Liikenne- ja viestintäministeriö E-KIRJELMÄ LVM2009-00186

VPO Pääkkönen Nina 23.06.2009

Eduskunta
Suuri valiokunta

Viite

Asia
Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle - Sähköisiä allekirjoituksia ja sähköistä tunnistusta koskeva toimintasuunnitelma rajat ylittävien julkisten palveluiden tarjoannan helpottamiseksi yhtenäismarkkinoilla

U/E-tunnus: **EUTORI-numero:**
EU/2008/1667

Ohessa lähetetään perustuslain 97§:n mukaisesti selvitys eduskunnan suurelle valiokunnalle asiakohdassa mainitusta Euroopan komission tiedonannosta.

Osastopäällikkö, ylijohtaja Liisa Ero

LIITTEET LVM2009-00187, KOM(2008) 798 lopullinen

Asiasanat	viestintäpolitiikka, sähköinen asiointi, teletoiminta
Hoitaa	**LVM, OM, VM**
Tiedoksi	EUE, OPM, PLM, SM, TEM, TH, VNEUS, VNK

Liikenne- ja viestintäministeriö PERUSMUISTIO LVM2009-00187

VPO Pääkkönen Nina,Miettinen Kirsi 23.06.2009

Asia

Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle - Sähköisiä allekirjoituksia ja sähköistä tunnistusta koskeva toimintasuunnitelma rajat ylittävien julkisten palveluiden tarjonnan helpottamiseksi yhtenäismarkkinoilla

Kokous

Liitteet Viite

EUTORI/Eurodoc nro:

EU/2008/1667

U-tunnus / E-tunnus:

-

Käsittelyn tarkoitus ja käsittelyvaihe:

-

Asiakirjat:

Komission asiakirja KOM(2008) 798 lopullinen; *Komission tiedonanto neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle sähköisiä allekirjoituksia ja sähköistä tunnistusta koskevaksi toimintasuunnitelmaksi rajat ylittävien julkisten palveluiden tarjonnan helpottamiseksi yhtenäismarkkinoilla*

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely:

-

Käsittelijä(t):

Liikenne- ja viestintäministeriö, neuvotteleva virkamies Kirsi Miettinen, puh. 160 28570, kirsi.miettinen@lvm.fi

Suomen kanta/ohje:

Asiassa ei ole olemassa Suomen kantaa. Asiaa ei ole käsitelty EU:n neuvostossa eikä sen johdosta myöskään valtioneuvostossa.

Liikenne- ja viestintäministeriön alustavan näkemyksen mukaan sähköiseen allekirjoittamiseen liittyy varsin huomattavia rakenteellisia ja oikeudellisia ongelmia. Tämän johdosta on epätodennäköistä, että sähköisiin allekirjoituksiin liittyvien

palveluiden tarjonta ja käyttö yleistyisi suuressa mittakaavassa EU:ssakaan. Tiettyyn teknologiaan (varmenteet) liittyvien edistämistoimien asemesta huomio tulisi kääntää teknologianeutraaleihin toimiin, joilla rajat yli tapahtuvaa sähköistä tunnistamista voitaisiin edistää. Komission ehdottamista toimista ei kuitenkaan ole mitään haittaa, joten niitä ei ole syytä ryhtyä vastustamaan.

Pääasiallinen sisältö:

Komission antoi 28.11.2008 tiedonantonsa neuvostolle, Euroopan parlamentille, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle sähköisiä allekirjoituksia ja sähköistä tunnistusta koskevaksi toimintasuunnitelmaksi rajat ylittävien julkisten palveluiden tarjonnan helpottamiseksi yhtenäismarkkinoilla (KOM(2008) 798 lopullinen). Toimintasuunnitelman tavoitteena on auttaa jäsenvaltioita toteuttamaan vastavuoroisesti tunnustettuja ja yhteentoimivia sähköisten allekirjoitusten sekä sähköisen tunnistuksen ratkaisuja, jotta helpotettaisiin rajatylittävien julkisten palvelujen tarjoamista sähköisessä ympäristössä. 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.

Tiedonanto on jaettu sähköisiin allekirjoituksiin kohdistuviin toimiin ja sähköiseen tunnistamiseen kohdistuviin toimiin. Painopiste on selkeästi sähköisten allekirjoitusten puolella. Niiden osalta komission toimenpiteet jakautuvat niin ikään kahteen ryhmään. Ensimmäinen ryhmä koskee varmennettujen sähköisten allekirjoitusten (QES) ja hyväksyttyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten (QC:hen perustuva AES) rajat ylittävää käyttöä. Komission arvion mukaan tätä aluetta voitaisiin kehittää suhteellisen nopeasti. 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.

Komissio toteaa, että käytännössä suurin este sähköisten allekirjoitusten rajat ylittävälle käytölle on se, että muista jäsenvaltioista lähtöisin oleviin sähköisiin allekirjoituksiin ei luoteta ja että näiden allekirjoitusten validointiin liittyy ongelmia.

Komission johtopäätösasiassa on, että sähköisten allekirjoitusten validointimenettelyä voitaisiin sen vuoksi helpottaa toimittamalla vastaanottavalle osapuolelle tarpeelliset tiedot kansallisella tasolla hyväksytyistä ja valvotuista varmennepalvelujen tarjoajista ja antamalla ohjeistusta nykyisten standardien ja käytäntöjen soveltamisesta yhteentoimivuuden varmistamiseksi.

Asiaintilan parantamiseksi komissio ehdottaa neljää toimenpidettä, joista erityisen kiinnostava on tavoite laatia viimeistään vuoden 2009 toisella neljänneksellä luotettava luettelo valvotuista hyväksyttyjä varmenteita myöntävistä varmennepalvelujen tarjoajista (Trusted List of Supervised Qualified Certification Service Providers) Euroopan tasolla. Luettelon on tarkoitus sisältää kaikki vaaditut tiedot nykyisistä ja valvotuista hyväksyttyjä varmenteita myöntävistä varmennepalvelujen tarjoajista. Työ on jo parhaillaan käynnissä palveludirektiivin täytäntöönpanoa valmistelevassa komission työryhmässä.

Lisäksi komission tavoitteena on viimeistään vuoden 2009 kolmannella neljänneksellä saattaa ajan tasalle päätös 2003/511/EY14, jossa vahvistetaan luettelo sähköisiin allekirjoituksiin liittyvien tuotteiden yleisesti tunnustetuista standardeista, ja tarkastella päätöksen mahdollista ulottamista muihin sähköisiin allekirjoituksiin liittyviin tuotteisiin kuin komission nykyisen päätöksen soveltamisalaan kuuluviin tuotteisiin. Samoin viimeistään vuoden 2009 kolmannella neljänneksellä komission tavoitteena on laatia yleisiä vaatimuksia koskevat suuntaviivat ja ohjeet auttaakseen sidosryhmiä käyttämään varmennettuja sähköisiä allekirjoituksia ja hyväksyttyyn varmenteeseen perustuvia kehittyneitä sähköisiä allekirjoituksia yhteentoimivalla tavalla. Jatkuvana toimenpiteenä mainitaan se, että jäsenvaltioita kehotetaan säännöllisesti toimittamaan tarpeelliset tiedot komissiolle ja tarvittaessa toteuttamaan toimenpiteitä, jotka perustuvat edellä mainittuihin sähköisiä allekirjoituksia koskeviin toimiin.

Toisena sähköisten allekirjoitusten ryhmänä komissio pitää kehittyneitä sähköisiä allekirjoituksia (AES). Niihin liittyy samankaltaisia yhteentoimivuuteen liittyviä kysymyksiä kuin edellä on tuotu esille varmennettujen sähköisten allekirjoitusten ja hyväksyttyyn 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.

Komissio toteaa, että 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 hyväksyttyyn varmenteeseen perustuvan kehittyneen sähköisen allekirjoituksen. Komissio johtopäätöksenä on, että toimintasuunnitelmassa on käytännössä mahdotonta laatia kehittyneitä sähköisiä allekirjoituksia koskeva yhteinen toimintapolitiikka ja yhteiset perusteet. Yhtenä ratkaisuna voisi kuitenkin olla, että tarkastus- ja validointitehtävät delegoidaan keskitetylle tai hajautetulle validointipalvelujärjestelylle. Näin voitaisiin asteittain poistaa tämä kehittyneiden sähköisten allekirjoitusten yhteentoimivuuden huomattavin este. Komissio ilmoittaa tarkastelevansa vuoden 2009 toisella neöjänneksellä toteutettavuustutkimuksen avulla, mitä vaihtoehtoja on käytettävissä tällaisen validointijärjestelyn luomiseksi EU:n tasolle.

Lisäksi komissio saattaa viimeistään vuoden 2009 toisella neljänneksellä 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). Viimeistään vuonna 2010 komissio raportoi lisätoimista, joita tarvitaan helpottamaan kehittyneiden sähköisten allekirjoitusten rajatylittävää käyttöä sen pohjalta, mitä tuloksia saadaan käynnissä olevasta työstä.

Jäsenvaltioita pyydetään toimittamaan komissiolle kaikki merkitykselliset tiedot ja huolehtimaan toimien toteuttamisessa tarvittavasta yhteistyöstä, erityisesti validointipalvelun perustamiseksi tarvittavien toimien osalta riippuen siitä, millaisia tuloksia toteutettavuustutkimuksesta saadaan. Jäsenvaltioita pyydetään myös testaamaan validointipalvelua CIP:n18 laaja-alaisessa rajat ylittävässä sähköisen hankinnan PEPPOL-pilottihankkeessa (Pan European Public Procurement Online).

Sähköisen tunnistamisen osalta komissio toteaa, sähköisen tunnistuksen ratkaisujen yhteentoimivuus on kuitenkin ennakkoedellytys rajat ylittävälle pääsylle sähköisiin

julkisiin palveluihin. Tähän saakka sähköisen tunnistuksen keinoja on käytetty vailla jäsenvaltioiden välistä yhteensovittamista. Jos unionissa ei hyödynnetä yhteentoimivia sähköisen tunnistuksen järjestelmiä, käytännössä luodaan uusia esteitä, mikä on ristiriidassa sisämarkkinavälineiden kanssa, sillä näillä välineillä pyritään parantamaan sisämarkkinoiden toimintaa.

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 kysymyksiä, jotta käytännössä mahdollistettaisiin sähköisen tunnistuksen rajat ylittävä käyttö ja hyväksyminen.

Ensimmäisenä askeleena on laaja-alainen STORK-pilottihanke, jossa erityisesti keskitytään julkisissa palveluissa hyödynnettävän sähköisen tunnistuksen yhteentoimivuuteen. Hankkeessa pyritään luomaan yhteentoimivan sähköisen tunnistuksen malli, joka tunnustetaan vastavuoroisesti kaikissa jäsenvaltioissa mutta joka antaa jäsenvaltioille mahdollisuuden säilyttää nykyiset järjestelmänsä ja käytäntönsä. Komissio käynnistää vuoden 2009 loppuun mennessä yhteistyössä jäsenvaltioiden kanssa sähköisen tunnistuksen käyttöä jäsenvaltioissa koskevia erityisiä kyselyitä, joilla täydennetään ja tuetaan STORK-hanketta. Hankkeen tulosten valmistuttua komissio päättää, edellyttääkö sähköisen tunnistuksen EU:n laajuinen tehokas käyttö lisätoimia, ja millaisia tällaiset mahdolliset lisätoimet olisivat. Edelleen jäsenvaltioita kehotetaan viimeistään vuonna 2012 demonstroimaan sähköisen tunnistuksen rajat ylittävän käytön ratkaisuja STORK-pilottihankkeessa.

Kansallinen käsittely:

-

Eduskuntakäsittely:

-

Käsittely Euroopan parlamentissa:

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema:

-

Taloudelliset vaikutukset:

-

Muut mahdolliset asiaan vaikuttavat tekijät:

-

Asiasanat
Hoitaa

Tiedoksi

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

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

(ETA:n kannalta merkityksellinen teksti)

1. JOHDANTO

1.1. Toimintasuunnitelman sisältö

EU on osana Lissabonin strategiaa sitoutunut kehittämään oikeudellista ja hallinnollista ympäristöä liiketoimintapotentiaalin 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 rajatylittäville 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[1]). 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[2] 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.

---

[1] 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.

[2] 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[3], 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[4] tarkoituksena on edistää sähköisten välineiden kehitystä ja käyttöä julkisia hankintoja koskevissa menettelyissä, mikä voisi tuoda yrityksille huomattavia säästöjä[5]. Jäsenvaltiot voivat säännellä sähköisten allekirjoitusten vaadittua tasoa sähköisiä allekirjoituksia koskevassa direktiivissä säädettyjen velvoitteiden mukaisesti, ja ne voivat määrätä hankintaviranomaiset hyväksymään ainoastaan varmennetut allekirjoitukset[6].

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). [7]

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

---

3 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.

4 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.

5 Lisätietoja on saatavilla sähköisten julkisten hankintojen sääntelykehyksen täytäntöönpanemisesta 13. joulukuuta 2004 esitetyssä toimintasuunnitelmassa, KOM(2004) 841.

6 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).

7 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 arvonlisäverojärjestelmästä 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 merkittävin sähköisiä allekirjoituksia käyttävä transaktiokanava. [8]

1.2.2. i2010-aloitteeseen kuuluva sähköisen hallinnon toimintasuunnitelma

Rajatylittävässä sähköisessä tunnistuksessa ei ole vieläkään 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[9] 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 tunnistautumisvälineellä, 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**[10].

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.

---

[8] Euroopan komissio valmistelee 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.

[9] i2010-aloitteeseen kuuluva sähköisen hallinnon toimintasuunnitelma – Vauhtia sähköiselle hallinnolle Euroopassa kaikkien hyväksi, KOM(2006) 173 lopullinen.

[10] 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 kehittynyttä sähköistä allekirjoitusta, joka perustuu hyväksyttyyn 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[11].

[11] 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 hyväksyttyyn varmenteeseen perustuvat kehittyneet sähköiset allekirjoitukset

Varmennettujen sähköisten allekirjoitusten (QES) ja hyväksyttyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten (QC:hen perustuva AES) rajatylittävää käyttöä voidaan arvioiden mukaan kehittää suhteellisen nopeasti[12]. 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 hyväksyttyjä 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, hyväksyttyjä varmenteita yleisölle myöntäviä varmennepalvelujen tarjoajia.

Vastaanottavan osapuolen on toiseksi pystyttävä tarkastamaan allekirjoituksen laatu validoidakseen toisesta jäsenvaltiosta peräisin olevan varmennetun sähköisen allekirjoituksen tai hyväksyttyyn 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 hyväksytty 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 hyväksytyn varmenteen 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 vastaanottavalle osapuolelle, jonka on ehkä erikseen arvioitava kutakin toisesta jäsenvaltiosta lähtöisin olevaa allekirjoitusta.

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

---

[12] Tämänkaltainen 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 hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajien valvontamalliin, luotettavan luettelon laatimiseen näistä palveluntarjoajista, valvottujen varmennepalvelujen tarjoajien jäsenvaltioissa myöntämien hyväksyttyjen 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[13].

Toimet:

- **Viimeistään vuoden 2009 kolmannella neljänneksellä**: Komissio saattaa ajan tasalle päätöksen 2003/511/EY[14], 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 hyväksyttyjen 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 hyväksyttyjä varmenteita myöntävistä varmennepalvelujen tarjoajista (Trusted List of Supervised Qualified Certification Service Providers) Euroopan tasolla. Luettelo sisältää kaikki vaaditut tiedot nykyisistä ja valvotuista hyväksyttyjä varmenteita myöntävistä varmennepalvelujen tarjoajista, jotta voidaan helpottaa hyväksyttyyn 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 hyväksyttyyn varmenteeseen perustuvia kehittyneitä sähköisiä allekirjoituksia yhteentoimivalla tavalla.

- **Jatkuvasti:** Jäsenvaltioita kehotetaan säännöllisesti toimittamaan tarpeelliset tiedot komissiolle ja tarvittaessa toteuttamaan toimenpiteitä, jotka perustuvat edellä mainittuihin sähköisiä allekirjoituksia koskeviin toimiin.

---

13 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).

14 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 hyväksyttyyn 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 kehittynyt 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 kehittynyt 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 hyväksyttyyn 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)[15] .

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 hyväksyttyyn 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)[16] [17].

- **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 hyväksyttyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten hyödyntämisessä ja rajatylittävässä tunnustamisessa.

---

15 Osa kilpailukyvyn ja innovoinnin puiteohjelmaa: http://ec.europa.eu/cip

16 IDABC-ohjelma päättyy joulukuussa 2009. Komissio on ehdottanut IDABC-ohjelman seuraajaksi julkishallinnon yhteentoimivia ratkaisuja koskevaa ISA-ohjelmaa.

17 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[18] 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 ennakkoedellytys rajatylittävälle pääsylle 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[19] kehotetaan 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

---

[18] Kilpailukyvyn ja innovoinnin puiteohjelma 2007–2013.

[19] 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

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[20].

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 kehotetaan demonstroimaan sähköisen tunnistuksen rajatylittävän käytön ratkaisuja STORK-pilottihankkeessa.

4. SEURANTA JA TOIMEENPANO

Tässä toimintasuunnitelmassa esiteltyjen toimien toteuttaminen varmistaa horisontaalisen ja yhteensovitetun 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. Käyttöönotettavilla välineillä parannetaan nykyistä kehystä ja lisätään teknisten ratkaisuiden lähentymistä. Yksityissektorille koituu lisäarvoa turvallisia sähköisiä menettelyjä kehittävien välineiden

[20] 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 kehotetaan 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.

EUROPEISKA GEMENSKAPERNAS KOMMISSION

Bryssel den 28.11.2008
KOM(2008) 798 slutlig

MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET, EUROPAPARLAMENTET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

Handlingsplan för bättre e-signaturer och e-legitimation för att förenkla tillhandahållandet av gränsöverskridande offentliga tjänster på den inre marknaden

MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET, EUROPAPARLAMENTET, EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN SAMT REGIONKOMMITTÉN

Handlingsplan för bättre e-signaturer och e-legitimation för att förenkla tillhandahållandet av gränsöverskridande offentliga tjänster på den inre marknaden

(Text av betydelse för EES)

1. INLEDNING

1.1. Aktuella frågor som tas upp i handlingsplanen

Europeiska unionen har inom ramen för Lissabonstrategin åtagit sig att förbättra de juridiska och administrativa förutsättningarna och därmed frigöra företagens potential. Genom att de offentliga förvaltningarna görs tillgängliga på nätet och företag och privatpersoner därigenom kan kommunicera med förvaltningar i andra medlemsstater skapas ett klimat som främjar företagande och som förenklar medborgarnas kontakter med myndigheterna.

Den elektroniska kommunikationen blir allt viktigare inom många delar av det ekonomiska och offentliga livet. Över hela EU börjar de offentliga förvaltningarna att erbjuda elektroniska tjänster. Hittills har de mest inriktat sig på nationella behov och resurser, vilket har gett ett komplicerat system med många olika lösningar. Det finns en risk för att detta skapar nya hinder för gränsöverskridande handel och för att det uppstår störningar i den inre marknadens funktion.

Den gränsöverskridande tillgången till de elektroniska tjänster som erbjuds av offentliga förvaltningar försvåras av det faktum att det krävs e-legitimation och e-signatur. På samma sätt som i den icke-digitala världen krävs det för vissa elektroniska tjänster en legitimation och en signatur. För att få åtkomst till de offentliga förvaltningarnas elektroniska tjänster måste användaren således kunna legitimera sig (så att förvaltningen kan kontrollera användarens identitet[1] och vara säkra på att användaren är den person som han eller hon utger sig för att vara) och kunna tillhandahålla en elektronisk signatur som förvaltningen kan verifiera; dessutom måste förvaltningen kunna kontrollera att uppgifterna inte har förvanskats under överföringen. Det största hindret är bristen på juridisk, teknisk och organisatorisk driftskompatibilitet.

Den nuvarande EU-lagstiftningen tillhandahåller övergripande och sektorsspecifika instrument för att underlätta och främja användningen av e-signaturer och e-legitimation. Genom direktivet om elektroniska signaturer[2] ges rättsligt erkännande för elektroniska signaturer och det skapas ett ramverk vars syfte är att sörja för driftskompatibilitet. För driftskompatibilitet krävs att ett antal praktiska, tekniska och organisatoriska krav uppfylls.

Dessutom krävs effektiv driftskompatibilitet om medlemsstaterna ska kunna fullgöra sina åligganden enligt övrig EU-lagstiftning, särskilt vad gäller specifika instrument för den inre marknaden. Inom flera initiativ för den inre marknaden föreskrivs att företag bör kunna använda sig av elektroniska medel för att kommunicera med offentliga organ, utöva sina rättigheter och göra affärer över gränserna.

---

[1] Identifiering är en process inom vilken påstådda eller observerade attribut hos en enhet används för att bestämma vem eller vad enheten är. Begreppet identifiering används också när det är fråga om entitetsautenticering. (Se Modinis uppsats om IDM-terminologi: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc.

[2] Direktiv 1999/93/EG, EGT L 13, 19.1.2000, s. 12 och rapporten om tillämpningen av direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer, KOM(2006)120 slutlig.

Enligt tjänstedirektivet ska medlemsstaterna, senast vid utgången av 2009[3], se till att alla förfaranden och formaliteter för att få tillträde till och utöva en tjänsteverksamhet kan fullgöras enkelt, på distans och på elektronisk väg. För detta krävs bland annat att det är möjligt att identifiera tjänsteleverantörer över gränserna och att det är möjligt att verifiera de uppgifter som skickas.

Syftet med direktiven om offentlig upphandling[4] är att främja utveckling och användning av elektroniska hjälpmedel inom offentlig upphandling, vilket kan ge avsevärt lägre kostnader för företagen[5]. Medlemsstaterna får, på grundval av direktivet om elektroniska signaturer, fastställa regler för vilken nivå en elektronisk signatur ska ha och de får också begränsa urvalet av upphandlande myndigheter till sådana som har kvalificerade signaturer[6].

Elektronisk fakturering, dvs. elektronisk överföring av betalningsuppgifter (faktura och betalningsuppgifter) mellan affärspartner (säljare och köpare) är grundläggande för effektiv hantering av betalningar. I samband med införandet av ett gemensamt eurobetalningsområde håller man på att förbereda ett initiativ för e-fakturering (kommissionen har tillsatt en expertgrupp som har fått i uppgift att skapa en europeisk ram för elektroniska fakturor till 2009) som kommer att möjliggöra ytterligare besparingar för företagen[7].

Syftet med denna handlingsplan är därför att skapa en övergripande och pragmatiskt ram för e-signaturer och e-legitimation, som kan göra det lättare för företagen och medborgarna att få tillgång till gränsöverskridande elektroniska offentliga tjänster. Handlingsplanen inriktas därför på ett antal praktiska, organisatoriska och tekniska frågor i syfte att komplettera den befintliga rättsliga ramen.

1.2. Det nuvarande ramverket för e-signaturer och e-legitimation på EU-nivå

1.2.1. Direktivet om elektroniska signaturer

Direktivet om elektroniska signaturer antogs 1999 i syfte att främja rättsligt erkännande av elektroniska signaturer och att säkra fri rörlighet på den inre marknaden för produkter, utrustning och tjänster för elektroniska signaturer. En juridisk och teknisk undersökning av hur e-signaturer används i praktiken visar emellertid att det finns problem med

---

3 Artikel 8 i Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden. Sista dag för att genomföra direktivet är den 28 december 2009.

4 Artikel 42.5 b och bilaga X i direktiv 2004/18/EG och artikel 48.5 b och bilaga XXIV i direktiv 2004/17/EG om offentlig upphandling.

5 För mer information, se Handlingsplan för genomförandet av den rättsliga ramen för elektronisk offentlig upphandling av den 13 december 2004, KOM(2004)841.

6 Vid upphandling online måste offentliga upphandlare kunna ta emot och behandla gränsöverskridande elektroniska anbud. Ett fullständigt elektronisk anbud är ett helt paket som innehåller ett stort antal elektroniskt signerade handlingar och intyg från olika källor och länder och som tas fram med olika tekniska hjälpmedel. Dessutom ingår styrkta översättningar (bland annat beträffande en tjänsteleverantörs yrkeskvalifikationer). Detta innebär att beslutsfattarna måste skapa omfattande öppna kommunikationsnät inom vilka de som tar emot informationen (den upphandlande parten) inte känner samtliga potentiella avsändare (anbudsgivarna).

7 Expertgruppen för e-fakturering har bland annat förklarat att e-faktureringen inte får förhindras av skillnader i nationell lagstiftning vad gäller elektroniska signaturer. I målen för denna övergripande handlingsplan ingår inte bedömning av vilka följder användningen av elektroniska fakturor och signaturer får för momslagstiftningen (elektroniska signaturer i fakturor behandlas i rådets direktiv 2006/112/EG om ett gemensamt system för mervärdesskatt (artikel 233)); inte heller ingår bedömning av vilka hinder som finns eller vilka åtgärder som måste vidtas för att undanröja dessa.

driftskompatibiliteten vilket begränsar användningen över gränserna. Undersökningen visar på att det finns behov av effektivare system för ömsesidigt erkännande. Den splittring på den inre marknaden som uppstår på grund av den bristande gränsöverskridande driftskompatibiliteten kommer sannolikt främst att påverka de tjänster som avser e-förvaltning, dvs. det idag viktigaste användningsområdet för e-signaturer[8].

1.2.2. i2010 – Handlingsplanen för e-förvaltning

Vad gäller gränsöverskridande e-legitimation finns det fortfarande ingen gemenskapslagstiftning som kan ligga till grund för åtgärder på gemenskapsnivå. Trots detta ger kommissionen sitt stöd (både politiskt och ekonomiskt stöd) till verksamhet som syftar till att finna lösningar som möjliggör driftskompatibel e-legitimation på EU-nivå. I detta sammanhang anges i *i2010 – Handlingsplan för e-förvaltning*[9], som antogs av kommissionen den 25 april 2006, att driftskompatibel elektronisk id-hantering är en av grundförutsättningarna för att möjliggöra tillträde till offentliga tjänster. Medlemsstaterna inser att driftskompatibel elektronisk id-hantering är av stor betydelse för att man ska kunna uppnå att ”*europeiska medborgare och företag senast 2010 kan använda sig av säkra och praktiska lokala, regionala eller nationella elektroniska tillämpningar som uppfyller dataskyddskrav, för att därigenom kunna legitimera sig för offentliga tjänster i sin egen eller någon annan medlemsstat*”.

1.3. Förbättrad gränsöverskridande driftskompatibilitet för e-signaturer och e-legitimation

De bestämmelser som redan finns och de politiska åtaganden som har gjorts av medlemsstaterna och kommissionen är inte tillräckliga utan det krävs mer samordnade och övergripande åtgärder för att förenkla gränsöverskridande användning av e-legitimation och e-signaturer i praktiken. Detta är nödvändigt om man vill undvika splittring av den inre marknaden.

Kommissionen föreslog därför i sitt meddelande *En inre marknad för framtidens Europa* av den 20 november 2007 att det skulle antas en **handlingsplan för elektroniska underskrifter och autenticering**[10].

Syftet med handlingsplanen är att hjälpa medlemsstaterna att införa ömsesidigt godkända och kompatibla system för e-signaturer och e-legitimation i syfte att göra det lättare att tillhandahålla elektroniska offentliga tjänster över gränserna. Det fastställs särskilda åtgärder för e-signaturer (del 1) och för e-legitimering (del 2). Handlingsplanen inriktas huvudsakligen på e-förvaltningstillämpningar, men de föreslagna åtgärderna kan också vara till nytta för företagstillämpningar eftersom de funktioner som ska införas också kan användas vid transaktioner mellan företag och vid transaktioner mellan företag och konsumenter.

---

8 Europeiska kommissionen arbetar också på ett projekt för att underlätta införandet av elektroniska signaturer inom sina interna och externa förfaranden. Projektet kallas *Electronic Signature Service Infrastructure(ESSI).* Projektet är en grundförutsättning för den dematerialisering av Europeiska kommissionens förfaranden som föreskrivs i bestämmelser om elektroniska och digitala handlingar (SEK(2005)1578).

9 Handlingsplan för e-förvaltning inom ramen för initiativet i2010 - Ett snabbare införande av e-förvaltning i Europa till nytta för alla [KOM(2006) 173 slutlig].

10 Med e-autenticering avses här entitetsautenticering, dvs. e-legitimation. Begreppet e-legitimation används här för att göra en klar åtskillnad mellan entitetsautenticering och meddelandeautenticering.

Vid Europeiska rådets vårmöte 2008 förklarade regeringscheferna att det är av avgörande betydelse att det införs gränsöverskridande driftskompatibla lösningar för e-signaturer och e-legitimation för att förbättra den inre e-marknadens funktion.

Kommissionen kommer att bidra till att man tar fram en samordnad lösning på kompatibilitetsfrågan genom att man övervakar utvecklingen och ger råd till medlemsstaterna och till aktörerna om genomförandet av handlingsplanen.

2. DEL 1: ÅTGÄRDER FÖR ATT FÖRBÄTTRA DEN GRÄNSÖVERSKRIDANDE DRIFTSKOMPATIBILITETEN FÖR E-SIGNATURER

Huvudsyftet med direktivet om elektroniska signaturer är att skapa en gemenskapsram som gör det möjligt för produkter och tjänster för elektroniska signaturer att flöda fritt över gränserna, och att se till att elektroniska signaturer får ett grundläggande rättsligt erkännande.

I direktivet behandlas tre typer av elektroniska signaturer. Den första är vad som kallas en enkel elektronisk signatur. Det är fråga om ett vitt begrepp och syftet är att identifiera den person som signerar och att verifiera uppgifter. Det kan röra sig om något så enkelt som att underteckna ett e-postmeddelande med en persons namn eller använda en PIN-kod. Den andra typen är vad som kallas en avancerad elektronisk signatur (nedan kallad *AES*). Denna typ av signatur är för det första knuten uteslutande till undertecknaren, för det andra kan undertecknaren identifieras genom den, för det tredje är den skapad med medel som undertecknaren kan behålla uteslutande under sin egen kontroll och för det fjärde är den kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas (se artikel 2.2 i direktivet). Den tredje typen, en så kallad kvalificerad elektronisk signatur (nedan kallad *KES*), som baseras på ett kvalificerat certifikat (nedan kallat *KS*) och som skapas genom en säker anordning för skapande av signaturer. Den ger den högsta nivån av garantier för att uppgifterna kommer från den angivna avsändaren och för att de överförda uppgifterna inte har ändrats.

Den allmänna principen om rättsligt erkännande avser alla de tre typer av elektroniska signaturer som föreskrivs i direktivet. Detta innebär att en elektronisk signatur inte kan förvägras rättslig verkan på grund av att den är i elektronisk form (se artikel 5 i direktivet om elektroniska signaturer). I artikel 5.1 anges dessutom att en avancerad elektronisk signatur juridiskt ska motsvara en handskriven signatur. Det är emellertid endast kvalificerade signaturer som kan komma ifråga för gränsöverskridande erkännande eftersom det i artikel 4.2 föreskrivs fri rörlighet för produkter för elektroniska signaturer vilka överensstämmer med direktivet (vilket i princip innebär produkter som uppfyller kraven för kvalificerade signaturer enligt bilagan till direktivet).

Medlemsstaterna måste också se till att de ytterligare krav på grundval av artikel 3.7 i direktivet som de inför för e-signaturer som används inom den offentliga sektorn inte utgör hinder för gränsöverskridande tjänster i enlighet med direktivets rättsliga grund, dvs. den inre marknaden[11].

[11] Enligt artikel 3.7 ska sådana krav vara objektiva, tydliga, proportionella och icke-diskriminerande och ska endast gälla de särskilda egenskaperna för den berörda tillämpningen.

Utöver de åtgärder som måste vidtas för att säkra en korrekt tillämpning av direktivet om elektroniska signaturer måste ett antal tekniska och organisatoriska frågor lösas så att den gränsöverskridande användningen av e-signaturer kan förbättras i praktiken.

2.1. Kvalificerade elektroniska signaturer och avancerade elektroniska signaturer som är baserade på ett kvalificerat certifikat

Det anses möjligt att relativt snabbt[12] förbättra den gränsöverskridande användningen av kvalificerade e-signaturer (*KES*) och avancerade e-signaturer som är baserade på ett kvalificerat certifikat (*AES* som baseras på *KC*). Båda dessa typer av signaturer har en tydlig rättslig status enligt direktivet om elektroniska signaturer, dvs. KES betraktas som likvärdiga med en handskriven signatur och det åligger medlemsstaterna att ömsesidigt erkänna kvalificerade certifikat. Dessutom har det redan gjorts mycket för att standardisera de båda typerna av signaturer (KES och AES som är baserade på KC).

I praktiken är det främsta hindret för gränsöverskridande användning av e-signaturer bristande förtroende för signaturer från andra medlemsstater och de svårigheter som förknippas med valideringen av signaturerna.

För att förbättra förtroendet för e-signaturer från andra medlemsstater bör, för det första, den mottagande parten ges möjlighet att kontrollera status för de tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat i andra medlemsstater. Enligt artikel 3.3 i direktivet om elektroniska signaturer ska medlemsstaterna garantera att ett lämpligt system införs vilket gör det möjligt att övervaka de tillhandahållare av certifikattjänster som är etablerade på deras territorium och som utfärdar kvalificerade certifikat.

För det andra bör den mottagande parten, för att kunna validera KES och AES som är baserade på KC, ges möjlighet att kontrollera kvaliteten på signaturen. Detta innebär att den mottagande parten måste kunna kontrollera om en signatur är en avancerad elektronisk signatur och om den baseras på ett kvalificerat certifikat som har utfärdats av en tillhandahållare av certifikattjänster som står under övervakning (se texten om övervakning enligt artikel 3.3 ovan). När det gäller KES måste mottagaren också kunna kontrollera om signaturen har skapats med hjälp av en säker anordning för skapande av signaturer.

Denna information kan i princip inhämtas från själva signaturen och från innehållet i det kvalificerade certifikatet. Det är emellertid i nuläget svårt att inhämta informationen på grund av de skillnader som finns när det gäller hur man använder befintliga standarder och förfaranden. Detta gör att de den information som faktiskt kan inhämtas från de erhållna signaturerna och certifikaten skiljer sig vad gäller typen av information och informationens kvalitet. Detta skapar i sin tur extraarbete för den mottagande parten som måste göra en enskild bedömning av varje signatur som kommer in från en annan medlemsstat.

Valideringen av e-signaturer skulle därför kunna förenklas genom att den mottagande parten ges nödvändig information om de tillhandahållare av certifikattjänster som är godkända och föremål för tillsyn på nationell nivå och genom att det utfärdas riktlinjer för hur de befintliga standarderna och förfarandena ska användas för att vara driftskompatibla.

---

[12] Frågan behandlas redan i samarbete med medlemsstaterna inom ramen för genomförandet av tjänstedirektivet.

För att förbereda de åtgärder som krävs för att förbättra förtroendet och förenkla gränsöverskridande validering av e-signaturer genomför kommissionen en undersökning om vad som krävs för gränsöverskridande elektroniska signaturer (KES och AES som är baserade på KC). Undersökningen inriktas särskilt på en modell för tillsynen av de aktörer som tillhandahåller kvalificerade certifikat, vidare på inrättandet av en tillförlitlig förteckning över tillhandhållare av kvalificerade certifikat som är föremål för tillsyn, på profiler för kvalificerade certifikat som utfärdas av tillhandahållare som är föremål för tillsyn i medlemsstaterna, på en profil för säkra anordningar för skapande av signaturer, samt på formatet på kvalificerade och avancerade signaturer. Undersökningen bygger på de relevanta bestämmelserna i direktivet om elektroniska signaturer, på hur dessa genomförs i medlemsstaterna och på det standardiseringsarbete som har utförts på grundval av direktivet[13].

Åtgärder:

- **Senast tredje kvartalet 2009:** Kommissionen kommer att aktualisera beslut 2003/511/EG[14], som innehåller en förteckning över allmänt erkända standarder för produkter för elektroniska signaturer, och undersöka om det finns möjlighet att utvidga beslutets tillämpningsområde till andra e-signaturprodukter (till exempel profiler för kvalificerade certifikat och profiler för säkra anordningar för skapande av signaturer). Härigenom kan den nuvarande komplicerade situationen förenklas och det blir lättare för aktörerna att genomföra standarderna på ett kompatibelt sätt.

- **Senast andra kvartalet 2009:** Kommissionen kommer att sammanställa en *tillförlitlig förteckning över tillhandhållare av kvalificerade certifikat som är föremål för tillsyn* på EU-nivå. Förteckningen kommer att innehålla all nödvändig information om befintliga tillhandhållare av kvalificerade certifikat som är föremål för tillsyn. Syftet med detta är att förenkla valideringen av e-signaturer som baseras på kvalificerade certifikat.

- **Senast tredje kvartalet 2009**: Kommissionen kommer att ta fram riktlinjer avseende de gemensamma kraven för att hjälpa aktörerna att genomföra KES och AES som är baserade på KC på ett kompatibelt sätt.

- **Pågående åtgärder:** Medlemsstaterna uppmanas att regelbundet lämna in den information som kommissionen behöver och vid behov vidta de åtgärder som följer av den åtgärdsplan som anges här.

2.2. Avancerade elektroniska signaturer

När det gäller gränsöverskridande användning av avancerade elektroniska signaturer uppstår ungefär samma kompatibilitetsproblem som har diskuterats ovan när det gäller kvalificerade elektroniska signaturer och avancerade elektroniska signaturer som baseras på ett kvalificerat certifikat. I praktiken är emellertid situationen mer komplicerad när det gäller AES, eftersom

---

[13] På grundval av direktivet om elektroniska signaturer har det utarbetats standarder av Europeiska standardiseringsorganisationen (CEN) och Europeiska institutet för telestandarder (ETSI) inom ramen för EESSI (European Electronic Signature Standardisation Initiative).

[14] EUT L 175, 15.7.2003, s. 45. Förteckningen innehåller allmänt erkända standarder för produkter för elektroniska signaturer som medlemsstaterna ska betrakta som förenliga med kraven i direktivet om elektroniska signaturer.

det för närvarande finns fler juridiska, tekniska och organisatoriska svårigheter när det gäller AES än när det gäller KES.

I artikel 2.2 ges en allmän definition av begreppet avancerad elektronisk signatur. Detta har gjort att medlemsstaterna använder sig av många olika tekniska lösningar med olika grader av säkerhet. Medlemsstaterna får också införa specifika nationella lösningar för specifika tillämpningar, vilket skapar ytterligare hinder för gränsöverskridande användning av avancerade elektroniska signaturer.

Enligt direktivet om elektroniska signaturer har avancerade elektroniska signaturer inte samma tydliga rättsliga status som kvalificerade elektroniska signaturer som är likvärdiga med en handskriven signatur. Den enda skyldighet som åligger medlemsstaterna är att de inte får förvägra en avancerad elektronisk signatur rättslig verkan på grund av den är i elektronisk form. Detta innebär att medlemsstaterna har större möjligheter att välja vilka avancerade elektroniska signaturer som ska godkännas eller inte, beroende vilka krav som gäller för en viss tillämpning. Dessutom är det så att även om en AES från en annan medlemsstat i princip skulle kunna godkännas, om den uppfyller kraven för en viss tillämpning, kan det visa sig att det är svårt att godkänna signaturen i praktiken på grund av att det finns så många möjliga tekniska lösningar.

Både valideringen av en AES och bedömningen av dess juridiska status eller dess säkerhetsnivå i en viss tillämpning är svåra uppgifter och för närvarande krävs det ofta att det görs en separat bedömning/hantering av den mottagna signaturen i varje enskilt fall. För att förenkla gränsöverskridande användning av AES bör det skapas förutsättningar som gör att den mottagande parten kan lita på och validera en AES från en annan medlemsstat på samma sätt som en KES och AES som är baserad på KC.

Som ett första steg kommer informationen om de avancerade elektroniska signaturer som används inom e-förvaltningstillämpningar att förbättras. För det ändamålet kommer kommissionen att förbättra de relevanta landsprofiler som offentliggjordes 2007 i IDABC-undersökningen om ömsesidigt erkännande av e-signaturer inom e-förvaltningstillämpningar, samt göra dessa tillgängliga på Internet.

På grund av det stora antal olika lösningar som finns när det gäller AES och de många olika krav som tillämpas i medlemsstaterna beträffande dessa (även tillsynskriterierna) är det inom ramen för denna handlingsplan omöjligt att ta fram en gemensam strategi och gemensamma kriterier för AES. För att ändå förhindra att medlemsstaterna inför många olika valideringsåtgärder, vilket ju är det främsta hindret för gränsöverskridande driftskompatibilitet, är det möjligt att delegera verifieringen och valideringen till en central eller decentraliserad valideringstjänst. Härigenom skulle det vara möjligt att stegvis undanröja det främsta hindret för driftskompatibla AES.

Kommissionen kommer att göra en genomförbarhetsundersökning för att se om det är möjligt att införa en sådan valideringstjänst på EU-nivå. Undersökningen kommer att inriktas på juridiska, tekniska och driftsrelaterade aspekter samt på det eventuella behovet av gemensamt definierade kravnivåer för olika typer av AES med utgångspunkt från de AES som används inom e-förvaltningstillämpningar. Om möjligt bör resultaten också tas till vara inom det storskaliga gränsöverskridande pilotprojektet för offentlig upphandling – PEPPOL (Pan European Public Procurement Online) – som kommissionen inledde i maj 2008 i samarbete

med flera medlemsstater (som ett led i programmet för politiskt stöd till informations- och kommunikationsteknik (ICT PSP)[15].

Utöver ovannämnda undersökning kommer kommissionen att definiera närmare vilka åtgärder som behövs för att främja gränsöverskridande användning av AES. Kommissionen kommer att basera sitt arbete på resultaten av det pågående arbetet och de erfarenheter som har gjorts i samband med användningen och det gränsöverskridande erkännandet av kvalificerade elektroniska signaturer och avancerade elektroniska signaturer som baseras på kvalificerade certifikat.

Åtgärder:

- **Senast andra kvartalet 2009**: Kommissionen kommer att aktualisera landsprofilerna i den undersökning[16] om ömsesidigt erkännande av e-signaturer för e-förvaltningstillämpningar som har tagits fram av IDABC (Interoperable Delivery of European e-Government Services to public Administrations, Business and Citizens)[17].

- **Senast andra kvartalet 2009**: Kommissionen kommer att göra en genomförbarhetsundersökning avseende de juridiska, driftsrelaterade och tekniska förutsättningarna för en gemensam europeisk valideringstjänst. Utifrån resultaten av genomförbarhetsundersökningen kommer kommissionen att avgöra om och hur en sådan valideringstjänst ska införas.

- **Senast 2010**: Kommissionen kommer att rapportera om vilka åtgärder som behövs för att främja gränsöverskridande användning av AES. Kommissionen kommer att basera sitt arbete på resultaten av det pågående arbetet och de erfarenheter som har gjorts i samband med användningen och det gränsöverskridande erkännandet av KES och AES som baseras på KC.

- **Efter det att genomförbarhetsundersökningen avseende en gemensam europeisk valideringstjänst avslutats** kommer medlemsstaterna att uppmanas att lämna in all relevant information till kommissionen och att sörja för det samarbete som krävs för åtgärderna, särskilt de åtgärder som, enligt genomförandeundersökningen, är nödvändiga för inrättandet av valideringstjänsten.

- Beroende på **resultatet av genomförbarhetsundersökningen** avseende en gemensam europeisk valideringstjänst kommer medlemsstaterna att uppmanas att i samarbete med projektkonsortiet testa valideringstjänsten inom ramen för det storskaliga gränsöverskridande pilotprojektet för offentlig upphandling – PEPPOL

---

15 Programmet ingår i ramprogrammet för konkurrenskraft och innovation: http://ec.europa.eu/cip

16 Undersökningens syfte (preliminära resultat finns tillgängliga och undersökningen kommer att avslutas 2009) är att undersöka vad som krävs för driftskompatibla e-signaturer inom olika e-förvaltningstillämpningar och tjänster utifrån bestämmelserna i direktivet om elektroniska signaturer och de nationella genomförandebestämmelserna till detta. Undersökningen förväntas producera en förteckning som visar vilken typ av e-signatur som krävs per e-förvaltningstillämpning och per medlemsstat, samt vilka tekniska begränsningar som finns.

17 IDABC-programmet avslutas i december 2009. Kommissionen har föreslagit att IDABC-programmet ska få en efterföljare i ett program om driftskompatibla lösningar för offentliga förvaltningar (ISA).

– (Pan European Public Procurement Online) som ingår i ramprogrammet för konkurrenskraft och innovation[18].

3. DEL 2: ÅTGÄRDER FÖR ATT FÖRBÄTTRA DEN GRÄNSÖVERSKRIDANDE DRIFTSKOMPATIBILITETEN FÖR E-LEGITIMATION

Idag använder medlemsstaterna system för elektronisk id-hantering för att erbjuda moderna tjänster. Elektronisk ID-hantering är grundläggande för tillhandahållandet av alla typer av e-tjänster. Dels ger e-legitimeringen användarna garantier för att deras identiteter och personliga uppgifter inte används på obehörigt sätt och dels kan förvaltningarna vara säkra på att varje användare verkligen är den person som han eller hon utger sig för att vara och har de rättigheter som han eller hon yrkar på (t.ex. att erhålla den begärda tjänsten).

Vissa medlemsstater har redan infört system för e-legitimering för den som vill få tillgång till medlemsstatens offentliga e-tjänster. De tekniska lösningarna skiljer sig åt, även om tendensen idag går mot elektroniska ID-kort.

Medlemsstaterna har infört olika system för e-legitimering utan någon samordning. För att vidareutveckla de gränsöverskridande offentliga e-tjänsterna krävs emellertid att systemen för e-legitimering är kompatibla. Om det inte införs ett kompatibelt system för e-legitimering inom unionen kommer det i praktiken att uppstå nya hinder, på samma sätt som skedde med de inremarknadsinstrument som var avsedda att förbättra den inre marknadens funktion.

På politisk nivå har man i två ministerförklaringar från 2005 respektive 2007[19] begärt att det ska införas ett driftskompatibelt system för id-hantering i EU varigenom medborgarna och företagen kan legitimera sig för de offentliga förvaltningarna.

Vissa gemensamma åtgärder har vidtagits för att försöka finna ett system för gränsöverskridande e-legitimering som kan bygga på befintliga identifieringssystem. På samma sätt som när det gäller e-signaturer söker man finna en övergripande lösning som fungerar för sektorstillämpningarna och som bygger på ömsesidigt erkännande av motpartens system för e-legitimering. Ett antal frågor behöver emellertid fortfarande lösas innan e-signaturerna kan godtas och användas gränsöverskridande i praktiken.

Som ett första steg kommer man, inom det redan nämnda programmet för politiskt stöd till informations- och kommunikationsteknik, genomföra ett storskaligt pilotprojekt (STORK) som särskilt inriktas på driftskompatibilitet för e-legitimering inom offentlig förvaltning. STORK-projektet arbetar med att ta fram en modell för kompatibla e-identiteter som kan erkännas i alla medlemsstater, samtidigt som medlemsstaterna kan behålla sina befintliga system och förfaranden.

Pilotprojektet är ett första steg mot driftskompatibilitet. Det förväntas finna lösningar på specifika områden som därefter kan utvidgas till andra områden. Utifrån de resultat som

[18] Ramprogrammet för konkurrenskraft och innovation 2007–2013.

[19] 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

pilotprojektet ger kommer kommissionen att besluta om det behövs fler åtgärder efter det att projektet slutförs 2012[20] och i så fall vilka åtgärder.

Åtgärder:

- **Senast i slutet av 2009:** Kommissionen kommer att aktualisera landsprofilerna i den undersökning om driftskompatibilitet för e-legitimation inom EU-täckande e-förvaltningstillämpningar som har tagits fram av IDABC (Interoperable Delivery of European e-Government Services to public Administrations, Business and Citizens). Härigenom kommer medlemsstaterna och kommissionen att kunna göra sig en aktuell bild av hur användningen av e-legitimation utvecklas i medlemsstaterna.

- **Senast i slutet av 2009:** Kommissionen kommer i samarbete med medlemsstaterna att göra specifika undersökningar om användningen av e-legitimation i medlemsstaterna, dels som ett komplement till STORK-projektet och dels som ett led i projektet (dvs. till stöd för gemensamma specifikationer för driftskompatibel e-legitimering).

- **När STORK-projektet har presenterat sina resultat**: Kommissionen kommer att avgöra om det behövs fler åtgärder för att säkra effektiv användning av e-legitimation i hela EU, och i så fall vilka.

- **Senast 2012:** Medlemsstaterna uppmanas att inom ramen för STORK-projektet lägga fram lösningar för gränsöverskridande e-legitimering.

4. KONTROLL OCH GENOMFÖRANDE

Åtgärderna i denna handlingsplan kommer att möjliggöra en övergripande och samordnad strategi för enklare och frekventare användning av e-förvaltningstjänster på den inre marknadens samtliga områden. Handlingsplanen kommer att bidra till att den inre marknaden fungerar bättre genom att den ger en övergripande strategi som gör det lättare för företag och medborgare att använda e-förvaltningstjänster över gränserna. De åtgärder som ska vidtas kommer att förbättra den nuvarande ramen och samordna de tekniska lösningarna. Mervärdet för den privata sektorn utgörs av det faktum att användningen av redskap för säkra elektroniska transaktioner kommer att öka och av det faktum att redskapen också kan användas i transaktioner mellan företag och mellan företag och konsumenter.

Kommissionen kommer i samarbete med medlemsstaterna att följa genomförandet av handlingsplanen uppmärksamt. Syftet med detta är att sörja för koherens avseende de föreslaga åtgärderna, avseende de juridiska aspekterna på EU-nivå och avseende de relevanta operativa projekten, som pilotprojekten inom ramprogrammet för konkurrenskraft och innovation. Kommissionen kommer att föra en kontinuerlig dialog med medlemsstaterna om denna handlingsplan, inbegripet med de myndigheter i medlemsstaterna som ansvarar för frågor som rör konkurrenskraft och den inre marknaden.

---

[20] De aktuella områdena är gränsöverskridande autenticeringsplattformar för e-tjänster, studentutbyten, adressändring, elektroniskt utbyte av handlingar och säker internetanvändning för barn Tretton medlemsstater deltar för närvarande tillsammans med Island. Totalt har projektet 29 deltagare (privata och offentliga).

Kommissionens och medlemsstaternas genomförande av denna handlingsplan och övervakningen av resultaten är ett led i uppföljningen av översynen av den inre marknaden. Ett år efter det att denna handlingsplan antas kommer kommissionen och medlemsstaterna att se över vilka framsteg som har gjorts och därefter överlämna en rapport om utvecklingen till rådet under 2010. Medlemsstaterna uppmanas att förse kommissionen med all relevant information om genomförandet och resultaten av de åtgärder som föreslås för att förbättra den gränsöverskridande driftskompatibiliteten.

På grundval av rapporten om utvecklingen och efter samråd med medlemsstaterna inom relevanta forum kommer kommissionen att avgöra om det behövs fler övergripande och/eller sektorsspecifika åtgärder och i så fall vilka.