LIIKENNE- JA VIESTINTÄMINISTERIÖN JULKAISUJA 52/2004
Viestintä

Turvalliset sähköisen allekirjoituksen luomisvälineet

Vaatimusten arviointi

Liikenne- ja viestintäministeriö
Helsinki, 2004

LIIKENNE- JA VIESTINTÄMINISTERIÖ

KUVAILULEHTI

Julkaisun päivämäärä
6.9.2004

Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)	Julkaisun laji
Valimo Wireless Oy	Raportti
	Toimeksiantaja: Liikenne- ja viestintäministeriö
	Toimielimen asettamispäivämäärä

Julkaisun nimi

Turvalliset sähköisen allekirjoituksen luomisvälineet. Vaatimusten arviointi

Tiivistelmä

Tutkimus tehtiin konsulttityönä liikenne- ja viestintäministeriön toimeksiannosta. Tutkimuksessa selvitettiin turvallisten sähköisten allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arviointia eri Euroopan maissa. Jotta allekirjoituksen luomisväline voidaan luokitella turvalliseksi allekirjoituksen luomisvälineeksi, tulee sen täyttää EU:n direktiivillä asettamat vaatimukset. EU:n direktiivi sähköisistä allekirjoituksista määrittelee yleiset vaatimukset turvallisille sähköisille allekirjoitusmenetelmille. Näitä yleisiä vaatimuksia tarkentaakseen EU:n komissio on julkaissut yksityiskohtaisen standardin (CWA 14169). EU:n direktiivin mukaisesti kaikki allekirjoituslaitteet, jotka täyttävät kyseisen standardin vaatimukset, täyttävät myös direktiivin vaatimukset.

Selvitystyössä keskityttiin tutkimaan, mitä turvallisia allekirjoitusten luomisvälineitä tutkituissa maissa on käytössä ja miten näiden luomisvälineiden vaatimustenmukaisuus on arvioitu. Lisäksi pyrittiin selvittämään, mitä kaikkea allekirjoitusten luomisvälineen käsitteeseen eri maissa kuuluu ja miten ja mitä seikkoja huomioiden ja millaisin menettelyin vaatimustenmukaisuuden arviointi olisi tarkoituksenmukaisinta ja joustavinta tehdä.

EU on direktiivillä antanut jäsenvaltioille perusteet, joiden perusteella jäsenvaltiot voivat nimetä tarkastus- ja arviointilaitoksia arvioimaan sähköisten allekirjoitusten luomisvälineiden vaatimustenmukaisuuden täyttymistä. Niissä tutkituissa maissa, joissa erillinen arviointi- tai tarkastuslaitos laitos on nimetty, keskityttiin tutkimaan kyseisen laitoksen toimintatapoja ja -periaatteita.

Niiden maiden osalta, joissa erillistä arviointilaitosta ei ole nimetty, pyrittiin selvittämään miten kyseisissä maissa arviointitoiminta on järjestetty.

Avainsanat (asiasanat)

sähköinen allekirjoitus, allekirjoituksen luomisväline, allekirjoituksen luomismenetelmä, julkisen avaimen menetelmä, PKI, varmenne, laatuvarmenne, hyväksytty varmenne, arviointilaitos, tarkastuslaitos

Muut tiedot

Yhteyshenkilö LVM/Juha Perttula

Sarjan nimi ja numero	ISSN	ISBN
Liikenne- ja viestintäministeriön julkaisuja 52/2004	1457-7488	951-723-738-3

Kokonaissivumäärä	Kieli	Hinta	Luottamuksellisuus
50	suomi	10 €	julkinen

Jakaja	Kustantaja
Edita Publishing Oy	Liikenne- ja viestintäministeriö

KOMMUNIKATIONSMINISTERIET

PRESENTATIONSBLAD

Utgivningsdatum
6.9.2004

Författare (uppgifter om organet: organets namn, ordförande, sekreterare)	Typ av publikation
Valimo Wireless Oy	Rapport
	Uppdragsgivare Kommunikationsministeriet
	Datum för tillsättandet av organet

Publikation (även den finska titeln)

Utredning över anordningar for säkra signaturer
(Turvalliset sähköisen allekirjoituksen luomisvälineet. Vaatimusten arviointi)

Referat

Undersökningen utfördes som konsultarbete på uppdrag av kommunikationsministeriet. Undersökningen utredde bedömningen av överensstämmelse för säkra elektroniska signaturer. För att en anordning för elektroniska signaturer skall kunna klassificeras som en anordning för säkra signaturer skall den uppfylla de krav som ställs i EU-direktivet om elektroniska signaturer. Direktivet definierar de allmänna kraven på säkra elektroniska signaturmetoder. För att precisera dessa allmänna krav har EU-kommissionen publicerat en detaljerad standard (CWA 14169). Alla signaturanordningar som uppfyller kraven i denna standard uppfyller enligt EU-direktivet samtidigt också direktivets krav.

Undersökningsarbetet fokuserades på att utreda vilka anordningar för säkra signaturer som används i de undersökta länderna och hur dessa signaturanordningars överensstämmelse med kraven har bedömts. Vidare strävade man efter att utreda vad som i de olika länderna inkluderas i begreppet anordning för signaturer och vilka faktorer som skall beaktas och vilka metoder som skall användas för att så ändmålsenligt och flexibelt som möjligt bedöma överensstämmelsen.

EU har i direktivet gett medlemsstaterna grunder enligt vilka de kan utse organ för att övervaka och bedöma överensstämmelsen med kraven för anordningar för elektroniska signaturer. I de undersökta länder som har utsett ett separat organ för att bedöma eller övervaka överensstämmelsen fokuserades undersökningen på att undersöka ifrågavarande organs verksamhetsmetoder och principer.

I fråga om de länder där ett särskilt organ inte hade utsetts för bedömningen strävade man efter att utreda hur bedömningsverksamheten har arrangerats.

Nyckelord

elektronisk signatur, anordningar for säkra signaturer, öppen nyckel-system, PKI, certifikat, kvalitets-certifikat

Övriga uppgifter

Kontaktperson vid ministeriet: Juha Perttula

Seriens namn och nummer		ISSN	ISBN
Kommunikationsministeriets publikationer 52/2004		1457-7488	951-723-738-3
Sidoantal	Språk	Pris	Sekretessgrad
50	finska	€ 10	offentlig
Distribution		Förlag	
Edita Publishing Ab		Kommunikationsministeriet	

MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

DESCRIPTION

Date of publication
6 September 2004

Authors (from body; name, chairman and secretary of the body)	Type of publication
Valimo Wireless Oy	Report
	Assigned by Ministry of Transport and Communications
	Date when body appointed

Name of the publication
Assessment of requirements for secure-electronic-signature-creation devices

Abstract

This study was commissioned by the Ministry of Transport and Communications of Finland. The purpose of the study was to examine the assessment of conformity of secure-electronic-signature-creation devices in European countries.

In order to be able to categorise a signature-creation-device as secure, it must meet the requirements laid down in an EU Directive. The EU Directive on Community Framework for Electronic Signatures defines the general requirements for secure-electronic-signature devices. For the purposes of specifying these general requirements, the EU Commission has published a detailed standard (CWA 14169). In accordance with the Directive, all signature hardware that meet the requirements of the standard also fulfil the requirements of the Directive.

The focus of the study was to find out what secure-signature-creation devices are used in the examined countries and how their conformity has been assessed. A further aim was to examine how the concept of a signature-creation device is defined in the countries and what aspects and measures should be used to assess the conformity in the most appropriate and flexible way.

By means of a Directive, the EU has provided Member States with guidelines for naming inspection and assessment bodies to assess the conformity of electronic-signature-creation devices.

If an examined country had a separate inspection and assessment body, the methods and principles of the body were analysed.

If a country did not have a separate assessment and inspection body, the aim was to find out how the assessments are carried out.

Keywords
electronic signature, secure-signature-creation device, public key infrastructure, PKI, certificate, qualified certificate, inspection body

Miscellaneous
Contact person at the Ministry: Mr Juha Perttula

Serial name and number		ISSN	ISBN
Publications of the Ministry of Transport and Communications 52/2004		1457-7488	951-723-738-3
Pages, total 50	Language Finnish	Price € 10	Confidence status Public
Distributed by Edita Publishing Ltd		Published by Ministry of Transport and Communications	

Esipuhe

Liikenne- ja viestintäministeriö teetti keväällä 2004 tarjouskilpailun perusteella selvityksen sähköisen allekirjoituksen turvallisista luomisvälineistä ja niitä koskevien vaatimusten arviointikäytännöistä muissa EU-maissa.

Sähköisistä allekirjoituksista annetun direktiivin (1999/93/EY) liitteessä III on yksilöity turvallista allekirjoituksen luomisvälinettä (SSCD) koskevat vaatimukset. Sähköisen allekirjoituksen luomisessa on käytettävä kyseiset vaatimukset täyttäviä luomisvälineitä, jotta allekirjoitus saisi direktiivin nojalla käsintehtyä allekirjoitusta vastaavat oikeusvaikutukset. Direktiiviä vastaavat vaatimukset sisältyvät Suomen sähköisistä allekirjoituksista annetun lain 5 §:ään.

Komissio on myös julkaissut luomisvälineitä koskevan standardin viitenumeron (CWA 14169) Euroopan yhteisöjen virallisessa lehdessä 15.7.2003. Kyseisen standardin mukaisia välineitä on pidettävä edellä mainittujen vaatimusten mukaisina. Direktiivi antaa jäsenvaltioille mahdollisuuden nimittää arviointilaitoksia arvioimaan sähköisen allekirjoituksen luomisvälineiden vaatimusten mukaisuutta. Tällaisia laitoksia on tällä hetkellä kuitenkin vasta muutamassa EU-maassa.

Selvityksessä pyrittiin selvittämään mm. mitä turvallisia allekirjoituksen luomisvälineitä eri maissa on käytössä, ja miten näiden luomisvälineiden vaatimustenmukaisuuden arviointi on toteutettu. Selvitykseltä toivottiin vastauksia erityisesti siihen, miten vaatimusten mukaisuuden arviointi on järjestetty niissä muissa EU-maissa, joissa ei ole nimetty erillistä arviointilaitosta tähän tehtävään.

Selvitys toteutettiin pääosin kyselytutkimuksena. Kyselyt lähetettiin esiselvityksen perusteella valittujen kymmenen EU-maan valvontaviranomaisille ja näissä maissa toimiville arviointilaitoksille.

Selvityksen toteuttamisesta vastasi Valimo Wireless Oy. Avainhenkilöinä toimivat Juha Remes ja Vesa Peltola. Liikenne- ja viestintäministeriön puolelta selvitystyötä ohjasi neuvotteleva virkamies Juha Perttula.

Liikenne- ja viestintäministeriö haluaa kiittää kaikkia niitä tahoja, jotka omalla panoksellaan tekivät selvityksen laatimisen mahdolliseksi.

Helsingissä 6 päivänä syyskuuta 2004

Juha Perttula

Neuvotteleva virkamies

SISÄLLYSLUETTELO

1 Yhteenveto 6
2 Johdanto 9
2.1 Aihealue ja tutkimuksen rakenne 9
2.2 Tutkimuksen työskentelymalli 9
3 EU:n direktiivi sähköisistä allekirjoituksista 10
3.1 Turvallisen allekirjoituksen luomisvälineen määrittely 10
3.2 Standardit 11
3.3 Arviointilaitokset 13
4 Sähköisen allekirjoituksen levinneisyys Euroopan valtioissa 15
5 EU-direktiivin huomioiminen kansallisessa lainsäädännössä 17
6 Vaatimukset turvalliselle allekirjoituksen luomisvälineelle 19
6.1 Itävalta 19
6.2 Belgia 20
6.3 Tanska 21
6.4 Viro 21
6.5 Ranska 21
6.6 Saksa 21
6.6.1 Historia 21
6.6.2 Vaatimukset nykylainsäädännössä (SigG and SigV) 22
6.7 Kreikka 23
6.8 Italia 23
6.9 Alankomaat 23
6.10 Norja 23
6.11 Yhteenveto 24
7 Arviointilaitosten toiminta 26
7.1 ITSEC 26
7.2 Common Criteria 26
7.3 FIPS 26
7.4 Arviointilaitokset 27
7.4.1 Arviointilaitokset organisaationa 27
7.4.2 Yleiset toimintatavat 29
7.5 Arviointiprosessit 31
7.5.1 Arviointia pyytäneet tahot 31
7.5.2 Arviointiperusteet valmistajaorganisaation arvioinnissa 31
7.5.3 Arviointiperusteet ja menettelytavat allekirjoituksen luomisvälineen arvioinnissa 31
7.5.4 Arvioinnin ajallinen kesto 35
7.5.5 Hyväksynnän voimassaolo 35
7.5.6 Kustannukset 35
7.5.7 Hyväksynnän käyttö markkinoinnissa 36
7.6 Kansainvälinen yhteistyö 36
7.7 Parannuskohteita 36
8 Toiminta ilman arviointilaitoksia 37
9 Lähdeluettelo 38

Liitteet

Liite 1: A-SIT:n arvioimat ja hyväksymät tuotteet

Liite 2: RegTp:n arvioimat ja hyväksymät tuotteet

Liite 3: DCSSI:n arvioimat ja hyväksymät tuotteet

Kuvaluettelo

Kuva 1: Vaihtoehtoiset menetelmät turvallisten allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arvioinnille.....12
Kuva 2: Arviointilaitosten toiminta ja toimintaa ohjaavat vaatimukset 14
Kuva 3: EU-direktiivi kansallisessa lainsäädännössä 17
Kuva 4: Sähköistä allekirjoitusta koskevan lainsäädännön voimaanastuminen eri Euroopan maissa.....18
Kuva 5: Arviointiprosessin kuvaus.....34

1 Yhteenveto

Sähköisen allekirjoituksen luomisvälineellä tarkoitetaan laitetta, ohjelmistoa tai niiden kombinaatiota, jolla sähköinen allekirjoitus voidaan luoda. Kyseisellä menetelmällä luodut sähköiset allekirjoitukset saavat samat oikeusvaikutukset kuin käsintehdyt allekirjoitukset, jos sähköisen allekirjoituksen luomisväline täyttää EU:n direktiivin asettamat vaatimukset turvallisille allekirjoituksen luomismenetelmille ja jos allekirjoitus perustuu hyväksyttyyn varmenteeseen.

Sähköistä allekirjoitusta koskevissa suomenkielisissä artikkeleissa sekä puhekielessä varsin yleisesti puhutaan joko allekirjoituksen ”luomisvälineestä” tai ”luomismenetelmästä”. Englannin kielessä käytetään yksiselitteisesti termiä ”Secure Signature Creation Device” (SSCD). Yleisesti ottaen näillä kaikilla termeillä tarkoitetaan itse fyysisen laitteen ja sen toiminnan mahdollistavien ohjelmistokomponenttien muodostamaa kokonaisuutta. Esimerkkinä mainittakoon toimikortti, sen lukijalaite, lukijalaitteen ajurit sekä esimerkiksi selainkäytön mahdollistavat ohjelmistomoduulit. Vastaavana esimerkkinä voidaan mainita matkapuhelin ja allekirjoitustoiminnallisuuden sisältävä SIM-kortti.

Jotta allekirjoituksen luomisväline voidaan luokitella turvalliseksi allekirjoituksen luomisvälineeksi, tulee sen täyttää EU:n asettamat vaatimukset. EU:n direktiivi sähköisistä allekirjoituksista määrittelee varsin yleiset vaatimukset turvallisille sähköisille allekirjoitusmenetelmille. Näitä yleisiä vaatimuksia tarkentaakseen EU:n komissio on julkaissut yksityiskohtaisen standardin (CWA 14169). Direktiivin perusteella kaikki allekirjoituksen luomisvälineet, jotka täyttävät kyseisen standardin vaatimukset, täyttävät myös EU-direktiivin vaatimukset. Näin ollen, allekirjoituksen luomisvälineen voidaan nähdä täyttävän EU:n asettamat vaatimukset, jos se täyttää joko suoraan EU-direktiivin vaatimukset tai standardin CWA 14169:n vaatimukset. Lisäksi yhtenä vaihtoehtona on arvioida täyttääkö allekirjoituksen luomisväline jonkun muun standardin vaatimukset, jonka lisäksi nähdään toteuttavan EU-direktiivin vaatimukset.

EU on asettanut jäsenvaltioille direktiivillä perusteet, jonka perusteella jäsenvaltiot voivat nimetä tarkastus- tai arviointilaitoksia arvioimaan sähköisten allekirjoitusten luomisvälineiden vaatimustenmukaisuuden täyttymistä. EU:n komissio on lisäksi päätöksellään määritellyt joukon yleisiä vaatimuksia, joita kyseisten arviointilaitosten tulee noudattaa omassa toiminnassaan.

EU:n jäsenvaltiot ovat saattaneet kansallisessa lainsäädännössään voimaan EU:n sähköisen allekirjoituksen direktiivin varsin laajasti. Käytännössä kaikissa tutkituissa maissa sähköisen allekirjoituksen lainsäädäntö on EU-direktiivin mukaisesti voimassa. Sen sijaan, sähköisten allekirjoitusten luomisvälineiden arviointitoiminta on vielä alkuvaiheessaan. Tutkituista maista vain Saksassa, Itävallassa ja Ranskassa oli nimetty varsinainen arviointilaitos tai -laitoksia arviointia suorittamaan. Muut maat käytännössä ilmoittivat käyttävänsä tarvittaessa edellä mainittujen maiden arviointilaitosten palveluita tai toteuttavansa mahdollisen arvioinnin tapauskohtaisesti valvovan viranomaisen toimesta.

Tutkittujen arviointilaitosten arviointitoiminta perustuu tuotteiden tietoturvan ja standardienmukaisuuden evaluointia varten kehitettyihin arviointimenetelmiin. Näistä arviointimenetelmistä selkeästi yleisin ja pisimmälle kehittynein on Common Criteria (CC) -käytäntö. Siinä arvioitava tuote evaluoidaan kyseiselle tuoteryhmälle määriteltyä Protection Profilea vasten. EU näyttäisi pyrkivän suosimaan CC-käytäntöä, sillä EU:n komission hyväksymä turvallisen sähköisen allekirjoituksen luomisvälineen standardi CWA 14169 määrittelee turvallisille allekirjoitusten luomisvälineille määritellyt Protection Profilet.

Missään tutkitussa arviointilaitoksessa arviointitoiminta ei rajoitu pelkästään sähköisten allekirjoitusten luomisvälineiden arviointiin, vaan kyseinen arviointilaitos suorittaa muutakin samantyyppistä tuotteiden ja ohjelmistojen arviointitoimintaa. Tutkituista maista arviointilaitosten toiminta on määritelty perusteellisimmin Saksan arviointilaitoksissa.

Eri toimialoilla toimivien tarkastuslaitosten ja tuotteiden arviointia ja sertifiointia suorittavien laitosten sisäiset toimintatavat on yleensä määritelty ja standardoitu varsin seikkaperäisesti. Yleisesti ottaen arviointilaitosten tulee täyttää tietyt määrittelyt, jotta laitoksella on oikeus toimia hyväksyttynä arviointi- ja sertifiointilaitoksena. Allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arviointia suorittavien arviointilaitosten tulisi muiden arviointilaitosten tapaan käydä läpi vastaavanlainen hyväksymis- eli akkreditointimenettely. Muodollisen akkreditoinnin myöntää kansallinen akkreditointilaitos. Lisäksi niiden tulee täyttää EU-direktiiviin ja komission arviointilaitoksia koskevaan päätökseen sisältyvät vaatimukset.

Itse arviointiprosessi on varsin suoraviivainen toimenpide. Allekirjoitusten luomisvälineelle suoritetaan aluksi tekninen evaluointi, jonka perusteella tiedetään suorittaako arvioitava tuote tietyn toiminnon standardien ja vaatimusten mukaisesti. Allekirjoitusvälineiden vaatimusten mukaisuutta arvioiva laitos voi suorittaa teknisen evaluoinnin joko itse tai tekninen evaluointi voidaan suorittaa kaupallisen evaluointilaitoksen toimesta. Jälkimmäisessä tapauksessa arviointilaitoksen vastuulle jää teknisen evaluoinnin hyväksyminen. Teknisen evaluoinnin ja sen hyväksymisen jälkeen suoritetaan oikeudellinen arviointi, jonka tarkoituksena on selvittää täyttääkö tuote sähköisiä allekirjoituksia koskevan lainsäädännön vaatimukset. Jos teknisessä evaluoinnissa on käytetty CWA 14169 -vaatimuksia, niin tällöin tuote jo EU-direktiivin mukaisesti täyttää myös lainsäädännön vaatimukset. Jos taas teknisessä evaluoinnissa on käytetty jotain muuta standardia tai vaatimusmäärittelyä, tulee oikeudellinen arviointi suorittaa tapauskohtaisesti. Koko arviointiprosessi päättyy tulosten hyväksymiseen ja julkaisemiseen.

Johtopäätökset ja toimenpide-ehdotukset

Tämän tutkimuksen perusteella voidaan nähdä, että tutkituissa maissa Saksaa lukuun ottamatta arviointitoiminta on varsin alkuvaiheessaan. Sen lisäksi, että arviointitoiminnan järjestämistavat ovat osittain epäselviä, on nähtävissä epäselvyyttä sille onko etukäteen suoritettava allekirjoitusvälineiden hyväksyttäminen ylipäätään tarpeellista. Monissa maissa arviointi ilmoitetaan suoritettavan tapauskohtaisesti joko muiden maiden arviointilaitosten, tai oman maan valvontaviranomaisen toimesta, jos arvioinnille ilmenee tarvetta.

Myös Suomessa tilanne on edellä kuvatun kaltainen. Tämän tutkimuksen tekijöiden näkemys on, että varsinaista akuuttia tarvetta Suomen omalle arviointilaitokselle ei ole. Tarvittaessa voidaan käyttää olemassa olevia muiden maiden arviointilaitoksia. Jos Suomesta löytyy jokin taho, joka on halukas ryhtymään allekirjoitusten luomisvälineiden arviointilaitokseksi, niin sinänsä mitään varsinaista estettä ryhtymiselle ei ole. Tällöin kyseisen tahon toimintamallien suunnittelussa suositellaan otettavan mallia Saksan toimintatavoista, kuitenkin siten, että varsinkin alkuvaiheessa Saksan toimintamalli saattaa olla turhan raskasrakenteinen Suomen tarpeisiin.

Muiden toimialojen arviointi- ja tarkastuslaitosten toimintamallien mukaisesti allekirjoituksen luomisvälineitä arvioivien laitosten sisäisiin toimintatapoihin suositellaan sovellettavan arviointi- ja sertifiointilaitoksille standardoituja toimintatapoja sen lisäksi, että niiden tulee täyttää sähköisistä allekirjoituksista annetusta laista johtuvat velvoitteet.

Valvovan viranomaisen rooli kuuluu suoraan sähköisistä allekirjoituksista annetun lain perusteella Viestintäviraston vastuulle.

Lainsäädännössä allekirjoituksen luomisvälineen määritelmä tulisi tarkentaa. Tällä hetkellä eri toimijoiden ja erityisesti yksityisten henkilöiden on vaikea ymmärtää mitä allekirjoituksen luomisvälineen määrittelyyn sisältyy. Onko luomisväline allekirjoituksen generoiva laite, esimerkiksi toimikortilla oleva siru, vai sen käyttöön liittyvien komponenttien, kuten kortinlukijan, tarvittavien ajurien ja ohjelmistojen muodostama kokonaisuus? Lisäksi näiden välillä on usein erilaisia teknisiä rajapintoja, liittimiä ja johdotuksia, joiden toiminnan oikeellisuudesta ei aina ole täyttä varmuutta. Varsinkin yksityisen kuluttajan intressissä on saada selkeät ohjeet siitä, mitkä laitteet tai laitekokonaisuudet ovat testattuja ja hyväksyttyjä.

Oman lisänsä tuo varsinaisia laitteita käyttävien ohjelmistojen toiminnan varmistaminen. Miten loppukäyttäjät voivat olla varmoja esimerkiksi siitä, että kortinlukijaohjelmisto käyttäytyy oikein, eikä esimerkiksi tallenna allekirjoitustoiminnon aloittavaa, käyttäjän syöttämään PIN-koodia mihinkään? Tai vastaavasti, miten voimme olla varmoja, että kortinlukijaohjelmisto ei generoi allekirjoituksia itsestään, käyttäjän tietämättä.

Palveluiden käyttäjien tulisi lisäksi voida olla täysin tietoisia siitä, milloin he generoivat sähköisen allekirjoituksen. Tämä on perusedellytys sille, että sähköisen allekirjoituksen mukanaan tuomat oikeusvaikutukset täyttyvät ja tahdonilmaisu on harkittu. Yksi tapa olisi määritellä yksiselitteisiä ohjeistuksia, käytäntöjä ja tarkastusmenettelyjä allekirjoitusvälineiden ja -ohjelmistojen käyttöliittymälle.

Edellä kuvattu epätietoisuus tulee kasvamaan myös Suomessa lähivuosien aikana. Syynä tähän on varmenteiden leviäminen eri korttialustoille, kuten pankkikorteille ja matkapuhelinoperaattoreiden SIM-korteille. Tämän sinänsä positiivisen kehityksen lisäksi, varmenteiden ja sähköisten allekirjoitusten käyttöä tulee lisäämään nähtävissä oleva voimakas sähköisten palveluiden kehittyminen lähivuosien aikana.

Allekirjoitusvälineiden arviointitoiminnan järjestämisen lisäksi viranomaisten tulisi harkita sekä kuluttajille että palvelutarjoajille suunnatun ohjeistuksen ja tiedottamisen laajentamista siten, että kaikilla osapuolilla on riittävä tietotaito palveluiden kehittämiseen ja niiden käyttämiseen myös sähköisten allekirjoitusten osalta.

2 Johdanto

Sähköisten allekirjoitusten avulla voidaan tehostaa verkon yli tapahtuvaa sähköistä asiointia. Sähköisellä allekirjoituksella voidaan yksiselitteisesti yksilöidä allekirjoittaja ja allekirjoitettu tieto. Jotta sähköinen allekirjoitus olisi käyttökelpoinen, tulee sen liittyä yksiselitteisesti allekirjoittajaan. Lisäksi toteutettava allekirjoitus tulee olla luotu välineellä, jota allekirjoittaja voi pitää omassa hallinnassaan. Näin saavutetaan tapahtuman kiistämättömyys: voidaan olla täysin varmoja siitä, että allekirjoitettu tieto on alkuperäinen ja että väitetty allekirjoittaja on todella allekirjoittanut tiedon.

Edellä kuvattujen seikkojen vuoksi sähköistä allekirjoitusta koskevaan lainsäädäntöön on määritelty turvallisia sähköisen allekirjoituksen luomisvälineitä koskevia vaatimuksia. Sähköisen allekirjoituksen luonnissa on käytettävä kyseiset vaatimukset täyttäviä luomisvälineitä, jotta allekirjoitus saisi käsintehtyä allekirjoitusta vastaavat oikeusvaikutukset.

2.1 Aihealue ja tutkimuksen rakenne

Tässä tutkimuksessa pyrittiin selvittämään, miten eri EU:n jäsenvaltioissa on kansallisissa lainsäädännöissä otettu huomioon turvallisten sähköisten allekirjoitusten luomisvälineiden vaatimukset ja miten vaatimusten täyttymistä arvioidaan.

Tiedossa oli, että joissakin jäsenvaltioissa on perustettu erillisiä arviointilaitoksia arvioimaan allekirjoitusvälineiden vaatimustenmukaisuutta. Niissä maissa, joissa arviointilaitos on olemassa, keskityttiin kyseisen laitoksen toimintatapojen selvittämiseen ja analysointiin. Vastaavasti niiden maiden osalta, joissa erillistä arviointilaitosta ei ole, pyrittiin selvittämään miten allekirjoitusvälineiden vaatimustenmukaisuus käytännössä arvioidaan.

Tutkimuksen painopiste oli tiedonkeruussa ja eri jäsenvaltioiden toimintatapojen selvittämisessä. Tämän lisäksi pyrittiin saamaan tietoja jäsenvaltioiden kokemuksista ja näkemyksistä menettelytapojen toimivuuden osalta.

2.2 Tutkimuksen työskentelymalli

Tämä tutkimus tehtiin Valimo Wireless Oy:n toimesta liikenne- ja viestintäministeriön toimeksiannosta.

Perusteellisen aihealueeseen tutustumisen jälkeen tehtiin analyysi eri Euroopan valtioiden sähköisen allekirjoituksen markkinatilanteesta ja lainsäädännön kypsyydestä. Analyysin pohjalta valittiin kymmenen valtiota, joiden menettelytapojen tutkimiseen ja analysointiin päätettiin keskittyä. Valittuihin kymmeneen valtioon lähetettiin kyselylomakkeet, joiden pohjalta pyrittiin saamaan riittävä kuva kyseisten maiden toimintatavoista ja -prosesseista. Jos tietystä maasta ei saatu vastauksia kyselylomakkeisiin, kyseisen maan tilanne pyrittiin kartoittamaan muita lähteitä hyväksi käyttäen.

Kyselyiden avulla saadut tiedot analysoitiin, ja koostettiin tähän loppuraporttiin.

3 EU:n direktiivi sähköisistä allekirjoituksista

3.1 Turvallisen allekirjoituksen luomisvälineen määrittely

Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY annettiin 13. joulukuuta 1999. Direktiivin tavoitteena oli helpottaa sähköisten allekirjoitusten käyttöä ja edistää osaltaan niiden oikeudellista tunnistamista. Lisäksi sillä vahvistettiin oikeudelliset puitteet sähköisille allekirjoituksille ja tietyille varmennepalveluille. [1]

Huomattavaa on, että direktiivi pyrkii olemaan teknologiariippumaton. Tällöin direktiiviä ja sen pohjalta luotuja kansallisia lainsäädäntöjä ei olisi tarvetta muuttaa teknologian kehittyessä.

Tämän tutkimuksen kannalta seuraavat direktiivin määritelmät ovat keskeisessä asemassa [1]:

Määritelmät (2. artikla)

Tässä direktiivissä tarkoitetaan:

1. ’sähköisellä allekirjoituksella’ sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään todentamisen välineenä;

2. ’kehittyneellä sähköisellä allekirjoituksella’ sähköistä allekirjoitusta, joka täyttää seuraavat vaatimukset:

    a. se liittyy yksiselitteisesti sen allekirjoittajaan;

    b. sillä voidaan yksilöidä allekirjoittaja;

    c. se on luotu keinoilla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan; ja

    d. se on liitetty sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita

3. ’allekirjoittajalla’ henkilöä, jolla on hallussaan allekirjoituksen luomismenetelmä ja joka toimii joko itsensä tai edustamansa luonnollisen henkilön tai oikeushenkilön taikka yhteisön puolesta,

4. ’allekirjoituksen luomiseen käytettävillä tiedoilla’ ainutlaatuista tietokokonaisuutta, esimerkiksi koodeja tai yksityisiä salausavaimia, joita allekirjoittaja käyttää luodakseen sähköisen allekirjoituksen,

5. ’allekirjoituksen luomismenetelmällä’ asetuksin varustettua ohjelmistoa tai laitteistoa allekirjoituksen luomiseen käytettävien tietojen toteuttamiseksi,

6. ’turvallisella allekirjoituksen luomismenetelmällä’ allekirjoituksen luomismenetelmää, joka täyttää liitteessä III vahvistetut vaatimukset,

…

Sähköisten allekirjoitusten oikeusvaatimukset (5. artikla)

1. Jäsenvaltioiden on varmistettava, että sellaiset kehittyneet sähköiset allekirjoitukset, jotka perustuvat hyväksyttyyn varmenteeseen ja jotka on luotu turvallisella allekirjoituksen luomismenetelmällä

    a. täyttävät sähköisessä muodossa olevan tiedon osalta allekirjoitukselle asetettavat oikeudelliset edellytykset samalla tavoin kuin käsin kirjoitettu allekirjoitus täyttää kyseiset vaatimukset paperilla olevan tiedon osalta; ja että

    b. ne kelpaavat todisteeksi oikeudellisissa menettelyissä.

…

Sähköinen allekirjoitus saa siis käsintehtyä allekirjoitusta vastaavat oikeusvaikutukset, jos se perustuu hyväksyttyyn varmenteeseen ja on lisäksi luotu turvallista allekirjoituksen luomismenetelmää käyttäen. Direktiivin liitteessä III on määritelty turvallisia allekirjoituksen luomismenetelmiä koskevat vaatimukset [1]:

Turvallisia allekirjoituksen luomismenetelmiä koskevat vaatimukset (Liite III)

1. Turvallisilla allekirjoituksen luomismenetelmillä on tarkoituksenmukaista tekniikkaa ja menettelytapoja käyttäen varmistettava ainakin, että

    a. allekirjoituksen luomiseen käytettäviä tietoja voi käytännössä käyttää vain kerran ja että niiden luottamuksellisuus voidaan kohtuudella varmistaa;

    b. allekirjoituksen luomiseen käytettäviä tietoja ei voi kohtuullisella varmuudella johtaa ja että allekirjoitus on suojattu kulloinkin käytössä olevaa tekniikkaa käyttäen suoritettavalta väärentämiseltä;

    c. laillinen allekirjoittaja voi luotettavasti suojata allekirjoituksen luomiseen käytettävät tiedot muiden käytöltä.

2. Turvalliset allekirjoituksen luomismenetelmät eivät saa muuttaa allekirjoitettavia tietoja eivätkä estää niiden esittämistä allekirjoittajalle ennen allekirjoittamismenettelyä.

Liitteen III vaatimukset ovat teknologiariippumattomia ja tästä syystä varsin yleispäteviä vaatimuksia.

3.2 Standardit

Liitteen III vaatimusten lisäksi komissiolla on direktiivin mukaan oikeus julkaista Euroopan yhteisöjen virallisessa lehdessä standardeja, jotka määrittelevät julkaistun standardin täyttävän tuotteen turvalliseksi allekirjoituksen luomismenetelmäksi. Jos jokin

menetelmä tai tuote täyttää julkaistun standardin vaatimukset, täyttää kyseinen tuote myös liitteen III vaatimukset:

Markkinoille pääsy (3. artikla)

…

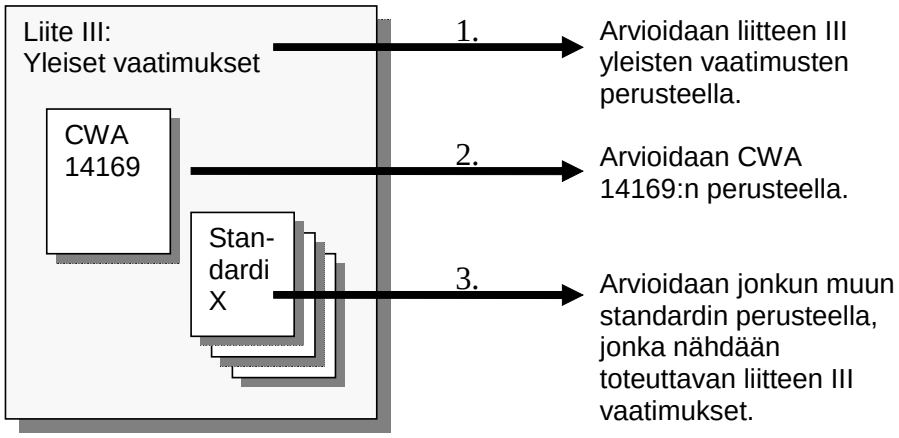
5. Komissio voi …vahvistaa ja julkaista sähköisiin allekirjoituksiin liittyviä tuotteita koskevien yleisesti tunnustettujen standardien viitenumeroita Euroopan yhteisöjen virallisessa lehdessä. Jäsenvaltioiden on oletettava sähköisiin allekirjoituksiin liittyvän tuotteen täyttävän … liitteessä III vahvistetut vaatimukset, jos tuote on kyseisten standardien mukainen.

…

Tähän liittyen komissio julkaisi 14.7.2003 standardin CWA 14169, jota noudattavan tuotteen voidaan olettaa olevan direktiivin liitteen III vaatimusten mukainen turvallinen sähköisen allekirjoituksen luomisväline.

Euroopan standardoimiskomitean (CEN = Comité Européen de Normalisation) standardi CWA 14169 (CWA = CEN Workshop Agreement) on erittäin yksityiskohtainen, noin 200-sivuinen dokumentti, joka on tehty erityisesti tarkentamaan EU:n direktiiviä ja määrittelemään selkeitä vaatimuksia turvallisille sähköisten allekirjoitusten luomismenetelmille, ja sen myötä edistämään sähköisten allekirjoitusten käyttöä ja sen leviämistä jäsenmaissa.

Jäsenvaltioilla on periaatteessa kolme vaihtoehtoista menetelmää turvallisten allekirjoitusten luomismenetelmien vaatimustenmukaisuuden arvioinnille:



Kuva 1: Vaihtoehtoiset menetelmät turvallisten allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arvioinnille

3.3 Arviointilaitokset

Direktiivi määrittelee jäsenvaltioille perusteet, jonka mukaan jäsenvaltiot voivat nimetä laitoksia, joiden tehtävänä on arvioida täyttävätkö turvalliset sähköisen allekirjoituksen luomisvälineet liitteen III tai hyväksyttyjen standardien vaatimukset:

Markkinoille pääsy (3. artikla)

…

4. Jäsenvaltioiden nimeämät asianmukaiset julkiset tai yksityiset laitokset määrittelevät, ovatko turvalliset allekirjoituksen luomismenetelmät liitteessä III vahvistettujen vaatimusten mukaisia. Komissio vahvistaa … perusteet, joiden mukaan jäsenvaltiot määrittelevät, onko laitos nimettävä.

   Kaikkien jäsenvaltioiden on tunnustettava ensimmäisessä alakohdassa tarkoitettujen laitosten suorittama, liitteessä III vahvistettujen vaatimusten täyttyminen määrittely.

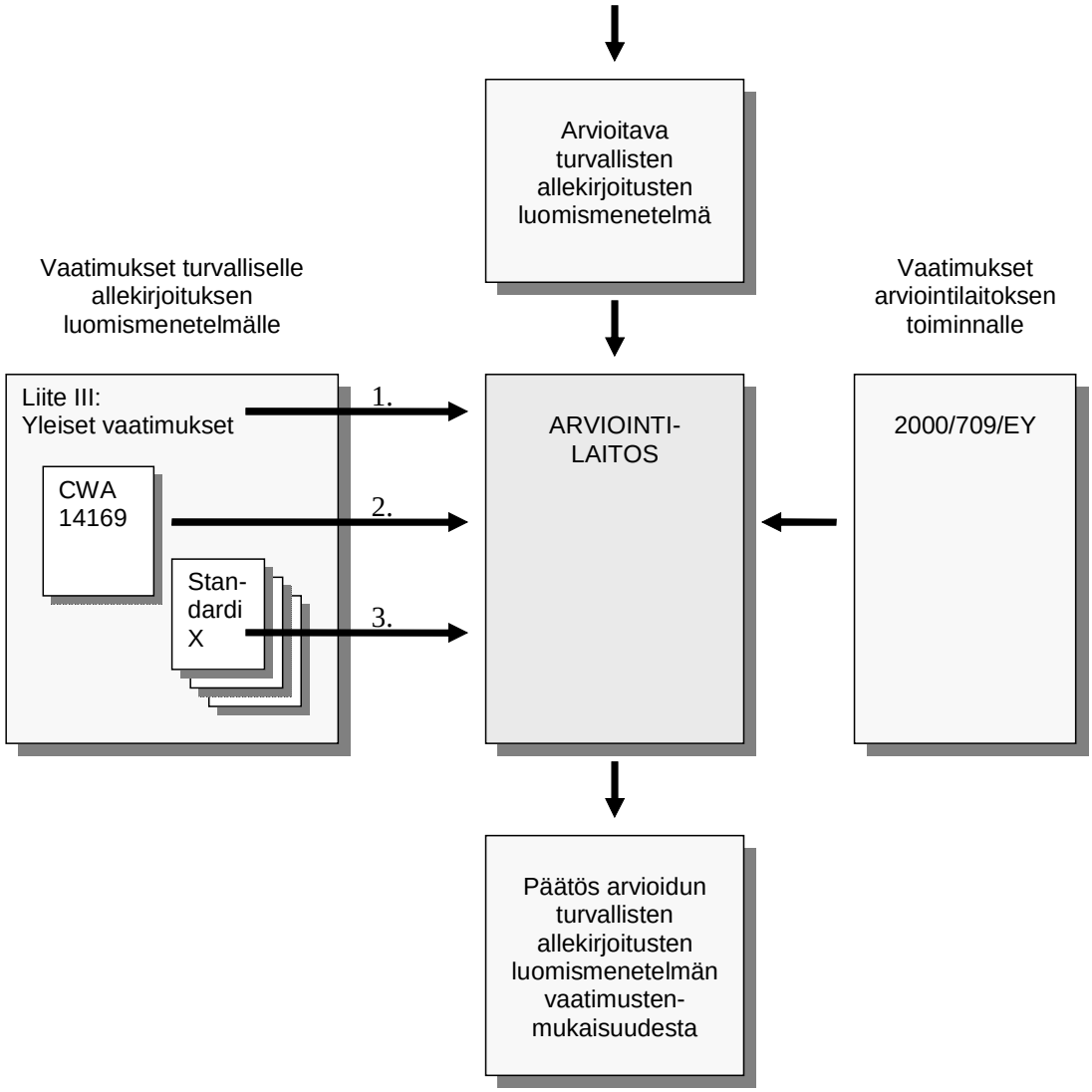
…

Komissio julkaisi 6.11.2000 päätöksen 2000/709/EY, joka vahvistaa perusteet, joita jäsenvaltiot käyttävät nimetessään turvallisten allekirjoitusten luomismenetelmien arviointia suorittavia kansallisia laitoksia. [2]

Päätöksessä määritellään joukko yleisiä vaatimuksia, joita arviointilaitosten tulee noudattaa. Vaatimuksissa määritellään muun muassa arviointilaitosten toimintatavoille seuraavia rajoituksia ja minimivaatimuksia: [2]

- Arviointitoiminnan tulee toimia erillisenä yksikkönä
- Arviointilaitoksen sekä sen henkilökunnan riippumattomuus tulee turvata
- Toiminnan tulee olla ammattitaitoista ja puolueetonta
- Laitoksen palveluiden tulee olla kaikille avointa ja syrjimätöntä
- Laitoksella tulee olla käytettävissään riittävät tilat ja resurssit
- Laitoksella tulee olla riittävä suoja vastuiden kattamiseksi
- Toiminnan tulee olla luottamuksellista
- Laitos vastaa alihankkijoidensa toiminnasta

Arviointilaitoksille on täten luotu varsin selkeät yleiset vaatimukset ja toimintaperiaatteet sekä arviointimenettelyn järjestämiseksi että itse arvioitavien turvallisten allekirjoitusten luomismenetelmien arviointiperusteiksi.



Kuva 2: Arviointilaitosten toiminta ja toimintaa ohjaavat vaatimukset

Huomattavaa on, että arviointilaitoksen perustaminen on vapaaehtoista. Jäsenvaltio voi halutessaan nimittää arviointilaitoksen, joka suorittaa turvallisten allekirjoitusten luomismenetelmien vaatimustenmukaisuuden arvioinnin, mutta halutessaan jäsenvaltiolla on oikeus huolehtia vaatimustenmukaisuuden toteutumisesta myös ilman erillistä arviointilaitosta.

4 Sähköisen allekirjoituksen levinneisyys Euroopan valtioissa

Tämän selvityksen tarkoituksena oli tutkia turvallisten allekirjoitusten luomismenetelmien vaatimustenmukaisuuden arviointia eri Euroopan maissa. Koska sähköisen allekirjoituksen käyttö ei ole käytännössä vielä kovinkaan laajalle levinnyttä, voitiin olettaa, että arviointitoimintaakaan ei suoriteta kovin useassa valtiossa. Tutkittaviksi valtioiksi valittiin ensinnäkin ne valtiot, joissa esiselvityksen tuloksena jo tiedettiin erillisen arviointilaitoksen olemassaolosta.

Lisäksi keskityttiin tutkimaan niitä valtioita, joissa sähköinen allekirjoitus on otettu käyttöön, jolloin voitiin olettaa, että kyseisissä valtioissa saatetaan suorittaa turvallisten allekirjoitusten luomismenetelmien arviointia. Sähköisen allekirjoituksen käyttöönoton laajuutta voidaan arvioida laatuvarmentajien olemassa olon ja lukumäärän perusteella.

Lähtökohdaksi otettiin seuraavat tiedot [3, 4]:

	Laatuvarmentajia (akkreditoituja laatuvarmentajia)		Arviointilaitoksia
Lähde:	ICRI [3]	FESA [4]	FESA [4]
Ajankohta:	lokakuu 2003	tammikuu 2004	tammikuu 2004
Belgia	2 (0)		
Bulgaria	1		
Espanja	0		
Alankomaat	1 (1)		
Irlanti	0		
Islanti	1		
Italia	14 (14)		
Itävalta	6 (2)	2	1
Kreikka	5 (2)		
Luxemburg	0		
Portugal	0		
Ranska	0		1
Ruotsi	0		
Saksa	23 (23)	16	1
Suomi	1		
Tanska	3	3	
UK	0 (3)		
Kypros			
Latvia	0		
Liechtenstein	0		
Liettua	0		
Malta	0		
Norja	1		
Puola	4		
Romania	1 (0)		
Slovakia	5 (0)		
Slovenia	4 (0)		
Sveitsi	0		
Tshekki	1 (1)		1
Turkki			
Unkari	2		
Viro	1 (1)		

ICRI:n (Interdisciplinary centre for Law & Information Technology) lokakuussa 2003 julkaiseman tutkimuksen mukaan noin puolessa Euroopan maista toimii laatuvarmentajia. Kuitenkin FESA:n (Forum of European Supervisory Authorities for Electronic Signatures) tammikuussa 2004 tiedossa olevien virallisten tietojen mukaan laatuvarmentajia on huomattavasti vähemmän.

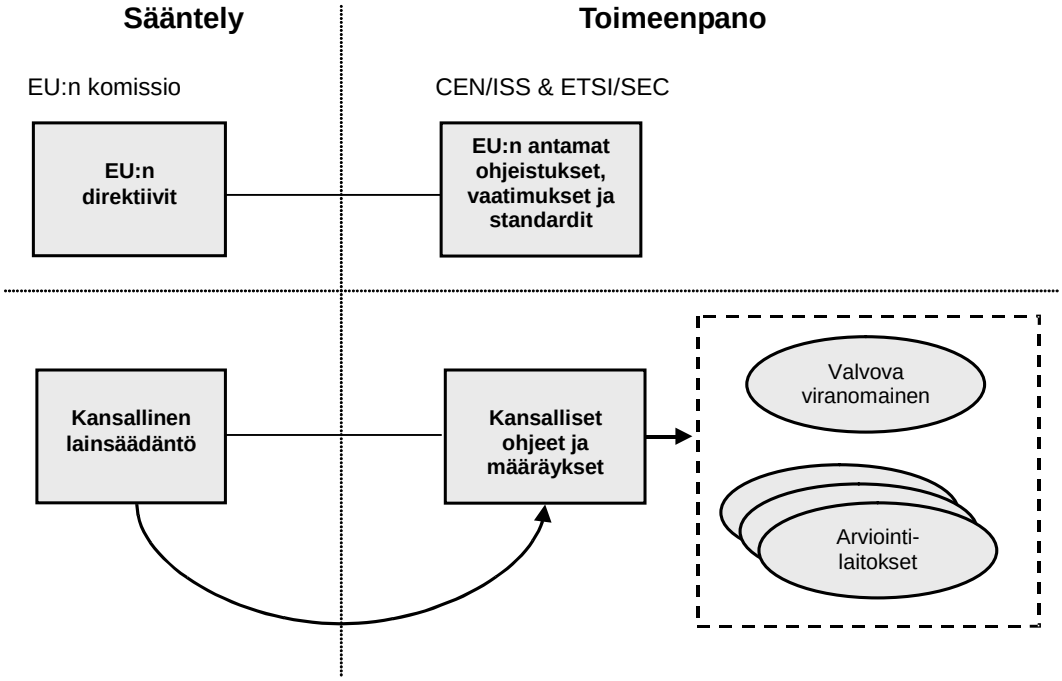
Tietojen eroavaisuudet voivat selittyä sillä, että FESA:n tiedot eivät ole aivan ajan tasalla, ja toisaalta ICRI:n tiedot voivat osin perustua laatuvarmentajiksi pyrkivien tahojen ennakkoilmoituksiin suunnitelmista ryhtyä laatuvarmentajaksi. Joka tapauksessa, näiden tietojen pohjalta pystyttiin valitsemaan seuraavat kymmenen valtioita, joihin tässä tutkimuksessa keskityttiin:

- Belgia
- Alankomaat
- Italia
- Itävalta
- Kreikka
- Norja
- Ranska
- Saksa
- Tanska
- Viro

FESA:n tietojen perusteella tiedettiin lisäksi, että EU:n jäsenvaltioista ainakin Saksassa, Itävallassa ja Ranskassa on nimetty turvallisten allekirjoitusten luomisvälineitä arvioiva laitos.

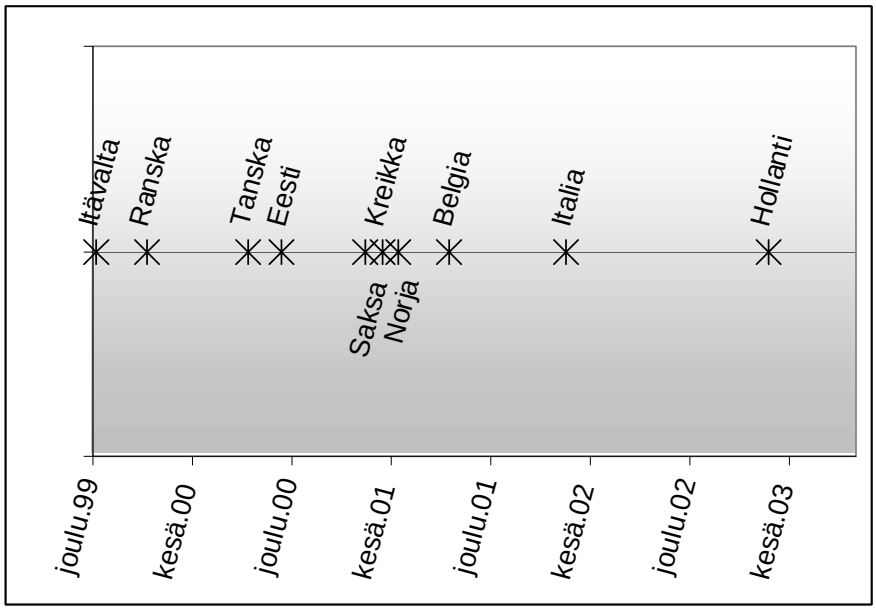
5 EU-direktiivin huomioiminen kansallisessa lainsäädännössä

Kussakin EU:n jäsenvaltiossa on valvova elin, joka valvoo kansallisen sähköisistä allekirjoituksista annetun lain säädösten noudattamista.



Kuva 3: EU-direktiivi kansallisessa lainsäädännössä

Kaikissa tutkituissa jäsenvaltioissa sähköisen allekirjoituksen EU-direktiivi on saatettu voimaan kansallisessa lainsäädännössä. Seuraavassa taulukossa on listattu kunkin tutkitun maan sähköisen allekirjoituksen lainsäädännön voimaanastumisen ajankohta:



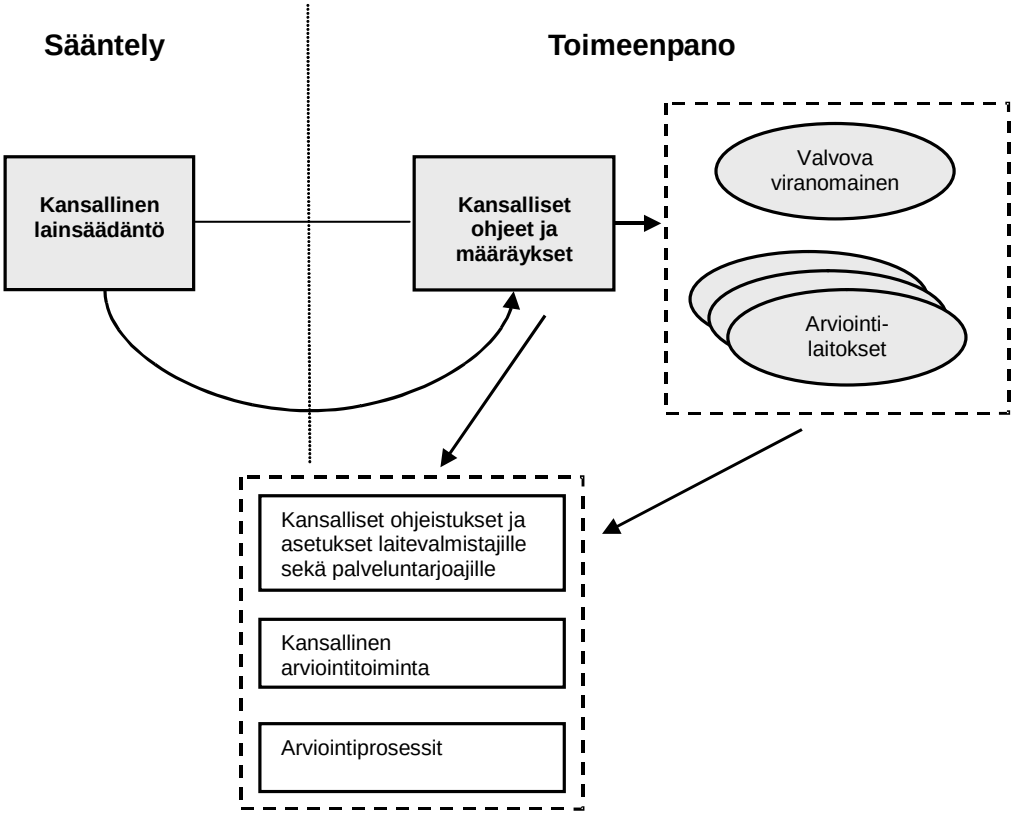
Kuva 4: Sähköistä allekirjoitusta koskevan lainsäädännön voimaanastuminen eri Euroopan maissa

6 Vaatimukset turvalliselle allekirjoituksen luomisvälineelle

Kansallinen lainsäätäjä tai valvova viranomainen voi myös määritellä omia vaatimuksia ja suosituksia turvallisille allekirjoituksen luomisvälineille ja niiden vaatimustenmukaisuuden arvioinnille.

Näin ollen arviointitoiminta perustuu kansalliseen lainsäädäntöön sekä kansallisen lainsäätäjän ja valvovan viranomaisen antamiin määräyksiin ja suosituksiin.

Kaiken edellä mainitun sekä arviointilaitosten oman toiminnan tuloksena syntyvät kansalliset ohjeistukset turvallisten allekirjoitusten luomismenetelmien laite- ja ohjelmistovalmistajille sekä palveluntarjoajille. Vastaavasti kansallinen arviointitoiminta ja siihen liittyvät prosessit määrittyvät tätä kautta.



Seuraavissa maakohtaisissa kappaleissa on kuvattu kunkin tutkitun maan antamat kansalliset vaatimukset turvallisille allekirjoitusten luomismenetelmille sekä niiden vaatimustenmukaisuuden arvioinnille. Lisäksi on pyritty kuvaamaan mitä laitteita ja ohjelmistoja ja mahdollisesti muita komponentteja turvallisen allekirjoituksen luomisvälineen käsitteeseen käytännössä sisältyy.

6.1 Itävalta

Itävalta on asettanut tiukat vaatimukset turvallisen allekirjoituksen luomisvälineelle. Vaatimuksena allekirjoituksen luomisvälineelle on muun muassa se, että allekirjoitusvä-

lineen tulee pystyä selväkielisenä näyttämään käyttäjälleen allekirjoitettava tieto. Lisäksi allekirjoitettavan tieto ei saa sisältää mitään piilotettuja tietokenttiä (”hidden data fields”). Toiminnallisuusvaatimus voidaan tiivistää termeihin ”What you see is what you sign” ja “What you see is what has been verified". Kyseiset vaatimukset ovat EU:n direktiivin mukaisia.

Muita turvallisen allekirjoituksen luomisvälineelle Itävallassa asetettuja vaatimuksia ovat:

- HASH-funktiot ja julkisen avaimen menetelmän algoritmit tulee valita Itävallan lainsäätäjän määrittämästä valikoimasta.
- Laatuvarmentajien tulee pystyä osoittamaan tekniset menetelmät piilotettujen tietokenttien suodattamiselle.
- Erilliset PIN-koodit allekirjoittamiselle ja sovelluksille. Tämä tarkoittaa siis tapausta, jossa toimikortilla on muitakin sovelluksia tai toiminnallisuuksia kuin allekirjoittaminen, esimerkiksi pankkikorttitoiminnallisuus.
- PIN-koodeja ei saa tallettaa allekirjoituslaitteen muistiin. PIN-koodi tulee aina jokaisella allekirjoituskerralla syöttää erikseen. (Vastaava vaatimus on olemassa pankkiautomaattien PIN-koodeille.)

Edellä mainittuja lisävaatimuksia lukuun ottamatta Itävallan lainsäädännön vaatimukset turvallisille allekirjoitusten luomismenetelmille ovat yhtenevät EU-direktiivin (1993/93/EY) vaatimusten kanssa. Vastaavasti, EU-direktiivin vaatimusten mukaisesti, muissa maissa turvallisiksi hyväksytyt allekirjoitusten luomisvälineet tulee hyväksyä myös Itävallassa.

Turvallisella allekirjoituksen luomisvälineellä nähdään tarkoitettavan allekirjoituslaitteen ja sen ohjelmiston muodostamaa kokonaisuutta. Perinteinen näkemys on, että turvallinen allekirjoituksen luomisväline on älykortti, kortinlukija liitettynä PC:hen ja kortinlukijan vaatimat ohjelmistot asennettuna PC:hen.

Itävallan lainsäädäntö määrittelee, että turvallisen allekirjoituksen luomisvälineiden vaatimustenmukaisuus tulee arvioida erillisen arviointilaitoksen toimesta. Arviointilaitos suorittaa jatkuvaa arviointia ja varmentaa, että luomisvälineet täyttävät lain asettamat vaatimukset.

Itävallan arviointilaitoksen julkistama ajantasainen lista hyväksytyistä turvallisista allekirjoituksen luomisvälineistä on saatavissa A-SIT:n verkkosivuilta. [5] (Ks. Liite 1)

6.2 Belgia

Belgian sähköistä allekirjoitusta koskevan lainsäädännön mukaan turvallisella allekirjoituksen luomisvälineellä tarkoitetaan allekirjoituslaitteen ja sen ohjelmiston muodostamaa kokonaisuutta.

Muissa maissa turvallisiksi allekirjoitusten luomisvälineiksi hyväksytyt välineet hyväksytään myös Belgiassa.

Belgian lainsäädäntö määrittelee, että valvovan viranomaisen tulee valvoa ja seurata allekirjoitustuotteiden vaatimustenmukaisuutta. Arvioivaa elintä ei ole nimetty, joten vaatimusta turvallisen allekirjoituksen luomisvälineiden vaatimustenmukaisuuden arvioinnille ei tällä hetkellä ole olemassa.

6.3 Tanska

Tanska määrittelee turvallisen allekirjoituksen luomisvälineet EU-direktiivin mukaisesti. Turvallisella allekirjoituksen luomisvälineellä tarkoitetaan käytännössä fyysistä laitetta, joka suorittaa allekirjoituksen. Tämä voi olla älykortti, USB-väylään asetettava turvamoduuli, ohjelmisto tai kortinlukija.

Allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arviointi on vapaaehtoista. Maan Tiedeministeriöllä on lain mukaan mahdollisuus nimittää arviointia suorittava taho, mutta tällä hetkellä mitään arviointielintä ei ole toiminnassa. ETA:an kuuluvissa maissa hyväksytty turvallinen allekirjoituksen luomisväline hyväksytään myös Tanskassa.

6.4 Viro

Turvallisella allekirjoituksen luomisvälineellä tarkoitetaan allekirjoituksen tuottavien laitteiden kombinaatiota. Siihen voi kuulua joitakin seuraavista: älykortti, ohjelmisto ja/tai kortinlukija.

6.5 Ranska

Sähköistä allekirjoitusta koskevan lainsäädännön mukaan turvallisella allekirjoituksen luomisvälineellä tarkoitetaan allekirjoituslaitteen ja sen ohjelmiston muodostamaa kokonaisuutta.

Ranska on myös julkaissut listan hyväksytyistä turvallisista allekirjoitusten luomisvälineistä, joka on saatavissa SSI:n verkkosivuilta. [6] (Ks. Liite 3)

6.6 Saksa

Saksa on säätänyt lain, jonka sisältämät ”Signaturgesetz (SigG)” ja ”Signaturverordnung (SigV)” määrittelevät yleiset toimintaperiaatteet. SigG määrittelee yleiset puitteet, kun taas SigV kuvaa yksityiskohtaiset toiminnalliset vaatimukset sähköisen allekirjoituksen infrastruktuurille sekä erityisesti laatuvarmentajien järjestelmille ja menettelytavoille.

6.6.1 Historia

Sähköistä allekirjoitusta koskevan lain tullessa voimaan vuonna 1999, julkaistiin myös ”Signatur-Interoperbilitätsspezifikation (SigI)”, joka kuvaa tekniset vaatimukset SiGG:n ja SigV:n implementoinnille. SigI määrittelee käytettävät tietomuodot, algoritmit, aikaleima- ja varmenneformaatit. Turvallisia allekirjoituksen luomismenetelmiä koskevat vaatimukset on kuvattu dokumentissa “B.2 Signaturkomponente”. [7]

6.6.1.1 ISIS-MTT

Myöhemmin, samalla kun EU-direktiivi saatettiin voimaan kansallisessa lainsäädännössä, SigI kumottiin ja osa SigI:n sääntelemistä kokonaisuuksista siirrettiin toimialavetoisen ryhmän, T7:n, yhteistoimintaa koskeviin määrittelyihin.

T7 on sittemmin yhdistynyt saksalaisen TeleTrust-nimisen organisaation kanssa, joka on julkaissut dokumentaation ISIS-MTT (Industrial Signature Interoperability Standard-MailTrusT). ISIS-MTT pyrkii toimimaan standardien rinnalla yleisenä lisäohjeistuksena käsitellen muun muassa seuraavia standardeja ja toimielimiä: S/MIME, PKIX, PKCS, X.509, ETSI and CEN ESI. [8]

6.6.1.2 Deutsches Institut für Normung (DIN)

Lainsäätäjän pyrkiessä määrittelemään vaatimuksia turvallisille allekirjoituksen luomismenetelmille, DIN julkaisi oman standardinsa älykorteilla tehtäville sähköisille allekirjoituksille. Standardi “DIN V 66291-1” julkaistiin vuonna 2000.

6.6.2 Vaatimukset nykylainsäädännössä (SigG and SigV)

6.6.2.1 SigG

Kappale 14 käsittelee turvallisia allekirjoituksen luomismenetelmiä. Laissa määritellään, että luomisvälineet tulee testata ja evaluoida hyväksytyn arviointilaitoksen toimesta. Muissa EU-maissa hyväksytyt allekirjoituksen luomisvälineet hyväksytään automaattisesti myös Saksassa.

6.6.2.2 SigV

Kappale 15 määrittelee sähköisiä allekirjoituksia käsitteleville tuotteille vaatimuksia. Mainitsemisen arvoisia seikkoja ovat muun muassa:

- Yksityisellä avaimella tehtävä toimenpide tulee suojata perustuen käyttäjän hallussa olevaan tietoon tai biometriseen ominaisuuteen.

- Allekirjoituksen luomisprosessi tulee käynnistyä vain käyttäjän tietoisesta aloitteesta.

- Turvallisen allekirjoituksen luomisvälineen valmistajan tulee julkaista seuraavat dokumentit:

    - Tuotekuvaus

    - Kuvaus siitä, miten tuote tuotteen valmistajan näkemyksen mukaan täyttää lainsäädännön vaatimukset (SigI ja SigV)

SigV:n liite 1 määrittelee vaatimustenmukaisuuden arvioinnissa noudatettavat menettelytavat.

6.7 Kreikka

Tietoja ei saatu ajoissa tämän tutkimuksen tarpeisiin.

6.8 Italia

Englanninkielistä käännöstä Italian kansallisesta sähköisen allekirjoituksen laista ei saatu tätä tukimusta tehtäessä. Seuraavat tiedot on saatu suullisesti Italian valvontaviranomaisen edustajalta:

”The Italian laws state that…

- SSCD conformity with the requirements laid down in annex III of 1999/93/EC shall be determined using the national scheme for security assessment and certification.

- SSCD conformity with annex III of 1999/93/EC can be certified by an appropriate body designed by a Member State and notified to Commission and other States as prescribed by Article 11 of 1999/93/EC.”

Italian näkemys allekirjoitusmenetelmien vaatimustenmukaisuuden arvioinnista noudattaa Belgian näkemystä: Valvovan elimen tulee valvoa ja seurata allekirjoitustuotteiden vaatimustenmukaisuutta. Arvioivaa elintä ei ole nimetty, joten varsinaista vaatimusta turvallisen allekirjoituksen luomismenetelmien vaatimustenmukaisuuden arvioinnille ei tällä hetkellä ole voimassa.

6.9 Alankomaat

Turvallisella allekirjoituksen luomisvälineellä tarkoitetaan kaikkia laitteita, joita käytetään allekirjoituksen luomiseen. Käytössä olevia turvallisia allekirjoituksen luomisvälineitä ovat toistaiseksi vain älykortit.

Turvalliseksi allekirjoituksen luomisvälineeksi hyväksytään laitteet, jotka täyttävät jonkin seuraavista kriteereistä:

- FIPS 140-2 taso 3 tai ylempi
- CEN Workshop Agreement 14167-2 ja/tai 14167-1
- EAL 4 tai korkeampi standardi kuten kuvattu ISO/IEC 15408
- muu vastaava turvallisuusstandardi

6.10 Norja

Allekirjoituksen luomisvälineen katsotaan täyttävän kansallisessa laissa tarkoitetun turvallisen allekirjoituksen luomisvälineen kriteerit, kun käytettävä laitteisto ja/tai ohjelmisto on yhdenmukainen EU:n komission julkaisemien standardien kanssa.

ETA:an kuuluvissa maissa hyväksytty turvallinen allekirjoituksen luomisväline hyväksytään myös Norjassa.

6.11 Yhteenveto

Kaikissa tietoja lähettäneissä maissa turvallinen allekirjoituksen luomisväline on määritelty suoraan EU-direktiivin mukaisesti. Muutamissa maissa määritelmää on tosin tarkennettu omilla lisämäärityksillä.

Kysyttäessä käytännön esimerkkejä hyväksytyistä turvallisen allekirjoituksen luomisvälineistä, vastaukseksi saadaan käytännössä aina yhtenevä määrittely: Turvallisella allekirjoituksen luomisvälineellä tarkoitetaan allekirjoituksen tuottavien laitteiden kombinaatiota. Siihen voi kuulua joitakin seuraavista: älykortti, ohjelmisto ja/tai kortinlukija.

Osassa maista vaatimustenmukaisuuden arviointi on määritelty pakolliseksi, mutta selkeästi enemmistö maista on jättänyt arvioinnin suorittajan avoimeksi: Turvallisten allekirjoitusten luomisvälineiden tulee olla vaatimusten mukaisia, mutta pakollista arviointia ei ainakaan vielä ole.

Sen sijaan valvovan viranomaisen velvollisuus on seurata miten allekirjoitusten luomisvälineet täyttävät lain asettamat vaatimukset. Mahdollisessa kiistatilanteessa valvova viranomainen suorittaa vaatimustenmukaisuuden arvioinnin aina tapauskohtaisesti.

Niissä maissa, joissa arviointi on pakollista, on myös nimetty arviointilaitos tähän tehtävään. Tyypillisesti arviointilaitokset julkaisevat hyväksytyistä menetelmistä merkki- ja mallikohtaisia listoja.

Lisäksi, EU-direktiivin mukaisesti, kaikki tutkitut EU-maat hyväksyvät muissa EU-maissa hyväksytyt turvalliset allekirjoituksen luomisvälineet.

Seuraavassa taulukossa on yhteenveto eri maiden vaatimustenmukaisuuden arvioinnista sekä mahdollisista arvioinnin suorittavista tahoista:

Maa	**Lainsäädännön määritelmä arvioinnista**	**Arvioiva taho**
Itävalta	Pakollinen arviointi. Ylimääräisiä vaatimuksia.	A-Sit
Belgia	Ei pakollista arviointia. Arviointilaitos voidaan nimittää.	Arviointia suorittavaa tahoa ei ole.
Tanska	Ei pakollista arviointia. Arviointilaitos voidaan nimittää.	Arviointia suorittavaa tahoa ei ole.
Viro	Ei mainintaa arvioinnista.	Arviointia suorittavaa tahoa ei ole.
Ranska	Arviointi on pakollista, jos halutaan, että tuotteella tehdyt allekirjoitukset saavat käsintehtyä allekirjoitusta vastaavat oikeusvaikutukset.	Arvioivana tahona toimii kansallisesta puolustuksesta vastaavan ministeriön alaisuudessa toimiva tietoturvasta vastaava virasto: DCSSI (Direction centrale de la sécurité des systèmes d'information)

Maa	**Lainsäädännön määritelmä arvioinnista**	**Arvioiva taho**
Saksa	Pakollinen arviointi.	Saksassa toimivat seuraavat arviointilaitokset: - TÜV-IT - T-Systems - BSI
Kreikka	Tietoa ei saatu	Tietoa ei saatu
Italia	Ei pakollista arviointia. Arviointilaitos voidaan nimittää.	Arviointia suorittavaa tahoa ei ole.
Alankomaat	Pakollisesta arvioinnista ei mainintaa. Arviointilaitos tullaan kuitenkin nimittämään.	Arviointia suorittavaa tahoa ei ole, mutta se tullaan nimittämään.
Norja	Ei pakollista arviointia. Arviointilaitos voidaan nimittää.	Arviointia suorittavaa tahoa ei ole.

7 Arviointilaitosten toiminta

Tutkituista maista vain Itävallassa, Ranskassa ja Saksassa arviointi on pakollista. Kustakin maasta löytyy oma arviointilaitos: Saksassa kolme kappaletta, muissa maissa yksi kussakin.

Tuotteiden tietoturvaa tai standardienmukaisuutta tutkivat laitokset perustavat arviointitoimintansa yleensä ITSEC-, Common Criteria- ja FIPS-104-1 arviointiperusteisiin. Seuraavissa kappaleissa on lyhyesti kuvattu nämä menetelmät.

7.1 ITSEC

ITSEC on 1990-luvun alussa kehitetty IT-tuotteiden tietoturvatason arviointikäytäntö. Se oli ensimmäinen Eurooppalaisten ja Pohjois-amerikkamaisten arviointimenettelyjen yhdistävä arviointimäärittely. Sittemmin ITSEC-menettelyn on korvannut kansallisten turvallisuus- ja standardoimisorganisaatioiden määrittelemä Common Criteria -menettelytapa. [9]

7.2 Common Criteria

Common Criteria (CC) on tietotekniikkatuotteiden tietoturvallisuustason määrittely- ja evaluointistandardi. Syynä Common Criterian kehittämiseen kansallisista standardeista on ollut tarve kehittää yhteinen menettelytapa. Aktiivisesti CC:tä kehittämässä ovat olleet Kanada, Ranska, Saksa, Alankomaat, Iso-Britannia ja Yhdysvallat. Common Criteriasta on saatu sangen laajalle levinnyt kansainvälinen standardi, sillä Common Criteria v.2.1 on hyväksytty ISO 15408 -standardiksi. [10, 11, 12]

CC:tä noudattaen tehty tuote-evaluointi antaa arvioinnin siitä ”mitä tuote tekee” (security functionality) ja ”miten varmaa se on” (security assurance).

CC-arvioinnin yhtenä olennaisimpana seikkana on Protection Profile, joka määrittelee kuvaustavan ja menettelyn, jonka avulla organisaatio tai kuluttaja voi määrittää tietoturvavaatimuksia. Nämä vaatimukset ovat yleisiä vaatimuksia, joita ei ole välttämättä vielä liitetty mihinkään tiettyyn tuotteeseen. Protection Profile on myös riippumaton siitä, millä teknologilla, ohjelmointikielellä yms. tuote on toteutettu. Tavoitteena on kuvata Protection Profile niin, että sen avulla voidaan asettaa jollekin tietylle tuoteryhmälle tai palvelulle yhteiset tietoturvavaatimukset. Näitä vaatimuksia voi sitten käyttää aina arvioitaessa tähän ryhmään kuuluvien tuotteiden tietoturvallisuuden tasoa. Protection Profiileja on kehitetty valmiiksi eri tuoteryhmiä, kuten palomuureja, tietokantajärjestelmiä yms., varten. [10, 11]

CWA 14169 määrittelee turvallisille allekirjoitusten luomisvälineille määritellyt Protection Profilet.

7.3 FIPS

FIPS-140-1 ja 2 on USA:n kansallisen standardi- ja teknologiainstituutin (National Institute of Standards and Technology, NIST) ylläpitämä standardi kryptografisten moduulien tietoturvavaatimuksille. Vaatimukset koostuvat yhdestätoista erillisestä kryptografis-

ten moduulien suunnittelun ja toteutuksen osa-alueesta. Arvioitavalle moduulille annetaan tietoturvaluokitus (1-4) riippuen siitä miten hyvin vaatimukset saavutetaan. [13, 14]

7.4 Arviointilaitokset

Arviointilaitoksille lähetettiin kyselylomakkeet, joissa kysyttiin yksityiskohtaisia tietoja laitoksen toiminnasta ja menettelytavoista. Kaikki laitokset vastasivat kyselyyn, mutta osaan kysymyksistä jouduttiin etsimään vastauksia muista lähteistä.

Seuraavissa kappaleissa on koostettu yhteenveto arviointilaitoksille lähetettyjen kyselylomakkeiden vastauksista sekä puhelimitse ja sähköpostitse saaduista lisätarkennuksista.

7.4.1 Arviointilaitokset organisaationa

7.4.1.1 Yhteystiedot ja arviointitoiminnan aloitusajankohta

Tutkimuksessa löydettiin seuraavat Itävallassa, Ranskassa ja Saksassa toimivat turvallisten allekirjoitusten luomismenetelmien vaatimustenmukaisuutta arvioivat laitokset:

Arviointilaitos	**Yhteystiedot**	**Arviointitoiminnan aloitusvuosi**
A-SIT (Itävalta)	Wien (Vereinssitz) Weyringergasse 35 1040 Wien 4.Stock Tel.: +43 1 - 503 19630 Fax: +43 1 - 503 1963 66	1999
BSI (Saksa)	Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63 53133 Bonn bsi@bsi.bund.de	Tietoa ei saatu
TÜV-IT (Saksa)	TÜV Informationstechnik GmbH - ein Unternehmen der RWTÜV-Gruppe - Zertifizierungsstelle Am Technologiepark 1 45307 Essen	1998
T-Systems (Saksa)	Zertifizierungsstelle der T-Systems T-Systems GEI GmbH, BU ITC Security Rabinstr. 8	1998

Arviointilaitos	Yhteystiedot	Arviointitoiminnan aloitusvuosi
	53111 Bonn	
DCSSI (Ranska)	SGDN/DCSSI Communication unit 51 bd de la Tour Maubourg 75700 PARIS 07 SP phone: 01 71 75 84 04 fax: 01 71 75 84 00 E-mail: communication.dcssi@sgdn.pm.gouv.fr	2002

7.4.1.2 Muu toiminta

Kaikki arviointilaitokset ilmoittivat tekevänsä myös muuta toimintaa allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arvioinnin lisäksi. Muu toiminta liittyy selkeästi samantyyppiseen tuotteiden ja ohjelmistojen arviointi- ja evaluointitoimintaan sekä erityisesti tietoturva-asioiden analysointiin ja tiedottamiseen.

Arviointilaitos	Muu toiminta
A-SIT	- Kansallisen sähköisen henkilökortin tukitoimet - Kansallinen tietoturvavirasto - Kansallisen maksuliikenteen ja sen teknologian valvonta
BSI	- Paikallisen hallituksen perustama tietotekniikan käyttäjien, laitevalmistajien ja myyjien tukiorganisaatio kattaen seuraavat alueet: o Yleinen tietoturva o Tietoturvan perusteet o Verkon kautta tapahtuvien hyökkäysten torjunta
TÜV-IT	- Muiden tietoturvatuotteiden sertifiointi - Laatuvarmentajien sertifiointi
T-Systems	- Muiden tietoturvatuotteiden sertifiointi
DCSSI	- Paikallisen hallituksen nimittämä tietoturva-asioiden toimeenpaneva organisaatio

Komission 2000/709/EY-päätöksen toisen artiklan mukaan arviointitoiminnan tulee olla eroteltu organisaation muusta toiminnasta. Itävallan arviointilaitos käyttää sisäistä laatujärjestelmää arviointitoiminnan itsenäisyyden takaamiseksi. Saksan ja Ranskan arviointilaitokset ilmoittavat noudattavansa EN45011 -standardin vaatimuksia.

7.4.1.3 Yhteistyö muiden tahojen kanssa

Kaikki arviointilaitokset ilmoittivat tekevänsä yhteistyötä kansallisen lainsäädännöstä ja sen valmistelusta vastaavan viranomaisen ja valvovan viranomaisen sekä laatuvarmentajien, allekirjoituksen luomisvälineiden valmistajien kanssa. Lisäksi yhteistyötä tehdään muiden maiden arviointilaitosten kanssa.

7.4.2 Yleiset toimintatavat

Erilliset testaus- ja arviointilaitokset suorittavat tuotteiden standardienmukaisuuden arviointia. Näiden niin kutsuttujen sertifiointilaitosten toiminnan tulee täyttää EN45011- tai ISO/IEC 17025:1999 -standardin vaatimukset, jotta kyseinen laitos voidaan hyväksyä eli akkreditoida viralliseksi sertifiointilaitokseksi. [15]

Kansalliset akkreditointilaitokset arvioivat sertifiointilaitoksen toiminnan. Muodollisen akkreditoinnin voi myöntää ainoastaan kansallinen akkreditointilaitos. Kansalliset akkreditointilaitokset ovat EU-tasoisen yhteistyöelimen, EA:n (European Co-operation for Accreditation), jäseniä. [15]

Edellä mainitut standardit määrittelevät yleiset vaatimukset tuotteiden testaus- ja arviointilaitoksille. Vanhempi EN45011-standardi on korvautumassa yksityiskohtaisemmalla ISO/IEC 17025:1999 -standardilla.

Tämän tutkimuksen puitteissa haastatellut turvallisten sähköisten allekirjoitusten luomismenetelmien vaatimustenmukaisuutta arvioivat laitokset ilmoittavat käyttävänsä edellä mainittuja standardeja oman toimintansa organisoimiseksi ja toiminnan laadun takaamiseksi.

7.4.2.1 Riippumattomuus

Komission 2000/709/EY -päätöksen 3 ja 8 artiklan perusteella arviointilaitoksen sekä sen henkilökunnan tulee olla puolueettomia ja riippumattomia muista organisaatioista. Arviointilaitokset näkivät koko arviointitoiminnan luonteen olevan sellaista, että riippumattomuus on jo luonnostaan taattu. Lisäksi Itävallan arviointilaitoksella on käytössään sisäinen laatujärjestelmä, jolla asia pyritään varmistamaan. Saksa ja Ranska sen sijaan ilmoittivat noudattavansa EN45011 -standardin vaatimuksia.

7.4.2.2 Pätevyys

Komission 2000/709/EY -päätöksen 7 artiklan mukaan arviointilaitosten tulee huolehtia arviointitoimintaa suorittavan henkilökuntansa riittävästä koulutuksesta ja ammattitaidosta.

Arviointilaitosten mukaan EN45011 –standardi ja niiden omat sisäiset menettelytavat määrittelevät riittävät pätevyysvaatimukset.

Lisäksi henkilökunnan riittävä pätevyys on pyritty varmistamaan samalla tavoin kuin missä tahansa muussakin organisaatiossa. Työprosessit ja ryhmätyöskentely takaavat, että tietotaito ja kokemuksen tuoma osaaminen pysyy ja leviää oman organisaation sisällä. Lisäksi kompetenssikartoitukset ja niiden avulla muodostetut työryhmät edistävät tietotaidon tehokasta leviämistä.

A-SIT ilmoitti tekevänsä tiivistä yhteistyötä Grazin yliopiston osaamiskeskuksen kanssa.

7.4.2.3 Varautuminen vastuisiin

Komission 2000/709/EY -päätöksen 9 artiklan mukaan arviointilaitoksen tulee järjestää riittävä suoja toiminnastaan syntyvien vastuiden kattamiseksi.

Kaupalliset laitokset ovat varautuneet tähän vakuutusyhtiöiden tarjoamien vastuuvakuutusten avulla. Valtiolliset organisaatiot eivät ole hankkineet vakuutussuojaa, koska näkevät, etteivät sellaista valtiollisen organisaation ominaisuudessa tarvitse.

7.4.2.4 Tietoturva ja luottamuksellisuus

Komission 2000/709/EY -päätöksen 10 artiklan mukaan arviointilaitoksen tulee huolehtia riittävästä tietoturvasta ja luottamuksellisen tiedon suojaamisesta.

Arviointilaitokset ilmoittivat omaavansa menetelmät dokumenttien sisältämien tietojen julkisuusasteen määrittelylle. Lisäksi kaikkien työntekijöiden ja ulkopuolisten kumppaneiden kanssa tehdään riittävät salassapitosopimukset (non-disclosure agreements, NDA).

Lisäksi laitoksissa on käytössä fyysisen tietoturvan takaamiseksi riittävät kulunvalvontajärjestelyt. Tietojärjestelmien tietoturvan osalta käytössä on riittävät pääsynhallinnan ja käyttäjien valtuutustiedon hallinnan ohjelmistot ja laitteet.

7.4.2.5 Alihankkijat

Vain TÜV-IT ilmoitti käyttävänsä alihankkijoita arviointitoiminnassaan. Alihankkijoiden pätevyys evaluoidaan käyttäen ISO/IEC17025 -standardia, joka on heidän tulkintansa mukaan riittävä näyttö alihankkijoiden pätevyydestä. Komission 2000/709/EY-päätöksen 11 artiklan mukaan arviointilaitoksen tulee pystyä osoittamaan alihankkijoidensa riittävä pätevyys sekä vastuunkantokyky.

7.4.2.6 Toiminnan tasapuolisuus ja läpinäkyvyys

Komission 2000/709/EY -päätöksen 5 artiklan mukaan arviointilaitoksen tulee käyttää selkeitä arviointikäytänteitä. Lisäksi laitosten tulee toimia syrjimättömällä tavalla.

Ranskan arviointilaitos ilmoitti, että heidän toimintaprosessinsa ovat julkisesti saatavilla heidän verkkosivuilla. Itävallan A-SIT ilmoitti, että he ovat julkinen laitos, ja toimivat siten tasapuolisesti kaikkia kohtaan.

Saksan arviointilaitosten oman näkemyksensä mukaan heidän toiminnan syrjimättömyyden takaa riippumaton hallintoneuvosto (”Independent Advisory board”), jonka toiminta on määritelty EN45011 -standardissa.

7.5 Arviointiprosessit

7.5.1 Arviointia pyytäneet tahot

Turvallisten allekirjoitusten luomisvälineiden arviointia ovat tyypillisesti pyytäneet laatuvarmenteiden tarjoajat. Arviointia on pyydetty joko osana varmennejärjestelmän tarjouspyyntöä tai arviointi on suoritettu, jotta käyttäjille pystytään suosittelemaan tiettyjä allekirjoituksen luomislaitteita tai -ohjelmistoja.

Viime aikoina allekirjoitusten luomisvälineiden laite- ja ohjelmistovalmistajat ovat omaaloitteisesti ryhtyneet pyytämään omien tuotteidensa arviointia. Tämä kehitys on selkeästi nähtävissä erityisesti Saksassa.

Arviointiprosessi alkaa, kun arviointia pyytävä taho ottaa arviointilaitokseen yhteyttä ja pyytää arviointia. Arvioinnissa arvioidaan arvioitavan tuotteen lisäksi tuotteen valmistaja ja sen toimintaprosessit.

7.5.2 Arviointiperusteet valmistajaorganisaation arvioinnissa

Allekirjoitusten luomisvälineen valmistajan arvioinnissa arviointilaitokset ilmoittivat tutkivansa pääasiassa valmistajan käytössä olevia toimintaprosesseja. Lisäksi valmistajaorganisaation luotettavuus, kokemus ja toimintavuosien lukumäärä vaikuttavat arviointiin organisaationa.

7.5.3 Arviointiperusteet ja menettelytavat allekirjoituksen luomisvälineen arvioinnissa

7.5.3.1 Saksa

Tutkituista maista Saksan menettelytapa on ehkä kaikkein pisimmälle kehittynyt.

Ensiksi arvioitava allekirjoituksen luomisväline arvioidaan ITSEC- tai CC-vaatimuksia vasten. Arvioinnin suorittaa yksi kahdestatoista ITSEC- tai CC-arviointeja suorittavasta organisaatiosta (“Prüstellen”). Jos hakija ei ole arvioittanut tai ei jostain syystä halua arvioittaa tuotetta kaupallisella ITSEC- tai CC-arviointilaitoksella, niin CC-arviointi suoritetaan SSCD-arviointilaitoksen toimesta.

CC- tai ITSEC-arvioinnin jälkeen yksi kolmesta arviointilaitoksesta (“Bestätigungsstellen”) suorittaa varsinaisen arvioinnin. Arviointi sisältää CC- tai ITSEC-arvioinnin katselmoinnin sekä varsinaisen tuotteen ja sen valmistajan evaluoinnin lainsäädännön (SigG ja SigV) vaatimuksia vasten. Evaluoinnin tulos julkaistaan arviointilaitoksen verkkosivuilla.

Tämän jälkeen Saksan valvontaviranomainen (”Reg TP”) käsittelee evaluoinnin ja antaa lopullisen päätöksen. Päätöksen tulos julkaistaan valvontaviranomaisen verkkosivuilla. Lisäksi Saksan virallinen julkaisulaitos ”Bundesanzeiger” julkaisee tuloksen omassa julkaisussaan.

Evaluointiprosessi päättyy, kun valvontaviranomainen julkaisee tuloksensa omilla verkkosivuillaan. Jotkut tuotteet tosin saattavat läpäistä arviointilaitoksen tekemän arvioinnin, mutta eivät silti lopulta saa valvontaviranomaisen hyväksyntää.

Kaikki kolme arviointilaitosta ovat oikeutettuja arviointitoimintaan. Kaikki käytetyt evaluointimenetelmät ja vaatimusmäärittelyt perustuvat Eurooppalaisiin standardeihin ja vaatimusmäärittelyihin. Käytännössä arviointilaitosten toimintatavat ja -prosessit saattavat kuitenkin hieman erota toisistaan. Valvontaviranomainen on perustanut yhteisten toimielimen, jonka puitteissa kaikki kolme arviointilaitosta voivat yhtenäistää ja koordinoida toimintatapojaan.

7.5.3.2 Itävalta

Itävallassa allekirjoituksen luomisväline tulee arvioida akkreditoidun arviointilaitoksen toimesta. Arviointi suoritetaan käyttäen ITSEC-, CC- tai FIPS-140-1 -vaatimuksia.

Itävallan lainsäädäntö sähköisestä allekirjoituksesta tuli voimaan ennen CWA 14169:n julkaisemista. Lainsäädäntö viittaa CC- tai ITSEC-vaatimuksiin erittäin yleisellä tasolla. Arviointi voidaan suorittaa CWA 14169 perusteella, mutta myös muita vaatimusmäärittelyjä voidaan käyttää.

Tämän tutkimuksen aikana ei selvinnyt hyväksyykö Itävallan arviointilaitos kaupallisen arviointiorganisaation suorittaman ITSEC-, CC-, tai FIPS-140-1-arvioinnin vai täytyykö arviointilaitoksen tehdä kyseinen arviointi itse.

7.5.3.3 Ranska

Ranskassa toimiva tietoturvaviranomainen, DCSSI, suorittaa myös sähköisten allekirjoitusten luomisvälineiden vaatimustenmukaisuuden arvioinnin. Ranskassa toimii myös kaupallisia tietoturvaa arvioivia organisaatioita. Nämä kaupalliset organisaatiot voivat suorittaa osan arviointiprosessista, kuten esimerkiksi laitteen tai menetelmän standardinmukaisuuden arvioinnin. Tällöin käytetty vaatimusmäärittely tulee olla DCSSI:n ja French Evaluation and Certification Scheme:n (ECF) hyväksymä. Vaatimusmäärittely määrittelee ne vaatimukset, jonka turvallisen allekirjoitusten luomisvälineen tulee täyttää.

7.5.3.4 Yhteenveto ja prosessikuvaus

Vaikka tutkittujen maiden menettelytavoissa on eroavaisuuksia ja osassa maista tietyillä toimijoilla on useita eri rooleja[*], on arviointikäytänteistä löydettävissä selkeästi yhtenevät menettelytavat.

---

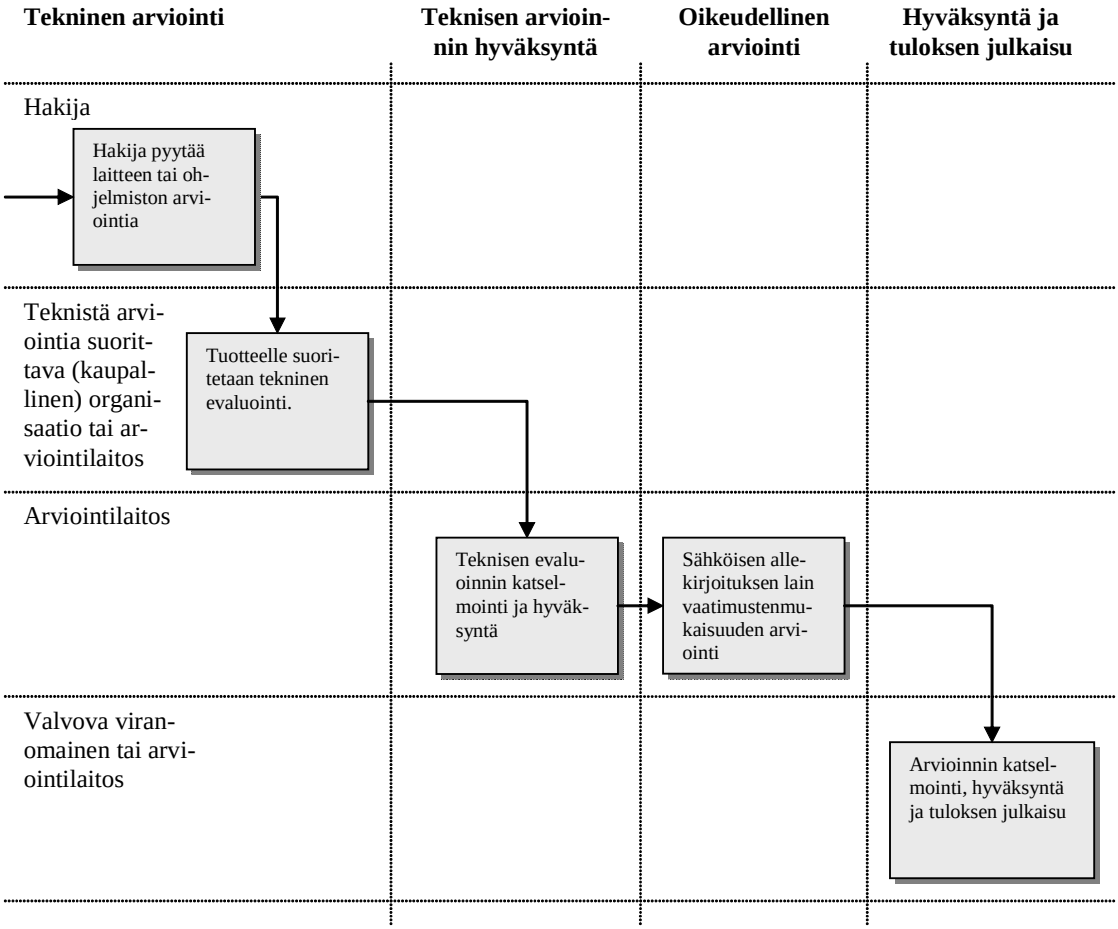
[*] Esimerkiksi Ranskassa DCSSI toimii sekä arviointilaitoksena että valvovana viranomaisena.

Arviointiprosessi voidaan jakaa seuraaviin vaiheisiin:

Vaihe ***Tyypillinen suorittaja***	**Kuvaus**
Tekninen arviointi *Arviointilaitos tai tuotteiden tietoturvaa ja standardien mukaisuutta arvioiva (kaupallinen) organisaatio*	Tuotteelle suoritetaan tekninen evaluointi. Tällöin selvitetään onko arvioitava tuote tietyn standardin tai vaatimusmäärittelyn mukainen. Pisimmälle kehittynyt ja selkeästi yleistyvä menettelytapa on Common Criteria -arviointikäytänne. Tällöin tuotteelle määritellään muun muassa Protection Profile ja Security Target, joiden vaatimuksia vasten tuote arvioidaan. Markkinoilla on löydettävissä useita teknistä arviointia suorittavia kaupallisia toimijoita.
Teknisen arvioinnin hyväksyntä *Arviointilaitos*	Tämän vaiheen pääasiallisena tehtävänä on katselmoida tekninen arviointi ja selvittää onko se suoritettu hyväksyttävästi. Teknisen arvioinnin laadusta varmistutaan tyypillisesti siten, että vain akkreditoitujen eli etukäteen hyväksyttyjen organisaatioiden tekemät arvioinnit hyväksytään. Jos arviointi hyväksytään, niin tiedetään, että arvioitava tuote täyttää tietyt tekniset vaatimukset.
Oikeudellinen arviointi *Arviointilaitos*	Tässä vaiheessa siis tiedetään, että arvioitava tuote täyttää tietyt tekniset vaatimukset. Tämän vaiheen tavoitteena on selvittää täyttääkö tuote myös sähköisen allekirjoituksen lainsäädännön mukaiset vaatimukset. Jos teknisessä arvioinnissa on käytetty CWA 14169-vaatimuksia, niin arvioitu tuote täyttää jo EU:n direktiivin mukaisesti myös sähköisen allekirjoituksen lainsäädännön vaatimukset. Jos taas teknisessä arvioinnissa on käytetty jotain muuta vaatimusmäärittelyä, niin asia joudutaan tutkimaan tapauskohtaisesti. Teknisen evaluoinnin lisäksi arvioidaan arvioitavan laitteen tai ohjelmiston valmistajaorganisaatioita ja sen menettelytapoja.

Hyväksyntä ja tuloksen julkaisu *Valvontaviranomainen tai arviointilaitos*	Tässä vaiheessa suoritetaan koko arviointiprosessin katselmointi ja julkaistaan arvioinnin tulokset. Tyypillisesti arviointilaitos toimittaa teknisen arvioinnin ja oikeudellisen arvioinnin tulokset valvontaviranomaiselle, joka julkaisee tulokset, auktorisoi tuotteen ja myöntää tuotteelle kansallisen laatusertifikaatin.

Seuraavassa on kuvattu arviointiprosessin kuvaus:



Kuva 5: Arviointiprosessin kuvaus

Ennen varsinaista sähköisen allekirjoituksen lainsäädännön vaatimustenmukaisuuden arviointia, varsinaiset arviointilaitokset hyväksyvät tuotteelle jonkin kaupallisen evaluointiorganisaation toimesta tehdyn teknisen evaluoinnin.

Tällöin arviointilaitoksen tehtävänä on ylläpitää teknisten evaluointien vaatimuksia ja ainoastaan tarkastaa, että tekninen evaluointi on tehty vaatimusten mukaisesti. Arvioin-

tilaitoksen pääasialliseksi tehtäväksi muodostuu tällöin teknisten evaluointien valvonnan ja ohjeistuksen hallinnan lisäksi muu tuotteeseen, sen valmistajaan ja valmistusprosesseihin liittyvä arviointitoiminta.

Toisaalta esimerkiksi Saksassa arviointilaitokset ovat valmiita suorittamaan myös tuotteen teknisen evaluoinnin, jolloin he kilpailevat kaupallisten toimijoiden kanssa.

7.5.4 Arvioinnin ajallinen kesto

Arviointiprosessi kestää Itävallan arviointilaitoksen mukaan kuudesta viikosta kolmeen kuukauteen. Prosessi voi pitkittyä, jos arvioitava laite tai ohjelmisto ei täytä kaikkia vaatimuksia. Tällöin arviointiprosessi on keskeytetty kunnes valmistaja toimittaa hyväksytysti vaaditut tiedot tai suorittaa vaaditut muutokset.

Saksassa arvioinnin keskimääräinen kesto on noin 12 kuukautta. Tämä pitänee sisällään myös CC-arvioinnin. Arviointiprosessi voidaan keskeyttää ja aloittaa alusta, jos käytetyissä algoritmeissa tai itse laitteessa havaitaan ongelmia.

7.5.5 Hyväksynnän voimassaolo

Itävallassa arvioinnin hyväksyntä on voimassa kaksi vuotta. Tämän jälkeen tuote tai ohjelmisto on arvioitava uudelleen. Tällöin suoritetaan täydellinen uudelleenarviointi, kuitenkin siten, että muuttumattomat osa-alueet, esimerkiksi tuotteen CC-evaluointi, voidaan hyväksyä sellaisenaan.

Saksassa arvioinnin hyväksyntä on voimassa niin ikään kaksi vuotta. Lisävaatimuksena kuitenkin on, että allekirjoituslaitteessa tai -ohjelmistossa käytössä olevat algoritmit pysyvät tuon ajan Saksan valvontaviranomaisen (Reg TP) ylläpitämällä hyväksyttyjen algoritmien listalla. Itävallan tapaan uudelleenarviointi suoritetaan muuttumattomia osa-alueita lukuun ottamatta täysin uudestaan.

Ranskassa allekirjoitusten luomisvälineet tulee arvioida toistuvasti kahdesti vuodessa. Tasaisin määräajoin tehtävillä tarkastuksilla halutaan varmistua, että laitteet ja ohjelmistot pystyvät torjumaan viimeisetkin tietoturvahyökkäykset. Niin kauan kuin väline läpäisee nämä puolivuosittain tehtävät tarkastukset, niin tuote pysyy hyväksyttyjen tuotteiden listalla.

7.5.6 Kustannukset

Itävallan arviointilaitos veloittaa arviointitoiminnastaan noin 400 euron kertamaksun lisäksi työhön käytetyt kustannukset. Saksassa kustannukset koostuvat noin 75-300 euron kertamaksusta. Lisäksi veloitetaan Itävallan tapaan työhön käytetyt kustannukset. Molemmissa maissa työhön käytettyjen kustannusten keskimääräiseksi summaksi arvioitiin 5 000 - 15 000 euroa.

Ranskassa arviointitoiminta on ilmaista arvioinnin hakijalle. Tarkempaa tietoa erillisestä pyynnöstä huolimatta ei saatu, esimerkiksi siitä onko arviointi ilmaista myös ulkomaalaiselle hakijalle.

7.5.7 Hyväksynnän käyttö markkinoinnissa

Kaikissa maissa laitteen tai ohjelmiston valmistajalla on oikeus käyttää hyväksynnän tulosta markkinoinnissaan ja mainonnassaan.

7.6 Kansainvälinen yhteistyö

Itävallan arviointilaitos ilmoitti tekevänsä yhteistyötä Sveitsin ja Saksan BSI:n kanssa. Saksan arviointilaitokset sen sijaan ilmoittivat, että virallista yhteistyötä muiden maiden vastaavien tahojen kanssa ei juurikaan tehdä, mutta arviointilaitoksen henkilökunta osallistuu alan kansainvälisiin tapahtumiin seuratakseen alan kansainvälistä kehitystä. Samalla muodostetaan epävirallisia yhteistyöverkostoja.

Kaikki arviointilaitokset ilmoittivat hyväksyvänsä EU-direktiivin vaatimuksen mukaisesti muissa EU-maissa tehdyt ja hyväksytyt arvioinnit.

7.7 Parannuskohteita

Saksassa pyritään keskittymään yksittäisten tuotteiden sijasta kokonaisten allekirjoitusten luomisympäristöjen evaluointiin.

Muilta osin kaikki arviointilaitokset ovat valmiita suosittelemaan omia arviointikäytänteitään muillekin toimijoille.

8 Toiminta ilman arviointilaitoksia

Niissä maissa, joissa erillistä arviointilaitosta ei ole, on havaittavissa, että koko arviointitoiminnan järjestäminen on vielä varsin alkuvaiheessaan. Arviointitoiminnan ja erillisen arviointilaitoksen perustamista harkitaan ja muiden maiden kokemuksia sekä toimintatapoja kartoitetaan muun muassa erilaisten yhteistyötahojen, kuten FESA:n avulla.

Varsin yleisesti maat ilmoittivat tukeutuvansa tapauskohtaisesti oman maansa valvontaviranomaisen palveluihin, mikäli allekirjoituksen luomisvälineen vaatimustenmukaisuuden arvioinnille on tarvetta.

Belgia ilmoitti käyttävänsä tarvittaessa muissa maissa olevia arviointilaitoksia, jos arviointiin ylipäätään tulee tarvetta. Tällöin viitattiin erityisesti Saksan kehittyneeseen toimintamalliin, ja siellä toimiviin arviointilaitoksiin.

9 Lähdeluettelo

Tämän raportin tiedot perustuvat suurelta osin eri maiden valvontaviranomaisille ja arviointilaitoksille lähetettyjen kyselykaavakkeiden vastauksiin. Lisäksi vastauksia on täydennetty sähköpostitse ja puhelimitse käydyin keskusteluin.

Suorien vastausten lisäksi tässä raportissa on käytetty muun muassa seuraavia lähteitä:

[1] Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY

[2] Komission päätös 2000/709/EY, 6.11.2000

[3] Interdisciplinary centre for Law & Information Technology (ICRI): The Legal and Market Aspects of Electronic Signatures, lokakuu 2003

[4] Forum of European Supervisory Authorities for Electronic Signatures (FESA): tiedot verkkosivuilta (http://www.fesa.rtr.at/countries.html), tammikuu 2004

[5] A-SIT: Verkkosivuilla oleva lista Itävallassa hyväksytyistä turvallisen allekirjoituksen luomismenetelmistä (http://www.a-sit.at/signatur/bestaetigungsstelle/bescheinigung/veroeffentlichung_18_5_/veroeffentlichung_18_5_.html), maaliskuu 2004

[6] (http://www.ssi.gouv.fr/en/confidence/certificats.html), maaliskuu 2004

[7] BSI: Interoperabilitätsspezifikationen (http://www.bsi.de/esig/basics/techbas/interop/bsi/index.htm), maaliskuu 2004

[8] ISIS-MTT: 1.02 Release (http://www.t7-isis.de/ISIS-MTT/isis-mtt.html), maaliskuu 2004

[9] BSI: Information Technology Security Evaluation Criteria (http://www.bsi.de/zertifiz/itkrit/itsec-en.pdf), kesäkuu 1991

[10] Juha-Pekka Leskinen, Helsingin yliopisto: Tietoturva nykyaikaisessa liiketoimintaympäristössä -seminaari; Common Criteria (http://www.cs.helsinki.fi/group/turvasem/papers/leskinen_commoncriteria.pdf), 10.4.2003

[11] NIST: Common Criteria for IT Security Evaluation (http://csrc.nist.gov/cc/index.html), maaliskuu 2004

[12] Decisive Analytics Corporation: The Common Criteria (http://www.commoncriteria.com/cc.html), maaliskuu 2004

[13] NIST: Cryptographic Module Validation Program (http://csrc.nist.gov/cryptval), maaliskuu 2004

[14] NIST: Security Requirements for Cryptographic Modules (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf), tammikuu 1994

[15] ISO: ISO/IEC 17025:1999 (http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30239&ICS1=3)

Lähdeviitteissä käytetty päivämäärä on dokumenttien osalta dokumentin julkaisupäivämäärä ja verkkosivujen osalta tiedon haun päivämäärä.

Liite 1: A-SIT:n arvioimat ja hyväksymät tuotteet

Lähde: http://www.a-sit.at/signatur/bestaetigungsstelle/bescheinigung/veroeffentlichung_18_5_/veroeffentlichung_18_5_.html (20.4.2004)

Folgende Bescheinigungen nach §18 (5) Signaturgesetz wurden erteilt:

2004-02-16
BDC hot:Sign, Signatur-Client zur Erstellung sicherer Signaturen, Version 1.2 SR4 rev.3 (PDF)

2003-11-03
Signatursoftware MBS Modul zur Erstellung sicherer Signaturen, Version 2.0, Rel. 1.2 (PDF)

2003-09-25
Sicherheitsmodul mit CP/Q++ (IBM), HW: P/N 04K9036, EC CF75600M, FW: Miniboot 0 Version A, Miniboot 1 Version A (PDF)

2003-08-04
BDC hot:Sign, Signatur-Client zur Erstellung sicherer Signaturen, Version 1.2 SR3 (PDF)

2003-01-24
Chipkartenleser cyberJack, HW- und FW-Version 3.0 (PDF)

2003-01-23
Signatursoftware trustview, Version 2.1.0 (PDF)

2003-01-07
Chipkartenleser mit Tastatur: cyberJack e-com, HW- und FW-Version 2.0 (PDF)

2002-12-18
Chipkartenleser mit Tastatur: cyberJack pinpad, HW- und FW-Version 2.0 (PDF)

2002-11-04
Chipkartenterminal mit Tastatur und Display: "Sign@tor Terminal Version 2.0" (PDF)

2002-09-17
IBM 4758-023 PCI Cryptographic Coprocessor mit Miniboot 0 und Miniboot 1 V2.41 und CP/Q++ V2.41 und Common Cryptographic Architecture V2.41 (PDF)

2002-06-24
"Chipkartenleser mit Tatatur und Display KOBIL KAAN Professional, HW-Version KCT199, FW-Version 2.08 GK 1.04" (PDF)

2002-06-20
"BDC hot:Sign, Signatur-Client zur Erstellung sicherer Signaturen, Version 1.0" (PDF)

2002-05-23
"Prozessorchipkarte mit Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 v 7.0 und Digital Signature Application StarCert v 2.2" (PDF)

2002-05-13
“Prozessorchipkarte mit Smart Card IC SLE 66CX320P und Betriebssystem CardOS/M4.01 (Version C803) und Applikation für digitale Signatur Version 0.20” (PDF)

2002-04-12
“MBS-Sign” - MBS Modul zur Erstellung sicherer Signaturen, V 1.0, Rel. 2.2 (PDF)

2001-10-22
“Smart Card mit Chip” - Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 und Digital Signature Application Trust Sign (PDF)

2001-06-12
“Smart Card mit Chip” - Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 (PDF)

2001-06-01:
E4 KeyCard V3.0 (PDF)

2001-05-23:
Sign@tor Terminal V1.0 (PDF)

Liite 2: RegTp:n arvioimat ja hyväksymät tuotteet

Lähde: http://www.regtp.de/tech_reg_tele/start/in_06-02-05-00-00_m/index.html#Signaturkomponenten (20.4.2004)

Signaturkomponenten	Bestätigungsurkunde	Veröffentlichung	Gütezeichen
Telesec Signaturkarte PKS-Card Version 1.0	PDF- Format	März 1999	
Telesec Signaturkarte PKS-Card Version 2.0	PDF- Format	November 1999	
Signtrust Signaturkarte SEA-Card, Version 1.0	PDF- Format	März 2000	
Telesec Signaturkarte PKS-Card, E4KeyCard, E4NetKeyCard, Version 3.0	PDF- Format	März 2001	
DATEV Signaturkarte e:secure-Card Version 1.0	PDF- Format	März 2001	
STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration)	PDF- Format	Juni 2001	
Signtrust Signaturkarte SEA-Card, Version 2.0	PDF- Format	Juli 2001	
STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration)	PDF- Format	September 2001	
Signaturkarte D-TRUST-CARD, Version 1.0	PDF- Format	März 2002	
Signaturerstellungseinheit "Chipkarte mit Prozessor SLE66CX320P, Betriebssystem CardOS/M4.01 mit Applikation für digitale	PDF-Format	August 2002	P0001

Signatur, konform mit SigG, SigV und DIN V 66291-1"			
Signaturerstellungseinheit "Prozessorchipkarte mit Prozessor P8WE5032V0G und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2"	PDF- Format	Oktober 2002	P0002
Signaturerstellungseinheit "Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur"	PDF-Format	August 2003	
Signaturerstellungseinheit "MICARDO Elliptic Version 2.3 136/32 R1.0 Signaturkarte Version 1.0"	PDF-Format	Oktober 2003	

Liite 3: DCSSI:n arvioimat ja hyväksymät tuotteet

Lähde: http://www.ssi.gouv.fr/en/confidence/certificats.html (20.4.2004)

The contact person mentioned that only one SSCD has been assessed and confirmed according to the process, but it is not singled out among the other evaluated (Non-SSCD) products.