

Luottamuskehys

– ruotsalainen sähköinen tunniste

Versio 4.10.2022

1. Tausta ja tarkoitus

Ruotsalaista sähköistä tunnistetta koskevan luottamuskehyksen tavoitteena on vahvistaa yhteiset vaatimukset Ruotsin digihallintoviraston (DIGG) tarkastamien ja hyväksymien sähköisten tunnisteiden tarjoajille. Vaatimukset on jaettu eri suojaustasoihin – varmuustasoihin – sen mukaan, mikä on tarjoajan teknisen ja toiminnallisen turvallisuuden taso ja millä varmuudella henkilö, jolle sähköinen tunnistusväline tarjotaan, on todella se, joka hän väittää olevansa.

Luottamuskehyksen vaatimuksia sovelletaan varmuustasoihin 2–4, ja taso 4 vastaa korkeinta suojaustasoa.

Vaatimustenmukaisuutta tulkitaan seuraavasti:

- (a) jos varmuustasoa ei ole määritetty, vaatimus on täytettävä kaikilla tasoilla, ja
- (b) jos varmuustaso määritetään, vaatimustenmukaisuus on varmistettava vähintään asiaankuuluvalla tasolla.

Vaatimuksia, jotka on asetettu kyseistä tasoa alemmalle tasolle, ei oteta huomioon.

2. Organisaatio ja hallinto

Yleiset toiminnalliset vaatimukset

- K2.1 Jos ruotsalaisten sähköisten tunnisteiden tarjoajat eivät ole julkisia elimiä, niiden on harjoitettava toimintaansa rekisteröityinä oikeushenkilöinä ja otettava liiketoiminnan edellyttämä vakuutus ja pidettävä se voimassa.
- K2.2 Ruotsalaisten sähköisten tunnisteiden tarjoajilla on oltava vakiintunutta liiketoimintaa, niiden toiminnan on katettava kaikki tässä asiakirjassa määritetyt osa-alueet ja niiden on tunnettava hyvin oikeudelliset vaatimukset, jotka niille on asetettu ruotsalaisten sähköisten tunnisteiden tarjoajina.
- K2.3 Ruotsalaisten sähköisten tunnisteiden tarjoajilla on oltava valmiudet kantaa vahingonkorvausvelvollisuuteen liittyvä riski, ja niillä on oltava riittävät taloudelliset resurssit toimintansa harjoittamiseen vähintään vuoden ajan.

Tietoturva

K2.4 Ruotsalaisten sähköisten tunnisteiden tarjoajien on perustettava luottamuskehysten soveltamisalaan kuuluvia toimintansa osa-alueita varten tietoturvallisuuden hallintajärjestelmä, joka perustuu soveltuvin osin standardiin ISO/IEC 27001 tai vastaaviin tietoturvatyön hallintaa ja valvontaa koskeviin periaatteisiin, mukaan lukien seuraavat:

- (a) Kaikki turvallisuuden kannalta kriittiset hallinnolliset ja tekniset prosessit on dokumentoitava, ja niiden lähtökohtana on oltava virallinen perusta, jossa määritetään selvästi tehtävät, vastuut ja valtuudet.
- (b) Ruotsalaisten sähköisten tunnisteiden tarjoajien on varmistettava, että niillä on aina riittävät henkilöresurssit velvoitteidensa täyttämiseksi.
- (c) Ruotsalaisten sähköisten tunnisteiden tarjoajien on otettava käyttöön riskinhallintaprosessi, jossa analysoidaan liiketoiminnan uhkia ja haavoittuvuuksia asianmukaisella tavalla jatkuvasti tai vähintään 12 kuukauden välein ja jossa riskejä tasapainotetaan hyväksyttävälle tasolle ottamalla käyttöön turvatoimenpiteitä.
- (d) Ruotsalaisten sähköisten tunnisteiden tarjoajien on otettava käyttöön poikkeamien hallintaprosessi, jolla varmistetaan järjestelmällisesti palvelun laatu, jatkoraportoinnin muodot ja se, että tällaisista tapahtumista aiheutuvien vahinkojen lieventämiseksi tai ehkäisemiseksi toteutetaan asianmukaisia reaktiivisia ja ehkäiseviä toimenpiteitä.
- (e) Ruotsalaisten sähköisten tunnisteiden tarjoajien on laadittava jatkuvuussuunnitelma, joka täyttää liiketoiminnan saavutettavuusvaatimukset ja mahdollistaa kriittisten prosessien palauttamisen kriisitilanteessa tai vakavien poikkeamien yhteydessä, ja testattava sitä säännöllisesti.
- (f) Ruotsalaisten sähköisten tunnisteiden tarjoajien on säännöllisesti arvioitava tietoturvatyötä ja toteutettava kehitystoimia hallintajärjestelmässä.

K2.5 Hallintajärjestelmän soveltamisala ja kypsyysaste:

Taso 4: Tietoturvallisuuden hallintajärjestelmän on oltava standardin SS-ISO/IEC 27001:2017 tai vastaavien myöhempien tai kansainvälisten versioiden mukainen, ja sen on katettava kaikki ruotsalaisten sähköisten tunnisteiden tarjoajille asetetut vaatimukset.

Alihankintaa koskevat ehdot

- K2.6 Ruotsalaisten sähköisten tunnisteiden tarjoajan, joka on ulkoistanut yhden tai useamman turvallisuuden kannalta kriittisen prosessin suorittamisen toiselle osapuolelle, on määritettävä sopimuksella, mistä kriittisistä prosesseista alihankkija on vastuussa ja mitä vaatimuksia niihin sovelletaan, ja selvennettävä sopimussuhde tarjoajan ilmoituksessa.

Asiakirjojen jäljitettävyys, poistaminen ja säilyttäminen

- K2.7 Ruotsalaisten sähköisten tunnisteiden tarjoajien on säilytettävä
- (a) hakemusasiakirjat ja sähköisten tunnisteiden myöntämiseen, vastaanottamiseen tai sulkemiseen liittyvät asiakirjat;
 - (b) sopimukset, periaateasiakirjat ja tarjoajan ilmoitukset; ja
 - (c) käsittelyhistoria ja muut asiakirjat, joita tarvitaan osoittamaan ruotsalaisten sähköisten tunnisteiden tarjoajille asetettujen vaatimusten noudattaminen ja joiden avulla voidaan toteuttaa seurantaa ja osoittaa, että turvallisuuden kannalta kriittiset prosessit ja valvontatoimet ovat käytössä ja tehokkaita.
- K2.8 Säilytysajan on oltava vähintään viisi vuotta, ja aineisto on voitava tuottaa luettavassa muodossa koko tämän ajan, paitsi jos tietojen poistamista koskeva vaatimus on tarpeen yksityisyyden kannalta ja se on perusteltua lainsäädännön tai muun määräyksen nojalla.

Uudelleentarkastelu ja seuranta

- K2.9 Ruotsalaisten sähköisten tunnisteiden tarjoajien on perustettava sisäinen tarkastustoiminto, joka tarkastelee säännöllisesti tarjoamistoimintaa. Sisäisen tarkastajan on hoidettava tehtäviään riippumattomasti tavalla, jolla varmistetaan objektiivinen ja puolueeton tarkastelu, ja hänellä on oltava tehtäviensä hoitamisen edellyttämä pätevyys ja kokemus. Sisäisen tarkastajan on suunniteltava tarkastuksen suorittaminen riippumattomasti ja dokumentoitava se tarkastussuunnitelmaan, joka kattaa kolmen vuoden jakson. Tarkastuskohteet on valittava riski- ja olennaisuusanalyysin perusteella, ja niiden on perustuttava toimintakuvauksiin, jotka tarjoaja toimittaa digihallintovirastolle.

Tasot 3 ja 4: Sisäinen tarkastus on suoritettava hyväksytyjen tarkastusstandardien mukaisesti.

3. Fyysinen, hallinnollinen ja henkilöihin liittyvä turvallisuus

- K3.1 Toiminnan keskeiset osat on suojattava fyysisesti ympäristöön liittyvien tapahtumien, luvattoman pääsyn tai muiden ulkoisten häiriöiden aiheuttamilta vahingoilta. Kulunvalvontaa on sovellettava siten, että pääsy arkaluonteisille alueille sallitaan vain valtuutetulle henkilöstölle, tietovälineitä säilytetään ja ne hävitetään turvallisesti ja pääsyä suojatuille alueille valvotaan jatkuvasti.
- K3.2 Ennen kuin henkilö valitaan johonkin K2.4 kohdan a alakohdan mukaisesti yksilöityyn rooliin, joka on erityisen tärkeä turvallisuuden kannalta, ruotsalaisten sähköisten tunnisteiden tarjoajan on tehtävä taustaselvitykset sen varmistamiseksi, että henkilöä voidaan pitää luotettavana ja että henkilöllä on tarvittava pätevyys ja koulutus, jotta hän voi suorittaa roolistaan johtuvat tehtävät turvallisesti ja varmasti.
- K3.3 Tarjoajilla on oltava menettelyt sen varmistamiseksi, että ainoastaan erikseen valtuutetulla henkilöstöllä on pääsy K2.7 kohdan mukaisesti kerättyihin ja säilytettyihin tietoihin.
- K3.4 **Tasot 3 ja 4:** Tarjoajien on varmistettava koko tarjoamisprosessin ajan, että tehtävät erotetaan toisistaan siten, ettei yksikään henkilö voi saada sähköistä tunnistetta toisen henkilön nimissä.

4. Tekninen turvallisuus

- K4.1 Ruotsalaisten sähköisten tunnisteiden tarjoajien on varmistettava, että käytössä olevat tekniset valvontatoimet ovat riittäviä, jotta saavutetaan liiketoiminnan luonteeseen, laajuuteen ja muihin olosuhteisiin nähden tarpeelliseksi katsottu suojaustaso, ja että nämä valvontatoimet toimivat ja ovat tehokkaita.

- K4.2 Arkaluonteisten tietojen siirtämiseen käytettävät sähköiset viestintävälineet on suojattava sieppaukselta, muuttamiselta ja toistolta.
- K4.3 Sähköisten tunnisteiden tarjoamiseen, haltijoiden tunnistamiseen ja tunnistusvälineiden tarjoamiseen käytettävä arkaluonteinen salausavainaineisto on suojattava siten, että
- (a) pääsyä rajoitetaan loogisesti ja fyysisesti vain niihin rooleihin ja käyttötarkoituksiin, jotka ovat ehdottoman välttämättömiä;
 - (b) avainaineistoa ei koskaan tallenneta pysyvälle tallennusvälineelle selkotekstinä;
 - (c) avainaineisto suojataan käyttämällä salauslaitteistomodulia, jonka aktiiviset turvamekanismit torjuvat sekä fyysisiä että loogisia avainaineiston varastamisyrityksiä;
 - (d) avainaineiston suojaamiseen käytettävät turvamekanismit ovat avoimia ja perustuvat tunnustettuihin ja vakiintuneisiin standardeihin; ja
 - (e) **Tasot 3 ja 4:** avainaineiston suojauksen aktivointitietoja hallitaan useaan henkilöön perustuvalla valvonnalla.
- K4.4 Tarjoajilla on oltava dokumentoidut menettelyt, joilla varmistetaan, että vaadittua suojaustasoa asianomaisessa tietoteknisessä ympäristössä voidaan pitää yllä ajan mittaan ja muutosten yhteydessä, mukaan lukien säännölliset haavoittuvuusarviointit ja asianmukainen valmius vastata muuttuviin riskitasoihin ja ilmeneviin poikkeamiin.

5. Hakemus, tunnistaminen ja rekisteröinti

Ehtoja koskevat tiedot

- K5.1 Ruotsalaisten sähköisten tunnisteiden tarjoajien on annettava tietoa sopimuksista, ehdoista ja niihin liittyvistä tiedoista sekä mahdollisista palvelun käyttöä koskevista rajoituksista liitetyille käyttäjille, sähköisten palvelujen tarjoajille ja muille tarjoajan palveluun mahdollisesti luottaville.
- K5.2 Ruotsalaisten sähköisten tunnisteiden tarjoajan on selkeästi viitattava ehtoihin ja suunniteltava menettelyt siten, että ehdot toimitetaan hakijalle tarjoamisprosessin aikana.
- K5.3 Ruotsalaisten sähköisten tunnisteiden tarjoajien on annettava tarjoajan ilmoitus, johon on sisällytettävä seuraavat:
- (a) tarjoajan henkilöllisyys ja yhteystiedot,
 - (b) lyhyet kuvaukset tarjoajan tarjoamista palveluista ja ratkaisuihin, mukaan lukien hakemiseen, myöntämiseen ja sulkemiseen sovellettavat menetelmät,
 - (c) tarjottuun palveluun liittyvät ehdot, mukaan lukien käyttäjän velvollisuudet suojella sähköistä tunnistettaan, tarjoajan velvollisuudet ja vastuut sekä annetut takuut ja luvattu käytettävyyys,
 - (d) tiedot henkilötietojen käsittelystä ja tavasta, jolla käsittely suoritetaan, ja
 - (e) järjestelyt tarjotun palvelun ehtojen tai muiden ehtojen muuttamiseksi, mukaan lukien toimenpiteet, jotka on toteutettava palvelun lopettamiseksi hallitusti.
- K5.4 **Tasot 3 ja 4:** Ruotsalaisten sähköisten tunnisteiden tarjoajien on digihallintoviraston (DIGG) tai muun tarjoajan palveluja käyttävän sopimuspuolen pyynnöstä annettava tietoa yrityksen omistussuhteista ja hallinnosta.
- K5.5 Ruotsalaisten sähköisten tunnisteiden tarjoajan, joka lopettaa toimintansa, on noudatettava ennalta laadittua suunnitelmaa palvelun lopettamiseksi. Suunnitelmaan on sisällyttävä tiedottaminen kaikille palvelun käyttäjille ja DIGG-virastolle. Tarjoajan on lisäksi pidettävä arkistoitu aineisto saatavilla K2.7 ja K2.8 kohdan mukaisesti myös lopettamisen jälkeen.

Hakeminen

K5.6 Ruotsalainen sähköinen tunniste voidaan myöntää ainoastaan hakijan pyynnöstä tai muulla vastaavalla hyväksymismenettelyllä ja vasta sen jälkeen, kun hakijalle on ilmoitettu tunnisteiden tarjoamisen edellytyksistä ja hakijalle asetettavasta vastuusta.

Jos sähköisellä tunnisteella korvataan saman tarjoajan aiemmin myöntämä voimassa oleva tai äskettäin suljettu sähköinen tunnistusväline tai täydennetään saman tarjoajan aiemmin myöntämää voimassa olevaa tai äskettäin suljettua sähköistä tunnistusvälinettä, tunniste voidaan kuitenkin tarjota ilman edeltävää hakumenettelyä.

K5.7 Ruotsalaista sähköistä tunnistetta koskevaan hakemukseen on liitettävä henkilötunnus tai väliaikainen henkilötunnus sekä tiedot, jotka tarjoaja yleisesti tarvitsee tämäntyyppisen sähköisen tunnisteiden tarjoamiseksi.

Hakijan henkilöllisyyden toteaminen

K5.8 Ruotsalaisten sähköisten tunnisteiden tarjoajien on varmistettava, että hakemukseen liitetyt tiedot ovat täydelliset ja vastaavat viralliseen rekisteriin kirjattuja tietoja.

K5.9 Jos virallisesta rekisteristä tarkastettavat tiedot on merkitty luottamuksellisiksi (niin kutsuttu suojattu henkilöllisyys), tarvittavat tarkastukset voidaan tehdä muilla vastaavilla menetelmillä.

K5.10 Hakijan tunnistaminen henkilökohtaisen käynnin aikana:

Ruotsalaisten sähköisten tunnisteiden tarjoajat voivat tarkistaa hakijan henkilöllisyyden henkilökohtaisen käynnin aikana samalla tavalla kuin myöntäessään tavanomaisen henkilöllisyydestodistuksen.

K5.11 Hakijan etätunnistaminen olemassa olevassa suhteessa:

Taso 3: Jos ruotsalaisten sähköisten tunnisteiden tarjoajat ovat jo tunnistaneet hakijan suhteessa, johon liittyy taloudellisesti tai oikeudellisesti merkittäviä tapahtumia, tai jos hakija voidaan tunnistaa etäyhteydellä muilla luotettavilla menetelmillä, jotka vastaavat ruotsalaisten sähköisten tunnisteiden tason 3 vaatimuksia, ruotsalaisten sähköisten tunnisteiden tarjoajat voivat käyttää tätä menetelmää hakijan henkilöllisyyden toteamiseen.

Taso 4: Ei sovelleta.

K5.12 Tunnistaminen ruotsalaisen sähköisen tunnisteiden avulla:

Ruotsalaisten sähköisten tunnisteiden tarjoaja voi etätunnistaa hakijan aiemmin myönnettyllä voimassa olevalla ruotsalaisella sähköisellä tunnisteella, jonka varmuustaso on vähintään sama kuin myönnettävän sähköisen tunnisteiden varmuustaso, jos tarjoaja voi ilman sopimusperusteisia esteitä käyttää tällaista tunnistamista myöntääkseen uuden sähköisen tunnisteiden.

Taso 4: Uuden sähköisen tunnisteiden voimassaoloaika ei saa olla pidempi kuin aiemmin myönnetyn sähköisen tunnisteiden voimassaoloaika.

K5.13 Hakijan etätunnistaminen:

Taso 2: Ruotsalaisten sähköisten tunnisteiden tarjoajat voivat todeta hakijan henkilöllisyyden etänä käyttämällä tähän luotettavaa kuvatallennetta voimassa olevasta vakiomuotoisesta henkilöllisyydestodistuksesta sekä hakijan kasvokuvaa, jos vertailu ei anna aihetta epäillä hakijan todellista henkilöllisyyttä.

Taso 3: Ruotsalaisten sähköisten tunnisteiden tarjoajat voivat sähköisesti tallennettuja biometrisiä tietoja sisältävän voimassa olevan vakiomuotoisen henkilöllisyydestodistuksen suojatun lukemisen avulla todeta hakijan

henkilöllisyyden etänä kyseisten tietojen perusteella, jos tunnistettavan henkilön vastaavat biometriset tiedot voidaan kerätä riittävän turvallisella tavalla niin, että tietoja voidaan vertailla yhtä luotettavasti kuin henkilökohtaisen käynnin yhteydessä, ja jos vertailu ei anna aiheutta epäillä hakijan todellista henkilöllisyyttä.

Taso 4: Ei sovelleta.

Rekisteröinti

- K5.14 Ruotsalaisten sähköisten tunnisteiden tarjoajien on – henkilötietojen suojaan koskevat sovellettavat säännöt huomioon ottaen – pidettävä rekisteriä liitettyistä käyttäjistä ja osoitetuista sähköisistä tunnistusvälineistä ja pidettävä rekisteri ajan tasalla.

6. Sähköisen tunnisteen myöntäminen ja sulkeminen

Teknisten apuvälineiden suunnittelu

K6.1 Tekniset apuvälineet:

Tasot 2 ja 3: Tekniset apuvälineet, joita käytetään sähköiseen tunnistamiseen sähköisellä tunnisteella, jolla on ruotsalaista sähköistä tunnistetta koskeva laatumerkintä (Svensk e-legitimation), on suunniteltava kaksivaiheiseksi siten, että yhtenä osana ovat sähköisesti tallennetut tiedot, jotka ovat käyttäjän hallussa, ja yhtenä osana jokin, mitä käyttäjän on käytettävä sähköisen tunnisteiden aktivoimiseksi.

Taso 4: Tekniset apuvälineet, joita käytetään sähköiseen tunnistamiseen sähköisellä tunnisteella, jolla on ruotsalaista sähköistä tunnistetta koskeva laatumerkintä (Svensk e-legitimation), on suunniteltava kaksivaiheiseksi siten, että yhtenä osana on henkilökohtainen turvamuodi, joka on käyttäjän hallussa, ja yhtenä osana jokin, mitä käyttäjän on käytettävä turvamuodin aktivoimiseksi.

K6.2 Aktivointimekanismi ja henkilökohtainen koodi on suunniteltava siten, että on epätodennäköistä, että kolmannet osapuolet voisivat murtaa suojauksen edes mekaanisesti.

Tasot 3 ja 4: Suojaukseen on sisällytettävä mekanismeja, joilla estetään sähköisen tunnistusvälineen kopiointi ja muuttaminen.

K6.3 Jos käyttäjän sähköisellä tunnisteella on ruotsalaista sähköistä tunnistetta koskeva laatumerkintä (Svensk e-legitimation), käyttäjän on voitava omasta aloitteestaan sähköisen tunnisteiden voimassaoloaikana vaihtaa tai pyytää uutta henkilökohtaista koodia maksutta ja ilman merkittävää haittaa, ja käyttäjää on autettava ohjeistuksen tai automaattisten kommentojen avulla huolehtimaan siitä, että K6.2 kohdan vaatimukset täyttyvät.

Jos sähköinen tunniste on suunniteltu siten, että henkilökohtaista koodia ei voida vaihtaa, käyttäjän on sen sijaan voitava samoin edellytyksin saada viipymättä uusi sähköinen tunniste ja uusi henkilökohtainen koodi, joilla korvataan aiemmat toteuttamalla sulkumenettely.

K6.4 Ruotsalaisten sähköisten tunnistusten tarjoajien on varmistettava, että haltijoiden sähköiseksi tunnistamiseksi rekisteröitävät tiedot edustavat hakijaa yksilöllisesti ja että ne osoitetaan kyseiselle henkilölle, kun sähköinen tunniste myönnetään.

K6.5 Tarjottujen sähköisten tunnistusten voimassaoloaikaa on rajoitettava ottaen huomioon sähköisen tunnistusvälineen turvaominaisuudet ja väärinkäytön riskit. Sähköisen tunnisteiden enimmäisvoimassaoloaika on viisi vuotta.

Sähköisen tunnistusvälineen toimittaminen

K6.6 Etätoimitus:

Taso 2: Ruotsalaisten sähköisten tunnisteiden tarjoajan on toimitettava sähköinen tunnistusväline tavalla, jolla varmistetaan virallisessa rekisterissä olevat yhteystiedot tai yhteystiedot, jotka on kirjattu K5.13 kohdassa kuvatun tason 2 mukaisen sähköisen menettelyn yhteydessä.

Taso 3: Ruotsalaisten sähköisten tunnisteiden tarjoajan, joka toimittaa sähköisen tunnisteiden K5.11 kohdassa kuvatun tason 3, K5.12 kohdassa kuvatun tason 3 tai K5.13 kohdassa kuvatun tason 3 mukaisella sähköisellä menettelyllä, on uutta tunnistetta myöntäessään varmistettava, että käyttäjälle ilmoitetaan erikseen ja turvallisuuden kannalta toimituksesta riippumatta, että tämäntyyppinen sähköinen tunnistusväline on toimitettu, tai tarjoajan on muilla toimenpiteillä valvottava vastaavalla tasolla, että henkilö on tietoinen toimittamiseen liittyvästä identiteettivarkauden riskistä.

Taso 4: Ruotsalaisten sähköisten tunnisteiden tarjoajan, joka toimittaa sähköisen tunnisteiden K5.12 kohdassa kuvatun tason 4 mukaisella sähköisellä menettelyllä, on uutta tunnistetta myöntäessään varmistettava, että käyttäjälle ilmoitetaan erikseen ja turvallisuuden kannalta toimituksesta riippumatta, että tällainen sähköinen tunnistusväline on luovutettu.

K6.7 Toimittaminen henkilökohtaisen käynnin aikana:

Ruotsalaisten sähköisten tunnisteiden tarjoajan on henkilökohtaisen käynnin aikana ja K5.10 kohdan mukaisen henkilöllisyyden tarkastamisen jälkeen toimitettava sähköinen tunnistusväline allekirjoitettua vastaanottotodistusta vastaan, ja toimitettava lisäksi osa, jota käyttäjän on käytettävä sähköisen tunnisteiden aktivointiin, erillään ja turvallisuuden kannalta sähköisen tunnistusvälineen toimittamisesta riippumatta käyttäen virallisessa rekisterissä olevia yhteystietoja tai muita yhtä luotettavia tietoja.

Sulkupalvelu

- K6.8 Ruotsalaisten sähköisten tunnisteiden tarjoajien on tarjottava sulkupalvelu, joka on helposti käyttäjän saatavilla, jotta hän voi sulkea sähköisen tunnisteensa.
- K6.9 Ruotsalaisten sähköisten tunnisteiden tarjoajien on käsiteltävä ja toimeenpantava sulkupyynnöt nopeasti ja turvallisesti sekä toteutettava toimenpiteitä, joilla estetään sulkupalvelun järjestelmällinen väärinkäyttö tai muut tahalliset toimet, jotka johtavat sähköisten tunnistusvälineiden laajamittaiseen sulkemiseen, ja varmistettava, että käyttäjien sähköiset tunnisteet ovat käytettävissä, kun niitä tarvitaan.

7. Haltijoiden sähköisten tunnisteiden todentaminen

- K7.1 Ruotsalaisten sähköisten tunnisteiden tarjoajien on varmistettava, että haltijan henkilöllisyyden todentamisen yhteydessä tehdään luotettavia tarkastuksia, jotka koskevat sähköisen tunnistusvälineen aitoutta ja voimassaoloa.
- K7.2 Ruotsalaisten sähköisten tunnisteiden tarjoajien on varmistettava, että haltijoiden sähköisiä tunnisteita todennettaessa on toteutettu teknisiä turvallisuustarkastuksia niin, että on epätodennäköistä, että kolmannet osapuolet voivat arvaamalla, salakuuntelemalla, toistamalla tai prosessia manipuloimalla murtaa suojaimekanismit.

8. Tunnistusvälineiden myöntäminen

Myös niiden ruotsalaisten sähköisten tunnisteiden myöntäjien, jotka tarjoavat tunnistusvälineiden myöntämiseen liittyvää palvelua luottaville sähköisille palveluille, on noudatettava tämän kohdan säännöksiä.

K8.1 Ruotsalaisten sähköisten tunnisteiden tarjoajien on varmistettava, että tunnistusvälineiden tarjoamispalvelu on helposti käytettävissä ja että tunnistusvälineiden myöntämistä edeltää luotettava tunnistaminen 7 kohdan säännösten mukaisesti.

Taso 4: Välineissä on viitattava salausavainaineistoon, jonka tarjoaja on varmistanut olevan yksinomaan haltijan hallussa.

K8.2 Toimitetut tunnistusvälineet ovat voimassa vain niin kauan kuin on tarpeen, jotta käyttäjällä on pääsy pyydettyyn sähköiseen palveluun, ja tunnistusvälineet on suojattava siten, että ainoastaan aiottu vastaanottaja voi lukea tiedot ja että välineiden vastaanottajat voivat todentaa välineiden aitouden.

K8.3 Ruotsalaisten sähköisten tunnisteiden myöntäjien on – tunnistuspalvelun väärinkäytön riskit huomioon ottaen – rajoitettava ajanjaksoa, jonka kuluessa tietylle haltijalle voidaan tarjota useita peräkkäisiä tunnistusvälineitä ennen kuin haltija tunnistetaan uudelleen 7 kohdan säännösten mukaisesti.