

**FI**

**FI**

**FI**



EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 28.11.2008  
KOM(2008) 798 lopullinen

**KOMISSION TIEDONANTO NEUVOSTOLLE, EUROOPAN PARLAMENTILLE,  
EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE SEKÄ ALUEIDEN  
KOMITEALLE**

**Sähköisiä allekirjoituksia ja sähköistä tunnistusta koskeva toimintasuunnitelma  
rajatylittävien julkisten palveluiden tarjonnan helpottamiseksi yhtenäismarkkinoilla**

**KOMISSIION TIEDONANTO NEUVOSTOLLE, EUROOPAN PARLAMENTILLE,  
EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE SEKÄ ALUEIDEN  
KOMITEALLE**

**Sähköisiä allekirjoituksia ja sähköistä tunnistusta koskeva toimintasuunnitelma  
rajatylittävien julkisten palveluiden tarjonnan helpottamiseksi yhtenäismarkkinoilla**

(ETA:n kannalta merkityksellinen teksti)

1.	Johdanto .....	3
1.1.	Toimintasuunnitelman sisältö .....	3
1.2.	Sähköisiä allekirjoituksia ja sähköistä tunnistusta koskeva nykyinen EU-kehys .....	4
1.2.1.	Sähköisiä allekirjoituksia koskeva direktiivi .....	4
1.2.2.	i2010-aloitteeseen kuuluva sähköisen hallinnon toimintasuunnitelma.....	5
1.3.	Sähköisten allekirjoitusten ja sähköisen tunnistuksen rajatylittävän yhteentoimivuuden parantaminen .....	5
2.	1 osa: Toimet sähköisten allekirjoitusten yhteentoimivuuden parantamiseksi .....	6
2.1.	Varmennetut sähköiset allekirjoitukset ja hyväksytyyn varmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset .....	7
2.2.	Kehittyneet sähköiset allekirjoitukset .....	9
3.	2 osa: Toimet sähköisen tunnistuksen yhteentoimivuuden parantamiseksi.....	11
4.	Seuranta ja toimeenpano .....	12

## 1. JOHDANTO

### 1.1. Toimintasuunnitelman sisältö

EU on osana Lissabonin strategiaa sitoutunut kehittämään oikeudellista ja hallinnollista ympäristöä liiketoimintapotentialin vapauttamiseksi. Julkishallintojen siirtyminen internetin käyttöön ja se, että yritykset ja yksityishenkilöt voivat viestiä sähköisesti julkishallintojen kanssa yli valtioiden rajojen, auttaa osaltaan luomaan ympäristöä, joka suosii yrittäjyyttä ja helpottaa kansalaisten yhteyksiä viranomaisiin.

Sähköisen viestinnän merkitys kasvaa koko ajan monilla talous- ja julkisen elämän aloilla. Viranomaiset eri puolilla Eurooppaa ovat ryhtyneet tarjoamaan sähköistä pääsyä julkishallinnon palveluihin. Näin tehdessään viranomaiset ovat enimmäkseen keskittyneet kansallisiin tarpeisiin ja välineisiin, mikä on johtanut erilaisiin ratkaisuihin ja monimutkaiseen järjestelmään. Tilanteeseen sisältyy riski siitä, että luodaan uusia esteitä rajatylittävälle markkinoille ja ehkäistään yhtenäismarkkinoiden toimivuutta yritysten ja kansalaisten kannalta.

Kun kyseessä on rajatylittävä pääsy julkishallinnon sähköisiin palveluihin, suurimmat esteet liittyvät sähköisen tunnistuksen ja sähköisten allekirjoitusten käyttöön. Kuten ei-digitaalisessa ympäristössäkin, tietyt sähköiset menettelyt voivat edellyttää tunnistusta ja allekirjoituksia. Näin ollen pääsy julkishallinnon sähköisiin menettelyihin merkitsee usein, että henkilöiden on osoitettava, keitä he ovat (eli hallinnolle on tarjouduttava mahdollisuus henkilöllisyys tarkastamalla varmistaa, että henkilöt ovat niitä, keitä he väittävät olevansa<sup>1</sup>). Hallinnon on myös sähköisen allekirjoituksen avulla pystyttävä tunnistamaan allekirjoittaja, ja sen on pystyttävä varmistamaan, etteivät toimitetut tiedot ole muuttuneet lähetyksen aikana). Suurin este on yhteentoimivuuden puute, olipa kyseessä sitten oikeudellinen, tekninen tai organisatorinen yhteentoimivuus.

Euroopan unionin nykyinen kehys tarjoaa horisontaalisia ja alakohtaisia välineitä sähköisten allekirjoitusten ja sähköisen tunnistuksen käytön helpottamiseksi ja kehittämiseksi. Sähköisiä allekirjoituksia koskevassa direktiivissä<sup>2</sup> säädetään sähköisten allekirjoitusten oikeudellisesta tunnustamisesta ja vahvistetaan oikeuskehys niiden yhteentoimivuuden edistämiseksi. Tällainen yhteentoimivuus edellyttää useiden käytännön, teknisten ja organisatoristen vaatimusten noudattamista.

Tehokasta yhteentoimivuutta tarvitaan lisäksi, jotta jäsenvaltiot voivat noudattaa EU:n muun lainsäädännön, varsinkin erityisten sisämarkkinavälineiden mukaisia oikeudellisia velvoitteitaan. Useissa sisämarkkina-aloitteissa ehdotetaan, että yritysten pitäisi pystyä käyttämään sähköisiä välineitä yhteydenotoissaan julkisiin laitoksiin, harjoittaessaan oikeuksiaan ja käydessään kauppaa yli rajojen.

---

<sup>1</sup> Tunnistusmenettelyssä käytetään hyväksi osapuolen ilmoitettuja tai havaittuja ominaisuuksia henkilöllisyyden päättelemiseksi. Ilmaisun ”tunnistus” sijasta voidaan myös puhua osapuolen todentamisesta (entity authentication). (*ModinisIDM Terminology paper*, <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc>).

<sup>2</sup> Direktiivi 1999/93/EY, EYVL L 13, 19.1.2000, s. 12, ja kertomus sähköisiä allekirjoituksia koskevista yhteisön puitteista annetun direktiivin toteuttamisesta, KOM(2006) 120 lopullinen.

Palveludirektiivi velvoittaa jäsenvaltiot varmistamaan vuoden 2009 loppuun mennessä<sup>3</sup>, että palveluntarjoajat voivat hoitaa sähköisesti ja etäältä kaikki palvelutoiminnan tarjoamiseen liittyvät menettelyt ja muodollisuudet. Tämä merkitsee muun muassa mahdollisuutta tunnistaa palveluntarjoajat yli rajojen ja todentaa toimitetut tiedot.

Julkisia hankintoja koskevien direktiivien<sup>4</sup> tarkoituksena on edistää sähköisten välineiden kehitystä ja käyttöä julkisia hankintoja koskevissa menettelyissä, mikä voisi tuoda yrityksille huomattavia säästöjä<sup>5</sup>. Jäsenvaltiot voivat säännellä sähköisten allekirjoitusten vaadittua tasoa sähköisiä allekirjoituksia koskevassa direktiivissä säädettyjen velvoitteiden mukaisesti, ja ne voivat määrätä hankintaviranomaiset hyväksymään ainoastaan varmennetut allekirjoitukset<sup>6</sup>.

Sähköinen laskutus eli laskutustietojen (veloitus ja maksaminen) sähköinen siirto liikekumppaneiden (toimittajan ja ostajan) välillä on olennainen osa tehokasta taloudellista toimitusketjua. Yhtenäisen euromaksualueen (SEPA) perustamisen ohessa valmistellaan sähköistä laskutusta koskevaa aloitetta, jonka pitäisi tuoda yrityksille lisäsäästöjä (Euroopan komissio on perustanut asiantuntijaryhmän, jonka tehtävänä on kehittää vuoteen 2009 mennessä sähköistä laskutusta koskevat eurooppalaiset oikeudelliset puitteet).<sup>7</sup>

Tämän toimintasuunnitelman tavoitteena on näin ollen tarjota sähköisiä allekirjoituksia ja sähköistä tunnistusta koskeva kattava ja käytännöllinen kehys, jolla yksinkertaistetaan yritysten ja kansalaisten pääsyä rajatylittäviin sähköisiin julkisiin palveluihin. Tämän tavoitteen saavuttamiseksi toimintasuunnitelmassa keskitytään käytännöllisiin, organisatorisiin ja teknisiin seikkoihin sekä täydennetään nykyistä oikeudellista kehystä.

## **1.2. Sähköisiä allekirjoituksia ja sähköistä tunnistusta koskeva nykyinen EU-kehys**

### *1.2.1. Sähköisiä allekirjoituksia koskeva direktiivi*

Sähköisiä allekirjoituksia koskeva direktiivi annettiin vuonna 1999 edistämään sähköisten allekirjoitusten oikeudellista hyväksymistä ja varmistamaan sähköisiin allekirjoituksiin liittyvien tuotteiden, laitteiden ja palvelujen vapaa liikkuvuus yhtenäismarkkinoilla. Sähköisten allekirjoitusten käytön oikeudellinen ja tekninen tarkastelu osoittaa kuitenkin, että yhteentoimivuudessa on ongelmia, jotka nykyisellään rajoittavat sähköisten allekirjoitusten

---

<sup>3</sup> Euroopan parlamentin ja neuvoston direktiivi 2006/123/EY, annettu 12 päivänä joulukuuta 2006, palveluista sisämarkkinoilla, 8 artikla. Palveludirektiivi on saatettava osaksi kansallista lainsäädäntöä 28. joulukuuta 2009 mennessä.

<sup>4</sup> Julkisia hankintoja koskevan direktiivin 2004/18/EY 42 artiklan 5 kohdan b alakohta ja liite X sekä julkisia hankintoja koskevan direktiivin 2004/17/EY 48 artiklan 5 kohdan b alakohta ja liite XXIV.

<sup>5</sup> Lisätietoja on saatavilla sähköisten julkisten hankintojen sääntelykehysten täytäntöönpanemisesta 13. joulukuuta 2004 esitetystä toimintasuunnitelmasta, KOM(2004) 841.

<sup>6</sup> Kun hankinta suoritetaan verkossa, hankintaviranomaisten on pystyttävä ottamaan vastaan ja käsittelemään sähköisiä tarjouksia yli valtioiden rajojen. Täydelliset sähköiset tarjoukset ovat monimutkaisia kokonaisuuksia, jotka sisältävät erilaisia sähköisesti allekirjoitettuja, eri lähteistä peräisin olevia ja eri kansallista alkuperää olevia teknisesti erimuotoisia asiakirjoja ja todistuksia, mukaan lukien oikeaksi todistetut käännökset (esimerkiksi todisteena palveluntarjoajan pätevyydestä). Tämä merkitsee, että päättäjien on harjoitettava monimutkaista sähköistä viestintää avoimessa piirissä, eli tietojen vastaanottaja (hankintaviranomainen) ei ennalta tunne kaikkia mahdollisia tietojen toimittajia (tarjoajia).

<sup>7</sup> Sähköistä laskutusta käsittelevä asiantuntijaryhmä on eritoten todennut, ettei sähköisiä allekirjoituksia koskevan kansallisen lainsäädännön hajanaisuus saisi estää sähköistä laskutusta. Tässä horisontaalisessa toimintasuunnitelmassa ei arvioida sähköisten allekirjoitusten vaikutuksia alv-sääntöjen noudattamiseen (laskujen sähköisiin allekirjoituksiin viitataan yhteisestä arvonnäköalajärjestelmästä annetussa neuvoston direktiivissä 2006/112/EY (233 artikla)). Toimintasuunnitelmassa ei myöskään arvioida sähköistä laskutusta, siihen liittyviä esteitä tai näiden esteiden poistamisen edellyttämiä toimia.

rajatylittävää käyttöä. Tarkastelussa korostuu, että tarvitaan tehokkaampaa vastavuoroista tunnustamista. Rajatylittävän yhteentoimivuuden puutteesta johtuva pirstoutuminen vaikuttaa todennäköisesti erityisesti sähköisen hallinnon palveluihin, jotka ovat nykyisin merkittävien sähköisiä allekirjoituksia käyttävä transaktiokanava.<sup>8</sup>

### *1.2.2. i2010-aloitteeseen kuuluva sähköisen hallinnon toimintasuunnitelma*

Rajatylittävässä sähköisessä tunnistuksessa ei ole vielä kukaan yhteisön välinettä, johon yhteisön tason toimet voitaisiin perustaa. Tästä huolimatta komissio tukee (sekä poliittisesti että taloudellisesti) toimia, joilla EU:n tasolla pyritään löytämään ratkaisuja yhteentoimivaan sähköiseen tunnistukseen. Euroopan komission 25. huhtikuuta 2006 antamassa i2010-aloitteeseen kuuluvassa sähköisen hallinnon toimintasuunnitelmassa<sup>9</sup> pidetään yhteentoimivaa sähköisen identiteetin hallintajärjestelmää (eIDM) keskeisenä toimintaedellytyksenä, kun kyseessä on pääsy julkisiin palveluihin. Jäsenvaltiot ovat tunnustaneet yhteentoimivan sähköisen identiteetin hallintajärjestelmän merkityksen sitoutuessaan selvästi varmistamaan, että ”vuoteen 2010 mennessä Euroopan kansalaiset ja yritykset voivat käyttää julkisia palveluja omassa maassaan tai jossakin muussa EU:n jäsenvaltiossa turvallisella ja helppokäyttöisellä, tietoturvamääräysten mukaisella sähköisellä tunnistautumismallilla, jonka he ovat paikallis-, alue- tai keskusviranomaiselta saaneet”.

### **1.3. Sähköisten allekirjoitusten ja sähköisen tunnistuksen rajatylittävän yhteentoimivuuden parantaminen**

Nykyisistä säännöksistä sekä jäsenvaltioiden ja komission tekemistä poliittisista sitoumuksista huolimatta tarvitaan yhteensovitetumpaa ja kattavampaa lähestymistapaa helpottamaan käytännössä sähköisen tunnistuksen ja sähköisten allekirjoitusten rajatylittävää käyttöä. Tämä on olennaista yhtenäismarkkinoiden pirstoutumisen välttämiseksi.

Sen vuoksi komissio ehdotti 20. marraskuuta 2007 antamassaan tiedonannossaan ”2000-luvun Euroopan yhtenäismarkkinat”, että laadittaisiin **sähköisiä allekirjoituksia ja sähköistä todentamista koskeva toimintasuunnitelma**<sup>10</sup>.

Tämän toimintasuunnitelman tavoitteena on auttaa jäsenvaltioita toteuttamaan vastavuoroisesti tunnustettuja ja yhteentoimivia sähköisten allekirjoitusten sekä sähköisen tunnistuksen ratkaisuja, jotta helpotettaisiin rajatylittävien julkisten palvelujen tarjoamista sähköisessä ympäristössä. Toimintasuunnitelma sisältää sähköisiä allekirjoituksia (1 osa) ja sähköistä tunnistusta (2 osa) koskevia erityisiä toimia. Vaikka toimintasuunnitelmassa keskitytään lähinnä sähköisen hallinnon sovelluksiin, myös yritysten sovellukset voivat hyötyä ehdotetuista toimista sikäli kuin käyttöönotettavia välineitä voidaan hyödyntää myös yritysten välisissä (B2B) sekä yritysten ja kuluttajien välisissä (B2C) liiketoimissa.

---

<sup>8</sup> Euroopan komissio valmistelelee myös hanketta, jolla helpotettaisiin sähköisten allekirjoitusten käyttöönottoa komission sisäisessä ja ulkoisessa viestinnässä. Hanke on nimeltään ”*Electronic Signature Service Infrastructure*” (ESSI), ja se on keskeisessä asemassa Euroopan komission menettelyjen muuttamisessa aineettomiksi, kuten asiakirjassa ”*Rules for the provisions on electronic and digitised documents*” (SEC(2005) 1578) edellytetään.

<sup>9</sup> i2010-aloitteeseen kuuluva sähköisen hallinnon toimintasuunnitelma – Vauhtia sähköiselle hallinnolle Euroopassa kaikkien hyväksi, KOM(2006) 173 lopullinen.

<sup>10</sup> Sähköisellä todentamisella tarkoitetaan tässä osapuolen todentamista eli sähköistä tunnistusta. Tässä asiakirjassa käytetään ilmaisua sähköinen tunnistus, jotta voidaan tehdä selkeä ero osapuolen todentamisen ja tietojen autenttisuuden todentamisen välillä.

Maaliskuussa 2008 pidetyssä kevään Eurooppa-neuvostossa valtioiden ja hallitusten päämiehet totesivat, että on hyvin tärkeää parantaa yhtenäismarkkinoiden toimintaa ottamalla käyttöön sähköisiä allekirjoituksia ja sähköistä todentamista koskevia rajatylittäviä yhteentoimivia ratkaisuja.

Komissio myötävaikuttaa jatkossakin siihen, että yhteentoimivuuteen liittyviin seikkoihin reagoidaan yhteensovitetulla tavalla, ja antaa jäsenvaltioille ja sidosryhmille ohjeistusta toimintasuunnitelman täytäntöönpanosta.

## **2. 1 OSA: TOIMET SÄHKÖISTEN ALLEKIRJOITUSTEN YHTEENTOIMIVUUDEN PARANTAMISEKSI**

Sähköisiä allekirjoituksia koskevan direktiivin päätavoitteena on luoda sähköisten allekirjoitusten käytölle yhteisön puitteet, jotka mahdollistavat sähköisiin allekirjoituksiin liittyvien tuotteiden ja palvelujen vapaan liikkuvuuden rajojen yli ja varmistavat sähköisten allekirjoitusten oikeudellisen perusaseman.

Direktiivissä käsitellään kolmentyyppisiä sähköisiä allekirjoituksia. Ensimmäisenä on yksinkertainen sähköinen allekirjoitus, joka on laaja käsite. Sen tarkoituksena on tunnistaa allekirjoittaja ja todentaa tiedot. Kyseessä voi yksinkertaisimmillaan olla sähköpostin allekirjoittaminen henkilön nimellä tai käyttäen PIN-koodia. Toinen muoto on kehittynyt sähköinen allekirjoitus (AES). Tämänkaltaisen allekirjoituksen on ensinnäkin liityttävä yksiselitteisesti sen allekirjoittajaan, toiseksi sillä on voitava yksilöidä allekirjoittaja, kolmanneksi se on luotava keinoilla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan, ja neljänneksi se on liitettävä sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita (ks. direktiivin 2 artiklan 2 kohta). Kolmas muoto eli varmennettu sähköinen allekirjoitus (QES) tarkoittaa kehittyneitä sähköistä allekirjoitusta, joka perustuu hyväksytyyn varmenteeseen (QC) ja on luotu turvallisella allekirjoituksen luomismenetelmällä. Se tarjoaa korkeimman tietoturvatason sen suhteen, että tiedot ovat peräisin väitetyltä lähettäjältä ja että toimitettuja tietoja ei ole voitu muuttaa.

Oikeudellisen tunnustamisen yleistä periaatetta sovelletaan kaikkiin kolmeen direktiivissä vahvistettuun sähköisen allekirjoituksen tyyppiin. Tämä tarkoittaa sitä, ettei mitään näistä allekirjoituksista voida hylätä yksinomaan sillä perusteella, että allekirjoitus on sähköisessä muodossa (ks. sähköisiä allekirjoituksia koskevan direktiivin 5 artikla). Lisäksi 5 artiklan 1 kohdan mukaan laillisuusolettamana on varmennetun sähköisen allekirjoituksen ja käsin kirjoitetun allekirjoituksen välinen vastaavuus. Sähköisten allekirjoitusten hyväksyminen yli valtioiden rajojen koskee kuitenkin ainoastaan varmennettua tasoa, sillä 4 artiklan 2 kohdan mukaan direktiivin mukaiset sähköisiin allekirjoituksiin liittyvät tuotteet saavat liikkua vapaasti sisämarkkinoilla (käytännössä tämä tarkoittaa tuotteita, jotka täyttävät varmennettuja allekirjoituksia koskevat vaatimukset direktiivin liitteissä vahvistetulla tavalla).

Jäsenvaltioiden on myös varmistettava, että jos ne asettavat lisävaatimuksia sähköisten allekirjoitusten käytölle julkisella sektorilla direktiivin 3 artiklan 7 kohdan perusteella, tällaiset vaatimukset eivät direktiivin sisämarkkinaperustan vastaisesti aiheuta rajatylittäville palveluille lisäesteitä<sup>11</sup>.

---

<sup>11</sup> Direktiivin 3 artiklan 7 kohdan mukaan tällaisten lisävaatimusten on oltava objektiivisia, avoimia, suhteellisia ja syrjimättömiä, ja niiden on liityttävä vain kyseessä olevan sovelluksen erityispiirteisiin.

Sen lisäksi, että näitä sähköisiä allekirjoituksia koskevan direktiivin vaatimuksia on noudatettava oikein, on kiinnitettävä huomiota useisiin teknisiin ja organisatorisiin seikkoihin, jotta sähköisten allekirjoitusten rajatylittävää käyttöä voidaan käytännössä helpottaa.

## **2.1. Varmennetut sähköiset allekirjoitukset ja hyväksytyyn varmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset**

Varmennettujen sähköisten allekirjoitusten (QES) ja hyväksytyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten (QC:hen perustuva AES) rajatylittävää käyttöä voidaan arvioiden mukaan kehittää suhteellisen nopeasti<sup>12</sup>. Molemmilla allekirjoituksilla on selkeä sähköisiä allekirjoituksia koskevaan direktiiviin perustuva oikeudellinen asema, eli niitä koskee oletus siitä, että varmennettu sähköinen allekirjoitus vastaa käsin kirjoitettua allekirjoitusta, ja jäsenvaltioilla on oikeudellinen velvoite hyväksyä hyväksytyt varmenteet vastavuoroisesti. Lisäksi molemmantyyppisten allekirjoitusten (QES ja QC:hen perustuva AES) osalta on jo tehty paljon standardointityötä.

Käytännössä suurin este sähköisten allekirjoitusten rajatylittävälle käytölle on se, että muista jäsenvaltioista lähtöisin oleviin sähköisiin allekirjoituksiin ei luoteta ja että näiden allekirjoitusten validointiin liittyy ongelmia.

Jotta lisättäisiin luottamusta toisista jäsenvaltioista lähtöisin oleviin sähköisiin allekirjoituksiin, vastaanottavan osapuolen olisi ensinnäkin pystyttävä tarkastamaan toisessa jäsenvaltiossa hyväksytyjä varmenteita myöntävien varmennepalvelujen tarjoajien (CSP) asema. Sähköisiä allekirjoituksia koskevan direktiivin (3 artiklan 3 kohdan) mukaan kunkin jäsenvaltion on varmistettava sellaisen asianmukaisen järjestelmän käyttöönotto, jonka avulla voidaan valvoa sen alueelle asettautuneita, hyväksytyjä varmenteita yleisölle myöntäviä varmennepalvelujen tarjoajia.

Vastaanottavan osapuolen on toiseksi pystyttävä tarkastamaan allekirjoituksen laatu validoidakseen toisesta jäsenvaltiosta peräisin olevan varmennetun sähköisen allekirjoituksen tai hyväksytyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen. Tämä tarkoittaa sitä, että vastaanottavan osapuolen on pystyttävä tarkastamaan, onko allekirjoitus kehittynyt sähköinen allekirjoitus ja onko sen tukena valvotun varmennepalvelujen tarjoajan myöntämä hyväksyty varmenne (ks. edellä valvontaa koskeva selitys (3 artiklan 3 kohta)). Jos kyseessä on varmennettu sähköinen allekirjoitus, vastaanottavan osapuolen on myös pystyttävä varmistamaan, onko allekirjoitus luotu turvallisella allekirjoituksen luomismenetelmällä.

Kaikki nämä tiedot löytyvät periaatteessa itse allekirjoituksesta ja hyväksytyyn varmenteeseen sisällöstä. Nykyisin näiden tietojen saaminen on kuitenkin vaikeaa, sillä nykyisten standardien ja käytäntöjen soveltamisessa on eroja. Tämä johtaa eroihin niiden tietojen laajuudessa ja laadussa, joita tosiasiallisesti saadaan vastaanotetuista allekirjoituksista ja varmenteista. Tämä vuorostaan aiheuttaa lisärasitteen vastaanotavalle osapuolelle, jonka on ehkä erikseen arvioitava kutakin toisesta jäsenvaltiosta lähtöisin olevaa allekirjoitusta.

Sähköisten allekirjoitusten validointimenettelyä voitaisiin sen vuoksi helpottaa toimittamalla vastaanotavalle osapuolelle tarpeelliset tiedot kansallisella tasolla hyväksytyistä ja

---

<sup>12</sup> Tämänkaltaisen työ on jo pohdinnan alla jäsenvaltioiden kanssa palveludirektiivin täytäntöönpanon yhteydessä.



valvotuista varmennepalvelujen tarjoajista ja antamalla ohjeistusta nykyisten standardien ja käytäntöjen soveltamisesta yhteentoimivuuden varmistamiseksi.

Valmistellakseen toimia, joita tarvitaan lisäämään luottamusta ja helpottamaan sähköisten allekirjoitusten rajatylittävää validointia, komissiolla on parhaillaan käynnissä tutkimus, jonka avulla arvioidaan sähköisten allekirjoitusten (QES ja QC:hen perustuva AES) rajatylittävää käyttöä koskevia vaatimuksia. Tutkimuksessa keskitytään erityisesti hyväksytyjä varmenteita myöntävien varmennepalvelujen tarjoajien valvontamalliin, luotettavan luettelon laatimiseen näistä palveluntarjoajista, valvottujen varmennepalvelujen tarjoajien jäsenvaltioissa myöntämien hyväksytyjen varmenteiden profiileihin, turvallisten allekirjoituksen luomismenetelmien profiiliin ja varmennettujen/kehittyneiden allekirjoitusten muotoon. Tutkimus perustuu sähköisiä allekirjoituksia koskevan direktiivin asianomaisiin säännöksiin, niiden kansalliseen täytäntöönpanoon ja direktiiviin pohjautuvaan nykyiseen standardointityöhön<sup>13</sup>.

#### Toimet:

- **Viimeistään vuoden 2009 kolmannella neljänneksellä:** Komissio saattaa ajan tasalle päätöksen 2003/511/EY<sup>14</sup>, jossa vahvistetaan luettelo sähköisiin allekirjoituksiin liittyvien tuotteiden yleisesti tunnustetuista standardeista, ja tarkastelee päätöksen mahdollista ulottamista muihin sähköisiin allekirjoituksiin liittyviin tuotteisiin kuin komission nykyisen päätöksen soveltamisalaan kuuluviin tuotteisiin (esimerkiksi hyväksytyjen varmenteiden profiilit ja turvallisten allekirjoituksen luomismenetelmien profiilit). Näin yksinkertaistetaan nykyistä monimutkaista standardointitilannetta ja autetaan sidosryhmiä täytäntöönpanemaan standardeja yhteensopivalla tavalla.
- **Viimeistään vuoden 2009 toisella neljänneksellä:** Komissio laatii luotettavan luettelon valvotuista hyväksytyjä varmenteita myöntävistä varmennepalvelujen tarjoajista (Trusted List of Supervised Qualified Certification Service Providers) Euroopan tasolla. Luettelo sisältää kaikki vaaditut tiedot nykyisistä ja valvotuista hyväksytyjä varmenteita myöntävistä varmennepalvelujen tarjoajista, jotta voidaan helpottaa hyväksytyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten validointimenettelyä.
- **Viimeistään vuoden 2009 kolmannella neljänneksellä:** Komissio laatii yleisiä vaatimuksia koskevat suuntaviivat ja ohjeet auttaakseen sidosryhmiä käyttämään varmennettuja sähköisiä allekirjoituksia ja hyväksytyyn varmenteeseen perustuvia kehittyneitä sähköisiä allekirjoituksia yhteentoimivalla tavalla.
- **Jatkuvasti:** Jäsenvaltioita kehoitetaan säännöllisesti toimittamaan tarpeelliset tiedot komissiolle ja tarvittaessa toteuttamaan toimenpiteitä, jotka perustuvat edellä mainittuihin sähköisiä allekirjoituksia koskeviin toimiin.

<sup>13</sup> Sähköisiä allekirjoituksia koskevan direktiivin mukaisesti standardeja ovat kehittäneet CEN (European Committee for Standardisation) ja ETSI (European Telecommunications Standards Institute) osana eurooppalaista sähköisten allekirjoitusten standardointialoitetta (European Electronic Signature Standardisation Initiative eli EESSI).

<sup>14</sup> EUVL L 175, 15.7.2003, s. 45. Luettelo sisältää sähköisiin allekirjoituksiin liittyviä tuotteita koskevat yleisesti tunnustetut standardit, joiden noudattamisen perusteella jäsenvaltioiden on oletettava tuotteiden olevan sähköisiä allekirjoituksia koskevan direktiivin vaatimusten mukaisia.

## 2.2. Kehittyneet sähköiset allekirjoitukset

Kehittyneiden sähköisten allekirjoitusten (AES) rajatylittävä käyttö herättää hyvin samankaltaisia yhteentoimivuuteen liittyviä kysymyksiä kuin edellä on tuotu esille varmennettujen sähköisten allekirjoitusten ja hyväksytyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten osalta. Käytännössä kehittyneiden sähköisten allekirjoitusten tilanne on kuitenkin monimutkaisempi, koska niihin liittyy nykyisin useampia oikeudellisia, teknisiä ja organisatorisia rajoitteita kuin varmennettuihin sähköisiin allekirjoituksiin.

Sähköisiä allekirjoituksia koskevan direktiivin 2 artiklan 2 kohdassa määritellään kehittyneet sähköiset allekirjoitukset hyvin yleisellä tasolla. Tämän johdosta jäsenvaltiot ovat päätyneet hyvin erilaisiin teknisiin ratkaisuihin ja erilaisiin turvallisuustasoihin. Jäsenvaltiot voivat myös soveltaa tiettyihin sovelluksiin erityisiä kansallisia ratkaisuja, mikä luo lisäesteitä kehittyneiden sähköisten allekirjoitusten rajatylittävälle käytölle.

Kehittyneillä sähköisillä allekirjoituksilla ei ole sähköisiä allekirjoituksia koskevassa direktiivissä samaa selkeää oikeudellista asemaa kuin varmennetuilla sähköisillä allekirjoituksilla sen suhteen, että ne vastaisivat käsinkirjoitettuja allekirjoituksia. Jäsenvaltiot on velvoitettu ainoastaan siihen, etteivät ne voi kieltää kehittyneen sähköisen allekirjoituksen oikeusvaikutusta yksinomaan siltä perustalta, että allekirjoitus on sähköisessä muodossa. Tämä merkitsee sitä, että jäsenvaltioilla on enemmän harkintavaltaa sen suhteen, millaisia kehittyneen sähköisen allekirjoituksen ratkaisuja ne hyväksyvät (tai eivät hyväksy), riippuen tietyn sovelluksen erityisistä vaatimuksista. Lisäksi, vaikka toisesta jäsenvaltiosta lähtöisin oleva kehittyneen sähköinen allekirjoitus voidaan periaatteessa hyväksyä, jos se täyttää kyseisen sovelluksen vaatimukset, käytettävissä olevien teknisten ratkaisujen määrä voi tehdä kehittyneen sähköisen allekirjoituksen hyväksymisestä käytännössä vaikeaa.

Tässä tilanteessa vastaanottavalla osapuolella on haasteellinen tehtävä validoida kehittyneen sähköinen allekirjoitus. Samoin on haasteellista arvioida kyseisen allekirjoituksen oikeudellista arvoa tai turvallisuustasoa tietyssä sovelluksessa. Nykyisin nämä tehtävät usein edellyttävät vastaanotetun allekirjoituksen tapauskohtaista arviointia ja käsittelyä. Kehittyneen sähköisen allekirjoituksen rajatylittävän käytön helpottamiseksi olisi luotava tarpeelliset edellytykset, joiden turvin vastaanottava osapuoli voi luottaa toisesta jäsenvaltiosta lähtöisin olevaan kehittyneeseen sähköiseen allekirjoitukseen ja validoida sen samaan tapaan kuin varmennetun sähköisen allekirjoituksen ja hyväksytyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen.

Tarkoituksena on ensimmäiseksi parantaa sähköisen hallinnon sovelluksissa nykyisin käytettäviä kehittyneitä sähköisiä allekirjoituksia koskevia tietoja. Tätä varten komissio saattaa ajan tasalle asianomaiset nykyiset maaprofiilit, jotka on vahvistettu vuonna 2007 sähköisen hallinnon sovelluksissa käytettävien sähköisten allekirjoitusten vastavuoroista tunnustamista koskevassa IDABC-tutkimuksessa. Komissio asettaa myös nämä maaprofiilit saataville verkkoon.

Koska nykyisin on kuitenkin olemassa useita kehittyneen sähköisen allekirjoituksen ratkaisuja, joihin eri jäsenvaltiot soveltavat eri vaatimuksia (mukaan lukien valvontaa koskevat perusteet), tässä toimintasuunnitelmassa on käytännössä mahdotonta laatia kehittyneitä sähköisiä allekirjoituksia koskeva yhteinen toimintapolitiikka ja yhteiset perusteet. Jotta samaan aikaan vältettäisiin se, että validointi aiheuttaa moninkertaista työtä kaikissa jäsenvaltioissa — mikä on huomattavin rajatylittävän yhteentoimivuuden este —

yhtenä ratkaisuna voisi olla, että tarkastus- ja validointitehtävät delegoidaan keskitetylle tai hajautetulle validointipalvelujärjestelylle. Näin voitaisiin asteittain poistaa tämä kehittyneiden sähköisten allekirjoitusten yhteentoimivuuden huomattavin este.

Komissio tarkastelee toteutettavuustutkimuksen avulla, mitä vaihtoehtoja on käytettävissä tällaisen validointijärjestelyn luomiseksi EU:n tasolle. Tutkimuksessa tarkastellaan erityisesti tällaisen palvelun oikeudellisia, teknisiä ja operatiivisia vaatimuksia, mukaan lukien erityyppisiä kehittyneitä sähköisiä allekirjoituksia koskevat mahdollisesti tarvittavat yhteisesti määriteltävät vaatimustasot, ja aluksi keskitytään sähköisen hallinnon sovelluksissa käytettyihin kehittyneisiin sähköisiin allekirjoituksiin. Toteutettavuustutkimuksen tulokset olisi mahdollisuuksien mukaan myös otettava huomioon laaja-alaisessa rajatylittävässä sähköisen hankinnan PEPPOL-pilottihankeessa (Pan European Public Procurement Online), jonka komissio ja useat jäsenvaltiot käynnistivät toukokuussa 2008 (osana tieto- ja viestintätekniikkapolitiikan tukiohjelmaa (ICT PSP)<sup>15</sup>.

Edellä mainitun tutkimuksen lisäksi komissio täsmentää jatkossa mahdollisia toimia, joita tarvitaan edistämään kehittyneiden sähköisten allekirjoitusten rajatylittävää käyttöä, sen pohjalta, mitä tuloksia saadaan käynnissä olevasta työstä ja millaista kehitystä tapahtuu varmennettujen sähköisten allekirjoitusten ja hyväksytyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten hyödyntämisessä ja rajatylittävässä tunnustamisessa.

#### Toimet:

- **Viimeistään vuoden 2009 toisella neljänneksellä:** Komissio saattaa ajan tasalle maaprofiilit, jotka on vahvistettu sähköisen hallinnon sovelluksissa käytettävien sähköisten allekirjoitusten vastavuoroista tunnustamista koskevassa IDABC-tutkimuksessa (yleiseurooppalaisten sähköisten viranomaispalveluiden yhteentoimiva toimittaminen julkishallinnolle, yrityksille ja kansalaisille)<sup>16 17</sup>.
- **Viimeistään vuoden 2009 toisella neljänneksellä:** Komissio tarkastelee eurooppalaisen yhdistetyn validointipalvelun toteutettavuutta (oikeudellisten, operatiivisten ja teknisten vaatimusten suhteen). Toteutettavuustutkimuksen perusteella komissio päättää, otetaanko tällainen validointipalvelu käyttöön ja miten tämä tapahtuu.
- **Viimeistään vuonna 2010:** Komissio raportoi lisätoimista, joita tarvitaan helpottamaan kehittyneiden sähköisten allekirjoitusten rajatylittävää käyttöä, sen pohjalta, mitä tuloksia saadaan käynnissä olevasta työstä ja millaista kehitystä tapahtuu varmennettujen sähköisten allekirjoitusten ja hyväksytyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten hyödyntämisessä ja rajatylittävässä tunnustamisessa.

<sup>15</sup> Osa kilpailukyvyyn ja innovoinnin puiteohjelmaa: <http://ec.europa.eu/cip>

<sup>16</sup> IDABC-ohjelma päättyi joulukuussa 2009. Komissio on ehdottanut IDABC-ohjelman seuraajaksi julkishallinnon yhteentoimivia ratkaisuja koskevaa ISA-ohjelmaa.

<sup>17</sup> Tutkimuksen tavoitteena (alustavat tulokset jo saatavilla, tutkimus saadaan päätökseen vuonna 2009) on tarkastella erilaisissa sähköisen hallinnon sovelluksissa ja palveluissa käytettävien sähköisten allekirjoitusten yhteentoimivuuden vaatimuksia ottaen huomioon sähköisiä allekirjoituksia koskevan direktiivin asianomaiset säännökset ja niiden kansallisen täytäntöönpanon. Tutkimuksessa on tarkoitus selvittää sovellus- ja jäsenvaltiokohtaisesti, minkä tyyppistä sähköistä allekirjoitusta edellytetään oikeudellisesti ja mitkä ovat sovellettavat tekniset rajoitukset.

- **Kun** Euroopan yhdistettyä validointipalvelua koskevan **toteutettavuustutkimuksen tulokset ovat valmiina**, jäsenvaltioita pyydetään toimittamaan komissiolle kaikki merkitykselliset tiedot ja huolehtimaan toimien toteuttamisessa tarvittavasta yhteistyöstä, erityisesti kun kyseessä ovat validointipalvelun perustamiseksi tarvittavat toimet, siitä riippuen, millaisia tuloksia toteutettavuustutkimuksesta saadaan.
- **Riippuen** Euroopan yhdistettyä validointipalvelua koskevan **toteutettavuustutkimuksen tuloksista** ja hankekonsortion suostumuksella jäsenvaltioita pyydetään testaamaan validointipalvelua CIP:n<sup>18</sup> laaja-alaisessa rajatylittävässä sähköisen hankinnan PEPPOL-pilottihankkeessa (Pan European Public Procurement Online).

### 3. 2 OSA: TOIMET SÄHKÖISEN TUNNISTUKSEN YHTEENTOIMIVUUDEN PARANTAMISEKSI

Jäsenvaltiot käyttävät nykyisin sähköisen identiteetin hallintajärjestelmiä (e-IDM) osana palveluntarjonnan nykyaikaistamista. Sähköisen identiteetin hallinta on olennainen osa minkä tahansa sähköisen palvelun tarjontaa. Toisaalta sähköinen tunnistus tarjoaa sähköisiä menettelyitä käyttäville henkilöille varmuuden siitä, ettei heidän henkilöllisyyttään ja henkilötietojaan voida käyttää luvatta. Toisaalta hallinto voi varmistaa, että henkilöt ovat niitä, keitä he väittävät olevansa, ja että heillä on ne oikeudet, joita he väittävät heillä olevan (esimerkiksi pyydetyn palvelun saamiseksi).

Joillakin jäsenvaltioilla on jo käytössä sähköisen tunnistuksen järjestelmiä tarjoamaan pääsy kyseisten jäsenvaltioiden julkishallinnon sähköisiin menettelyihin. Tekniset keinot vaihtelevat kuitenkin paljon, vaikka sähköisten henkilökorttien käyttö onkin nykysuuntauksena.

Sähköisen tunnistuksen keinoja on käytetty vailla jäsenvaltioiden välistä yhteensovittamista. Sähköisen tunnistuksen ratkaisujen yhteentoimivuus on kuitenkin ennakoedellytys rajatylittävälle pääsulle sähköisiin julkisiin palveluihin. Jos unionissa ei hyödynnetä yhteentoimivia sähköisen tunnistuksen järjestelmiä, käytännössä luodaan uusia esteitä, mikä on ristiriidassa sisämarkkinavälineiden kanssa, sillä näillä välineillä pyritään parantamaan sisämarkkinoiden toimintaa.

Poliittisella tasolla vuosien 2005 ja 2007 ministerijulistuksissa<sup>19</sup> kehoitetaan hyödyntämään yhteentoimivia identiteetin hallintajärjestelmiä Euroopassa, jotta kansalaiset ja yritykset pystyisivät osoittamaan, keitä ne ovat, jos julkishallinto tätä vaatii.

Parhaillaan on käynnissä tiettyjä yhteisiä toimia, joiden tavoitteena on löytää rajatylittävään sähköiseen tunnistukseen sellainen ratkaisu, jossa voitaisiin turvautua nykyisiin tunnistusratkaisuihin. Sähköisten allekirjoitusten mallin mukaisesti pyritään horisontaaliseen ratkaisuun, johon voitaisiin turvautua alakohtaisissa sovelluksissa ja joka perustuisi sähköisen tunnistuksen järjestelyjen vastavuoroiseen hyväksymiseen. On kuitenkin ratkaistava useita

<sup>18</sup> Kilpailukyvyn ja innovoinnin puiteohjelma 2007–2013.

<sup>19</sup> [http://ec.europa.eu/information\\_society/activities/egovernment/conferences/2005/index\\_en.htm](http://ec.europa.eu/information_society/activities/egovernment/conferences/2005/index_en.htm)  
[http://ec.europa.eu/information\\_society/activities/egovernment/docs/lisbon\\_2007/ministerial\\_declaration\\_180907.pdf](http://ec.europa.eu/information_society/activities/egovernment/docs/lisbon_2007/ministerial_declaration_180907.pdf)

kysymyksiä, jotta käytännössä mahdollistettaisiin sähköisen tunnistuksen rajatylittävä käyttö ja hyväksyminen.

Ensimmäisenä askeleena osana jo aiemmin mainittua ICT PSP -ohjelmaa laaja-alaisessa STORK-pilottihankkeessa erityisesti keskitytään julkisissa palveluissa hyödynnettävän sähköisen tunnistuksen yhteentoimivuuteen. STORK-pilottihankkeessa pyritään luomaan yhteentoimivan sähköisen tunnistuksen malli, joka tunnustetaan vastavuoroisesti kaikissa jäsenvaltioissa mutta joka antaa jäsenvaltioille mahdollisuuden säilyttää nykyiset järjestelmänsä ja käytäntönsä.

Pilottihanke on ensimmäinen askel kohti yhteentoimivuutta. Sen avulla on tarkoitus havainnollistaa erityisillä aloilla ratkaisuja, jotka voitaisiin sitten ulottaa muille aloille. Lisäksi pilottihankkeen tuloksista riippuen komissio päättää, tarvitaanko lisätoimia ja millaisia ne olisivat. Tämä tapahtuu sen jälkeen, kun tulokset on saatu vuonna 2012<sup>20</sup>.

#### Toimet:

- **Vuoden 2009 loppuun mennessä:** Komissio saattaa ajan tasalle maaprofiilit, jotka on vahvistettu sähköisen tunnistuksen yhteentoimivuutta Euroopan laajuisissa sähköisen hallinnon palveluissa koskevassa IDABC-tutkimuksessa. Näin jäsenvaltiot ja komissio pysyvät ajan tasalla sen suhteen, miten sähköisen tunnistuksen käyttö kehittyy jäsenvaltioissa.
- **Vuoden 2009 loppuun mennessä:** Komissio käynnistää yhteistyössä jäsenvaltioiden kanssa sähköisen tunnistuksen käyttöä jäsenvaltioissa koskevia erityisiä kyselyitä, joilla täydennetään ja tuetaan STORK-hanketta (esimerkiksi yhteisten eritelmien lisäkehittämisen tueksi sähköisen tunnistuksen yhteentoimivuutta varten).
- **Kun STORK-hankkeen tulokset ovat valmiina:** Komissio päättää, edellyttääkö sähköisen tunnistuksen EU:n laajuinen tehokas käyttö lisätoimia ja millaisia tällaiset mahdolliset lisätoimet olisivat.
- **Viimeistään vuonna 2012:** Jäsenvaltioita kehoitetaan demonstroimaan sähköisen tunnistuksen rajatylittävän käytön ratkaisuja STORK-pilottihankkeessa.

#### 4. SEURANTA JA TOIMEENPANO

Tässä toimintasuunnitelmassa esiteltyjen toimien toteuttaminen varmistaa horisontaalisen ja yhteensovitettun lähestymistavan, jolla helpotetaan ja parannetaan sähköisen hallinnon sovellusten rajatylittävää käyttöä kaikilla sisämarkkinoiden aloilla. Sillä myötävaikutetaan sisämarkkinoiden parempaan toimintaan tarjoamalla kattava lähestymistapa, jotta yritysten ja kansalaisten pääsy rajatylittäviin julkishallinnon palveluihin helpottuisi. Käyttöön otettavilla välineillä parannetaan nykyistä kehystä ja lisätään teknisten ratkaisuiden lähentymistä. Yksityissektorille koituu lisäarvoa turvallisia sähköisiä menettelyjä kehittävien välineiden

<sup>20</sup> Erityisaloja ovat rajatylittävä sähköisten palveluiden todentamisalusta, opiskelijoiden liikkuvuus, osoitteenmuutos, asiakirjojen sähköinen toimittaminen ja internetin turvallinen käyttö lasten parissa. Työssä on nykyisin mukana 13 jäsenvaltiota ja Islanti, ja hankkeessa on yhteensä 29 osanottajaa (yksityistä ja julkista).

laaja-alaisen käytön myötä, kun näitä välineitä voidaan käyttää myös yritysten välisissä sekä yritysten ja kuluttajien välisissä liiketoimissa.

Komissio seuraa läheisessä yhteistyössä jäsenvaltioiden kanssa toimintasuunnitelman täytäntöönpanoa. Tavoitteena on varmistaa, että ehdotetut toimenpiteet, erilaiset EU:n tason oikeudelliset vaatimukset ja asianomaiset operatiiviset hankkeet, kuten CIP-pilottihankkeet, ovat johdonmukaisia. Erityisesti komissio pyrkii käymään koko ajan vuoropuhelua jäsenvaltioiden kanssa tämän toimintasuunnitelman ohella. Tämä koskee myös kilpailupolitiikasta ja sisämarkkinoista vastaavia jäsenvaltioiden viranomaisia.

Toimintasuunnitelman täytäntöönpano komissiossa ja jäsenvaltioissa sekä kehityksen seuranta ovat osa sisämarkkinakatsauksen jatkotoimia. Vuoden kuluttua tämän toimintasuunnitelman hyväksymisestä komissio ryhtyy yhdessä jäsenvaltioiden kanssa tarkastelemaan tapahtunutta kehitystä. Tarkoituksena on esittää neuvostolle seurantakertomus vuonna 2010. Jäsenvaltioita kehoitetaan toimittamaan komissiolle kaikki merkitykselliset tiedot ehdotettujen toimien täytäntöönpanosta ja tuloksista rajatylittävän yhteentoimivuuden varmistamiseksi.

Seurantakertomuksen ja jäsenvaltioiden kanssa asianmukaisilla foorumeilla käytyjen keskustelujen perusteella komissio arvioi, tarvitaanko uusia horisontaalisia ja/tai alakohtaisia aloitteita.