnuslukulista

Tunnuslukulista on hallussapitoon perustuva todentamistekijä, joka on erityisen altis mm. kalastelulle.

Ks. LOA Guidance edellisessä kohdassa.

Tunnistustekijän nojalla paperisia tunnuslukulistoja ei toistaiseksi ole valvonnassa katsottu vaatimustenvastaiseksi korotetulla varmuustasolla. eIDAS-säätelyssä vertaisarvioinneissa tekijä on tullut esille Tanskan tunnistusjärjestelmän vertaisarvioinnissa, jonka yhteydessä Tanska on ilmoittanut luopuvansa tunnuslukulistoista. Ks. eIDAS Cooperation network Opinion 1/2020 <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=200867911>

Finanssivalvonta on linjannut, ettei tunnuslukulista täytä hallussapitoon perustuvan todentamistekijän vaatimuksia ilman vahvistustekijää ja tunnistusvälineen tarjoajat ovat esim. lisänneet listan käyttöön maksupalvelutapahtumissa tekstiviestivahvistuksen. Linjaus perustuu RTS SCA & CSC:ssä 7 artiklassa säädettyyn nimenomaiseen vaatimukseen.

Ks. EBA-Op-2019-06

28. Following the publication of the EBA Opinion on the implementation of the RTS, which stated that the card details and card security code that are printed on the card cannot constitute a knowledge element, a number of industry participants have queried if such details could constitute a possession element. The EBA is of the view that such details cannot do so for approaches currently observed in the market, in particular given the requirements under Article 7 of the RTS, and it advises CAs to closely monitor their application. That being said, dynamic card security codes (where the code is not printed on the card and changes regularly) may provide evidence of possession in line with Article 7 of the RTS.

29. The EBA is also of the view that printed matrix cards or printed OTP lists that are designed to authenticate the PSU are not a compliant possession element for approaches currently observed in the market, for similar reasons to those mentioned for card details above, namely that they are unlikely to comply with the requirements under Article 7 of the RTS.

3.3.5 SMS OTP (kertakäyttösalasana tekstiviestillä)

Tekstiviestillä lähetettävä kertakäyttösalasana on puhelimen hallussapitoon perustuva todentamistekijä, joka on altis mm. tekstiviestin lähettäjän väärennöksille ja vastaanoton kaappaamiselle.

eIDAS-säätelyssä asiaan ei ole vakiintunutta kantaa, mutta eräiden vertaisarviointien yhteydessä on arvioitu, että SMS OTP ei täytä korkean varmuustason hyökkäyksen sietovaatimuksia.

Ks. EBA Q&A

Kysymys 2018_4039 Qualification of SMS OTP as an authentication factor

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039

Paragraph 35 of the [EBA opinion on the implementation of the Commission Delegated Regulation \(EU\) 2018/389](#) (Regulatory Technical Standards on Strong customer authentication and secure communication) clarifies that "For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device".

In this context, a one-time password sent via SMS would constitute a possession element and should therefore comply with the requirements under Article 7 of the Delegated Regulation, provided that its use is 'subject to measures designed to prevent replication of the elements', as required under Article 7(2) of this Delegated Regulation. The possession element would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number.

In addition, regardless of whether a strong customer authentication element is possession, knowledge or inherence, Article 22(1) of the [Delegated Regulation](#) requires that "payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication" and Article 22(4) of the Delegated Regulation states that "payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognised industry standards".

Ks. EBA-Op-2019-06

25. As stated in the EBA Opinion on the implementation of the RTS (paragraph 35), a device could be used as evidence of possession, provided that there is a 'reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device'. Evidence could, in this context, be provided through the generation of a one-time password (OTP), whether generated by a piece of software or by hardware, such as a token, text message (SMS) or push notification. In the case of an SMS, and as highlighted in Q&A 4039, the possession element 'would not be the SMS itself, but rather, typically, the SIM-card associated with the respective mobile number'.

3.3.6 Mobiilisovellus

Mobiilisovellus on puhelimen hallussapitoon perustuva todentamistekijä, jonka turvallisuus riippuu siitä, mitä turvaominaisuuksia puhelimessa ja sen käyttöjärjestelmässä on tarjolla ja käytetäänkö niitä. Lisäksi turvallisuuteen vaikuttaa tietoliikenneyhteys taustajärjestelmään ja taustajärjestelmän turvallisuus.

eIDAS-sääntelyn ja tunnistus- ja luottamuspalvelulain vaatimusten valvonnassa ja tulkinnessa merkitykselliset tekijät ilmenevät Liikenne- ja viestintäviraston ohjeessa 211/2019 osan C mobiilisovelluskriteeristöä. Tarkastelutapa vastaa EU-vertaisarvioinneissa syntyneitä yhteistoimintaryhmän linjauksia sääntelyn turvallisuusvaatimuksista. Mobiilisovelluksen käyttö korkealla varmuustasolla edellyttäisi turvaelementtien sertifiointia.

eIDAS-varmuustasoasetus

Johdantokappale (11) *Kansainvälisiin standardeihin perustuva tietotekninen tietoturvasertifiointi on tärkeä väline tarkastettaessa, vastaatko tuotteet turvallisuudeltaan tämän täytäntöönpanosäädöksen vaatimuksia*

EBA Q&A

Kysymys 2018-4047 liittyy asiaan ja siinä todetaan tarve arvioida sovellusturvallisuutta ja esim. käyttää SEE-elementtiä

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4047

Ks. EBA-Op-2019-06

24. Article 4(30) of PSD2 defines possession as 'something only the user possesses'. Possession does not solely refer to physical possession but may refer to something that is not physical (such as an app). Recital 6 of the RTS refers to the requirement to have adequate security features in place and provides examples of possession, 'such as algorithm specifications, key length and information entropy'. Article 7 of the RTS refers to the requirement for PSPs to have mitigation measures to prevent unauthorised use and to have measures designed to prevent the replication of the elements.

26. The EBA is of the view that approaches relying on mobile apps, web browsers or the exchange of (public and private) keys may also be evidence of possession, provided that they include a device binding process that ensures a unique connection between the PSU's app, browser or key and the device. This may, for instance, be through hardware crypto-security, web-browser and mobile-device registration or keys stored in the secure element of a device. By contrast, an app or web browser that does not ensure a unique connection with a device would not be a compliant possession element.

3.3.7 Tunnuslukulaitteet

Tunnuslukulaite on hallussapitoon perustuva todentamistekijä, jonka turvallisuuteen vaikuttavat laitteen ohjelmisto, käytetyt algoritmit ja fyysiset komponentit.

eIDAS-varmuustasoasetus

Johdantokappale (11) *Kansainvälisiin standardeihin perustuva tietotekninen tietoturvasertifiointi on tärkeä väline tarkastettaessa, vastaatko tuotteet turvallisuudeltaan tämän täytäntöönpanosäädöksen vaatimuksia*

Traficom on neuvontamuistiossaan 12/2018 edellyttänyt, että vuoden 2019 määräaika-arviointien yhteydessä arvioidaan tunnuslukulaitteiden turvallisuus.

Laitteiden sertifiointia ei ole toistaiseksi vaadittu korotetulla varmuustasolla, mutta korkealla varmuustasolla sertifiointia voisi pitää perusteltuna ottaen huomioon vaadittu hyökkäyksensietokyky.

EBA:n seuraavassa lausunnossa otetaan kantaa hallussapidon osoittamiseen. Itse laitteen turvallisuusvaatimuksista ei löytynyt kantaa.

EBA-Op-2018-04

35. ...For a device to be considered possession, there needs to be a reliable means to confirm possession through the generation or receipt of a dynamic validation element on the device.

3.3.8 Tietoon perustuva todentamistekijä

LOA Guidance 2016

(FI) Tiedossaoloon perustuva todentamistekijä on sellainen, joka on todennäköisesti vain tekijän haltijan sekä varmentavan tahon tiedossa. Esimerkkejä ovat PIN-koodit, salasanat, muistettavat sanat tai päivämäärät, tunnuslauseet, aiemmin rekisteröidyt tiedot ja muut vastaavat tiedot, jotka ovat todennäköisesti vain henkilön omassa tiedossa. Joissakin tapauksissa edes varmentava taho ei tiedä varsinaista tiedossaoloon perustuvaa todentamistekijää, mutta se kykenee varmistamaan, että sen ja hakijan tiedossa on tarkalleen sama tieto; esimerkkinä on salasanan tiivisteen käyttäminen.

Jos tietoa käytetään todentamistekijänä, on syytä yrittää tehdä kyseisen tiedon arvaamisesta (joko satunnaisesti tai ns. raajan voiman/laskentatehon avulla) vastapuolelle mahdollisimman vaikeaa. Esimerkki: kun tieto on salasanana, hyvä toimintatapa edellyttää sopivaa salasana-käytäntöä (ks. esimerkiksi BSI IT-Grundschutz -opas S.2.11 "Provisions concerning the use of passwords" sekä NIST 800-63-2, liite A, kohdat "Single Token Authentication" ja "Password Entropy").

Tyypillisiä tiedossaoloon perustuviin todentamistekijöihin kohdistuvia hyökkäyksiä ovat arvaaminen, tietojen kalastelu (phishing), salakuuntelu tai toisintaminen. Tiedossaoloon perustuvilla todentamistekijöillä ominaista on, että sähköisen tunnistamisen menetelmää käyttävä henkilö ei välttämättä edes huomaa hyökkäyksiä. Esimerkkejä: raakaan voimaan tai sanakirjan käyttöön perustuvat hyökkäykset, joiden kohteena ovat salasanat, joiden entropia on heikko ja joita kysyttäessä ei lasketa uudelleenyritysten määrää; kirjeestä tai sähköpostiviestistä haltijan tai varmentajan huomaamatta kopioidut salasanat.

(EN) The knowledge-based factor likely to be known only by the owner of the factor and the verifying entity, for example: PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to only be known by the subject. In some cases even the verifying entity may not know the actual knowledge-based factor, but are able confirm that they and the applicant know the exact same information, for example using the hash of a password.

If knowledge is used as a factor it is necessary to mitigate against guessing (either random or brute force) of the knowledge by an adversary. For example: where the knowledge is a password, good practice prescribes a suitable password policy (e.g. see safeguard S 2.11 "Provisions governing the use of passwords" of the BSI IT-Grundschutz catalogues, Single token authentication & Password entropy of NIST 800-63-2 Appendix A).

Typical attacks on knowledge-based authentication factors are guessing, phishing eavesdropping or duplication. A characteristic of knowledge-based factors is that attacks are not necessarily noticed by the subject of the electronic identification means. For example: brute force/dictionary attacks on a password with low entropy and without retry counter or a password that has been copied from a letter or email without knowledge of the owner or the verifier.

EBA-Op-2019-06

31. Article 4(30) of PSD2 defines knowledge as 'something only the user knows'. Article 6 of the RTS refers to the requirement for PSPs to mitigate the risk that the element is 'uncovered by, or disclosed to, unauthorised parties' and to have mitigation measures in place 'in order to prevent their disclosure to unauthorised parties'.

32. The EBA is of the view that the following elements could constitute a knowledge element: a password, a PIN, knowledge-based responses to challenges or questions, a passphrase and a memorised swiping path (as opposed to keystroke dynamics, namely the manner in which the PSU types or swipes, which may be considered an inherence element).

34. The same opinion also stated that a user ID (username) would not constitute a compliant knowledge element. Neither would an email address.

36. Table 3 summarises the views expressed above on what does or does not constitute a knowledge element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.

- Password - Yes*
- PIN - Yes
- Knowledge-based challenge questions - Yes*
- Passphrase - Yes*
- Memorised swiping path - Yes*
- Email address or user name - No
- Card details (printed on the card) - No
- OTP generated by, or received on, a device (hardware or software token generator, SMS OTP) - No (for approaches currently observed in the market)
- Printed matrix card or OTP list - No

**Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.*

3.3.9 Biometrinen todentamistekijä

Biometrisen todentamistekijän käyttö liittyy nykyisissä tunnistusmenetelmissä yleensä mobiililaitteen ominaisuuksilla toteutettuun sormenjäljen tai kasvotunnistuksen käyttöön mobiilisovelluksessa. Muita biometrisen tekijän lukulaitteita käyttäjille ei tällä hetkellä juurikaan ole tarjolla tai käytössä. Biometrisen todentamistekijän turvallisuus riippuu mm. sensoreiden tarkkuudesta ja biometristä tietoa käsittelevän ohjelmiston ja laitteiston toteutustavasta.

eIDAS-sääntelyssä tai määräyksessä 72 ei ole eriteltyjä vaatimuksia biometriselle todentamistekijälle, vaan sen turvallisuuden ja luotettavuuden arviointi on osa tunnistusmenetelmän ja todentamismekanismien hyökkäyksenkeston kokonaisarviointia.

Belgian mobiilisovelluksen perustuvan tunnistusmenetelmän vertaisarvioinneissa on 2019 linjattu, että biometrinen todentamistekijä ei ole riittävän luotettava korkealla varmuustasolla. Ks. eIDAS Cooperation network Opinion 8/2019
<https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=148898042&src=contextnavpagetreemode>

LOA Guidance (määritelmän soveltamisohje)

(FI) Luontaisissa todentamistekijöissä on syytä olla vaihtelua myös ominaisuuksiltaan samanlaisten ihmisten välillä, jotta henkilön yksilöinti on mahdollista; esimerkkejä ovat sormenjälki, kämmenjälki, kämmenen verisuonisto, kasvot, käden geometria ja silmän iiris.

Biometrisiä tekijöitä käytettäessä on tärkeää varmistaa, että henkilö, johon todentamistekijä liittyy, on varmentamispaikassa fyysisesti läsnä. Näin vähennetään huijausten tai toisintamisen vaaraa.

(EN) Inherent authentication factors should have a variance even between people of similar characteristics so that a person may be uniquely identified, for example: fingerprints, palm prints, palm veins, face, hand geometry, iris, etc.

A key consideration when a biometric factor is being used is to ensure that the person to whom it relates is physically present at the point of verification. This is to mitigate against spoofing or duplication.

EBA-Op-2019-06

17. Article 4(30) of PSD2 defines inherence as 'something the user is'. Article 8 of the RTS on SCA and CSC refers to the 'authentication elements categorised as inherence and read by access devices and software' and recital 6 refers to the need to have 'adequate security features' in place that could, for example, be 'algorithm specifications, biometric sensor and template protection features'.

18. As stated in the Opinion on the implementation of the RTS, inherence may include behavioural biometrics identifying the specific authorised user. The EBA is of the view that inherence, which includes biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. In addition, it is (the quality of) the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence

element. Inherence is the category of elements that is the most innovative and fastest moving, with new approaches continuously entering the market.

20. The swiping path memorised by the PSU and performed on a device would not constitute an inherence element, but may rather constitute a knowledge element, something only the user knows.

22. Table 1 summarises the views expressed above on what does or does not constitute an inherence element under the RTS on SCA and CSC. The table is for illustrative purposes only and is not intended to be exhaustive; the possible elements included reflect current practices and developments in the market at the time of publication of the opinion.

Table 1 — Non-exhaustive list of possible inherence elements

- *Fingerprint scanning - Yes*
- *Voice recognition - Yes*
- *Vein recognition - Yes*
- *Hand and face geometry - Yes*
- *Retina and iris scanning - Yes*
- *Keystroke dynamics - Yes*
- *Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices) - Yes*
- *The angle at which the device is held - Yes*

**Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.*

3.3.10 Istunnon tunniste, dynaaminen todentaminen/tunnistamiskoodi

Vaatus liittyy siihen, että jokaisen tunnistusistunnon täytyy olla ainutkertainen, eikä se saa olla toistettavissa. Istunto/tunnistustapahtuma perustuu todentamistekijöiden käyttöön ja mm. salaukseen.

Tunnistustilain ja eIDAS-asetuksen vaatimukset sisältyvät yleiseen dynaamisen todentamisen vaatimukseen ja todentamismekanismiin hyökkäyksensietoon:

Todentamismekanismia ja hyökkäyksen sietokykyä käsitellään jäljempänä.

eIDAS-varmuustasoasetus

Liite kohta 1 Määritelmät

3) 'dynaamisella todentamisella' tarkoitetaan sähköistä prosessia, jossa käytetään salausta tai muita tekniikoita, joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot, sekä muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa;

Liite kohta 2.3.1 Todentamismekanismi

Korotettu varmuustaso

1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käytämällä dynaamista todentamista.

LOA Guidance 2016

(FI) Dynaamisen todentamisen ensisijainen tarkoitus on vähentää esimerkiksi mies välissä (Man in the Middle) -tyyppisten hyökkäysten vaaraa tai riskiä siitä, että aiemmin tallennetun todentamiskerran varmentamistietoja käytetään uudelleen. Tähän sisältyvät esimerkiksi seuraavat:

☐ *replay-hyökkäykset eli varmentamistietojen kaappaaminen ja uudelleen käyttäminen toisessa todentamistilanteessa*

tietynlaiset istuntokaappaukset, esimerkiksi tapaukset, joissa vaihdetaan keskenään osittain tai kokonaan kaksi tai useampia yhtäaikaista todentamistilanteita.

On syytä muistaa, että useaan tekijään perustuva ja dynaaminen todentaminen eivät tarkoita samaa asiaa. Useaan tekijään perustuvassa todentamisessa ei edellytetä, että todentaminen tapahtuu dynaamisesti (esimerkkejä ovat PIN-koodi ja sormenjälkitiedot), joten tällainen todentamistapa voi olla alttiimpi replay-hyökkäykselle kuin dynaaminen todentaminen.

Dynaaminen todentaminen voidaan toteuttaa todentamistekijän avulla (esimerkiksi laitteesta saatava kertakäyttöinen avain) tai todentamismekanismeilla (esimerkiksi dynaaminen kysymys haaste-vaste-todentamisessa).

Esimerkkejä dynaamisista todentamistavoista:

☐ *henkilön hallussa oleva älykortti, jolle tallennettu yksityinen avain varmennetaan haaste-vaste-menetelmällä*

☐ *protokollat, jotka perustuvat tilapäisiin Diffie-Hellman-avaimiin ja tuottavat todentamismenetelmän (esimerkiksi PACE), salaukseen tarkoitetun tilapäismuodosteen (nonce), aikaleiman ja/tai kertaluontaisen numerosarjan.*

☐ *protokollat, jotka perustuvat staattisesti muodostettuihin tilapäisiin DiffieHellman-avaimiin, jos luottava osapuoli antaa tilapäisen avaimen (esimerkiksi laajennettu pääsynvalvonta)*

☐ *dynaamisesti muodostettavat kertakäyttöiset pääsykoodit (esimerkiksi OTP-tunnisteet) tai haaste-vaste-protokollat, joissa kertakäyttöinen koodi on tuotettu aiemmin ja jaettu kaistan ulkopuolella ja joissa koodi valitaan dynaamisesti todentamisen yhteydessä (esimerkiksi OTP-kortit).*

Jos henkilön yksityinen avain on tallennettu etäpalveluna (keskitetysti esimerkiksi tunnistustietojen tarjoajan käyttämälle HSM-laitteelle), yksityisen avaimen käyttämiseen vaadittavan todentamistavan on myös oltava dynaaminen.

(2.3.1) Käytännössä tämä tarkoittaa sitä, että todentamistavassa on oltava mukana joko kertakäyttöinen koodi tai kertakäyttöinen haaste-vaste, jotta voidaan varmistaa, että se on aidosti dynaaminen. Kertakäyttöinen koodi tai kysymys on muodostettava siten, ettei sitä ole mahdollista muuttaa.

Jos haaste-vaste-protokollassa käytetään satunnaisia numeroita, kyseisten numeroiden laatu on varmistettava huolellisesti esimerkiksi noudattamalla salauksella suojattujen näennäissatunnaislu-kugeneraattoreiden käyttöä koskevia hyviä toimintatapoja.

(EN) The primary purpose of dynamic authentication is to mitigate against attacks such as 'man-in-the-middle' or misusing verification data from a previously recorded authentication replay to the verifier. This includes:

- replay attacks, i.e. intercepting verification data and reusing them in a different authentication context*
- certain types of session hijacking, e.g. exchanging (parts of) the authentication contexts of two or more simultaneously occurring authentications.*

It is important to understand that multifactor and dynamic authentication are not the same; multifactor authentication does not require that the authentication is dynamic (e.g. PIN and fingerprint) and can therefore be more exposed to replay attack than a dynamic authentication.

Dynamic authentication might be implemented by the authentication factor (e.g. a one time key from a device) or by the authentication mechanism (e.g. dynamic challenge in a challenge-response authentication).

Examples for dynamic authentications are:

- possession of a private key stored on a smart card and verified using a challenge-response-protocol*
- protocols based on an ephemeral Diffie-Hellman and providing authentication (e.g. PACE), cryptographic nonces, timestamps and/or non-repeating sequence numbers.*
- protocols based on a static-ephemeral Diffie-Hellman, if the ephemeral key is provided by the relying party (e.g. EAC)*
- dynamically generated one time access code (e.g. OTP tokens) or challenge response protocols where the one time code has been previously generated and distributed out of band but selected dynamically during authentication (e.g. OTP cards)*

If the subject's private key is stored remotely (centrally stored, e.g. in an HSM operated by the identity provider), the authentication used to access the private key should also be dynamic.

(2.3.1) In practice this means the authentication means should include either a one-time code or one time challenge-response to ensure it is truly dynamic. The one-time code or challenge should be generated in a way where it cannot be tampered with.

When using random numbers in a challenge-response protocol care should be taken to ensure the "quality" of these numbers, for example by following good practice for cryptographically secure pseudo-random number generators.

PSD2, RTS SCA & CSC -asetus

Johdantokappale 4) Dynaamisen yhdistämisen mahdollistaa tunnistamiskoodien tuottaminen, jonka on täytettävä tiukat turvallisuusvaatimukset. Teknologianeutraaliuden säilyttämiseksi ei saisi vaatia, että tunnistamiskoodit toteutetaan tietyllä teknologialla. Sen vuoksi tunnistamiskoodien olisi perustuttava sellaisiin ratkaisuihin kuin kertakäyttösalasanojen tai digitaalisten allekirjoitusten tuottaminen ja validointi tai muut salaukseen perustuvat validiuden vahvistamiset, joissa käytetään tunnistamisen tekijöihin tallennettuja avaimia tai salausteknistä aineistoa, edellyttäen, että turvallisuusvaatimukset täytetään.

RTS SCA & CSC 4 artikla Tunnistamiskoodi

1. Jos maksupalveluntarjoajat soveltavat asiakkaan vahvaa tunnistamista direktiivin (EU) 2015/2366 97 artiklan 1 kohdan mukaisesti, tunnistamisen on perustuttava kahteen tai useampaan tekijään, jotka kuuluvat ryhmiin "tieto", "hallussapito" ja "erityinen ominaisuus", ja sen on johdettava tunnistamiskoodin tuottamiseen.

Maksupalveluntarjoajan on hyväksyttävä tunnistamiskoodi ainoastaan kerran, kun maksaja käyttää sitä päästäkseen maksutililleen verkon kautta, käynnistääkseen sähköisen maksutapahtuman tai toteuttaakseen etäkanavan kautta minkä tahansa toimen, joka voi aiheuttaa maksupetoksen tai muunlaisen väärinkäytöksen riskin.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on toteutettava turvatoimenpiteet, joilla varmistetaan kaikkien seuraavien vaatimusten täyttyminen:

- a) tunnistamiskoodin ilmoittamisesta ei ole mahdollista johtaa mitään tietoja 1 kohdassa tarkoitetuista tekijöistä;
- b) uutta tunnistamiskoodia ei ole mahdollista tuottaa mihinkään muuhun, aiemmin tuotettuun tunnistamiskoodiin liittyvien tietojen perusteella;
- c) tunnistamiskoodin väärentäminen ei ole mahdollista.

3. Maksupalveluntarjoajien on varmistettava, että tunnistamiseen, joka perustuu tunnistamiskoodin tuottamiseen, kuuluvat kaikki seuraavat toimenpiteet:

- a) jos tunnistamisessa, joka suoritetaan etäkäyttöä, sähköisiä etämaksuja ja muita toimia varten etäkanavan kautta, johon voi liittyä maksupetoksen tai muunlaisen väärinkäytöksen riski, ei ole kyetty tuottamaan tunnistamiskoodia 1 kohdan tarkoituksia varten, ei ole mahdollista määrittää, mikä mainitussa kohdassa tarkoitetuista tekijöistä on ollut virheellinen;
- b) tunnistamisyhtiöksiä, jotka voidaan tehdä peräkkäin, minkä jälkeen direktiivin (EU) 2015/2366 97 artiklan 1 kohdassa tarkoitettut toimet estetään väliaikaisesti tai pysyvästi, saa olla enintään viisi tietyn ajanjakson aikana;
- c) viestintäistunnot suojataan tunnistamisen aikana lähetettävien tunnistamistietojen sieppaamiselta ja oikeudettomien tahojen suoritamalta manipuloinnilta V luvun vaatimusten mukaisesti;

d) *enimmäisaika, jonka maksaja voi olla passiivinen sen jälkeen, kun se on tunnistettu verkon kautta tapahtuvaa maksutilin käyttöä varten, on viisi minuuttia.*

EBA Q&A 2018-4053, jossa käsitellään tunnistuskoodin turvallisuutta.

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4053

Article 4(2) of the Commission Delegated Regulation (EU) 2018/389 states that no information on any of the two elements necessary for strong customer authentication can be derived from the disclosure of the authentication code; that no new authentication code should be generated based on the knowledge of any other authentication code previously generated and that such code cannot be forged. Article 4(3) and 4(4) of the Delegated Regulation provides further requirements on authentication codes. Recital 4 of the Delegated Regulation states that "authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled". The Delegated Regulation does not specify the length for the authentication code. Accordingly, a three decimal-digit authentication code could be valid, providing that it complies with the requirements under the Delegated Regulation and in particular, that it is resistant against the risk of being forged in its entirety or by disclosure of any of the elements from which the code was generated.

Further, given that 'the authentication code shall be only accepted once' as stated in Article 4(1) phrase 2 of the Delegated Regulation meaning a 3-decimal digit authentication code would only give 1000 combinations, and since Article 4(3)(b) of the Delegated Regulation specifies the maximum of 5 failed authentication attempts, there is a higher probability of guessing the value of the authentication code.

Arvio: RTS SCS & CSC:n 4 artiklan tunnistuskoodin vaatimus koskee samoja asioita kuin eIDAS-säätelyn dynaamisen todentamisen ja todentamismekanismin hyökkäyksenkestävyyden vaatimus. eIDAS-säätelyn kannalta samaa asiaa suojataan mm. määräyksen 7 §:n salausvaatimuksilla.

3.3.11 Todentamistekijöiden riippumattomuus vrt. tunnistusmenetelmän ominaispiirteet ja todentamismekanismin hyökkäyksensieto

eIDAS-säätelyssä tai määräyksessä 72 ei ole eriteltyjä vaatimuksia todentamistekijöiden riippumattomuudesta, vaan se on osa tunnistusmenetelmän ominaispiirteiden ja todentamismekanismin hyökkäyksenkestävyyden kokonaisarviointia (varmuustasoasetus Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu sekä 2.3.1 Todentamismekanismi)

eIDAS-varmuustasoasetus

Liite kohta 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja laatiminen

Korotettu varmuustaso

1. Sähköisen tunnistamisen menetelmässä käytetään vähintään kahta todentamistekijää eri todentamistekijäluokista

2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa, jolle se kuuluu.

Korkea varmuustaso

Taso "korotettu" lisättynä seuraavalla:

1. Sähköisen tunnistamisen menetelmä on suojattu toisintamiselta ja väärentämiseltä sekä hyökkäyksiltä, joiden vakavuusaste on korkea ("high").

2. Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.

Liite kohta 2.3.1 Todentamismekanismi

Korotettu varmuustaso

1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käytämällä dynaamista todentamista.

2. Todentamismekanismeissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen ("moderate"), voi heikentää todentamismekanismeja.

Korkea varmuustaso

Taso "korotettu" lisättynä seuraavalla:

Todentamismekanismeissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea ("high"), voi heikentää todentamismekanismeja.

LOA Guidance 2016

(FI)(1. todentamistekijän määritelmä) Useaan tekijään perustuvaa todentamista käytettäessä eri tekijät on valittava niin, että niillä torjutaan eri uhkia/hyökkäystapoja.

Todentamisen tehokkuutta arvioitaessa on syytä ottaa huomioon paitsi itse tekijä tai tekijät, myös tekijöiden varmentamisessa käytettävä menettely.

(2.2.1) Useiden eri luokkiin kuuluvien todentamistekijöiden käyttämisellä toinen toisiaan täydentävästi voidaan parantaa tunnistamismenetelmän yleistä turvallisuustasoa. Yleinen esimerkki on hallussapitoon perustuvan tunnisteiden yhdistäminen salasanaan tai PIN-koodiin, joilla tunniste avataan. Vaikka tunniste katoaa tai varastetaan, sitä ei voi käyttää todentamiseen ilman PIN-koodia.

(2.2.1) Suojaamisella toisintamiselta ja väärentämiseltä tarkoitetaan koko sähköisen tunnistamisen menetelmää, ei pelkästään yksittäisiä todentamistekijöitä. Eri todentamistekijöiden käytöllä on tarkoitus vähentää riskiä, sillä eri luokkiin kuuluvat todentamistekijät ovat alttiita erilaisille uhkille. Salasanoja saatetaan saada haltuun, kun henkilöt tai järjestelmät käyttävät niitä (esimerkiksi näppäinnauhuri ohjelman avulla) tai jos ne on kirjoitettu muistiin, hallussapitoon perustuvat todentamistekijät saatetaan varastaa tai ne voivat kadota, luontaisiin todentamistekijöihin perustuvat järjestelmät saattavat olla alttiita väärennetyjen todisteiden käytölle (esimerkiksi henkilöiden samannäköisyys, todellisten biometristen ominaisuuksien muuttaminen, keino-tekoiset todisteet ja latex-sormenjäljet).

Esimerkkejä yhteen tekijään kohdistuvalta väärentämiseltä ja toisintamiselta suojaamisesta ovat mm. seuraavat:

- ☐ Hallussapitoon perustuvat todentamistekijät: salausavainaineisto upotetaan väärentämiseltä suojattuun laitteeseen, jolla estetään avaimen joutuminen laitteen ulkopuolelle tai sen fyysinen tai sähköinen väärentäminen laitteen sisällä; HSM-laite
- ☐ Luontaiset todentamistekijät: elävyyden havainnointi, luotettu ympäristö, alhainen virheellisten hyväksyntöjen osuus

Hyvää toimintatapaa noudatettaessa sähköisen tunnistamisen menetelmäksi valitaan sellainen, jonka on osoitettu pystyvän vastustamaan väärentämis- ja toisintamisyrityksiä. Menetelmä on esimerkiksi testattu huolellisesti ja sertifioitu asiaankuuluvien teknisten standardien (kuten CC) mukaisesti.

(2.2.1) "Luotettava suojaaminen" tarkoittaa toimenpiteitä, joiden avulla sähköisen tunnistamisen menetelmä voidaan suojata niin, ettei sitä voi käyttää henkilön tietämättä ja ilman hänen aktiivista suostumustaan. Esimerkiksi salausavaintunnisteen yksityinen avain ei voi olla sellainen, jota voidaan käyttää koneellisissa prosesseissa ilman käyttäjän aktiivista suostumusta (kuten PIN-koodin antamista).

Tällä vaatimuksella suojaudutaan toisintamisen, arvaamisen, toiston ja viestinnän väärentämisen muodostamilta uhilta.

Edellä mainittujen tekniikoiden lisäksi voidaan käyttää myös seuraavia:

- ☐ vahvat staattiset salasanat
- ☐ käyttäjän biometrinen varmentaminen
- ☐ ympäristön tarkistaminen haitallisen koodin varalta
- ☐ kaistan ulkopuolella tapahtuva varmentaminen.
- ☐ Kaikkien salassa pitämiseen perustuvien todentamistekijöiden (staattiset salasanat, laitteiston kertakäyttöiset salasanat) osalta arvaaminen muodostaa uhan, jota on syytä lieventää korkean varmuustason saavuttamiseksi esimerkiksi rajaamalla yritysten määrää tai käyttämällä hidastusmekanismeja sekä huolehtimalla riittävästä entropiasta.

(2.3.1) Todentamisvaiheessa käytetyillä todentamismekanismeilla ei voi estää täysin kaikkia hyökkäyksiä, vaan niillä voidaan vain vastustaa hyökkäyksiä tietyllä turvallisuus- tai varmuustasolla. Tavanomainen tapa mitata eri mekanismien tuottamaa sietokykyä on asettaa

mekanismit järjestykseen sen mukaan, miten hyvin ne kestävät tietyn vakavuusasteen hyökkäyksiä (eli hyökkääjän voimaa).

Varmuustasossa eri vakavuusasteista käytettävät termit ovat "korkeampi perustaso" (enhanced-basic), "kohtuullinen" (moderate) ja "korkea" (high). Nämä termit on lainattu standardeista ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standardien teksti on vapaasti luettavissa osoitteessa www.commoncriteriaportal.org/cc (CCPART1-3 vastaa standardia ISO/IEC 15408 ja CEM standardia ISO/IEC 18045).

Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismeja] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.

Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.

Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.

Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.

Hyökkäysten sietokyvyn arvioinnissa on syytä ottaa huomioon koko todentamismekanismi, myös sähköisen tunnistamisen menetelmän hallussapidon varmentamisesta aiheutuvat riskit.

Esimerkkejä:

- ☐ *Korkeassa varmuustasossa ei riitä, että älykortti suojaa salausavainta korkean vakavuustason väärentämisyrityksiltä, vaan myös salausprotokollan on suojattava avaimen hallussapidon varmentamista korkean vakavuustason väärentämis- tai toistoyrityksiltä.*
- ☐ *Kun kyse on kertakäyttöisestä salasanatunnisteesta, jossa muodostettu kertakäyttösalasana toimitetaan suojatussa kanavassa (esimerkiksi TLS), hallussapitoon perustuvan tekijän vahvuuteen vaikuttavat tunnisteiden vahvuus ja suojatun kanavan vahvuus.*
- ☐ *Aikaperusteiselle kertakäyttösalasanojen muodostajalle hallussapidon todistamismekanismi on muodostetun kertakäyttösalasanan lähettäminen varmentajalle. Tämän mekanismin vahvuutta rajoittaa muun muassa kertakäyttösalasanan pituus, salasanan voimassaoloaika sekä toimitustavan luottamuksellisuus.*

Riskinarvioinnissa on otettava huomioon kohtuulliset olettamukset sellaisten komponenttien turvallisuustasosta, joita todentamisjärjestelmä

hyödyntää, mutta jotka eivät ole sen osia (esimerkiksi käyttäjän ympäristö, selain ja älypuhelin).

Komponentteja voidaan käyttää eri kokoonpanoissa ja eri suojausasetuksilla.

Arvioinnissa voidaan esimerkiksi olettaa, että käyttäjän tietokone on suojattu palomuurilla ja virustorjuntaohjelmalla.

Toisaalta tällä hetkellä ei ole kohtuullista olettaa, että käyttäjän selain on määriteltä käyttämään vain TLS-protokollan mukaisia turvallisia suojauspaketteja, mutta palvelu voi kuitenkin tätä edellyttää.

Arvioinnissa voidaan olettaa, että todentamisjärjestelmän ulkopuolisten komponenttien asetukset ovat kohtuulliset.

(EN)(1. Definitions, authentication factor) If multi-factor authentication is used, the different factors should be chosen in a way to counter different threats/attack vectors.

Evaluating the strength of authentication needs to take into account not only the factor(s) itself, but also the mechanism to verify the factor(s).

(2.2.1) Using multiple authentication factors from different categories in a complementary manner can increase the overall security of the identification means. A common example is combining a possession-based token with a password or PIN to unlock the token. Even if the token is lost or stolen, it still cannot be used for authentication without the PIN.

(2.2.1) Protection against duplication and tampering refers to the whole electronic identification means and not to each individual authentication factor. The use of different authentication factors is meant to reduce risk, since different authentication factor categories are susceptible to different threats. Passwords might be observed when used by persons or systems (keyloggers) or if written down, possession based authentication factors might be stolen or lost, systems based on inherent authentication factors might be vulnerable to construed evidence (lookalikes/alterations of real biometrics, synthetic evidence, latex fingerprints etc).

Factor-specific examples of protection against tampering and duplication, include:

☐ *Possession-based authentication factors: embed cryptographic key material in tamper-resistant hardware that prevents the key from being extracted outside the device either or manipulated in the device through physical or electronic means, hardware security module*

☐ *Inherent authentication factors: liveness detection, trusted environment, low false match rate*

According to good practice, an electronic identification means should have been proven to be resistant to tampering and duplication. This

may include through testing; for example by being certified against relevant technical standards (e.g. Common Criteria). ...

(2.2.1) 'reliably protected' refers to the efforts taken to prevent the electronic identification means from being used without the subject's knowledge and active consent. As an example, a private key in a cryptographic key token should not be usable by a machine process without the user's active consent (e.g. by using a PIN).

This is a requirement to protect against: duplication, guessing, replay and manipulation of communication threats.

Other techniques that might be used, in addition to those mentioned previously:

- ☐ Strength of static passwords
- ☐ Biometric verification of the user
- ☐ Checks of the environment against malicious code
- ☐ Out of band verification
- ☐ For all secrecy based authentication factors (static passwords, one time password in hardware), guessing is a threat which should be mitigated in order to reach a very high level of resilience – e.g. by limiting the number of attempts/slowdown mechanisms and by ensuring sufficient entropy

(2.3.1) The authentication mechanisms used in the authentication phase cannot prevent all attacks completely, they can only offer resistance to attacks on a certain level of security/assurance. A standard way to quantify the resistance of different mechanisms is to rank them according their resistance against attacks with a certain attack potential (i.e. strength of an attacker).

The Level of Assurance use the terms "enhanced-basic", "moderate" and "high" to denote the different attack potentials. This terminology is borrowed from ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" and ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". The text of the standards is also freely available at www.commoncriteriaportal.org/cc (CCPART1-3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045).

ISO/IEC 15408-1 defines "attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation".

Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.

In order to meet the requirements set out in the implementing act, some assessment of resistance against potential attacks should be carried out.

The assessment should take relevant threats into accounts. For example, ISO 29115 mentions: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading.

During assessing attack resistance, the whole authentication mechanism should be taken into account including the risks resulting from verification of the possession of the electronic identification means.

For example

- *For LoA high, it is not sufficient that a smart card protects a cryptographic key against manipulation with high attack potential, also the cryptographic protocol should protect the verification of the possession of the key against manipulation/replay against high attack potential.*
- *For a one-time-password token, where the generated one-time-password is transmitted via a secure channel (e.g. TLS), the strength of the possession-based-factor is limited not only by the strength of the token, but also by the strength of the secure channel.*
- *The mechanism for proof-of-possession of a time-based one-time-password generator is the submission of a generated one-time-password to the verifier. The strength of this mechanism is limited, among others, by the length of the one-time-password, the time-window for validity of the password, and the confidentiality of the transmission.*

Reasonable assumptions on the level of security of components used by, but not part of, the authentication scheme (e.g. the environment of the user, browser, smart phone, etc.) should be taken into account during the risk assessment.

Components can be operated in different configurations with different security settings.

As an example, the assessment might assume that the user operates a personal firewall and virus protection on his/her computer.

As a counterexample, currently it would not be reasonable to assume that the browser of the user is configured to use only secure cipher suites for Transport Layer Security (TLS); however this can be enforced by the service.

The assessment might presume reasonable settings for the components not part of the authentication scheme.

EBA-Op-2019-06

38. Another requirement under the RTS, in line with PSD2, is that the two elements used for SCA be independent. Independence under Article 9 of the RTS requires that the use of the elements 'is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements'.

3.3.12 Tietoliikenneturvallisuus tunnistuspalvelun yhteyksillä käyttäjään ja asiointipalveluun.

eIDAS-säätelyssä ja määräyksessä 72 edellytetään tietoliikenneyhteyksien turvallisuutta (osapuolten välisiä rajapintoja käsitellään tarkemmin toisessa muistiossa). Määräyksen 7 §:ssä määritellään TLS:n vähimmäistaso, liikenteen salausvaatimus

ja hyväksytyt salausalgoritmit. Salausta edellytetään luottamuksellisuuden turvaamiseksi myös sanomatasolla.

eIDAS-varmuustasoasetus Liite, 2.3.1 Todentamismekanismit, ks. edellä.

eIDAS-varmuustasoasetus Liite, 2.4.6 Tekniset tarkastukset

2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.

LOA Guidance 2016

(FI)

(2.4.6) On syytä huomata, että viestintäkanavia voi syntyä samaan tunnistamisjärjestelmään osallistuvien osapuolten välille, esimerkiksi tunnistamismenetelmän omistajan ja palvelun tai kunnan ja valmistajan välille.

Yhtenä tapana toteuttaa viestintäkanavien teknistä valvontaa ovat viranomaisen antamat tekniset ohjeet, joissa määritellään käytettäviä salauksia ja turvatoimenpiteitä koskevat vaatimukset. Tässä käytetään yleensä salausprotokollaa, jonka varmennuksen vaiheet on kuvattu erikseen.

eIDAS-yhteentoimivuusjärjestelmän solmupisteiden välisiä viestinnän kanavia koskevat vaatimukset on ilmoitettu järjestelmää koskevassa teknisessä erittelyssä.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.10 "Cryptography", A.13 "Communications security" ja A.18.1.5 "Regulation of cryptographic controls" mukaisia turvatoimenpiteitä. Kohdissa saatetaan myös viitata edellä mainittuihin teknisiin ohjeisiin.

(EN)

(2.4.6) It has to be considered that communication channels may arise between different parties involved within an identification scheme, e.g. between the owner of the identification means and a service or between municipality and manufacturer.

One possibility for technical controls for communication channels are technical guidelines issued by an authority that gives requirements on cryptography and security measures to be used. This will typically be achieved using cryptographic protocols with described verification steps.

Requirements for communication channels between nodes of the eIDAS Interoperability Framework are given in the eIDAS Technical Specification for the framework.

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.10

'Cryptography', A.13 'Communications security' and A.18.1.5 'Regulation of cryptographic controls', which may also include references to technical guidelines as stated above.

RTS SCA & CSC 35 artikla Viestintäistuntojen turvallisuus

1. Tiliä ylläpitävien maksupalveluntarjoajien, korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien, tilitietopalveluntarjoajien ja maksutoimeksiantopalvelun tarjoajien on varmistettava, että vaihdettaessa tietoja internetissä viestinnän osapuolten välillä sovelletaan turvallista salausta koko viestintäistunnon ajan käyttämällä vahvoja ja yleisesti tunnustettuja salaustekniikoita, jotta turvataan tietojen luottamuksellisuus ja eheys.

2. Korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien, tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on pidettävä tiliä ylläpitävien maksupalveluntarjoajien tarjoamat pääsyistunnot mahdollisimman lyhyinä, ja niiden on aktiivisesti lopetettava nämä istunnot heti, kun pyydetty toimi on saatu päätökseen.

3. Ylläpitäessään rinnakkaisia verkkoistuntoja tiliä ylläpitävän maksupalveluntarjoajan kanssa tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on varmistettava, että nämä istunnot liitetään turvallisesti maksupalvelunkäyttäjän (maksupalvelunkäyttäjien) kanssa käynnistettyihin istuntoihin, jotta estetään niiden välillä vaihdettujen viestien tai tietojen ohjaaminen väärille tahoille.

4. Tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien tarjoajien on kommunikoidessaan tiliä ylläpitävän maksupalveluntarjoajan kanssa viitattava yksiselitteisesti kaikkiin seuraaviin seikkoihin:

- a) maksupalvelunkäyttäjä tai maksupalvelunkäyttäjät ja vastaava viestintäistunto, jotta samalta maksupalvelunkäyttäjältä tai samoilta maksupalvelunkäyttäjiltä tulevat pyynnöt voidaan erottaa toisistaan;
- b) kun on kyse maksutoimeksiantopalveluista, käynnistetty maksutapahtuma, joka on varmennettu yksilöllisesti;
- c) kun on kyse varojen saatavuuden vahvistamisesta, yksilöllisesti varmennettu pyyntö, joka koskee korttipohjaisen maksutapahtuman toteuttamiseen tarvittavaa määrää.

[...]

EBA-Op-2018-04, joitakin viittauksia tietoliikenneturvallisuuteen. Ne voivat liittyä erityisesti maksutoimeksiantopalveluille tai tilitietopalveluille tarjottuun dedikoituun rajapintaan, joka voi kuitenkin olla eri rajapinta kuin yleisen tunnistamisen tai muille maksupalvelutoimijoille tarjottu rajapinta.

EBA-Op-2018-04

Table 1. Main requirements for dedicated interfaces and API initiatives

Enabling a secure data exchange between the ASPSP and the PISP, AISP and CBPII, mitigating the risk of any misdirection of communication to other parties

Articles 28 and 35 RTS

*Ensuring security at transport and application levels Article 97(3)
PSD2 Articles 30(2)(c) and 35 RTS*

EBA Q&A 2018-4054 koskee tietoliikenteen salausta.

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4054

Are EMV (Europay, MasterCard, Visa) transactions (for which the application cryptogram is not enciphered during its transmission) compliant with the RTS on strong customer authentication?

In accordance with Article 22(1) of the Commission Delegated Regulation (EU) 2018/389 payment service providers are required to "ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication".

In that regard, in the case where the issuer uses a cryptogram, which contains personalised security credentials, including authentication codes, the issuer would need to protect the confidentiality and integrity of the respective personalised security credentials in accordance with Article 22 of the Delegated Regulation, including during the transmission of the cryptogram. This also applies when the cryptogram is used as an authentication code.

The issuer is responsible for ensuring compliance with the requirements of Article 22 of the Delegated Regulation.

3.3.13 Tietoliikenteen osapuolten varmentaminen

PSD2-sääntelyssä tietyiltä tunnistusta hyödyntäviltä kolmansilta toimijoilta edellytetään eIDAS-asetuksen mukaisen qualified varmenteen käyttämistä (sähköisen leiman eli "järjestelmällekirjoituksen" varmenteen tai verkkosivun todentamisen varmenteen).

eIDAS-sääntelyssä ei ole vastaavia täsmällisiä vaatimuksia. Määräyksen 72 8 §:ssä määrätään yleisellä tasolla osapuolten tunnistamisesta luottamusverkoston sisällä.

Asiaa käsitellään 8 §:n muutosta valmistelevassa muistiossa.

3.3.1 Dynaaminen linkitys

Sääntelyjen suhteessa kysymyksiä on liittynyt ainakin siihen, miten maksunvahvistuksen vaatimukset vaikuttavat mahdollisuuteen käyttää samaa tunnistusmenetelmää pohjana yleisessä tunnistamisessa ja maksupalveluissa. Maksun vahvistaminen edellyttää tunnistamista ja maksutietojen dynaamista linkittämistä tunnistustapahtumaan (tunnistamiskoodiin).

EBA-Op-2019-06

40. The EBA also notes (as published in Q&A 4141) that an element used for the purpose of SCA may be reused within the same session for the purpose of applying SCA at the time that a payment is initiated, provided that the other element required for SCA is carried out at the time of the payment initiation and that the dynamic linking element is present and linked to that latter element.

EBA:n Q&A 2018-4141, käsitellään mm. tunnistamisen ja maksunvahvistuksen suhdetta

https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4141

Arvio: kysymyksen 2018-4141 perusteella vaikuttaa siltä, että suhteessa yleiseen tunnistamiseen on mahdollista tehdä tunnistus samalla menetelmällä kuin missä tahansa palvelussa ja tunnistautuneena vahvistaa maksu RTS SCA & CSC:n edellyttämällä tavalla istunnon myöhemmässä vaiheessa.

3.3.2 Muut PSD2-asiat

Ks. EBA-Op-2018-04, jossa huomioidaan, että tunnistuksen voi tuottaa myös muu kuin tilinpitäjäpankki.

Kohta 38. The articles mentioned above are to be read in conjunction with one another, which means that the PSP applying SCA is the PSP that issues the personalised security credentials. It is consequently also the same provider that decides whether or not to apply an exemption in the context of AIS and PIS. The ASPSP may, however, choose to contract with other providers such as wallet providers or PISPs and AISPs for them to conduct SCA on the ASPSP's behalf and determine the liability between them. The EBA also notes that a number of governmental (national) agreements on universal sets of personalised security credentials that can be used by PSUs with multiple PSPs already exist in some Member States.

3.4 Yleistä blockchain ja self sovereign identity

Seuraava teksti on esittelyteksti Liikenne- ja viestintäviraston toimialakyselyssä 2020.

Komission SSI eIDAS Legal Report

Sähköisen tunnistuspalvelun vallitsevaa perusmallia voi luonnehtia esimerkiksi seuraavasti: tunnistuspalveluntarjoaja kerää luotettavista lähteistä tunnistusvälineen hakijan henkilötiedot ja kytkee ne teknisesti tunnistusvälineen todentamistekijöihin. Asiointitapahtumassa henkilö autentikoidaan luottavalle osapuolelle todentamistekijöiden perusteella.

Blockchain voidaan nähdä teknisenä toteutustapana, jota tunnistuspalvelut voisivat käyttää tietojen käsittelyssä ja varmentamisessa. SSI puolestaan voitaisiin nähdä modernina tunnistusvälineenä, jolla käyttäjä pystyisi nykyisin tarjolla olevia menetelmiä paremmin itse hallinnoimaan henkilötietojensa (*attestation*) käytön luvitusta eri asiointitilanteissa ilman, että tunnistuspalvelun tarjoajan on tarpeen välittää tietoja osapuolten välillä. Merkittävästi pidemmälle menevässä kehityksessä lohko-
ketjuteknologian ja PKI-arkkitehtuurin perusluonteisen muutoksen voi ilmeisesti nähdä muuttavan tunnistuspalvelun roolin nykyisessä muodossaan tarpeettomaksi.

EU:n komissio on hiljan julkaissut selvityksen lohkoketjuteknologian ja itsehallittavan identiteetin suhteesta eIDAS-asetukseen: *SSI eIDAS Legal Report, How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*

https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

Selvityksessä kuvataan teknistä perustaa ja oikeudellista eIDAS-perustaa. Siinä arvioidaan erilaisia lyhyen ja pitkän tähtäimen kehitysvaihtoehtoja ja niiden suhdetta eIDAS-asetukseen. Raportin lähitulevaisuuden näkökulma on arvioida lohkoketjun ja SSI:n toteutuksia voimassa olevan eIDAS-säätelyn valossa.

3.5 Toimialakysely 2020 muutostarpeista

Seuraavaan on koottu viraston elokuussa 2020 tekemästä muutostarvekyselystä aiheeseen liittyviä kysymyksiä ja vastauksia. Vastauksia on tässä koosteessa osittain niputettu ja anonymisoitu.

3.5.1 Kysymys tietoturvauhkista

24) Uhkat, fraud. Onko tunnistamisessa jotain käyttäjä- tai asiointipalveluun liittyviä tietoturvauhkia tai fraud-ilmiöitä, joita määräysvalmistelun yhteydessä olisi hyvä käsitellä?

- Hyökkääjä voi perustaa klooni-sivuston tunnistusvälineen tarjoajasta ja toimia ns. man-in-the-middle. Tavallisella kansalaisella ei ole keinoja havainnoida kyseistä tilannetta, ellei esimerkiksi muistua ulkoa "pankin" verkkotunnusta jota on mahdollisesti aikaisemmin käyttänyt vahvasti tunnistautumiseen.

3.5.2 Kysymys todentamistekijöistä

13) Todentamistekijät. Onko tunnistusmenetelmän ominaispiirteiden suunnittelussa ja todentamistekijöiden turvallisuudessa osa-alueita, joita olisi arvioitava määräysvalmistelussa?

- Tunnistusmenetelmien ominaispiirteitä ja todentamistekijöiden turvallisuutta arvioitaessa tulisi huomioida myös tunnistusmenetelmien saavutettavuus ja elinkaari.

- Voidaanko turvattomaksi todettuja mobiililaitteita käytännössä rajata tunnistusmenetelmän ulkopuolelle ja miten se tehdään? Todentamistekijöiden teknisten vaatimuksien tiukentuessa kasvaa monesti myös käyttäjältä edellytetty osaamisen taso. Lähtökohtaisesti tunnistusmenetelmien pitäisi kuitenkin olla kaikkien ulottuvilla. Mikäli tunnistusmenetelmän käyttö edellyttää paljon tukea, kasvaa riski tunnistusmenetelmän luovuttamisesta kolmannen osapuolen haltuun.

3.5.3 Kysymykset PSD2

31) PSD2 ja eIDAS. Onko tunnuslukulistojen tarkastelu määräysvalmistelun yhteydessä tarpeen? Onko niiden käyttöä tarkoitus jatkaa vielä?

- vaatimuksien olisi kansallisella tasolla hyvä olla yhdenmukaiset

- tunnuslukulistoja käyttävät pankit ovat korvaamassa tunnuslukulistat, emme pidä tunnuslukulistojen tarkastelua määräysvalmistelun yhteydessä tarpeellisena

- Tämän hetken PSD2-eIDAS -tulkinta on pankin näkökulmasta toimiva. Pankille on välttämätöntä, että samaa tunnistusvälinettä voi käyttää sekä maksupalveluissa ja yleisessä tunnistamisessa.

- Toisaalta maksupalveluun liittyvien erityisvaatimusten ei pidä heijastua tunnistamiseen vahvan sähköisen tunnistamisen luottamusverkostossa. Jos esimerkiksi nyt edellytettäisiin, että myös tunnistustapahtumiin pitää liittyä SMS OTP -lisävahvistus...vahvistustekijän lisääminen ei ole kustannustehokasta nykyisellä säännellyllä hinnoittelulla

32) PSD2 ja eIDAS. Onko SMS OTP:n tarkastelu määräysvalmistelun yhteydessä tarpeen?

- SMS OTP liittyy tunnuslukulistojen käyttöön. Koska tunnuslukulistoista ollaan luopumassa lähivuosina, emme pidä SMS OTP:n tarkastelua tarpeellisenä määräysvalmistelun yhteydessä.

- Ei huomioita, mutta vaatimuksien olisi kansallisella tasolla hyvä olla yhdenmukaiset.

33) PSD2 ja eIDAS. Onko PSD2-sääntelyn vaatimuksissa mobiilisovellusten turvallisuudelle nähdäksenne eroja suhteessa tunnistuslain ja eIDAS-asetuksen vaatimuksiin? Estävätkö mahdolliset erot saman sovelluksen käyttämisen maksupalveluissa ja yleisessä tunnistamisessa?

- Vaatimuksissa ei merkittäviä eroja, emmekä näe siis esteenä.

- Emme ole tehneet analyysia PSD2:n ja eIDAS-sääntelyn välillä näiltä osin. Olisi hyvä, mikäli vaatimukset kansallisella tasolla olisivat yhtenevät.

34) PSD2 ja eIDAS. Oletettavasti kansainväliset laitesertifioinnit eivät ole riippuvaisia siitä, minkä alan palvelussa niitä käytetään. Onko tunnuslukulaitteiden sääntelyssä eroja, joita olisi tarkasteltava määräysvalmistelun yhteydessä?

- Ei huomioita.

35) PSD2 ja eIDAS. Onko biometrisen todentamistekijän sääntelyssä eroja, joita olisi tarkasteltava määräysvalmistelussa?

- Emme ole tehneet analyysia PSD2:n ja eIDAS-sääntelyn välillä. Mikäli biometrisen todentamistekijän osalta tunnistetaan eroja, olisi tärkeää tunnistaa erot ja noudattaa näiden osalta tiukempaa tulkintaa. Biometristen todentamistekijöiden toteutuksen poikkeama yhdessä palvelussa voi pahimmillaan johtaa myös muiden toteutuksien turvallisuuden pettämiseen.

- ...kiittää viranomaista hyvästä PSD2 ja eIDAS sääntelyjen koosteesta tunnistamistekijöiden suhteen.

- Yleisesti ottaen todetaan PSD2- ja eIDAS-sääntelyjen sovittamisen olevan haastavaa tehtävän vaatiessa vahvaa tunnistamisen käytänteiden ja lainsäädännön osaamista.

36) PSD2 ja eIDAS. Onko PSD2-sääntelyssä tietoliikenteen salauksesta yleisiä vaatimuksia, joita ei ole teknisesti mahdollista toteuttaa, jos täyttää määräyksen 72 7 §:n vaatimukset TLS:stä (vähintään TLS 1.1) ja salausalgoritmeista?

- PSD2:ssa kolmas osapuoli tunnistetaan sertifikaatin perusteella. M72 ei ota tähän kantaa, mutta ei sulje mahdollisuutta poiskaan.

- Ei huomioita.

37) PSD2 ja eIDAS. Onko tietoliikenteen osapuolten varmentamisessa (tunnistusvälineen tarjoaja, välityspalvelu, asiointipalvelu) ristiriitaisia vaatimuksia tai eroja, joita olisi tarkasteltava?

- Ei ole. Sopimukset solmitaan kahden osapuolen kesken ja rajapintojen turvallisuus perustuu avainten vaihtoon käyttäen turvallisia prosesseja.

- Ei huomioita.

38) PSD2 ja eIDAS. Sääntelyjen yhteensopivuutta on selvitetty jo vuoden 2018 yhteensopivuustarkastelun yhteydessä. Onko sääntelyssä teknisiä tekniseen luotettavuuteen tai yhteentoimivuuteen liittyviä vaatimuksia tai eroja, joita olisi tarkasteltava mahdollisten yhteensopivuusongelmien takia uudestaan määräysvalmistelun yhteydessä?

- Eroja löytyy, mutta niillä ei vaikutusta tunnistamisen rajapintoihin.

- Ei huomioita.

39) PSD2 ja eIDAS. Estääkö jokin PSD2- ja eIDAS-sääntelyn liittyvä tekninen vaatimus saman tunnistusmenetelmän tarjonnan ja käytön yleisessä tunnistamisessa ja maksupalvelutunnistamisessa?

- PSD 2 ja sitä kautta maksupalvelulaki edellyttävät dynamic linking -menetelmän käyttämistä maksutapahtumien yhteydessä. Nähdäksemme sääntelyiden eroavuus on tarkoituksenmukaista, eikä näiden vaatimusten tulekaan olla yhdenmukaisia muilta kuin ehkä vahvan tunnistamisen käsitteen osalta.

- Ei huomioita.

Ensitunnistamisesta (kyselyssä ei nimenomaisia kysymyksiä ensitunnistamisesta, koska se ei ole TunnL 42 § nojalla viraston määräystoimivallassa)

- Yleiskommenttina todetaan, että Finanssialalla on oltu huolissaan PSD2 ja eIDAS sääntelyn epäsuhdasta tunnistustekijöissä. Erityisesti covid-19 pandemian vaikutukset liiketoiminnalle ovat olleet merkittäviä siten, että asiakkaiden tunnistaminen ja erityisesti ensitunnistaminen sähköisesti ilman fyysistä tapaamista on entistä tärkeämmässä roolissa. ...on käytetty FTN-verkostossa tapahtuvan ensitunnistamisen rinnalla muita tunnistustekijöitä vahventavia menettelyjä. ...esimerkiksi finanssialan yleisesti käyttämiä rekisterejä tehdäkseen ristiin tarkistuksia paitsi asiakkaalta itseltään saataviin, mutta myös FTN-verkostossa tehtävän ensitunnistamisen yhteydessä saataviin tietoihin.

- Markkinassa olisi hyvä olla yhtenäinen linja ensitunnistamisen vahvuuden tasolle. Positiivisena ilmiönä markkinassa on voitu seurata joidenkin toimijoiden reagoivan tunnistamisen vahvuuteen jälkikäteisesti vahventamalla tunnistustekijöitä esimerkiksi KYC-tietojen ajoittaisen keräämisen yhteydessä. Vaikuttaa siltä, että jotkin markkinaosapuolet käyttävät riskiperustaista ja jälkikäteistä KYC-prosessia ensitunnistamisen tason vahvistamisessa.

- EU-jäsenmaissa on otettu käyttöön etätunnistusratkaisuja ja DVV:llä on käytössä oma etätunnistusratkaisu ulkomaalaisille suunnatussa FinnAuth-palvelussa. Etätunnistusratkaisuille tulisi olla selkeämmät tekniset vaatimuksia eri LoA-tasaille.

3.5.4 Kysymykset blockhainista ja SSI:stä

40) Blockchain ja SSI. Miten yleisesti ottaen näette lohkoketjuteknologian ja itse hallittavan identiteetin suhteen vahvan sähköisen tunnistuspalvelun tarjontaan?

Findy

- Vahva sähköinen tunnistuspalvelu ja itse hallittava identiteettidata (SSI) ovat toisiaan täydentäviä tulevaisuuden digitaalisen asiainnin peruspilareita. Vahvan tunnistautumisen kautta henkilö saa identiteettidataansa digitaalisen todisteen siitä kuka hän on (juuri-identiteetti). Tämän todisteen esittämällä henkilö voi saada palveluista omaan identiteettidataansa lisätodisteita ja näitä voi yhdessä esittämällä käyttää edelleen muihin palveluihin. Tunnistautuminen on kriittinen osa SSI-pohjaista identiteettidatan hallintaa ja se voi olla kertaluontoinen tapahtuma identiteettidatan linkittämiseksi henkilöön. Vaativan luotettavuustason tapahtumissa tunnistautuminen voi tapahtua myös identiteettidatan todisteiden esityshetkellä.

Tunnistustapahtumat identiteettidatan hyödyntäjien kohdalla riippuvat käyttötapauksesta eli luottamus ei ole enää joko vahvaa tai heikkoa, vaan se voi olla palvelu- tai tapauskohtaisesti myös jotain siltä väliltä. SSI-teknologioita voidaan siis soveltaa yhdessä vahvan tunnistautumisen kanssa luomaan monipuolisempia ja monitasoisempia tunnistamismekanismeja eri tasoihin käyttötarkoituksiin. Monitasoinen tunnistaminen sekä tunnistustapahtumassa välitettävien henkilötietojen vaatimukset pitää arvioida, jotta voidaan tukea tulevia kehityssuuntia joustavammin.

- Tunnistustapahtumat identiteettidatan hyödyntäjien kohdalla riippuvat käyttötapauksesta eli luottamus ei ole enää joko vahvaa tai heikkoa, vaan se voi olla palvelu- tai tapauskohtaisesti jotain siltä väliltä. Identiteettidata tuo myös mahdollisuuden yhdistää eri palveluista dataa ja luoda näiden pohjalta vahvempia todisteita mihin pelkällä tunnistautumisella päästään. Tällä tullaan pääsemään siihen, että tunnistamisen tasoa voidaan tarpeen mukaan säädellä ilman, että asiakkaalla on useita tunnistusvälineitä.

Muut

- ...yhtyy viranomaisen näkemykseen, että lohkoketjuteknologia ja eurooppalaisen tulkinnan kehitys ei ole vielä riittävän pitkällä, jotta lohkoketjuteknologiaa voitaisiin harkita tosielämän käyttötapauksissa. Lisää tutkimusta ja tuotekehitystä tarvitaan, jotta myös itsehallittavasta identiteetistä (SSI-Self-Sovereign Identity) voisi tulla vartenotettava vaihtoehto markkinoille lähivuosina

- ...arvostaa alalla tehtävää kehitystä ja tutkimusta etenkin itsehallittavan identiteetin kannalta erityisesti yksityisyyden suojan näkökulmasta. Perinteisenä finanssialan toimijana asiakkaan yksityisyys ja etenkin alalle tärkeä pankkisalaisuus on toiminnan ytimessä ja tästä näkökulmasta itsehallittava identiteetti parantaa asiakkaan mahdollisuutta kontrolloida tunnistuspalvelusta asiointipalveluille luovutettavaa henkilötietoa.

- Uudenlaiset tunnistamisen menetelmät ja tunnistamisen eriyttäminen substanssipalveluista omaksi toiminnokseen voi parantaa substanssipalvelujen digitaalisen kehittymisen edellytyksiä ja auttaa uudenlaisten palvelukonseptien muodostumisessa. Tällaisesta kehityksestä konkreettisena esimerkkinä on täysin digitaalinen asuntokauppa...

- Suomessa tunnistusratkaisut ovat vakiintuneet nykyisen mallin ympärille. Tällä hetkellä DVV ei näe tarvetta siirtyä tunnistusratkaisuihin lohkoketjuteknologian hyödyntämiseen.

41) Blockchain. Ovatko nykyiset tunnistussääntelyn tekniset vaatimukset ristiriidassa lohkoketjuteknologian hyödyntämisen kanssa? Estääkö mahdollinen ristiriita nähdäksenne teknologian käytön vai onko kysymys siitä, että soveltamiskäytäntö lohkoketjuteknologiaan on epäselvä?

Findy

- Lohkoketjuteknologia mahdollistaa myös ei-identiteettidataan liittyviä hajautettuja liiketoimintaprosesseja. Nämä transaktiot voivat toteuttaa olemassa olevia sopimuksia, sekä luoda uusia digitaalisia sopimuksia, jolloin vastapuolten luotettava tunnistaminen on tärkeää. Sopimuksen osapuolten tunnistaminen edellyttää, että kaikki sopimuksen osapuolet hyödyntävät yhteistä digitaalista menetelmää. Tässä tilanteessa kyseeseen tulee joko pelkkä tunnistuspalvelu tai vaihtoehtoisesti tunnistuspalvelun ja itse hallinnoidun identiteettidatan yhdistävä malli.

Esimerkiksi DIAS.fi (asuntokaupan lohkoketjuverkosto) käyttää transaktioiden allekirjoitukseen perinteistä tunnistuspalvelua ja sähköistä allekirjoitusta. Tämä vastaa nykyisin vallalla olevaa palvelumallia. Identiteettidatan hallinnan yhdistämisellä kyetään tehostamaan ja nopeuttamaan uusia sähköisiä palvelumalleja.

Tunnistuspalvelun yhdistäminen identiteettidataan mahdollistaa lisäksi sen, että lohkoketjupohjaisiin transaktioihin voidaan liittyä ilman transaktio-osapuolten välisiä etukäteissopimuksia tai tarkistuksia. Tässä tilanteessa transaktiossa vaaditut todisteet voidaan esittää itsehallitun identiteettilompakon sisältämällä vahvistetuilla tiedoilla. Tämä mahdollistaa usean osapuolen välisten liiketoimintaverkostojen toteuttamisen dynaamisesti. Verkon toimijoiden välinen yhteentoimivuus ja sopimusten allekirjoitukset tapahtuvat käyttämällä tunnistuksen lisäksi itsehallittua, vahvistettavaa identiteettidataa. Käytännössä lohkoketjua hyödyntävien liiketoimintaverkostojen toteuttaminen on mahdollista myös nykyisen tunnistamissääntelyn puitteissa, mutta käyttökokemus ja ratkaisujen soveltaminen uudessa hajautetussa liiketoimintaympäristössä toteutuu tehokkaammin (hajautetuin periaattein) soveltamalla SSI-mallia.

Muut

- Emme ole arvioineet nykyistä sääntelyä lohkoketjuteknologiaa vasten, koska emme hyödynnä lohkoketjuja.

42) SSI. Ovatko tunnistussääntelyn nykyiset tekniset vaatimukset ristiriidassa SSI-toteutusten kanssa? Estääkö mahdollinen ristiriita nähdäksenne SSI-toteutukset vai onko kysymys siitä, että soveltamiskäytäntö on epäselvä?

Findy

- Tällä hetkellä täysimittaisen SSI-mallin toteuttaminen on ristiriidassa tunnistussääntelyn kanssa ja soveltamiskäytäntö on epäselvää. Teknisestä näkökulmasta esimerkiksi tekninen protokollamäärittely ei tällä hetkellä mahdollista SSI-pohjaisten Verifiable Credentials -tunnistautumisten tekemistä (<https://www.w3.org/TR/vc-data-model/>).

- Tällä hetkellä SSI-ratkaisut ymmärretään sähköisten tunnistuspalveluiden tyyli-
senä ratkaisuna, jossa palvelua tarjoava taho voi varmistua asiakkaan henkilölli-

syystä. Tämä on kuitenkin vain yksi SSI-mallin käyttötapauksista. Uuden tunnistautumismallin lisäksi SSI:n keskeinen etu on mahdollisuus laajaan vahvistettavan tiedon jakamiseen, jolla saavutetaan suurempi luottamus transaktion osapuolten välille. Suppea käsitys SSI:n hyödyntämismahdollisuuksista aiheuttaa tulkinnallisia ristiriitoja ja epäselvyyttä. Esimerkiksi vahvistettavan tiedon (verifiable credentials) käytettävyys juridisesti validina dokumenttina - saati tunnistusvälineenä - on ollut tähän asti epäselvää.

- SSI-ratkaisujen kehittyminen on osaltaan riippuvainen EU:n (eIDAS) ja Suomen viranomaisen kannanotoista ja siitä kuinka määräyksiä sovelletaan SSI-ratkaisujen käyttöönotossa. SSI-standardien (mm. DID, VC) käyttö henkilötiedon ja tunnistamisen hallinnassa tarvitsee lisää juridista selkeyttä. Tällä hetkellä SSI-ratkaisujen kehittäminen nähdään liian suurena investointiriskinä, koska juridiset seikat eivät ole täysin selkeitä, mikä hidastaa yleistä markkinan kehitystä. Tästä johtuen on tärkeää, että EU:n ja Suomen vastuuviranomaisilta tulisi selkeä kannanotto ja ohjeistus määräysten soveltamiseen SSI-ratkaisuja käytettäessä. Nykyinen eIDAS-sääntely on kirjoitettu federoidun identiteettimallin käsitteitä käyttäen, josta syystä kaikki sääntelyssä esitetyt roolit ja velvoitteet eivät ole yksiselitteisesti tulkittavissa ja sovellettavissa SSI-mallissa. eIDAS-sääntelyä tulisi voida tulkita ja soveltaa erityyppisten verkostojen ja identiteettidatan hallintamalleihin kuten uusiin hajautettuihin malleihin.

- Edellä mainitusta syystä viranomaisten tulisi tehdä Suomessa selvitys ja ohjeistus SSI:n soveltamisesta nykymääräysten puitteissa. Euroopan Komission "SSI eIDAS Legal Report" tarjoaa hyvän perustan selvitykselle ja ohjeistukselle. Keskeisintä kannanotossa olisi selkiyttää, kuinka SSI:n käyttö tulkitaan vallitsevien määräysten mukaisesti. Erityisesti komission raportin kappale 9.2 "Issuance of qualified certificates based on a specific DID method and verifiable credential" antaa esimerkin DID ja VC standardien soveltamisesta eIDAS sähköisen leiman luomisessa ja kuvaa, kuinka eIDASin määrittämiä rooleja ja elementtejä voidaan tulkita tässä esimerkissä. Kyseinen kappale sisältää taulukon, joka yhdistää sähköisen leiman määräyksen sisältövaatimuksen vaaditun sisällön SSI-mallin elementtiin.

Muut

- Tietääksemme ei estä, mutta emme ole tehneet tähän liittyvää kattavaa selvitystä.

43) Muut tekniset kehitysilmiöt. Onko muita vastaavia kehityssuuntia, joita tunnistuspalvelujen teknisessä sääntelyssä olisi huomioitava?

Findy

- SSI-mallin adoption kasvaessa, tulevia SSI-lompakoita tulisi saada Suomessa yhtenäisen käyttökokemuksen piiriin. Tämä tarkoittaa samanlaisen tunnistautumisen käyttökokemuksen määrittämistä kaikilla SSI-lompakoilla, huolimatta niiden käyttökontekstista. Käyttökonteksteja on mm. www-sivut, kasvokkain tiskiasioinnissa, digitaaliset päätelaitteet, jne. Asioinnissa tulisi myös yhteisesti arvioida ja päättää käytettävät standardit (esim. onko ISO/IEC standard 18013-5 järkevä ottaa kansallisesti sääntelyn piiriin).

- Uusien tunnistustapojen käyttöönoton helpottaminen tulisi ottaa huomioon. Esimerkiksi käyttäytymiseen ja biometriseen tunnistamiseen liittyvät teknologiat edistyvät nopeasti ja niiden liittäminen hajautettujen identiteettitietojen esittämiseen ei välttämättä täytä nykysääntelyn kriteerejä, vaikka ovat yhtä turvallisia käyttää. Uudet tunnistustavat tulevat myös vaatimaan yksityisen ja viranomaisten välisen

yhteistyön kehittämistä ja vastuualueiden uudelleen määrittämistä. Esimerkiksi henkilön tulisi pystyä valtuuttamaan yksityinen tunnistuspalveluntarjoaja käyttämään Poliisin rekisterissä sijaitsevaa passikuva biometristä tunnistamista varten.

- Yksi kehityssuunta joka erityisesti korostuu hajautettujen verkkojen sovellutuksissa on tunnistamisen ketjutus siten, että tunnistustapahtuma tehdään ennen varsinaista transaktiota, jossa tunnistaminen vahvistetaan. Samaa tunnistamista näin sovelletaan useaan kertaan, mahdollisesti useissa käyttökonteksteissa. Esimerkki tällaisesta käyttötapauksesta olisi maksaminen ilman debit-korttia pelkällä biometrisellä tunnistautumisella, kuten esimerkiksi kasvojen tunnistuksella. Esimerkissä asiakas tunnistautuu ennen kaupakäyntiä vahvan tunnistamisen välineellä ja luo pankin sovellukseen virtuaalisen maksuvälineen. Tämä maksuväline on käytettävissä biometrisellä tunnistusvälineellä kaupan kassalla. Tällainen maksumekanismi on jo käytössä keskitetysti mm. Kiinassa. Hajautetulla verkkomallilla voidaan luoda tällainen maksujärjestelmä yksityisesti ja tietoturvalisest.

- Minimaalisen interaktion mahdollistaminen

- Edellä annetussa esimerkissä, sekä kaikissa hajautettujen liiketoimintaverkkojen transaktioissa, tarvitaan kyvykkyys ketjuttaa tunnistautuminen siten, että asiakkaalta vaaditaan vain minimaalinen määrä toimia tunnistuksen tekemiseen. Tämä mahdollistaisi mm. aikaisemmin mainittujen biometrisesti vahvistettavien virtuaalisten maksuvälineiden toteuttamisen (ilman maksukortin näyttöä) sekä transaktioiden niputuksen. Käytännössä henkilöt voivat näissä tapauksissa tunnistautua ja vahvistaa transaktioita käyttäen omia tai kassan maksupäätteitä samalla tavoin kuin esimerkiksi Google Pay tai Apple Pay järjestelmät tänä päivänä.

- Tunnistuspäalveluiden rajapintojen avaaminen

- Määräysten tulisi myös mahdollistaa tunnistuspäalveluiden parempi rajapintojen käyttö, velvoittamalla identiteettidatapäalveluntarjoajien rajapintojen avaaminen. Rajapintojen avaamista ja kehittämistä tarvitaan monipuolisempien tunnistustapahtumien ja tunnistuksen ketjuttamisen mahdollistamisessa. Esimerkiksi, jos henkilö on tunnistatunut vahvan tunnistamisen välineellä, tulee tunnistamisen yhteydessä pystyä määrittämään kuinka tunnistusta voidaan käyttää tai pyytää esimerkiksi vahvistusta tunnistamisesta. Vaatimus voi tapahtua tunnistustapahtuman yhteydessä, tunnistustietoja esittäessä tai niitä vahvistaessa, tai jossain näiden kombinaatiossa. Identiteetti ja sen vahvistaminen tapahtuu tulevaisuudessa monimutkaisissa ketjutetuissa transaktioissa, mikä tarvitsee monipuolisemman tunnistautumismekanismien.

- Siirtyessämme uusiin hajautettuihin teknologioihin on tärkeää, että tuetaan sekä vallitsevia että tulevia teknologisia standardeja. Niiden kautta voidaan rakentaa digitaalisen identiteetin yhteensopivuus juuri-identiteetistä liiketoimintaprosesseihin asti. Tässä tapauksessa keskeisessä roolissa on nähdäksemme Findy-konsortio, jonka tavoitteena on perustaa vuoden 2020 aikana voittoa tavoittelematon osuuskunta hallinnoimaan ja operoimaan vahvistetun datan SSI-verkkoa. Osuuskunta tulee määrittämään yhteisiä käytäntöjä, vaatimuksia ja sääntökirjan. Tämä tulisi tehdä yhteistyössä osuuskunnan ja viranomaisten kesken.

4 2021 muutosvaihtoehdot ja vaikutusarviointi

4.1 Säännöksen alustava muutosehdotus

6. Tunnistusmenetelmän tietoturva-vaatimukset

6.1 Todentamistekijöiden turvallisuus ja riippumattomuus

Hallussapitoon, tietoon ja ominaisuuteen perustuvien todentamistekijöiden eri turvaominaisuuksien ja tunnistusmenetelmän turvallisuustoimenpiteiden yhdistelmän on suojattava tunnistusmenetelmää oikeudettomalta käytöltä. Todentamistekijöiden riskit on arvioitava erikseen ja tunnistusmenetelmän suojautumiskyvyn on perustuttava varmuustason mukaiseen uhka- ja riskiarvioon.

Tunnistusmenetelmän toteutuksen on estettävä se, että yhden todentamistekijän vaarantuminen ei vaaranna muiden todentamistekijöiden luotettavuutta. Tunnistusmenetelmän turvatointenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, kun niitä käytetään samalla päätelaitteella.

Siirtymäsäännös (?): riskiarvio menetelmästä laadittava  mennessä, uusilla toimijoilla aloitusilmoituksen yhteydessä.

6.2 Todentamismekanismin turvallisuus

Käyttäjän tunnistusvälineen ja tunnistusvälineen tarjoajan järjestelmän välisen tietoliikenneturvallisuuden tulee täyttää soveltuvien osien määräyksen 7 kohdan salausvaatimukset.

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistua siitä, että hän vahvistaa oikean tunnistuspyynnön (session binding). Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luotavasta osapuolesta, jolle tunnistus välitetään. Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista. (RP-name)

6.3 Tunnistusvälineen henkilöön kytkeminen

Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.

Tunnistusvälinettä ei saa yhdistää hakijaan ennen hakijan ensitunnistamista tai tunnistusvälineen myöntämisprosessissa on muutoin varmistettava, että tunnistusväline ei ole käytettävissä ennen kuin tunnistus- ja luottamuspalvelulain 17 §:n mukainen ensitunnistaminen on tehty.

6.4 Tunnistusmenetelmän käyttäjäkohtaisten tietojen käsittely

Tunnistuspalvelun ~~Palveluntarjoajan~~ on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.

Tunnistuspalvelun tarjoaja ~~Palveluntarjoaja~~ ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja.

4.2 Todentamistekijöiden turvallisuuden sääntelytapa

Arvioitava kysymys

Miten määritellään turvalliset/turvattomat todentamistekijät ja tunnistusmenetelmän kokonaisuus?

- a) Määräyksen tarkennetut todentamistekijäkohtaiset vaatimukset?
- b) Suojautumiskyvyn/lopputuloksen määrittely?
- c) Riskiarvion vaatimukset?

4.2.1 Alustava sääntelyehdotus

6.1 Todentamistekijöiden turvallisuus ja riippumattomuus

Hallussapitoon, tietoon ja ominaisuuteen perustuvien todentamistekijöiden eri turvaominaisuuksien ja tunnistusmenetelmän turvallisuustoimenpiteiden yhdistelmän on suojattava tunnistusmenetelmää oikeudettomalta käytöltä. Todentamistekijöiden riskit on arvioitava erikseen ja tunnistusmenetelmän suojautumiskyvyn on perustuttava varmuustason mukaiseen uhka- ja riskiarvioon.

Siirtymäsäännös(?): riskiarvio menetelmästä X mennessä, uusilla toimijoilla aloitusilmoituksen yhteydessä

4.2.2 Riskiarviomalli

Lähteet

LOA guidance

Todentamisvaiheessa käytetyillä todentamismekanismeilla ei voi estää täysin kaikkia hyökkäyksiä, vaan niillä voidaan vain vastustaa hyökkäyksiä tietyllä turvallisuus- tai varmuustasolla. Tavanomainen tapa mitata eri mekanismien tuottamaa sietokykyä on asettaa mekanismit järjestykseen sen mukaan, miten hyvin ne kestävät tietyn vakavuusasteen hyökkäyksiä (eli hyökkääjän voimaa).

Varmuustasossa eri vakavuusasteista käytettävät termit ovat "korkeampi perustaso" (enhanced-basic), "kohtuullinen" (moderate) ja "korkea" (high). Nämä termit on lainattu standardeista ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standardien teksti on vapaasti luettavissa osoitteessa www.commoncriteriaportal.org/cc (CCPART1-3 vastaa standardia ISO/IEC 15408 ja CEM standardia ISO/IEC 18045).

Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismia] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.

Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.

Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.

Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.

Hyökkäysten sietokyvyn arvioinnissa on syytä ottaa huomioon koko todentamismekanismi, myös sähköisen tunnistamisen menetelmän hallussapidon varmentamisesta aiheutuvat riskit.

Esimerkkejä:

- ☐ *Korkeassa varmuustasossa ei riitä, että älykortti suojaa salausavainta korkean vakavuustason väärentämisyrityksiltä, vaan myös salausprotokollan on suojattava avaimen hallussapidon varmentamista korkean vakavuustason väärentämis- tai toistoyrityksiltä.*
- ☐ *Kun kyse on kertakäyttöisestä salasanatunnisteesta, jossa muodostettu kertakäyttösalasana toimitetaan suojatussa kanavassa (esimerkiksi TLS), hallussapitoon perustuvan tekijän vahvuuteen vaikuttavat tunnisteen vahvuus ja suojatun kanavan vahvuus.*
- ☐ *Aikaperusteiselle kertakäyttösalasanojen muodostajalle hallussapidon todistamismekanismi on muodostetun kertakäyttösalasanan lähettäminen varmentajalle. Tämän mekanismin vahvuutta rajoittaa muun muassa kertakäyttösalasanan pituus, salasanan voimassaoloaika sekä toimitustavan luottamuksellisuus.*

Riskinarvioinnissa on otettava huomioon kohtuulliset olettamukset sellaisten komponenttien turvallisuustasosta, joita todentamisjärjestelmä hyödyntää, mutta jotka eivät ole sen osia (esimerkiksi käyttäjän ympäristö, selain ja älypuhelin).

Komponentteja voidaan käyttää eri kokoonpanoissa ja eri suojausasetuksilla.

Arvioinnissa voidaan esimerkiksi olettaa, että käyttäjän tietokone on suojattu palomuurilla ja virustorjuntaohjelmalla.

Toisaalta tällä hetkellä ei ole kohtuullista olettaa, että käyttäjän selain on määritelty käyttämään vain TLS-protokollan mukaisia turvallisia suojauspaketteja, mutta palvelu voi kuitenkin tätä edellyttää.

Arvioinnissa voidaan olettaa, että todentamisjärjestelmän ulkopuolisten komponenttien asetukset ovat kohtuulliset.

Alustava arviomalli

- ISO 29115 kategoriat, LOA Guidance
- [Huom. Ilman track changes ja no markup taulukon värien takia]

Uhka	Salasana/fraasi	Tunnuslukulista	Tunnuslukulaite	SMS OTP	Tunnussovel-lus (sormi)	Tunnussovel-lus (kasvot)	Tunnussovel-lus (PIN)
Online guessing							
Offline guessing							
Credential duplication							
Phishing							

Eavesdrop- ping							
Replay at- tack							
Session hi- jacking							
Man-in- the-middle							
Credential theft							
Spoofing							
Mas- querading							

4.2.3 Muut ohjauskeinot

- Ohje
- Suositus
- Yhteissääntely
- Informaatiolla ohjaaminen

4.3 Todentamistekijöiden uhkat ja turvaominaisuudet

Arvioitava kysymys:

Mitä uhkia ja turvaominaisuuksia on huomioitava erityyppisten todentamistekijöiden valinnassa, mm.

- Tunnuslukulista
- Tunnuslukulistan ja SMS OTP:n yhdistelmä
- Tunnuslukulaitteiden turvallisuus - käytössä oleva algoritmi
- Turvattomaksi todetut mobiililaitteet (laitteistotason haavoittuvuuksien takia) ja käyttöjärjestelmät
- Käyttöjärjestelmät/käytetyt ohjelmistoalustat
- Riittävät salasana/PIN-koodikäytännöt?
- Tietoon perustuvan tekijän (PIN) riippumattomuus tunnistussovelluksissa, ilman erillistä tietoon perustuvaa tekijää (salasana)
- Ominaisuutta mittaavat tekniset ratkaisut (anturit)
- Kasvotunnistuksen turvallisuus vs. sormenjäljen turvallisuus
- Jatkuvaan ominaisuuden mittaukseen perustuvien toteutusten soveltuvuus (kävely, kirjoitustyyli jne.)

4.3.1 Alustava sääntelyehdotus

6.1 Todentamistekijöiden turvallisuus ja riippumattomuus

Hallussapitoon, tietoon ja ominaisuuteen perustuvien todentamistekijöiden eri turvaominaisuuksien ja tunnistusmenetelmän turvallisuustoimenpiteiden yhdistelmän on suojattava tunnistusmenetelmää oikeudettomalta käytöltä. Todentamistekijöiden riskit on arvioitava erikseen ja tunnistusmenetelmän suojautumiskyvyn on perustuttava varmuustason mukaiseen uhka- ja riskiarvioon.

...

LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu

Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.

LOA guidance: Tunnistusmenetelmän suunnittelussa on otettu huomioon se, että eri todentamistekijöihin kohdistuu erityyppisiä uhkia.

4.3.2 Hallussapitoon perustuva todentamistekijä

Lähteet:

LOA guidance

Hallussapitoon perustuvan todentamistekijän (esimerkiksi tunnistevälineen) olennaisena turvaominaisuutena on se, että se on yksinomaan omistajansa hallinnassa. Tämä edellyttää, että todentamistekijän jäljentäminen on kolmannelle osapuolelle niin vaikeaa ja epätodennäköistä, että tällainen vaara on merkityksetön. Varmuustasoon vaikuttaa jäljentämisyritysten sietokyky. Esimerkkejä: epäsymmetriset (yksityiset) salausavaimet, erityiseen laitteeseen (esimerkiksi älykortille) tallennetut yksityiset avaimet, ohjelmistotunnisteet, yksilöivät tunnisteet (esimerkiksi matkapuhelimen SIM-kortti) tai kertakäyttöistä salasanaa (esimerkiksi RSA-tunnistetta tai perikortilla olevaa salasanaa) käyttävät laitteet.

Tyypillisiä hallussapitoon perustuviin todentamistekijöihin kohdistuvia hyökkäyksiä ovat varkaus, toisintaminen tai väärentäminen (muuttaminen) sekä hallussapitoa koskeviin todisteisiin kohdistuvat hyökkäykset todentamishetkellä.

LOA Johdantokappale (11) Kansainvälisiin standardeihin perustuva tietotekninen tietoturvasertifiointi on tärkeä väline tarkastettaessa, vastaavatko tuotteet turvallisuudeltaan tämän täytöntöönpanosäädöksen vaatimuksia

Vrt. PSD2 RTS SCA&CSC 7 artikla Ryhmään "hallussapito" kuuluvia tekijöitä koskevat vaatimukset

1. Maksupalveluntarjoajien on toteutettava toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot käyttävät ryhmään "hallussapito" kuuluvia asiakkaan vahvan tunnistamisen tekijöitä.
2. Maksajan käyttäessä näitä tekijöitä niiden käyttöön sovelletaan toimenpiteitä, joiden tavoitteena on estää kyseisten tekijöiden kopioituminen.

LOA guidance: Tämä edellyttää, että todentamistekijän jäljentäminen on kolmannelle osapuolelle niin vaikeaa ja epätodennäköistä, että tällainen vaara on merkityksetön

Tunnuslukulista

- Uhkat: kopioitavuus, kalastelu, varastaminen, kohdepalvelun maskeeraus, ...
- Turvakeinot/ominaisuudet: käyttäjän ohjeistus,

SMS OTP

- Uhkat: Päätelaitteessa olevat haittaohjelmat, SIM-kortin vaihto, SMS-yhdyskäytävien puutteellinen suojaus, puhelinlukitusten ohitus (SMS -viesti näkyy lukitun puhelimen ruudulla), kalastelu/huijaussivut, kohdepalvelun maskeeraus, ...
- Turvakeinot/ominaisuudet: Tunnistuspalvelun ulottumattomissa; SMS-yhdyskäytävän turvaaminen, SIM-korttien/eSIM:n vaihtoprosessi. Käyttäjän ohjeistus, ftn_spname esittäminen välittäjän selainkäyttöliittymässä

Tunnuslukulaitteet

- Uhka: sivukanavahyökkäys (side channel attack), varastaminen, kalastelu/huijaussivut
- Turvakeinot/ominaisuudet: sertifiointi/sertifioitujen sirujen/teknologisten ratkaisujen käyttö, jotka ovat vastustuskykyisiä sivukanavahyökkäykselle, käyttäjän ohjeistus, ftn_spname esittäminen välittäjän selainkäyttöliittymässä, ...

Tunnistussovellukset

- Uhka: Päätelaitteessa olevat haittaohjelmat, varastaminen+tietoon perustuvan tekijän selvitys (esim. olan yli) tai huono biometrinen sensori, istunnon kaappaus, kohdepalvelun "maskeeraus", ...
- Turvakeinot/ominaisuudet: S211, liite C, istunnon sitominen/yhdistäminen, ftn_spname välitys sovellukselle asti, käyttäjän ohjeistus

4.3.3 Tietoon perustuva todentamistekijä

Lähteitä

LOA guidance

Tiedossaoloon perustuva todentamistekijä on sellainen, joka on todennäköisesti vain tekijän haltijan sekä varmentavan tahon tiedossa. Esimerkkejä ovat PIN-koodit, salasanat, muistettavat sanat tai päivämäärät, tunnuslauseet, aiemmin rekisteröidyt tiedot ja muut vastaavat tiedot, jotka ovat todennäköisesti vain henkilön omassa tiedossa. Joissakin tapauksissa edes varmentava taho ei tiedä varsinaista tiedossaoloon perustuvaa todentamistekijää, mutta se kykenee varmistamaan, että sen ja hakijan tiedossa on tarkalleen sama tieto; esimerkkinä on salasanan tiivisteen käyttäminen.

Jos tietoa käytetään todentamistekijänä, on syytä yrittää tehdä kyseisen tiedon arvaamisesta (joko satunnaisesti tai ns. raajan voiman/laskentatehon avulla) vastapuolelle mahdollisimman vaikeaa. Esimerkki: kun tieto on salasana, hyvä toimintatapa edellyttää sopivaa salasanaikäytäntöä (ks. esimerkiksi BSI IT-Grundschutz -opas S.2.11 "Provisions concerning the use of passwords" sekä NIST 800-63-2, liite A, kohdat "Single Token Authentication" ja "Password Entropy").

Tyypillisiä tiedossaoloon perustuviin todentamistekijöihin kohdistuvia hyökkäyksiä ovat arvaaminen, tietojen kalastelu (phishing), salakuuntelu tai toisintaminen. Tiedossaoloon perustuvilla todentamistekijöille ominaista on, että sähköisen tunnistamisen menetelmää käyttävä henkilö ei välttämättä edes huomaa hyökkäyksiä. Esimerkkejä: raakaan voimaan tai sanakirjan käyttöön

perustuvat hyökkäykset, joiden kohteena ovat salasanat, joiden entropia on heikko ja joita kysyttäessä ei lasketa uudelleenyritysten määrää; kirjeestä tai sähköpostiviestistä haltijan tai varmentajan huomaamatta kopioidut salasanat.

Vrt. RTS SCA&CSC 6 artikla

Ryhmään "tieto" kuuluvia tekijöitä koskevat vaatimukset

- 1. Maksupalveluntarjoajien on toteutettava toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot ottavat tai saavat ryhmään "tieto" kuuluvat asiakkaan vahvan tunnistamisen tekijät selville.*
- 2. Maksajan käyttäessä näitä tekijöitä niiden käyttöön sovelletaan riskinhallintatoimenpiteitä, joiden tavoitteena on estää kyseisten tekijöiden paljastuminen oikeudettomille tahoille.*

Salasana/salasanalausekkeet

- Uhka: Arvaaminen, selvitys, varastaminen, kalastelu/huijaussivut
- Turvakeinot/ominaisuudet: Käyttäjien ohjeistus, vaatimukset monimuotoiselle salaisuudelle

PIN-koodi(t)

- Uhka: Arvaaminen, selvitys, varastaminen, kalastelu/huijaussivut
- Turvakeinot/ominaisuudet: Käyttäjien ohjeistus, pituusvaatimus, sovelluksen/alustan tarjoamien turvakeinojen käyttö syöttövaiheessa

Oletettuun tietoon perustuvat tekijät (kysymys-vastausparit)

- Uhka: Arvaaminen, selvitys, varastaminen, kalastelu/huijaussivut
- Turvakeinot/ominaisuudet: Käyttäjien ohjeistus, useampi kysymys-vastauspari, kysymysten ei pidä pohjautua muista rekistereistä/paikoista saatavaan tietoon

4.3.4 Biometriset todentamistekijät

Lähteet

LOA guidance

Luontaisissa todentamistekijöissä on syytä olla vaihtelua myös ominaisuuksiltaan samanlaisten ihmisten välillä, jotta henkilön yksilöinti on mahdollista; esimerkkejä ovat sormenjälki, kämmenjälki, kämmenen verisuonisto, kasvot, käden geometria ja silmän iiris.

Biometrisiä tekijöitä käytettäessä on tärkeää varmistaa, että henkilö, johon todentamistekijä liittyy, on varmentamispaikassa fyysisesti läsnä. Näin vähennetään huijausten tai toisintamisen vaaraa.

Tunnistuspalvelun arviointikriteeristö O211

- Tunnistussovelluksen ja biometrisen todentamistekijän käytön riskiarvio:
- mitkä seikat otettava huomioon hyväksytyissä sovelluksissa/laitteissa
-

Vrt. EBA-Op-2019-06

17. Article 4(30) of PSD2 defines inherence as 'something the user is'. Article 8 of the RTS on SCA and CSC refers to the 'authentication elements categorised as inherence and read by access devices and soft-ware' and recital 6 refers to the need to have 'adequate security features'

in place that could, for example, be 'algorithm specifications, biometric sensor and template protection features'.

18. As stated in the Opinion on the implementation of the RTS, inherence may include behavioural biometrics identifying the specific authorised user. The EBA is of the view that inherence, which includes biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. In addition, it is (the quality of) the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence element. Inherence is the category of elements that is the most innovative and fastest moving, with new approaches continuously entering the market.

20. The swiping path memorised by the PSU and performed on a de-vice would not constitute an inherence element, but may rather constitute a knowledge element, something only the user knows.

Vrt. RTS SCA&CSC 8 artikla Ryhmään "erityinen ominaisuus" kuuluiin tekijöihin liittyviä laitteita ja ohjelmistoja koskevat vaatimukset

1. Maksupalveluntarjoajien on toteutettava toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot ottavat selville ryhmään "erityinen ominaisuus" kuuluvia tekijöitä, joita maksajalle toimitetut pääsyn mahdollistavat laitteet ja ohjelmistot lukevat. Maksupalveluntarjoajien on varmistettava ainakin, että oikeudettoman tahon tunnistaminen maksajaksi on hyvin epätodennäköistä pääsyn mahdollistavien laitteiden ja ohjelmistojen käytön yhteydessä.

2. Kun maksaja käyttää näitä tekijöitä, niiden käyttöön sovelletaan toimenpiteitä, joilla varmistetaan, että laitteet ja ohjelmistot tarjoavat suojan niiden oikeudettomasta käytöstä johtuvalta kyseisten tekijöiden oikeudettomalta käytöltä.

Sormenjälki

- Uhka: Teknisestä toteutuksesta johtuva alhainen FAR (False Acceptance Rate), kopiointi (pinnoilta, valokuvista), haittaohjelmat, onko käyttäjä tiedoton
- Turvakeinot/ominaisuudet: O211/2019

Kasvot

- Uhka: Teknisestä toteutuksesta johtuva alhainen FAR (False Acceptance Rate), presentatiohyökkäykset
- Turvakeinot/ominaisuudet: O211/2019

Jatkuvaan mittaukseen perustuvat

- Uhka: Teknisestä toteutuksesta johtuva alhainen FAR (False Acceptance Rate), haittaohjelmat
- Turvakeinot/ominaisuudet: Soveltuvien osien O211/2019

4.3.5 Tunnistuspalveluiden kehitys

- Tunnuslukulistojen käyttö vähenemässä, mutta ei kokonaan poistumassa
- PSD2-eIDAS ero tunnuslukulistoissa, vain maksupalveluissa käytetään lisävahvistusta
- Tunnuslukulaitteiden lisääntyvä käyttö
- Tunnistussovelluksen lisääntyvä käyttö hallussapitoon perustuvana tekijänä
- Muuta

4.3.6 Taloudelliset vaikutukset

- Tunnuslukulistoista luopumisen/niiden korvaamisen kustannukset - muutenkin muutos käynnissä
- SMS-lisävahvistuksen kustannukset
- Sertifioitujen ja sertifioimattomien tunnuslukulaitteiden hintaerot?
- siirtymäaika

4.4 Riippumattomuus ja turvallisuus

Arvioitava kysymys:

Miten tunnistusmenetelmän ominaispiirteitä vrt. todentamistekijöiden riippumattomuusvaatimusta voidaan tarkentaa?

4.4.1 Alustava sääntelyehdotus

6.1 Todentamistekijöiden turvallisuus ja riippumattomuus

.....

Tunnistusmenetelmän toteutuksen on estettävä se, että yhden todentamistekijän vaarantuminen ei vaaranna muiden todentamistekijöiden luotettavuutta. Tunnistusmenetelmän turvatoimenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, kun niitä käytetään samalla päätelaitteella.

...

LOA Guidance 2016

(1. todentamistekijän määritelmä) Useaan tekijään perustuvaa todentamista käytettäessä eri tekijät on valittava niin, että niillä torjutaan eri uhkia/hyökkäystapoja.

Todentamisen tehokkuutta arvioitaessa on syytä ottaa huomioon paitsi itse tekijä tai tekijät, myös tekijöiden varmentamisessa käytettävä menettely.

(2.2.1) Useiden eri luokkiin kuuluvien todentamistekijöiden käyttämisellä toinen toisiaan täydentävästi voidaan parantaa tunnistamismenetelmän yleistä turvallisuustasoa. Yleinen esi-merkki on hallussapitoon perustuvan tunnisteiden yhdistäminen salasanaan tai PIN-koodiin, joilla tunniste avataan. Vaikka tunniste katoaa tai varastetaan, sitä ei voi käyttää todentamiseen ilman PIN-koodia....

(2.2.1) Suojaamisella toisintamiselta ja väärentämiseltä tarkoitetaan koko sähköisen tunnistamisen menetelmää, ei pelkästään yksittäisiä todentamistekijöitä. Eri todentamistekijöiden käytöllä on tarkoitus vähentää riskiä, sillä eri luokkiin kuuluvat todentamistekijät ovat alttiita erilaisille uhkille.

Vrt. O211 B 5.1

2 Todentamistekijät ovat toisistaan riippumattomia

LOA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu

Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.

4.4.2 Turvallisuusvaikutukset

Riippumattomuus

- Uhka: Tunnistusvälineen/välineiden jouduttua väärin käsiin saadaan kaikki tekijät haltuun, järjestelmätasolla tapahtunut muutos/haittaohjelma heikentää tekijöiden suojausk-
- Turvakeinot/ominaisuudet:

Todentamismekanismiin liittyvän teknisen toteutuksen turvallisuus

- Uhka: Tunnistussovellusten osalta S211/2019, tunnuslukulaitteen kohdalla huonosti toteutettu/huono suojaus ulkoista kuuntelua vastaan, SMS OTP:ssä huonosti suojattu SMS-yhdyskäytävä (usein tunnistuspalvelun tarjoajan ulottumattomissa),...
- Turvakeinot/ominaisuudet: S211/2019, tunnuslukulaitteissa käytettyjen laitteistoratkaisujen arvointi/sertifiointi, yhdyskäytäväratkaisujen kovennukset, ...

Tunnistusmenetelmän turvallisuus

- Uhka:
- Turvakeinot/ominaisuudet:

4.5 Todentamismekanismien turvallisuus

Arvioitava kysymys:

- Miten voidaan mahdollistaa käyttäjälle väärän tunnistuspyynnön havaitseminen
- Miten voidaan mahdollistaa käyttäjälle helpottaa käyttäjien kohdalla väärään palveluun tunnistautumisen estämistä/havainnointia

4.5.1 Alustava sääntelyehdotus

6.2 Todentamismekanismien turvallisuus

Käyttäjän tunnistusvälineen ja tunnistusvälineen tarjoajan järjestelmän välisen tietoliikenneturvallisuuden tulee täyttää soveltuvin osin määräyksen 7 kohdan salausvaatimukset.

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistua siitä, että hän vahvistaa oikean tunnistuspyynnön (session binding). Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista.

Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luotavasta osapuolesta, jolle tunnistus välitetään. Tieto on näytettävä tunnistusmenetelmässä, jossa se on teknisesti mahdollista. (RP-name)

4.5.2 Perustelut, lähteet

- todentamismekanismissa noudatetaan salausvaatimuksia tunnistusvälineen tarjoajan ja käyttäjän välillä
- sanomat/viestit tunnistusvälineen käyttäjän ja IdP:n välillä

- vrt. määräykseen 7 kohta ja TLS-tason vaatimus ja 9 kohdan sanomatason salausvaatimukset selaintoteutukselle
- lisäksi istunnon kesto? Vrt. rajapintasuositus 212 ja 213
- tunnistuspyynnön yksilöinti
- Tavoite: sitoa/yhdistää selain/sovellustunto tunnistustapahtumaan, session binding
- tunnistusvälineen käyttöliittymässä
- C-kriteeristössä vaatimuksena mobiilisovellukselle
- Mahdollinen vain tunnistusvälineessä, jolla on oma näyttö
- kohdepalvelun tieto
- SP/RP -tieto tunnistustapahtumassa
- tunnistuspalvelun (välityspalvelun ja/tai välineen tarjoajan) käyttäjälle tarjoamassa selain-käyttöliittymässä ja mahdollisesti tunnistussovelluksessa (mobiilisovellus tunnistusvälineenä ainoa, jossa on tämä kyvykkyys)
- selaimen käyttöliittymässä näytetään yleensä
- Erilaisia toteutustapoja: Kirjainmerkkijono (mobiilivarmenne, myös allekirjoitettava tieto), luettava teksti, QR-koodi (ei tarvitse käyttäjän tekemää vertailua), kuva tai kuvia, kuva ja teksti (selaimessa auton kuva, tekstinä tunnistusvälineessä "Auto")

4.6 Blockhain ja SSI

Arvioitava kysymys:
Onko SSI-malleja tai lohkoketjutoteutuksia huomioitava määräyksen vaatimuksia laadittaessa.

4.6.1 Linjaus

- julkisen ja yksityisen sektorin yhteistyön politiikkaratkaisut eivät kuulu valvontaviranomaisen toimivaltaan tai tehtäviin
- Määrästyön yhteydessä varataan tilaisuus käsitellä lohkoketjuteknologian ja SSI -lompakototeutusten suhdetta tunnistuksen teknisiin vaatimuksiin ja arviointivaatimuksiin
- virasto ei ole tässä vaiheessa tekemässä omaa teknistä yksityiskohtaista arviota, mutta seuraa tarkasti eIDAS-asetuksen uudelleenarviointia ja EU-tason hankkeita

4.6.2 Muut ohjauskeinot

- Ohje
- Suositus
- Yhteissäätely
- Informaatiolla ohjaaminen

5 Säädäntö

5.1 Määräyksen antamisen perusta

42 § (23.11.2018/1009) Yleinen ohjaus sekä Liikenne- ja viestintäviraston määräykset

Vahvan sähköisen tunnistamisen ja sähköisten luottamuspalveluiden yleinen ohjaus ja kehittäminen kuuluvat liikenne- ja viestintäministeriölle.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä:

1) tunnistusjärjestelmän 8 §:n 1 momentin 4 ja 5 kohdan mukaisista turvallisuutta ja luotettavuutta koskevista vaatimuksista;

...

TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

...

4) **tunnistusjärjestelmä on turvallinen ja luotettava** siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa **2.2.1, 2.3.1** ja 2.4.6 vähintään korotetulle varmuustasolle säädetty edellytykset täyttyvät **ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat** sekä tunnistuspalvelun tarjoamiseen käytettävät tilat ovat turvallisia sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.4.5 säädetyllä tavalla;

LOA 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu

Korotettu

1. Sähköisen tunnistamisen menetelmässä käytetään vähintään kahta todentamistekijää eri luokista.

2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.

Korkea Taso "korotettu" lisättynä seuraavalla:

1. Sähköisen tunnistamisen menetelmä on suojattu toisintamiselta ja väärentämiseltä sekä hyökkäyksiltä, joiden vakavuusaste on korkea ("high").

2. Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.

LOA 2.3.1 Todentamismekanismi

Seuraavassa taulukossa esitetään vaatimukset varmuustasoittain todentamismekanismista, jolla luonnollinen tai oikeushenkilö käyttää sähköisen tunnistamisen menetelmää vahvistaakseen henkilöllisyytensä luotettavalle osapuolelle.

Matala

1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen.

2. Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.

3. Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkeampaa perustasoa ("enhanced-basic"), voi heikentää todentamismekanismia.

Korotettu

Taso "matala" lisättynä seuraavalla:

1. Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista.

2. Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen ("moderate"), voi heikentää todentamismekanismeja.

Korkea

Taso "korotettu" lisättynä seuraavalla: Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea ("high"), voi heikentää todentamismekanismeja.

5.2 Asiaan liittyvät säännökset

5.3 Muu sääntely