**Sähköisen tunnistuspalvelun arviointiohje**

Liikenne- ja viestintäviraston ohje

211/2023 O Liite B

**LUONNOS 26.5.2023**

Contents

[1. Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi 3](#_Toc135992563)

[2. Yhteentoimivuus 16](#_Toc135992564)

[3. Tekniset tietoturvavaatimukset 20](#_Toc135992565)

[3.1 Tietoliikenneturvallisuus 23](#_Toc135992566)

[3.2 Tietojärjestelmäturvallisuus 28](#_Toc135992567)

[3.3 Käyttöturvallisuus 33](#_Toc135992568)

[4. Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset 38](#_Toc135992569)

[5. Tietojen säilyttäminen ja käsittely 44](#_Toc135992570)

[6. Tilaturvallisuus 51](#_Toc135992571)

[7. Riittävät ja pätevät henkilöresurssit 53](#_Toc135992572)

[8. Tietoturvallisuuden hallinta 54](#_Toc135992573)

[9. Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen) 58](#_Toc135992574)

[10. Tunnistusvälineen eli tunnistusmenetelmän elinkaari 69](#_Toc135992575)

LIITE B: Tunnistuspalvelun yleinen arviointikriteeristö

# Tunnistamisen menetelmän ominaispiirteet ja todentamismekanismi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **M72B 15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot**  Tunnistuspalvelun tunnistus- ja luottamuspalvelulain 29 §:n mukaisen arvioinnin täytyy kattaa kaikki laissa ja tässä määräyksessä asetetut vaatimukset, jotka kohdistuvat:  […]  2) tunnistusmenetelmään eli tunnistusvälineen:  […]  c) tunnistusmenetelmän ominaispiirteisiin ja laatimiseen;  […]  g) todentamismekanismeihin.  M72B 6 Tunnistusmenetelmän tietoturvavaatimukset  6.1 Tunnistusjärjestelmän ominaispiirteet ja suojautumiskyky  6.1.1  Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat tunnistusmenetelmän eheyden ja luottamuksellisuuden. Tunnistusmenetelmällä on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.  Suojautumiskyvyn on perustuttava riskiarvioon, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet.  6.1.2  Tunnistusmenetelmän ominaispiirteiden ja turvatoimenpiteiden on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaisi muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, jos niitä käytetään samalla päätelaitteella.  6.1.3  Tunnistusmenetelmässä ja todentamisessa on käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja. Tunnistusvälineen ja tunnistusjärjestelmän välisellä tietoliikenneyhteydellä on käytettävä teknisesti soveltuvin osin määräyksen 7 kohdan mukaisia salausratkaisuja, ellei suojautumiskyky kokonaisuutena arvioiden toteudu muilla turvatoimenpiteillä.  6.2 Erityiset turvatoimenpiteet  6.2.1  Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistaa, että tunnistusvälineeseen käyttäjän saama tunnistuspyyntö liittyy käyttäjän omaan asiointitapahtumaan. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.  6.2.2  Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luottavasta osapuolesta, jolle tunnistus välitetään. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.  6.2.3  Kertakirjautumisella tarkoitetaan tässä määräyksessä sitä, että tunnistuspalvelu tarjoaa useammalle kuin yhdelle luottavalle osapuolelle vahvistuksen yhden vahvalla sähköisellä tunnistusmenetelmällä tehdyn tunnistusvälineen haltijan todentamisen perusteella.  Tunnistuspalvelun on kertakirjautumisen suunnittelussa, toteutuksessa ja ylläpidossa huolehdittava kertakirjautumiseen liittyvien istuntojen keston, siirtämisen ja lopettamisen hallintaan perustuvista turvatoimenpiteistä sekä  6.3 Tunnistusvälineen kytkeminen henkilöön  6.3.1  Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.  6.3.2  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 haltijakohtaisten tietojen käsittely  6.4.1  Tunnistuspalvelun tarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.  6.4.2  Tunnistuspalvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja. | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  |  | Tunnistusmenetelmästä on olemassa riskiarvio (hyökkäyspotentiaalin laskeminen). | **TunnL 8 §** **Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**  8.1 § 3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;  **LoA Liite 2.3.1 Todentamismekanismi**  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.  M72B 6.1.1  Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat tunnistusmenetelmän eheyden ja luottamuksellisuuden. Tunnistusmenetelmällä on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.  Suojautumiskyvyn on perustuttava **riskiarvioon**, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet. | ISO 29115  ISO/IEC 15408-1  ISO/IEC 18045, liite B  Common Criteria CCDB 2009 03, kappale 3  ETSI TS 102 165-1, kappale 6.6 ja 6.7 | Esim. Common Criteria CCDB 2009 03, kappale 3, tai ETSI TS 102 165-1, kappale 6.6 ja 6.7 miten laskea hyökkäyspotentiaali. Riskiarvion asianmukainen toteuttaminen on peruslähtökohta hyökkäyspotentaalin laskemiselle. |
| 1. 1 | S, H | Tunnistusmenetelmässä käytetään vähintään kahta todentamistekijää eri luokista | TunnL 8 a § Tunnistusmenetelmässä käytettävät todentamistekijät  […]  1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;  2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;  3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.  […]  LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu  Sähköisen tunnistamisen menetelmässä käytetään vähintään kahta todentamistekijää eri luokista. |  |  |
| 1. 2 | S,H | 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.  M72B 6.1.2  Tunnistusmenetelmän ominaispiirteiden ja turvatoimenpiteiden on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaisi muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, jos niitä käytetään samalla päätelaitteella. |  | Todentamistekijöiden riippumattomuuteen toisistaan on syytä kiinnittää erityistä huomiota mobiililaitteella käytettävissä tunnistusmenetelmissä. |
|  | S,H | Tunnistusmenetelmän suunnittelussa on otettu huomioon se, että eri todentamistekijöihin kohdistuu erityyppisiä uhkia | 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.  M72B 6.1.2  Tunnistusmenetelmän ominaispiirteiden ja turvatoimenpiteiden on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaisi muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, jos niitä käytetään samalla päätelaitteella. |  |  |
|  | S,H | Tunnistusmenetelmään liittyvät salaiset tiedot eivät tule tunnistuspalveluntarjoajan henkilökunnan tai alihankkijoiden tietoon | M72B 6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely  6.4.1  Tunnistuspalvelun tarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.  6.4.2  Tunnistuspalvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja. |  | Salaisia tietoja ovat tyypillisesti esimerkiksi PIN-koodit tai muut tietoon perustuvat todentamistekijät.  Vaatimuksen tarkoitus on huomioida tunnistuspalvelun vilpillisen henkilökunnan riski. |
|  | S,H | Todentamistekijät on vahvistettu henkilöön liittyväksi | LoA Liite, 1. Sovellettavat määritelmät  2) ’todentamistekijällä’ tarkoitetaan tekijää, joka on vahvistettu henkilöön kytkeytyväksi ja joka kuuluu johonkin seuraavista luokista […]  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.  M72B 6.3 Tunnistusvälineen kytkeminen henkilöön  6.3.1  Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.  6.3.2  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. |  | Esimerkiksi tunnistussovelluksen kytkeminen henkilöön, sirun personointi, tunnuslukulistan tai laitteen kytkeminen henkilöön. |
|  | S,H | Todentamismekanismi on suunniteltu siten, että jokaisella tunnistustapahtumalla on yksilöllinen sähköinen todiste | TunnL 8 a §  […] Jokaisessa tunnistusmenetelmässä on käytettävä sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3.1 tarkoitettua sellaista dynaamista todentamista, joka muuttuu jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamistapahtumassa.  **LoA Liite 1. Sovellettavat 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;  LoA Liite 2.3.1 Todentamismekanismi  Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista. |  | myös tunnistusvälityspalvelu  LoA guidance (otteita)  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.  …  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.  …  Jos henkilön yksityinen avain on tallennettu etäpalveluna (keskitetysti esimerkiksi tunnistustietojen tarjoajan käyttämälle HSM-laitteelle), yksityisen avaimen käyttämiseen vaadittavan todentamistavan on myös oltava dynaaminen. |
|  | S,H | Tunnistustapahtuman sähköinen todiste perustuu henkilöön liitettyihin todentamistekijöihin | **LoA Liite 1. Sovellettavat 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;    **M72B 6.3 Tunnistusvälineen kytkeminen henkilöön**  6.3.1  Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.  **LoA liite 2.3.1 Todentamismekanismi**  Korotettu:  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. |  | Todentamistekijät eivät saa olla kopioitavissa. |
|  | H | Käyttäjä voi suojata menetelmän (välineen) ja todentamistekijänsä luotettavasti muiden käytöltä. | **LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu**  Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.  Myös **LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi**  Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu.  **M72B 6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky**  6.1.1  Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat tunnistusmenetelmän eheyden ja luottamuksellisuuden. Tunnistusmenetelmällä on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan. […]  6.1.2  Tunnistusmenetelmän ominaispiirteiden ja turvatoimenpiteiden on estettävä se, että yhden todentamistekijän vaarantuminen vaarantaisi muiden todentamistekijöiden luotettavuuden. Tunnistusmenetelmän turvatoimenpiteillä on eriytettävä ja suojattava todentamistekijät erityisesti, jos niitä käytetään samalla päätelaitteella.  **M72B 6.4 Tunnistusmenetelmän haltijakohtaisten tietojen käsittely**  6.4.1  Tunnistuspalvelun tarjoajan on varmistettava, etteivät tunnistusvälineeseen liittyvät salaiset tiedot paljastu sen henkilöstölle missään tilanteessa.  6.4.2  Tunnistuspalvelun tarjoaja ei saa kopioida tunnistusvälineeseen liittyviä salaisia tietoja. |  | Esimerkkejä LoA-guidance:  ”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 (ks. Myös LoA-guidance kohta 2.2.1 korkea 1) 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.   LoA-guidance kohta 2.2.2 korkea  Tasolla ”korkea” aktivointiprosessilla on varmistettava, että vain laillinen omistaja voi aktivoida sähköisen tunnistamisen menetelmän ja että aktivointiprosessi on suojattu vahingossa tapahtuvalta häviämiseltä sekä sisäpiiriuhilta, kuten vilpilliseltä yhteistyöltä.  HUOM! Käyttäjän tulee voida varmistua, etteivät turvatekijät, tai esimerkiksi tunnistusvälineeseen liittyvä resetointikoodi voi olla muiden saatavilla. Mahdollinen aktivointi- tai resetointikoodi ovat kertakäyttöisiä. |
|  | S,H | Tunnistetietoja ei luovuteta luottavalle osapuolelle eli tunnistustapahtumaa ei toteuteta ennen kuin tunnistusväline/menetelmä on varmennettu dynaamisella todentamisella | **LoA Liite 2.3.1 Todentamismekanismi**  Henkilön tunnistetietojen luovutusta edeltää sähköisen tunnistamisen menetelmän ja sen voimassaolon luotettava varmentaminen käyttämällä dynaamista todentamista. | A.14.1  Järjestelmien hankkiminen, kehittäminen ja ylläpito/Tietojärjestelmiä koskevat turvallisuusvaatimukset  A.14.1.2 sovelluspalvelutapahtumien suojaaminen julkisissa verkoissa    A.14.1.3 sovelluspalvelutapahtumien suojaaminen | myös tunnistusvälityspalvelu |
|  | S,H | Tunnistustapahtumassa tallentuvat tunnistetiedot (henkilötiedot) suojataan | **LoA Liite 2.3.1 Todentamismekanismi**Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.  **M72B 7.1 Tietoliikenteen salausmenetelmät**  7.1.1  Tunnistuspalvelun tarjoajien välisten ja tunnistuspalvelun tarjoajan ja luottavan osapuolen välisten rajapintojen liikenne on salattava. [kts. menetelmät määräyksestä tai jäljempänä]  **M72B 9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä**  9.1.1  Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on **suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus** joko:  a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai  b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitetulla avaimella. |  | myös tunnistusvälityspalvelu  huomioitava kaikki tunnistustapahtumaan osallistuvien tekniset ympäristöt, joissa tunnistetietoja tallentuu |
|  | S | Todentamismekanismin turvatoimenpiteet suojaavat vakavuusasteeltaan kohtuulliselta hyökkäykseltä | **TunnL 8 §** **Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**  8.1 § 3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;  **LoA Liite 2.3.1 Todentamismekanismi**  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. | ISO 29115  ISO/IEC 15408-1  ISO/IEC 18045, liite B  Common Criteria CCDB 2009 03, kappale 3  ETSI TS 102 165-1, kappale 6.6 ja 6.7 | Vrt. kriteeri 1 riskiarvio ja hyökkäyspotentaalin laskeminen  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.  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.  Common Criteria ja ETSI 102 165-1 sisältävät ohjeita hyökkäyspotentaalin laskemiselle.  todentamismekanismissa on huomioitava myös uhka väärän asiointipalvelun käynnistämästä tunnistuspyynnöstä tai kaappaamasta tunnistusistunnosta (phishing)  ks. LoA guidance kohdan 2.3.1 kuvaus  myös tunnistusvälityspalvelu |
|  | H | Todentamismekanismin turvatoimenpiteet suojaavat vakavuusasteeltaan korkean tason hyökkäykseltä | **TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**  8.1 § 3) tunnistusmenetelmällä voidaan varmistua, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1 ja 2.3 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;  **LoA Liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu**  Sähköisen tunnistamisen menetelmä on suojattu toisintamiselta ja väärentämiseltä sekä hyökkäyksiltä, joiden vakavuusaste on korkea (”high”).  **LoA Liite 2.3.1 Todentamismekanismi**  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. | ks. yllä | myös tunnistusvälityspalvelu  kaikki todentamismekanismiin liittyvät turvallisuusseikat suhteutettuna korkean vakavuustason hyökkäyspotentiaaliin |
|  | S, H | Todentamismekanismi näyttää asiointipalvelun nimen niissä välineissä ja tunnistusprosessin vaiheissa missä se on mahdollista | **M72B 6.2.2** Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto luottavasta osapuolesta, jolle tunnistus välitetään. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista.  **M72B 12.1 Pakolliset tiedot**  Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:  [...]4) tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta. |  | myös tunnistusvälityspalvelu |
|  | S, H | Todentamismekanismi näyttää istuntotunnisteen niissä välineissä ja tunnistusprosessin vaiheissa missä se on mahdollista | **M72B 6.2.1** Tunnistuspalvelun on näytettävä tunnistusvälineen käyttäjälle tunnistustapahtumassa tieto, jonka perusteella käyttäjä voi varmistaa, että tunnistusvälineeseen käyttäjän saama tunnistuspyyntö liittyy käyttäjän omaan asiointitapahtumaan. Tiedon näyttäminen on pakollista sellaisessa tunnistusmenetelmässä, jossa se on teknisesti mahdollista. |  | myös tunnistusvälityspalvelu |
|  | S,H | Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia **tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välillä** | **LoA Liite 2.4.6 Tekniset tarkastukset** (controls)  2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.  **M72B 7.1 Tunnistusjärjestelmän rajapintojen salausvaatimukset**  7.1.1  Tunnistuspalvelun tarjoajien välisten ja tunnistuspalvelun tarjoajan ja luottavan osapuolen välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa, varmenteissa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:  1) Avaintenvaihto: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE-menetelmässä vähintään 2048 bittiä ja ECDHE-menetelmässä vähintään 224 bittiä.  2) Allekirjoitus tai epäsymmetrinen salaus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen tai salaukseen avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmiä ECDSA:ta tai EdDSA:ta äärellisen kunnan koon tulee olla vähintään 224 bittiä.  3) Symmetrinen salaus: Salausalgoritmin on oltava AES, Serpent tai ChaCha20. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, CCM, GCM tai CTR.  4) Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305..  7.1.2  Kohdassa 7.1.1 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi 1-4 alakohdissa tarkoitettuun käyttöön seuraavien asiakirjojen ajantasaisissa versioissa:  a) Liikenne- ja viestintävirastossa toimivan salaustuotteiden hyväksyntäviranomaisen (Crypto Approval Authority) ohje Kryptografiset vahvuusvaatimukset luottamuksel-lisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015); tai  b) eräiden Euroopan unionin tai ETA-alueen jäsenvaltioissa toimivien sertifiointielinten välisen SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recog-nition Agreement) asiakirja SOG-IS Crypto Evaluation Scheme Agreed Crypto-graphic Mechanisms.  7.1.3  Salausasetukset tulee teknisesti pakottaa edellä lueteltuihin vähimmäistasoihin, jotta yhteyskättelyissä ei päädyttäisi vähimmäistasoja heikompiin asetuksiin.  7.2 Tietoliikenteen salausprotokolla  Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2.  Henkilötietoja sisältävien sanomien eheys ja luottamuksellisuus on suojattava edellä 1 momentissa tarkoitetun liikenteen salauksen lisäksi sanomatasolla 1 momentin mukaisesti.  **M72B 8 Tietoliikenteen osapuolten varmentaminen**  8.1 Tietoliikenneyhteyden osapuolten tunnistaminen  Tunnistuspalveluiden välisessä sekä tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenneyhteyden perustamisessa on todennettava tietoliikenteen tai sanomien salaamisessa käytettävien varmenteiden ja avainten aitous ja eheys sekä niiden haltijat.  Todentamisen on perustuttava eIDAS-asetuksen mukaiseen hyväksyttyyn sähköiseen allekirjoitukseen tai hyväksyttyyn sähköiseen leimaan taikka suoraan kahdenväliseen menettelyyn. Todentaminen ei voi perustua pelkästään yleisesti luotettuun varmenteeseen.  8.2 Varmenteiden ja avainten uusiminen  Edellä 8.1 kohdassa tarkoitetut varmenteet ja avaimet on uusittava säännöllisesti.  Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:   1. 8.1 kohdan mukaisella menettelyllä; 2. toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne 8.1 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai 3. allekirjoittamalla uusi avain 8.1 kohdan mukaisesti toimitetulla avaimella tai sellaisesta ketjutetulla avaimella.   **M72B 9 Tunnistussanomien eheys ja luottamuksellisuus**  9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä  9.1.1  Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:   1. varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai 2. salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimite-tulla avaimella.   9.1.2  Tunnistusvälityspalvelun ja luottavan osapuolen välisessä tietoliikenteessä tunnistussanomat on todennettava allekirjoittamalla.  9.2 Sanomien suojaaminen käyttäjärajapinnassa  Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.1.b) alakohdan mukaisesti.  9.3 Salausalgoritmit ja menettelyt  Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä. | A.10.1.1 salauksen käytön periaatteet  A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä | myös tunnistusvälityspalvelu |
|  | S,H | Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia **tunnistuspalvelun ja asiointipalvelun välillä** | **LoA Liite 2.4.6 Tekniset tarkastukset** (controls)  2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.  **M72B 7-9 (yllä)**  **M72B 9 Tunnistussanomien eheys ja luottamuksellisuus**  **9.1 Sanomien suojaaminen tunnistuspalveluiden ja luottavan osapuolen välillä**  9.1.1  Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:  a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai  b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitetulla avaimella.  […]  **9.2 Sanomien suojaaminen käyttäjärajapinnassa**  Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.1.b) alakohdan mukaisesti.  **9.3 Salausalgoritmit ja menettelyt**  Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä. | A.10.1.1 salauksen käytön periaatteet  A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä | huom. myös tunnistusvälityspalvelu |
|  |  |  |  |  |  |
|  | S,H | Todentamismekanismissa noudatetaan pakollisia salausvaatimuksia **käyttäjärajapinnassa (selain, mobiili)** | **LoA Liite 2.4.6 Tekniset tarkastukset** (controls)  2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.  **M72B 7 (yllä)**  **M72B 9.2 Sanomien suojaaminen käyttäjärajapinnassa**  Jos tunnistussanomat välitetään käyttäjän selaimen tai päätelaitteen kautta, sanomat on salattava ja allekirjoitettava 9.1.1.b alakohdan mukaisesti.  **M72B 9.3 Salausalgoritmit ja menettelyt**  Sanomien salaamisessa ja allekirjoittamisessa on käytettävä soveltuvin osin 7.1 kohdan mukaisia menettelyjä. | A.10.1.1 salauksen käytön periaatteet  A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä | huom. myös tunnistusvälityspalvelu |
|  | H | Todentamismekanismissa noudatetaan **suosituksen** mukaisia tiukennettuja/korkean tason salausvaatimuksia tunnistusvälityspalvelun ja tunnistusvälityksen välillä, tunnistuspalvelun ja asiointipalvelun välillä ja käyttäjärajapinnassa (selain, mobiili) | **MPS72B kohta 4.7.1.3 (20.5.2022) suositus**  Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä säännöksessä 7.1 edellytettyjen korotetun varmuustason vaatimusten sijaan seuraavassa esitettyjä suluissa olevia arvoja, **joilla saavutetaan vähintään 128 bitin vahvuustaso**:  1) **Avaintenvaihto**: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (*finite field*) koon tulee olla DHE-menetelmässä vähintään 2048 (**korkealla varmuustasolla 4096**) bittiä ja ECDHE-menetelmässä vähintään 224 (**korkealla varmuustasolla 256**) bittiä.  IANA:n IKEv2-määritysten mukaiset DH-ryhmät 14 - **21**, 23, 24 ja 26 (korkealla varmuustasolla***16 - 21***) toteuttavat edellä mainitut edellytykset.  2) Allekirjoitus tai epäsymmetrinen salaus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen tai salaukseen, avaimen pituuden tulee olla vähintään 2048 (**korkealla varmuustasolla 3072**) bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta tai EdDSA:ta, alla olevan kunnan koon tulee olla vähintään 224 (**korkealla varmuustasolla 256**) bittiä.  3) Symmetrinen salaus: Salausalgoritmin on oltava AES, Serpent tai ChaCha20 *(***korkealla varmuustasolla *AES tai Serpent****)*. Avaimen pituuden tulee olla vähintään 128 (**korkealla varmuustasolla 128**)bittiä. Salausmoodin on oltava CBC, CCM, GCM tai CTR.  4) Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512 (**korkealla varmuustasolla *SHA-3-256, SHA-3-384, SHA-3-512***) | A.10.1.1 salauksen käytön periaatteet  A.13.2.3 viestintäturvallisuus/tietojen siirtäminen: sähköinen viestintä | huom. myös tunnistusvälityspalvelu |

# Yhteentoimivuus

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| KESKEISET SÄÄNNÖKSET  TunnL 29 § Sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointi  Tunnistuspalvelun tarjoajan on määräajoin teetettävä palvelulleen 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu tässä laissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset.  …  M72B 15 Vaatimuksenmukaisuuden arviointikriteerit  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  d) teknisiin toimenpiteisiin  e) yhteentoimivuuteen luottamusverkostossa  TunnL 12 a §  …  Tunnistuspalvelun tarjoajien on tehtävä yhteistyötä sen varmistamiseksi, että luottamusverkoston jäsenten väliset tekniset rajapinnat ovat yhteen toimivia ja että ne mahdollistavat yleisesti tunnettujen standardien mukaisten rajapintojen tarjoamisen luottaville osapuolille.  …  M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot  12.1 Pakolliset tiedot  Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:   1. luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama henkilön yksilöivä tunniste, henkilön etunimi, henkilön suku-nimi ja henkilön syntymäaika; 2. oikeushenkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja organisaation yksilöivä tunniste; 3. tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; sekä 4. tunnistusvälityspalvelun varmistama tieto luottavasta osapuolesta.   12.2 Valinnaiset tiedot  Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava teknisesti suunniteltu valmius välittää:   1. tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua; 2. luonnollista henkilöä koskevassa tunnistustapahtumassa etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä, syntymäpaikka, nykyinen osoite ja sukupuoli; ja 3. oikeushenkilöä koskevassa tunnistustapahtumassa: 4. nykyinen osoite; 5. arvonlisäverotunniste; 6. verorekisterinumero; 7. Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY1 3 artiklan 1 kohdassa tarkoitettu tunniste; 8. komission täytäntöönpanoasetuksessa (EU) N:o 1247/20122 tarkoitettu oikeushenkilötunnus (LEI); 9. komission täytäntöönpanoasetuksessa (EU) N:o 1352/20133 tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä 10. neuvoston asetuksen N:o 389/20124 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero.   12.3 Tunnistuksen pseudonymisointi  Edellä 12.1 ja 12.2 kohdassa määrätyt velvoitteet koskevat tunnistusvälineen käyttäjän todentamisessa tunnistusvälineen ja tunnistusvälityspalvelun välistä rajapintaa siinäkin tapauksessa, että tunnistusvälityspalvelu ilmoittaa tunnistus- ja luottamuspalvelulain 8 §:n 2 momentissa tarkoitetulla tavalla luottavalle osapuolelle vain tunnistusvälineen käyttäjän salanimen tai rajoitetun määrän henkilötietoja.  14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset  14.1 Tiedonsiirrossa käytettävä protokolla  Tunnistuspalvelun tarjoajan on osaltaan mahdollistettava tunnistuslain 17 §:n mukainen ensitunnistamisen ketjuttaminen ja tunnistuslain 12 a §:n mukainen tunnistustapahtumien välitys luottamusverkostossa vähintään OpenID Connect- tai SAML-protokollan mukaisella rajapinnalla.  14.2 Rajapinnan muut ominaisuudet  Tunnistusvälineen tarjoaja, tunnistusvälityspalvelun tarjoaja ja luottava osapuoli sekä kansallisen solmupisteen toteuttaja sopivat keskenään niiden välisten rajapintojen muista kuin tässä määräyksessä määrätyistä ominaisuuksista ja käytettävästä protokollasta. | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | S, H | Tunnistuspalvelun tarjoaja tarjoaa luottamusverkostossa vähintään yhtä yleisesti käytetyn standardin mukaista rajapintaa. | **VNA 169/2016 Valtioneuvoston asetus vahvan sähköisen tunnistuspalvelun tarjoajien luottamusverkostosta**  **1 § Luottamusverkoston tekniset rajapinnat**  Vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (617/2009), jäljempänä tunnistuslaki, 12 a §:n 2 momentissa tarkoitettuja teknisiä rajapintoja ovat:  1) tunnistusvälineen tarjoajien välinen rajapinta;  2) tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välinen rajapinta;  3) tunnistusvälityspalvelun tarjoajan ja tunnistuspalveluun luottavan osapuolen välinen rajapinta.  Luottamusverkostoon kuuluvat tunnistuspalvelun tarjoajat voivat sopia tunnistuslain 12 a §:n 3 momentissa tarkoitetun tunnistetiedon veloituksen välittämiseen tarvittavasta tai muusta luottamusverkoston toiminnassa tarpeellisesta rajapinnasta.  Luottamusverkostoon kuuluvan tunnistuspalvelun tarjoajan on tarjottava 1 momentin 1 ja 2 kohdassa tarkoitetuissa rajapinnoissa kummassakin vähintään yhtä yleisesti käytetyn standardin mukaista teknistä rajapintaa.  **M72B 14 Tiedonsiirrossa käytettävä protokolla ja muut vaatimukset**  **14.1 Tiedonsiirrossa käytettävä protokolla**  Tunnistuspalvelun tarjoajan on osaltaan mahdollistettava tunnistuslain 17 §:n mukainen ensitunnistamisen ketjuttaminen ja tunnistuslain 12 a §:n mukainen tunnistustapahtumien välitys luottamusverkostossa vähintään OpenID Connect- tai SAML-protokollan mukaisella rajapinnalla. |  | **Soveltaminen: M72B kohta 14.1 tiukentunut vaatimus "vähintään OpenID Connect tai SAML-protokollan mukaisella rajapinnalla"** Liikenne- ja viestintävirasto on laatinut luottamusverkoston yhteistoimintaryhmää kuullen suositusprofiilit SAML ja Open IDConnect -protokollille.  212/2023 S Finnish Trust Network SAML 2.0 Protocol Profile version 2.1  213/2023 S Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 2.1  Suositukset löytyvät viraston verkkosivulta <https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen> |
|  | S,H | Tunnistusvälineen tarjoaja tarjoaa vaatimusten mukaiset tiedot (attribuutit) **luonnollisen henkilön** tunnistamisessa | **M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot**  **12.1 Pakolliset tiedot**  Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:  1) luonnollista henkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja henkilön syntymäaika; […]  3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; […] |  | Välityspalvelu voi tarvittaessa rikastaa tai köyhdyttää tunnistusvälineen tarjoajalta saatuja tietoja (kts. M72B 12.3 kohta). Tunnistusvälineen tarjoajan on joka tapauksessa välitettävä M72B:n 12.1 kohdan mukaiset tiedot. |
|  | S, H | Tunnistusvälineen tarjoajalla on vaadittu **suunniteltu** **valmius** välittää optionaaliset tiedot **luonnollisen henkilön** tunnistamisessa | **M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot**  **12.2 Valinnaiset tiedot**  Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava teknisesti suunniteltu valmius välittää:  1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;  2) luonnollista henkilöä koskevassa tunnistustapahtumassa etunimi (-nimet) ja sukunimi (-nimet) syntymähetkellä, syntymäpaikka, nykyinen osoite ja sukupuoli; […] |  | MPS72 12.1 § perustelut, s. 56:  Valmius välittää valinnaisia attribuutteja tarkoittaa, että valinnaisten attribuuttien käsittely täytyy suunnitella rajapinnassa ja tunnistusjärjestelmässä siten, että tunnistuspalvelun tarjoajalla on käsitys käyttöönotossa tarvittavista teknisistä toimenpiteistä. Teknistä toteutusta järjestelmiin ei vaadita valinnaisille attribuuteille. Teknisissä konfiguroinneissa tulee kuitenkin huomioida, etteivät tunnistussanomiin sisältyvät valinnaiset attribuutit haittaa tunnistustapahtumia silloinkaan, kun niiden käytöstä ei ole sovittu. Valvontaa varten suunnitelma täytyy käytännössä dokumentoida. |
|  | S, H | Tunnistusvälineen tarjoaja tarjoaa vaatimusten mukaiset tiedot (attribuutit) **oikeushenkilön** tunnistamisessa | **M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot**  Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on välitettävä:  […]  2) oikeushenkilöä koskevassa tunnistustapahtumassa ainakin tunnistusvälineen tarjoajan varmistama oikeushenkilöä edustavan luonnollisen henkilön yksilöivä tunniste, henkilön etunimi, henkilön sukunimi ja organisaation yksilöivä tunniste;  3) tieto tunnistusvälineen korotetusta tai korkeasta varmuustasosta; […] |  | vain, jos ryhdytään tarjoamaan oikeushenkilön vahvaa sähköistä tunnistusta |
|  | S, H | Tunnistusvälineen tarjoajalla on vaadittu suunniteltu valmius välittää optionaaliset tiedot **oikeushenkilön** tunnistamisessa | **M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot**  **12.2 Valinnaiset tiedot**  Tunnistusvälineen tarjoajan ja tunnistusvälityspalvelun tarjoajan välisessä rajapinnassa on oltava teknisesti suunniteltu valmius valmius välittää:  1) tieto siitä, koskeeko tunnistustapahtuma julkisen hallinnon asiointipalvelua vai yksityistä asiointipalvelua;  […]  3) oikeushenkilöä koskevassa tunnistustapahtumassa  a) nykyinen osoite;  b) arvonlisäverotunniste;  c) verorekisterinumero;  d) Euroopan parlamentin ja neuvoston direktiivin 2009/101/EY 3 artiklan 1 kohdassa tarkoitettu tunniste;  e) komission täytäntöönpanoasetuksessa (EU) N:o 1247/2012 tarkoitettu oikeushenkilötunnus (LEI);  f) komission täytäntöönpanoasetuksessa (EU) N:o 1352/2013 tarkoitettu taloudellisen toimijan rekisteröinti- ja tunnistenumero (EORI-numero); sekä  g) neuvoston asetuksen N:o 389/2012 2 artiklan 12 kohdassa tarkoitettu valmisteveronumero. |  |  |

# Tekniset tietoturvavaatimukset

|  |
| --- |
| KESKEISET SÄÄNNÖKSET  M72B 15 Vaatimuksenmukaisuuden arviointikriteerit  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  d) teknisiin toimenpiteisiin  TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset  4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa…2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat  LoA Liite 2.4.6 Tekniset tarkastukset (controls)  1) Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  M72B 5 Tunnistusjärjestelmän tietoturvavaatimukset  5.1 Tunnistusjärjestelmän suojautumiskyky  5.1.1  Tunnistusjärjestelmän tietoliikenne, tietojärjestelmät ja niiden käyttö on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä koko elinkaaren ajan siten, että tunnistuspalvelun eheys ja luottamuksellisuus on suojattu. Tunnistuspalvelulla on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.  5.1.2  Tunnistuspalvelun tarjoajien välisten sekä tunnistuspalvelun ja luottavan osapuolen välisten tietoliikenneyhteyksien salausvaatimukset määrätään kohdassa 7. Tunnistus-järjestelmän muiden tietoliikenneyhteyksien sekä tietojärjestelmien ja tiedon salauksessa on käytettävä teknisesti soveltuvin osin määräyksen 7 kohdan mukaisia salausratkaisuja, ellei suojautumiskyky kokonaisuutena arvioiden toteudu muilla turvatoimenpiteillä.  5.2 Tietoliikenneturvallisuus  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:   1. verkon rakenteellinen turvallisuus; 2. tietoliikenneverkon vyöhykkeistäminen; 3. suodatussäännöt vähimpien oikeuksien periaatteilla; 4. suodatuksen ja valvontajärjestelmien hallinnointi; 5. turvalliset hallintayhteydet; sekä 6. käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.   5.3 Tietojärjestelmäturvallisuus  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:   1. pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella; 2. järjestelmien käyttäjien yksilöity tunnistaminen; 3. järjestelmien koventaminen; 4. haittaohjelmasuojaus; 5. turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi; 6. poikkeamien havainnointikyky ja korjausprosessi; sekä 7. käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.   5.4 Käyttöturvallisuus  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:   1. muutosten hallinta; 2. tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys; 3. etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta; 4. ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta; 5. varmuuskopiointi; sekä 6. käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.   5.4 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet  Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on:   1. korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja 2. korkealla varmuustasolla kokonaisuutena arvioiden estetty. |

## Tietoliikenneturvallisuus

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.1 Tietoliikenneturvallisuus | | | | | |
| **nro** | **varmuustaso** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **Säännökset** | **Standardiviittaus** | **huomioita** |
|  | S,H | Tietoliikenneturvallisuus:  Tunnistusjärjestelmän **tietoliikenneyhteydet, hallintayhteydet, prosessit** (tunnistuspalvelun tuotantoon ml. hallintaan liittyvien osaprosessien tietoliikenne) ja niiden **suojauskäytännöt** on **tunnistettu, dokumentoitu ja ylläpidetty**  Tunnistusjärjestelmän tietoliikenneyhteyksien vyöhykkeistäminen ja suodatussäännöstöt on toteutettava ja ylläpidettävä vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:   1. verkon rakenteellinen turvallisuus; 2. tietoliikenneverkon vyöhykkeistäminen; 3. suodatussäännöt vähimpien oikeuksien periaatteilla; 4. suodatuksen ja valvontajärjestelmien hallinnointi; 5. turvalliset hallintayhteydet; sekä 6. käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.   **LoA Liite 2.4.6 Tekniset tarkastukset** (controls)  2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta. | A.8.1.1 Suojattavan omaisuuden luetteloiminen  A.13.1 viestintäturvallisuus/verkon turvallisuuden hallinta:  A.13.1.1 verkon hallinta  A.13.1.3 ryhmien eriyttäminen verkossa | Tunnistusjärjestelmän kokonaisarkkitehtuurissa huolehditaan tietoliikenneturvallisuudesta.  Huom. suunnittelussa on huolehdittava myös kaikista relevanteista tietoliikenneyhteyksistä alihankkijoihin (infra, ohjelmistot, käyttöpalvelut, korttitehdas jne. jne.)  Ilmoitukseen/**tarkastuskertomukseen** on liitettävä arkkitehtuurista kuvaus, josta ilmenevät tunnistusjärjestelmän osien väliset tietoliikenneyhteydet ja niiden suojauskäytännöt. Dokumentaatioon tulee selkeästi kuvata eri turvatason verkkoalueet, sekä niiden välissä toimivat suodatus- ja valvontajärjestelmät |
|  | S, H | Tietoliikenneturvallisuus:  Tunnistusjärjestelmän **tietoliikennelaitteet**  **ja -järjestelmät** on tunnistettu ja dokumentoitu. | **M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet**  Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän   1. tietoliikenneturvallisuus   a) verkon rakenteellinen turvallisuus  **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) verkon rakenteellinen turvallisuus; | A.8.1.1 Suojattavan omaisuuden luetteloiminen |  |
|  | S, H | Tietoliikenneturvallisuus:  **Tuotantoverkko** tulee olla **eriytettynä** ylläpito- ja hallinnointiverkosta.  Ylläpito- ja hallinnointiverkon tulee olla eriytettynä muusta toimistoverkosta.  Käytössä on tuotannosta eriytetty kehitysympäristö. | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) verkon rakenteellinen turvallisuus;  b) tietoliikenneverkon vyöhykkeistäminen;  […]  **5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet**  Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on:  a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja  b) korkealla varmuustasolla kokonaisuutena arvioiden estetty. | A.12.1.4 Käyttöturvallisuus: Kehitys-, testaus- ja tuotantoympäristöjen erottaminen | Eriyttäminen voidaan tehdä loogisesti tai fyysisesti. Eriyttämiseltä vaadittavaan tasoon vaikuttavat kokonaisuutena verkon kriittisyys ja siinä käsiteltävät tiedot. Vaatimuksen tarkoitus on vähentää tietoliikenneyhteyksien kautta aiheutuvia riskejä verkkojen eheydelle, luottamuksellisuudelle ja käytettävyydelle. |
|  | S,H | Tietoliikenneturvallisuus:  Tunnistusjärjestelmän tietoliikenneyhteyksillä **huolehditaan suodatuksista** vähimpien oikeuksien periaatteilla | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  c) suodatussäännöt vähimpien oikeuksien periaatteilla;  d) suodatuksen ja valvontajärjestelmien hallinnointi;  […] | A.13.1.1-3 viestintäturvallisuus/verkon turvallisuuden hallinta:  A.13.1.1 verkon hallinta  A.13.1.2 Verkkopalvelujen turvaaminen  A.13.1.3 Ryhmien eriyttäminen verkossa  ks. myös pääsynhallinta |  |
|  | S, H | Tietoliikenneturvallisuus:  Tuotantoverkon **yhteyksien julkiseen verkkoon** tulee olla riskiperusteisia, vain palvelun toiminnallisuudet mahdollistavia yhteyksiä. | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) verkon rakenteellinen turvallisuus;  […]  c) suodatussäännöt vähimpien oikeuksien periaatteilla;  d) suodatuksen ja valvontajärjestelmien hallinnointi;  e) turvalliset hallintayhteydet; sekä  […]  **5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet**  Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on:  a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja  b) korkealla varmuustasolla kokonaisuutena arvioiden estetty. | ks. ed. rivi | Kaikki muut kuin toiminnalle tarpeelliset yhteydet on nimenomaisesti kielletty tai suljettu. |
|  | S, H | Tietoliikenneturvallisuus:  Tunnistuspalveluiden ja luottavien osapuolten **kryptografinen avainmateriaali** tai **metadata** vaihdetaan turvallisesti | **M72B 8 Tietoliikenteen osapuolten varmentaminen**  **8.1 Tietoliikenneyhteyden osapuolten tunnistaminen**  Tunnistuspalveluiden välisessä sekä tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenneyhteyden perustamisessa on todennettava tietoliikenteen tai sanomien salaamisessa käytettävien varmenteiden ja avainten aitous ja eheys sekä niiden haltijat.  Todentamisen on perustuttava eIDAS-asetuksen mukaiseen hyväksyttyyn sähköiseen allekirjoitukseen tai hyväksyttyyn sähköiseen leimaan taikka suoraan kahdenväliseen menettelyyn. Todentaminen ei voi perustua pelkästään yleisesti luotettuun varmenteeseen.  **8.2 Varmenteiden ja avainten uusiminen**  Edellä 8.1 kohdassa tarkoitetut varmenteet ja avaimet on uusittava säännöllisesti.  Uusien varmenteiden ja avainten aitouden ja eheyden varmistamiseksi uusiminen on tehtävä joko:   1. 8.1 kohdan mukaisella menettelyllä; 2. toimittamalla uudet avaimet tietoliikenneyhteydellä, jonka eheys ja luottamuksellisuus on varmistettu sitomalla osapuolten tietoliikenne 8.1 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai 3. allekirjoittamalla uusi avain 8.1 kohdan mukaisesti toimitetulla avaimella tai sellaisesta ketjutetulla avaimella.   **LoA 2.4.6 Tekniset tarkastukset**  1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.  […]  5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.  **LoA 2.4.6 Tekniset tarkastukset**  Substantial: Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.  **LoA 2.3.1   Todentamismekanismi**  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 todentamismekanismeja. | A.10.1.2 Salauksenhallinta: salausavainten hallinta | vrt. PSD2/RTS eIDAS art45 tai eSeal varmennevaatimus osapuolen tunnistamiselle  Osapuoleten välille on määritelty prosessi turvalliseen luottosuhteen perustamiseen ja osapuolten todentamiseen ja pitkäikäisten avainten/salaisuuksien vaihtamiseen.  Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja  Prosessit edellyttävät vähintään kryptografisesti vahvojen avaimien käyttöä, turvallista avaintenjakelua, turvallista avainten säilytystä, säännöllisiä avaintenvaihtoja, vanhojen tai paljastuneiden avainten vaihdon, sekä valtuuttamattomien avaintenvaihtojen estämisen  KATAKRI v.2015 (I12) |
|  | H | Tietoliikenneturvallisuus:  Tunnistuspalveluiden ja luottavien osapuolten kryptografinen avainmateriaali tai metadata vaihdetaan turvallisesti | vrt. yllä sekä **LoA 2.3.1   Todentamismekanismi**  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. | A.10.1.2 Salauksenhallinta: salausavainten hallinta |  |
|  |  | Tunnistuspalvelun (välityspalvelu tai oman välineen välitys) tarjoajan ja luottavan osapuolen tunnistussanomat on todennettava, |  |  |  |
|  | S, H | Tunnistussanomien eheydestä ja luottamuksellisuudesta huolehditaan. | **M72B 9.1.1**  Tunnistuspalveluiden välisessä ja tunnistuspalvelun ja luottavan osapuolen välisessä tietoliikenteessä on suojattava henkilötietoja sisältävien tunnistussanomien eheys ja luottamuksellisuus joko:  a) varmistamalla tietoliikenneyhteyden eheys ja luottamuksellisuus sitomalla osapuolten tietoliikenne 8 kohdan mukaisesti toimitettuihin varmenteisiin tai avaimiin; tai  b) salaamalla ja allekirjoittamalla sanomat 8 kohdan mukaisella menettelyllä toimitetulla avaimella.  **LoA liite 2.4.6 Tekniset tarkastukset**  1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta. |  | Kohdassa 8 kuvataan eri menetelmiä, joilla voidaan toteuttaa osapuolten riittävä tietoliikennesuojaus. |
|  | S,H | Tietoliikenneturvallisuus:  Tunnistusjärjestelmän tietoliikenneyhteyksien **suodatusten ja valvontajärjestelmien hallinnoinnista** huolehditaan | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) suodatuksen ja valvontajärjestelmien hallinnointi;  e) turvalliset hallintayhteydet; sekä  […] | A.13.1 viestintäturvallisuus/verkon turvallisuuden hallinta:  A.13.1.1 verkon hallinta |  |
|  | S | Tietoliikenneturvallisuus/hallinta:  Tunnistusjärjestelmän etäkäytössä ja hallinnassa on **arvioitu ja minimoitu** sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat. | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) suodatuksen ja valvontajärjestelmien hallinnointi;  e) turvalliset hallintayhteydet; sekä  […]  **5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  c) etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta;  […]  **5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet**  Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on:  a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja  […] | A.9.4. Järjestelmien ja sovellusten pääsynhallinta:  A.9.4.1 Tietoihin pääsyn rajoittaminen  A.9.4.4 Ylläpito-ja hallintasovellukset  A.13.1.3 verkon turvallisuu-den hallin-ta: Ryhmien eriyttäminen verkossa | MPS72: internetiä ja toimistoverkkoa pidetään ei-luotettuna verkkona, ellei toimistoverkko kuulu vaatimustenmukaisuuden arvioinnin piiriin. Tiedonsiirtokanavan täytyy siis olla etäkäytössä suojattu ja toimistoverkon aiheuttamat riskit täytyy huomioida. Korotetun varmuustason vaatimukset ovat tavanomaisia ja ne katetaan jo esimerkiksi ISO 27001 -vaatimusten kautta, jos sovelletaan sitä. |
|  | H | Tietoliikenneturvallisuus/hallinta:  Tunnistusjärjestelmän (tuotantoverkon) etäkäytössä ja etähallinnassa on **estetty** sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) suodatuksen ja valvontajärjestelmien hallinnointi;  e) turvalliset hallintayhteydet; sekä  […]  **5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  c) etäkäytön ja -hallinnan suojaaminen etäkäyttöympäristön uhkilta;  […]  **5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet**  Tuotantoverkko ja sen edellä 5.2.e) ja 5.4.c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on:  […]  b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.  **MPS72B soveltamisohje:**  Korkealla varmuustasolla vaatimukset voi toteuttaa ainakin siten, että etäkäytössä olevasta työasemasta estetään pääsy muihin organisaation palveluihin kuten sähköpostiin ja poistetaan työasemasta mahdollisuus käyttää muita kuin hallintaverkon käytön kannalta välttämättömiä toimintoja. Käytännössä tämä tarkoittaa siis erillistä työasemaa hallintakäyttöä varten.  Korkealla varmuustasolla edellytetty kokonaisarvio tarkoittaa sitä, että jos käytettään muuta kuin edellä kuvattua kovennettua työasemaa, otetaan toteutuksessa huomioon tuotantojärjestelmän eriyttäminen ja muut järjestelyt, joilla tietoturvauhkat voidaan hallita. Lähtökohtaisesti tällöin edellytetään virtualisoitua terminointia tai kvm-periaatteeseen (etätyöpöytä) perustuvaa ratkaisua.  Olennaista on, mitä tehdään sillä päätelaitteella, josta virtualisoitua yhteyttä otetaan ja siten esimerkiksi two-factor VPN-yhteys virtualisoituun työasemaan ei yksin riitä ratkaisuksi. Riittävää ei ole myöskään, että käytetään virustorjuntaa ja web-proxya.  Välttämättömien tiedostojen siirrossa koneelta toiselle on myös huomioitava haittaohjelmien riski mm. pitämällä huolta siitä, että käytetään vain luotettavia lähteitä ja varmistetaan tietoturvallisuus (eheys) kaikilla tarpeellisilla menetelmillä. | ks. ed. rivi |  |

## Tietojärjestelmäturvallisuus

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.2 Tietojärjestelmäturvallisuus | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | S, H | Tietojärjestelmäturvallisuus:  Tunnistusjärjestelmän **tietojärjestelmät ja prosessit** (tunnistuspalvelun tuotantoon ml. hallintaan liittyvät tietojärjestelmiä käyttävät prosessit) on **tunnistettu, dokumentoitu ja ylläpidetty.**  Tunnistusjärjestelmän tietojärjestelmät on **luokiteltu** huomioiden niissä käsiteltävä tieto ja niiden mahdollistamat toiminnot. Järjestelmien luokittelussa tulee huomioida suojattavan tiedon koko elinkaari.  Hallintaan käytettävä tietojenkäsittely-ympäristö on erotettu muista ympäristöistä | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  […] | A.8.1.1 suojattavan omaisuuden hallinta, vastuu suojattavasta omaisuudesta: suojattavan omaisuuden luetteloiminen  A.8.2.1 Suojattavan omaisuuden hallinta: tietojen luokittelu | Luokittelu: mm. laitteiden, ohjelmistojen ja muu omaisuuden hyväksytty käyttö tulee olla määriteltynä |
|  | S, H | Tietojärjestelmäturvallisuus:  Tunnistusjärjestelmän **pääsyoikeudet** on määritelty ja dokumentoitu.    Pääsyoikeudet **perustuvat** tietojärjestelmien luokitteluun ja henkilön/käyttäjän tehtäviin.  Pääsy tulee myöntää vain tehtävien mukaisesti (vähimpien oikeuksien periaate). | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  c) järjestelmien koventaminen;  […] | A.9.1.1 pääsynhallinnan liiketoiminnalliset vaatimukset: pääsynhallintapolitiikka  A.9.1.2 pääsy verkkoihin ja verkko verkkopalveluihin  A.9.4.1 järjestelmien ja sovellusten pääsynhallinta: tietoihin pääsyn rajoittaminen | Pääsyoikeuksien hallinnoinnin avulla rajoitetaan pääsy tietoon ja tiedonkäsittely-ympäristöihin suunnitelmallisesti ja dokumentoidusti |
|  | S, H | Tietojärjestelmäturvallisuus:  Tunnistusjärjestelmän tietojärjestelmien **käyttäjät tunnistetaan** tunnetulla ja turvallisena pidetyllä tekniikalla/menetelmällä. | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  c) järjestelmien koventaminen;  […]  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  […] | A.9.4.2 järjestelmien ja sovellusten pääsynhallinta: turvallinen kirjautuminen | esim. varmenteet, 2FA  pääsääntöisesti muu kuin salasana, mutta jos mukana salasana, kunnolliset salasanapituudet ja yksilölliset (ei yhteiskäyttöiset) salasanat ja käyttäjätunnukset |
|  | S, H | Tietojärjestelmäturvallisuus:  Pääsyoikeuksia valvotaan ja niiden **ajantasaisuudesta** huolehditaan. | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  c) järjestelmien koventaminen;  […]  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  f) poikkeamien havainnointikyky ja korjausprosessi; sekä  […] | A.9.2 pääsyoikeuksien hallinta  A.9.2.1 Käyttäjien rekisteröinti ja poistaminen  A.9.2.3 Ylläpito-oikeuksien hallinta  A.9.2.5 pääsyoikeuksien uudelleenarviointi  A.9.2.6 pääsyoikeuksien poistaminen ja muuttaminen |  |
|  | S,H | Tietojärjestelmäturvallisuus:  Henkilöstön **tehtävät ja toiminnot on määriteltävä** siten, ettei yksi henkilö pysty omalla toiminnallaan tahattomasti tai tahallisesti aiheuttamaan vakavaa turvallisuuspoikkeamaa (vaaralliset työyhdistelmät). | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  c) järjestelmien koventaminen;  […]  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  f) poikkeamien havainnointikyky ja korjausprosessi; sekä  ~~[…]~~ |  | Esimerkiksi vilpillisen tai huolimattoman työntekijän mahdollisuutta myöntää tunnistusmenetelmä vaatimusten vastaisesti voidaan ehkäistä tehtävien määrittelyllä tai muilla kontrolleilla, jotka vähentävät erehdyksen ja väärinkäytöksen riskiä.  Arvioinnissa on huomioitava tunnistusmenetelmän varmuustason mukaisesti kohtuullinen tai korkea hyökkäyspotentiaali, kuten muissakin kohdissa |
|  | S,H | Tietojärjestelmäturvallisuus:  Tunnistusjärjestelmän **kovennuksista** huolehditaan; käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.  Tunnistusjärjestelmässä käytetään **vain** sen toiminnan kannalta **tarvittavia** palveluita, toimintoja, prosesseja, laitteita ja komponentteja. Niiden käyttö on määritelty siten, että asennuksesta on poistettu kaikki tarpeettomat oikeudet ja toiminnot/elementit. | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  c) järjestelmien koventaminen;  […] | A.12.5. tuotantokäytössä olevien ohjelmistojen hallinta | ks. myös tietoliikenne  Ohjeessa 211/2016 oli seuraavia kriteereitä, jotka ovat tässä mukana informatiivisina:  Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi  Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut |
|  | S, H | Tietojärjestelmäturvallisuus:  Tunnistusjärjestelmässä huolehditaan **haittaohjelmien** aiheuttamien haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta. | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) haittaohjelmasuojaus;  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  f) poikkeamien havainnointikyky ja korjausprosessi; sekä  […] | A.12.2 haittaohjelmilta suojautuminen  A.12.6. teknisten haavoittuvuuksien hallinta | Ks. myös poikkeamien havainnointikyky |
|  | S, H | Tietojärjestelmäturvallisuus:  Tunnistusjärjestelmässä käytetään kaikilta osin suositeltavia **salausratkaisuja**. | **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  g) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja. | A.10.1 salauksen käytön periaatteet  A.18.1.5 salaustekniikan hallintaa koskevat säädökset | MPS72:ssa mainitaan lähteinä seuraavia:  SOGIS-MRA  NCSA-FI  NIST  Enisa  SANS  Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:  Prosessit edellyttävät vähintään kryptografisesti vahvojen avaimien käyttöä, turvallista avaintenjakelua, turvallista avainten säilytystä, säännöllisiä avaintenvaihtoja, vanhojen tai paljastuneiden avainten vaihdon, sekä valtuuttamattomien avaintenvaihtojen estämisen.  (KATAKRI v.2015 (I12) |
|  | S,H | Tietojärjestelmäturvallisuus:  Salaustekninen aineisto on suojattu koko elinkaaren ajan | **LoA 2.4.6 Tekniset tarkastukset**  3) Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä.  Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.  **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  c) järjestelmien koventaminen;  […]  g) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.  **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;  […]  f) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja. | A.8.2.1 tiedon luokittelu  A.10.1.1 salauksen käytön periaatteet  A.10.1.2 salausavainten hallinta | Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:  Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä  Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja  Prosessit edellyttävät vähintään kryptografisesti vahvojen avaimien käyttöä, turvallista avaintenjakelua, turvallista avainten säilytystä, säännöllisiä avaintenvaihtoja, vanhojen tai paljastuneiden avainten vaihdon, sekä valtuuttamattomien avaintenvaihtojen estämisen  KATAKRI v.2015 (I12) |

## Käyttöturvallisuus

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.3 Käyttöturvallisuus | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | **S,H** | Käyttöturvallisuus:  Tunnistusjärjestelmän **muutostenhallinta** on suunniteltua ja huolellista. | **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) muutosten hallinta;  […] | A.12.1.2 käyttöturvallisuus/toimintaohjeet ja velvollisuudet: muutoksenhallinta  A.14.2.2 järjestelmien hankkiminen, kehittäminen ja ylläpito/kehitys- ja tukiprosessien turvallisuus: järjestelmään tehtävien muutosten hallintamenettelyt  A.14.2.3 sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen  A.14.2.4 ohjelmistopakettien muutoksia koskevat rajoitukset | Muutosten hallintaan määriteltynä selkeät prosessit. Uusien ominaisuuksien tai muutosten toteutuksessa testaussuunnitelmassa on myös negatiiviset testitapaukset huomioitu. Testaus ei perustu pelkästään automaattisiin testeihin. |
|  | S,H | Käyttöturvallisuus:  Tunnistusjärjestelmän **ohjelmistohaavoittuvuuksien** hallinta on suunnitelmallista.  Tunnistusjärjestelmässä huolehditaan **ohjelmistohaavoittuvuuksien** aiheuttamien haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta. | **M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet**  Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän  3) käyttöturvallisuus  c) ohjelmistohaavoittuvuuksien hallinta  **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta;  […] | A.12.5.1 käyttöturvallisuus: ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin  A.12.6.1 käyttöturvallisuus: teknisten haavoittuvuuksien hallinta  A.14.2. järjestelmien hankkiminen, kehittäminen ja ylläpito/kehitys- ja tukiprosessien turvallisuus  A.14.2.1 turvallisen kehittämisen politiikka  A.14.2.2 järjestelmään tehtävien muutosten hallintamenettelyt  A.14.2.3 sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen  A.14.2.4 ohjelmistopakettien muutoksia koskevat rajoitukset  A.14.2.5 turvallisen järjestelmän suunnittelun periaatteet  A.14.2.6 turvallinen kehitysympäristö  A.14.2.7 ulkoistettu kehittäminen  A.14.2.8 järjestelmän turvallisuustestaus  A.14.2.9 järjestelmän hyväksymistestaus | Organisaation tulee ylläpitää tietokantaa tai listausta kaikista tunnistusjärjestelmän eri ohjelmistokomponenteista.  Organisaatiolla tulee olla prosessi ohjelmistohaavoittuvuuksien havainnointiin ja seurantaan. Haavoittuneet ohjelmistokomponentit tulee päivittää ajantasaisiin versioihin.  Tunnistusjärjestelmässä käytettävien ohjelmistojen tulee noudattaa turvallisen ohjelmoinnin periaatteita.  Tunnistusjärjestelmän uudet versiot tulee testata, myös niin että testitapaukset sisältävät negatiivisa testitapauksia. |
|  |  | Käyttöturvallisuus:  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava, ja jatkuvasti ylläpidettävä:  Ohjelmistokehityksen hallinta | **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) muutosten hallinta;  […];  d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien hallinta;  […] | Kts edellinen | Ohjelmistokehityksen ylläpidossa erityisesti huomioitava toimitusketjun rakenne ja ylläpidettävä tietoa ohjelmiston eri komponenteista ja seurattava niiden päivityksiä.  Turvallinen ohjelmistokehitys  Testaus |
|  | S,H | Käyttöturvallisuus:  Tunnistusjärjestelmän **varmuuskopioinnista** huolehditaan suunnitelmallisesti.  Varmuuskopioinnissa huomioidaan tiedon luokittelu (henkilötiedot, salaustekniset tiedot jne.), järjestelmien palautettavuus ja varmuuskopioiden säilytys. | **M72A 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet**  Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän  3) käyttöturvallisuus  d) varmuuskopiointi  **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  e) varmuuskopiointi; sekä  […] | A.12.3.1 tietojen varmuuskopiointi | Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:  Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä. |

# Poikkeamien havainnointikyky ja hallinta ja häiriöilmoitukset

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| KESKEISET SÄÄNNÖKSET  M72B 15 Vaatimuksenmukaisuuden arviointikriteerit  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  d) teknisiin toimenpiteisiin  Yleiset vaatimukset  TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset  4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa…2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat  LoA Liite 2.4.6 Tekniset tarkastukset (controls)  1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin.  TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä  Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä tunnistuspalveluunsa luottaville osapuolille, tunnistusvälineiden haltijoille, muille luottamusverkostossa toimiville sopimuspuolilleen sekä Liikenne- ja viestintävirastolle palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. […]  Edellä 1 momentissa tarkoitetussa ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.  …  Vaatimuksia on tarkennettu määräyksen M72B 5 kohdassa ja 11 kohdassa | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | S, H | Tunnistusjärjestelmän poikkeamien havaitsemiseen on **kyvykkyys** ja ennalta **määritellyt prosessit**.  Määrittelyissä huomioidaan järjestelmän tietoliikenneyhteyksien ja tietojärjestelmien komponenttien ja prosessien tärkeys/kriittisyys/luokittelu ja se, että turvallisuuteen liittyvät/vaikuttavat tapahtumat kyetään jäljittämään myös jälkikäteen.  Tunnistusjärjestelmässä kerätään ja tallennetaan **tapahtumalokeja** järjestelmän toiminnasta ja tietoturvaan vaikuttavista/liittyvistä tapahtumista ja poikkeamista. | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) suodatuksen ja valvontajärjestelmien hallinnointi;  […]  **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  […]  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  f) poikkeamien havainnointikyky ja korjausprosessi; sekä  […] | A.12.4.1 käyttöturvallisuus: tapahtumien kirjaaminen  A.12.4.2 käyttöturvallisuus: lokitietojen suojaaminen  A.12.4.3 käyttöturvallisuus: pääkäyttäjä- ja operaattorilokit  A.16.1 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta  A. 16.1.1 vastuut ja menettelyt  A.16.1.6 tietoturvahäiröistä oppiminen | Prosessit sisältävät niin automaattiset kuin manuaalisetkin keinot. Prosessit ovat ylläpidettyjä. |
|  | S, H | Tunnistusjärjestelmän **hallintalokit** on määritelty ja eriytetty muista lokeista. Niiden eheydestä on huolehdittu. | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) suodatuksen ja valvontajärjestelmien hallinnointi;  e) turvalliset hallintayhteydet; sekä  […]  **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  a) pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella;  b) järjestelmien käyttäjien yksilöity tunnistaminen;  […]  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  f) poikkeamien havainnointikyky ja korjausprosessi; sekä  […] | A.12.4.1 käyttöturvallisuus: tapahtumien kirjaaminen  A.12.4.2 käyttöturvallisuus: lokitietojen suojaaminen  A.12.1.4 kehitys-, testaus- ja tuotantoympäristöjen erottaminen | hallintalokeihin tallennetaan tiedot tunnistusjärjestelmässä tehtävistä muutoksista |
|  | S, H | Tunnistusjärjestelmän toimintaa, muutoksia ja tapahtumalokeja **monitoroidaan** poikkeamien ja tietoturvaloukkausten havaitsemiseksi.  Tunnistusjärjestelmän **poikkeamat ja häiriöt käsitellään ja analysoidaan** ja niiden vaikuttavuus/vakavuus luokitellaan suunnitelmallisesti. | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) suodatuksen ja valvontajärjestelmien hallinnointi;  […]  **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  f) poikkeamien havainnointikyky ja korjausprosessi; sekä  […] | A.16.1 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta:  A.16.1.2 tietoturvatapahtumien raportointi  A.16.1.3 tietoturvaheikkouksien raportointi  A.16.1.4 tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen | Kaikki havainnot käsitellään ja niiden vaikuttavuus luokitellaan sovittujen menetelmien mukaan.  Lokien analysointiin käytetään automaattisia prosesseja/työkaluja, kuten SIEM. |
|  |  | Tunnistusjärjestelmän poikkeamien ja häiriöiden edellyttämät **korjaavat toimenpiteet** ovat suunnitelmallisia ja tehokkaita.  Toiminnan jatkuvuussuunnittelu sisältää ennalta ehkäiseviä ja korjaavia toimenpiteitä, joilla minimoidaan merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset. | **M72B 5.2 Tietoliikenneturvallisuus**  Tunnistusjärjestelmän tietoliikenteessä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  d) suodatuksen ja valvontajärjestelmien hallinnointi;  […]  **M72B 5.3 Tietojärjestelmäturvallisuus**  Tunnistusjärjestelmän tietojärjestelmissä on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  e) turvallisuuteen liittyvien tapahtumien jäljityskyky ja jäljitysprosessi;  f) poikkeamien havainnointikyky ja korjausprosessi; sekä  […] | A.16.1. tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta:  A.16.1.5 tietoturvahäiriöihin vastaaminen  7.5 Dokumentointu tieto  10.1 Poikkeamat ja korjaavat toimenpiteet | Korjaavat toimeniteet tulee dokumentoida.  Saatavuusvaatimukset (SLA) ovat sopimusasia, huomioitava syrjimättömyys |
|  | S, H | Häiriönhallintaprosesseissa on huomioitu **ilmoitusvelvollisuus muille luottamusverkostoon kuuluville tunnistuspalveluille.** | **TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä**  Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä …tunnistuspalveluunsa muille luottamusverkostossa toimiville sopimuspuolilleen …palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. …  Tunnistuspalvelun tarjoaja voi salassapitosäännösten estämättä ilmoittaa kaikille luottamusverkoston jäsenille 1 momentissa tarkoitetuista uhkista ja häiriöistä sekä palvelun tarjoajista, joiden on syytä epäillä tavoittelevan oikeudetonta taloudellista hyötyä, antavan merkityksellisiä totuudenvastaisia tai harhaanjohtavia tietoja tai käsittelevän henkilötietoja lainvastaisesti.  **Soveltaminen:**  Luottamusverkoston yhteistoimintaryhmässä on laadittu yhteinen käytäntö keskinäisistä häiriöilmoitustilanteista ja ilmoituskynnyksistä. | A.16.1.2 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi | Vastuut poikkeamatilateisiin ja sidosryhmäviestintään on määritelty |
|  | S, H | Häiriönhallintaprosesseissa on huomioitu **ilmoitusvelvollisuus käyttäjille ja luottaville osapuolille.** | **TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä**  Tunnistuspalvelun tarjoajan on…ilmoitettava ilman aiheetonta viivästystä tunnistuspalveluunsa luottaville osapuolille, tunnistusvälineiden haltijoille, …palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista. | A.16.1.2 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi | Vastuut poikkeamatilateisiin ja sidosryhmäviestintään on määritelty  Luottavilla osapuolilla tarkoitetaan asiointipalveluita |
|  | S, H | Häiriönhallintaprosesseissa on huomioitu **ilmoitusvelvollisuus Liikenne- ja viestintävirastolle** | **TunnL 16 § Tunnistuspalvelun tarjoajan velvollisuus ilmoittaa toimintaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä**  Tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä…Liikenne- ja viestintävirastolle palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä. Ilmoituksessa on kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.  **M72B 11 Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja viestintävirastolle**  **11.1 Merkittävät uhkat tai häiriöt**  Liikenne- ja viestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti ilmoitettavia merkittäviä tunnistuspalvelun häiriöitä ovat tapahtumat, jotka liittyvät sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittäviä ovat myös ennakoimattomat toimivuushäiriöt, joilla on vähäistä suurempia haittavaikutuksia luottamusverkostoon.  **11.2 Ilmoitettavat tiedot**  Liikenne- ja viestintävirastolle tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot:  1) tunnistusväline tai tunnistusvälityspalvelu, johon häiriö tai uhka vaikuttaa;  2) kuvaus häiriöstä tai uhkasta ja sen tiedossa olevista syistä sekä kestosta;  3) kuvaus häiriön tai uhkan vaikutuksista, mukaan lukien vaikutus uusien tunnistusvälineiden myöntämiseen, käyttäjiin, luottaviin osapuoliin, muihin luottamusverkoston toimijoihin ja rajat ylittävään käyttöön;  4) kuvaus korjaustoimenpiteistä; sekä  5) kuvaus häiriöstä tai uhkasta tiedottamisesta luottaville osapuolille, tunnistusvälineiden haltijoille, luottamusverkostolle ja tieto ilmoittamisesta muille viranomaisille.  **11.3 Ilmoitusmenettely**  Ilmoitus merkittävästä häiriöstä tai uhkasta on tehtävä sähköisesti Liikenne- ja viestintäviraston verkkolomakkeella, sähköpostilla tai turvasähköpostilla.  Ilmoituksen tietoja voi täydentää myöhemmin, jos kaikki tiedot eivät ole käytettävissä, kun tehdään ensi-ilmoitus tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti ilman aiheetonta viivästystä.  **MPS72B soveltamisohje ilmoituskynnyksestä Liikenne- ja viestintävirastolle,** kappale 4.11.1 Säännös 11.1:  Määräyksen säännöksessä 11.1 määritellään yleisellä tasolla niitä tekijöitä, jotka ovat olennaisia häiriön tai uhkan merkittävyyden eli ilmoituskynnyksen kannalta. Tällaisia merkittäviä häiriöitä ovat muun muassa:  tunnistusvälineen myöntäminen väärälle henkilölle,  sellaiset sulkulistojen toimivuuteen liittyvät häiriöt, joissa ajantasaista sulkulistaa ei ole saatavilla,  tunkeutuminen palveluntarjoajan järjestelmiin,  tunnistusvälineen tarjoajan varmenteiden allekirjoitusavaimien paljastuminen,  tunnistusvälineiden vakavat väärinkäytökset kuten tapaukset, jotka liittyvät tunnusten ketjuttamiseen,  vakavat sisäiset väärinkäytökset.  Sähköisen henkilöllisyyden virheitä tai väärinkäytöksiä pidetään merkittävinä hyvin matalalla kynnyksellä, samoin esimerkiksi haavoittuvuuksia tai virheitä, jotka vaarantavat tunnistamistiedon oikeellisuuden. Sen sijaan käytettävyys- tai laatuongelmien ilmoituskynnys on lähtökohtaisesti korkeampi ja niiden merkittävyyttä lisää lähinnä se, että ongelma vaikuttaa muihin luottamusverkoston toimijoihin. Tällaisia ongelmia ovat pitkät tunnistusvälineen tai tunnistusvälityspalvelun häiriötilanteet, jotka estävät tunnistuspalveluiden välittämisen asiointipalveluille. Myös ensitunnistamisen ketjuttamisen pitkään estävä häiriö on merkittävä. | A.16.1.2 tietoturvahäiriöiden hallinta/tietoturvahäiriöiden ja parannusten hallinta: tietoturvatapahtumien raportointi | Noudatetaan luottamusverkoston yhdessä määrittelemää dokumenttia ilmoituskynnyksen ylittymisestä. [dokumentti numero]  Vastuut poikkeamatilateisiin ja sidosryhmäviestintään on määritelty |

# Tietojen säilyttäminen ja käsittely

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B 15 Vaatimuksenmukaisuuden arviointikriteerit  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  b) tietojen säilyttämiseen ja käsittelyyn  d) teknisiin toimenpiteisiin  Yleiset vaatimukset  TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet  Tunnistuspalvelun tarjoajan tunnistamiseen liittyvien tietojen säilyttämisen, henkilökunnan ja alihankintana käyttämien palvelujen tulee täyttää sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.4.4 ja 2.4.5 vähintään korotetulle varmuustasolle säädetyt vaatimukset.  […]  Tunnistamispalvelun tarjoajan on lisäksi huolehdittava palvelujensa henkilötietolain 32 §:ssä tarkoitetusta tietojen suojaamisesta sekä riittävästä tietoturvasta.  LoA Liite 2.4.4 Tietojen säilyttäminen   1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt. 2. Järjestelmään kirjatut tiedot säilytetään siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja suojataan niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.   TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset  4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa…2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat  LoA Liite 2.4.6 Tekniset tarkastukset (controls)  1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä. | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | S, H | Tunnistusjärjestelmään ja tunnistamiseen liittyvien **tietojen hallinta on suunnitelmallista** ja perustuu **tietojen luokitteluun.** | **LoA Liite 2.4.4 Tietojen säilyttäminen**  1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt.  **LoA Liite 2.4.6 Tekniset tarkastukset (controls)**  1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.  **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys; | A.8.2.1 suojattavan omaisuuden hallinta/tietojen luokittelu: tiedon luokittelu  A.18.1.4 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen: tietosuoja ja henkilötietojen suojaaminen | Luokittelussa huomioidaan esim. salaustekniset tiedot, tunnistustapahtumatiedot, henkilötiedot, liikesalaisuudet ja järjestelmien turvallisuuteen vaikuttavat tiedot. |
|  | S, H | Tiedonhallinnan suunnittelussa on huomioitu tiedon koko **elinkaari**.  Tietojen **säilytysajat** on määritelty. | **LoA Liite 2.4.4 Tietojen säilyttäminen**  2. Järjestelmään kirjatut tiedot säilytetään siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja suojataan niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.  **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys; | A.18.1.4 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen: tietosuoja ja henkilötietojen suojaaminen | Huomioon on otettava mm. turvallisuuteen liittyvien tapahtumien jäljitettävyys ja tunnistuslain 24 §:ää *vastaavien* käsittelyperusteiden aiheuttamat tarpeet.  Yksityiskohtana ftn\_chain\_level -attribuutin käyttäminen ensitunnistuksen yhteydessä.  Ohjeessa 211/2016 oli seuraavia huomioita, jotka ovat tässä mukana informatiivisina:  Lokeille pitää määritellä säilöntään riittävän pitkä aika jälkikäteen tapahtuvaa selvitystä varten |
|  | S, H | Tunnistuslain **24 §:ssä säädetyistä erityisistä tallennusvelvollisuuksista** on huolehdittu. | **TunnL 24 § Tunnistustapahtumaa ja tunnistusvälinettä koskevien tietojen tallentaminen ja käyttö**  Tunnistuspalvelun tarjoajan on tallennettava:  1) yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot;  2) tiedot 18 §:ssä tarkoitetuista tunnistusvälineen käyttöön liittyvistä estoista ja käyttörajoituksista;  3) varmenteen osalta 19 §:ssä tarkoitetun varmenteen tietosisältö.  Tunnistusvälineen tarjoajan on tallennettava tarvittavat tiedot 17 ja 17 a §:ssä tarkoitetusta hakijan ensitunnistamisesta ja siinä käytetystä asiakirjasta tai sähköisestä tunnistamisesta.  Edellä 1 momentin 1 kohdassa tarkoitetut tiedot on säilytettävä viiden vuoden ajan tunnistustapahtumasta. Muut 1 ja 2 momentissa tarkoitetut tiedot on säilytettävä viiden vuoden ajan vakituisen asiakassuhteen päättymisestä.  Tunnistustapahtuman yhteydessä syntyneet henkilötiedot on hävitettävä tunnistustapahtuman jälkeen, jollei tallentaminen ole välttämätöntä yksittäisen tunnistustapahtuman todentamiseksi.  Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksiensa turvaamista varten riitatilanteissa, väärinkäytöstilanteiden selvittämisessä sekä tunnistuspalvelua käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. Tunnistuspalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsittelijästä.  Jos palveluntarjoaja ainoastaan laskee liikkeelle tunnistusvälineitä:  1) 1 momentin 1 kohtaa ja 4 momenttia ei sovelleta siihen;  2) 3 momentissa tarkoitettu viiden vuoden tallennusaika lasketaan tunnistusvälineen voimassaolon päättymisestä. | A.12.4.1 käyttöturvallisuus: tapahtumien kirjaaminen | "*…ainoastaan laskee liikkeelle tunnistusvälineitä*" tarkoittaa säännöksessä VRK:n varmenteen kaltaista tunnistuspalvelua, jossa tunnistusvälineen myöntäjä ei välitä tunnistussanomia tunnistustapahtumassa |
|  | S, H | Tunnistuslain **24 §:n erityisvaatimus** tallennettavaksi säädettyjen tietojen käsittelyyn liittyvien tietojen tallentamisesta. | **Tunnistustapahtumiin ja tunnistuspalveluun liittyvästä käsittelystä säädetään TunnL 24 §:ssä.**  **TunnL 24 §**  **…**  Tunnistuspalvelun tarjoaja saa käsitellä tallennettuja tietoja ainoastaan palvelun toteuttamiseksi ja ylläpitämiseksi, laskutusta varten, omien oikeuksiensa turvaamista varten riitatilanteissa, väärinkäytöstilanteiden selvittämisessä sekä tunnistuspalvelua käyttävän palveluntarjoajan tai tunnistusvälineen haltijan pyynnöstä. Tunnistuspalvelun tarjoajan on tallennettava tieto käsittelyn ajankohdasta, syystä ja käsittelijästä. | A.12.4.1 käyttöturvallisuus: tapahtumien kirjaaminen  A. A.12.4.3 Pääkäyttäjä- ja operaattorilokit | huomioitava käsittelytietojen jäljitettävyys ja lokien eheyden turvaaminen |
|  | S, H | Tunnistusjärjestelmässä **käsiteltävien ja säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittu teknisillä toimenpiteillä.** | **TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**  4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa…2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat  **LoA Liite 2.4.6 Tekniset tarkastukset (controls)**  1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.  **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;  […]  e) varmuuskopiointi; sekä  f) käytettävä kansainvälisesti tai kansallisesti suositeltuja salausratkaisuja.  **M72B 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset**  **7.1 Tietoliikenteen salausmenetelmät**  7.1.1  Tunnistuspalvelun tarjoajien välisten ja tunnistuspalvelun tarjoajan ja luottavan osapuolen välisten rajapintojen liikenne on salattava. Salauksessa, avaintenvaihdossa, varmenteissa sekä salaukseen liittyvässä allekirjoituksessa on noudatettava seuraavia menetelmiä:   1. Avaintenvaihto: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (finite field) koon tulee olla DHE-menetelmässä vähintään 2048 bittiä ja ECDHE-menetelmässä vähintään 224 bittiä. 2. Allekirjoitus tai epäsymmetrinen salaus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen tai salaukseen avaimen pituuden tulee olla vähintään 2048 bittiä. Käytettäessä elliptisen käyrän menetelmiä ECDSA:ta tai EdDSA:ta äärellisen kunnan koon tulee olla vähintään 224 bittiä. 3. Symmetrinen salaus: Salausalgoritmin on oltava AES, Serpent tai ChaCha20. Avaimen pituuden tulee olla vähintään 128 bittiä. Salausmoodin on oltava CBC, CCM, GCM tai CTR. 4. Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305.   7.1.2  Kohdassa 7.1.1 mainittujen lisäksi voidaan noudattaa menetelmiä ja arvoja, jotka on arvioitu turvallisiksi 1-4 alakohdissa tarkoitettuun käyttöön seuraavien asiakirjojen ajantasaisissa versioissa:   1. Liikenne- ja viestintävirastossa toimivan salaustuotteiden hyväksyntäviranomaisen (Crypto Approval Authority) ohje Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat (Dnro 190/651/2015); tai 2. eräiden Euroopan unionin tai ETA-alueen jäsenvaltioissa toimivien sertifiointielinten välisen SOGIS-MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement) asiakirja SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.   7.1.3  Salausasetukset tulee teknisesti pakottaa edellä lueteltuihin vähimmäistasoihin, jotta yhteyskättelyissä ei päädyttäisi vähimmäistasoja heikompiin asetuksiin.  **7.2 Tietoliikenteen salausprotokolla**  Mikäli yhteyskäytännössä käytetään TLS-protokollaa, tulee käyttää vähintään TLS versiota 1.2. | A.9.1.1 pääsynhallintapolitiikka  A.9.1.2 pääsy verkkoihin ja verkkopalveluihin  A.10.1.1 salauksen käytön periaatteet  A.12.4.2 käyttöturvallisuus: lokitietojen suojaaminen | tiedon salaus ja/tai pääsynhallinta  eriyttäminen tarvittaessa (vrt. erityisesti salaustekninen aineisto)  varmuuskopiointi/palautettavuus  suosituksessa salausvaatimuksille määritelty avaintenvaihto voi olla relevantti tunnistuspalvelun ja sen alihankkijan välillä, vaikka se ei ole relevantti levysalauksessa  luottosuhteen perustana olevien salaisuuksien hallinta ja turvaaminen  Säilyttämisessä täytyy huomioida fyysisen sijoituspaikan eriyttäminen varsinaisesta järjestelmästä. |
|  | H | Tietojen käsittelyssä ja säilyttämisessä noudatetaan **suosituksen** mukaisia tiukennettuja/korkean tason salausvaatimuksia. | **MPS72B kohta 4.7.1.3 (20.5.2022) suositus**  Korkealla varmuustasolla tunnistusjärjestelmässä suositellaan sovellettavaksi määräyksessä säännöksessä 7.1 edellytettyjen korotetun varmuustason vaatimusten sijaan seuraavassa esitettyjä suluissa olevia arvoja, **joilla saavutetaan vähintään 128 bitin vahvuustaso**:  1) **Avaintenvaihto**: Avaintenvaihdossa on käytettävä DHE-menetelmiä tai elliptisiä käyriä käyttäviä ECDHE-menetelmiä. Laskutoimituksissa käytetyn äärellisen kunnan (*finite field*) koon tulee olla DHE-menetelmässä vähintään 2048 (**korkealla varmuustasolla 4096**) bittiä ja ECDHE-menetelmässä vähintään 224 (**korkealla varmuustasolla 256**) bittiä.  IANA:n IKEv2-määritysten mukaiset DH-ryhmät 14 - **21**, 23, 24 ja 26 (korkealla varmuustasolla***16 - 21***) toteuttavat edellä mainitut edellytykset.  2) Allekirjoitus tai epäsymmetrinen salaus: Käytettäessä RSA:ta sähköiseen allekirjoitukseen tai salaukseen, avaimen pituuden tulee olla vähintään 2048 (**korkealla varmuustasolla 3072**) bittiä. Käytettäessä elliptisen käyrän menetelmää ECDSA:ta tai EdDSA:ta, alla olevan kunnan koon tulee olla vähintään 224 (**korkealla varmuustasolla 256**) bittiä.  3) Symmetrinen salaus: Salausalgoritmin on oltava AES, Serpent tai ChaCha20 *(***korkealla varmuustasolla *AES tai Serpent****)*. Avaimen pituuden tulee olla vähintään 128 (**korkealla varmuustasolla 128**)bittiä. Salausmoodin on oltava CBC, CCM, GCM tai CTR.  4) Tiivistefunktiot: Tiivistefunktion tai autentikaatiokoodin on oltava SHA-2, SHA-3, Whirlpool tai Poly1305. SHA-2:lla tarkoitetaan funktioita SHA224, SHA256, SHA384 ja SHA512 (**korkealla varmuustasolla *SHA-3-256, SHA-3-384, SHA-3-512***) | ks. yllä | avaintenvaihto voi olla relevantti tunnistuspalvelun ja sen alihankkijan välillä |
|  | S, H | Kaikki **laitteet ja välineet**, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla. | **LoA Liite 2.4.6 Tekniset tarkastukset** (controls)  5) Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.  **M72B 5.4 Käyttöturvallisuus**  Tunnistusjärjestelmän operoinnissa on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä:  […]  b) tiedon luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys;  […] | A.8.3 Suojattava omaisuus/tietovälineiden käsittely  A.11.2.6 toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus  A.11.2.7 laitteiden turvallinen käytöstä poistaminen ja kierrättäminen | hallinta, hävittäminen, siirtäminen |

# Tilaturvallisuus

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B 15 Vaatimuksenmukaisuuden arviointikriteerit  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  c) tiloihin ja […]  TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset  4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että […] tunnistuspalvelun tarjoamiseen käytettävät tilat ovat turvallisia sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.4.5 säädetyllä tavalla; | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | S, H | **Tilaturvallisuus**  Tunnistusjärjestelmän tilat on jaettu turvavyöhykkeisiin käsiteltävän tiedon luottamuksellisuus ja kriittisyys huomioiden. | **LoA Liite 2.4.5 Tilat ja henkilökunta**  3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.  4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että pääsy alueille, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita. | A.11.1 fyysinen turvallisuus ja ympäristön turvallisuus/turva-alueet:  A.11.1.1 fyysinen turva-alue | Kaikki tunnistuspalvelun tuotantoon liittyvät/vaikuttavat tilat, myös alihankkijat  Mahdollinen Katakrin täyttäminen oletusarvoisesti riittävä, jos tunnistusjärjestelmän tuottaminen ko. tiloissa. Muiden standardien kattavuutta ei ole selvitetty. |
|  | S, H | Tunnistuspalvelun tuotannossa käytettävät laitteistot **on suojattu** murtoa, ilkivaltaa, paLoA, lämpöä, kaasuja, pölyä, tärinää, vettä ja sähkönkäytön katkoksia vastaan. Suojauksen vahvuudessa on huomioitu turvavyöhykkeet.  Tiloissa on toteutettu tarkoituksenmukainen **kulunvalvonta**/pääsynvalvonta jolla varmistutaan siitä, että vain asianomaisilla henkilöillä on pääsy.  Tietojen fyysiseen suojaamiseen tarkoitetut turvallisuusjärjestelmät ja laitteet ovat yleisesti käytettyjen teknisten standardien tai vähimmäisvaatimusten mukaisia. | **LoA Liite 2.4.5 Tilat ja henkilökunta**  3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.  4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että pääsy alueille, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita. | A.11.1.2 kulunvalvonta    A.11.1.3 toimistojen, tilojen ja laitteistojen suojaus,  A.11.1.4 suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastan  A.11.2.1 laitteiden sijoitus ja suojaus  A.11.2.3 kaapeloinnin turvallisuus |  |
|  | S, H | Turvavyöhykkeillä huolehditaan siitä, ettei niillä ole **asiaankuulumattomia** laitteita tai yhteyksiä. | **LoA Liite 2.4.5 Tilat ja henkilökunta**  3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.  4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että pääsy alueille, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita. | A.11. fyysinen turvallisuus ja ympäristön turvallisuus |  |

# Riittävät ja pätevät henkilöresurssit

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B 15 Vaatimuksenmukaisuuden arviointikriteerit  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  c) […] ja henkilökuntaan | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | S, H | **Henkilökunnan riittävyys ja pätevyys**  Tunnistuspalvelun tuotanto-organisaatiolla on käytössään riittävä asiantuntemus ja henkilöstöresurssit tietoturvallisuuden ja tietosuojan varmistamiseksi. | **TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet**  Tunnistuspalvelun tarjoajan tunnistamiseen liittyvien … henkilökunnan ja alihankintana käyttämien palvelujen tulee täyttää sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa …ja 2.4.5 vähintään korotetulle varmuustasolle säädetyt vaatimukset.  **LoA Liite 2.4.5 Tilat ja henkilökunta**  Vaatimukset, jotka koskevat tiloja ja henkilöstöä sekä tarvittaessa alihankkijoita, jotka suorittavat tämän asetuksen soveltamisalaan kuuluvia tehtäviä. Kunkin vaatimuksen noudattaminen on suhteutettava siihen, minkä tasoinen riski tarjottavaan varmuustasoon liittyy.  1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä.  2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti. | A.7.2.2 Henkilöstöturvallisuus/työsuhteen aikana: Tietoturvatietoisuus, -opastus ja -koulutus | Arviointi  - henkilöresurssien riittävyys toiminnan luonteeseen nähden (24/7/365)  - tekniset valvontajärjestelyt huomioidaan, ei tarkkoja vaatimuksia henkilöstömäärälle tai päivystykselle  - tarpeellisten osa-alueiden osaamisesta (tekninen, oikeudellinen mm. henkilötietojen käsittelyn takia) |
|  | S, H | Tunnistusjärjestelmään alihankitut palvelut ja toiminnot on tunnistettu ja dokumentoitu.  Alihankkijoiden henkilöstöresurssien pätevyys ja riittävyys on varmistettu. | **ks. ed. rivi** | ks. ed. rivi  A.15.1.1 Toimittajasuhteiden tietoturvapolitiikka  A.15.2.1 toimittajien palvelujen seuranta ja katselmointi | Tiedot tunnistusjärjestelmän alihankkijoista (toimistojärjestelmät, käyttöpalvelut, ohjelmistot, infra…) ja vähintään yleisellä tasolla arvio näiden henkilöresursseista. |

# Tietoturvallisuuden hallinta

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M72B 15 Vaatimuksenmukaisuuden arviointikriteerit  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  a) tietoturvallisuuden hallintaan  M72B 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä  4.1 Tietoturvallisuuden hallinnan standardi  Tunnistuspalveluntarjoajan on noudatettava tunnistusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään.  4.2 Tietoturvallisuuden hallinnan kattavuus  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;  2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;  3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;  4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;  5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja  6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.  TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset  Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:  5) tietoturvallisuuden hallinnasta on huolehdittu siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.4 johdanto-osassa ja kohdissa 2.4.3 ja 2.4.7 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät.  LoA Liite 2.4 Hallinto ja organisointi  Kaikilla osallistujilla, jotka tarjoavat sähköiseen tunnistamiseen liittyvää rajat ylittävää palvelua (jäljempänä tässä liitteessä ”palveluntarjoajat”), on oltava käytössä dokumentoidut tietoturvallisuuden hallintakäytännöt, toimintaperiaatteet, lähestymistavat riskien hallintaan ja muut hyväksytyt turvatoimenpiteet siten, että asiaankuuluvilla sähköisen tunnistamisen järjestelmien hallintoelimillä on kyseeseen tulevissa jäsenvaltioissa varmuus siitä, että tehokkaat menettelyt ovat käytössä. Kaikki 2.4 jakson vaatimukset/osatekijät on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.  LoA Liite 1. Sovellettavat määritelmät  4. 'tietoturvallisuuden hallintajärjestelmällä' tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen liittyvät riskit hyväksyttävällä tasolla.  LoA Liite 2.4.7 Noudattaminen ja tarkastus  Määräajoin tehdään riippumattomia sisäisiä tai ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen. | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDIVIITTAUS** | **HUOMIOITA** |
|  | S, H | Tunnistuspalvelun tarjoajalla on käytössä tehokas **tietoturvallisuuden hallintajärjestelmä** tunnistusjärjestelmän (ml. organisatoriset ja tekniset toimet) tunnistuspalvelun toiminnan tietoturvaan liittyvien riskien hallintaa ja valvontaa varten. | **LoA Liite 2.4.3 Tietoturvallisuuden hallinta**  Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.  Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten. | A.5 tietoturvapolitiikat | ISO 27001 noudattaminen ilman merkittäviä poikkeamia osoittaa tietoturvallisuuden hallinnan vaatimuksen täyttämisen. |
|  | S, H | Tietoturvallisuuden hallintajärjestelmä perustuu yleisesti tunnettuun standardiin tai standardeihin | **M72B 4 Tunnistuspalvelun tarjoajan tietoturvallisuuden hallintajärjestelmä**  **4.1 Tietoturvallisuuden hallinnan standardi**  Tunnistuspalveluntarjoajan on noudatettava tunnistusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään. |  |  |
|  | S, H | Tietoturvallisuuden hallintajärjestelmä kattaa tunnistusjärjestelmään vaikuttavat olennaiset sisäiset ja ulkoiset tekniset, oikeudelliset ja hallinnolliset vaatimukset ja tarpeet. | **M72B 4.2 Tietoturvallisuuden hallinnan kattavuus**  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;  2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;  […] | 4 organisaation toimintaympäristö | Tunnistuspalvelussa tulee mm. noudattaa ajantasaisia lainsäädäntöjä ja määräyksiä, kuten tunnistus- ja luottamuspalvelulakia, määräystä 72 ja yleistä tietosuoja-asetusta. |
|  | S, H | Tietoturvallisuuden hallintajärjestelmä kattaa hallinnan johtamisen, organisoinnin ja ylläpidon.  Käytössä on ajantasainen ja johdon hyväksymä **tietoturvapolitiikka**. Turvallisuusperiaatteet ja politiikat ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset.    Henkilökunnan ja alihankkijoiden tietoturvallisuuteen liittyvät vastuut on kuvattu. | **M72B 4.2 Tietoturvallisuuden hallinnan kattavuus**  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  […]  2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;  […]  4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;  […] | 5 johtajuus  9.2 sisäinen auditointi  9.3 johdon katselmus  10 hallintajärjestelmän parantaminen  A.5.1.1 Tietoturvapolitiikat  A.6.1.1 Tietoturvaroolit ja -vastuut  A.15.1.1 toimittajasuhteiden tietoturvapolitiikka |  |
|  | S, H | Tietoturvallisuuden hallintajärjestelmä kattaa tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinnan.  Riskienhallinta on säännöllinen ja jatkuva, dokumentoitu prosessi.  Tunnistetut riskit luokitellaan ja priorisoidaan.  Riskienhallintaprosessi tunnistaa tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat riskit.  Riskienhallintaprosessia ja sen tuloksia hyödynnetään tunnistuspalvelun/tunnistusjärjestelmän turvatoimien suunnittelussa. | **M72B 4.2 Tietoturvallisuuden hallinnan kattavuus**  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  […]  3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;  […] | MPS72 viittaus:  6 suunnittelu  8 Toiminta |  |
|  | S, H | Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden resursoinnin, pätevyysvaatimukset, henkilöstön tietoisuuden tietoturvallisuudesta, viestinnän ja dokumentoinnin sekä dokumentoidun tiedon hallinnan.  Ajantasaiset tietoturvaohjeet ja käytännöt ovat kaikkien sähköisen tunnistamisen tehtäviin osallistuvien saatavilla ja tiedossa  Henkilöstön turvallisuuskoulutus on säännöllistä ja dokumentoitua. Koulutuksen tehokkuutta seurataan | **M72B 4.2 Tietoturvallisuuden hallinnan kattavuus**  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  […]  4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;  […] | MPS72:  7 tukitoiminnot |  |
|  | S, H | Tietoturvallisuuden hallintajärjestelmässä huolehditaan tunnistuspalvelun tarjonnan suunnittelusta ja ohjauksesta siten, että tunnistuspalvelulle säädetyt tietoturvavaatimukset täyttyvät. | **M72B 4.2 Tietoturvallisuuden hallinnan kattavuus**  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  […]  5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja  […] | MPS72: 8 toiminta  A.18.1.1 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen: sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen | tunnistuspalvelulle säädetyt vaatimukset  soveltuvin osin tietosuojasääntely  soveltuvin osin luottamusverkoston sopimussääntely |
|  | S, H | Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden säännöllisen arvioinnin. | **M72B 4.2 Tietoturvallisuuden hallinnan kattavuus**  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  […]  6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi. | MPS72:  9.1 seuranta, mittaus, analysointi, arviointi | Miten hyvin tietoturvallisuuden hallinta tehoaa/vaikuttaa niihin tekijöihin, prosesseihin ja ongelmiin, jotka vaikuttavat tunnistusjärjestelmän tietoturvallisuuteen |

# Tunnistusvälineen hakijan henkilöllisyyden todistaminen ja varmentaminen (ensitunnistaminen)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **M72B 15 Vaatimuksenmukaisuuden arviointikriteerit**  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  2) tunnistusmenetelmään eli tunnistusvälineen  b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen  **TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset**  Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:  1) tunnistusmenetelmän perustana on 17 ja 17 a §:n mukainen tunnistaminen, jota koskevat tiedot ovat jälkikäteen 24 §:n mukaisesti tarkastettavissa;  2) tunnistusmenetelmällä voidaan yksiselitteisesti tunnistaa tunnistusvälineen haltija siten, että teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti annetussa komission täytäntöönpanoasetuksen (EU) 2015/1502, jäljempänä *sähköisen tunnistamisen varmuustasoasetus*, liitteen kohdissa 2.1.2, 2.1.3 ja 2.1.4 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät;  […]  **TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen**  Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. Lisäksi henkilöllisyyden varmentaminen voi perustua julkisen tai yksityisen tahon aiemmin muuhun tarkoitukseen kuin vahvan sähköisen tunnistusvälineen myöntämiseen käyttämään menettelyyn, jonka Liikenne- ja viestintävirasto hyväksyy menettelyä koskevien säännösten ja viranomaisvalvonnan perusteella tai 28 §:n 1 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella.  Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia.  Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen tekee poliisi.[…]  **LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  **OIKEUSHENKILÖ**  **Oikeushenkilön tunnistusvälineen myöntämistä koskevia vaatimuksia ei käsitellä tarkemmin tässä kriteeristössä. Jos tunnistuspalvelun tarjoaja ryhtyy tarjoamaan vahvoja tunnistusvälineitä oikeushenkilöille, arvioinnissa on huomioitava tätä koskevat säännökset.**  **TunnL 17 a § Tunnistusvälineen hakijana olevan oikeushenkilön tunnistaminen**  Oikeushenkilön ilmoitettu henkilöllisyys tulee varmentaa yritys- ja yhteisörekistereistä tai siten, että vähintään oikeushenkilön henkilöllisyyden todistamista ja varmentamista koskevat sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.3 korotetulle varmuustasolle säädetyt vaatimukset täyttyvät.  **TunnL 7 a § yritys- ja yhteisörekisterien tietojen käyttäminen**  Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä oikeushenkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot yritys- ja yhteisörekistereistä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla yritys- ja yhteisörekisterien tietojen kanssa.  **LoA Liite 2.1.3 Henkilöllisyyden todistaminen ja varmentaminen (oikeushenkilö)**  **LoA Liite 2.1.4 Luonnollisten ja oikeushenkilöiden sähköisen tunnistamisen menetelmien välinen kytkös**  **MÄÄRITELMÄT**  **TunnL 2 § Määritelmät**  7) ensitunnistamisella tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä;  **LoA Liite 1. Sovellettavat määritelmät**   1. ’luotettavalla lähteellä’ tarkoitetaan mitä tahansa sellaista lähdettä muodosta riippumatta, josta voidaan luotettavasti saada paikkansapitäviä tietoja ja/tai todisteita, joita voidaan käyttää henkilöllisyyden todistamiseen;   Standardi: ETSI TS 119 461 | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖS** | **STANDARDI** | **HUOMIOITA** |
| **Tapa 1: Ensitunnistus perustuu Suomessa hyväksytyn henkilöllisyystodistuksen esittämiseen** | | | | | |
|  | S, H | Henkilöllisyyden todistaminen perustuu tunnistuslaissa hyväksyttyihin henkilöllisyystodistuksiin.  Muiden kuin laissa lueteltujen valtioiden myöntämien henkilöllisyystodistuksen hyväksyminen on selkeästi määritelty. | **TunnL 17 §**  Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia. |  | Jos käytössä on henkilöllisyystodistuksiin perustuva ensitunnistaminen |
|  | S, H | Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan **paikan päällä**.  Henkilöstö tuntee henkilöllisyystodistusten aitoustekijät ja pystyy tarkistamaan ne.  Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma. | **TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen**  Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen.  **LoA Liite 1 2.1.2**  1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;  tai  2. henkilöllisyystodistus esitetään rekisteröintiprosessin aikana siinä jäsenvaltiossa, jossa todistus on myönnetty, ja todistus näyttää liittyvän sen esittäneeseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; |  | Jos käytössä on etätunnistusratkaisu, kts. Kriteerit kohdassa "Tapa 5". |
|  | S | Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan **etäyhteydellä**.  Henkilöstö tuntee henkilöllisyystodistusten aitoustekijät ja pystyy tarkistamaan ne.  Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma.  Etäyhteyden luotettavuusvaatimuksissa huomioidaan korotetun tason hyökkäyspotentiaali. | **TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen**  Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen.  **LoA Liite 1 2.1.2**  1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;  tai  2. henkilöllisyystodistus esitetään rekisteröintiprosessin aikana siinä jäsenvaltiossa, jossa todistus on myönnetty, ja todistus näyttää liittyvän sen esittäneeseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; |  | ks. tämän ohjeen kohta 3.9 |
|  | H | Henkilöllisyystodistus esitetään ja sen aitous tarkistetaan etäyhteydellä.  Henkilöllisyystodistuksen aitous tarkistetaan sen myöntäjän sähköisen allekirjoituksen perusteella henkilöllisyystodistuksen sirulta.  Varmistetaan, että henkilöllisyystodistus on sen esittävän henkilön oma vertaamalla esittäneen henkilön ominaisuuksia henkilöllisyystodistuksesta saatuun sähköisesti allekirjoitettuun vertailutietoon.  Etäyhteyden luotettavuusvaatimuksissa huomioidaan korkean tason hyökkäyspotentiaali. | **LoA Liite 2.1.2 korkea**  1.a) Jos henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä valokuva tai biometrinen tunniste, jossa sähköisen tunnistamisen menetelmää haetaan, ja kyseinen todiste edustaa ilmoitettua henkilöllisyyttä, todiste tarkistetaan sen määrittämiseksi, onko se luotettavan lähteen mukaan voimassa;  ja  hakijalla todetaan olevan ilmoitettu henkilöllisyys vertaamalla yhtä tai useampaa henkilön fyysistä ominaisuutta luotettavaan lähteeseen; |  | ks. tämän ohjeen kohta 3.9 |
|  | S, H | Tieto passin tai henkilökortin voimassaolosta tarkistetaan käytettävissä olevista poliisin tietojärjestelmästä tai kansainvälisistä luotettavista lähteistä. | **LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  Menettelyt 1 ja 2, osavaatimus  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;  **TunnL 7 b § Tieto passin tai henkilökortin voimassaolosta**  Tunnistuspalvelun tarjoajalla on oikeus saada salassapitosäännösten estämättä rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta. |  | Ei pakolliseksi säädetty vaatimus, mutta vaikuttaa riskiarviointiin ja voi vaikuttaa korvausvastuuseen.  Korkealla varmuustasolla välttämätön. |
|  | S, H | Henkilön olemassaolo tarkistetaan väestötietojärjestelmästä | **TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen**  Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa. |  | Koskee kaikkia ensitunnistusmenettelyjä. |
| **Tapa 2: Ensitunnistus sähköisellä tunnistusvälineellä** | | | | | |
|  | S | Henkilöllisyyden todistaminen perustuu tunnistuslaissa hyväksyttyihin vahvoihin sähköisiin tunnistusvälineisiin. | **TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen**  Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen.  **LoA Liite 2.1.2**  4. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korotettu” tai ”korkea”, ja ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista, henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason ”korotettu” tai ”korkea” on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama. |  | Jos käytössä on vahvaan sähköiseen tunnistamiseen perustuva ensitunnistaminen.  Tunnistuslain mukaisesti hyväksytyt korotetun varmuustason tunnistusvälineet ovat Liikenne- ja viestintäviraston rekisterissä. |
|  | H | Henkilöllisyyden todistaminen perustuu tunnistuslaissa hyväksyttyihin vahvoihin sähköisiin tunnistusvälineisiin.  Korkean varmuustason tunnistusvälineen myöntäminen sähköisen tunnistuksen perusteella on mahdollista vain korkean varmuustason välineellä. | **LoA Liite 2.1.2 korkea**  3. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korkea”, henkilöllisyyden todistamis- ja varmentamismenettelyjä ei tarvitse toistaa. Jos perustana olevaa sähköisen tunnistamisen menetelmää ei ole ilmoitettu, varmuustason ”korkea” on oltava asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen tai vastaavan elimen vahvistama  ja  on ryhdytty toimiin sen osoittamiseksi, että sen menettelyn tulokset, jossa ilmoitettu sähköisen tunnistamisen menetelmä aiemmin myönnettiin, ovat edelleen voimassa. |  | Jos käytössä on vahvaan sähköiseen tunnistamiseen perustuva ensitunnistaminen.  Tunnistuslain mukaisesti hyväksytyt korkean varmuustason tunnistusvälineet ovat Liikenne- ja viestintäviraston rekisterissä. |
| **Tapa 3: Ensitunnistus muuhun tarkoitukseen tehdyn tunnistamisen perusteella ("aikaisempi asiakkuus")** | | | | | |
|  | S, H | Henkilöllisyyden varmentamisessa luotetaan menettelyyn, jolla henkilöllisyys on todistettu ja varmennettu aikaisemmin muuta kuin vahvan sähköisen tunnistusvälineen myöntämistä varten.  Menettely perustuu muuhun sääntelyyn kuin tunnistuslakiin tai eIDAS-asetukseen ja sitä valvoo viranomainen.  Menettely tarjoaa vastaavan varmuuden kuin tunnistussääntelyn mukainen henkilöllisyystodistuksen esittämiseen perustuva tai sähköisellä tunnistusmenetelmällä tunnistamiseen perustuva menettely. | **TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen**  Ensitunnistamisessa luonnollisen henkilön tunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.1.2 korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Henkilön henkilöllisyyden varmentaminen voi perustua viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan tai tässä laissa tarkoitettuun vahvaan sähköiseen tunnistusvälineeseen. Lisäksi henkilöllisyyden varmentaminen voi perustua julkisen tai yksityisen tahon aiemmin muuhun tarkoitukseen kuin vahvan sähköisen tunnistusvälineen myöntämiseen käyttämään menettelyyn, jonka Liikenne- ja viestintävirasto hyväksyy menettelyä koskevien säännösten ja viranomaisvalvonnan perusteella tai 28 §:n 1 kohdassa tarkoitetun vaatimustenmukaisuuden arviointilaitoksen vahvistuksen perusteella.  **LoA Liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  3. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.2. kohdassa esitetyt menettelyt varmuustasolla ”korotettu”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 (1) 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin; |  | Tämän kohdan mukaisen ensitunnistusmenettelyn käyttö edellyttää Liikenne- ja viestintäviraston nimenomaista vahvistusta. Menettelyä koskevaan ilmoitukseen täytyy liittää arviointi vaatimustenmukaisuudesta. |
| **Tapa 4: Poliisin tekemä ensitunnistus** | | | | | |
|  | S, H | Ensitunnistamisen tekee tarvittaessa poliisi. | **TunnL 17 §**  Jos tunnistusvälineen hakijan henkilöllisyyttä ei voida luotettavasti todentaa, hakemukseen liittyvän ensitunnistamisen tekee poliisi.  **LoA Liite 2.1.2 korkea**  3. Jos hakija ei esitä valokuvaa tai biometristä tunnistetta, sovelletaan samoja menettelyjä, joita tällaisen hyväksytyn valokuvan tai biometrisen todisteen saamiseksi käytetään kansallisella tasolla rekisteröinnistä vastaavan tahon jäsenvaltiossa. |  |  |
| **Tapa 5: Etäensitunnistus** | | | | | |
|  | S | Etäensitunnistuksen ratkaisu tulee perustua riskiarvioon (Level of Identity Proofing, LoIP) | **Viittaus (LoA, Guidance, M72B)**  esim. TunnL 8 § Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset  **M72B 6.1 Tunnistusmenetelmän ominaispiirteet ja suojautumiskyky**  6.1.1  Tunnistusmenetelmän todentamistekijät, todentamismekanismi ja turvatoimenpiteet on suunniteltava, toteutettava ja ylläpidettävä siten, että ne suojaavat tunnistusmenetelmän eheyden ja luottamuksellisuuden. Tunnistusmenetelmällä on oltava suojautumiskyky vähintään tunnistuspalvelun varmuustason mukaista sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua kohtuullisen tai korkean vakavuustason uhkaa ja hyökkäyspotentiaalia vastaan.  Suojautumiskyvyn on perustuttava riskiarvioon, jossa arvioidaan erikseen hallussapitoon, tietoon ja ominaisuuteen perustuviin todentamistekijöihin ja todentamismekanismiin kohdistuvat uhkat sekä uhkilta suojaavat turvatoimenpiteet.  **LoA liite 2.4.3 Tietoturvallisuuden hallinta**  Matala:  Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.  Korotettu:  Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten. | ETSI TS 119 461  ISO/IEC TS 29003:2018 | Hyökkäyspotentiaali (korotettu/korkea) ja sen selvittäminen, määritellyt kriteerit mitkä tulee täyttyä, jotta myöntöprosessi voidaan viedä loppuun, toimitusketjun turvallisuus, jos käytetään palveluntarjoajaa, perustuuko kuvalliseen (selfie) vai videomateriaalin tarkasteluun, kriteerit, joiden täyttyessä siirrytään automaattisesta prosessista manuaaliseen prosessiin. |
|  | S | Asiakkaan tiedottaminen ehdoista ja edellytyksistä | **TunnL 20 § Tunnistusvälineen myöntäminen**  Tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä kirjallisesti. Sopimus voidaan tehdä myös sähköisesti, jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla. Tunnistuspalvelun tarjoajan tulee kohdella asiakkaitaan syrjimättä ja tunnistusvälineiden hakijoita tasapuolisesti sopimuksen tekemisen yhteydessä.  […]  **TunnL 23 § Tunnistusvälineen haltijan velvollisuudet**  Tunnistusvälineen haltijan on käytettävä tunnistusvälinettä sopimuksen ehtojen mukaisesti. Haltijan on säilytettävä tunnistusvälinettä huolellisesti. Haltijan velvollisuus huolehtia tunnistusvälineestä alkaa, kun hän on vastaanottanut sen.  Tunnistusvälineen haltija ei saa luovuttaa välinettä toisen käyttöön.  **LoA 2.1.1. Hakemus ja rekisteröinti**  1.Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmien käyttöön liittyvistä ehdoista ja edellytyksistä.  2.Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmiin liittyvistä suositelluista varotoimista.  […] |  |  |
|  | S | Hyväksytyt ensitunnistusasiakirjat ja niiden voimassaolon tarkistus | **TunnL 17 § Tunnistusvälineen hakijana olevan luonnollisen henkilön tunnistaminen**  […]  Ensitunnistamisessa, joka perustuu yksinomaan viranomaisen myöntämään henkilöllisyyttä osoittavaan asiakirjaan, hyväksyttäviä asiakirjoja ovat voimassa oleva Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä passi tai henkilökortti. Halutessaan tunnistusvälineen tarjoaja voi käyttää henkilöllisyyden varmentamisessa myös muun valtion viranomaisen myöntämää voimassa olevaa passia.  […]  **TunnL 7 b § Tieto passin tai henkilökortin voimassaolosta**  Tunnistuspalvelun tarjoajalla on oikeus saada salassapitosäännösten estämättä rajapinnan kautta tai muutoin sähköisesti poliisin tietojärjestelmässä oleva tieto ensitunnistamisessa käytettävän passin tai henkilökortin voimassaolosta.  **LoA 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  Matala:  1.Henkilöllä voidaan olettaa olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan.  2. Todisteen voidaan olettaa olevan aito tai luotettavan lähteen mukaan olemassa oleva, ja se näyttää olevan voimassa.  3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.  Korotettu:  Lisäksi vähintään 1 kpl kohdasta korotettu, esim.  1.Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; |  | Tällä hetkellä käytännössä passi, mahdollisesti myös henkilökortti. Ensitunnistusasiakirjan voimassaolo on tarkistettava poliisin rajapintaa tai muuta kansainvälisesti luotettua rajapintaa vasten (Interpol). |
|  | S | Henkilön olemassaolo tarkistetaan väestötietojärjestelmästä | **TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen**  Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa.  **LoA 2.1.2** **Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  Matala:  3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys. |  | Koskee kaikkia ensitunnistusmenettelyjä. |
|  | S | Etäensitunnistusta tekevä sovellus ja ulkopuoliset ratkaisut tai komponentit tulee arvioida tai niiden pitää olla arvioituja | **TunnL 29 § Sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointi**  Tunnistuspalvelun tarjoajan on määräajoin teetettävä palvelulleen 28 §:ssä mainitun arviointielimen arviointi siitä, täyttääkö tunnistuspalvelu tässä laissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset.  […]  **M72B 4.2 Tietoturvallisuuden hallinnan kattavuus**  Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet:  1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;  2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;  3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;  4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;  5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja  6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.  **M72B 15 Vaatimuksenmukaisuuden arviointikriteerit**  15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot  Tunnistuspalvelun tunnistus- ja luottamuspalvelulain 29 §:n mukaisen arvioinnin täytyy kattaa kaikki laissa ja tässä määräyksessä asetetut vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  a) tietoturvallisuuden hallintaan;  b) tietojen säilyttämiseen ja käsittelyyn;  c) tiloihin ja henkilökuntaan;  d) teknisiin toimenpiteisiin; ja  […]  2) tunnistusmenetelmään eli tunnistusvälineen:  a) hakemiseen ja rekisteröintiin;  b) hakijan henkilöllisyyden todistamiseen ja varmentamiseen;  […]  d) myöntämiseen, toimittamiseen ja aktivointiin;  e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin;  f) uusimiseen ja korvaamiseen; ja  g) todentamismekanismeihin.  **LoA 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  Korotettu:  1.Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; | ETSI TS 119 461  ISO/IEC TS 29003:2018  ISO/IEC 30107 | Arviointilaitoksen tekemä arviointi, FAR-arvo, mihin testidataan FAR perustuu, vastaavuus hyökkäyspotentiaaliin (korotettu/korkea). PAD-kyvykkyys (Presentation Attack Detection). FRR ei oleellinen. Sovellus tulee myös arvioida tai muuten todentaa turvallisuus Liite C:n mukaisella tai muulla vastaavalla menettelyllä |
|  | S | Varmistetaan esitetyn dokumentin aitous ja tietojen muuttumattomuus. Ensitunnistuksessa käytettävän dokumentin aktiivinen ja passiivinen todennus, dokumentin tarkastelu videoyhteyden yli (MRZ, visuaaliset turvatekijät) | **LoA liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  Matala:  2. Todisteen voidaan olettaa olevan aito tai luotettavan lähteen mukaan olemassa oleva, ja se näyttää olevan voimassa.  Korotettu:  1.  […]  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  […] |  | Ensitunnistusdokumentin (passi, henkilökortti) aitous ja sirulle tallennettu tiedon aitous on tarkistettava |
|  | S | Etätunnistustapahtuma ja henkilön todennus videoyhteyden yli suoritetaan olosuhteissa, joiden vähimmäisvaatimukset on määritelty. | **LoA liite 2.1.2**  Korotettu:  1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; |  | Etäensitunnistustapahtuma suoritetaan sellaisessa tilanteessa tai olosuhteissa, joissa pystytään maksimoimaan automaattisten turvakontrollien toteutuminen. |
|  | S | Etäensitunnistuksen biometriikkaa analysoivat automaattiset turvakontrollit ovat sattumanvaraisia | **LoA liite 2.1.2**  Matala:  3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.  Korotettu:  1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; |  | Toiminnalla pyritään estämään esim. ennalta valmisteltujen videosyötteiden luominen |
|  | S | Etäensitunnistustapahtumalle on määritelty tekniset vähimmäisvaatimukset, joiden alittuessa etäensitunnistusta ei voida suorittaa | **LoA liite 2.1.2**  Matala:  3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.  Korotettu:  […]  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; |  | Esim. laitteistotason vähimmäisvaatimukset, tietoliikenneyhteyden katkottomuus ja nopeus, resoluutio, kameran kyvykkyydet, artefaktien esiintyminen, Liite C:n resilienssikriteerit |
|  | S | Tietojen siirtäminen, tallennus | **LoA liite 2.4.4 Tietojen säilyttäminen**  1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt.  2. Järjestelmään kirjatut tiedot säilytetään siltä osin kuin tämä on kansallisen lainsäädännön tai muun kansallisen hallinnollisen järjestelyn mukaan sallittua ja suojataan niin kauan kuin niitä tarvitaan tarkastuksia ja tietoturvaloukkausten tutkimista varten ja säilytetään siihen asti, kun tiedot hävitetään turvallisesti.  **myös M72B 7 Tunnistusjärjestelmän rajapintojen salausvaatimukset** |  | Tietosuoja, varsinkin jos tietoa siirtyy EU-alueen ulkopuolelle. Tallennus myöhäisempää tarkastelua varten jos esim. havaitaan väärinkäytös. |
|  | S | Etäensitunnistuksen suorittava ohjelmistokomponentti tulee olla todennettu | **TunnL 13 § Tunnistuspalvelun tarjoajan yleiset velvollisuudet**  […]  Tunnistuspalvelun tarjoaja vastaa apunaan käyttämiensä henkilöiden tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.  **LoA liite 2.4.6 Tekniset tarkastukset**  1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.  2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.  […]  **15 Vaatimuksenmukaisuuden arviointikriteerit**  **15.1 Tunnistusjärjestelmän ja tunnistusmenetelmän arvioitavat toiminnot**  Tunnistuspalvelun tunnistus- ja luottamuspalvelulain 29 §:n mukaisen arvioinnin täytyy kattaa kaikki laissa ja tässä määräyksessä asetetut vaatimukset, jotka kohdistuvat:  1) tunnistuspalvelun tarjoamiseen vaikuttavien toimintojen (tunnistusjärjestelmän):  a) tietoturvallisuuden hallintaan; |  | Käytännössä mobiilisovellus ja sovelluksen attestaatio taustajärjestelmälle |
|  | S | Etätunnistuksen on perustuttava ainakin osaltaan automatisoituihin prosesseihin | **LoA liite 2.4.6 Tekniset tarkastukset**  4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin. |  | Pelkän virkailijan käyttö etäensitunnistamisessa ei ole riittävää, vaan prosessin on perustuttava ainakin osittain tietokoneella tehtyyn vertailuun edellä olevien kriteerien kohdalla |
|  | S | Etätunnistusprosessiin osallistuvien työntekijöiden tulee olla koulutettuja | **LoA liite 2.4.5 Tilat ja henkilökunta**  1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä.  2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti. |  | Jos etäensitunnistusprosessissa päätöksentekoon osallistuu myös työntekijä, tulee hänet kouluttaa riittävällä tasolla arvioimaan mahdollisen videomateriaalin aitoutta, ensitunnistusdokumentin aitoustekijöitä |

# Tunnistusvälineen eli tunnistusmenetelmän elinkaari

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **M72B 15 Vaatimuksenmukaisuuden arviointikriteerit**  Tunnistuspalvelun arvioinnin täytyy kattaa vaatimukset, jotka kohdistuvat:  2) tunnistusmenetelmään eli tunnistusvälineen  a) hakemiseen ja rekisteröintiin  b) […]  c) […]  d) myöntämiseen, toimittamiseen ja aktivointiin  e) voimassaolon keskeyttämiseen, peruuttamiseen ja uudelleen aktivointiin  f) uusimiseen ja korvaamiseen  g) […] | | | | | |
| **NRO** | **VARMUUSTASO** | **TUNNISTUSPALVELUN VAATIMUKSEN TIIVISTELMÄ** | **SÄÄNNÖKSET** | **STANDARDI** | **HUOMIOITA** |
|  | S, H | Tunnistusvälinettä ei liitetä henkilöön eli personoida ennen ensitunnistamista. Tunnistusmenetelmän tekijät kytketään tunnistusmenetelmän haltijaan. | **M72B 6.3 Tunnistusvälineen kytkeminen henkilöön**  6.3.1  Tunnistusmenetelmän todentamistekijät on kytkettävä tunnistusjärjestelmässä tunnistusvälineen haltijaan.  6.3.2  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. |  |  |
|  | S, H | Luonnollisen henkilön henkilötiedot tarkistetaan väestötietojärjestelmästä tunnistusvälinettä myönnettäessä ja säännöllisesti tunnistusvälineen voimassaolon aikana. | **TunnL 7 § Väestötietojärjestelmän tietojen käyttäminen**  Tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan on hankittava ja päivitettävä luonnollisen henkilön tunnistuspalvelun tarjoamiseksi tarvitsemansa tiedot väestötietojärjestelmästä. Tämän lisäksi tunnistuspalvelun tarjoajan on varmistettava, että sen tunnistuspalvelun tarjoamiseksi tarvitsemat tiedot ovat ajan tasalla väestötietojärjestelmän tietojen kanssa.  […]  **Ks. M72B 12 Luottamusverkostossa välitettävät vähimmäistiedot**  **LoA liite 2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)**  Korotettu:  1.Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan  ja  todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön  ja  on ryhdytty toimiin sen riskin minimoimiseksi, että henkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todiste on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt; |  | Säännöllisen tarkistamisen tiheyttä ei ole säädetty.  Hyvä vakiintunut käytäntö on tarkistus viikottain.  vrt. (ei viittausta tunnistuslaissa eli muodollisesti sovelletaan vain, jos menetelmä notifioidaan)  **LoA 2.1.1 Hakemus ja rekisteröinti**  3. Kerätään asiaankuuluvat tunnistetiedot, jotka tarvitaan henkilöllisyyden todista |
|  | S, H | **Tunnistusvälineen myöntäminen, toimittaminen, aktivointi**  Tunnistusvälineen luovutus- tai toimitusmenettelyssä varmistetaan, ettei tunnistusväline joudu oikeudettomasti toisen haltuun. | **TunnL 20 § Tunnistusvälineen myöntäminen**  Tunnistusvälineen liikkeelle laskeminen perustuu tunnistusvälineen hakijan ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Sopimus on tehtävä kirjallisesti. Sopimus voidaan tehdä myös sähköisesti, jos sen sisältöä ei voida yksipuolisesti muuttaa ja se säilyy osapuolten saatavilla.  […]  vrt. (Kohtaan LoA 2.1.1 ei ole viittausta tunnistuslaissa eli muodollisesti sitä sovelletaan vain, jos menetelmä notifioidaan)  **LoA 2.1.1 Hakemus ja rekisteröinti**  1. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmien käyttöön liittyvistä ehdoista ja edellytyksistä.  2. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmiin liittyvistä suositelluista varotoimista.  **TunnL 21 § Tunnistusvälineen luovuttaminen hakijalle**  Tunnistusvälineen tarjoajan on luovutettava tunnistusväline sen hakijalle siten kuin sopimuksessa on sovittu. Tunnistuspalvelun tarjoajan on varmistettava, ettei tunnistusväline joudu oikeudettomasti toisen haltuun välinettä luovutettaessa siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.2 vähintään korotetulle varmuustasolle säädetyt vaatimukset täyttyvät.  **LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi**  Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu. |  | sopimusehdot (mm. TunnL 15 §) kuuluvat toimijan itse selvitettäviin asioihin, eivät kuulu auditoinnin piiriin  TunnL 8 §:n ja LoA 2.2.1 mukainen vaatimus varmistaa, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä, liittyy myös luovuttamisen osalta 21 §:ssä erikseen säädettyyn vaatimukseen, jonka mukaan tunnistus-palvelun tarjoajan on varmistettava, ettei tunnistusväline joudu oikeudettomasti toisen haltuun välinettä luovutettaessa.  Ks. LoA-guidance:  Mahdollisia mekanismeja ovat esimerkiksi seuraavat:  • henkilökohtainen toimitus  • toimitus kirjattuna kirjeenä  • sellaisen aktivointimenettelyn käyttö, josta voidaan kohtuudella olettaa, että vain henkilöllä on menetelmän aktivointiin tarvittavat tiedot (esimerkiksi oletus-PIN-koodi, joka toimitetaan erillään tunnistamismenetelmästä).  Tasolla ”korotettu” on käytettävä useita todentamistekijöitä. Aktivointikoodeja ei välttämättä tarvita. Tason ”korotettu” vaatimukset voidaan täyttää monenlaisilla myöntämis-, toimitus- ja aktivointitapojen yhdistelmillä:  • Sähköisen tunnistamisen menetelmä voidaan toimittaa postitse ja aktivointi tehdä lähettämällä koodi henkilön pankkitilille. Hakija antaa koodin, jolla sähköisen tunnistamisen menetelmä aktivoidaan. Oletuksena on, että pankin todentaminen on vähintään tasolla ”korotettu”.  • Sähköisen tunnistamisen menetelmä ja aktivointikoodi toimitetaan erikseen postitse henkilön varmennettuun osoitteeseen.  • Sähköisen tunnistamisen menetelmä toimitetaan postitse hakijan osoitteeseen.  • Sähköisen tunnistamisen menetelmä annetaan käyttöön, kun hakijan henkilöllisyys on varmennettu. |
|  | H | **Tunnistusvälineen myöntäminen, toimittaminen, aktivointi**  Tunnistusväline luovutus- tai toimitusmenettelyssä varmistetaan, ettei tunnistusväline joudu oikeudettomasti toisen haltuun. | **LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi**  **korkea**  Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu. |  | Aktivointiprosessi lähtökohtaisesti edellyttää aktivointikoodin käyttöä. Erityisesti tulee huolehtia, että aktivointikoodi ei voi päätyä muiden haltuun toimittamisprosessissa, ja että aktivointikoodi on kertakäyttöinen, eikä sitä voi käyttää esimerkiksi uudelleenaktivointiin tai uuden pin-koodin luomiseen. |
|  | S, H | **Tunnistusvälineen voimassaolon keskeyttäminen, peruuttaminen ja uudelleen aktivointi**  Tunnistusvälineen tarjoajalla on 24/7 -sulkupalvelu käyttäjille sekä sulkulista luottaville osapuolille tai mahdollisuus teknisesti estää käyttäjän kadonneeksi tai varastetuksi ilmoittaman tunnistusvälineen käyttö. | **TunnL 25 § Tunnistusvälineen peruuttamista tai käytön estämistä koskeva ilmoitus**  Tunnistusvälineen haltijan on ilmoitettava tunnistusvälineen tarjoajalle tai tämän nimeämälle muulle taholle tunnistusvälineen katoamisesta, joutumisesta oikeudettomasti toisen haltuun tai oikeudettomasta käytöstä ilman aiheetonta viivytystä havaittuaan asian.  Tunnistusvälineen tarjoajan on tarjottava mahdollisuus tehdä 1 momentissa tarkoitettu ilmoitus milloin tahansa. Tunnistusvälineen tarjoajan on viipymättä peruutettava tunnistusväline tai estettävä sen käyttö saatuaan asiaa koskevan ilmoituksen.  Tunnistusvälineen tarjoajan on asianmukaisesti ja viipymättä merkittävä järjestelmään tieto peruuttamisen tai käytön estämisen ajankohdasta. Tunnistusvälineen haltijalla on oikeus saada pyynnöstä todistus siitä, että hän on tehnyt 1 momentissa tarkoitetun ilmoituksen. Todistusta on pyydettävä 18 kuukauden kuluessa ilmoituksesta.  Järjestelmän on oltava sellainen, että tunnistuspalvelua käyttävä palveluntarjoaja voi helposti tarkastaa siihen merkityt tiedot ympäri vuorokauden. Velvollisuutta järjestää tarkastusmahdollisuutta ei kuitenkaan ole, jos tunnistusvälineen käyttö voidaan teknisesti estää tai se voidaan sulkea.  […]  **26 § Tunnistusvälineen tarjoajan oikeus peruuttaa tai estää tunnistusvälineen käyttö**  Sen lisäksi, mitä 25 §:ssä säädetään, tunnistusvälineen tarjoaja voi peruuttaa tunnistusvälineen tai estää sen käytön, jos:  1) tunnistusvälineen tarjoajalla on syytä epäillä, että joku muu kuin se, jolle tunnistusväline on myönnetty, käyttää sitä;  2) tunnistusväline sisältää ilmeisen virheellisyyden;  3) tunnistusvälineen tarjoajalla on syytä epäillä, että tunnistusvälineen käytön turvallisuus on vaarantunut;  4) tunnistusvälineen haltija käyttää tunnistusvälinettä olennaisesti sopimusehtojen vastaisella tavalla;  5) tunnistusvälineen haltija on kuollut.  Tunnistusvälineen tarjoajan tulee ilmoittaa haltijalle niin pian kuin mahdollista tunnistusvälineen peruuttamisesta tai käytön estämisestä ja sen ajankohdasta sekä siihen johtaneista syistä.  Tunnistusvälineen tarjoajan on palautettava mahdollisuus käyttää tunnistusvälinettä tai annettava haltijalle uusi väline välittömästi 1 momentin 2 ja 3 kohdassa tarkoitetun syyn poistuttua.  **LoA liite 2.2.3 Voimassaolon keskeyttäminen, peruuttaminen ja uudelleenaktivointi**  1. Sähköisen tunnistamisen menetelmän voimassaolo on mahdollista keskeyttää ja/tai peruuttaa viivyttelemättä ja tehokkaasti.  2. Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi.  3. Uudelleenaktivoinnin ehtona on, että ennen voimassaolon keskeyttämistä tai peruuttamista asetetut varmuusvaatimukset täyttyvät edelleen. |  | vrt. (kohtaan LoA 2.2.3 ei ole viittausta tunnistuslaissa eli sitä sovelletaan vain, jos menetelmä notifioidaan)  **LoA Liite 2.2.3** **Voimassaolon keskeyttäminen, peruuttaminen ja uudelleenaktivointi**  1. Sähköisen tunnistamisen menetelmän voimassaolo on mahdollista keskeyttää ja/tai peruuttaa viivyttelemättä ja tehokkaasti.  2. Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi.  3. Uudelleenaktivoinnin ehtona on, että ennen voimassaolon keskeyttämistä tai peruuttamista asetetut varmuusvaatimukset täyttyvät edelleen. |
|  | S, H | **Tunnistusvälineen uusiminen ja korvaaminen** | **TunnL 22 § Tunnistusvälineen uusiminen**  Tunnistusvälineen tarjoaja saa toimittaa tunnistusvälineen haltijalle uuden välineen ilman nimenomaista pyyntöä vain, jos aikaisemmin annettu tunnistusväline on korvattava uudella. Tunnistusvälineen uusimisessa tulee noudattaa sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.2.4 vähintään korotetulle varmuustasolle säädettyjä vaatimuksia.  **LoA Liite 2.2.4 Uusiminen ja korvaaminen**  Ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista uusimisen tai korvaamisen on täytettävä samat varmuusvaatimukset kuin henkilöllisyyden alkuperäisen todistamisen ja varmentamisen yhteydessä tai sen on perustuttava saman tai korkeamman varmuustason voimassa olevaan sähköisen tunnistamisen menetelmään.  **LoA liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu**  Korotettu:  2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että sitä voidaan olettaa käytettävän vain, jos se on sen henkilön hallinnassa tai hallussa, jolle se kuuluu.  **LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi**  Korotettu:  Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu. |  | TunnL 8 §:n ja LoA 2.2.1 ja 2.2.2 mukaisen varmistusvaatimuksen, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä, täytyy toteutua myös kaikissa tilanteissa, joissa osa tai kaikki todentamistekijät tai uusi aktivointikoodi luovutetaan uusimisen/korvaamisen tai uudelleenaktivoinnin yhteydessä.  Ks. Tulkintakannanotto *Dnro: Traficom/106/09.02.00/2019 (25.3.2019) Liikenne- ja viestintäviraston tulkintamuistio ajokortin käyttämisestä henkilöllisyyden todentamisessa tunnistusvälineen lukkiutuessa tai uusittaessa tunnistusväline tai todentamistekijä.* Kannanotto löytyy viraston verkkosivuilta <https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen> |
|  | H | **Tunnistusvälineen uusiminen ja korvaaminen** | **LoA Liite 2.2.4 Uusiminen ja korvaaminen**  **Korkea:**  Ottaen huomioon riskit henkilön tunnistetiedoissa tapahtuvista muutoksista uusimisen tai korvaamisen on täytettävä samat varmuusvaatimukset kuin henkilöllisyyden alkuperäisen todistamisen ja varmentamisen yhteydessä tai sen on perustuttava saman tai korkeamman varmuustason voimassa olevaan sähköisen tunnistamisen menetelmään.  Jos uusiminen tai korvaaminen perustuu voimassa olevaan sähköisen tunnistamisen menetelmään, tunnistetiedot varmennetaan luotettavasta lähteestä.  **LoA liite 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu**  Korkea:  2. Sähköisen tunnistamisen menetelmä on suunniteltu niin, että henkilö, jolle se kuuluu, voi suojata sen luotettavasti muiden käytöltä.  **LoA Liite 2.2.2 Myöntäminen, toimittaminen ja aktivointi**  Korkea:  Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu. |  | TunnL 8 §:n ja LoA 2.2.1 ja 2.2.2 mukaisen varmistusvaatimuksen, että ainoastaan tunnistusvälineen haltija voi käyttää välinettä, täytyy toteutua myös kaikissa tilanteissa, joissa osa tai kaikki todentamistekijät tai uusi aktivointikoodi luovutetaan uusimisen/korvaamisen tai uudelleenaktivoinnin yhteydessä. |