Ohje eIDAS-asetuksessa tarkoitettujen varmuustasojen soveltamisesta

1. Sovellettavat määritelmät

Tässä liitteessä käytetään seuraavia määritelmiä:

Huomautus ohjeen käytöstä: Ohjeessa käytettyjä esimerkkejä ei ole tarkoitettu ehdottomiksi tai poissulkeviksi, vaan niiden tarkoituksena on helpottaa ohjeen ymmärtämistä.

Tässä ohjeessa käytetään seuraavia termejä:

- ”hakijalla” tarkoitetaan henkilöä, joka yrittää todentamista tai jonka ei ole vielä todettu olevan laillinen luonnollinen tai oikeushenkilö
- ”henkilöllä” tarkoitetaan laillista luonnollista tai oikeushenkilöä, jota sähköisen tunnistamisen menetelmällä edustetaan tai on tarkoitus edustaa

Onnistuneen todentamisen jälkeen ”henkilöstä” ja ”hakijasta” tulee käytännössä yksi ja sama.

Varmuustasossa ja tässä ohjeessa termillä *asiakirja* tarkoitetaan sekä fyysisiä että sähköisiä asiakirjoja. Termillä *todiste(et)* tarkoitetaan sekä fyysisiä että sähköisiä todisteita ja myös kaikkia muita todisteita, joiden muoto on kansallisesti hyväksytty.

(1) ”luotettavalla lähteellä” tarkoitetaan mitä tahansa sellaista lähdettä muodosta riippumatta, josta voidaan luotettavasti saada paikkansapitäviä tietoja ja/tai todisteita, joita voidaan käyttää henkilöllisyyden todistamiseen;

OHJE:

Luotettava lähde on mikä tahansa lähde, jonka luotetaan kansallisella tasolla tuottavan kelvollista tietoa. Luotettava lähde on esimerkiksi rekisteri tai jokin muu vastuussa olevan tahon tuottama tieto. Lähde voi olla luotettava vain sen tuottamaan tietoon nähden.

On syytä varmistaa, että tuotettu tieto on aitoa.

Kun luotettava lähde toimittaa todisteita henkilöllisyydestä, voidaan kyseisten henkilöllisyyttä koskevista todisteista annettujen tietojen katsoa edustavan henkilöllisyyttä sellaisena, kuin luotettava lähde sen myöntämishetkellä tuntee, jos kyseiset todisteet henkilöllisyydestä voidaan vahvistaa aidoiksi.

Rekisteriä, myös yksityisen palveluntuottajan (esimerkiksi pankin) pitämää, voidaan käyttää luotettavana lähteenä, jos rekisteriin kirjaamisessa noudatettavat käytännöt ovat riittävän luotettavia ja riittävät varmistamaan tietojen laadukkuuden ja jos rekisteriä tuottavaa tahoa

pidetään kansallisesti uskottavana ja luotettavana. Erityisen hyödyllistä voi olla riskiperusteisen lähestymistavan noudattaminen, jolloin tiedot tarkistetaan useista toisistaan riippumattomista tietolähteistä. Näin saadaan vähennettyä riskiä siitä, että rekisterissä voi olla epätäsmällistä tai huonolaatuista tietoa.

Esimerkkejä luotettavista lähteistä:

- *kansalliset väestörekisterit yksityishenkilöiden henkilötietojen lähteenä (kun on esimerkiksi yhdistettävä nimi kansalliseen henkilötunnukseen tai varmennettava, että henkilö on elossa)*
- *valtion rekisterit, joissa olevan tiedon luotettavuus ja virheettömyys varmistetaan noudattamalla tiettyjä menettelytapoja; tällaisia rekistereitä ovat esimerkiksi passi-, ajokortti-, vero- ja sosiaaliturvarekisterit*
- *yritysrekisterit oikeushenkilöiden tunnistetietoja ja niihin yhteydessä olevia luonnollisia henkilöitä koskevan tiedon lähteenä*
- *viralliset henkilöllisyystodistukset, kuten passit ja henkilökortit*
- *viranomaisen henkilöstä antamat vakuutukset, kuten viralliset asiakirjat*

(2) ”todentamistekijällä” tarkoitetaan tekijää, joka on vahvistettu henkilöön kytkeytyväksi ja joka kuuluu johonkin seuraavista luokista:

OHJE:

Sähköisen tunnistamisen menetelmän keskeisiä ominaisuuksia ovat sen hyödyntämien todentamistekijöiden määrä ja luokka. Seuraavat määritelmät auttavat ymmärtämään, mistä eri luokissa on kyse.

Todentamistekijät voidaan jakaa seuraaviin luokkiin, joita tarkastellaan lähemmin seuraavilla sivuilla:

- tiedossaoloon perustuvat todentamistekijät
- hallussapitoon perustuvat todentamistekijät
- luontaiset todentamistekijät.

Eri luokkiin kuuluvia todentamistekijöitä voidaan myös yhdistää; esimerkkinä tästä on salaustunniste, joka on suojattu sormenjälkitiedolla tai PIN-koodilla. Useampaa kuin yhtä eri luokkiin kuuluvaa todentamistekijää hyödyntävää tunnistamismenetelmää kutsutaan useaan tekijään perustuvaksi menetelmäksi. *Esimerkkinä on älykortti (hallussapitoon perustuva todentamistekijä), joka otetaan käyttöön PIN-koodilla (tiedossaoloon perustuva todentamistekijä)*.

Useaan tekijään perustuvaa todentamista käytettäessä eri tekijät on valittava niin, että niillä torjutaan eri uhkia/hyökkäystapoja.

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

(a) ”hallussapitoon perustavalla todentamistekijällä” tarkoitetaan todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;

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

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

(b) ”tiedossaoloon perustavalla todentamistekijällä” tarkoitetaan todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;

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

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

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

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

(c) ”luontaisella todentamistekijällä” tarkoitetaan todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen, jonka henkilön on osoitettava fyysiseksi ominaisuudekseen;

OHJE:

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

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

(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

OHJE:

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

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

tietynlaiset istuntokaappaukset, esimerkiksi tapaukset, joissa vaihdetaan keskenään osittain tai kokonaan kaksi tai useampia yhtäaikaisia todentamistilanteita. On syytä muistaa, että useaan tekijään perustuva ja dynaaminen todentaminen eivät tarkoita samaa asiaa. Useaan tekijään perustuvassa todentamisessa ei edellytetä, että todentaminen tapahtuu dynaamisesti (esimerkkejä ovat PIN-koodi ja sormenjälkitiedot), joten tällainen todentamistapa voi olla alttiimpi replay-hyökkäykselle kuin dynaaminen todentaminen.

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

Esimerkkejä dynaamisista todentamistavoista:

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

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

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

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

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

(4) ”tietoturvallisuuden hallintajärjestelmällä” tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen liittyvät riskit hyväksyttävällä tasolla.

OHJE:

2. Tekniset eritelmät ja menettelyt

Tässä liitteessä esitettyjen teknisten eritelmien ja menettelyjen osatekijöitä käytetään määriteltäessä, miten asetuksen (EU) N:o 910/2014 8 artiklan vaatimuksia ja perusteita on sovellettava sähköisen tunnistamisen järjestelmän puitteissa myönnettyihin sähköisen tunnistamisen menetelmiin.

OHJE:

Kohdissa 2.1–2.2 mainitut vaatimukset tarkoittavat rekisteröinti- ja myöntämismenettelyä koskevia edellytyksiä. Näiden toiminnallisten vaatimusten on täytyttävä viimeistään sähköistä henkilöllisyyttä käytettäessä.

2.1 Rekisteröinti

OHJE:

Tässä asiakirjassa käytetään termiä ”rekisteröinti” tarkoittamaan koko prosessia, joka koostuu myöhemmissä alaluvuissa käsiteltävistä vaiheista:

- Hakemus ja rekisteröinti (kohta 2.1.1)

- Henkilöllisyyden todistaminen ja varmentaminen (luonnollisten henkilöiden osalta kohta 2.1.2, oikeushenkilöiden osalta kohta 2.1.3 ja luonnollisten ja oikeushenkilöiden välisen kytköksen osalta kohta 2.1.4).

2.1.1 Hakemus ja rekisteröinti

MATALA

1. Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmien käyttöön liittyvistä ehdoista ja edellytyksistä.

OHJE:

Tähän vaikuttavat useat seikat, esimerkiksi sähköisen tunnistamisen järjestelmän varmuustaso sekä järjestelmän toimintaa ja turvallisuutta koskevien ehtojen ja edellytysten kriittisyys.

Esimerkkejä:

- *tieto on osa kansallista lainsäädäntöä, jolloin voidaan olettaa, että se on hakijan tiedossa*

- *hakija saa tarvittavat tiedot kirjallisessa muodossa*

- *hakija nimenomaisesti hyväksyy ehdot ja edellytykset.*

2. **Varmistetaan, että hakija on tietoinen sähköisen tunnistamisen menetelmiin liittyvistä suositelluista varotoimista.**

OHJE:

Katso kohta 1.

Esimerkkejä varotoimista:

- *valitaan ohjeistuksen mukainen, tietoturvallinen salasana tai PIN-koodi*

- *tallennetaan tietoturvallisesti hallussapitoon perustuvat sähköisen tunnistamisen menetelmät*

- *ei luovuteta omia sähköisen tunnistamisen menetelmiä toisille henkilöille.*

Katso myös kohta 2.4.6, jossa käsitellään teknisen kehityksen jatkuvaa seurantaa sekä tarvittavista varotoimista tiedottamista hakijoille.

3. Kerätään asiaankuuluvat tunnistetiedot, jotka tarvitaan henkilöllisyyden todistamista ja varmentamista varten.

OHJE:

Sähköisen tunnistamisen järjestelmässä on oltava ainakin vähimmäisdatan tuottamiseen tarvittavat tiedot. Vähimmäisdatan edellyttämät tiedot, jotka eivät ole tiedossa tai joita järjestelmä ei tuota, on kerättävä esimerkiksi hakijalta tai muista lähteistä.

Katso myös seuraavat kohdat sekä asetuksen 7 artiklan d kohta.

2.1.2 Henkilöllisyyden todistaminen ja varmentaminen (luonnollinen henkilö)

MATALA

1. Henkilön voidaan kohtuudella olettaa pitävän hallussaan sen jäsenvaltion hyväksymää todistetta ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan.

OHJE:

Todisteen voidaan *kohtuudella* olettaa olevan henkilön hallussa, jos muusta ei ole viitteitä ja kokemuksen perusteella voidaan katsoa, että oletusta tukevat todisteet ovat käytännössä riittäviä.

Esimerkkejä:

- *Hallussapito voidaan osoittaa esittämällä todisteita fyysisesti tai sähköisesti.*
- *Hallussapito voidaan osoittaa esittämällä henkilön tunnettuun osoitteeseen lähetettyihin asiakirjoihin sisältyviä tietoja, jotka eivät ole julkisia.*

2. Todisteen voidaan olettaa olevan aito tai luotettavan lähteen mukaan olemassa oleva, ja se näyttää olevan voimassa.

OHJE:

Termillä ”aito” tarkoitetaan todisteen aitoutta myöntämishetkellä. Todisteen voidaan edelleen olettaa olevan aito, jos sitä ei ole väärennetty tai muutettu ja sen on myöntänyt valtuutettu taho.

Termillä ”voimassaolo” tarkoitetaan todisteen paikkansapitävyyttä esittämishetkellä. Tähän sisältyy muun muassa todisteen sisältämien tietojen paikkansapitävyys sekä todisteen mahdollinen peruuttaminen määräajaksi tai pysyvästi.

Jos kansallisessa lainsäädännössä tai hallinnollisessa käytännössä ei muuta määrätä, fyysisen todisteen aitous tarkistetaan yleensä fyysisellä tarkastuksella. Sähköisissä todisteissa paras toimintatapa on todisteen myöntäneen viranomaisen sähköisten allekirjoitusten varmentaminen.

Todisteen ilmeisen aitouden ja voimassaolon havaitsemiseen ei tarvita erityisiä tarkistuksia tasolla ”matala”.

3. Luotettavan lähteen tiedossa on, että ilmoitettu henkilöllisyys on olemassa, ja voidaan olettaa, että henkilöllisyyden ilmoittaneella henkilöllä on tämä sama henkilöllisyys.

OHJE:

Useissa jäsenvaltioissa väestörekisteri on luotettava lähde sille, että henkilö on olemassa. Muita luotettavia lähteitä asiassa ovat myös viralliset todisteet, kuten rekisteriotteet, henkilöllisyystodistukset tai muut viranomaisen myöntämät todistukset.

Olemassaolo tarkoittaa myös, että ilmoitettu henkilö on elossa.

Näyttönä siitä, että hakija on luotettavan lähteen väittämä henkilö, voidaan käyttää esimerkiksi fyysistä vertaamista vaikkapa valokuvaan, tai todiste voidaan yhdistää sähköiseen tunnistustapaan, jossa tunnistamiseen liittyvät määritelmät ovat samat kuin luotettavan lähteen hallussa olevat määritelmät (esimerkiksi tunnistetiedot, nimi ja syntymäaika).

KOROTETTU

Sama kuin tasolla ”matala”, minkä lisäksi yhden kohdissa 1–4 mainituista vaihtoehdoista on täytyttävä:

1. Henkilöllä on varmennettu olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan

OHJE:

Fyysisen todisteen hallussapito varmennetaan yleensä siten, että todiste on esitettävä joko hakemisvaiheessa tai ennen sitä, mutta viimeistään hakemishetkellä sen on oltava luotettavasti saatavilla. Todisteen tyypin mukaan voidaan joko edellyttää fyysistä esittämistä varmentamispaikassa, tai todisteen esittäminen ilman fyysistä läsnäoloa voi olla mahdollista.

Muun kuin fyysisen todisteen varmentaminen voi tarkoittaa esimerkiksi sitä, että hakijan pääsy pankkitilille tai vastaavalle varmennetaan pyytämällä häntä tekemään maksutapahtuma, joka edellyttää pankkitilin käyttöä.

ja

todiste on tarkastettu sen varmistamiseksi, että se on aito; tai luotettavasta lähteestä tiedetään sen olevan olemassa ja liittyvän todelliseen henkilöön

OHJE:

Huomaa, että myös kohdassa ”matala” mainittuja turvatoimenpiteitä sovelletaan edelleen, mikä tarkoittaa sitä, että todisteen on näytettävä olevan voimassa.

Fyysisen todisteen aitous tarkistetaan yleensä tutkimalla todisteen fyysiset turvaominaisuudet. Esimerkkejä turvaominaisuuksista ovat vesileimat, erilaiset musteet, hologrammit ja mikropainatukset.

Sähköisten todisteiden varmentaminen tehdään esimerkiksi sähköisistä allekirjoituksista tai varmentamalla todiste verkossa luotettavasta lähteestä. Sähköisiä todisteita ovat esimerkiksi väestörekisteriotteet tai otteet viranomaisrekistereistä, joihin kirjatut henkilötiedot on varmennettava rekisteröitymishetkellä.

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;

OHJE:

Jäsenvaltioiden käytännöt saattavat vaihdella kansallisen infrastruktuurin mukaan. Joissakin jäsenvaltioissa saatetaan luottaa yhteen viranomaiseen ja sen tietoturvatoimiin, esimerkiksi yhteen henkilöllisyystodistuksia myöntävän viranomaisen tekemään henkilöllisyyden varmentamiseen. Toisissa jäsenvaltioissa taas henkilöllisyyttä koskevan todistuksen tueksi saatetaan vaatia monitasoisia turvatoimenpiteitä, joissa useiden viranomaisten tietojen on täsmättävä (esimerkkinä veroilmoitukseen liittyvä henkilöä koskeva vakuutus, jossa henkilön tietojen on täsmättävä verottajan tietojen kanssa ja edelleen väestörekisterin tietojen kanssa, kun väestörekisteri lähettää aktivointikoodin henkilön viralliseen kotiosoitteeseen).

Asiakirjojen katoamiseen tai varastamiseen taikka niiden voimassaolon keskeyttämiseen, peruuttamiseen tai päättymiseen liittyvään riskiin vaikuttaa se, kuinka monta toisistaan riippumatonta lähdettä käsittelyyn osallistuu ja kuinka luotettavia ne ovat, mutta myös todennäköisyys, että kadonneista tai varastetuista tunnistetiedoista ilmoitetaan pikaisesti. Tähän todennäköisyyteen vaikuttavia tekijöitä ovat esimerkiksi käytön säännöllisyys ja tunnistetietojen arvo niiden hallussapitäjälle. Vanhentuneiden asiakirjojen todistusarvo saattaa myös vaihdella olosuhteiden mukaan ja määräytyä esimerkiksi niiden ominaisuuksien perusteella, jotka vanhentumisen aiheuttavat (joissakin jäsenvaltioissa saatetaan esimerkiksi sallia ajokortin käyttäminen todisteena, vaikka ajokortin haltijan oikeus ajaa autoa tai tietynlaista ajoneuvoa ei ole enää voimassa).

Esimerkkejä toimenpiteistä, joilla riskejä voidaan vähentää:

- *voimassaolon tarkistaminen rekistereistä*

- *julkisen avaimen infrastruktuuriin/älykorttiin perustuvien todisteiden peruuttamista koskevat tarkistukset*

- *hakijan fyysisten ominaisuuksien vertaaminen todisteeseen*

- *vakiintuneiden alan käytäntöjen, kuten asiakkaan tuntemista koskevan velvollisuuden, soveltaminen rahoitusalalla (vrt. rahanpesudirektiivi)*

- *toimenpiteet, joilla estetään asiakirjojen käyttö huijaamistarkoituksessa, kuten senhetkisen biometrisen ominaisuuden tallentaminen hakijalta (valokuva, sormenjälkitiedot).*

tai

2. henkilöllisyystodistus esitetään rekisteröintiprosessin aikana siinä jäsenvaltiossa, jossa todistus on myönnetty, ja todistus näyttää liittyvän sen esittäneeseen henkilöön

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

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;

OHJE:

Kohtaa koskevista ohjeista ks. edeltävät luetelmakohdat.

tai

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 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin;

OHJE:

Esimerkkejä aiemmin käytetyistä menettelyistä ovat rekisteröityminen sellaisessa viranomaisessa, joka vaatii henkilön yksilöintiä (esimerkiksi veroviranomainen), tai pankkitilin avaaminen, kun pankissa sovelletaan pankkitoimintaa koskevassa lainsäädännössä säädettyjä tunnistamista ja asiakkaan tuntemista koskevia edellytyksiä.

Tämä vaihtoehto kuvastaa eIDAS-asetuksen 24 artiklan 1 kohdan d alakohdassa mainittuja menettelyjä, eli siinä otetaan selkeästi huomioon asetuksen johdanto-osan 16 kappaleen vaatimus, jonka mukaan ”...on huolehdittava tämän asetuksen johdonmukaisesta soveltamisesta erityisesti hyväksyttyjen varmenteiden myöntämiseen liittyvän henkilöllisyyden todistamisen edellyttämän korkean varmuustason osalta”.

Varmuuden vastaavuuden vahvistaminen tarkoittaa, että kullakin tasolla käytössä olevien edellytysten mukaiset aiemmat menettelyt vastaavat varmuustasosta saatuja tuloksia.

Esimerkkejä asetuksen 765/2008 mukaisia vaatimustenmukaisuuden arviointilaitoksia vastaavista elimistä ovat kansalliset valvontaelimet.

tai

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.

OHJE:

Henkilöllisyyden todistamista ja varmentamista koskevat vaatimukset voidaan täyttää käyttämällä aiemmin myönnettyjä sähköisen tunnistamisen menetelmiä. On huomattava, että henkilöllisyyden todistaminen ja varmentaminen on vasta osa rekisteröinti- ja myöntämismenettelyä. Henkilöllisyyden todistamista ja varmentamista tiukempia edellytyksiä on tarkasteltava erikseen.

Huomaa, että uusimista ja korvaamista käsitellään kohdassa 2.2.4. Tasoilla ”matala” ja ”korotettu” uusiminen ja korvaaminen voidaan tehdä tässä kohdassa kuvattuja menettelyjä käyttäen.

KORKEA

Joko kohdan 1 tai 2 vaatimusten on täytyttävä:

1. Sama kuin tasolla ”korotettu”, minkä lisäksi yhden kohdissa a–c mainituista vaihtoehdoista on täytyttävä:

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;

OHJE:

Ks. luotettavan lähteen määritelmää koskeva ohje.

ja

hakijalla todetaan olevan ilmoitettu henkilöllisyys vertaamalla yhtä tai useampaa henkilön fyysistä ominaisuutta luotettavaan lähteeseen;

OHJE:

Fyysisten ominaisuuksien vertaamisen on tapahduttava riittävän luotettavasti, jotta henkilön henkilöllisyys saadaan selkeästi varmennettua.

Osoitus menettelyiden riittävyydestä on esimerkiksi alhaiseksi jäävä virheellisten hyväksyntöjen osuus. Tässä huomioon otettavana tekijänä voi olla esimerkiksi vertailutiedon riittävä laatu.

- Jos henkilöstö osallistuu vertaamiseen, on tärkeää ottaa huomioon myös kohdan 2.4.5 vaatimukset riittävästä osaamisesta, jota vertaaminen henkilöstöltä edellyttää.

- Vastaavasti automaattista vertaamista käytettäessä on huomioitava noudatettavat parhaat toimintatavat.

tai

b. 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 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin

ja

on ryhdytty toimiin sen osoittamiseksi, että kyseisen aiemman menettelyn tulokset ovat edelleen voimassa;

OHJE:

Aiemmalla kerralla varmennetut tunnistetiedot ovat voineet vanhentua esimerkiksi nimen- tai osoitteenmuutoksen vuoksi. Tämän vaatimuksen tarkoituksena on varmistaa, että tunnistetietojen voimassaolo tarkistetaan ja tiedot päivitetään tarvittaessa. Ks. myös asetuksen 7 artiklan d kohta.

Tason ”korotettu” 3. kohdassa käytettyjen veroviranomaisia ja pankkeja koskevien esimerkkien mukaisesti voimassaolo voidaan todeta esimerkiksi tarkistamalla muuttuvat tunnistusominaisuudet (kuten nimi ja osoite) muista lähteistä, esimerkiksi väestörekisteristä.

c. 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

ja

on ryhdytty toimiin sen osoittamiseksi, että sen menettelyn tulokset, jossa ilmoitettu sähköisen tunnistamisen menetelmä aiemmin myönnettiin, ovat edelleen voimassa.

OHJE:

Ks. 4. kohta, kohta ”korotettu”.

TAI

2. 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.

OHJE:

Tässä kohdassa todetaan, että hyväksytyn valokuvan tai biometrisen todisteen saamiseksi käytettävät kansalliset menettelyt ovat kelvollisia menettelyitä, jos kyseiset todisteet muuten hyväksytään.

Esimerkkejä hyväksyttävistä valokuvista tai biometrisistä todisteista ovat passit ja henkilöllisyystodistukset.

2.1.3 Henkilöllisyyden todistaminen ja varmentaminen (oikeushenkilö)

OHJE:

Kohdan 2.1.2 ohjeissa mainittuja seikkoja voidaan useissa tapauksissa soveltaa myös tässä kohdassa. Sovellettavat tietolähteet ovat tässä kohdassa todennäköisesti monipuolisempia.

MATALA

1. Oikeushenkilön ilmoitettu henkilöllisyys osoitetaan sen jäsenvaltion hyväksymällä todisteella, jossa sähköisen tunnistamisen menetelmää haetaan.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2. Todiste näyttää olevan voimassa ja sen voidaan olettaa olevan aito tai luotettavan lähteen mukaan olemassa oleva, jos oikeushenkilön kirjaaminen luotettavaan lähteeseen on vapaaehtoista ja sitä säännellään oikeushenkilön ja luotettavan lähteen välisellä sopimuksella.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

3. Luotettavan lähteen tiedossa ei ole, että oikeushenkilö olisi asemassa, joka estää sitä toimimasta kyseisenä oikeushenkilönä.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

KOROTETTU

Sama kuin tasolla ”matala”, minkä lisäksi yhden kohdissa 1–3 mainituista vaihtoehdoista on täytyttävä:

1. Oikeushenkilön ilmoitettu henkilöllisyys osoitetaan sen jäsenvaltion hyväksymällä todisteella, jossa sähköisen tunnistamisen menetelmää haetaan ja jossa mainitaan oikeushenkilön nimi, oikeudellinen muoto ja (oikeushenkilöön sovellettavan tapauksen mukaan) rekisterinumero

OHJE:

Jäsenvaltioiden hyväksymiä todisteita ovat esimerkiksi yritysnimirekisterit, kaupparekisterit, yhdistysrekisterit ja vastaavat viralliset lähteet.

ja

todiste tarkistetaan sen määrittämiseksi, onko se on aito tai luotettavan lähteen mukaan olemassa oleva, jos oikeushenkilön kirjaaminen luotettavaan lähteeseen on pakollinen ehto oikeushenkilön toiminnalle

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

ja

on ryhdytty toimiin sen riskin minimoimiseksi, että oikeushenkilön henkilöllisyys ei ole ilmoitettu henkilöllisyys, ml. riski siitä, että todistus on kadonnut tai varastettu tai sen voimassaolo on keskeytetty, peruutettu tai päättynyt;

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.3 kohdassa esitetyt menettelyt varmuustasolla ”korotettu”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin;

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

tai

3. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korotettu” tai ”korkea”, 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.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

KORKEA

Sama kuin tasolla ”korotettu”, minkä lisäksi yhden kohdissa 1–3 mainituista vaihtoehdoista on täytyttävä:

1. Oikeushenkilön ilmoitettu henkilöllisyys osoitetaan sen jäsenvaltion hyväksymällä todisteella, jossa sähköisen tunnistamisen menetelmää haetaan ja jossa mainitaan oikeushenkilön nimi, oikeudellinen muoto ja vähintään yksi kansallisessa yhteydessä käytetty oikeushenkilön yksilöllinen tunniste

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

ja

todiste on tarkastettu sen varmistamiseksi, että se on luotettavan lähteen mukaan voimassa;

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

tai

2. Jos julkisen tai yksityisen tahon samassa jäsenvaltiossa aiemmin muuhun tarkoitukseen kuin sähköisen tunnistamisen menetelmien myöntämiseen käyttämät menettelyt tarjoavat vastaavan varmuuden kuin 2.1.3 kohdassa esitetyt menettelyt varmuustasolla ”korkea”, rekisteröinnistä vastaavan tahon ei tarvitse toistaa kyseisiä aiempia menettelyjä edellyttäen, että tällaisen vastaavantasoisen varmuuden on vahvistanut asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitettu vaatimustenmukaisuuden arviointilaitos tai vastaava elin

ja

on ryhdytty toimiin sen osoittamiseksi, että kyseisen aiemman menettelyn tulokset ovat edelleen voimassa;

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

tai

3. Jos sähköisen tunnistamisen menetelmiä myönnetään sellaisen voimassa olevan ilmoitetun sähköisen tunnistamisen menetelmän perusteella, jonka varmuustaso on ”korotettu” tai ”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.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2.1.4 Luonnollisten ja oikeushenkilöiden sähköisen tunnistamisen menetelmien välinen kytkös

MATALA

1. Oikeushenkilön puolesta toimivan luonnollisen henkilön henkilöllisyyden todistamisen varmennetaan tapahtuneen vähintään tasolla ”matala”.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2. Kytkös on vahvistettu kansallisesti hyväksyttyjen menettelyjen mukaisesti.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

3. Luotettavan lähteen tiedossa ei ole, että luonnollinen henkilö olisi asemassa, joka estää häntä toimimasta oikeushenkilön puolesta.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

KOROTETTU

Tason ”matala” 3 kohta lisättynä seuraavalla:

1. Oikeushenkilön puolesta toimivan luonnollisen henkilön henkilöllisyyden todistamisen varmennetaan tapahtuneen tasolla ”korotettu” tai ”korkea”.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2. Kytkös on vahvistettu kansallisesti hyväksyttyjen menettelyjen mukaisesti, joiden tuloksena kytkös on kirjattu luotettavaan lähteeseen.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

3. Kytkös on varmennettu luotettavasta lähteestä saatavan tiedon perusteella.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

KORKEA

Tason ”matala” 3 kohta ja tason ”korotettu” 2 kohta lisättynä seuraavalla:

1. Oikeushenkilön puolesta toimivan luonnollisen henkilön henkilöllisyyden todistamisen varmennetaan tapahtuneen tasolla ”korkea”.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2. Kytkös on varmennettu kansallisessa yhteydessä käytetyn oikeushenkilöä edustavan yksilöllisen tunnisteen perusteella ja luotettavasta lähteestä saatavan, luonnollista henkilöä yksilöivästi edustavan tiedon perusteella.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2.2 Sähköisen tunnistamisen menetelmien hallinta

OHJE:

Tässä kohdassa on syytä pitää mielessä, että hyvän toimintatavan ja varmentajaa koskevien perusteltujen odotusten perusteella varmentajan on muistettava, että henkilöiden käyttämä ympäristö ei todennäköisesti ole luotettu.

2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja laatiminen

MATALA

1. Sähköisen tunnistamisen menetelmässä käytetään vähintään yhtä todentamistekijää.

OHJE:

Todentamistekijöitä voidaan käyttää todentamisessa joko suoraan (esimerkiksi salasanan lähettäminen) tai välillisesti, jolloin niillä avataan tunniste, jolla todentaminen suoritetaan (esimerkiksi avaimen todiste).

2. Sähköisen tunnistamisen menetelmä on suunniteltu siten, että myöntäjä toteuttaa kohtuulliset toimenpiteet tarkistaakseen, että sitä käytetään vain sen henkilön hallinnassa tai hallussa, jolle se kuuluu.

OHJE:

Kun viitataan toimenpiteisiin, joilla varmistetaan, että sähköisen tunnistamisen menetelmä on henkilön hallinnassa, on syytä huomata, että toimenpiteet voivat olla vain sellaisia, joita myöntäjän voidaan kohtuudella odottaa toteuttavan. Käytännön toteutus on yhteydessä kohdassa [2.2.2] mainittuihin vaatimuksiin.

KOROTETTU

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

OHJE:

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

On syytä huomata, että tässä puheena on aina yksi sähköisen tunnistamisen menetelmä. Selvyyden vuoksi todettakoon, että eri tekijät liittyvät siis samaan sähköisen tunnistamisen menetelmään. Todentamisessa käytetään useita tekijöitä yhdessä toistensa kanssa.

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

OHJE:

Sähköisen tunnistamisen menetelmän kytkeminen henkilöön on edellytys sille, että menetelmää voidaan käyttää todentamisessa. Esimerkiksi sellainen tunniste ei ole riittävä, johon ei liity käyttäjän henkilökohtaista PIN-koodia tai salasanaa, sillä kuka tahansa voi

käyttää kadonnutta tai varastettua tunnistetta. Tämän vuoksi ainakin yhden tekijän olisi liityttävä henkilön hallussa olevaan tietoon tai hänen ominaispiirteisiinsä.

KORKEA

Taso ”korotettu” lisättynä seuraavalla:

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

OHJE:

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

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

- *Hallussapitoon perustuvat todentamistekijät: salausavainaineisto upotetaan väärentämiseltä suojattuun laitteeseen, jolla estetään avaimen joutuminen laitteen ulkopuolelle tai sen fyysinen tai sähköinen väärentäminen laitteen sisällä; HSM-laite*

- *Luontaiset todentamistekijät: elävyyden havainnointi, luotettu ympäristö, alhainen virheellisten hyväksyntöjen osuus*

Hyvää toimintatapaa noudatettaessa sähköisen tunnistamisen menetelmäksi valitaan sellainen, jonka on osoitettu pystyvän vastustamaan väärentämis- ja toisintamisyrityksiä. Menetelmä on esimerkiksi testattu huolellisesti ja sertifioitu asiaankuuluvien teknisten standardien (kuten CC) mukaisesti.
Korkean vakavuusasteen hyökkäyksiä koskevia ohjeita on kohdassa 2.3.1.

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

OHJE:

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

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

Edellä mainittujen tekniikoiden lisäksi voidaan käyttää myös seuraavia:

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

2.2.2 Myöntäminen, toimittaminen ja aktivointi

MATALA

Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta sen voidaan olettaa saavuttavan vain aiotun henkilön.

OHJE:

Jos kyseessä on verkossa myönnettävä yksittäinen tekijä (esimerkiksi salasana), aktivointikoodi voidaan toimittaa postitse henkilön varmennettuun osoitteeseen tai lähettää hakijan matkapuhelimeen esimerkiksi tekstiviestinä, kun ensin on varmennettu vaikkapa takaisinsoiton avulla, että puhelinnumero todella kuuluu henkilölle.

Jos tekijöitä on useita, niistä ainakin yksi on toimitettava mainitulla menetelmällä, jolloin aktivointikoodin käyttöä ei järjestelmän perusteella välttämättä edellytetä.

KOROTETTU

Sähköisen tunnistamisen menetelmän myöntämisen jälkeen se toimitetaan käyttäen mekanismia, jonka kautta se voidaan olettaa toimitettavan vain sen henkilön haltuun, jolle se kuuluu.

OHJE:

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.

KORKEA

Aktivointiprosessi varmistaa, että sähköisen tunnistamisen menetelmä on toimitettu vain sen henkilön haltuun, jolle se kuuluu.

OHJE:

Tämä turvatoimenpide vaatii aktivointiprosessia, joten pelkkä tietoturvallinen toimitus ei riitä. Aktivointiprosessi edellyttää yleensä jonkinlaisia käyttäjän toimia.

Aktivointiprosessissa tavoitteena on paitsi sen varmistaminen, että menetelmä toimitetaan oikealle henkilölle, myös henkilön suorittama nimenomainen toimenpide, jolla hän ottaa menetelmän haltuunsa. Vasta tämän jälkeen menetelmää voidaan käyttää todentamiseen.

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.

Sähköisen tunnistamisen menetelmän rekisteröinti ja myöntäminen ei saa koskaan olla yhden henkilön vastuulla.

Aktivointikoodia käytettäessä hakijan on aktivoitava koodi määräajan kuluessa.

Esimerkkejä:

- *Sähköisen tunnistamisen menetelmä myönnetään rekisteröintipisteessä ja aktivointikoodi toimitetaan postitse henkilön varmennettuun osoitteeseen.*
- *Verkossa haettu sähköisen tunnistamisen menetelmä toimitetaan postitse ja aktivointikoodi myönnetään luotetulle osapuolelle (esimerkiksi lähipostissa). Osanottajan on noudettava aktivointikoodi henkilökohtaisesti ja esitettävä samalla henkilöllisyystodistus.*
- *Sähköisen tunnistamisen menetelmää haetaan verkossa ja luotettu kuriiri toimittaa sen fyysisesti varmennettuaan ensin hakijan henkilöllisyyden. Aktivointikoodi lähetetään erikseen postitse henkilön varmennettuun osoitteeseen.*

2.2.3 Voimassaolon keskeyttäminen, peruuttaminen ja uudelleenaktivointi

MATALA

1. Sähköisen tunnistamisen menetelmän voimassaolo on mahdollista keskeyttää ja/tai peruuttaa viivyttelemättä ja tehokkaasti.

OHJE:

Keskeytys- tai peruutustavan on oltava yleisesti käytössä. Esimerkkejä ovat keskeyttäminen puhelimitse, verkkosivustolla tai sähköpostitse. Varmentajan on ryhdyttävä toimiin mahdollisimman nopeasti pyynnön vastaanotettuaan.

2. Käytössä ovat toimenpiteet, joilla estetään voimassaolon luvaton keskeyttäminen, peruuttaminen ja/tai uudelleenaktivointi.

OHJE:

Tällä tarkoitetaan yleensä pyytäjän antaman luvan todentamista. On syytä määrittää, onko käyttäjän lisäksi esimerkiksi asianomaisilla viranomaisilla mahdollisuus antaa lupa keskeyttämiseen ja/tai peruuttamiseen.

3. Uudelleenaktivoinnin ehtona on, että ennen voimassaolon keskeyttämistä tai peruuttamista asetetut varmuusvaatimukset täyttyvät edelleen.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2.2.4 Uusiminen ja korvaaminen

MATALA

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.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

KORKEA

Taso ”matala” lisättynä seuraavalla:

Jos uusiminen tai korvaaminen perustuu voimassa olevaan sähköisen tunnistamisen menetelmään, tunnistetiedot varmennetaan luotettavasta lähteestä.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

Edellä annetun luotettavan lähteen määritelmää koskevan ohjeen mukaisesti kyseeseen voi tulla myös sähköisen tunnistamisen menetelmä itsessään. Tätä seikkaa koskevaa ohjeistusta on vielä tarkasteltava.

2.3 Todentaminen

Tässä jaksossa käsitellään todentamismekanismin käyttöön liittyviä uhkia ja luetellaan vaatimukset kullekin varmuustasolle. Tässä jaksossa turvatoimenpiteet on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.

2.3.1 Todentamismekanismi

OHJE:

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

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

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

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

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

Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.

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

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

Esimerkkejä:

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

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

Komponentteja voidaan käyttää eri kokoonpanoissa ja eri suojausasetuksilla.

> *Arvioinnissa voidaan esimerkiksi olettaa, että käyttäjän tietokone on suojattu palomuurilla ja virustorjuntaohjelmalla.*
>
> *Toisaalta tällä hetkellä ei ole kohtuullista olettaa, että käyttäjän selain on määritelty käyttämään vain TLS-protokollan mukaisia turvallisia suojauspaketteja, mutta palvelu voi kuitenkin tätä edellyttää.*

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

MATALA

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

OHJE:

Henkilön tunnistetietojen luovutuksessa on kyse vähimmäisdatan siirtämisestä luottavalle osapuolelle.

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

OHJE:

Tallennettuihin henkilötietoihin pääsyä on valvottava huolellisesti. Henkilön tunnistetietojen suojaamisessa käytettäviä menetelmiä ovat esimerkiksi Euroopan unionin verkko- ja tietoturvaviraston ENISAn ”Algorithms, Key Sizes and Parameters Report” -asiakirjan, kansallisten salausohjeiden tai muiden hyvien toimintatapojen mukainen salaaminen ja tiivistäminen.

Käyttöoikeuksia on aina valvottava.

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

OHJE:

Kaikki vaadittavat varmentamisvaiheet on kuvattava selkeästi, toteutettava ja testattava.

KOROTETTU

Taso ”matala” lisättynä seuraavalla:

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

OHJE:

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

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

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.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

KORKEA

Taso ”korotettu” lisättynä seuraavalla:

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

OHJE:

Jos todentamismekanismin suojaamisessa käytetään salausta, on valittava vahvat salausprotokollat ja pituudeltaan riittävät avaimet.

Tärkeitä menetelmiä salausprotokollan vahvuuden varmistamisessa ovat salausanalyysit, kuten salauksen turvallisuutta koskevat todisteet.

Kun tiedossa on, että jokin protokolla ei ole turvallinen (esimerkiksi SSLv3), tämä on otettava huomioon; sama koskee tiettyihin salausprotokolliin kohdistuneita tunnettuja hyökkäyksiä sekä toimenpiteitä, joita hyökkäyksiä vastaan on otettu käyttöön, jos näitä protokollia käytetään.

Kun todentamismekanismissa hyödynnetään salausratkaisua, on huomioon otettava paitsi salausprimitiivit, myös protokollat ja ympäristö, etenkin avainten hallinta.

> *Esimerkki: Tyypillinen avainten hallinnassa käytettävä mekanismi on julkisen avaimen infrastruktuurin (Public Key Infrastructure, PKI) käyttäminen. Varmenneviranomaisen toiminnan tietoturva vaikuttaa suoraan todentamismekanismin turvallisuuteen paitsi varmenneviranomaisen puhtaasti teknisen tietoturvan, myös organisatoristen näkökohtien osalta.*
>
> *Jos sähköisen tunnistamisen järjestelmän tiettyjä osia koskevien varmenteiden myöntäjinä on useita luotettuja varmenneviranomaisia, on huomioon otettava kaikkien luotettujen varmenneviranomaisten yleinen tietoturvan taso.*
>
> *Esimerkkinä viimeksi mainitusta on tilanne, jossa viestinnän alku- ja loppupisteiden tunnistamisessa käytetään internet-PKI:stä peräisin olevia varmenteita eli varmenteita, joiden myöntäneiden varmenneviranomaisten juurivarmenne on käyttäjän selaimen luotettujen varmenteiden luettelossa. Tässä tapauksessa on otettava huomioon kaikkien luotettujen varmenteiden luettelossa olevien varmenneviranomaisten tietoturva. Hyvien toimintatapojen mukaista yleensä on, että jos sähköisen tunnistamisen järjestelmän infrastruktuurissa käytetään internet-PKI:tä, silloin korkea varmuustaso edellyttää, että käyttäjälle suositellaan riittävien turvamekanismien käyttämistä.*
>
> *Todentamisella olisi suojattava todentamistietoja sellaiselta manipuloinnilta, jonka tarkoitus on saada henkilö uskomaan, että todentaminen annetaan toiselle luottavalle osapuolelle.*

2.4 Hallinto ja organisointi

Kaikilla osallistujilla, jotka tarjoavat sähköiseen tunnistamiseen liittyvää rajat ylittävää palvelua (jäljempänä ”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.

OHJE:

Kaikkiin osallistujiin kuuluvat rajat ylittävän todentamisprosessin osapuolet, mukaan lukien tunnistustietojen tarjoaja ja jäsenvaltion käyttämät validointipalvelut (jos sellaisia on), mutta eivät käytetyt luotettavat lähteet.

Riskienhallinnassa yleisenä periaatteena on, että organisaation on itsensä valittava, minkä tasoista riskiä se pitää hyväksyttävänä. Kohdan 2.4 vaatimuksella muutetaan tätä yleistä periaatetta, sillä sen mukaan organisaation turvatoimenpiteiden on oltava suhteutettuja riskeihin kulloisellakin tasolla.

Suuri(n) osa tämän kohdan vaatimuksista täyttyy, jos

- käytössä on standardin ISO/IEC 27001:2013 mukainen auditoitu tietoturvallisuuden hallintajärjestelmä, tai

- operatiivisten palveluiden tuottajat ovat eIDAS-asetuksen mukaisia hyväksyttyjä luottamuspalveluiden tarjoajia.

Tämä ei kuitenkaan estä hyödyntämästä muita normeja, esimerkiksi soveltuvia kansallisia järjestelmiä, jotka täyttävät tämän kohdan vaatimukset.

Selvitys standardin ISO/IEC 27001:2013 vaatimuksista sekä hyväksyttyjä luottamuspalveluiden tarjoajia koskevista vaatimuksista annetaan vaatimusten soveltamista koskevien ohjeiden mukana [päätetään myöhemmin]. Standardin ISO/IEC 27001:2013 mukaista tietoturvallisuuden hallintajärjestelmää käytettäessä kyseisen standardin turvatoimenpiteet kattavat kaikki kohtien 2.4.4–2.4.6 vaatimukset.

2.4.1 Yleiset säännökset

MATALA

1. Palveluntarjoajat, jotka tarjoavat tämän asetuksen soveltamisalaan kuuluvaa operatiivista palvelua, ovat viranomaisia tai jäsenvaltion lainsäädännössä tunnustettuja oikeushenkilöitä, joilla on vakiintunut organisaatio ja jotka ovat täysin toiminnallisia kaikilla palvelujen tarjoamisen kannalta merkityksellisillä toimintalohkoilla.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2. Tarjoajat täyttävät kaikki oikeudelliset vaatimukset, jotka koskevat niitä liittyen palvelun harjoittamiseen ja tarjoamiseen, mukaan lukien niiden tietojen luokat, joita voidaan pyytää, henkilöllisyyden todistamistavat sekä tiedot, joita voidaan säilyttää, ja ajanjaksot, joiden ajan niitä voidaan säilyttää.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

3. Palveluntarjoajat voivat osoittaa valmiutensa ottaa vahinkovastuuriski, ja niillä on riittävät taloudelliset varat turvata toiminnan jatkuminen ja palvelujen tarjoaminen.

OHJE:

Voidaan olettaa, että julkisella viranomaisella on riittävät taloudelliset varat asetuksesta johtuvan vastuun kantamiseksi. Muita tapoja, joilla tämän vaatimuksen täyttyminen voidaan osoittaa, ovat esimerkiksi

- asianmukainen velvoitteita koskeva vakuutusturva
- julkisen viranomaisen kanssa solmittu sopimus, joka kattaa velvoitteet
- julkisen viranomaisen lakiin perustuva velvollisuus kantaa tarpeen vaatiessa vastuu tai ottaa toiminta omalle vastuulleen.

4. Palveluntarjoajat ovat vastuussa mahdollisten muille tahoille ulkoistettujen sitoumusten täyttämisestä ja järjestelmän toimintaperiaatteiden noudattamisesta samalla tavoin kuin jos palveluntarjoajat olisivat suorittaneet tehtävät itse.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

5. Sähköisen tunnistamisen järjestelmille, jotka eivät perustu kansalliseen lakiin, on oltava tehokas suunnitelma järjestelmän päättämisen varalta. Tällaisen suunnitelman on sisällettävä palvelun hallittu lopettaminen tai siirto toiselle palveluntarjoajalle, tapa ilmoittaa tästä asiaankuuluville viranomaisille ja loppukäyttäjille sekä tiedot siitä, miten järjestelmään kirjatut tiedot suojataan, säilytetään ja hävitetään järjestelmän toimintaperiaatteiden mukaisesti.

OHJE:

Tämä koskee sekä palvelun lopettamista että sen sulkemista ulkopuolisten viranomaisten taholta. Tällaisten suunnitelmien on katettava kaikki ennakoitavissa olevat olosuhteet, jotka saattavat johtaa palvelun lopettamiseen tai sen siirtämiseen toiselle palveluntarjoajalle.

2.4.2 Julkaistut ilmoitukset ja käyttäjätiedot

MATALA

1. Käytössä on julkaistu palvelun määritelmä, joka sisältää kaikki sovellettavat ehdot, edellytykset ja maksut, mukaan lukien mahdolliset käyttörajoitukset. Palvelun määritelmään on sisällytettävä tietosuojaperiaatteet.

OHJE:

Julkaisusta voidaan huolehtia seuraavilla tavoilla:

- tieto on kirjattu lakiin
- tieto annetaan saataville julkisesti saatavana olevissa asiakirjoissa.

2. Käytössä on asianmukaiset toimintaperiaatteet ja menettelyt sen varmistamiseksi, että palvelun käyttäjille ilmoitetaan hyvissä ajoin ja luotettavasti kaikista muutoksista palvelun määritelmässä ja sovellettavissa ehdoissa, edellytyksissä ja tietosuojaperiaatteissa kulloisenkin palvelun osalta.

OHJE:

Käyttäjä on järjestelmän aktiivinen osallistuja. Tilaaja voi olla myös hakija ennen sähköisen tunnistamisen menetelmän myöntämistä (ja tarvittaessa aktivointia).

Tässä yhteydessä ilmoittaminen ei tarkoita vain sitä, että tieto on aina suunnattava suoraan käyttäjälle. Vaatimuksessa tarkoitetusta ilmoittamisesta voidaan huolehtia myös julkaisemalla tarvittavat tiedot tarjoajan verkkosivulla muutoksen sisällön ja kansallisen lainsäädännön mukaisesti.

3. Käyttöön on otettava asianmukaiset toimintaperiaatteet ja menettelyt, jotta voidaan antaa asianmukaiset ja täydelliset vastaukset tietopyyntöihin.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

2.4.3 Tietoturvallisuuden hallinta

MATALA

Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.

OHJE:

Tietoturvaan kohdistuvien riskien hallinta koskee kaikkia sähköisen tunnistamisen järjestelmän osa-alueita. Toimivassa tietoturvallisuuden hallintajärjestelmässä otetaan huomioon järjestelmän kaikkiin osa-alueisiin kohdistuvat riskit.

Sähköisen tunnistamisen järjestelmän organisaatiorakenteen perusteella voi olla tarpeen käyttää useita tietoturvallisuuden hallintajärjestelmiä eri komponenteista vastaaville toimijoille.

KOROTETTU

Taso ”matala” lisättynä seuraavalla:

Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.

OHJE:

Standardi ISO/IEC 27001:2013 on tunnettu ja toimivaksi osoittautunut tietoturvaan kohdistuvien riskien hallintaa koskeva normi. Katso myös kohta 2.4.7, jossa käsitellään toimintaperiaatteiden noudattamisesta huolehtimista.

2.4.4 Tietojen säilyttäminen

MATALA

1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt.

OHJE:

Jos tietoja säilytetään, on tiedonhallintajärjestelmällä varmistettava, että tietojen eheys ja luottamuksellisuus säilyvät läpi niiden koko käyttöajan.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.12 ”Operational security” (etenkin kohdan A.12.4 ”Logging and monitoring”) sekä kohdan A.18 ”Compliance” mukaisia turvatoimenpiteitä.

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.

OHJE:

Kirjanpidosta, etenkin kiistattomuusasioissa käytettävästä, huolehditaan riittävän kauan kansallisessa lainsäädännössä määrätyn tai sallitun mukaisesti, jotta kirjanpitoa voidaan hyödyntää mahdollisissa erimielisyystapauksissa tai oikeusprosesseissa. Kun kirjanpitoa ei enää tarvita, se on hävitettävä asianmukaisesti. Tämä koskee kaikkia tietovälineitä, joille kirjanpitoa on tallennettu, niin sähköisessä kuin painetussa muodossa olevia.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.18 ”Compliance” (vertaa kohta A.18.1.3) mukaisia turvatoimenpiteitä.

2.4.5 Tilat ja henkilökunta

MATALA

1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä.

OHJE:

Jos henkilöstöltä edellytetään todistettua osaamista, on käytössä oltava koulutusohjelma, jolla varmistetaan, että henkilöstö pystyy osoittamaan taitonsa ja ylläpitämään niitä.

Esimerkkejä:
Fyysisiä asiakirjoja (esimerkiksi passeja ja henkilökortteja) tarkastavaa henkilöstöä koskevien hyvien toimintatapojen mukaisia vaatimuksia voivat olla esimerkiksi seuraavat:
Matala

- *Tiedostaa, että asiakirjapetoksia tapahtuu.*
- *Kykenee täsmällisesti ja johdonmukaisesti tarkistamaan, onko asiakirjoissa poikkeavuuksia, kuten kirjoitusvirheitä, erilaisia kirjasintyyppejä, puuttuvia sivuja tai epäjohdonmukaisuuksia asiakirjan asettelussa ja kohdentamisessa.*

Korotettu

- *On saanut asiakirjaväärennösten havaitsemista koskevaa koulutusta, jossa on hyödynnetty kansallisesti tunnustettuja, laadukkaita koulutusmateriaaleja.*
- *Kykenee tunnistamaan muutetut asiakirjat/laminointipinnan.*
- *Kykenee tunnistamaan yleisimmät painotekniikat.*

Suuri

- *Tuntee hyvin käytännön tasolla asiakirjojen mallit ja niiden turvaominaisuudet.*
- *On asianmukaisen koulutuksen kautta oppinut tuntemaan erilaiset vesileimat, turvakuidut ja painotekniikat.*
- *Kykenee asiakirjojen tarkastelun perusteella tunnistamaan väärennetyt ja tekaistut asiakirjat.*
- *Kykenee käyttämään tehokkaasti viitemateriaaleja.*

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.7 ”Human resource security” (vertaa etenkin kohta A.7.2.2) mukaisia turvatoimenpiteitä.

2. Käytössä on riittävästi henkilöstöä ja alihankkijoita, jotta palvelua voidaan toteuttaa ja resursoida asianmukaisesti sen toimintaperiaatteiden ja menettelyjen mukaisesti.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.12 ”Operations security” (vertaa kohta A.12.1.2 ”Capacity management”) mukaisia turvatoimenpiteitä, joissa otetaan huomioon myös henkilöstöresurssien kapasiteetti.

3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.

OHJE:

Turvallisuuden kannalta kriittisten palveluiden, kuten voimassaolon peruuttamisen, olisi siedettävä katkoksia ja keskeytyksiä. Palvelut olisi riittävällä tavalla suojattava katkoksilta ja yksittäiseen tilaan vaikuttavilta luonnonilmiöiltä, kuten tulipaloilta, tulvilta, myrskyiltä ja maanjäristyksiltä.

Tarvittaessa tiloista olisi tehtävä myös fyysisesti turvalliset hyödyntämällä asianmukaisia lukituksia, kulunvalvontajärjestelmiä ja fyysisiä valvontajärjestelmiä (esimerkiksi valvontakameroita). Tämä voidaan toteuttaa myös palveluna, sillä edellytyksenä ei ole, että palvelun tarjoaja suorittaa itse kaikki toimenpiteet.

Käytössä on oltava valvontamenettely luvattoman käytön varalta ja mahdollisuus tehdä palvelussa hälytyksiä, jos luvatonta käyttöä ilmenee.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.11 ”Physical and environmental security” ja A.9 ”Access control” mukaisia turvatoimenpiteitä. Seurantamekanismit huomioidaan myös osana kohdan A.12 ”Operations security” mukaisia turvatoimenpiteitä.

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.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.9 ”Access control” (jonka erityisenä tavoitteena on rajoittaa pääsyä tietoihin ja tiloihin, joissa tietoja käsitellään), A.10 ”Cryptography” ja A.18.1.5 ”Regulation of cryptographic controls” mukaisia turvatoimenpiteitä.

2.4.6 Tekniset tarkastukset

MATALA

1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.

OHJE:

On tärkeää pitää erillään luottamuksellisuuden ja eheyden suojaamista koskevien vaatimusten arviointi. Eheyden (tai aitouden) suojaaminen määräytyy periaatteessa varmuustason mukaan, mutta henkilöihin liittyvän tiedon luottamuksellisuuteen vaikuttavat myös tietojen tyyppi sekä mahdolliset suojaamista koskevat lainsäädännölliset vaatimukset.

Henkilötietojen luottamuksellisuus on suojattava ja käytössä on oltava turvatoimenpiteitä, jotka pohjautuvat riskiperusteista lähestymistapaa hyödyntävään arviointiin valitun tietoturvallisuuden hallintajärjestelmän mukaisesti. Turvatoimenpiteiden kattamia osa-alueita ovat esimerkiksi tietomurrot, väärinkäytökset, palvelunestohyökkäykset ja hajautetut palvelunestohyökkäykset.

Henkilötietojen luottamuksellisuutta ja aitoutta/eheyttä rajat ylittävissä siirroissa käsitellään yhteentoimivuusjärjestelmää koskevassa täytäntöönpanoasetuksessa.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.10 ”Cryptography”, (saatavuutta koskevan kohdan) A.12 ”Operations security”, A.17 ”Information security aspects of business continuity management” ja A.18.1.5 ”Regulation of cryptographic controls” mukaisia turvatoimenpiteitä.

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

OHJE:

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

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

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

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

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.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.9 ”Access control” ja A.10 ”Cryptography” mukaisia turvatoimenpiteitä.

4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.14 ”Security in development and support processes” ja A.16 ”Information security incident management” mukaisia turvatoimenpiteitä.

5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.8 ”Asset management” mukaisia turvatoimenpiteitä.

KOROTETTU

Taso ”matala” lisättynä seuraavalla:

Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.

OHJE:

Arkaluonteisella salausteknisellä aineistolla tarkoitetaan avainaineistoja, joita käytetään sähköisen tunnistamisen menetelmien myöntämisessä, käyttäjien todentamisessa ja vakuutusten myöntämisessä (tarvittaessa). Tällaisten salausavainten suojaaminen on ensiarvoisen tärkeää sähköisen tunnistamisen järjestelmän turvallisuuden kannalta.

Luvattomalta käsittelyltä suojautumiseen tarkoitetuilla mekanismeilla pyritään estämään salausavainaineistojen julkistaminen, muuttaminen tai väärinkäyttö koko niiden elinkaaren ajan. Tätä varten avainten suojaamisessa käytetään sekä fyysisiä että loogisia turvatoimenpiteitä.

Yleisenä käytäntönä on, että turvatoimenpiteet toteutetaan osana laitteiston turvamoduulia (HSM). Tarkoituksen täyttävissä tuotteissa käytettyjen turvamekanismien on oltava läpinäkyviä, ja niiden on oltava parhaiden laatua ja turvallisuutta koskevien standardien mukaisia. Turvallisuussertifiointi toimii lisätodisteena ja on hyvä toimintatapa laitteiston turvamoduulin laadun arvioinnissa. Sertifiointi voidaan tehdä esimerkiksi Criteria Recognition Arrangement (CCRA) -järjestelyn, Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOGIS-MRA) -sopimuksen ja/tai FIPS-140-normin mukaisesti. Tuotteet hankitaan luotetuilta myyjiltä ja alkuperäketjusta huolehditaan tuotteen valmistuksesta aina turvamoduulin tuotantokäyttöön ottamiseen saakka.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.10 ”Cryptography” ja A.11 ”Physical and environmental security” mukaisia turvatoimenpiteitä.

2.4.7 Noudattaminen ja tarkastus

MATALA

Määräajoin tehdään sisäisiä tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

OHJE:

Tarkastuksissa huomioidaan järjestelmään/järjestelmän osiin liittyvä riskitaso. Tämä tarkoittaa, että tarkastuksen perinpohjaisuus saattaa eri varmuustasoilla olla hyvinkin erilainen.

Sisäistä tarkastusta koskeva vaatimus voidaan täyttää myös käyttämällä ulkopuoliselta hankittua tarkastusta. Tasolla ”matala” ei vaadita riippumatonta tarkastusta (riippumattoman määritelmästä tarkemmin jäljempänä).

Tietoturvallisuuden hallintajärjestelmää koskevassa tarkastuksessa tavanomaisena menettelynä on, että kaikki järjestelmän osat käydään läpi kolmen vuoden aikana, mihin sisältyvät myös vuosittain toistuvat valvontatarkastukset.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.18 ”Compliance” (vertaa kohta A.18.2, ”Information security review”) mukaisia turvatoimenpiteitä.

KOROTETTU

Määräajoin tehdään riippumattomia sisäisiä tai ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

OHJE:

Tarkastus, joka hoidetaan sisäisesti organisaation omien normien mukaisesti ja jonka tulokset ilmoitetaan ensisijaisesti organisaation omalle johdolle, on hyväksyttyjen määritelmien mukaisesti sisäinen tarkastus (silloinkin, kun mukana on ulkopuolelta hankittua osaamista). Sisäisen tarkastuksen tekee objektiivisesti riippumaton tarkastustoiminto, ja se voi toimia pohjana organisaation itsensä antamalle vakuutukselle siitä, että sovellettavia määräyksiä on noudatettu. Tarkastus olisi tehtävä siten, että tarkastettavan toiminnon esimiehet eivät osallistu siihen, jotta tulosten vääristymiseltä ja eturistiriidoilta vältytään.

Ulkopuolisella (kolmannen osapuolen suorittamalla) tarkastuksella tarkoitetaan tarkastuksia, jotka tekee riippumaton tarkastusorganisaatio, kuten sääntelyviranomainen tai sertifiointitaho. Tavoitteena on arvioida tarkastettavaa organisaatiota suhteessa tiettyihin periaatteisiin ja kriteereihin ja antaa lausunto siitä, onko johdon vakuutus kyseisten periaatteiden täyttymisestä perusteltu. Ulkopuolisessa tarkastuksessa tarvitaan yleensä tarkastusstandardia, joka voi olla esimerkiksi auditointistandardi SFS-ISO/IEC 27007 tai AICPAn/CICAn kehittämä SysTrust/WebTrust-standardi.

Standardissa SFS-EN ISO 19011 on johtamisjärjestelmien auditointia koskevia ohjeita, mukaan lukien sisäisen ja ulkopuolisen tarkastuksen periaatteet sekä ohjeita siitä, miten tarkastusprosessiin osallistuvien henkilöiden osaamista voidaan arvioida.

KORKEA

1. Määräajoin tehdään riippumattomia ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

OHJE:

Tämä vaatimus voidaan täyttää standardin SFS-ISO/IEC 27007 mukaisella auditoinnilla tai todentamisella.

2. Jos järjestelmää hallinnoi suoraan julkinen elin, tarkastukset tehdään kansallisen lainsäädännön mukaisesti.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.