

# SÄHKÖISEN TUNNISTAMISEN KEHITTÄMISRYHMÄ

## VAHVAN SÄHKÖISEN TUNNISTAMISEN KANSALLISET LINJAUKSET SUOMESSA:

1. Suomeen luodaan edellytykset toimivien vahvan sähköisen tunnistamisen markkinoiden syntymiselle. Markkinoille tunnusomaista on tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu.
2. Keskeisenä edellytyksenä vahvan tunnistamisen markkinoiden syntymiselle ja toimimiselle on osapuolten välinen tehokkaasti toimiva yhteistyö. Tarvitaan avoimia yhteistyöjärjestelyjä, joita edistetään tarvittaessa aktiivisesti. Samalla huolehditaan siitä, etteivät yhteistyöjärjestelyt estä kilpailua.
3. Sähköisessä tunnistamisessa erotetaan toisistaan vahva ja heikko tunnistaminen. Lainsäädännöllä säännellään vahvan sähköisen tunnistamisen palveluiden tarjonnan puitteet.
4. Vahvan tunnistamisen luotettavuus perustuu käytettyyn menetelmään, palvelumallin turvallisiin ja auditoitaviin prosesseihin ja toteutustapoihin, lainsäädännössä vahvan sähköisen tunnistamisen palveluiden tarjoamiselle asetettaviin perusedellytyksiin, vahvan tunnistamisen palvelua tarjoavien ja sitä käyttävien palveluntarjoajien muodostamaan luottamusverkostoon sekä viranomaisvalvontaan. Näin toteutettu vahva sähköinen tunnistaminen soveltuu lähtökohtaisesti kaikkeen luotettavaan sähköiseen tunnistamiseen niin yksityisellä kuin julkisellakin sektorilla.
5. Käyttäjien luottamus vahvan sähköisen tunnistamisen palveluihin edellyttää lisäksi, että vahvaa tunnistamista tarjoavat ja käyttävät palveluntarjoajat huolehtivat kuluttajansuojaa ja yksityisyyden suojaa koskevien säännösten huolellisesta noudattamisesta.
6. Yksityisen ja julkisen sektorin palveluntarjoajat hankkivat tarvitsemansa sähköisen tunnistamisen palvelut toimivilta vahvan sähköisen tunnistamisen palveluiden markkinoilta. Palveluntarjoajat voivat valita ne vahvan tunnistamisen palvelut, joita käyttävät. Julkinen valta ei rajoita tätä valinnan mahdollisuutta joitakin erityisiä poikkeuksia lukuun ottamatta.
7. Vahvan sähköisen tunnistamisen palveluiden tarjonta perustuu käyttäjälähtöisyyteen. Jokainen käyttäjä voi valita itselleen sopivimman tunnistamismenetelmän markkinoilla tarjolla olevista vahvan tunnistamisen vaihtoehdoista. Tavoitteena on, että jokainen käyttäjä voi käyttää itselleen sopivinta vahvan sähköisen tunnistamisen menetelmää mahdollisimman monessa tunnistamista tarvitsevassa palvelussa. Samalla on kuitenkin otettava huomioon edellinen linjaus.
8. Oikeustoimi voidaan saada aikaan sähköisessä maailmassa sähköisen allekirjoituksen lisäksi myös vahvan tunnistamisen välineillä, jos osapuolet niin haluavat.
9. Sähköinen tunnistaminen ei ole itse tarkoitus vaan luotettavan sähköisen asioinnin mahdollistaja. On olemassa myös sellaisia palveluita, joissa tunnistaminen ei ole lainkaan tarpeen. Vahvaa sähköistä tunnistamista käyttävien palveluntarjoajien on erotettava ne palvelut, joissa tunnistaminen on tarpeen.
10. Suomi pyrkii aktiivisesti edistämään näitä periaatteita myös EU-tasolla ja kansainvälisillä tasoilla.

## **Linjaukset perusteluineen:**

**1. Suomeen luodaan edellytykset toimivien vahvan sähköisen tunnistamisen markkinoiden syntymiselle. Markkinoille tunnusomaista on tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu.**

### **Perustelut:**

Näiden linjausten tavoitteena on ilmaista ne peruseriaatteet, joille vahva sähköinen tunnistaminen Suomessa perustuu. Linjausten tavoitteena ei ole toimintaohjelman laatiminen. Toimivien markkinoiden aikaan saamisessa nämä linjaukset muodostavat yhden askeleen eteenpäin. Työtä on jatkettava tulevana vuosina usealla eri saralla, ja erityisesti arjen tietoyhteiskunnan neuvottelukunnan alaisessa sähköisen tunnistamisen kehittämissäryhmässä.

Sähköinen tunnistaminen on monien sähköisten palveluiden ja sähköisen asioinnin palveluiden mahdollistaja. Myös nämä linjaukset on nähtävä mahdollistajana. Ne eivät siis pakota vahvan sähköisen tunnistamisen palvelun tarjoajia tai käyttäjiä eivätkä loppukäyttäjiä sen paremmin sähköisen tunnistamisen kuin yleisesti sähköisten palveluidenkaan käyttöön tai tarjontaan.

Linjaukset muodostavat yhden kokonaisuuden. Yksittäisistä linjauksista käy ilmi erilaisia tulokulmia vahvaan sähköiseen tunnistamiseen, ja vain yhdessä niiden muodostama kuva on kokonainen. Linjauksia on siksi myös luettava kokonaisuutena.

Kansalaiset alkavat vähitellen tottua sähköisiin palveluihin ja sähköiseen asiointiin. Ne ovat mukavuudeltaan yliverkaisia, koska asioita voi hoitaa paikasta ja kellonajasta riippumatta ilman jonottamista. Tämän johdosta sähköisen palveluiden kysyntä tulee jatkossa kasvamaan huomattavasti. Myös palveluiden kirjo kasvaa, mikä lisää tarvetta luotettavaan sähköiseen tunnistamiseen. Toimivat sähköiset palvelut ja sähköisen asioinnin palvelut sekä niihin liitetyt vahvan sähköisen tunnistamisen palvelut on tarjottava niille kansalaisille, jotka haluavat ottaa ne käyttöön. Luonnollisesti on huolehdittava myös sellaisten kansalaisten palveluista, jotka eivät ole valmiita sähköiseen maailmaan. Kehitys ei kuitenkaan voi tapahtua vasta siinä vaiheessa, kun kaikki ovat valmiita uusiin palvelumalleihin. Muussa tapauksessa tietoyhteiskuntakehityksemme hidastuu huomattavasti.

Linjausten ensimmäisessä kohdassa todetaan, että sähköisen tunnistamisen edistäminen Suomessa edellyttää ennen kaikkea vahvan sähköisen tunnistamisen markkinoiden syntymistä. Näiden markkinoiden lähtökohtina ovat tunnistusvälineiden yleiskäyttöisyys ja vapaa kilpailu.

Sähköisen tunnistamisen kenttään liittyvät ongelmat ovat todennäköisesti osaltaan hidastaneet sähköisten palveluiden kehitystä maassamme. Sähköisen tunnistamisen ongelmat eivät kuitenkaan ole liittyneet tunnistusvälineisiin tai niiden puutteeseen, vaan ongelmana on ollut juuri toimivien markkinoiden puute.

Vahva tunnistaminen koostuu jostain, mitä käyttäjä 1) tietää (esimerkiksi käyttäjätunnus), 2) omistaa (esimerkiksi salasanalista tai kertakäyttöisiä tunnuksia generoiva laite, varmenne tai muu väline), tai 3) on (esimerkiksi sormenjälki). Vähintään kahden näistä vaatimuksista on toteuduttava samanaikaisesti, jotta tunnistustapahtuma täyttää vahvan tunnistamisen määritelmän.

Vahvalla sähköisellä tunnistamisella tarkoitetaan näissä linjauksissa luonnollisten henkilöiden tunnistamista. Luonnollinen henkilö voi edustaa oikeushenkilöä tai toista luonnollista henkilöä, mutta roolitiedon liittäminen tunnistamiseen tapahtuu tunnistamisprosessista erillisessä, vaikkakin mahdollisesti liitännäisessä prosessissa. Vahvalla tunnistamisella tarkoitetaan tässä edelleen toimijan

laajalle yleisölle kaupallisin perustein tarjoamia vahvan tunnistamisen palveluita. Linjaukset eivät sovellu suljetuille käyttäjäryhmille tarjottaviin vahvan tunnistamisen palveluihin. Esimerkkinä tällaisesta olisi yrityksen sisäisiin tarkoituksiin käytettävä tunnistaminen.

Tällä hetkellä kuluttajille suunnattuja vahvan tunnistamisen palveluita Suomessa tarjoavat pankit ja Väestörekisterikeskus (VRK). Vahvoista menetelmistä tällä hetkellä käytetyin on pankkien tarjoama Tupas-tunnistus. Tämän lisäksi käytössä on VRK:n tarjoamia PKI-järjestelmään pohjautuvia varmenteita. On oletettavaa, että toimiville vahvan sähköisen tunnistamisen markkinoille tulee muutama palveluntarjoaja. Vahvaa sähköistä tunnistamista tarjoavien palveluntarjoajien määrä jäänee joka tapauksessa rajalliseksi sen johdosta, että kyseessä on varsin pieni markkina.

Arjen tietoyhteiskunnan neuvottelukunnan alaisuuteen asetetun sähköisen tunnistamisen kehittämissuunnitelman piirissä on kuluvana vuonna 2008 pyritty edistämään mobiilitunnistamista erityisenä painopisteenä. Asiassa on edetty sellaiseen vaiheeseen, että uusien palveluiden ja palveluntarjoajien tuleminen markkinoille on mahdollista jo vuonna 2009.

**2. Keskeisenä edellytyksenä vahvan tunnistamisen markkinoiden syntymiselle ja toimimiselle on osapuolten välinen tehokkaasti toimiva yhteistyö. Tarvitaan avoimia yhteistyöjärjestelyjä, joita edistetään tarvittaessa aktiivisesti. Samalla huolehditaan siitä, etteivät yhteistyöjärjestelyt estä vapaata kilpailua.**

#### **Perustelut:**

Kansainväliset esimerkit muun muassa Turkista, Virosta ja Norjasta osoittavat, että niissä maissa, joissa sähköinen tunnistaminen on edennyt vertailumaita paremmin, on kyetty kahden tai useamman osapuolen välisiin toimiviin yhteistyöjärjestelyihin. Suomessa on perinteisesti ollut vahvuutena yksityisen ja julkisen sektorin yhteistyö. Nämä perinteet on syytä ottaa käyttöön myös vahvan sähköisen tunnistamisen osalta, sillä toimivien vahvan sähköisen tunnistamisen markkinoiden vaikutus tietoyhteiskuntakehityksemme hyödyttää voimakkaasti kaikkia osapuolia.

Toimivien markkinoiden toteuttamiseksi tarvitaan avoimia yhteistyöjärjestelyjä (nelikulmamalleja, federointiratkaisuja, operaattoreiden tunnistus-verkkovierailuratkaisuja, tms). Erityisesti tällaisten järjestelyjen aikaan saaminen edellyttää yhteistyötä. Markkinoille saattaa syntyä myös joitakin tunnistamis- tai todentamiskeskuskeskuksia tai tunnistamishubeja. Pidemmällä aikavälillä nämä ”hubit” saattavat toimia kansainvälisesti. Tällaisten yhteistyöjärjestelyjen syntymistä on tarvittaessa aktiivisesti edistettävä. Samalla on huolehdittava siitä, että yhteistyöjärjestelyt eivät estä vapaata kilpailua.

Sähköisen tunnistamisen kehittämissuunnitelman piirissä on vuonna 2008 edistetty pankkien nelikulmamallin syntymistä ja selvitetty todentamiskeskusmallin edellytyksiä. Mobiilitunnistamisselvityksen yhteydessä on nähty mobiilitunnistamisvälineet ja yhteensopivat tunnistamispalvelut luontevana osana myös operaattoripalveluita. Työtä vahvan sähköisen tunnistamisen seuraavien kehitysvaiheiden edistämiseksi on jatkettava vuosina 2009 ja 2010.

**3. Sähköisessä tunnistamisessa erotetaan toisistaan vahva ja heikko tunnistaminen. Lainsäädännöllä säännellään vahvan sähköisen tunnistamisen palveluiden tarjonnan puitteet.**

Kuten kohdassa 1 todettiin, vahvoista menetelmistä tällä hetkellä käytetyin on pankkien tarjoama Tupas-tunnistus. Tämän lisäksi käytössä on Väestörekisterikeskuksen tarjoamia PKI-järjestelmään pohjautuvia varmenteita. Mobiilivarmenteiden tuloa markkinoille helpottaa se, että niitä on jo käy-

tössä yritystunnistamisessa. Heikon tunnistamisen menetelmistä käytetyin on käyttäjätunnus-salasanapari.

Yhdellä luonnollisella henkilöllä voi olla vain yksi todellinen henkilöllisyys, joka on yhteydessä henkilöön oikeussubjektina. Heikossa tunnistamisessa henkilö voi niin sanotusti luoda itselleen tai hänelle voidaan luoda useita sähköisiä ”identiteettejä”, jotka voivat myös poiketa henkilön todellisista ominaisuuksista. Henkilö voi antaa virheellistä tietoa esimerkiksi iästään tai sukupuolestaan.

Sen sijaan vahvalle tunnistamiselle on ominaista, että tunnistamisväline ja sen käyttö voidaan aina viime kädessä yhdistää henkilön todelliseen henkilöllisyyteen. Näin siitä huolimatta, että vahvaa sähköistä tunnistamista käyttävälle palveluntarjoajalle ei palvelun käytön yhteydessä ilmoitettaisi todellisia henkilötietoja (anonyymi käyttö). Myös vahvassa tunnistamisessa henkilöllä voi olla useita rooleja, joissa hän toimii, ja häneen voidaan liittää eri palveluissa vaihtelevia määriä henkilöistä kertovia tietoja. Henkilöllä voi kuitenkin olla yksi ainoa identiteetti, jonka Suomessa luo valtio.

Edellisessä kappaleessa sanottua voidaan Suomessa entisestäänkin tehostaa sillä, että vahvan tunnistamisen välineeseen sisällytetään henkilön yksilöivänä tunnisteena HETU (henkilötunnus) tai SATU (sähköinen asiointitunnus). Parhaillaan eduskunnassa käsiteltävänä olevassa väestötietolain kokonaisuudistuksessa tehdyt nykytilaa muuttavat ratkaisut mahdollistavat sen, että varmentajat voivat varmenteissaan käyttää SATUa. HETUn käyttö muissa vahvan tunnistamisen välineissä on mahdollista henkilötietolain puitteissa. Vahvaa sähköistä tunnistamista tarjoavia palveluntarjoajia on rohkaistava HETUn tai SATUn käyttöön henkilötietoja koskevan sääntelyn huomioon ottaen tiedottamisen, sääntelyn ja muiden tarpeellisten keinojen avulla.

Vahvaa sähköistä tunnistamista suoranaisesti koskevaa lainsäädäntöä ei ole voimassa toistaiseksi Suomessa eikä muuallakaan Euroopassa. Kuitenkin tarve palveluiden tarjonnan sääntelylle on suuri, jotta vahvan sähköisen tunnistamisen luotettavuudella olisi tarpeellinen ja pitävä pohja. Liikenne- ja viestintäministeriössä on parhaillaan käynnissä lainsäädäntöhanke, jolla nykyinen sähköisistä allekirjoituksista annettu laki korvattaisiin lailla vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Laki on tarkoitus valmistella siten, että se voisi tulla voimaan jo vuoden 2009 aikana.

Heikkona tunnistamisena pidettyjä tunnistamismenetelmiä ei kannata pyrkiä sääntelemään lainsäädäntöteitse. Sähköisen tunnistamisen kehittämissuunnan työssä myös niiden käytettävyyttä ja tietoturvasuutta voidaan tulevina vuosina pyrkiä erilaisin keinoin parantamaan.

**4. Vahvan tunnistamisen luotettavuus perustuu käytettyyn menetelmään, palvelumallin turvallisiin ja auditoitaviin prosesseihin ja toteutustapoihin, lainsäädännössä vahvan sähköisen tunnistamisen palveluiden tarjoamiselle asetettaviin perusedellytyksiin, vahvan tunnistamisen palvelua tarjoavien ja sitä käyttävien palveluntarjoajien muodostamaan luottamusverkostoon sekä viranomaisvalvontaan. Näin toteutettu vahva sähköinen tunnistaminen soveltuu lähtökohtaisesti kaikkeen luotettavaan sähköiseen tunnistamiseen niin yksityisellä kuin julkisella sektorilla.**

#### **Perustelut:**

Sähköisille palveluille ja sähköiselle asioinnille on ominaista se, että osapuolten kesken tarvitaan luottamusta. Tämän takia vahvan tunnistamisen palvelun tarjoajien ja niiden palveluiden on oltava luotettavia. Tässä kohdassa luetellaan ne seikat, jotka tekevät vahvasta tunnistamisesta luotettavan. Viittauksella lainsäädäntöön tarkoitetaan edellisessä kohdassa mainittua liikenne- ja viestintäminis-

teriössä käynnissä olevaa hanketta, jolla nykyinen sähköisistä allekirjoituksista annettu laki korvataisiin lailla vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista. Yhtenä tärkeänä yksityiskohtana laissa on tarkoitus säännellä vahvan sähköisen tunnistamisen välineen hakijan henkilöllisyyden tarkistamista tunnistetta haettaessa.

Suomalaisessa järjestelmässä sekä mahdollinen vahvan sähköisen tunnistamisen välineiden tai menetelmien luokittelu että luokittelun hyväksi käyttäminen on jätettävä markkinoiden, eli vahvan tunnistamisen palveluita tarjoavien ja käyttävien palveluntarjoajien sekä loppukäyttäjien omaan harkintaan. Lainsäädännön tasolla Suomessa riittää jako heikkoon (käytännössä sääntelemättömään) ja vahvaan (säänneltyyn) tunnistamiseen.

### **5. Käyttäjien luottamus vahvan sähköisen tunnistamisen palveluihin edellyttää lisäksi, että vahvaa tunnistamista tarjoavat ja käyttävät palveluntarjoajat huolehtivat kuluttajansuojaa ja yksityisyyden suojaa koskevien säännösten huolellisesta noudattamisesta.**

Kuten edellisessä kohdassa todetaan, sähköisille palveluille ja sähköiselle asioinnille ominaista on kysymys luottamuksesta. Palveluntarjoajan ja käyttäjän on voitava luottaa toisiinsa. Palveluntarjoajan kannalta luottamuksessa on usein kyse juuri luotettavasta sähköisestä tunnistamisesta. Käyttäjän kannalta luottamuksen syntymisen edellytyksenä 4 kohdassa mainittujen seikkojen lisäksi on se, että vahvan sähköisen tunnistamisen palveluita tarjoavat ja käyttävät palveluntarjoajat huolehtivat myös kuluttajansuojaa ja yksityisyyden suojaa koskevien säännösten huolellisesta noudattamisesta. Vahvan sähköisen tunnistamisen edistäminen auttaa myös identiteettivarkauksien torjunnassa.

### **6. Yksityisen ja julkisen sektorin palveluntarjoajat hankkivat tarvitsemansa sähköisen tunnistamisen palvelut toimivilta vahvan sähköisen tunnistamisen palveluiden markkinoilta. Palveluntarjoajat voivat valita ne vahvan tunnistamisen palvelut, joita käyttävät. Julkinen valta ei rajoita tätä valinnan mahdollisuutta joitakin erityisiä poikkeuksia lukuun ottamatta.**

#### **Perustelut:**

Palveluntarjoajilla niin julkisella kuin yksityiselläkin sektorilla on oltava valinnan vapaus. Olennaista asiassa on se, että julkisen vallan taholta tätä mahdollisuutta ei rajoiteta mahdollisesti joitakin hyvin harvoja poikkeuksia lukuun ottamatta. Edellytyksenä on joka tapauksessa tällöinkin oltava, että poikkeukset ovat objektiivisia, avoimia, suhteellisia ja syrjimättömiä, ja ne saavat liittyä vain kyseessä olevan palvelun erityispiirteisiin.

Julkisella sektorilla tähän valinnan mahdollisuuteen saattaa kohdistua joitakin rajoituksia voimassa olevan lainsäädännön johdosta. Huomioon saattaa tapauksesta riippuen tulla otettavaksi esimerkiksi kilpailulainsäädännöstä, julkisista hankinnoista tai sähköisestä asioinnista viranomaisessa annettua lainsäädäntöä. Edelleen on otettava huomioon, että valtiovarainministeriö ohjaa julkishallinnon sähköisissä asiointipalveluissa käytettyjä tunnistusratkaisuja. Myös VAHTI antaa suosituksia ja ohjeita. On huomattava, että tämäkin linjaus ei pakota palveluntarjoajia sen paremmin sähköisten palveluiden kuin vahvan sähköisen tunnistamisen palveluiden tarjoamiseen tai käyttöön.

Joissakin tapauksessa tilanne voi olla se, että toimijan tarvitsemia vahvan tunnistamisen menetelmiä tai välineitä tai niihin liittyviä palveluita ei ole saatavilla markkinoilta. Tällöin toimija voi joutua kehittämään tarvitsemansa välineen tai palvelun.

**7. Vahvan sähköisen tunnistamisen palveluiden tarjonta perustuu käyttäjälähtöisyyteen. Jokainen käyttäjä voi valita itselleen sopivimman tunnistamismenetelmän markkinoilla tarjolla olevista vahvan tunnistamisen vaihtoehdoista. Tavoitteena on, että jokainen käyttäjä voi käyttää itselleen sopivinta vahvan sähköisen tunnistamisen menetelmää mahdollisimman monessa tunnistamista tarvitsevassa palvelussa. Samalla on kuitenkin otettava huomioon edellinen linjaus.**

**Perustelut:**

Käyttäjänäkökulma tulee ottaa vahvan sähköisen tunnistamisen peruslähtökohdaksi myös käytännössä. Käyttäjien tulee voida valita käyttöönsä sellainen vahvan sähköisen tunnistamisen menetelmä, joka tuntuu itsestä parhaalta. Usein valinta perustuu johonkin käyttäjän aikaisempaan käyttötottumukseen. Tavoitteena on, että toimivilla markkinoilla tarjolla on muutama vaihtoehtoinen vahvan tunnistamisen väline, joiden joukosta erilaiset käyttäjät voivat löytää itselleen sopivimman.

Sähköisen tunnistamisen luonteva käyttö edellyttää sitä, että käyttäjille kertyy riittävästi ja toistuvasti käyttökokemuksia tunnistamismenetelmän käytöstä. Jos käyttäjiltä käytännössä vaaditaan usean sähköisen tunnistamisen välineen hallintaa, ei käyttökertoja voi välinettä kohti toteutua riittävästi käyttötottumuksen ja sitä kautta käytön mukavuuden takaamiseksi. Käyttäjä voi toki hankkia useamman välineen itse niin halutessaan.

Vahva sähköinen tunnistaminen on sekä käyttäjän että palveluntarjoajan kannalta turvallisempaa kuin heikon tunnistamisen käyttäminen. Esimerkiksi identiteettivarkaudet ovat vahvan sähköisen tunnistamisen menetelmissä helpommin torjuttavissa kuin heikon tunnistamisen menetelmissä. Myös sellaisissa palveluissa, jotka eivät itsessään välttämättä tarvitsisi vahvaa tunnistamista, tulee siksi viime kädessä pyrkiä siihen, että käyttäjät voisivat käyttää itselleen tuttua ja helppokäyttöistä vahvan tunnistamisen menetelmää. Tämän toteutumiseksi vahvan tunnistustapahtuman kustannustason täytyy olla riittävän edullinen kaikkien toimijoiden kannalta. Toimivien markkinoiden yhtenä tavoitteena onkin pitää hintataso kohtuullisena, mikä toteutuu markkinoilla riittävien vaihtoehtojen ollessa tarjolla.

Vaikka tavoitteena on se, että kukin käyttäjä voisi käyttää valitsemaansa vahvan tunnistamisen välinettä mahdollisimman monessa palvelussa, ei palveluntarjoajia voida kuitenkaan pakottaa hyväksymään jotakin välinettä tai vahvan sähköisen tunnistamisen palvelun tarjoajaa. Asiassa on siten huomioitava se, mitä edellisessä linjauksessa todettiin palveluntarjoajien mahdollisuudesta valita. Kuten kohdassa 1 todettiin, on oletettavaa, että vahvan sähköisen tunnistamisen palveluntarjoajien ja välineiden määrä jää joka tapauksessa rajalliseksi markkinoillamme. Tämän johdosta vahvaa sähköistä tunnistamista käyttävien palveluntarjoajien ja loppukäyttäjien intressien yhteen sovittamisesta ei myöskään muodostune ongelmaa.

**8. Oikeustoimi voidaan saada aikaan sähköisessä maailmassa sähköisen allekirjoituksen lisäksi myös vahvan tunnistamisen välineillä, jos osapuolet niin haluavat.**

**Perustelut:**

Käsitteellisesti on selkeästi erotettava toisistaan vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja oikeustoimien tekeminen sähköisesti. Vahvassa sähköisessä tunnistamisessa tunnistamispalvelua tarjoavat ja sitä käyttävät palveluntarjoajat muodostavat sopimussuhteen säännellyn verkoston. Sen sijaan sähköisessä allekirjoituksessa peruslähtökohta on se, että allekirjoituspalvelun tarjoaja ei ole sopimussuhteessa allekirjoitukseen luottavan osapuolen kanssa. Määritelmällisesti sähköallekirjoitusdirektiivin mukainen sähköinen allekirjoitus käsittää aina myös tunnistamisele-

mentin. Sähköallekirjoitusdirektiivin mukaan sähköisen allekirjoituksen määritelmä pyrkii olemaan teknologianeutraali, mutta käytännössä sillä tarkoitetaan lähes aina julkisen avaimen järjestelmään perustuvaa sähköistä allekirjoitusta.

Sähköisestä allekirjoituksesta on erotettava oikeustoimen tekemiseen tarvittava tahdonilmaisu. Tämä on erityisen tärkeää Suomessa, jossa hyvin harvaa oikeustointa koskevat tietyt muutovaatimukset. Mikäli oikeustoimi kiistetään, Suomessa vallitsee tuomioistuinten vapaa todistusharkinta. Oikeustoimen tekemiseen tarvittava tahdonilmaisu voidaan saada aikaan Suomessa sähköisen allekirjoituksen lisäksi myös vahvan tunnistamisen menetelmillä, mikäli osapuolet niin haluavat. Tällä tarkoitetaan sitä, että mitään osapuolta ei voida yleisesti tai tapauskohtaisesti pakottaa oikeustoimien tekemiseen vahvan tunnistamisen välineillä, mutta sellaista vaihtoehtoa haluaville on tarjottava siihen mahdollisuus. Loppukäyttäjän ja palveluntarjoajan yhdenvertaisuus asiassa on tärkeää. Palveluntarjoajan on huolehdittava muun muassa siitä, että käyttäjä on tosiasiallisesti tietoinen oikeustoimen tekemisestä sekä kaikista palveluun liittyvistä seikoista.

**9. Sähköinen tunnistaminen ei ole itse tarkoitus vaan luotettavan sähköisen asioinnin mahdollistaja. On olemassa myös sellaisia palveluita, joissa tunnistaminen ei ole lainkaan tarpeen. Vahvaa sähköistä tunnistamista käyttävien palveluntarjoajien on erotettava ne palvelut, joissa tunnistaminen on tarpeen.**

**Perustelut:**

Sähköisistä palveluista suuri osa on sellaisia, joissa sähköistä tunnistamista ei lainkaan tarvita. Asiassa on tapahtunut jonkin verran ylilyöntejä siten, että tunnistamista on vaadittu sellaisissakin palveluissa, joissa se ei olisi tarpeen.

Yksityisen sektorin palveluntarjoajien on syytä harkita, voitaisiinko heikkoa tunnistamista vähentää myös siten, että nykyistä useampi palvelu olisi käyttäjille avoin. Julkisen sektorin on erityispiirteidensä johdosta erotettava ne palvelut, joissa tunnistamista voidaan edellyttää.

**10. Suomi pyrkii aktiivisesti edistämään näitä periaatteita myös EU-tasolla ja kansainvälisillä tasoilla.**

**Perustelut:**

Suomen tulee aktiivisesti ajaa näitä periaatteita myös EU:ssa ja kansainvälisesti tehtävässä työssä. Keskeisiä vaikutuskanavia ovat DG DIGIT pääosaston IDABC-ohjelma ja DG INFOSOC pääosaston rahoittama STORK-hanke, jossa Suomi ei ole varsinaisena jäsenenä, mutta on sen seurantaryhmässä. Erityisesti STORKin kautta tulevat eurooppalaiset ratkaisut rajat ylittävään tunnistamiseen. Tavoitteena on, että olemassa olevaa kansallista infrastruktuuria voidaan hyödyntää, mutta tunnistusviestit kulkevat välityspalvelun kautta maasta toiseen.

Alan standardointi jatkuu ja uusien standardien päälle tullaan rakentamaan uusia ratkaisuja. Ne todennäköisesti tulevat pohjautumaan luottamusverkostoihin (eli federaatioihin). Tätä työtä tehdään esimerkiksi SEPAssa e-mandate tunnistautumisen sekä mobiilioperaattoreiden verkkovierailumallien parissa.