Traficomin havaintoja eIDAS-asetuksen arviointiin

Sisältö

1 Muistion tarkoitus

1.1 eIDAS-asetuksen arviointi käynnissä

Komissiolla on käynnissä EU:n nk. eIDAS-asetuksen (EU) 910/2014 49 artiklan mukainen asetuksen arviointi, josta komissio toimittaa raportin parlamentille ja neuvostolle. Komission raportin määräaika on 1.7.2020, mutta tiettävästi raportti ei valmistu tässä aikataulussa.

Muistion tarkoitus on koota **Traficomin Kyberturvallisuuskeskuksen valvonta- ja neuvontatehtävissä ja niihin liittyvässä kansainvälisessä yhteistyössä kertyneitä havaintoja,** jotta toimiala ja hallinto voivat puolestaan muodostaa Suomessa näkemystä eIDAS-asetuksen vaikutuksesta, mahdollisuuksista ja mahdollisista muutostarpeista.

Lisätietoa

Linkki: Komission eIDAS-observatory

Linkki: Komission eIDAS-sivut

Linkki: Komission sivut eIDAS-asetus ja täytäntöönpanosäädökset

Linkki: Komission lausuntopyynnöt (eIDAS-konsultaatio tulossa ennakkotietojen perusteella kesäkuussa)

1.2 eIDAS-asetuksessa säädettävien asioiden hallinto Suomessa

Liikenne- ja viestintäministeriön (LVM) hallinnonalalle kuuluvat tunnistuspalveluiden vertaisarvioinnit sekä luottamuspalvelutarjoajien ja luottamuspalveluiden hyväksyntä ja valvonta.

- Liikenne- ja viestintävirasto (Traficom) on valvova viranomainen, tehtäviä hoitaa Kyberturvallisuuskeskus.
- On hyvä huomata, että kansallinen vahvan sähköisen tunnistamisen luottamusverkostosääntely eli kilpailusääntely ei liity eIDAS-asetukseen. Asetus koskee tunnistusta vain, jos valtio notifioi tunnistusmenetelmän rajat ylittäväksi.
- Kansallisen tunnistuslain vaatimukset vahvan sähköisen tunnistuspalvelun luotettavuudelle on harmonisoitu eIDAS-asetuksen kanssa.

Valtiovarainministeriön (VM) alaan kuuluu julkishallinnon sähköisten asiointipalveluiden ohjaus.

- Digi- ja väestötietovirasto (DVV) ylläpitää kansallista rajat ylittävän tunnistuksen solmupistettä ja suomi.fi -tunnistusta, jonka kautta rajat ylittävä tunnistus välitetään ulkomailla suomalaisille julkishallinnon asiointipalveluille.
- DVV tarjoaa asetuksen mukaisia hyväksyttyjä luottamuspalveluita.

Oikeusministeriön hallinnonalalle kuuluu oikeusvaikutuksiin (sähköisen allekirjoituksen, sähköisen leiman ja sähköisen asiakirjan oikeusvaikutukset) liittyvä sääntely. Sitä ei käsitellä tässä muistiossa.

2 Traficomin eIDAS -valvontatehtävät ja kansainväliset työryhmät

Traficomin eIDAS -valvontatehtävät perustuvat lakiin vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista sekä (617/2009) ja eIDAS-asetuksen 12 artiklaan (tunnistaminen) sekä 17 artiklaan (luottamuspalvelut).

2.1 Tunnistuspalvelut

- Traficom osallistuu eIDAS-asetuksen nojalla annetun komission täytäntöönpanopäätöksen (EU) 2015/296 mukaisen yhteistyöverkoston toimintaan ja EU:lle notifioitujen kansallisten tunnistusmenetelmien vertaisarviointeihin
  - eIDAS cooperation network eli yhteistyöverkosto
  - komission täytäntöönpanopäätöksellä (EU) 2015/296 perustettu ryhmä
  - tunnistuspalveluiden notifiointiin, vertaisarviointien organisointiin ja rajat ylittävän tunnistamisen yhteentoimivuuteen liittyvät asiat
  - tämä toiminta on käytännössä erittäin aktiivista

- Traficom ilmoittaa EU:lle suomalaisen tunnistusjärjestelmän, joka halutaan Suomesta notifioida
  - ei ole toistaiseksi tapahtunut

- Traficom valvoo eIDAS-asetuksen mukaisen rajat ylittävän tunnistusvälityksen kansallisen solmupisteen vaatimustenmukaisuutta, solmupisteen ylläpito säädetty DVV:n tehtäväksi
  - Teemme säännöllisesti yhteistyötä DVV:n kanssa rajat ylittävän notifioidun tunnistuksen teknisen yhteentoimivuuden kehittämiseksi.

2.2 Luottamuspalvelut

Traficomin valvontatehtävät:

- Traficom hyväksyy ja listaa EU-tasolla tunnustettuun luetteloon (trusted list) eIDAS-asetuksen 21 ja 22 artiklan mukaisesti asetuksen vaatimukset täyttävät hyväksytyt luottamuspalvelut (qualified trust services)
  - Toistaiseksi DVV:n ilmoittamat hyväksytyt allekirjoitusvarmenteet ja hyväksytyt verkkosivujen todentamisen varmenteet

- Traficom valvoo hyväksyttyjen luottamuspalveluiden vaatimustenmukaisuutta, myös häiriöilmoitusten perusteella
  - em. DVV:n luottamuspalvelut

- Traficom valvoo tarvittaessa resurssien salliessa ei-hyväksyttyjä luottamuspalveluita, jos niistä tehdään valitus tai häiriöilmoitus
  - Ohje 214/2016 O sähköisten tunnistus- ja luottamuspalveluiden ilmoituksista, kohta 5
  - Sähköinen ilmoituslomake

Traficom osallistuu seuraaviin ryhmiin, joissa käsitellään eIDAS-asetuksen luottamuspalvelusääntelyn toimeenpanoa. Meidän havaitsemamme arviointitarpeet eIDAS-asetuksessa on työryhmäkeskustelujen perusteella havaittu myös lukuisissa muissa maissa.

- Enisa artikla 19 -ryhmä
  - eIDAS-asetuksen 19 artiklan asiat eli tietoturvan perusvaatimukset ja häiriötilanteet
  - Euroopan unionin verkko- ja tietoturvavirasto (ENISA) tukee toimintaa

- Komission eIDAS expert group

- komission tarvittaessa koolle kutsuma jäsenvaltioiden asiantuntijoiden epävirallinen valmistelu- ja tiedonvaihtoryhmä
- ryhmässä on viimeisimpänä asian ollut käsittelyssä komission täytäntöönpanopäätöksen (EU) 2015/296 muutosvalmistelu, joka liittyy sertifioidun sähköisen allekirjoituksen tai leiman luontivälineen uusiin standardeihin (ks. kohta 5.4 jäljempänä)

- FESA
  - epävirallinen valvovien viranomaisten ryhmä, joka on toiminut jo sähköisen allekirjoituksen direktiivin 1999/93/EY aikana (ko. direktiivi kumottiin eIDAS-asetuksella)
  - ryhmässä koottiin yhteiset näkemykset ja toimitettiin kirjallinen lausunto komissiolle keväällä 2020
  - LINKKI: FESAN lausunto 4.3.2020 (*In this Position Paper FESA presents seven suggestions of maximum importance unanimously supported by its members. These suggestions have been discussed extensively within the community over the years. The FESA members are requested to submit the other suggestions directly to the European Commission.)*

Lisätietoa

Linkki: Traficomin Kyberturvallisuuskeskuksen eIDAS-sivu

3 Traficomin havainnot sähköisistä tunnistuspalveluista

Tähän kohtaan on koottu eIDAS-asetuksen tunnistusosioon liittyviä havaintoja.

On tärkeää huomata, että eIDAS-asetuksen tunnistusta koskeva sääntely ja luottamuspalveluja koskeva sääntely ovat täysin erillisiä osioita vaatimusten, jäsenvaltioiden yhteistoiminnan ja valvonnan organisoinnin kannalta.

eIDAS-asetuksessa tunnistusosiota ja luottamuspalvelusääntelyä ei ole synkronoitu keskenään. Tunnistus- ja luottamuspalveluilla on kuitenkin käytännössä joitakin yhdistäviä tekijöitä tai tarkastelutarpeita.

3.1 Sähköisen tunnistamisen eIDAS-vaatimusten harmonisointi muiden sähköisen tunnistamisen EU-säädösten kanssa (kuten PSD2)

Yleisesti ottaen geneerisen ja toimialariippumattoman tunnistuspalvelun olisi tarkoituksenmukaista olla EU-sääntelyssä rakennuspalikka, jota käytetään tai johon viitataan toimialakohtaisissa sääntelyissä.

eIDAS-asetuksen vaatimukset notifioitaville sähköisen tunnistamisen järjestelmille ja niiden puitteissa myönnetyille tunnistusmenetelmille (tunnistusvälineille) tarkennetaan komission täytäntöönpanoasetuksessa (EU) 2015/1502, nk. Komission varmuustasoasetus. Vaatimukset on skaalattu kautta linjan kolmelle eri varmuustasolle, joista rajat ylittävän tunnustamisen vaatimus koskee vain kahta ylintä tasoa. Tunnistusmenetelmän vaatimukset ovat täysin toimialaneutraaleja eli ne eivät ole riippuvaisia siitä, minkä alan verkkopalveluissa menetelmiä käytetään henkilöllisyyden todentamiseen.

Maksupalveludirektiivissä (nk. PSD2) ei ole hyödynnetty eIDAS-sääntelyä, vaan on säädetty toimialakohtaisista vaatimuksista vahvasta tunnistamisesta maksupalveluissa. Vaatimukset on tarkennettu komission teknisessä sääntelystandardissa (EU) 2018/389. Vahvan tunnistamisen perusvaatimukset ovat

varsin samankaltaiset kuin eIDAS-sääntelyssä, koska tunnistuksen luotettavuuteen vaikuttavat tekijät eivät sinänsä ole riippuvaisia toimialasta.

Suomessa pankkien tarjoamiin sähköisen tunnistamisen menetelmiin soveltuvat sekä PSD2-sääntely että tunnistuslain sääntely, koska toimijat ovat ilmoittaneet tunnistusmenetelmät tunnistuslain mukaiseen rekisteriin. Tunnistuslain tekniset vaatimukset vastaavat eIDAS-sääntelyä.

Traficom ja Finanssivalvonta ovat selvittäneet yhdessä ja toimialaa kuullen vaatimusten yhteensopivuutta 2018 ja todenneet, että sama perusmenetelmä voi olla pohjana sekä tunnistuslain että PSD2-puolen käytössä. Olisi tarkoituksenmukaista, että toimialariippumatonta asiointikäyttöä ja maksupalveluita tai muuta finanssipuolen asiointia varten ei tarvitse kehittää, tarjota ja käyttää eri tunnistusmenetelmää. Jos tunnistuslain mukaista tunnistuspalvelua ei voi käyttää finanssialalla, tämä heikentää tunnistuspalveluiden tarjonnan ja kilpailun mahdollisuuksia.

Näemme, että EU-tasolla olisi arvioitava tai edistettävä sähköisen tunnistamisen vaatimusten harmonisointia toimialasta riippumatta.

3.2 Teknisten standardien hyödyntäminen varmuustasoasetuksessa ja vertaisarvioinneissa

Komission varmuustasoasetus on luonnollisesti säädöksenä tekniseltä kannalta yleispiirteinen. Tämä on välttämätöntäkin teknologianeutraaliuden ja teknisen kehityksen mahdollistamiseksi.

eIDAS yhteistyöverkosto on laatinut epävirallisen ja ei-sitovan varmuustasoasetuksen soveltamisohjeen. Yhteistyöverkosto voi antaa lausuntoja toimintaansa kuuluvista asioista. Soveltamisohjeessa mainitaan informatiivisesti joitakin standardeja, mutta viittaukset eivät ole kattavia.

Näemme, että komission varmuustasoasetuksella tulisi edellyttää hyödynnettäväksi teknisiä standardeja. Ne voisivat olla osittain samoja standardeja, joita teknisen kehityksen takia tarvitaan myös luottamuspalveluiden vaatimustenmukaisuuden arvioinnissa. Esimerkkejä tunnistus- ja luottamuspalveluille yhteisistä tekijöistä ovat etätunnistuksen vaatimukset (ks. luottamuspalveluiden kohdalla) ja vaikkapa mobiilisovelluksen luotettavuusvaatimukset.

3.3 eIDAS yhteistyöverkoston vertaisarvioinnin linjausten transparenssin lisääminen

eIDAS-asetuksen tunnistussääntelyn lähtökohta on kansallinen suvereniteetti. Asetuksen tavoitteena ei ole harmonisoida kansallisesti käytettäviä tunnistusmenetelmiä vaan mahdollistaa luottamus notifioitaviin tunnistusjärjestelmiin vertaisarvioinneilla.

Vertaisarvioinnit ovat kokemuksemme mukaan erittäin toimiva tapa lisätä luottamusta. Niihin osallistuu ammattitaitoisia asiantuntijoita ympäri Eurooppaa. Vertaisarvioinnit tarjoavat mahdollisuuden tiedonvaihtoon ja yhteisen näkemyksen muodostamiseen varmuustasoasetuksen tulkinnasta.

Tunnistusjärjestelmien notifiointiin liittyvä vertaisarviointi on luottamuksellisuutta edellyttävää toimintaa. Notifioiva valtio voi päättää, missä määrin se haluaa julkaista vertaisarviointiraportin tietoja. Vertaisarvioinnista muodostettava yhteistyöverkoston lausunto (*opinion*) on aina julkinen, mutta sisällöltään niukka.

Lausunnoissa on kuitenkin viime aikoina muodostunut käytäntö, jonka mukana lausunnossa luetellaan ne seikat, jotka yhteistyöverkoston näkemyksen mukaan tulee korjata tai muutoin huomioida, jotta varmuustason vaatimukset täyttyvät. Näitä voi käytännössä luonnehtia ehdoiksi.

Vertaisarviointiraportit ja niiden pohjalta laaditut julkiset lausunnot eivät kokonaisuutena palvele julkisen tiedon tuottamisen välineenä yhteistyöverkostossa tehdyistä tulkinnoista. Ei olisi mielekästäkään käyttää yksittäisten jäsenvaltioiden tunnistusjärjestelmien arviointimateriaalia tähän tarkoitukseen, vaan tietoa olisi mieluummin tuotettava yleisesti.

Näemme, että yhteistyöverkoston toiminnassa tulisi käyttää enemmän jotain ohjaavia sääntelyinstrumentteja (lausuntoja, ohjeita tai muita), joilla jaetaan nykyistä avoimemmin vertaisarvioinneissa muotoutuneita tulkintoja.

Jäsenvaltioiden näkemykset tästä aiheesta vaihtelevat. Suomi ja monet muut kannattavat yhteisiä näkemyksiä kokoavien dokumenttien laatimista, mutta osa jäsenvaltioista ei pidä sitä tarkoituksenmukaisena.

Näemme, että tilanne ei ole kypsä esimerkiksi yhteistyöverkoston vertaisarviointilausuntojen säätämiseksi sitoviksi (vrt. telepuolella Berec), mutta jotkin transparenssia ja harmonisointia edistävät toimet olisivat tarpeellisia. EU:n tasolla ennakoitavat ja toimijoiden tiedossa olevat vaatimukset edistäisivät tunnistuspalveluiden kehittymistä.

Lisätietoa

Linkki: Komission sivut tunnistamisen eIDAS yhteistyöverkosto

Linkki: Yhteistyöverkoston lausunnot

Linkki: Guidance on level of Assurance

3.4 Muita ajankohtaisia tunnistusasioita

Oikeushenkilöiden tunnistamisen vaatimukset on määritelty varmuustasoasetuksessa, mutta palveluita on tullut tarjolle erittäin vähän. Lisäksi on nähtävissä esim. sovellusten tai järjestelmien luotettavan identifioinnin tarpeita. **On siis arvioitava muidenkin kuin luonnollisten henkilöiden tunnistusmenetelmiä. Toisaalta oikeushenkilön sähköinen leima voisi palvella paremmin oikeushenkilön tunnistustarpeita** (ks. kohdat 5.4 ja 5.6 sähköisestä allekirjoituksesta ja leimasta).

Rajat ylittävässä tunnistamisessa on välitettävä eIDAS-sääntelyn perusteella vähimmäissetti pakollisia henkilötietoja (pakolliset attribuutit). Sääntelyssä on myös määritelty joukko valinnaisia tietoja (optionaaliset attribuutit). eIDAS-asetus koskee notifioidun tunnistusmenetelmän tunnustamista. Mahdolliset vaatimukset sähköisen asiointipalvelun varsinaiselle rajat ylittävälle tarjoamiselle tulevat muusta sääntelystä, kuten tulossa olevasta SDG-asetuksesta[1] (single digital gateway). Käytännössä sähköisissä asiointipalveluissa esimerkiksi Suomessa tukeudutaan henkilön yksilöinnissä henkilötunnukseen ja **ulkomaisen henkilön kohdalla tarvittaneen henkilötunnuksen puuttuessa vähimmäistietojen**

[1] EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2018/1724, annettu 2 päivänä lokakuuta 2018, tietoja, menettelyjä sekä neuvonta- ja ongelmanratkaisupalveluja saataville tarjoavan yhteisen digitaalisen palveluväylän perustamisesta ja asetuksen (EU) N:o 1024/2012 muuttamisesta

lisäksi lisätietoja, jotta voidaan varmistaa, ettei sama henkilö ole järjestelmässä usealla eri tunnuksella. Kaikkien jäsenvaltioiden eIDAS-PIDit (*personal identifier*) eivät ole henkilötunnuksen tapaan pysyviä. Tarvittavien lisäattribuuttien ja rekisteritietojen vaihtaminen rajojen yli on tarpeen, jotta palveluita voidaan aidosti tarjota. Tämä ei välttämättä ole eIDAS-asetuksen asia, mutta liitännäinen siihen. Käytännössä asioinnin edistäminen voi vaatia sektorikohtaista tarkastelua.

eIDAS-asetus edellyttää ja mahdollistaa **rajat ylittävän tunnistamisen** vain julkisissa asiointipalveluissa. Rajat ylittävässä tunnistamisessa julkisiin palveluihin ei saa periä maksuja rajojen yli. Valtiot eivät luonnollisestikaan pääsääntöisesti halua tai voi kustantaa tunnistuspalveluita **yksityiselle sektorille**, joten rajat ylittävän tunnistuksen välittämiseen yksityisen sektorin palveluille toiseen maahan olisi luotava käyttöehdot ja laskutusjärjestelmät. Asetuksen artiklassa 7 f) todetaan mahdollisuus tällaisten määrittelyjen laatimiselle ja julkaisemiselle, mutta näitä on toistaiseksi tehty erittäin vähän. Asetuksen mahdollisuuksien tarkastelu olisi kuitenkin toivottavaa, sillä yksityisen sektorin tarpeet ovat ilmeiset.

Suomessa yksityisen sektorin rajat ylittävän tunnistuksen fasilitointi ei ole vielä ollut DVV:n ja VM:n roadmapilla kansallisen solmupisteen kehittämisessä, koska julkishallinnon toimintojen käynnistäminen eri maiden kanssa vaatii sekin paljon työtä ja on asetuksen mukaan pakollista.

Traficom on tunnistusmääräyksen yhteydessä tarkastellut yleisellä tasolla yksityisten tunnistusvälityspalveluiden oikeudellista mahdollisuutta tarjota tunnistusta rajojen yli. Asiaa käsitellään määräyksen 72 12 §:ssä ja 13 §:ssä ja niiden perusteluissa. Tunnistuslain mukaan rekisteröidyistä tunnistusvälityspalveluista osa toimii yrityksinä useissa maissa. Tunnistusta voi tarjota myös ulkomaiselle asiointipalvelulle ainakin EU-alueella kuten Suomessakin huomioiden asiointipalvelun oikeus käsitellä henkilötietoja (GDPR) ja huomioiden rajapinnalle säädetyt turvallisuusvaatimukset.

4 Traficomin havainnot etätunnistamisesta tunnistus- ja luottamuspalveluissa

Tässä käsitellään asiaa, joka koskee sekä eIDAS-asetuksen tunnistus- että luottamuspalveluosaa: tunnistusvälineen tai varmenteen hakijan henkilöllisyyden todentaminen etäyhteydellä.

On tärkeää huomata, että eIDAS-asetuksen tunnistusta koskeva sääntely ja luottamuspalveluja koskeva sääntely ovat täysin erillisiä osioita vaatimusten, jäsenvaltioiden yhteistoiminnan ja valvonnan organisoinnin kannalta.

Mukana on lainaus FESAn lausunnosta Komissiolle.

4.1 Ensitunnistusvaatimusten synkronointi tunnistusmenetelmissä ja hyväksytyissä luottamuspalveluissa (henkilöille myönnettävissä varmenteissa)

Hakijan henkilöllisyyden varmistamisesta (ensitunnistamisesta) säädetään tunnistusvälineiden myöntämisessä komission varmuustasoasetuksessa (EU) 2015/1502 liitteen kohdassa 2.1.2 ja allekirjoitusvarmenteiden myöntämisessä artiklassa 24.1.

Näemme, että tunnistuspalveluiden sääntelyn ja hyväksyttyjen luottamuspalveluiden sääntelyn eli artiklan 24.1 varmenteiden myöntämisen

sääntelyn suhde tulisi selkeyttää. Tulisi selventää, minkä varmuustason tunnistusmenetelmä kelpaa art. 24.1 varmenteen myöntämisessä. Tunnistusmenetelmien hyväksymisen henkilöllisyyden verifioinnissa varmenteiden myöntämisessä tulisi olla jäsenvaltioissa yhdenmukaista.

4.2 Ensitunnistus etäyhteydellä tai muuten sähköisesti (remote identification) (eIDAS artikla 24.1)

Etäensitunnistukseen liittyvät kysymykset koskevat sekä tunnistusvälineiden myöntämistä että hyväksyttyjen allekirjoitusvarmenteiden myöntämistä.

Etäensitunnistuksen menetelmistä käsitellään tässä ajankohtaisinta Euroopan laajuista ongelmaa eli henkilöllisyystodistusten kuten passin tai henkilökortin esittämistä sähköisen yhteyden kautta. Tällöin on pystyttävä varmistamaan, että asiakirja on aito ja että se on oikealla haltijalla. Henkilöllisyyden todentaminen voi tapahtua joko näkö- ja ääniyhteydellä tai muutoin.

Sähköisen tunnistamisen sääntelyä ja luottamuspalveluiden sääntelyä ei ole eIDAS-asetuksessa synkronoitu.

Tunnistusmenetelmien notifioinneissa esitettäviä menetelmiä arvioidaan vertaisarvioinneissa eIDAS-asetuksen 8 artiklan nojalla annetun komission varmuustasoasetuksen (EU) 2015/1505 vaatimusten perusteella. Soveltamiskäytäntöä kertyy sitä kautta, mutta sitä ei ole vielä riittävästi.

Hyväksyttyjen luottamuspalveluiden eli esimerkiksi allekirjoitusvarmenteiden myöntämisessä vaadittavasta henkilöllisyyden verifioinnista säädetään eIDAS-asetuksen 24 artiklassa. Se ei ole kovin yksityiskohtainen ja mahdollistaa ja edellyttääkin siten kansallisia vaatimuksia menettelyissä. Tämä saa aikaan poikkeavia käytäntöjä, jotka ovat luotettavuudeltaan erilaisia. Tämä myös vaikeuttaa tarjontaa useammassa jäsenvaltiossa.

Pyrimme keräämään tietoa eri maiden käytännöistä ja lähteistä, jotta voisimme tasapuolisesti linjata, mitä voidaan pitää luotettavana tunnistuspalveluissa ja luottamuspalveluissa. Lähteiden kenttä on laaja ja kehittyvä. Emme ole toistaiseksi pystyneet resursoimaan oman toimijoita palvelevan kriteeristön määrittelyyn Suomessa, vaikka sille on tarvetta.

Näemme, että EU:n laajuinen tarkempi sääntely edistäisi paljon tehokkaammin etäensitunnistamisen menettelyjen arviointia ja käyttöönottoa ja harmonisointi tehostaisi tarjontaa ja myös tähän käytettyjen palvelujen saatavuutta. ETSI on käynnistänyt asiasta standardointityön, joka on alkuvaiheessa ja vienee joitain vuosia.

FESA

2. Practices regarding remote identification (eIDAS Arts. 24(1)(b) and (d))

2.1. Observation

Currently acceptance of remote identification methods (equivalent to physical face-to-face) is left to the discretion of each Member State SB, without any clear requirements. This creates a heavily unlevelled playing field for QTSPs at European level. The lack of requirements will presumably lead to a race to the bottom. We need clarification on the requirements applying to the physical presence mentioned in Art. 24(1)(b).

2.2. Motivation

Ensure a high level of assurance promoting the global reach of eIDAS. We aim at a level playing field for QTSPs delivering qualified certificates on a remote basis. SBs see a growing demand from the market

for remote identification according to Article 24(1). Harmonizing the requirements on practices regarding remote identification will further foster trust in the services from the eIDAS Regulation. An implementing act is needed referring to standards with respect to which remote identification tools and procedures can be evaluated.

2.3. Proposals

We propose to amend the eIDAS Regulation in order to give the European Commission the mandate for an implementing act specifying the requirements for remote identification according to Article 24(1). Eliminating the text "recognized at a national level" in matters concerning remote identification in Art. 24(1)(d) should also be considered.

5 Traficomin havainnot hyväksytyistä ja ei-hyväksytyistä luottamuspalveluista

Tähän kohtaan on koottu eIDAS-asetuksen luottamuspalveluosaan liittyviä havaintoja.

On tärkeää huomata, että eIDAS-asetuksen tunnistusta koskeva sääntely ja luottamuspalveluita koskeva sääntely ovat täysin erillisiä osioita vaatimusten, jäsenvaltioiden yhteistoiminnan ja valvonnan organisoinnin kannalta.

Mukana on lainaukset FESAn lausunnosta Komissiolle.

5.1 Mitä ovat eIDAS-asetuksen luottamuspalvelut

Luottamuspalvelut ovat eIDAS-asetuksessa säädettyjä sähköisiä toimintoja, joita käytetään osana sähköisiä palveluita ja transaktioita. Palvelutyypit määritellään asetuksessa.

Qualified. Tietyille luottamuspalveluille voi hankkia hyväksytyn (qualified) statuksen. Se edellyttää akkreditoidun arviointilaitoksen tekemää arviointia ja valvovan viranomaisen hyväksyntää. Hyväksytyt luottamuspalvelut merkitään luotettuun luetteloon (trusted list), jolla on luotettavuus koko EU:ssa.

Non-qualified. Jos luottamuspalvelulle ei ole hankittu hyväksyntää, sen status on ei-hyväksytty eli non-qualified. Tähän ryhmään voi sääntelyn puitteissa kuulua myös sellaisia palvelutyyppejä, joille ei ole edes mahdollista hankkia hyväksyntää. Keskeisin näistä on arviomme mukaan sähköisen allekirjoituksen tai leiman luontipalvelu. Ei-hyväksyttyjä palveluja valvotaan ainoastaan jälkikäteen mahdollisten valitusten ja häiriöilmoitusten perusteella.

Hyväksytyt (qualified) luottamuspalvelut voivat olla seuraavia

- Qualified certificate for electronic signature
- Qualified certificate for electronic seal
- Qualified certificate for website authentication
- Qualified validation service for qualified electronic signature
- Qualified preservation service for qualified electronic signature
- Qualified validation service for qualified electronic seal
- Qualified preservation service for qualified electronic seal
- Qualified time stamp
- Qualified electronic registrered delivery service

Ei-hyväksytyt (non-qualified) luottamuspalvelut voivat olla seuraavia

- Certificate for electronic signature
- Certificate for electronic seal
- Certificate for website authentication

- Validation service for electronic signature
- *Generation service for electronic signature*
- Preservation service for electronic signature
- Validation service for electronic seal
- *Generation service for electronic seal*
- Preservation service for electronic seal
- *Time stamp service*
- Electronic registrered delivery service
- *Non-regulatory, nationally defined trust service*
- *Undefined type*

Edellä oleva luottamuspalvelutyyppien lista on kopioitu komission hakukoneesta.

Lisätietoa

Linkki:

Komission hakusivu jäsenvaltioiden luottamuspalveluista Trusted list browser

5.2 Hyväksyttyjen luottamuspalveluiden vaatimusten täsmentäminen valmiilla ETSIn standardeilla (eIDAS useat artiklat)

eIDAS-asetuksessa säädetään tyhjentävästi ne palvelutyypit, joille on mahdollista hankkia hyväksytyn luottamuspalvelun status. Näiden palvelutyyppien varsinaisia vaatimuksia koskevat artiklat ovat luonnollisesti yleispiirteisiä, mutta niihin liittyy säännönmukaisesti komission toimivaltuus tarkentaa vaatimuksia täytäntöönpanoasetuksella. ETSI on laatinut kattavasti standardit eri palveluille, mutta niiden soveltaminen tuotannossa tai vaatimustenmukaisuuden arvioinnissa ei ole pakollista. Epäselvät vaatimukset aiheuttavat epävarmuutta ja tehottomuutta ja epäyhdenmukaisuutta palveluntarjoajille, vaatimustenmukaisuuden arvioijille ja valvoville viranomaisille.

Suomessa olemme lisänneet tunnistus- ja luottamuspalvelumääräykseen 72 viittaukset ETSI:n standardeihin niiden palveluiden osalta, joiden standardit olivat valmiina määräystä valmisteltaessa 2016. Määräys on notifioitu transparenssidirektiivin mukaisesti ja notifioinnissa ratkaisua ei kyseenalaistettu. Ottaen huomioon sen, että eIDAS-asetuksen on kaiketi tarkoitus olla luotettavuusvaatimusten osalta täysharmonisoiva ja hyväksytyille luottamuspalveluille on säädetty oikeusvaikutuksia, kansalliset sääntelyn tarkennukset eivät ole tyydyttävä ratkaisu.

Näemme, että komission täytäntöönpanosäädöksillä olisi tarkennettava luottamuspalveluiden vaatimuksia ja hyödynnettävä ETSIn tekemää kattavaa standardointityötä. FESAn jäsenten parissa pohdittu ehdotus on muuttaa täytäntöönpanosäädösten antaminen pakolliseksi ja tämä vaikuttaa selkeimmältä ratkaisulta ja helpottaisi myös komission harkintaa. eIDAS-asetuksen tunnistusta koskevassa osassa on määritelty pakollisia täytäntöönpanosäädöksiä ja ne komissio on antanut.

Yleisesti ottaen täytäntöönpanopäätösten antaminen edesauttaisi luottamuspalveluiden tarjoamista ja valvontaa, kun vaatimukset selkeytyisivät. Standardointi on edistynyt ja tarjoaa jo hyvän keinon tarkentaa vaatimukset.

FESA

4. Requirements of Qualified Trusted Services (eIDAS several articles).

4.1. Observation

ETSI has performed outstanding work producing almost all the standards called for by the Implementing Acts of the eIDAS Regulation regarding qualified trust services. These standards set a clear framework for (Qualified) Trusted Services ((Q)TSs) and help the eIDAS community to branch out on a global scale. Despite this work, the standards are yet not officially recognized and therefore there are still inconsistencies between (each of) the QTSs.

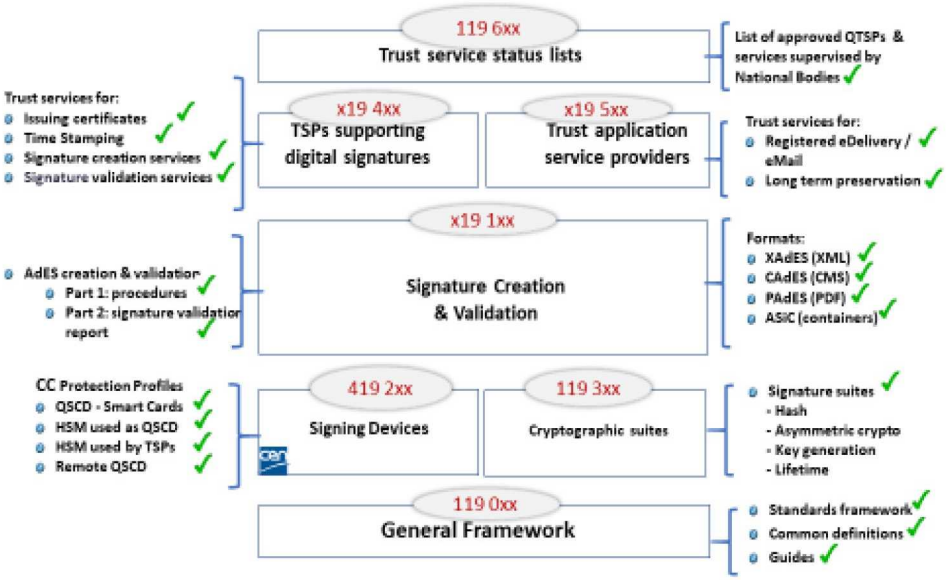
4.2. Motivation

Granting TSPs clarity on the requirements to comply with the eIDAS Regulation, thus harmonizing the products of European QTSPs. It would help data protection and privacy since these requirements would be a mandatory level of security guaranteeing a security framework. Ensuring harmonization of the different requirements and practices among the Member States, thus create a level playing field. Current ETSI standards set a clear framework for QTSs. This clear framework would help adoption outside of the EU and help the global reach of the eIDAS Regulation.

4.3. Proposal

We propose a mandatory adoption of the Implementing Acts already foreseen by the eIDAS Regulation, adopting the currently published standards concerning the requirements of QTSs (eIDAS Arts. 24(5), 28(6), 32(3), 33(2), 34(2), 38(6), 40, 42, 44(2) and 45).

5.2.1 ETSIN standardit



Lisätietoa

Linkki: ETSI Digital signature

Linkki: ETSI standards ja full list

5.3 Arviointilaitoksen akkreditointivaatimukset olisi tarkennettava (eIDAS art. 20.4 ja 24.2)

Hyväksytyn luottamuspalvelun tarjoajan on hankittava vaatimustenmukaisuuden arviointi arviointilaitokselta, joka on akkreditoitu nimenomaan eIDAS-vaatimusten arviointiin (*CAB, conformity assessment body*). Ilman arviointia hyväksytyn statuksen saaminen ei ole mahdollista.

Tunnistus- ja luottamuspalvelulain 4 luvun mukaan Suomessa akkreditoinnin tekee FINAS ja lisäksi Liikenne- ja viestintävirasto hyväksyy arviointilaitoksen.

eIDAS-asetuksessa itsessään ei tarkenneta akkreditointiperusteita eikä arviointilaitoksilta edellytettyjä arviointimenetelmiä. Asiaa koskevat standardit olisivat olemassa ja komissiolla olisi toimivalta saattaa standardit käyttöön täytäntöönpanosäädöksellä. Komissio ei ole käyttänyt tätä toimivaltaa ja se on saanut aikaan laadun hajontaa jäsenvaltioissa. Kansainvälisillä foorumeilla on käynyt selväksi, että kaikki osapuolet pitäisivät komission täytäntöönpanopäätöksiä ja tarkennuksia tarpeellisina. Myös arviointilaitokset, koska harmonisointi helpottaisi niiden toimintaa useammassa maassa. Kansallisten akkreditointiyksiköiden yhteistyöelin, EA (*European Co-operation for Accreditation*), on linjannut vaatimuksia: *EA Certification Committee Reference Paper; ETSI / EA Recommendations regarding; Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1.* Linjaus ei ole sitova, eikä sitä siten noudateta johdonmukaisesti.

Suomessa Traficom, FINAS ja tietoturvallisuuden arviointia harjoittavat yritykset ovat käyneet jonkin verran vuoropuhelua asiasta vuosina 2016-2017. Traficom on laatinut asiasta 8.3.2017 tiedonvaihtomuistion (dnro 81/060/2016), jonka pohjalta neuvontaa ja koordinointia voidaan tarvittaessa jatkaa. Arvioimme, että tietoturva-arvioijat ovat osoittaneet varovaista kiinnostusta akkreditoinnin hankkimiseen. Akkreditoitumista vaikuttaa hidastaneen ainakin vaatimusten epäselvyys ja epäselvyys siitä, olisiko akkreditoinnissa mahdollista lukea hyväksi muita akkreditointeja. Markkinaa on vaikea arvioida, mutta akkreditointi on voimassa koko EU:ssa. Suomen toistaiseksi ainoa hyväksytty luottamuspalvelun tarjoaja DVV hankkii arvioinnit ulkomailta.

Näemme, että vaatimustenmukaisuuden arviointilaitosten vaatimusten tarkentaminen komission täytäntöönpanoasetuksilla voisi edesauttaa myös kotimaisten toimijoiden akkreditoitumista ja parantaisi ulkomailta saamiemme arviointiraporttien laatua.

Vaatimustenmukaisuuden arviointilaitosten akkreditointiperusteet ja arviointiraporttien vaatimukset tulisi yhdenmukaistaa jäsenvaltioissa. Akkreditointia koskevat standardit ovat kypsiä ja laajalti käytettyjä, joten niiden noudattamista voisi jo edellyttää kaikilta. Myös raporttia koskeva standardointi on riittävän pitkällä. Sääntelyn tarkentaminen helpottaisi kaikkien osapuolten hallinnollista taakkaa ja parantaisi raportoinnin laatua, jonka vaihtelevuus hankaloittaa valvovien viranomaisten työtä. Näemme, että sääntelyn yhdenmukaistaminen tasoittaisi myös arviointilaitosten kilpailuedellytyksiä Euroopassa.

FESA

1. Standards for the accreditation of Conformity Assessment Bodies (eIDAS Arts. 20(4) and 24(2))

1.1. Observation

We see a wide variety in certification schemes used by Conformity Assessment Bodies (CABs), both in audit effort and quality, which is reflected in Conformity Assessment Reports (CARs) received by Supervisory Bodies (SBs). Although there is a recommendation of the EA, there is no mandatory accreditation scheme for the CABs, further increasing the risk of a nonharmonized approach of conformity assessments of trust services. This situation leads to a clear risk that (Qualified) Trust Service Providers ((Q)TSPs) will turn to the CABs that are operating a less demanding (and less costly) certification scheme.

1.2. Motivation

Harmonization in conformity assessment of Qualified Trust Services (QTSs) is essential for building actual trust in trust services and for mutual recognition of trust services. Harmonization of accreditation and Conformity Assessment Reports (CARs) will allow fair competition between the CABs and will reduce the incentive for QTSPs aiming at the lowest price. Clear and transparent accreditation and certification schemes will foster the uptake and global reach of the eIDAS Regulation. The credibility of conformity assessments and the quality of the CARs will enhance adoption of harmonized accreditation and certification schemes. It will enable TSPs to better make a weighed choice in selecting a CAB without having to make concessions on the quality of the CARs.

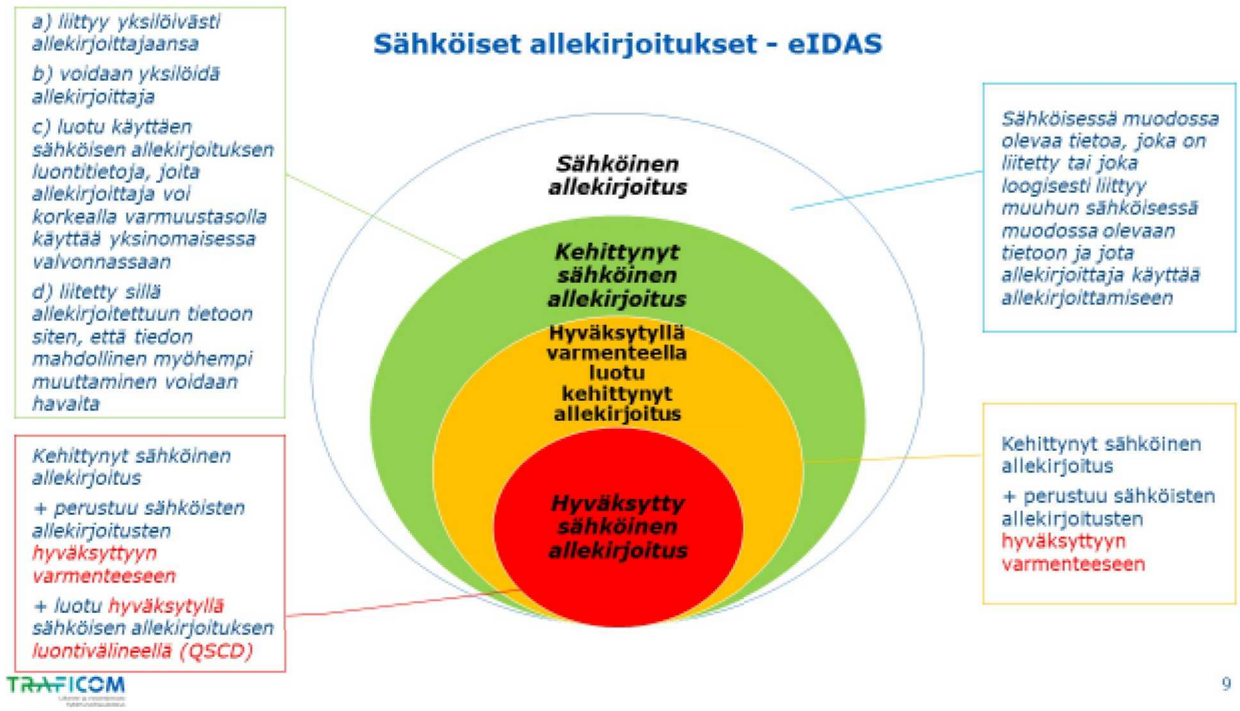
1.3. Proposal

We propose to promulgate an implementing act as foreseen in article 20(4) referencing ETSI EN 319 403-1 and ETSI EN 319 403-3.

5.4 Sähköisen allekirjoituksen tai sähköisen leiman luontipalvelut (eIDAS artikla 29.2 and Liite II kohdat 3 ja 4)

5.4.1 Kuva sähköisen allekirjoituksen tasoista

Seuraavassa kuvassa näkyvät eIDAS-asetuksen sähköisen allekirjoituksen tasot ja niiden osatekijät.



5.4.2 Sähköisen allekirjoituksen luontiväline (QSCD) allekirjoituksen osatekijänä

Käsityksemme mukaan sähköisen allekirjoituksen käyttäminen Suomessa on hajanaista ja pääasiassa organisaatiokohtaista eli allekirjoituksia tai leimoja ei välttämättä voida validoida organisaation ulkopuolella.

Käyttäjien (organisaatioiden) ja allekirjoituspalveluiden tarjoajien tietämys eritasoisista sähköisistä allekirjoituksista tai sähköisistä leimoista on neuvontakyselyjen perusteella vaihtelevaa. Tähän vaikuttanee osaltaan se, että ainoastaan eräille allekirjoituksen tai leiman osatoiminnoille on valvonta- ja hyväksyntämenettely, mutta allekirjoitus- tai leimapalvelun kokonaisuuden vaatimustenmukaisuudelle ei voi hankkia mitään objektiivista virallista vahvistusta.

Oikeusvaikutuksiltaan käsin tehtyä allekirjoitusta vastaavan (eIDAS art. 25) hyväksytyn sähköisen allekirjoituksen tekeminen edellyttää

1) kehittynyttä sähköistä allekirjoitusta (käytännössä julkisen avaimen menetelmää eli PKI:n käyttöä, *PKI eli public key infratructure*),
2) allekirjoittajan hyväksyttyä allekirjoitusvarmennetta (jolla julkisen avaimen menetelmä onkin mahdollista toteuttaa) ja
3) lisäksi sertifioitua sähköisen allekirjoituksen luontivälinettä (jolla PKI-menetelmän kriittisin tekijä eli julkista avainta vastaava yksityinen avain säilytetään, *QSCD eli Qualified electronic Signature Creation Device*).

Suomessa myös kutsutaan usein sähköiseksi allekirjoitukseksi sitä, että tehdään oikeustoimia vahvan sähköisen tunnistuksen perusteella. eIDAS-asetukseen nähden nämä menettelyt vastaavat arviomme mukaan kolmesta tasosta todennäköisesti alimman perustason sähköistä allekirjoitusta tai leimaa. Jos menettelyyn lisätään allekirjoittajan varmenteen käyttö, kysymyksessä voi olla kehittynyt sähköinen allekirjoitus. Pelkkään tunnistamiseen perustuvaa sähköistä oikeustointa voi verrata reaalimaailmassa siihen, että allekirjoittaja esittää henkilöllisyystodistuksensa virkailijalle ja virkailija allekirjoittaa tai leimaa asiakirjan. Sähköisen asioinnin tarpeiden lisääntyessä tämä on riittämätöntä eikä tue mahdollisuutta toimittaa ja validoida sähköisesti allekirjoitettuja asiakirjoja kotimaisten tai ulkomaisten organisaatioiden välillä.

Jos edellisessä kappaleessa kuvattuun menettelyyn lisätään allekirjoittajan varmenteen käyttö, kysymyksessä voi olla kehittynyt sähköinen allekirjoitus (*advanced electronic signature, AdES*).

Vanhastaan sähköisen allekirjoituksen luontivälineeksi on ollut mahdollista sertifioida ainoastaan siruja, jollainen on esimerkiksi henkilökortilla tai organisaatiokortilla. Standardit palvelimella säilytettävän luontivälineen sertifioinnille ovat valmistuneet 2019 ja komissio valmistelee parhaillaan niiden lisäämistä asiaa koskevaan täytäntöönpanosäädökseen (EU) 2016/650.

Sirujen tavoin uusien standardien mukaiset palvelinmodulit (*HSM, hard secure module)* ovat tuotteita, joita valmistavat ja sertifioivat erikoistuneet toimijat. Suomessa ei ole nimettyjä sertifiointilaitoksia (*designated certification body). Ks. eIDAS artikla 30 Hyväksyttyjen sähköisen allekirjoituksen luontivälineiden sertifiointi ja artikla 39 Hyväksytyt sähköisen leiman luontivälineet sekä tunnistus- ja luottamuspalvelulaki 36 § Hyväksytyn sähköisen allekirjoituksen ja sähköisen leiman luontivälineen sertifiointi*.

Palvelimella oleva luontiväline mahdollistaa nk. palvelinpohjaisen sähköisen allekirjoituksen eli nk. etäallekirjoituksen toteuttamisen. Nykyisellään eIDAS-asetuksen täytäntöönpanosäädöksen mukaisesti luontivälinettä voi säilyttää ainoastaan hyväksytty luottamuspalveluntarjoaja. Kun allekirjoituspalvelu ei sääntelyn perusteella voi saada tällaista statusta, jäsenvaltioiden markkinoilla on syntynyt kombinaatioita, joissa esimerkiksi hyväksytyn aikaleiman tarjoaja säilyttää allekirjoituksen luontivälinettä ja katsoo tämän yhdistelmän perusteella tarjoavansa hyväksytyn sähköisen allekirjoituksen luontipalvelua.

Näemme ensinnäkin, että sähköisen allekirjoituksen ja leiman luontivälineen vaatimusten tarkentaminen tuoreiden standardien avulla komission täytäntöönpanopäätöksessä edesauttaisi näiden palveluiden tarjoamisen lisäämistä myös Suomessa.

Toiseksi näemme, että sääntelyssä olisi arvioitava ja selvennettävä mahdollisuus osoittaa koko allekirjoituspalvelun luotettavuus, koska allekirjoittajan yksityisen avaimen säilytysmodulin tekninen luotettavuus ei yksin riitä vaan allekirjoituspalveluntarjoajan koko toteutuksella on merkitystä. Ts. tulisi olla mahdollista, että etäallekirjoituspalvelun tarjoaja voisi halutessaan hankkia hyväksytyn allekirjoituspalvelun statuksen. Sama koskee sähköistä leimaa.

Kehittyneen sähköisen allekirjoituksen ja leiman luontia tarkastellaan kohdassa 5.6

FESA

3. Server signing/sealing certification process (eIDAS Art. 29(2) and Annex II Arts. 3 and 4)

3.1. Observation

Stakeholders have different views on remote signing/sealing. With the increasing use of remote identification this issue will get more problematic and eventually put the trustworthiness of the eIDAS framework at stake.

3.2. Motivation

Providing greater clarity on the requirements for remote signing systems will lead to a higher level of assurance and confidence that such systems are meeting the requirements of the eIDAS Regulation. Similar to other harmonisation initiatives, this will provide enhanced confidence and easier decision making for consumers whilst also reducing potential variances in the security of such systems. This in turn will lead to greater confidence in the overall eIDAS scheme by non-EU parties and thus support global adoption. There is a need to make certification more comparable and give legal certainty to models like on the fly certification and subscribers managed Qualified electronic Signature Creation Devices (QSCDs).

3.3. Proposal

We propose to amend CID (UE) 2016/650 with the inclusion of EN 419 221-5 and EN 419 241-2 allowing a harmonized certification process in all Member States. Clarify the requirements regarding server signing services, also known as remote signing and signing on behalf. Specifying the type of QTSP that can manage signature or seal creation data on behalf of the signatory shall be considered. In particular Annex II of the eIDAS Regulation must be clarified.

Lisätietoa

Linkki: Komission sivut Compilation of Member States notification on SSCDs and QSCDs

5.5 Sähköisessä allekirjoituksessa/leimassa tarvittavan sirun tai palvelinmodulin (QSCD) sertifioinnin voimassaololle määräaika (eIDAS art. 24.2(d) ja (e) sekä 30.1)

Edellä käsiteltyyn sähköisen allekirjoituksen tai leiman luontivälineeseen liittyy myös sertifioinnin voimassaolon muutostarve.

Vertailun vuoksi hyväksytyt luottamuspalvelut on asetuksen mukaan arvioitava uudestaan kahden vuoden välein, joten niiden vaatimustenmukaisuuden arviointi ja ennakkovalvonta on säännöllistä.

Allekirjoituksen luontivälineiden sertifioinnin voimassaololle ei nyt ole säädetty määräaikaa. Näemme, että etäallekirjoituksen palvelinpohjaisten luontivälineiden

tuleminen sertifioinnin piiriin ja laajenevaan käyttöön lisää tarvetta arvioida säännöllisesti haavoittuvuutta.

FESA

5. Qualified electronic Signature Creation Devices (QSCDs) conformity certificate (eIDAS Arts. 24(2)(d), (e) and 30(1))

5.1. Observation

Assurance of conformity, for Qualified electronic Signature Creation Devices (QSCDs), is given once and is valid for an undefined period of time, regardless of discovered vulnerabilities and new requirements.

5.2. Motivation

The rise of remote QSCDs increases the need of periodic vulnerability assessment and set limitations to validity period of QSCDs. This might also impact the eID infrastructure of Member States, since some QSCDs are used as electronic identity cards.

5.3. Proposal

We propose to limit the validity of a QSCDs' conformity certificate and demand a periodic vulnerability assessment. This could be reached by promulgating Implementing Acts, containing details on the validity period of QSCDs, including SSCDs, on the withdrawal of the QSCD conformity certificate (e.g., in case of a vulnerability that has been discovered), and on the frequency of vulnerability assessments.

5.6 Ei-hyväksyttyjen luottamuspalveluiden statuksen ja valvonnan jäsentymättömyys (eIDAS art. 19, art. 17)

Ei-hyväksytyt luottamuspalvelut ovat samoja tyhjentävästi säädettyjä palvelutyyppejä/toimintoja kuin hyväksytyt luottamuspalvelut, mutta niille ei ole tehty vaatimustenmukaisuuden arviointia eikä niitä ole ilmoitettu ja hyväksytty trusted listille. Lisäksi on joitain toimintoja, jotka eivät voi olla hyväksyttyjä luottamuspalveluita, mutta ovat ei-hyväksyttyjä. Tällainen on esimerkiksi kehittyneen sähköisen allekirjoituksen luontipalvelu.

eIDAS-asetuksessa on ei-hyväksyttyjä luottamuspalveluita koskevaa sääntelyä, mm.

- 19 artiklan yleistasoiset tietoturva- ja häiriöraportointivelvoitteet
- Artiklat 13 Vastuu ja todistustaakka, 14 Kansainväliset näkökohdat, 15 Esteettömyys vammaisten näkökulmasta ja 16 Seuraamukset. Nämä eivät ole keskeisiä tietoturvavalvonnan kannalta, joten näitä ei selosteta tässä enemmälti.
- Rajallisesta jälkikäteisestä valvonnasta säädetään 17 artiklassa
- 18 artikla valvontaelimien keskinäisestä avunannosta soveltuu.
- Eri luottamuspalvelutyypeistä on säännöksiä, jotka koskevat toiminnon käyttämisen oikeusvaikutuksia tai toiminnon vaatimuksia: sähköiset allekirjoitukset (artiklat 25.1, 26, 27), sähköiset leimat (artiklat 35.1, 36, 27/, sähköiset aikaleimat (artikla 41) ja sähköiset rekisteröidyt jakelupalvelut (artikla 43).

Pidämme ongelmallisena sitä, että ei-hyväksyttyjen luottamuspalveluiden sääntely jää näennäiseksi ja ennakoimattomaksi. Palveluiden tarjoajat eivät voi hankkia objektiivista vahvistusta palveluiden vaatimustenmukaisuudelle. Palveluiden käyttäjät (yhteisöt tai kuluttajat) eivät voi varmistua palveluiden luotettavuudesta. Sääntelyn tulkinta jäsenvaltioissa ei voi olla yhdenmukaista, kun selkeitä vaatimuksia ei ole.

Suomessa tämä epävarmuus tulee meiltä pyydetyssä neuvonnassa esille erityisesti kehittyneen sähköisen allekirjoituksen palveluissa.

Näemme, että asetuksen arvioinnissa pitäisi tarkastella ei-hyväksyttyjen luottamuspalveluiden vaatimusten ja ennakkovalvonnan mahdollisuutta sekä listaamista trusted listille.

Näemme, että sähköisen allekirjoituksen palveluiden vaatimuksenmukaisuuden osoittamista ja luotettavuutta kuluttajille ja yrityksille on tarpeen parantaa. Erityisesti tämä koskee etäallekirjoituspalveluita. Sääntelyllä tulisi tarjota myös kehittyneen sähköisen allekirjoituksen tai leiman luontipalveluille tapa osoittaa vaatimustenmukaisuus yhdenmukaisesti kaikissa jäsenvaltioissa.

Toisen ääripään ratkaisu olisi poistaa koko ei-hyväksytyn luottamuspalvelun sääntely tai sen valvontatehtävä, koska se ei nykyisellään juurikaan tarjoa lisävarmuutta käyttäjille. Esimerkiksi palveluntarjoajan markkinointiväittämiä siitä, että palvelussa pystytään tuottamaan kehittynyt sähköinen allekirjoitus, ei ymmärtääksemme voida todentaa objektiivisesti.

Ei-hyväksytyn luottamuspalvelun säännöksiä:

19.1 artiklan mukaan *ei-hyväksyttyjen luottamuspalvelun tarjoajien on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet hallitakseen tarjoamiensa luottamuspalvelujen tietoturvaan kohdistuvat riskit. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu tietoturvataso, ottaen huomioon uusin tekninen kehitys.*

19.4 artiklan mukaan *Komissio voi täytäntöönpanosäädöksillä a) määrittää 1 kohdassa tarkoitetut toimenpiteet tarkemmin*

17.3 artiklan mukaan *Valvontaelimellä on seuraavat tehtävät: b) toimien toteuttaminen tarvittaessa nimeävän jäsenvaltion alueelle sijoittautuneiden ei-hyväksyttyjen luottamuspalvelun tarjoajien suhteen jälkikäteen toteutettavin valvontatoimin, jos sille ilmoitetaan, että nämä ei-hyväksytyt luottamuspalvelun tarjoajat tai niiden tarjoamat luottamuspalvelut eivät väitetysti täytä tässä asetuksessa säädettyjä vaatimuksia.*

Johdantokappale *36) Kaikkia luottamuspalvelun tarjoajia koskevan valvontajärjestelmän perustamisessa olisi varmistettava tasapuoliset edellytykset niiden toimien ja palvelujen tietoturvalle ja vastuuvelvollisuudelle, jolloin edistetään käyttäjien suojelua ja sisämarkkinoiden toimintaa. Ei-hyväksyttyihin luottamuspalvelun tarjoajiin olisi sovellettava joustavia ja reaktiivisia jälkikäteen toteutettavia valvontatoimia, jotka ovat perusteltavissa niiden palvelujen ja toimien luonteella. Valvontaelimellä ei siis pitäisi olla yleistä velvoitetta valvoa ei-hyväksyttyjä palveluntarjoajia. Valvontaelimen pitäisi toteuttaa toimia vain silloin, kun se saa tietää (esimerkiksi ei-hyväksytyn luottamuspalvelun tarjoajan itsensä tai muun valvontaelimen taholta, käyttäjän tai liikekumppanin ilmoituksen perusteella tai oman tutkintansa perusteella), että ei-hyväksytty luottamuspalvelun tarjoaja ei täytä tämän asetuksen vaatimuksia.*

Lisätietoa

Linkki: Traficomin tunnistus- ja luottamuspalvelumääräyksen perustelumuistio MPS72

Perustelumuistiossa käsitellään sähköistä allekirjoitusta vuoden 2016 tilanteessa seuraavissa kohdissa:

s. 37 Vaikutusarviointi, Ei-hyväksytyt luottamuspalvelut ja luotettu luettelo. Arvioitu kysymys: Olisiko Suomessa perusteita tai tarvetta merkitä luotettuun luetteloon (trusted list) muitakin palveluita kuin hyväksyttyjä luottamuspalveluita? Olisiko tämä mahdollista eIDASasetuksen ja tunnistus- ja luottamuspalvelulain perusteella?

s. 78 Muut määräyksen aihepiiriin liittyvät asiat, Kehittyneet sähköiset allekirjoitukset

s. 92 Luottamuspalvelut ja sähköiset allekirjoitukset, liitteessä esitellään hyvin yleisellä tasolla eIDAS-asetuksen tarkoittamat luottamuspalvelut ja sähköiset allekirjoitukset ja leimat.

5.7 Häiriöilmoitusvelvollisuus kattamaan myös uhkat ja haavoittuvuudet (eIDAS art. 19.2)

eIDAS-asetuksen 19.2 artiklassa säädetään hyväksyttyjen ja ei-hyväksyttyjen luottamuspalveluiden häiriöilmoitusvelvollisuudesta valvovalle viranomaiselle ja tarvittaessa jäsenvaltioiden välillä.

Ilmoitusvelvollisuus koskee "*tietoturvaloukkauksista ja eheyden menetyksiä, joilla on huomattavia vaikutuksia tarjottuun luottamuspalveluun" ("any breach of security or loss of integrity that has a significant impact on the trust service").* Sanamuoto ei kata tai vähintään jättää tulkinnanvaraiseksi tietoturvauhkista- tai haavoittuvuuksista ilmoittamisen ja läheltä-piti -häiriötilanteet. Tiedonsaanti näistä on ennaltaehkäisemisen kannalta yhtä tärkeää kuin tiedonsaanti vahinkoa aiheuttaneista häiriöistä.

Suomessa saamme toistaiseksi ainoalta hyväksytyltä luottamuspalveluntarjoajalta, DVV:ltä, erinomaisesti tietoa häiriöistä. Ei-hyväksytyille luottamuspalveluille on häiriöilmoituslomake, mutta yleisen tietoisuuden puuttumisen takia sitä kautta ei tule tietoa.

Näemme, että häiriöilmoitusvelvollisuus täytyy selkeästi ulottaa kattamaan tietoturvauhkat mukaan lukien haavoittuvuudet. Esimerkiksi nk. telekoodissa (EECC 40 artikla, "*threat of a security incident*") on tehty näin.

Näemme, että Komission asetuksella mahdollisesti tarkennettava häiriöilmoitusvelvollisuus ja lomake olisi kannaltamme tarkoituksenmukainen ratkaisu. Se voisi myös tehostaa tiedonsaantia ei-hyväksyttyjen luottamuspalveluiden häiriöistä, mutta tämän suhteen on kuitenkin huomioitava, että ei-hyväksyttyjen luottamuspalveluiden valvontaan ei ole suunniteltu resursseja.

FESA

6. Sharing information on vulnerabilities and almost incidents (eIDAS Art. 19(2))

6.1. Observation

In order to contribute to trust in the European Digital Single Market it is essential that the SBs receive the necessary information on vulnerabilities and almost incidents as soon as possible. Sharing information on vulnerabilities, almost incidents and threats is a pre-requisite for building trust. The ROCA vulnerability showed that all Member States and stakeholders had very different modus operandi.

6.2. Motivation

Sharing information in general and about technical vulnerabilities without providing specific details of national QTSPs will offer all involved parties convenience. Recent events show that early warnings are essential (e.g. ROCA, Grenfell Towers, Ponte Morandi Genua). Acting upon early warnings will help to mitigate possible negative impact on the trust ecosystem as a whole and help to retain the essential trustworthiness consumers expect from eIDAS governed Trust Services.

6.3. Proposal

We propose to provide clarity on sharing information on vulnerabilities and almost incidents. Notification to interested parties should be harmonized. We propose to provide guidelines based on recital 39 and to promulgate an Implementing Act as foreseen in Art.19(4).

5.8 Hyväksytyn luottamuspalvelun hallittu lopettaminen (eIDAS art. 24.2 (i))

Monet hyväksytyt luottamuspalvelut ovat sen luonteisia, että niiden palveluihin luottaneilla tahoilla on tarve pystyä varmistamaan toimien luotettavuus, vaikka hyväksytty luottamuspalveluntarjoaja lopettaa toiminnan. Esimerkiksi on kyettävä varmistamaan jälkikäteen, onko hyväksytty allekirjoitusvarmenne ollut voimassa allekirjoitushetkellä.

eIDAS-asetuksen vaatimukset hallitulle toiminnan lopettamiselle ja jälkikäteisten tarpeiden turvaamiselle ovat erittäin yleispiirteiset.

Suomessa on toistaiseksi yksi hyväksytty luottamuspalveluntarjoaja, joka on valtion virasto, joten sääntelyn ja vastuiden epätarkkuus eivät ole meillä akuutti ongelma.

Näemme kuitenkin, että digitalisaation eteneminen lisännee Suomessakin väistämättä jollain aikavälillä kysyntää hyväksytyille luottamuspalveluille ja markkinoille voi tulla myös yksityisiä toimijoita. Näin on varsinkin, jos etäallekirjoituspalveluiden asema eIDAS-asetuksessa muuttuu arvion myötä jollain aikavälillä. Jos tarjontaa ei synny Suomeen, yritykset hankkivat tarpeelliset luottamuspalvelut mahdollisuuksien mukaan ulkomailta ja tällöinkin niiden luotettavuus vaikuttaa suomalaisiin yhteisöihin. Vaikka kysymys ei ole akuutti, asian arviointi on relevanttia ja kannatettavaa.

FESA

7. Termination of Qualified Trust Services (eIDAS Art. 24(2)(i))

7.1. Observation

At the moment the eIDAS regulation does not have any requirements on the termination of QTSs except a general requirement for the termination plan, causing different practices and understandings of this process. Currently there is no common understanding on what should be arranged beforehand for example financially, on different scenario's, on the continuity of active services, logs or specific services for the signatory.

7.2. Motivation

QTSPs, like any other company, may find themselves in a situation where they have to voluntarily or forcefully terminate their services. To ensure sustainability and durability of qualified trust services and to boost user confidence in the continuity of qualified trust services it is essential that QTSPS have provisions in place to ensure a smooth transition. Harmonization of requirements and practices related to termination of qualified trust services among all Member States will ensure a common understanding and foster a levelled playing field.

7.3. Proposal We propose to harmonize the requirements related to termination of qualified trust services. We propose to promulgate an Implementing Act as foreseen in Art. 24(5).

Yksikönpäällikkö Heidi Kivekäs
Hyväksytty 10.6.2020

Johtava asiantuntija Anne Lohtander
Esitelty 10.6.2020

Tämä asiakirja on allekirjoitettu sähköisesti. Liikenne- ja viestintävirasto (Traficom). Allekirjoituksen oikeellisuuden voi todentaa Traficomin kirjaamosta.

Dokumentet har undertecknats elektroniskt. Transport- och kommunikationsverket (Traficom). Underskriftens riktighet kan verifieras hos Traficoms registratorskontor.

This document has been signed electronically. Finnish Transport and Communications Agency (Traficom). The authenticity of the signature can be verified from Traficom's registry.