Valtionhallinnon tietoturvallisuuden johtoryhmä

4/2001

SÄHKÖISTEN PALVELUIDEN JA ASIOINNIN TIETOTURVALLISUUDEN YLEISOHJE

SISÄLLYSLUETTELO

1 TAUSTA, TAVOITTEET, TARKOITUS JA TYÖTAVAT 4
1.1 HANKKEEN TAUSTA 4
1.2 SUOSITUKSEN LAATIMINEN 4
1.3 SUOSITUKSEN TARKOITUS, KOHDERYHMÄ JA RAJAUS 4
1.4 TERMINOLOGIA JA LYHENTEET 5
2 YHTEENVETO 7
2.1 YLEISTÄ 7
2.2 PALVELUTYYPIT 7
2.3 RISKIT JA NIIHIN VARAUTUMINEN 7
2.4 TIETOTURVALLISUUDEN TOTEUTUS 7
3 YLEISTÄ 10
3.1 TAUSTAOLETUKSET 10
3.2 SÄÄDÖSPOHJA JA OHJEET 10
3.2.1 Yleislait 10
3.2.2 Erityislait 11
3.3. SÄHKÖISTEN PALVELUPROSESSIEN LUOKKIA 12
4 SÄHKÖISEN PALVELUN TIETOTURVALLISUUDEN TOTEUTTAMINEN 14
4.1 SÄHKÖISIIN PALVELUIHIN LIITTYVÄT VAATIMUKSET 14
4.1.1 Vaatimukset tietojärjestelmille ja dokumenteille 14
4.1.2 Vaatimukset sähköisten palveluiden tarjoajalle 14
4.1.3 Vaatimukset asiakkaille ja asiakkaan oikeudet 15
4.1.4 Asiakkaan luottamuksen säilyttäminen 16
4.1.5 Yhteiskäyttö ja itsepalvelupisteet 16
4.1.6 Palveluiden saatavuus 16
4.2 SÄHKÖISTEN PALVELUIDEN TIETOTURVALLINEN TOTEUTUS 17
4.2.1 Sähköinen asiointi 18
4.2.2 Sähköpostin tietoturvallinen käyttö palvelukanavana 19
4.2.3 Sähköiset lomakkeet 19
4.2.4 Henkilön tiedonsaantioikeus 19
4.2.5 Ostaminen ja maksaminen (palvelut, luvat, tuotteet) 20
4.2.6 Tiedottaminen 20
4.2.7 Tietojen suorasiirto 20
5 RISKIENHALLINTA 21
5.1 TIETOTURVALLISUUDEN UHKAKUVIA 21
5.2 UHKAT JA VARAUTUMINEN 21
5.2.1 Potentiaalisia kohteita 21
5.2.2 Potentiaalisia uhan lähteitä 22
5.2.3 Suojautuminen hyökkäyksiltä 23
5.3 JÄRJESTELMIEN HALLINTAAN LIITTYVÄT RISKIT 24
5.4 PALVELUN TEKNINEN VALVONTA 24
5.5 PALVELUN JA JÄRJESTELMIEN TARKISTAMINEN JA SEURANTA 25
5.6 TEKNOLOGIAN KEHITYS 25
5.7 SÄHKÖISTEN PALVELUIDEN ELINKAARI JA TIETOTURVALLISUUS 25
5.7.1 Toteutusprojekti 26
5.7.2 Palvelun tuotanto 26
6 VASTUUT JA SOPIMUKSET 28
7 VARMENTEISIIN PERUSTUVIEN TOIMINTOJEN ERITYISKYSYMYKSIÄ 29
7.1 VARMENTEET JA VARMENNEPALVELUT 29
7.2 SÄHKÖINEN TUNNISTAMINEN JA TODENTAMINEN 29
7.3 SÄHKÖINEN ALLEKIRJOITUS 29
7.4 HST- JA VIRKAMIESKORTTI 30

7.5 ROOLI- ELI ATTRIBUUTTIVARMENTEET 30
7.6 VAHVAAN TODENTAMISEEN LIITTYVIEN RISKIEN TUNNISTAMINEN JA VARAUTUMINEN 30
7.7 LAATUVARMENTEET 30
8 TIETOTURVALLISUUDEN VARMISTAMINEN POIKKEUSTILANTEISSA JA POIKKEUSOLOISSA 31

LIITTEET

LIITE 1: Säädöspohja
LIITE 2: Keskeisiä tietoturvallisuustavoitteita ja niille asetettavia vaatimuksia
LIITE 3: Sähköisen palvelun turvallisuusanalyysi
LIITE 4: Sähköisestä palvelusta käyttötilanteessa ladattavan koodin tietoturvallisuus
LIITE 5: Auditoinnin tarkistuslista
LIITE 6: Tietoturvallisuus sähköisten palveluiden elinkaaren aikana
LIITE 7: Tarjoustyöskentely ja sopiminen
LIITE 8: Lähteitä

1 TAUSTA, TAVOITTEET, TARKOITUS JA TYÖTAVAT

1.1 Hankkeen tausta

Tietoturvallisuuteen liittyvät kysymykset tulevat esiin jo silloin kun sähköisiä palveluita ja niiden tarvetta lähdetään kartoittamaan ja määrittelemään. Tarve yleisohjeelle tulee esille viimeistään silloin, kun tietoturvallisuuden ongelmien ja ratkaisujen moninaisuus käy ilmi palvelun tuotantovaiheen käynnistyessä. Ohjeen laatimista ovat pitäneet tärkeänä erityisesti organisaatiot, jotka ovat kehittämässä palveluitaan.

Sähköisen asioinnin tietoturvallisuudessa on paljolti kyse normaalista tietoturvallisuustyöstä. Toisaalta sähköisissä palveluissa tietoturvallisuuden mahdolliset puutteet tulevat esiin aiempaa laajemmin, nopeammin ja vakavampina.

1.2 Suosituksen laatiminen

Valtiovarainministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä asetti työryhmän 13.11.2000 valmistelemaan valtionhallinnon sähköisen asioinnin tietoturvallisuuden yleisohjetta.

Yleisohjeen laati seuraava työryhmä:

Mikael Kiviniemi (pj.)	Neuvotteleva virkamies	Valtiovarainministeriö
Maija Kleemola	Toimistopäällikkö	Opetusministeriö
Ralf Ekebom	Projektipäällikkö	Sosiaali- ja terveysministeriö
Seppo Sundberg	Tietoturvapäällikkö	Väestörekisterikeskus
Timo Tuomaila	Tietoturvapäällikkö	Verohallitus
Markus Sadeniemi	Teknologiajohtaja	CSC
Harri Eskola	Yksikön päällikkö	Tekes
Heikki Haukirauma	Tietohallintopäällikkö	Työministeriö
Sami Paatero	Neuvotteleva virkamies	Liikenne- ja viestintäministeriö

Konsulttityöstä vastasivat seuraavat henkilöt:

Tapio Huomo	Konsultti	HM&V Research Oy
Tuomo Muhonen	Konsultti	HM&V Research Oy
Olli-Pekka Soini (siht.)	Konsultti	HM&V Research Oy

Työryhmä pyysi ja sai kommentteja yleisohjeen luonnokseen VAHTI:lta ja Sähköisen asioinnin yhteistyöfoorumilta. Työryhmä kokoontui yhdeksän kertaa, ja tutustui sähköisten palveluiden toteutuksesta saatuihin käytännön kokemuksiin.

Tämä yleisohje täydentää VAHTI:n suosituksia ja ohjeita, jotka on lueteltu liitteessä 8. VAHTI päätti tämän ohjeen julkaisusta toukokuussa 2001. Ohjeen viimeistely tehtiin valtiovarainministeriön hallinnon kehittämisosastolla.

1.3 Suosituksen tarkoitus, kohderyhmä ja rajaus

Suositus on tarkoitettu käytettäväksi yleisohjeena julkishallinnossa sekä niissä yksityisen sektorin organisaatioissa, jotka tarjoavat julkisia palveluita.

Yleisohjeen pääasiallisia käyttäjiä ovat sähköisten palveluiden suunnittelusta, toteutuksesta ja ylläpidosta vastaavat henkilöt sekä tietohallinnosta ja tietoturvallisuudesta vastaavat ja palvelua tarjoavien yksiköiden johto.

Päätavoitteena on kuvata sähköisten palveluiden tietoturvallisuuden kannalta keskeisiä kohtia. Tämä pyritään tekemään niin, ettei sähköisen asioinnin tietoturvallisuuden yleisohjeesta muodostu palveluiden kehitystä estävä vaan sitä edistävä.

Useat tämän yleisohjeen käsittelemät asiat ovat vasta hakemassa muotoaan. Lukijaa kehotetaan tutustumaan yleisiin lähteisiin erityisesti sähköisten palveluiden viitearkkitehtuurien, sähköisten allekirjoitusten, varmenneteknologian ja tunnistamisen osalta. Myös salausteknologioita ja yksittäisiä tuotteita on käsitelty vain lyhyesti.

Ohjeen ei ole tarkoitus olla kokonaisvaltainen sähköisen asioinnin ja sähköisten palveluiden kehittämisen ohje, vaikka tässä työssä kuvaillaan myös tyypillisiä palveluita ja palveluketjuja.

1.4 Terminologia ja lyhenteet

Keskeisimmät tietoturvallisuutta sivuavat käsitteet on määritelty VAHTI:n ohjeessa *Valtionhallinnon tietoturvallisuuskäsitteistö (1/2000)*. Tässä ohjeessa käytetty terminologia on pyritty pitämään tämän käsitteistön mukaisena.

Tässä ohjeessa käytetään seuraavia käsitteitä seuraavissa merkityksissä:

Sähköinen palvelu = Sähköinen asiointi sekä muut julkisyhteisön yleisölle tarjoamat sähköiset palvelut. Sähköisiä palveluita ovat mm. asiakasneuvonta, tiedotuspalvelut, sekä viranomaisen ja asiakkaan välinen kommunikointi silloin, kun palvelun käyttö tapahtuu sähköisellä tiedonsiirtomenetelmällä.

Sähköinen asiointi = Hallintoasian sähköinen vireillepano ja sen täydentäminen, käsittely (ml. ratkaisu) ja päätöksen tiedoksiantaminen tai oikeudenkäyntiasiakirjan lähettäminen sähköisenä viestinä yleiselle tuomioistuimelle tai sen määräämälle henkilölle.

Sähköisen asioinnin erityistapaus on *vaativa sähköinen asiointi*, jossa palvelun toteuttamisen tietoturvallisuusvaatimukset ovat tiukemmat kuin normaalista sähköisessä asioinnissa.

Palvelujärjestelmä = Tietojärjestelmä, johon asiakkaat ottavat yhteyden saadakseen sähköistä palvelua. Palvelupyyntö voidaan suorittaa joko palvelujärjestelmässä tai palvelujärjestelmä voi välittää pyynnön taustajärjestelmälle. *Edustajärjestelmä* on vaihtoehtoinen nimitys palvelujärjestelmälle.

Taustajärjestelmä = Tietojärjestelmä, joka osallistuu palvelun tarjoamiseen, mutta johon sähköisen palvelun asiakkaat eivät ole suoranaisessa yhteydessä. Taustajärjestelmä toteuttaa palvelujärjestelmältä tulevat palvelupyynnöt. Taustajärjestelmä voi olla palveluntarjoajan operatiivinen tietojärjestelmä, ja siitä on tässä raportissa käytetty myös nimitystä *perusjärjestelmä*.

Perinteiset palvelut = Muut palvelut kuin sähköiset palvelut. Useat sähköiset palvelut tarjoavat asiakkaille samoja palveluita kuin vastaavat perinteiset palvelut, mutta voidaan tuottaa myös uuden tyyppisiä sähköisiä palveluita.

Teknisten termien käyttöä itse ohjeessa on pyritty välttämään. Varsinaisessa ohjeessa on käytetty seuraavia termejä ja lyhenteitä:

SSL = Secure Socket Layer. Internetissä tapahtuvan tiedonsiirron salaukseen käytettävä protokolla. SSL:ää tukevat mm. useimmat käytössä olevat selaimet. Uudemmat selaimet tukevat vahvaa 128-bitin avaimella salattua tiedonsiirtoa. SSL on de facto –standardi ja sitä pidetään luotettavana ja toimivana ratkaisuna.

VPN = Virtual Private Network. Julkisen verkon kautta (esim. Internet) avattava salattu ”päästä-päähän tiedonsiirtoputki” , jolla tiedonsiirron turvallisuustaso nousee.

FTP = File Transfer Protocol. Tiedonsiirtoon käytettävä protokolla. Internetissä FTP:tä käytetään suurten tiedostojen nopeaan siirtoon. Ei sinällään tarjoa kuin rajattuja tietoturvapalveluita.

HTML = Hypertext Mark-Up Language. Internetissä käytetty sivunkuvauskieli. Internet-sivut tehdään HTML:ää käyttäen.

HST = Henkilön Sähköinen Tunnistaminen. Avoimiin kansainvälisiin standardeihin ja julkisena avaimen mekanismiin (PKI) perustuva tietoturvaratkaisu ja siihen liittyvä infrastruktuuri Suomessa.

Avain = Salausmenetelmät käyttävät tiedon salaamiseen eri pituisia salausavaimia. Avaimen pituus ilmaistaan yleensä bitteinä. Tietoturvallisuuden kannalta on keskeistä, että valitaan käyttötarkoituksen kannalta riittävän pitkä avain.

PKI = Public Key Infrastructure eli julkisen avaimen menetelmä. Tietoturvaratkaisuja tukeva järjestelmä, jossa kullakin oliolla (henkilö, yritys, ohjelma jne.) on kaksi salakirjoitusavainta: julkinen ja salainen. Julkinen avain on yleisesti saatavilla Internetistä ja sillä salattu viesti pystytään avaamaan vain salaisella avaimella, joka on vain kyseisen henkilön (olion) hallussa. PKI-ratkaisun vaatimia palveluita (avainten luonti ja hallinta, hakemistot jne) tarjoavat ns. luotettavat kolmannet osapuolet.

Palomuuri = Firewall. Yleisnimi laitteille ja ohjelmistoille, joiden tarkoituksena on erottaa kaksi verkkoa toisistaan siten, että verkkojen välistä liikennettä pystytään valvomaan. Yleisimmin palomuurilla erotetaan yrityksen sisäinen verkko Internetistä.

Eväste = Cookie. Internet-palvelun luoma tekstimuotoinen tiedosto, joka talletetaan käyttäjän koneelle. Evästeille talletetaan palvelukohtaisia tietoja ja niitä voidaan käyttää palvelun personointiin. Evästeiden käyttö voidaan estää selaimen asetuksissa.

24/7 = Myös 24*7; 24 tuntia päivässä, 7 päivää viikossa. Palvelut, jotka on suunniteltu olevan aina käytettävissä.

S/MIME = Secure Multipurpose Internet Mail Extensions. Sähköpostin liitetiedostojen salaukseen käytetty menetelmä.

PGP = Pretty Good Privacy. Tietojen, ml. sähköpostin salaamiseen käytetty ohjelma, jonka yksityishenkilöille tarkoitettu versio on vapaasti käytettävissä.

2 YHTEENVETO

2.1 Yleistä

Tietoturvallisuus ja sen hallinta ovat organisaation toimintaan ja palveluiden tarjoamiseen liittyviä perusvaatimuksia. Sähköisen asioinnin tietoturvallisuudelle asetettavat tiukkoja vaatimuksia ei tule tulkita niin, että palveluiden kehittämiseen ei ryhdytä.

Henkilöstön ammattitaidon merkitys korostuu entisestään. Perusjärjestelmien tietoturvallisuus ja toimiva tietoturvallisuustyö ovat ehdottomia edellytyksiä sähköisten palveluiden tietoturvallisuuden toteuttamiselle.

Lainmukaisuuden arvioinnissa on huomioitava palvelun tarjoajaa koskevien erityissäännösten lisäksi etenkin henkilötietolain sekä viranomaisten toiminnan julkisuudesta ja sähköisestä asioinnista annettujen lakien asettamat vaatimukset.

Asiakkaiden luottamuksen saavuttaminen ja sen säilyttäminen on ensiarvoisen tärkeää. Tämä edellyttää myös tiedotuksen järjestämistä ja informointia.

Tietoturvallisuustyö tulee ymmärtää kokonaisvaltaisesti, eikä vain yksittäisten hankkeiden ja palveluiden kautta.

2.2 Palvelutyypit

Palveluita voidaan luokitella useilla eri tavoilla. Tässä raportissa on käytetty kolmea luokittelua: vaativuuden mukaisesti, sähköisten palveluiden luonteen mukaisesti ja palvelun sisällön mukaisesti.

- Vaativuuden mukaisesti: sähköinen palvelu, sähköinen asiointi ja vaativa sähköinen asiointi.
- Palveluiden luonteen mukaisesti: anonyymit tiedotuspalvelut, tapahtumapalvelut ilman käyttäjätunnistusta, tunnistamista vaativat tiedotuspalvelut ja tunnistamista vaativat tapahtumapalvelut.
- Palvelun sisällön mukaisesti: sähköinen asiointi, sähköpostin käyttö, sähköiset lomakkeet, henkilön tiedonsaantioikeuden toteutus, ostaminen ja maksaminen, tiedottaminen sekä tietojen suorasiirto.

Palvelutyypin vaikutusta on käsitelty tarkemmin kohdassa 3.3.

2.3 Riskit ja niihin varautuminen

Sähköisiin palveluihin liittyvät riskit ovat suuremmat kuin perinteisiin palveluihin: vahingot tapahtuvat nopeammin ja voivat olla aiempaa vakavampia. Varautuminen riskeihin on suhteutettava palvelun tyyppiin.

Sähköisten palveluiden riskianalyysi tehdään samoin menetelmin kuin perinteisissä palveluissa. Analyysin merkitys on kuitenkin tietyissä palveluissa suurempi. Usein riskin lähteitä ja kohteita on enemmän.

Ennen kuin sähköisiä palveluita toteuttamista tulee selvittää riittävätkö organisaation voimavarat ja osaaminen sähköisen palvelun tietoturvalliseen tarjoamiseen.

2.4 Tietoturvallisuuden toteutus

Eri tekniset ratkaisut eroavat toisistaan tietoturvallisuusnäkökulmasta, eikä näitä eroja voi monesti poistaa tietoturvallisuutta optimoivalla konfiguroinnilla. Sähköisen asioinnin tietoteknisten kompo-

nenttien tietoturvallisuusominaisuuksiin on kiinnitettävä huomiota erityisesti vaativassa sähköisessä asioinnissa.

Ohjelmistokomponenttien päivittäminen ja tietoturvallisuusasioiden tiivis seuranta ovat ehdottomia edellytyksiä, jotta tekninen tietoturvallisuus olisi ajan tasalla.

Reaaliaikainen valvonta ja hyvin suunnitellut hälytykset ja niistä aiheutuvat toimenpiteet auttavat tietoturvallisuusrikkeiden havaitsemisessa ja nopeuttavat reagointia.

Ulkoistamisen ja hankittavien palveluiden tietoturvallisuus korostuu sähköisen asioinnin tietoturvallisuudessa. Tähän tulee varautua tekemällä selkeitä kirjallisia sopimuksia, joissa tietoturvallisuusvaatimukset ovat selkeästi esillä ja osapuolten vastuunjako on mahdollisimman yksiselitteinen. Sopimusten toteutusta on kyettävä valvomaan tietoturvallisuusauditoinneilla ja muilla soveltuvilla menetelmillä.

Uhkia torjutaan lukuisilla keinoilla, kuten tunnistusmenettely, tietoliikenteen ja tiedostojen salaus, palomuurit, järjestelmien erottaminen palvelu- ja taustajärjestelmiin sekä valvonta- ja hälytysohjelmat. Käyttöoikeuksien hallinta ja auditoinnit ovat myös tärkeitä keinoja riskien pienentämiseen.

Tietotekniikasta ja etenkin tietoturvallisuudesta vastaavien henkilöiden ammattitaidon ylläpitämisen ja kehittämisen merkitys korostuu entisestään. Koulutusta on suunnattava myös muille henkilöstöryhmille, jotta organisaatiossa voidaan kehittää ja ylläpitää sähköisen asioinnin tietoturvallisen totuttamisen edellyttämä hyvä tietoturvallisuuskulttuuri.

Asiakkaan tunnistus tulee tehdä vain tarvittaessa. Kun asiakas tunnistetaan, on se tehtävä luotettavasti ja sellaisilla ratkaisuilla, joiden toimivuus on hyvä. Vahvaa tunnistamista suositellaan.

Sähköisten palvelujen tietoturvallisuus on tekniikan ja toiminnan muodostama kokonaisuus. Tässä raportissa suositellaan käytettäväksi toisiaan täydentäviä lähestymistapoja:

- Sähköisissä palveluissa on pyrittävä niin hyvään tietoturvallisuuteen tasoon kuin on mahdollista, vaikka täydellistä tietoturvallisuutta ei voida saavuttaa.
- Elinkaarimallissa selvitetään tietoturvallisuuden painopisteet elinkaaren eri vaiheissa. Tietoturvallisuuden on oltava mukana jo palvelun esitutkimusvaiheessa. Elinkaaren alun laiminlyöntejä ei ole helppo korjata jälkikäteen.
- On pidettävä huoli siitä, että tietoturvallisuuteen varataan riittävästi resursseja.

Tietoturvallisuustavoitteet ja sähköisten palveluiden luonne kytkeytyvät toisiinsa seuraavasti:

Tietoturvallisuuden tavoitteet	**Palvelun luonne**			
	Anonyymit tiedotuspalvelut	**Tapahtumapalvelut ilman käyttäjätunnistusta**	**Tunnistamista vaativat tiedotuspalvelut**	**Tunnistamista vaativat tapahtumapalvelut**
Asiakkaan tunnistus ja todennus	-	-	Tarvitaan. Tunnistuksen taso riippuu palvelusta	Tarvitaan. Tunnistuksen taso riippuu palvelusta
Asiakkaan oikeuksien myöntäminen tunnistuksen perusteella	-	-	Välttämätön	Välttämätön
Palvelun tarjoajan henkilöstön tunnistus ja oikeuksien myöntäminen	Tärkeä	Tärkeä	Välttämätön	Välttämätön
Kiistämättömyys ja vastaanottokuittaus	-	Vastaanottokuittaus tarvittaessa	Ei yleensä tarpeen	Välttämätön
Tietojen eheys	Tärkeä	Tärkeä	Tärkeä	Välttämätön
Palvelujärjestelmän käytettävyys	Tärkeä luvattuina palveluaikoina	Tärkeä luvattuina palveluaikoina	Tärkeä luvattuina palveluaikoina	Tärkeä luvattuina palveluaikoina
Palvelutapahtuman seurantaketju (audit trail)	-	Palvelukohtainen	Tärkeä	Välttämätön
Palvelun ja järjestelmien seuranta- ja valvonta	Tärkeä	Tärkeä	Tärkeä	Erittäin tärkeä

Tunnistamisen osalta on yleensä oleellista, onko kyseessä ennakolta tiedettyjen sopimuskäyttäjien palvelu vaiko yleisempi, laajan käyttäjäkunnan palvelu. Molempiin tapauksiin soveltuu varmennepohjainen vahva tunnistus. Osassa sopimuskäyttäjän palveluista sopivana tunnistamistapana on myös perinteinen käyttäjätunnus/salasana-tunnistus, jonka turvallisempia muotoja ovat vaihtuvat ja kertakäyttöiset salasanat.

Tavoitteiden tiukkuuteen vaikuttavat lisäksi mm. seuraavat asiat

- Palvelujärjestelmän ja taustajärjestelmien väliset linkit ja niiden toteutus
- Palveluun liittyvät erityispiirteet
- Hallinnonalan säädökset, määräykset ja ohjeet
- Asiakkaiden odotukset
- Riskianalyysin tulokset

3 YLEISTÄ

Sähköisten palveluiden myötä siirrytään olennaisesti avoimempaan tietojenkäsittely-ympäristöön, jossa joudutaan varautumaan pysyvään muutokseen ja kehittämiseen myös tietoturvallisuuden osalta.

Tietoturvallisen palvelun tarjoaminen avoimissa verkoissa edellyttää sekä hallinnollisia että teknisiä toimenpiteitä.

Sähköisten palveluiden asiakkaat vaihtelevat suuresti palvelusta toiseen, mikä on huomioitava etenkin käytettävyyteen liittyvissä ratkaisuissa.

Tässä ohjeessa palveluiden, prosessien ja niihin liittyvien asiointitapahtumien oletetaan olevan kokonaan sähköisiä. Palvelu saattaa koostua osin perinteisestä manuaaliprosessista ja osin sähköisestä prosessista, mutta tämän yhdistelmän erityiskysymyksiä ei käsitellä.

3.1 Taustaoletukset

Tämän ohjeen tarkasteluissa käytetään seuraavia sähköisiin palveluihin liittyviä oletuksia:

1. Palvelun ja asiakkaan välinen tiedonvälitys tapahtuu pääosin julkisissa verkoissa, joissa tietoturvallisuuden taso on heikko ilman erityisiä toimenpiteitä.
2. Sähköisen palvelun tarjoajan taustajärjestelmät, lähiverkkoratkaisut ja muut tietotekniset ratkaisut oletetaan tietoturvallisiksi, toimiviksi ja lain mukaisiksi.
3. Tietoturvallisuus- ja muut ratkaisut suunnitellaan ja implementoidaan lakien ja asetusten mukaisesti, ammattitaidolla, huolella ja osana normaalia jatkuvaa toimintaa.

Erityisesti kun toteutetaan vaativia sähköisiä palveluita, on palvelun tarjoajalla syytä olla selkeä palvelustrategia. Tämä pienentää riskiä, että sähköiset palvelut olisivat erillisiä, kokonaisuuden kannalta toisarvoisia hankkeita, joiden tietoturvallisuuteen ei panosteta.

Käytännön toteutustyössä tietoturvallisuusratkaisut on pyrittävä toteuttamaan mahdollisimman vähin vaatimuksin palveluiden asiakkaille. Täydellistä tietoturvallisuutta ei pystytä saavuttamaan, vaikka oikeilla ennakoivilla toimenpiteillä on mahdollista toteuttaa erittäin hyvä tietoturvallisuustaso.

3.2 Säädöspohja ja ohjeet

Kansalaisten luottamuksen säilyttäminen verkkoasiointia kohtaan vaatii julkisen sektorin tarjoamilta palveluilta erinomaista tietoturvallisuutta. Tähän velvoittavat myös lait ja asetukset; julkisten palveluiden tietoturvallisuusvaatimuksia on johdettavissa jo valtiosäännöstä.

3.2.1 Yleislait

Yleislakeina kaikkia viranomaisia koskevat:

1. Laki viranomaisten toiminnan julkisuudesta (621/1999, 636/2000), erityisesti lain hyvää tiedonhallintatapaa koskeva 18§ sekä asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta. Julkisuuslain 18§ velvoittaa viranomaiset mm. selvittämään ja suunnittelemaan tietojärjestelmien käyttöönottoon liittyvät vaikutukset asiakirjojen julkisuuteen ja salassapitoon, saatavuuteen, käytettävyyteen, tiedon laatuun ja suojaamiseen sekä tietoturvallisuuteen liittyvät seikat.
2. Arkistolaki (831/1994) edellyttää viranomaisen suunnittelevan mm. asiakirjojen (ml. sähköiset asiakirjat), säilyttämisajat ja -tavat sekä niiden hävittäminen. Laadittavan arkiston-

muodostamissuunnitelman ja toiminnan tarkoituksena on varmistaa asiakirjojen säilyvyys ja käytettävyys.

3. Henkilötietolaki (523/1999) edellyttää henkilötietojen käsittelyn suunnittelua. Tämä tarkoittaa mm. henkilötietojen käsittelyn tarkoituksen sekä säännönmukaisten tietolähteiden ja tietojen luovutusten kohteiden määrittelyä. Sähköinen asioinnin avulla tapahtuva hakemusmenettely tai muu tiedon hankkiminen voi olla lain tarkoittamaa henkilötietojen keräämistä. Henkilötietoja kerättäessä tulee huolehtia lain 24§:ssä tarkoitetusta informointivelvoitteesta.

   Suostumukseen perustuvan tietojen keräämisen osalta henkilön tulee tietää, mihin hän suostuu.

   Päätös tiedon myöntämisestä ja siitä ilmoittaminen voivat olla osa ko. tarkoituksessa tapahtuvaa henkilötietojen käsittelyä ja henkilörekisterinpitoa.

   Suunniteltaessa sähköinen asioinnin toteuttamista osana rekisterinpitoa, tulee asioinnin toteuttamiseen liittyvät henkilötietojen käsittelyt ja niiden toteuttamistapa suunnitella ja asioinnin lainmukaisuus arvioida osana ko. loogisen henkilörekisterin käsittelyä. Kaikissa käsittelyvaiheissa tulee ottaa huomioon lain yleisvelvoitteet, huolellisuusvelvoite ja suojaamisvelvoite. Laki edellyttää luotettavien tietolähteiden käyttöä sekä tietojen tarpeellisuuden ja virheettömyyden arviointia suhteessa käyttötarkoitukseen.

   Henkilötietolaki korostaa sähköisen asioinnin riskien arviointia nimenomaan asiakkaan näkökulmasta.

Sekä julkisuuslain että henkilötietolain mukaan tilaaja vastaa tietojenkäsittelypalvelujen ulkoistamisen yhteydessä tapahtuvasta henkilötietojen käsittelyn lainmukaisuudesta, jos palvelut on hankittu toimeksiantopalveluna eli viranomaisen lukuun. Palvelun tuottajan vastuu toteutuu sopimusvastuuna. Henkilötietolain suojaamis- ja huolellisuusvelvoite ja useat salassapitosäännökset sitovat suoraan myös toisen lukuun toimivia. Sopimuksia tehtäessä on muun ohessa varmistettava, ettei sopimuksen oikeudellinen luonne jää epäselväksi.

3.2.2 Erityislait

Sähköisen asioinnin tietoturvallisuusvaatimuksia sisältyy erityisesti seuraaviin erityislakeihin:

1. Laki sähköisestä asioinnista hallinnossa (1318/1999)
2. Väestötietolakiin sisältyvät säännökset varmennepalveluista (527/1997)
3. Henkilökorttilaki (sähköinen henkilökortti; 829/1999)
4. Valmisteilla on laki sähköisestä allekirjoituksista, joka implementoi direktiiviin 1999/93/EY

Laki sähköisestä asioinnista säätelee sähköisen asioinnin kysymysten lisäksi varmennepalveluita, joihin liittyviä kohtia ollaan siirtämässä omaan lakiinsa. Tietoturvallisuuteen liittyviä kysymyksiä ei käsitellä yksityiskohtaisesti, vaan lain 18§ säädetään ”… Viranomaisten on pyrittävä käyttämään hallinnon asiakkaan kannalta teknisesti mahdollisimman yhteensopivia ja helppokäyttöisiä laitteistoja ja ohjelmistoja. Viranomaisen on lisäksi varmistettava riittävä tietoturvallisuus sekä hallinnossa asioitaessa että viranomaisten keskinäisessä tiedonvaihdossa.”

Käytettävyyteen liittyviä määräyksiä annetaan mm. lain 19§, jonka mukaan sähköisten palveluiden on oltava käytettävissä mahdollisuuksien mukaan muulloinkin kuin virastoaikana. Käyttökatkokset on pyrittävä pitämään lyhyinä ja niistä on tiedotettava etukäteen.

Sähköisen asiakirjan vastaanottamisesta on annettava vastaanottokuittaus, jotta asiakas tietää viestin tulleen perille. Kyseessä on tekninen kuittausilmoitus, eikä siitä oteta kantaa asian vireillepanoon tai käsittelyn edellytyksiin. Tämä on syytä ilmoittaa kuittausviestissä.

Sähköisen asiakirjan eheys ja alkuperäisyys on lain 25§ mukaan tarkistettava ja tästä on tehtävä merkintä. Tämä on tarpeen myös siksi, että asiakirjan eheys ei välttämättä säily sen käsittelyn myöhemmissä vaiheissa, sillä viranomaisella on lain 26§ mukaan oikeus muokata viestiä sen saattamiseksi lukukelpoiseksi.

Päätöksenannon tietoturvallisuudesta säädetään lain viidennessä luvussa. Sähköisen päätöksen noutaminen viranomaisen palvelimelta edellyttää päätöksen noutajan tunnistamisesta (29§). Mikäli päätöstä ei noudeta, on päätös saatettava tietoon muilla menettelytavoilla.

Varmennetoiminnasta ja varmenteiden tietoturvallisuudesta säädetään väestötietolaissa (viides luku), laissa sähköisestä asioinnista (toinen luku) ja valmisteilla olevassa laissa sähköisestä allekirjoituksesta. Näissä on asetettu luotettavalta varmenteelta vaadittavat ominaisuudet, varmennetoiminnan yleisistä asioista ja menettelytavoista sekä varmenteiden käytöstä.

Laki sähköisistä allekirjoituksista on tätä ohjetta laadittaessa lausuntokierroksella. Se tulee implementoimaan EU:n sähköisiä allekirjoituksia säätelevän direktiivin 1999/93/EY. Lain tarkoituksena on edistää varmenteisiin liittyvän liiketoiminnan kehitystä säätelemällä mm. sähköisen allekirjoituksen asemaa ja varmennepalveluiden erityiskysymyksiä. Viimeksi mainituista keskeisimpiä ovat laatuvarmenteiden kriteerit sekä Telehallintokeskukselle annettava vastuu lain toteutuksen seurannasta ja ohjeiden antamisesta.

Eri hallinnonaloja ja toimintoja koskevassa lainsäädännössä on sähköisen asioinnin ja tietoturvallisuuden toteutukseen liittyviä erityisvaatimuksia. Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvallisuudesta sääntelee mm. sähköpostiviestin käsittelyyn liittyvistä kysymyksistä.

Luettelo keskeisimmistä erityislakien säännöksistä on esitetty liitteessä 1.

3.3. Sähköisten palveluprosessien luokkia

Sähköisiä palveluprosesseja voidaan jaotella useilla eri tavoilla. Tässä esitetään neljä tapaa, ja tarkoituksena on auttaa hahmottelemaan eri tyyppisten palveluiden tietoturvallisuusvaatimuksia.

- Koneellinen tai ihmistä vaativa palveluprosessi. Koneellisessa prosessissa on tärkeää pystyä riittävällä varmuudella tunnistamaan asiakas sekä järjestää turvalliset yhteydet taustajärjestelmiin. Asiakaan tunnistuksen taso sekä tietoliikenteen salaustaso määräytyy palvelun sisällön mukaan.
- Palvelun osapuolten määrä. Helpoimmissa prosesseissa on vain yksi tietojärjestelmä. Laajennettuun palveluprosessiin saatetaan liittää organisaation omat tietojärjestelmät. Palveluun voidaan lisäksi liittää kolmannen osapuolen tietojärjestelmiä.
- Palveluprosessin yksi- tai kaksisuuntaisuus. Yksisuuntaisessa palvelussa on tärkeää asiakkaan luottamus palvelun aitouteen. Kaksisuuntainen palveluprosessi voi olla interaktiivinen tai vaste voi tulla pitkällä viiveellä, esim. päätös.
- Palvelun vaatiman tunnistuksen perusteella: anonyymit ja tunnistusta vaativat palvelut. Anonyymissa palvelussa asiakasta ei tunnisteta. Tunnistamisen osalta on yleensä oleellista, onko kyseessä ennakolta tiedettyjen sopimuskäyttäjien palvelu vaiko yleisempi, laajan käyttäjäkunnan palvelu. Molempiin tapauksiin soveltuu varmennepohjainen vahva tunnistus. Osassa sopimuskäyttäjän palveluista sopivana tunnistamistapana on myös perinteinen käyttäjätun-

nus/salasana-tunnistus, jonka turvallisempia muotoja ovat vaihtuvat ja kertakäyttöiset salasanat. Kunkin tunnistustavan sisällä tunnistuksen taso voi vaihdella palvelun luonteesta riippuen. Joissakin voidaan käyttää tunnistetta, joka ei välttämättä kerro asiakkaan henkilöllisyyttä. Vaativassa sähköisessä asioinnissa taas vaaditaan henkilöllisyyden osoittaminen luotettavasti, esim. laatuvarmenteella.

Eri jaotteluita voidaan yhdistää tarpeen mukaan. Tällöin saadaan palveluntarjoajan kannalta relevanteimmat piirteet yhdistettyä. Eräs mahdollinen ristiintaulukointi on esitetty ohessa.

	Tieto- ja tiedotuspalvelut	**Tapahtumapalvelut**
Anonyymit palvelut	Tiedotuspalvelut ilman asiakkaan tunnistusta, kuten yleiset verkkosivut. Oikeellisuuden ja käytettävyyden merkitys korostuu.	Tapahtumapalvelut ilman asiakkaan tunnistamista, kuten kyselyt verkkosivujen tai sähköpostin välityksellä. Asiankäsittelyprosessin tietoturvallisuus ja käytettävyys korostuvat.
Tunnistusta vaativat palvelut	Tiedotuspalvelut, joissa on asiakkaan tunnistaminen esim. personoitu tiedottaminen etuuksista. Tunnistaminen ja asiakkaiden luottamus korostuvat.	Tapahtumapalvelut, joissa asiakkaan tunnistus esim. vireillepano. Tunnistaminen ja asiankäsittelyprosessin kokonaisturvallisuus korostuvat.

4 SÄHKÖISEN PALVELUN TIETOTURVALLISUUDEN TOTEUTTAMINEN

4.1 Sähköisiin palveluihin liittyvät vaatimukset

Sähköisen palvelun tietoturvallinen toteutus asettaa vaatimuksia palvelun tuotanto- ja tukijärjestelmille, palvelun tarjoajalle sekä asiakkaille. Vaatimusten taso vaihtelee palvelun mukaan.

4.1.1 Vaatimukset tietojärjestelmille ja dokumenteille

- Vaatimus kiistämättömyydestä voidaan asettaa asioinnin molemmille osapuolille, ja sen on oltava ulkopuolisten todennettavissa. Kiistämättömyys on tärkeä etenkin niissä palveluissa, joissa perinteisissä palveluissa on vaadittu allekirjoituksia. Kiistämättömyys edellyttää sähköisiä allekirjoitusta ja mahdollisesti ulkopuolisia aikaleimapalveluja.
- Asiointitapahtuman elinkaari saattaa viraston kannalta olla sähköisen varmenteen voimassaoloa huomattavasti pidempi, ja asiointitapahtuman kiistämättömyys on voitava osoittaa vähintään niin kauan kuin asialla voi olla oikeudellista merkitystä asioinnin osapuolten tai muiden asianosaisten kannalta. Kiistämättömyyden toteaminen edellyttää sähköisten allekirjoitusten käsittelyjärjestelmää sekä järjestelmän, jossa asiakirja eheyden ja alkuperäisyyden tarkistamisesta tehty merkintä talletetaan.
- Sähköisen asiakirja on oltava saatettavissa kirjalliseen muotoon, ja tämä vaatimuksen voidaan olettaa säilyvän jatkossakin. Asiakirjojen tuottamiseen käytetyn ohjelman tai sen version elinikä saattaa olla lyhyempi kuin asiakirjan. On suositeltavaa tallettaa sähköiset asiakirjat arkistointikelpoiselle, muutoksilta suojatulle medialle siinä muodossa, jossa asiakas on ne lähettänyt ja tarvittaessa sellaisessa formaatissa, jota kyetään käsittelemään pitkän kuluttua, sekä tieto ohjelmasta, jolla asiakirja on laadittu.
- Asiakirjan sisällön saattaminen toiseen muotoon hävittää sellaisia muotoiluja, joilla voi olla merkitystä asian sisällön kannalta.
- Sähköisten asiakirjojen säilytyksen, arkistoinnin ja hävittämisen käytännöt ovat osittain vasta muotoutumassa. Tietojen käytettävyyden varmistaminen vielä vuosien jälkeen edellyttää hyvää etukäteissuunnittelua ja varautumista erilaisiin tiedostoformaatteihin ja jopa eri osapuolten varmenteiden arkistointiin.
- On mahdollista toteuttaa asiointitapahtumien hallinta, johon sisältyvät esim. asiakkaan aiemmat asioinnit virastossa, vireillä olevat asiat ja niiden tila. Vaikka yksittäinen asiointitapahtuma ei edellyttäisi vahvaa tunnistamista, saattaa tämä olla välttämätöntä asioinninhallintapalveluissa. Asioinnin hallintapalveluissa on huomioitava tietosuojaa koskevat säädökset, etenkin mikäli yhdistetään useita rekistereitä.
- Sähköisessä asioinnissa korostuu myös viranomaisten oma asianhallinta, tietojen hallinta, arkistointi ja rajatusti myös tietojen turvaluokitus.
- Kaikki luottamuksellinen tieto on siirrettävä salatulla yhteydellä. Eri tiedonsiirron tasolla tapahtuvien salaustekniikoiden kehitys on nopeaa, ja standardointityö on käynnissä. Tällä hetkellä yleinen ratkaisu on SSL, mutta muiden tekniikoiden kehitystä tulee seurata.
- Palvelujärjestelmän ja taustajärjestelmän välisien linkkien tietoturvaan on kiinnitettävä erityistä huomiota. Linkit on rakennettava esim. tapahtumapohjaisiksi ja siten, että järjestelmät on riittävästi eriytetty toisistaan. Järjestelmien välisten linkkien tietoturvallisuus on edellytys sähköisen palvelun toteuttamiselle.

4.1.2 Vaatimukset sähköisten palveluiden tarjoajalle

Sähköinen asiointi asettaa organisaatiolle mm. seuraavia uusia tai muuttuneita vaatimuksia:

- Tietoturvallisuusosaamisen ja tietoturvallisuusasenteiden merkitys korostuu. On huolehdittava tietoturvallisuuskoulutuksen tasosta ja etenkin Internetin aiheuttamista tietoturvallisuuteen liittyvistä osaamisvaatimuksista.
- Mikäli sähköisestä palvelusta on liittymiä olemassa oleviin tietokanta tai muihin organisaation tietojärjestelmiin, on huolehdittava, ettei sähköinen palvelu heikennä sen tietoturvaa. Sähköisen palvelun käyttäjillä tulee olla pääsy vain heille sallittuihin tietoihin ja asiakkaiden oikeudet tulee muutenkin hallita hyvin. Pitää myös varmistaa, ettei palvelua voida käyttää murtoreittinä.
- Sähköisen asioinnin palvelujärjestelmän toteutukseen ja ylläpitoon osallistuvien ammattitaidon on oltava ajan tasalla. Nopeasti muuttuvassa ympäristössä vaaditaan entistä aktiivisempaa seurantaa sekä halua levittää tietoturvallisuustietoa.
- Sähköisiin palveluihin liittyvät sopimukset voivat vaatia sellaisten asioiden tarkkaa sopimista, jotka perinteisissä palveluissa on voitu jättää yleisluontoisten ohjeiden varaan.
- Jo sopimuksia laadittaessa on hyödynnettävä eri viranomaisten omia tietoturvallisuuden asiantuntijoita ja viranomaisten tietoturvallisuusohjeistusta.
- Henkilötietolain mukaisten tietojen tarkistusoikeudesta tulee informoida. Myös muista lain vaatimasta tiedottamisesta tulee huolehtia.
- On tarkoin selvitettävä sellaisten toimien vaikutukset, joissa yhtä tietoturvallisuuden osa-aluetta heikennetään, jotta toista saadaan parannettua.
- Sähköiset palvelut on myös lain mukaan toteutettava mahdollisimman yhteensopivilla välineillä. Tulee arvioida, aiheutetaanko kohtuutonta haittaa, jos esimerkiksi vanhoille selainversioille annettu tuki lopetetaan.
- Mobiiliuden vaikutus tarjottavien palveluiden tietoturvallisuuteen on erikseen selvitettävä. Sähköiset palvelut tulee suunnitella siten, että asiakasta voidaan palvella eri kanavien kautta myös yhteen asiointitapahtumaan liittyen. Tietoturvallisuusmenettelyiden tulee olla mahdollisimman yhdenmukaiset eri kanavissa.
- Palvelun tarjoajan on huolehdittava, että sillä itsellään on riittävästi kykyä palvelun tarjoamiseen osallistuvien kolmansien osapuolten tietoturvallisuuden valvontaan.
- Palvelun tarjoamien tietojen on oltava ajan tasalla ja oikeita. On suositeltavaa selkeästi ilmoittaa, milloin tietojen ajantasaisuus on viimeksi tarkistettu.
- Mikäli palvelussa käytetään varmenteita, on huolehdittava, että järjestelmä käsittelee varmenteita oikein myös poikkeavissa tilanteissa. Jos sulkulistaa ei ole jostakin syystä saatavilla, on palvelun tarjoajan itse kannettava vastuu mahdollisista väärinkäytöksistä, mikäli hän hyväksyy varmenteen.

4.1.3 Vaatimukset asiakkaille ja asiakkaan oikeudet

Perinteisessä asiointipalvelussa ei useinkaan mielletä olevan tietoturvallisuusriskejä. Vaikka Internetin tietoturvallisuusongelmat tiedostetaan, asettaa asiakkaiden kyky ja mahdollisuudet rajoituksia tietoturvallisen asioinnin toteuttamiselle. Asiakkaille voidaan asettaa mm. seuraavia vaatimuksia:

- Vahvan tunnistamisen yhteydessä asiakkaalla edellytetään olevan tarvittavat laitteet.
- Asiakkaalla on palvelun tietoturvallisen käytön edellyttämä versio Internet-selaimesta.
- Palveluiden tarjoajan mahdollisuudet vaikuttaa asiakkaan käyttöympäristöön ovat rajatut. Varsinkin vaativassa sähköisessä asioinnissa on syytä tiedottaa tästä asiakkaalle.
- Asiakkaan perusoikeutena on anonyymi palvelu aina, kun henkilön yksilöivä tunnistaminen ei ole välttämätöntä. Vaikka tunnistamisella voitaisiin tarjota parempaa palvelua, esim. perso-

noinnin avulla, on mahdollisuuksien mukaan tarjottava myös anonyymi palvelu, jonka palvelutaso on heikompi.

4.1.4 Asiakkaan luottamuksen säilyttäminen

- On vältettävä sellaisten menettelyiden käyttöä, joiden tietoturvallisuus on tosiasiallisesti heikompi, kuin miltä ne asiakkaalle näyttävät.
- Internet-tiedonsiirrossa on salaamisen käyttäminen suositeltavaa, vaikka kyse olisi pelkästään informatiivisista WWW-sivuista.
- Vaativassa sähköisessä asioinnissa on käytettävä vahvaa tiedonsiirron salausta. Mikäli tämä toteutetaan SSL-protokollalla, suositellaan vähintään 128-bittistä avainta. Muussa sähköisessä asioinnissa ja sähköisissä palveluissa riittävä taso on yleensä alempi ja riippuu palvelun sisällöstä. Mikäli asiakkaan selain ei tue sellaista tiedonsiirron salaustasoa, jota palvelun tarjoaja pitää vähimmäisvaatimuksena, on asiakasta informoitava, ettei palvelupyyntöä voida tietoturvallisesti toteuttaa.
- Käyttäjälle ladattavan koodin ei tule aiheuttaa käyttäjän tietoturvallisuuden heikkenemistä.
- Palvelun tarjoajan on varauduttava ohjeistamaan käyttäjiä sekä vastaamaan käyttöön liittyviin tukipyyntöihin. Asiakkaalle voidaan myös antaa yleistä tietoturvallisuusohjeistusta. Kyseeseen tulee etenkin sellainen tiedotus, jossa annetaan asiakkaalle mahdollisuus tutustua lisätietoon.
- Palvelun tarjoajan on varauduttava toimimaan nopeasti tietoturvallisuusriskien torjunnassa. Tietoturvallisuusriskin toteutuessa on kyettävä nopeisiin ja suunniteltuihin toimenpiteisiin.
- Sähköisissä palveluissa tulee käyttää sellaista tunnistusta ja varmenteita, että asiakkaan ei itse tarvitse epäillä niiden luotettavuudesta.
- Omien edusta- ja taustajärjestelmien tietoturvallisuuden taso on pidettävä korkeana ja tästä on tarpeen mukaan tiedotettava asiakkaille.
- Käytettävyyteen vaikuttavista seikoista kuten käyttökatkoksista tai odotettavissa olevista ruuhkahuipuista on pyrittävä tiedottamaan aktiivisesti. On harkittava ratkaisuja, joissa määräaikoja porrastetaan ruuhkahuippujen tasaamiseksi.

4.1.5 Yhteiskäyttö ja itsepalvelupisteet

Itsepalvelupisteissä useat käyttäjän käyttävät samaa tietokonetta. Tällaisessa ympäristössä sivulliset saattavat nähdä itsepalvelupistettä käyttävän henkilön luottamuksellisia tietoja. Palvelut, joissa käsitellään luottamuksellista tietoa, on suunniteltava siten, ettei selaimessa kyetä siirtymään edellisille sivuille. Tietokoneelle jäävät tiedot asiakkaan käynnistä verkkopalvelussa on pyrittävä minimoimaan, mikäli palvelu sisältää tai saattaa sisältää asiakasta koskevaa luottamuksellista tai arkaluontoista tietoa.

Periaate, että tietoturvallisuus on toteutettava mahdollisimman vähin vaatimuksin asiakkaalle on korostetun tärkeää itsepalvelupisteiden kannalta. Asiakkaalle on syytä tiedottaa käyttöympäristöön liittyvistä riskeistä.

Itsepalvelupisteiden ylläpidosta vastaavien henkilöiden on omalta osaltaan huolehdittava siitä, että laitteet ja ohjelmat ovat tietoturvallisia. Tämä on tärkeää etenkin niissä laitteissa, jotka on tarkoitettu sähköiseen asiointiin.

4.1.6 Palveluiden saatavuus

Asiakkaiden odotukset palveluiden saatavuudesta ovat kasvaneet, sillä monet tietoverkossa toimivat palvelut ovat aina käytettävissä (ns. 24/7 palvelu). Tietoturvallisuuden kannalta palvelu, jonka on

suunniteltu olevan jatkuvasti käytettävissä tuo lukuisia haasteita. Palvelun keskeytymättömyys edellyttää laitteistojen käytettävyyteen liittyviä ratkaisuja (mm. kahdennukset, varakoneet, huoltosopimukset). Lisäksi on ratkaistava myös mm. asiakastuki. Mikäli jokin osa palvelukokonaisuudesta on ulkoistettu, on selvitettävä toimittajien kyky toimia 24/7 palvelun asettamien vaatimusten mukaan. Myös reaaliaikaisesta valvonnasta ja hälytyksistä aiheutuvien toimenpiteiden ympärivuorokautinen toimivuus on varmistettava.

Tavoitteena on oltava palvelun mahdollisimman korkea käytettävyys. Tämä tarkoittaa toisaalta palvelun mahdollisimman pitkää aukioloaikaa sekä toisaalta käyttökatkosten määrän ja keston minimointia luvattuina palveluaikoina. Jos palvelun tarjoaja ei pysty varmuudella tarjoamaan palveluaan ympärivuorokautisesti, jokaisena viikon päivänä, on suositeltavaa pitäytyä niissä palveluajoissa, joina palvelun korkea taso kyetään pitämään, vaikka palvelun 24/7 saatavuus on tavoite. Etenkin asiakasrajapinnassa olevan palvelujärjestelmän 24/7 käytettävyyteen tulee pyrkiä, vaikka palveluprosessin muiden osien (taustajärjestelmät, viranhaltijat jne.) käytettävyys ei ole samalla tasolla.

Vaikka taustajärjestelmät eivät olisi toiminnassa, tulisi häiriötilanteita hallita siten, että asiakasrajapinnasta huolehtivia järjestelmiä ei tarvitse sulkea.

Asioinnin volyymi on huipussaan usein juuri ennen määräaikoja. Tähän ja muihin odotettavissa oleviin ruuhkahuippuihin on varauduttava esimerkiksi laitteistoratkaisuilla ja määräaikojen porrastuksella (jos tälle ei ole esteitä).

4.2 Sähköisten palveluiden tietoturvallinen toteutus

Turvallinen palvelukokonaisuus edellyttää turvallisuuden säilyttämistä koko palvelukokonaisuuden ajan. Turvallisuusvaatimuksiin sisältyy vaatimukset tietoturvallisesta asiakkaan fyysisestä ympäristöstä, työasemasta, tietoliikenteestä, palvelimen tunnistamisesta, asiakkaan tunnistamisesta ja taustajärjestelmistä. Lisäksi kokonaisuuteen liittyvät kolmansien osapuolisen tarjoamat palvelut.

Toistaiseksi Internet on yleisin sähköisten palveluiden tietoliikennekanava, mutta muutkin kanavat (kuten WAP, SMS, langaton lähiverkko ja digitaalinen televisio) on otettava palvelua suunniteltaessa huomioon. Tiedonsiirron turvallisuus on rakennettava korkean tason protokollalla.

Kuhunkin uuteen kanavaan liittyy teknisiä ja toiminnallisia erityiskysymyksiä. Uudet ja vielä vakiintumattomat ratkaisut, kuten langattomat lähiverkot, sisältävät usein enemmän tietoturvaongelmia kuin vanhemmat ratkaisut.

Palvelun tunnistaminen edellyttää varmennetta palvelinkoneessa. Jos palvelinvarmentajia on monta, asiakkaan pitää määritellä omaan selaimeensa kaikki hyväksytyt varmentajat. Erityisesti yhteiskäyttöisissä tietokoneissa hyväksyttyjen varmenteiden hallinta voi olla varsin puutteellista. Esimerkiksi SSL tarkistaa, että palvelimessa oleva varmenne on asiakkaan hyväksymän varmentajan myöntämä, ja että se on tarkoitettu kyseiseen palvelinosoitteeseen. Asiakkaan täytyy lisäksi hyväksyä kyseinen varmenne.

Tietoturvallisuudeltaan vahvaa tunnistamista heikompi ratkaisu on asiakkaiden tunnistaminen käyttäjätunnuksella ja salasanalla. Käyttäjän antamia tunnisteita voidaan käyttää esim. palvelun personoimiseen tai häiriötä aiheuttavien asiakkaiden poissulkemiseen. Palveluntarjoajan luomia käyttäjätunnisteita voidaan käyttää luottamukselliseen asiointiin, kunhan asiakas on etukäteen tunnistettu riittävällä luotettavuudella ja salasanajärjestely on tietoturvallisuudeltaan hyvä.

Varmennepohjainen vahva tunnistaminen on turvallinen tapa identifioida asiakas. Mikäli palvelun luonne ei kuitenkaan edellytä henkilöllisyyden varmistamista, ei varmenteen tietoja tule liittää asiakkaan muihin henkilötietoihin, vaan käsitellä irrallisena.

4.2.1 Sähköinen asiointi

Laki sähköisestä asioinnista koskee hallintoasian sähköistä käsittelyä, ja laissa on asetettu myös tietoturvallisuusvaatimuksia. Sähköisen asioinnin vaiheet ovat vireillepano ja sen täydentäminen, käsittely (ml. ratkaisu) ja päätöksen tiedoksi antaminen. Vireillepanija on pystyttävä tunnistamaan. HST-kortilla tehty tunnistaminen voidaan aina hyväksyä. Vireillepanossa vaaditaan yleensä sähköinen allekirjoitus.

On arvioitava, vaatiiko palvelun luonne kiistämättömyyden varmistavia ratkaisuja ja mitkä ovat vaatimukset palvelun käytettävyydelle. Näitä arvioitaessa on otettava huomioon mm. liittyykö palveluun määräaikoja, kuinka suuret ja millaiset vahingot syntyvät, mikäli asiakas tai palvelu kiistää vireillepanon tai päätöksen tiedoksi saattamisen, sekä mitä menettelyjä noudatetaan vastaavassa perinteisessä palvelussa.

Lain mukaan on asiakkaalle on pystyttävä lähettämään vastaanottokuittaus, josta käy ilmi vireillepanon ajankohta. Vastaanottokuittaus on merkityksellinen asiakastyytyväisyyden ja palvelun luottamuksen kannalta, joten se olisi kyettävä järjestämään muulloinkin kuin lain edellyttämissä tapauksissa. Kuittaus on pyrittävä antamaan välittömästi samassa istunnossa, jossa vireillepano on tapahtunut tai sähköpostitse. Mikäli vastaanottokuittauksen antaminen ei näillä menetelmillä onnistu, on turvauduttava esim. tavalliseen kirjeeseen.

On suotavaa, että asiakkaalle kyetään sähköisesti antamaan tietoa asian käsittelyn etenemisestä.

Vireillepano tapahtuu usein määrämuotoisella lomakkeella, mutta etenkin täydentävää materiaalia saatetaan lähettää vaihtelevilla tavoilla. Tältä osin vireillepanon tietoturvallisuus sivuaa sähköisten lomakkeiden ja sähköpostitse tapahtuvan asioinnin tietoturvallisuusnäkökohtia.

Sähköisen asioinnin asiakkaan oikeusturvan varmistamiseksi voidaan käyttää kolmannen osapuolen ylläpitämää notariaattipalvelinta, joka varmistaa asiakirjan toimittamisen.

Päätöksen antaminen sähköisesti edellyttää asiakkaan nimenomaista suostumusta ja sitä, että päätös pystytään antamaan tietoturvallisesti vireillepanijalle tai tämän valtuuttamalle henkilölle.

Sähköisessä valtuutusmenettelyssä henkilö valtuuttaa jonkun toisen toimimaan puolestaan sähköisissä palveluissa. Tästä puuttuvat yleisratkaisut ja laajamittaiset kokemukset. Valtuutusmenettely voi sisältää tietoturvallisuusriskejä, on tarkoin harkittava menettelyn tarkoituksenmukaisuus.

Vaativassa sähköisessä asioinnissa ei päätöstä voi nykyisellä tekniikalla lähettää Internet-sähköpostilla. Hallintopäätöksen vastaanottamisesta saattaa alkaa kulua määräaika. Viranomaisen ei ole mahdollista kiistattomasti todeta, onko asiakas saanut sähköpostissa päätöksen. Internet-sähköpostin perillemenoa ei voida varmistaa. Kehityksen myötä sähköpostilla tapahtuva tiedoksianto saattaa tulla mahdolliseksi. Muussa kuin vaativassa sähköisessä asioinnissa voi sähköpostin käyttöä päätöksen antamisessa tulla kyseeseen.

Vaativan sähköisen asioinnin päätösten toimittamista varten tarvitaan järjestelmä, josta asiakas käy noutamassa sähköisesti allekirjoitetun päätöksen. Tämä voidaan järjestää joko kunkin viraston ja laitoksen itse toteuttamana palveluna tai yhteishankkeilla. On kiinnitettävä huomiota käyttöoikeuksiin, asiakkaan todentamiseen ja noutamisajankohdan aikaleimoihin sekä siihen, että tiedoksiantomenettely on kaikilta osiltaan lain mukainen.

Mikäli asiakas ei nouda vaativan sähköisen asioinnin päätöstä, ja päätös on sähköisestä asioinnista annetun lain mukaisesti toimitettava vireillepanijalle muilla tavoin, on käytettävä muita lain sallimia tiedoksiantomenettelyitä.

Sähköisen päätöksen myöhempää käyttöä varten on ratkaistava sen säilytys. Ensisijaisena ratkaisuna on sähköinen säilytys, mutta mahdollista on myös päätöksen tulostaminen paperille. Tietoja voi ottaa arkistotulosteina, joiden allekirjoittamista ei välttämättä vaadita, kun päätöksenteosta on kulunut aikaa arkistotulosteen ottamiseen. Tulostus voidaan tehdä myös mikrofilmille.

4.2.2 Sähköpostin tietoturvallinen käyttö palvelukanavana

Viranomaisella tulee olla virallisasiointiin tarkoitettu sähköpostiosoite eli asiointipostiosoite, ja asiakkaita tulee opastaa tämän käytössä.

Sähköpostiasioinnissa tulee varmistaa, että asiointitapahtuma noudattaa normaalia prosessia eikä esim. diariointi jää pois, jos vireillepano lähetetään suoraan virkamiehen sähköpostiosoitteeseen.

Mahdollisten asiointipostilaatikoiden osalta on asiakkaalle tehtävä selväksi, mikä on sähköpostin turvataso, minkälaiseen asiointiin kanavaa voi käyttää ja millaiset valmiudet virastolla on vastaanottaa suojattuja sähköpostiviestejä. Sähköpostin perillemenosta tulisi vastaanottajan lähettää kuittaus.

Sähköpostin tietoturvalliseen välittämiseen on olemassa teknisiä ratkaisuja, mutta niitä käytetään vähän. Tosiasialliseksi standardiksi on muodostumassa S/MIME. PGP on käytännöllinen vain rajatuissa ryhmissä, koska sen avaintenhallinta on rajatumpaa kuin varmennepohjaisissa ratkaisuissa.

4.2.3 Sähköiset lomakkeet

Sähköisten lomakkeiden tietojen tarkistukset on pyrittävä tekemään mahdollisimman pian tietojen syöttämisen jälkeen, jotta vastaanotettavien tietojen laatu (eheys) pysyy hyvänä. Lomakkeiden piilotettavan tai muun haitallisen koodin mahdollisuus tulee minimoida mm. teknologiavalinnan kautta (katso teknologioita liitteessä 4).

Tapauskohtaisesti on harkittava mahdollisuutta muuttaa, täydentää tai peruuttaa lomakkeella annettuja tietoja. Tällöin on huolehdittava asiakkaan tunnistamisesta ja tapahtuman kiistämättömyydestä.

Kaikkien lomakkeiden osalta on huolehdittava, että verkon kautta ei tarjota vanhentuneita lomakkeita ja että lomakkeiden käytettävyys on kohderyhmän kannalta riittävän hyvä.

4.2.4 Henkilön tiedonsaantioikeus

Henkilöllä on mahdollisuus tarkistaa tietoja julkisuuslain ja henkilötietolain nojalla. Ennen palvelun toteuttamista on lainsäädännön edellytykset ja vaatimukset selvitettävä huolellisesti. On selvitettävä ja määriteltävä mihin lakiin perustuvasta oikeudesta on kysymys, vai onko kysymys vain hyvästä palvelusta.

Henkilöllä on henkilötietolain mukaan oikeus saada tarkastaa henkilörekisterissä olevat itseään koskevat tiedot tai ettei hänestä ole rekisterissä tietoja. Tarkastusoikeus voidaan säädetyin edellytyksin myös evätä. Tarkastusoikeuden toteuttamista koskeva pyyntö tulee allekirjoittaa. Tarkastuspyynnöstä voi jäädä merkintä, mutta tietoa ei saa tallettaa kyseiseen henkilörekisteriin.

Mitä arkaluontoisemmista (ja usein samalla salassa pidettävistä) tiedoista on kysymys ja mitä suurempaa määrää tiedot koskevat, sitä suurempia vaatimuksia toteutukselle asetetaan.

Viranomaisten toiminnan julkisuudesta annettu lain mukaan jokaisella on oikeus saada tieto hänestä itsestään viranomaisen asiakirjaan sisältyvistä tiedoista. Epäämisperusteista on säädetty laissa eikä pyynnölle ole muotovaatimuksia. Palvelun edellytyksenä on pyynnön esittäjän vahva tunnistaminen ja vastauksen tietoturvallinen toimittaminen.

Viranomaisten toiminnan julkisuudesta annettu laki säätää myös asianosaisen oikeudesta saada tietoa muistakin kuin julkisista asiakirjoista, jos nämä vaikuttavat tai voivat vaikuttaa hänen asiansa

käsittelyyn. On huolehdittava vahvasta tunnistamisesta ja vastauksen toimittamisen tietoturvallisuudesta. Lisäksi on huomioitava, että asiakkaalla on oikeus saada asiakirjat virallisesti vahvistettuna.

4.2.5 Ostaminen ja maksaminen (palvelut, luvat, tuotteet)

Tiedon ostamiseen liittyy maksamisen turvallisuus ja ostetun aineiston luotettava toimittaminen asiakkaalle. Toistaiseksi vaikeasti hallittavaksi jää sähköisessä muodossa toimitetun aineiston kopioinnin estäminen. Sähköisessä maksamisessa oman ongelma-alueensa muodostaa tapahtumasta syntyvä sähköinen kuitti, jonka monistamista voi olla vaikea estää.

4.2.6 Tiedottaminen

Sähköinen tiedottaminen tapahtuu enimmäkseen WWW-palvelinten HTML-sivuilla. Tässä palvelussa tärkeintä on käytettävyys. Asiakkaalla tulee olla mahdollisuus varmistua palvelun aitoudesta, mikä voi tapahtua palvelinvarmenteen avulla. Kehittyneempi muoto tiedottamisesta on personoitu tiedottaminen, jolloin asiakas saa itselleen määrittelemänsä profiilin mukaista tietoa esim. sähköpostin välityksellä. Tietoturvallisuusvaatimukset määräytyvät tällöin varsinaisen palvelun sisällön ja käytetyn palautekanavan perusteella.

Tiedotuspalveluihin voidaan lukea myös kuntalain (365/1995) ja julkisuuslain (621/1999) mukainen tiedottaminen. Julkisuuslain perusteella tapahtuvaa tietojen hankkimista ei pääsääntöisesti saa tehdä tunnistusta vaativaksi. Poikkeuksen muodostavat tiedot, jotka saadaan luovuttaa vain tietyin edellytyksin (esim. henkilötiedot ja salassa pidettävät asiakirjat). Näissä on huolehdittava pyynnön esittäjän vahvasta tunnistamisesta ja muiden luovutuksen edellytysten täyttymisestä. Viranomaisella on kuitenkin oikeus käyttää harkintavaltaa ja vaatia pyynnön esittäjän henkilöllisyyden toteamista.

Viranomainen saa yleensä antaa asiakirjan sähköisesti, jos asiakas tätä pyytää. Muu asiakirjan luovuttamistapa voi tulla kyseeseen esimerkiksi tietoturvallisuussyistä. Asiakirjojen toimitus asiakkaalle voidaan tehdä esim. verkkosivujen välityksellä, sähköpostilla tai päätöksen toimittamismenettelyn tapaisella järjestelyllä (asianosaisjulkisuus). Viimeksi mainittu on hyvä tapa silloin, kun vaaditaan vahvaa tunnistamista.

4.2.7 Tietojen suorasiirto

Tietojen suorasiirrolla tarkoitetaan tietojen siirtoa asiakkaan tietojärjestelmästä viranomaisen tietojärjestelmään. Tähän kuuluu myös tiedon siirto viranomaisen ja viranomaistoimintaa toimeksiannon pohjalta hoitavan yksityisen tahon välillä.

Suorasiirto tehdään yleensä eräsiirtona, jolloin yleisin tiedonsiirtoprotokolla Internet-ympäristössä on FTP. Koska FTP ei sinällään tarjoa riittävää tietoturvallisuutta, on tästä huolehdittava muilla keinoin kuten tietoliikenteen salauksella (SSL, VPN) ja siirrettävien tiedostojen salauksella. Eräsiirto on sallittava ainoastaan tunnistetuille asiakkaille. Erityisesti on huolehdittava oikeuksien hallinnoinnista tietoja vastaanottavassa järjestelmässä.

Vastaanotettavaa dataa on kontrolloitava, jotta pystytään esim. estämään palvelun käytettävyyden heikkeneminen tilanteissa, joissa datan määrä nousee epätavallisen suureksi. Saapuvalle datalle on tehtävä tarkistukset esim. vahinko-ohjelmien eliminoimiseksi.

Suurten tietomäärien siirroissa voidaan hyödyntää esim. TYVI-operaattoreita, jolloin operaattori hoitaa tietojen keruun loppuasiakkailta ja siirtää tiedot eräsiirtona viranomaiselle.

5 RISKIENHALLINTA

Sähköisten palveluiden uhat muuttuvat ja monipuolistuvat. Tämä tapahtuu nopeudella, joka on toista luokkaa kuin perinteisissä palveluissa. Varautuminen uhkiin edellyttää jatkuvaa kehitystyötä ja aktiivista tietoturvallisuusasioiden seurantaa.

Uhkiin varaudutaan samalla menetelmällä kuin perinteisissä palveluissa. Ensisijaisesti pyritään välttämään riskejä ja toissijaisesti minimoimaan niiden aiheuttamaa uhkaa. Uhkan toteutumisesta aiheutuvaa vahinkoa pyritään rajoittamaan ja vahinkojen korjaamista nopeuttamaan ennakkosuunnittelulla. Sähköisessä maailmassa ennakoiva, laaja-alainen ja aktiivinen riskeihin varautuminen on entistä tärkeämpää (kts. VAHTI 1/2001).

Jotta tietoturvallisuusratkaisut eivät vanhenisi liian nopeasti, ja jotta ne kykenisivät vastaamaan myös sellaisiin uhkiin, joiden merkitystä ei kyetä arvioimaan, voi olla perusteltua mitoittaa turvatoimet paremmiksi, kuin mitä vain tunnistettuihin uhkiin varautuminen edellyttäisi.

5.1 Tietoturvallisuuden uhkakuvia

Sähköiset kanavat lisäävät tunkeutumisyritysten riskiä, sillä näistä tehty tunkeutumisyritys on vaivattomampaa ja kiinnijäämisriski on pienempi. Lisäksi tunkeutumisen onnistuttua tiedon hyväksikäyttäminen on paljon nopeampaa kuin fyysisessä ympäristössä.

Suurin riski on sisäisten tietoverkkojen ja palvelinten hallitsematon avautuminen Internetiin.

Tietoturvallisuusvahinkoja voi olla mahdotonta mitata rahallisesti. Useat virastoissa käsiteltävät asiat eivät ole taloudellisesti merkittäviä tai niiden taloudellisen arvon määrittäminen on mahdotonta, mutta ne on säädetty salassa pidettäviksi.

5.2 Uhkat ja varautuminen

Eri palveluiden osalta on tärkeää hahmottaa palvelun luonne ja sen pohjalta muodostuva riskiprofiili. Riskiprofiiliin liittyy uhkien tunnistaminen, uhkien todennäköisyyden arviointi sekä tietoturvallisuuden pettämisestä aiheuttamien vahinkojen merkityksen arviointi.

Uhkien tunnistamiseen kuuluu niiden asioiden määrittäminen, joihin uhat saattavat kohdistua, ketkä saattavat uhata tietoturvallisuutta ja keinot, joilla tämä saattaa tapahtua. Menetelmä on sinällään sama kuin perusjärjestelmien tietoturvallisuutta arvioitaessa.

5.2.1 Potentiaalisia kohteita

Sähköisen palvelu saattaa sisältää tietoja palvelun asiakkaista, palvelun tarjoajasta ja kolmansista osapuolista. Keinoja näiden suojaamiseen ovat käyttöoikeuksien hallinta, tietojärjestelmien ja tietokantojen eriyttäminen ja reaaliaikainen valvonta sekä palvelujärjestelmästä perusjärjestelmään tulevien palvelupyyntöjen rajaaminen vain ennalta määrättyihin. Verkon segmentoinnin merkitys on normaalia tärkeämpää sähköisissä palveluissa ja tietokantojen hajautuksella voidaan parantaa tietoturvallisuutta.

Sähköisillä palveluilla on arvoa niiden käyttäjille ja niitä tarjoavalle organisaatiolle. Erityisen houkuttelevia kohteita ovat sellaiset palvelut, joiden käyttäjämäärät ovat suuria, palvelun merkitys sen asiakkaille on suuri tai palvelun saama negatiivinen julkisuus olisi erityisen vahingollista, esimerkiksi julkisuuteen tulleiden tietoturvallisuutta tai palvelun toimivuutta koskevien epäilyjen vuoksi. Tätä kohdetta tulee suojella erityisesti estämällä asiattomien pääsy järjestelmään, varautumalla palvelunestohyökkäyksiin valvontaohjelmistolla ja -laitteilla sekä rakentamalla järjestelmä riittävän suorituskykyiseksi, jotta sen käytettävyys ei ole erityisen haavoittuva palvelunestohyökkäyksille.

On myös huomioitava mahdollisuus, että palvelun asiakkaita saatetaan hämätä oikealta näyttävän, mutta vahingollisia tarkoituksia ajavan verkkopalvelun avulla. Tätä uhkaa voidaan torjua palvelinvarmenteilla ja palvelujärjestelmän korkealla käytettävyydellä.

Palvelut saattavat sisältää asiakkaiden tai muiden käyttäjien tunnistetietoja, jotka mahdollistavat pääsyn muihin järjestelmiin tai joiden muuttaminen turmelisi palveluun luovutetun tiedon eheyden. Näiden tietojen joutuminen asiattomille on erittäin vaarallista, sillä tiedoilla on mahdollista tehdä vahinkoa muissa palveluissa tai tehdä sellaista vahinkoa, jonka paljastumiseen saattaa kulua aikaa. Tulee huolehtia siitä, että tunnistetietoja ei tarpeettomasti talleteta tai että ne muutetaan sellaiseen muotoon, jossa niiden käsittely on ulkopuoliselle hankalaa.

Erityisen kiinnostavia kohteita ovat taloudellista arvoa omaavat kohteet. Rahan ja rahanarvoisten etuuksien lisäksi tähän voidaan katsoa kuuluvaksi liikesalaisuuksia sekä ohjelmia ja tiedostoja, jotka eivät ole vapaasti saatavilla. Tämän ryhmän asioilta suojautumisesta on yksityisellä sektorilla kokemusta. Toimivia ratkaisuja voidaan saada myös yritysten tekemistä ratkaisuista.

Sähköisten palveluiden erityispiirre on tunkeutujien mahdollisuus vaurioittaa ohjelmallisesti palvelun tarjoajan ohjelmia esim. virusten avulla. Tätä uhkaa torjutaan palomuurilla, virustorjuntaohjelmistoilla sekä verkonvalvontaohjelmilla. Laitteiston fyysinen suojaaminen eroaa taustajärjestelmien suojaamisesta etenkin siinä, että eri tyyppisiä laitteita on enemmän.

Väärällä informaatiolla saatetaan vahingoittaa palvelun tarjoajan tai palvelun asiakkaiden etuja. Verkkosivujen sisällön suojaaminen tulee noudattaa samoja periaatteita kuin ohjelmistojen ja palveluiden suojaaminen. Lisäksi on huomioitava palvelun tarjoajan henkilöstön tai yhteistyökumppaneiden taholta tuleva uhka. Tähän voidaan varautua mm. verkkosivujen sisällön päivitysoikeuksien hallinnoinnilla ja organisatorisilla järjestelyillä.

Eräät organisaation tietoturvallisuusjärjestelyitä koskevat tiedot ovat erityisen arvokkaita ja niiden suojaaminen on erittäin tärkeää.

5.2.2 Potentiaalisia uhan lähteitä

Suuri ero perinteisten ja sähköisten palveluiden tietojärjestelmien uhkien lähteiden välillä on, että jälkimmäisessä asiakkaat pääsevät käyttämään järjestelmää. Uhka asiakkaiden tahoilta voi olla joko tahatonta, tahallista tai se voi olla silkkaa uteliaisuutta ilman ilmeistä vahingoittamis- tai hyötymistarkoitusta. Tältä taholta tulevaa uhkaa voidaan pienentää erottamalla palvelujärjestelmät taustajärjestelmistä, käyttäjätunnistuksen avulla sekä etenkin asiakkaiden käyttöoikeuksien hallinnalla.

Sähköisissä palveluissa uhkan tietoturvallisuudelle muodostaa myös oma henkilöstö huolimattomuuden, väärien asenteiden tai puutteellisen ammattitaidon vuoksi. Vahingoittamistarkoituksessa tehdyt tietoturvallisuusrikkeet ovat ilmeisesti harvinaisempia. Tähän uhan lähteeseen tulee vaikuttaa henkilökunnan käyttöoikeuksilla, koulutuksella, esimiesten tekemällä seurannalla ja johdon esimerkillä. Teknisen valvonnan mahdollisuudet ovat rajatut.

Palvelun tarjoamiseen osallistuvien kolmansien osapuolten muodostamaan uhkaan varaudutaan oikeuksien hallinnoinnilla, auditoinneilla ja sopimusten selkeydellä.

Asiattomat ulkopuoliset (ml. hakkerit) ovat kenties parhaiten tunnettu uhan lähde. Näiden toiminta on tarkoitushakuista ja heillä on tietomurtoihin vaadittavat tiedot, taidot ja välineet. Heillä on monesti paremmat tiedot tietojärjestelmien heikoista komponenteista ja juuri paljastuneista tietoturvallisuusaukoista kuin itse palvelun tarjoajalla. Vihamielisiä ulkopuolisia vastaan ovat käytössä lähes kaikki ulkopuolisia tahoja vastaan olevat keinot. Palomuurin ja muun tietoliikenteen valvonnan merkitys korostuu. Asiattomat ulkopuoliset pyrkivät usein käyttämään hyödyksi tietoturvallisuuden

kannalta keskeisten komponenttien heikkouksia, minkä vuoksi tietojärjestelmäkomponenttien konfigurointi ja päivitykset ovat tehokkaita keinoja näitä tahoja vastaan.

Rikollisuus eri muodoissaan muodostaa kasvavan uhan. Rikollisjärjestöjen ensisijaiset kohteet poikkeavat tavallisten hakkereiden kohteista siitä, että näiksi valitaan valtion turvallisuuden kannalta keskeisiä palveluita ja palveluita, joiden väärinkäyttö suo mahdollisuuden taloudelliseen hyötyyn tai joissain tapauksissa laajaan julkisuuteen. Tähän ryhmään on luettavissa myös järjestelmällistä tiedustelutoimintaa harjoittavat yritykset ja organisaatiot. Suojautuminen näitä vastaan edellyttää suojaustoimien ensiluokkaisuutta.

5.2.3 Suojautuminen hyökkäyksiltä

Sähköiseen palveluun kohdistuu monia hyökkäystapoja, joista erityisen vaarallisia ovat niiden erilaiset yhdistelmät.

Yleisiä keinoja, joita voidaan käyttää useita hyökkäystapoja vastaan ovat palomuurin, palvelinten ja muiden laitteiden lokitiedostojen seuranta ja analysointi. Seuranta voi olla jälkikäteen tapahtuvaa, mutta painopiste on siirtymässä reaaliaikaiseen valvontaan. Esimerkki tästä on hälytykset, jotka laukeavat, kun palvelupyyntöjen kokonaismäärä tai yksittäisen palvelupyynnön jokin kriteeri ylittää ennalta asetetun rajan.

Ehkä tunnetuin hyökkäystapa on luvaton tunkeutuminen tietojärjestelmiin (ns. hakkerointi). Pääasiallisena suojakeinona ovat järjestelmien ja niiden osien segmentointi, palomuurit sekä palvelujärjestelmien reaaliaikainen valvonta ja näistä saatavat hälytykset.

Tietoliikenteen kuuntelu tai reititys väärään paikkaan ovat keinoja, joilla pyritään saamaan selville tietoa, jota voidaan käyttää joko sellaisenaan tai hyödyntää tietojärjestelmiin tunkeutumisessa. Tätä hyökkäystapaa vastaan voidaan puolustautua mm. tietoliikenteen salauksella sekä palvelinvarmenteilla.

Virusuhkaa ei tule vähätellä, sillä nopeasti leviäviä, kiusaa tai paikallista tietojen tuhoutumista aiheuttavia viruksia vakavampi uhka saattaa muodostua viruksista, jotka on suunnattu tiettyä palvelua tai palveluntarjoajaa vastaan. Vahinko-ohjelmien uhkaa voidaan hallita paremmin virustorjuntaohjelmilla, palveluiden ohjelmistovalinnoilla, käyttöjärjestelmävalinnoilla, teknisillä palvelun seurantavälineillä sekä henkilöstön koulutuksella.

Palvelunestohyökkäyksiin voidaan varautua näiden torjuntaan tarkoitetuilla ohjelmilla, muiden ohjelmistojen ja niiden komponenttien valinnalla ja konfiguroinnilla, sekä mitoittamalla palvelun kapasiteetti riittävän suureksi. Reaaliaikainen valvonta ja hälytykset nopeuttavat reagointia.

Hyökkäys voi kohdistua paitsi koko palveluun myös yksittäiseen palvelutapahtumaan tai asiakkaaseen. Tällöin pyritään estämään asiakkaan pääsy palveluun tai muuttamaan tietoja, joita asiakas ja palvelu välittävät toisilleen. Suojautumiskeinoja ovat tietoliikenteen salaus ja tietojen luottamuksellisuuden ja eheyden tarkistus.

Palveluntarjoajan henkilökuntaa voidaan käyttää apuna joko suorassa yrityksessä tunkeutua järjestelmiin tai siten, että nämä toimillaan mahdollistavat tai auttavat muita hyökkäystapoja. Keinoja tämän tyyppisten hyökkäysten torjunnassa ovat käyttöoikeuksien hallinta, muutosten hyväksymismenettelyt, tietoturvallisuussopimukset sekä tarvittaessa henkilökunnan turvallisuuskartoitukset. Lähiverkkojen ja tietojärjestelmien seurantaa tulee myös hyödyntää.

Väärennetyillä tunnistetiedoilla voidaan suorittaa tietojärjestelmiin tunkeutuminen ilman, että asia tulee välittömästi ilmi. Keinoja tätä uhkaa vastaan ovat vahvan tunnistusmenettelyn käyttö sekä vain luotettavien ja hyväksi havaittujen apupalveluiden käyttäminen.

Asiakkaan omat virheet saattavat vaarantaa tietoturvallisuuden. Salasanat saattavat unohtua tai niitä saatetaan käsitellä huolimattomasti. On vaikeaa täysin estää tällaisia väärinkäytöksiä, joten pääpaino on syytä asettaa vahinkojen minimointiin. Käyttäjän käyttöoikeudet on kyettävä perumaan nopeasti. Palvelujärjestelmiä voidaan rakentaa siten, että vahinkojen määrää rajoitetaan esimerkiksi rajaamalla käyttäjän oikeuksia joidenkin toimenpiteiden tekoon tai rakentamalla useamman tason turvajärjestelmiä. Myös tiedottamisella voidaan jossain määrin vaikuttaa asiakkaisiin.

Ohjelmisto tai ohjelmistokomponentti, joka toimii väärin tai aiheuttaa tietoturvallisuuden heikkenemisen. Palvelun tietoturvallisuudesta vastaavan henkilöstön on saatava ajantasaista ja luotettavaa tietoa palvelukomponenttien tietoturvallisuusaukoista ja kyettävä nopeaan reagointiin näiden poistamiseksi.

5.3 Järjestelmien hallintaan liittyvät riskit

Kokonaisarkkitehtuurissa on välttämätöntä pitää julkisen verkon kautta tapahtuva toiminta selkeästi erillään organisaation omassa verkossa tapahtuvasta toiminnasta. WWW-palvelimet on sijoitettava sisäisen verkon ulkopuolelle ja niistä on avattava vain välttämätön tietoliikenneyhteys organisaation tietojärjestelmiin. Turvallinen ratkaisu on palvelupyyntöihin perustuva sovellusarkkitehtuuri. Olennaista on, että jokaisen palvelupyynnön lähde ja sisältö tarkistetaan ennen pyyntöön vastaamista.

Sähköisten palvelujen arkkitehtuurissa on käytettävä yleisiä ratkaisuja ja valmiita komponentteja. Komponenttipohjaisessa ratkaisussa mahdollistetaan tietoturvallisuuden joustava parantaminen, sillä kutakin komponenttia voidaan kehittää erikseen. Lisäksi tietoturvallisuuden kannalta keskeiset toiminnot voidaan tehdä omiksi komponenteiksi, joita muut komponentit käyttävät.

Komponenttiarkkitehtuureihin on jo valmiiksi rakennettu tietoturvallisuutta edistäviä ratkaisuja. Tällaisia ovat mm. tiedonsiirron salaus, vastapuolten tunnistaminen, käyttöoikeuksien tarkistaminen ja sopeuttaminen palomuuriratkaisuihin.

Organisaation nykyisten tietojärjestelmien muuttaminen sanoma- tai oliopohjaisiksi järjestelmiksi on huomattavan suuri työ, eikä kaikkia järjestelmiä edes välttämättä onnistu muuttamaan moderneja rajapintoja tarjoaviksi.

Sähköisten palvelujen alkuvaiheessa asiakasmäärät ovat vielä usein varsin alhaiset, mikä voi helposti johtaa palvelun kapasiteetin alimitoitukseen ja tästä johtuvaan käytettävyyden laskuun. Kuormitusta arvioitaessa on huomioitava mm. kokonaisasiakasmäärä, palvelutapahtumien määrä ja tämän vaihtelu eri ajanjaksoilla, käytettyjen salausmenetelmien vaatima kapasiteetti, palvelun laajeneminen sekä monimutkaistuminen lähitulevaisuudessa.

Merkittävän riskin palvelujen tietoturvallisuudelle aiheuttavat ulkopuoliset palvelut, ennen kaikkea niiden käytettävyys ja jatkuvuus pitkällä tähtäimellä. Jokainen uusi toimija palveluketjussa kasvattaa riskipotentiaalia.

5.4 Palvelun tekninen valvonta

Sähköiseen palvelun järjestelmiin tulee kohdistaa normaalit verkkoympäristön valvontatoimenpiteitä. Palomuurin lokitietoja ja palvelun kuormitusta tulee seurata jatkuvasti ja automaattisesti. Hälytyksestä aiheutuvat toimenpiteet tulee määritellä, harjoitella ja testata etukäteen.

Yleisiä verkonvalvontaohjelmistoja voidaan käyttää myös sähköisen palvelun eri komponenttien toiminnan valvontaan. Valvonnan painopiste on reaaliaikaisessa valvonnassa, mutta myös staattisia analysointiohjelmia tulee käyttää. Palvelunestohyökkäyksiä voidaan estää hyökkäyksiltä suojaavin laittein ja ohjelmistoin.

Kaikista palveluun kohdistuvista muutoksista on pidettävä muutoslokeja. Lokeihin perustuvan valvonnan tulee olla reaaliaikaista ja ympärivuorokautista, jotta mahdolliset tunkeutumisyritykset havaitaan heti. Lokitiedot on säilytettävä siten, ettei niitä päästä asiattomasti muuttamaan.

5.5 Palvelun ja järjestelmien tarkistaminen ja seuranta

Riskienhallinnan keskeinen väline on tietoturvallisuuden seuranta. Tähän kuuluvat lokitietojen kerääminen, analysointi ja raportointi, sekä tietoturvallisuuden eri osa-alueille tehtävät auditoinnit.

Monilla virastoilla ei itsellään ole resursseja auditoinnin toteuttamiseen, vaan auditointi tilataan kolmannelta osapuolelta. Tämä on perusteltua sähköisen asioinnin järjestelmissä, sillä järjestelmien tietoturvallisuusauditoinnin tekemiseen vaadittavaa osaamista ei asiointijärjestelmän omistavalla organisaatiolla välttämättä ole.

Sähköisen asioinnin tietojärjestelmien tietoturvallisuusauditoinnit eivät oleellisesti eroa muiden järjestelmien auditoinneista. Järjestelmän komponenttien ja toimintaympäristön nopean muutoksen vuoksi näitä on syytä järjestää useammin kuin muita tietoturvallisuusauditointeja. Myös valmiudet ad hoc –tyyppiseen, lyhyellä varoitusajalla suoritettavaan ja rajattuihin asioihin keskittyviin auditointeihin korostuvat. Auditoinnit tulee kohdistaa riskialteimpiin osiin ja toimintoihin. Tämä edellyttää kunnollista palvelun riskikartoitusta.

Asiakkaiden ja kolmansien osapuolten tietoverkkoihin tuntemien epäluulojen vuoksi on auditoinneista tiedottamista on syytä harkita. Tiedottaminen voi olla yleisluontoista, mutta mahdollista on myös antaa tietoa auditoinnin tuloksista niiltä osin kuin tiedottaminen itsessään ei vaaranna tietoturvallisuutta. Eräs keino tähän on ulkopuolisen luotettavan tahon tekemä tietoturvallisuusauditointi, jonka perusteella palvelulle myönnetään sertifikaatti tai muu vastaava todistus.

Tietoturvallisuuden ns. kahdeksasta osa-alueesta on tietoturvallisuusauditoinnissa syytä painottaa seuraavia: tietoliikenneturvallisuus, käyttöturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus (erityisen korostunut luottamuksellisia tietoja käsittelevissä palveluissa). Myös henkilöturvallisuuden merkitys on usein korostetun tärkeää.

Muista tietoturvallisuuden osa-alueisissa korostuvat tietyt osa-kokonaisuudet, kuten virastoajan ulkopuolisen käytettävyyden asettamat vaatimukset organisaatiolle, henkilöstölle ja laitteistoille. Nämä vaihtelevat kuitenkin palvelu- ja organisaatiokohtaisesti.

5.6 Teknologian kehitys

Teknologiavalinnoilla on keskeinen merkitys tietoturvallisen palvelun kannalta. Teknologiavalinnoissa tulee painottaa tietoturvallisuutta ja tämän ylläpidon kustannuksia.

Vain osa sähköisten palveluiden komponenteista on perusratkaisuiltaan pitkäaikaisia. Komponentteja voidaan joutua vaihtamaan niiden teknisen vanhenemisen vuoksi, mutta myös niissä todettujen tietoturvallisuuspuutteiden vuoksi. Eräiden komponenttien elinikä riippuu osittain vaadittavasta tietoturvallisuustasosta. Esimerkiksi salausavaimelta vaadittava pituus riippuu tietokoneiden laskentanopeuden kehityksestä ja dokumenttien säilytysajan pituudesta.

PKI on ilmeisen pitkäikäinen perusratkaisuna, mutta ohjelmat ja ratkaisut ovat vielä uusia ja kehittyviä.

5.7 Sähköisten palveluiden elinkaari ja tietoturvallisuus

Elinkaariajattelussa tarkastellaan tietoturvallisuuden kannalta keskeisiä asioita alkaen palvelun esitutkimuksesta ja päättyen palvelun lopettamiseen. Tietoturvallisuuden on oltava mukana esitutki-

muksesta alkaen. Tietoturvallisuus on palveluun kiinteästi kuuluva asia, eikä irrallinen osuus, joka voidaan haluttaessa liittää mukaan elinkaaren ensimmäisten vaiheiden jälkeen.

Sähköisen palvelun lainmukaisuudesta on huolehdittava elinkaaren kaikissa vaiheissa, mutta erityisen tärkeää tämä on esitutkimuksessa ja määrittelyssä.

Tietoturvallisuuden merkityksen korostaminen alkaa tarjouspyynnöistä, ja tietoturvallisuusratkaisujen merkitystä teknologia- ja toimittajavalinnoissa tulee korostaa.

Palvelun luonne on huomioitava myös elinkaaritarkastelussa.

5.7.1 Toteutusprojekti

Esitutkimusvaiheessa on selvitettävä, mitkä ovat sähköisen palvelun erot verrattuna perinteiseen palveluun. On tehtävä karkea riskianalyysi, jossa selvitetään, onko sähköisen palvelun tietoturvallinen toteuttaminen mahdollista. On myös pohdittava, onko palvelun sähköinen toteuttaminen järkevää.

Esitutkimusvaiheessa pyritään kartoittamaan tietoturvallisuuden kannalta keskeiset asiat, joihin on otettava kantaa toteutuksen myöhemmissä vaiheissa. Tietoturvallisuuden tavoitetaso on asetettava riittävän korkealle tasolle.

Johdon on sitouduttava tietoturvaan hankkeen alusta alkaen, ja sille on annettava oikea kuva tietoturvallisuuden rakentamisen ja ylläpidon vaatimista resursseista.

Määrittelyvaiheessa palvelun määrittelyvaiheessa on vältettävä sellaisten palveluiden ja komponenttien ottamista mukaan, joiden tietoturvallinen toteuttaminen tai ylläpito vaatii runsaasti resursseja.

Suunnittelussa on pidettävä mielessä palveluketjun kaikki osapuolet sekä heidän käyttöympäristönsä. Asiakkaille suunnattu tiedotus on myös suunniteltava.

Tietoturvallisuusvastuiden epäselvyydet toteutusprojektin aikana ovat tavallinen ongelma, etenkin monitoimittajaympäristössä. Tähän voidaan varautua sopimusten selkeydellä sekä tietoturvallisuuden merkityksen korostamisella myös muissakin yhteyksissä.

Järjestelmät koostuvat usein lukuisista, mahdollisesti hajautetuista ja usean osapuolen tekemistä komponenteista. Tällöin on kiinnitettävä huomiota rajapintojen hallintaan sekä palvelujärjestelmän ja taustajärjestelmän välisen tiedonsiirron hallintaan.

Tietoturvallisuus tulee testata tuotantoympäristössä. Sähköisellä palvelulla voi olla ulkopuolisia testikäyttäjiä, vaikka palvelu ei vielä täysimittaisesti toimikaan tuotantoympäristössä. On valittava sopiva testikäyttäjäryhmä, jolle palvelun keskeneräisyydestä on tiedotettava.

Testauksissa on arvioitava palvelujärjestelmän käytettävyys ruuhkahuipuissa. Tämä on erityisen tärkeää palveluissa, joihin liittyy aikarajoja tai joiden käytettävyydelle asetetaan poikkeuksellisen suuret vaatimukset.

Palomuuriin määriteltävät palvelukohtaiset oikeudet tulee minimoida.

Käyttöönottovaiheessa tietoturvallisuuden kannalta keskeistä on toimivan kokonaisuuden varmistaminen ennen laajaa käyttöönottoa. Käyttöönotossa esiintyy usein tilapäisiä katkoksia käytettävyydessä. Näihin syytä varautua esim. varajärjestelyjen harjoittelulla.

5.7.2 Palvelun tuotanto

Mikäli tietoturvallisuusratkaisut on hoidettu hyvin edellisissä vaiheissa, on tietoturvallisuuden pääpaino tuotantovaiheessa ylläpidossa ja yleisessä jatkokehittämisessä.

Internet-ympäristössä muutokset tapahtuvat nopeasti, mikä edellyttää tietoturvallisuudelta suurempaa reaktionopeutta kuin perinteisissä ratkaisuissa.

Palvelun lopettamisessa on olennaista pystyä käsittelemään palvelun riippuvuuksia oikein, jotta ei aiheuteta tietoturvallisuusongelmia jollekin toiselle palvelulle.

Tietoturvallisuuden sopeuttaminen muutoksiin on keskeinen vaatimus. Muutosten vaikutus muihin palveluihin on pyrittävä ennakoimaan. Muutokset saattavat vaatia uutta tekniikkaa, jonka soveltuvuus on arvioitava palvelukokonaisuuden kannalta. Modulaariseksi suunniteltu palvelu helpottaa muutosten tietoturvallista toteutusta.

6 VASTUUT JA SOPIMUKSET

Tietoturvallisuusriskien ymmärtämisen edellytyksenä on ymmärtää omat ja toisen osapuolen riskit sekä näiden väliset riippuvuudet, toisen osapuolen riskienhallinnan suunnitelmien tehokkuus ja toimivuus, sekä toisen osapuolen riskienhallinnan aiheuttamat kustannukset.

Kehitettävää palvelua on tarkasteltava kokonaisvaltaisesti sekä tilaajan (sähköisten palveluiden tarjoajan) että toimittajan kannalta. Tarkastelun tuloksena löydetyt tietoturvallisuuteen vaikuttavat riskit on analysoitava ja niiden hallinta on yhteisesti sovittava.

	Tilaajan riskit	**Toimittajan riskit**
Toiminnalliset riskit	Tietoturvallisuusratkaisu ei mahdollista palvelun jatkokehittämistä. Palvelun toimivuus lakkaa. Tietoturvallisuuden laatutasosta voidaan joutua tinkimään	Asiakasratkaisusta muodostuu vain yhtä asiakasta koskeva. Alihankkija tai kolmas osapuoli lopettaa oman palvelunsa kehittämisen tai tarjoamisen.
Tekniset riskit	Toimittaja ei tue asiakkaan haluaman arkkitehtuurin jatkokehitystä. Tietoturvallisuutta toteutetaan vanhalla, epätyydyttävällä arkkitehtuurilla.	Ei saada standardoitua tarjottua ratkaisua. Osaamattomuudesta aiheutuvat riskit
Taloudelliset riskit	Syntyy ennalta arvaamattomia kustannuksia tietoturvallisuuden tason saavuttamisesta ja ylläpitämisestä.	Joudutaan ylläpitämään osaamista vain yhtä tilaajaa varten. Tietoturvallisuuden laatutason alituksesta toimittajalle aiheutuvat sanktiot.

Sähköisen palvelun komponentit ja palvelut on hankittava luotettavilta toimittajilta, joilla on turvallisuuspolitiikka. Politiikassa määritellään toimittajan vastuu. Omat suojaustoimenpiteet on mitoitettava toimittajien tarjoamaa tasoa vastaavaksi.

Palveluja ulkoistettaessa kokonaisvastuu jää ulkoistajalle, vaikka toimittajalla on omat vastuunsa. Palvelun ulkoistaja on vastuussa tietoturvallisuusvaatimusten toteutumisesta. Tästä on tehtävä kirjallinen sopimus, jossa on määriteltävä osapuolten vastuut ja velvollisuudet. Sopimusten tietoturvaa käsittelevien kohtien ajantasaisuus on tarkistettava säännöllisesti.

Tietoturvallisuustuotteiden pitää olla luotettavia ja turvallisiksi todettuja, vapaita mahdollisista vientikielloista ja niiden turvallisuudesta pitää voida varmistua. Tuotteisiin on oltava syvällinen osaaminen kotimaassa. Turvallisuuden kannalta kriittisten palveluiden on käytettävä parasta mahdollista tekniikkaa.

On pyrittävä varmistamaan keskeisten palveluiden jatkuvuus esim. yritysjärjestelyissä ja siitä tapauksessa, että palvelun ulkoistus lopetetaan tai se siirretään toiselle toimittajalle. Näiden asioiden yleisyyden vuoksi ne on syytä kirjata sopimuksiin.

Tietoturvallisuuteen liittyviä vastuukysymyksiä on tarkemmin käsitelty ohjeessa *Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus (VAHTI 2/1999).*

Yhteistyökumppanin valinnassa atk-palveluyrityksen ja sen hankkeelle tarjoamien henkilöiden tietoturvallisuusosaaminen on keskeinen valintakriteeri sähköisten palvelujen kehityshankkeissa ja erityisesti vaativan sähköisen asioinnin hankkeissa.

7 VARMENTEISIIN PERUSTUVIEN TOIMINTOJEN ERITYISKYSYMYKSIÄ

7.1 Varmenteet ja varmennepalvelut

Varmenne on tietojoukko, jonka on allekirjoittanut luotettava taho. Sillä yksilöidään varmenteen haltija. Varmentajan allekirjoituksella varmistetaan tämän tietojoukon muuttumattomuus (eheys) ja alkuperä. Varmenteella on talletettuna ns. julkinen avain, joka yhdessä varmenteen haltijan hallitseman salaisen avaimen kanssa mahdollistaa sähköisen allekirjoituksen.

Kokonaisuus koostuu korteista tai muista välineistä, joille varmenne ja salainen avain on sijoitettu; julkisesta hakemistosta, josta on saatavissa tiedot asiakkaiden julkisista avaimista; ja sulkulistasta.

Sovelluksia rakennettaessa on olennaista hyödyntää infrastruktuurin tarjoamia palveluita, joita ovat: hakemistopalvelu, josta saadaan selville eri asiakkaiden julkiset avaimet; sulkupalvelu; sulkulista, jossa julkaistaan tiedot suljetuista korteista; notariaatti- ja aikaleimapalvelimet (eivät vielä ole laajamittaisessa käytössä).

Kunkin varmenteen luotettavuus riippuu varmenteen myöntämisen yhteydessä käytetystä tunnistamismenettelystä, varmenteen sijoittamisesta sekä käytettävien avainten pituudesta.

Turvallisena lähtökohtana luotettavassa todentamisessa ja allekirjoituksessa voidaan pitää varmenteisiin pohjautuvaa, tyypillisesti toimikorttipohjaista todentamista. Väliaikaisratkaisuja ei suositella.

Sähköisessä asioinnissa on palveluiden tarjoajan hyväksyttävä varmentajat ja varmenteet, jotka ovat valtiovarainministeriön ylläpitämällä listalla. Listalla olevat varmentajat ja varmenteet täyttäjät sähköisestä asioinnista annetussa laissa olevat vaatimukset ja se on osoitteessa: http://www.vn.fi/vn/vm/kehittaminen/julkisten_palvelujen_kehittaminen/hko24.htm.

7.2 Sähköinen tunnistaminen ja todentaminen

Tunnistamisessa todetaan vastapuolen henkilöllisyys jonkin yksilöivän tekijän perusteella, esim. sähköisen asiointitunnuksen perusteella. Todentamisessa varmistetaan, että asioinnin vastapuoli on varmasti se, joka hän väittää olevansa.

Todentamisen kautta voidaan yleisesti toteuttaa tietojärjestelmiin myös kiistämättömyyden ja jäljitysketjuja sisältäviä toimintoja. Tulee varautua riskiin, että ajallisesti pitkäaikainen, jälkikäteen tapahtuva kiistämättömyyden ja jäljityksen toteaminen voi epäonnistua esimerkiksi varmenteiden ja varmenteisiin liittyvien palveluiden muuttuessa tai vanhentuessa.

Suomessa varmenteisiin perustuva sähköinen tunnistaminen perustuu toimikortille talletettuihin varmenteisiin.

7.3 Sähköinen allekirjoitus

Yksittäinen dokumentti voidaan allekirjoittaa sähköisesti. Tapahtumaketju tai sähköpostisanoma voidaan myös allekirjoittaa. Itse allekirjoitukseen liittyvä tekninen ratkaisu on näissä kaikissa sama, mutta allekirjoitettavan datan kokoaminen sekä allekirjoituksen liittäminen dataan poikkeavat.

Sähköiseen allekirjoitukseen liittyy datan muokkaaminen tiivistettyyn muotoon, joka salakirjoitetaan allekirjoittajan salaisella avaimella. Allekirjoituksen tarkistamiseen käytetään vastaavaa julkista avainta. Allekirjoitukseen liittyviä salaus- ja tiivistetekniikoita käsitellään VAHTI:n suosituksessa Salauskäytännöt.

EU:n sähköisen allekirjoituksen direktiivi (1999/93/EY) sisältää sähköisiin allekirjoituksiin ja sen eri tasoihin liittyviä määritelmiä. Direktiivin implementointi kansalliseen lainsäädäntöön on valmis-

teilla. Sähköisen allekirjoitukseen perustuvat ratkaisut kehittyvät voimakkaasti ja standardointityö on osittain kesken.

7.4 HST- ja virkamieskortti

Viranomaisten kansalaisille tarjoamia palveluja varten on tehty HST-palvelustruktuuria ja HST-kortti. Viranomaiset voisivat periaatteessa käyttää samoja henkilökohtaisia HST-kortteja, mutta on nähty hyväksi toteuttaa erillinen HST-infrastruktuurin kanssa yhteensopiva virkamieskortti.

Kansalainen voi luottaa viranhaltijan varmenteeseen kun:

- Viranomaiskortin rekisteröintivaihe suoritetaan luotettavasti. Kukin organisaatio viime kädessä vastaa virkamiehensä toiminnasta sähköisessä asioinnissa.
- Virkamiehen henkilökohtaisen varmenteen hallinta on toteutettu tietoturvallisesti ja virkamieskortin eri osapuolten tehtävät ja vastuut ovat selkeitä.
- Viranomaisen toiminta ei ole riippuvainen yksittäisen virkamiehen varmenteesta ja organisaatiovarmenne on eriytetty.

7.5 Rooli- eli attribuuttivarmenteet

Rooli- ja attribuuttivarmenteet mahdollistaisivat yksinkertaisempien ja käyttötavoiltaan monipuolisempien järjestelmien rakentamisen kuin nykyiset yksilökohtaiset varmenteet. Perusideana on varmentaa jokin varmenteen käyttäjään liittyvä attribuutti (eli ominaisuus) tai rooli, jolloin palvelujen käyttäjiä voidaan käsitellä ryhminä eikä yksilöinä. Roolivarmenteet voidaan toteuttaa joko attribuuttivarmenteina tai tavalliseen yksilövarmenteeseen liitettävänä sekundäärivarmenteena.

Roolivarmenteiden käyttöön tulevaisuudessa voidaan varautua toteuttamalla palvelujärjestelmissä jo ennakkoon oikeuksien hallintaa roolipohjaisesti. Esimerkiksi HST-korttia voidaan käyttää virkaan liittyvissä roolivarmenneratkaisuissa.

7.6 Vahvaan todentamiseen liittyvien riskien tunnistaminen ja varautuminen

Vahvan todentamisen käyttöönotto ei ole välttämätöntä useissa sähköisissä palveluissa. Siihen tulee ryhtyä vasta kun sen toimivuus palvelussa on etukäteen suunniteltu ja tietoturvallisuusasiantuntijoiden hyväksymä. On myös varmistettava, että käyttäjäkunnan aiheuttamat riskit on hallittu.

Jotta käytettävyys ja eheys olisivat hyvät, tulee vahvaa tunnistamista vaativissa palveluissa:

- Välttää pitkiä, hankalia palveluketjuja sekä pitkäaikaisiksi muodostuvia riippuvuuksia teknologisista ratkaisuista.
- Suunnitella omat ratkaisut siten, että minimoidaan tarve varmenteiden avulla jälkikäteen tapahtuviin tarkistuksiin.
- Varautua eri varmennepalveluiden statuksen muutoksiin.

Sähköisen allekirjoituksen suurimpia haasteita ovat mm. käytettävien menetelmien kirjo sekä varmenteiden vanhentuminen.

7.7 Laatuvarmenteet

Laatuvarmenne (hyväksytty varmenne; qualified certificate) on korkeat kansainväliset turvallisuusvaatimukset täyttävä varmenne. Laatuvarmenteille tulee eurooppalainen standardi vuonna 2001. Hallinnossa hyväksyttyjen laatuvarmenteiden toimittajista pidetään listaa valtiovarainministeriössä.

8 TIETOTURVALLISUUDEN VARMISTAMINEN POIKKEUSTILANTEISSA JA POIKKEUSOLOISSA

Normaalioloissa tehtävä hyvä tietoturvallisuustyö on pohja poikkeustilanteiden hoitamiseen. Tarjottavan sähköisen palvelun kriittisyys poikkeusoloissa on määriteltävä, koska sähköisistä palveluista osa palvelee jatkossakin vain normaaliolojen toimintaa.

Poikkeustilanteiden kannalta on tehtävä riskianalyysi palvelun kriittisyystason mukaan. Tämä voi useissa palveluissa tarkoittaa paluuta vaihtoehtoisiin menettelyihin ja kanaviin kuten telefax, puhelin, paperihakemus tai toinen palvelu. Nämä perinteiset tavat säilynevät käytössä vielä pitkään.

Ohjeet ja määräykset poikkeusoloista koskevat myös sähköisten palveluiden järjestelmiä. Varauduttaessa poikkeusoloihin on otettava huomioon:

- Sähköisen palveluiden järjestelmät ovat erityisen alttiita informaatiosodankäynnin hyökkäyksille.
- Sähköisten palveluiden tuottamiseen osallistuu usein enemmän osapuolia kuin perinteisissä palveluissa. On otettava huomioon, että palvelun toiminta saattaa häiriintyä, mikäli jonkin keskeisen apupalvelun tarjoajan toiminta on häiriintynyt. Myös toimittajan sijaintimaa saattaa vaikuttaa palveluiden saatavuuteen.
- Sähköisten palveluiden jakelukanavat saattavat olla herkkiä häiriöille.
- Erityisesti niissä sähköisten palveluiden järjestelmissä, jotka ovat tärkeitä apupalveluita tai joiden toimintaa poikkeusoloissa tullaan jatkamaan, on ohjelmistokomponenttien valinnalla keskeinen merkitys. Suositeltavia ovat sellaiset ohjelmistot ja tekniikat, joiden ei tiedetä sisältävän tietoturvallisuutta tarkoituksellisesti heikentäviä ominaisuuksia kuten ns. takaportteja.

Raja normaaliolojen ja poikkeusolojen toiminnan välillä on hämärtynyt johtuen virastojen toiminnan jopa täydellisestä riippuvuudesta tietojenkäsittelystä ja tietoverkoista. Sähköisten palveluiden osalta kyseessä on normaaliajan palveluiden varmistaminen tilanteissa, joihin virasto ei voi itse vaikuttaa.

Poikkeusolojen vaatimukset on myös sähköisiä palveluita ulkoistettaessa otettava huomioon.

Mahdolliset valmiustoiminnan vaatimukset on otettava huomioon jo tietojärjestelmän elinkaaren alussa. Tietojärjestelmät on tärkeysluokiteltava kolmeen luokkaan: aina toiminnassa, tarvittaessa supistettava ja voidaan korvata tai lopettaa poikkeusoloissa.

Mikäli palvelun tarjoajan tulee jatkaa palvelun tuottamista myös poikkeusoloissa samalla tavalla kuin normaalioloissa, on kiinnitettävä huomiota toimittajan kotimaisuusasteeseen, toimitilojen turvallisuuteen, käytettävän teknologian saatavuuteen, tietoliikenneratkaisuihin sekä henkilöstön pysyvyyteen ja saatavuuteen poikkeusoloissa.

LIITE 1: SÄÄDÖSPOHJA

Yleislakien yhteinen vaatimus on etukäteissuunnittelun ja hyvän tiedonhallinta- ja tietojenkäsittelytavan varmistaminen. Lakien yleisvelvoitteita on noudatettava myös silloin, kun sähköisen asioinnin tietoturvallisuuskysymyksiä suunnitellaan. Lainmukaisuutta arvioitaessa on otettava huomioon luonnollisesti myös erityislakeihin sisältyvät säännökset.

Säädöspohjaa on käsitelty tarkemmin mm. VAHTI:n ohjeessa 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje.

1 TÄRKEIMMÄT LAIT

- Laki sähköisestä asioinnista (1318/1999)
- Tulossa olevaan laki sähköisistä allekirjoituksista (tällä hetkellä lausuntokierroksella; implementoi EU:n direktiivin 1999/93/EY)
- Henkilötietolaki (523/1999)
- Laki viranomaisten toiminnan julkisuudesta (621/1999 ja 636/2000) sekä tähän liittyvä asetus (1030/1999)
- Arkistolaki (831/1994)
- Henkilökorttilaki (829/1999)
- Väestötietolain muutos (527/1997)
- Asetus valtionhallinnon tietohallinnosta (155/1988, 1401/1992)
- Hallintomenettelylaki (598/1982)

2 ERÄITÄ MUITA LAKEJA (ALAKOHTAISIA)

- Laki sosiaali- ja terveydenhuollon saumattoman palveluketjun ja sosiaaliturvakortin kokeilusta (ns. Lex Makropilotti; 801/2000)
- Laki sähköisestä asioinnissa yleisissä oikeusistuimissa (594/1993 ja 199/1998)
- Potilaan asemaa sosiaali- ja terveydenhuollossa koskevat säädökset (785/1992 muutoksineen; 812/2000)
- Kuntalaki (365/1995)
- Laki työvoimahallinnon tietojärjestelmistä (1993/1254)

3 TAUSTALLA OLEVIA LAKEJA

- Laki asiakirjan lähettämisestä (74/1954)
- Laki ja asetus tiedoksiannosta (232 ja 662/1966)
- Valmiuslaki (1080/1991)
- Perustuslain velvoite hyvään hallintoon
- Rikoslaki (28, 30, 34-37, 38§; rangaistukset)
- Telemarkkinalaki (396/1997)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
- Laki julkisen hallinnon asiakaspalvelujen järjestämisestä yhteisissä palveluyksiköissä (802/1993)
- KKO 1996:34 (viestin perillemenosta)

LIITE 2: KESKEISIÄ TIETOTURVALLISUUSTAVOITTEITA JA NIILLE ASETETTAVIA VAATIMUKSIA

Sähköisen asioinnin tietoturvan arvioinnissa voidaan hyödyntää oheista listaa. Palvelutyyppi vaikuttaa siihen, miten vaatimukset käytännössä toteutetaan.

1 Tehokas käyttäjätunnistus ja todennus

- Käyttöoikeudet myönnetään vain tunnistetuille asiakkaille, käyttäjille ja järjestelmän hallinnoinnista vastaaville.
- Käyttöoikeuksia ei anneta laajempina kuin on tarpeen.
- Suositellaan, että käyttöoikeuksien antaminen liitetään PKI-pohjaisesti korttiin yms. ”avaimeen”, mikäli riskit eivät ole vähäisiä.
- Käyttäjä on tarvittaessa todennettava. Todennus voidaan sitoa esimerkiksi toimikorttipohjaiseen vahvaan tunnistukseen, mutta sitä voidaan täydentää tai se voidaan korvata esim. salasanoilla tai biometrisillä tunnistusmenetelmillä.
- Järjestelmä hallinnasta vastaavat kontrolloivat käyttäjien oikeuksia ja näiden oikeuksien myöntämistä.
- Käyttöoikeudet kyetään peruuttamaan nopeasti ilman, että käyttäjää tai asiakasta tarvitsee informoida ja ilman järjestelmävastuullisen toimia.

2 Tehokkaasti järjestetty oikeuksien myöntäminen tunnistuksen pohjalta

- Käyttöoikeuden järjestelmään myönnetään vasta kun a) käyttäjä on tunnistettu b) hän ei käytä järjestelmää jollakin toisella tunnuksella (käyttörooleja voi olla useita) ja c) hänellä on oikeus järjestelmän käyttöön.

3 Kiistämättömyys ja kuittaus vastaanotosta

- Tapahtuman ja palveluun lähetetyn materiaalin yhteys lähettäjään voidaan kiistattomasti osoittaa.
- Asiakkaan saaman materiaalin tai tapahtuman yhteys järjestelmään on pystyttävä osoittamaan kiistattomasti.
- Palvelu vahvistaa kuittauksella, että se on vastaanottanut sinne lähetetyt tiedot tai tapahtuman.

4 Tietojen luotettava käsittely

- Sovelluksessa käsitellään huolellisesti sille välitettyjä tietoja (esim. luottokorttinumerot, henkilötiedot).
- Sovellus pystyy tuottamaan todennettavissa olevan aineiston kaikista sitoumuksista, jotka järjestelmä on tehnyt tai ollut mukana tekemässä.

5 Tietojen eheys

- Palvelu ryhtyy tarpeellisiin toimenpiteisiin suojellakseen sille lähetettyjä tietoja tahalliselta tai tahattomalta hyväksikäytöltä (tietojen muuttaminen, tuhoaminen tai lukeminen).
- Palvelu turvaa myös sellaiset palvelun käyttöön liittyvät tiedot ja ohjelmat, jotka on talletettu asiakaan hallinnassa olevaan laitteeseen, ja jotka ovat palvelun suoran kontrollin ulkopuolella.
- Palvelu suojaa siinä olevat tiedot ulkopuoliselta hyökkäykseltä (hakkerointi).

- Palvelu suojaa siinä olevat tiedot vahingoittumiselta ja väärältä tuhoamiselta. Tämä edellyttää mm. varmuuskopiointijärjestelmiä ja käytön hallintaa.

6 Palvelun käytettävyys

- Palvelu suojataan palvelunestohyökkäyksiltä ja muilta hyökkäyksiltä, joiden tarkoituksen on vahingoittaa palvelua.
- Palvelu suojataan laiterikkoja vastaan. Laitteistoissa on oltava riittävästi redundanssia eli ylimääräistä kapasiteettia, joka voidaan tarvittaessa ottaa käyttöön. Laitteiden huoltojärjestelyiden on oltava toimivia ja tarvittaessa on pystyttävä nopeisiin huolto- ja korjaustoimenpiteisiin.
- Palvelun jatkuvuus on turvattava tietojen ja laitteiden menetyksen, vahingoittumisen ja muiden vahinkojen varalta. Tämä vaatii kattavan jatkuvuussuunnitelman. Vahingot on ensisijaisesti pyrittävä torjumaan, mutta mikäli vaaraa ei voi eliminoida, on myös toipumistoimenpiteisiin panostettava.

7 Tietojen saatavuus

- Vahinkojen tai hyökkäysten johdosta vaurioituneet tai muuttuneet tiedot on kyettävä palauttamaan.
- Palvelun on kyettävä tarvittaessa antamaan tietoja, vaikka asiakas tai systeemin hallinnasta vastaava ei pysty kirjautumaan järjestelmään. Salasanojen unohtamisen tai sähköisen tunnistekortin katoamisen varalle on luotava toimintamalli. Näitä saatetaan tarvita myös silloin, kun tutkitaan järjestelmän väärinkäyttöä.

8 Tehokas seuranta ja valvonta

- Järjestelmän on kyettävä tarjoamaan seuranta suoritetuista toimenpiteistä ja palvelutapahtumista (lokitiedot). Näitä lokeja saatetaan tarvita mm. kiistatapauksissa.
- Järjestelmästä on saatava reaaliaikaista valvontatietoa ja hälytyksiä. Hälytysten on oltava automatisoitu siten, että ne välittyvät sellaiselle henkilölle, joka kykenee päättämään antaako hälytys aihetta toimenpiteisiin, ja tarvittaessa välittömästi käynnistämään nämä toimenpiteet.
- Seurannan ja hälytyksen aiheuttamien toimien on oltava ennalta suunniteltuja ja testattuja.

9 Salausratkaisujen käyttö

- Käytettävät tietoliikenteen ja tietoaineistojen salausratkaisut ovat riittävän luotettavia ja niiden käyttö hallitaan. Noudatettavat salausperiaatteet ovat selkeitä.
- Salaukseen käytettävät menetelmät ja välineet ovat turvalliseksi tunnettuja ja yleisesti käytössä.

LIITE 3: SÄHKÖISEN PALVELUN TURVALLISUUSANALYYSI

Turvallisuusanalyysi voidaan laatia seuraavasti:

1. Tunnistetaan kohteet, joita riskit saattavat uhata
   - Henkilötiedot ja käyttäjien tunnistustiedot
   - Yritysten tiedot ja muut palvelun tarjoajan hallussa olevat tiedot
   - Sähköiset palvelut itsessään
   - Taloudellista arvoa omaavat asiat
   - Palvelimen ohjelmistot ja palvelinlaitteet
   - Verkkosivujen sisältö ja verkkoon tarkoitetut ohjelmat (esim. Java-appletit)
   - Asiakkaan ohjelmat, laitteet ja niissä olevat tiedot
2. Tunnistetaan, ketkä saattaisivat uhata palvelun tietoturvallisuutta
   - Palvelun sisäiset käyttäjät, kehittäjät, ylläpitäjät ja asiakaskäyttäjät, joilla on oikeus käyttöön
   - Palvelun tuottamiseen osallistuvat henkilöt ja organisaatiot
   - Muut (julkisen ja yksityisen sektorin) henkilöt ja organisaatiot, joilla on käyttövaltuuksia palvelutuotannon järjestelmiin
   - Vihamieliset ulkopuoliset tahot, rikolliset, rikollis- ja terroristijärjestöt
   - Tutkimus- ja tiedonhankintaa tekevät yritykset ja organisaatiot
3. Tunnistetaan, miten sähköisen palvelun tietoturvallisuutta saatetaan uhata
   - Luvaton tunkeutuminen tietojärjestelmiin (ns. hakkerointi)
   - Vahingolliset ohjelmat, kuten virukset
   - Palvelunestohyökkäykset ja yksittäistä palvelutapahtumaan kohdistuva hyökkäys
   - Palveluntarjoajan henkilökunnan käyttäminen apuna
   - Väärän sähköisen identiteetin avulla tapahtuvat rikkeet ja väärennösrikokset

   Lisäksi on varauduttava tyypillisesti jo perinteisissä tietojärjestelmien käytössä esiintyviin uhkiin:
   - Asiakkaiden virheistä johtuvat vahingot, kuten tietojen tahaton paljastuminen tai käyttöoikeuksien huolimaton käsittely
   - Palvelun tarjoajan henkilökunnan vahingossa tekemät virheet
   - Ohjelmisto- tai laitevirheistä johtuvat vahingot
   - Fyysiset onnettomuudet
4. Edellisten kohtien pohjalta laaditaan palvelun tietoturvallisuustavoitteet, joiden toteuttaminen takaa halutun tietoturvallisuustason saavuttamisen.
5. Asetetaan teknisiä tietoturvallisuusvaatimuksia, jotka järjestelmän on täytettävä, jotta se olisi tietoturvallinen.

LIITE 4: SÄHKÖISESTÄ PALVELUSTA KÄYTTÖTILANTEESSA LADATTAVAN KOODIN TIETOTURVALLISUUS

1 TAUSTA

Ladattava koodi tarkoittaa tässä sovellusosia tai sovelluksia, joita välitetään tietoverkon välityksellä asiakkaan laitteeseen (työasema, PDA-laite, WAP-puhelin tms.) suoritusta varten.

Palvelusta käyttötilanteessa ladattavan koodin käyttö (”ladattava koodi”) sisältää eri tasoisia tietoturvallisuusuhkia sekä työasema- että palvelinpäässä. Koodin käytöllä saavutettavia mahdollisuuksia ei tule kokonaan jättää käyttämättä, vaan on soveltamiskohtaisesti tunnistettava edellytettävät vaatimukset ja tehtävä valinnat tämän perusteella. Kyse on jatkuvasti kehittyvästä alueesta, jossa käytännön ratkaisuja tehtäessä tulee aina selvittää ajantasainen tilanne.

Tässä esitettäviä vaatimuksia voidaan kaupallisissa palveluissa harkita lievennettäviksi, jos sovellusalueella on kyse selkeistä, rajatuista uhkista.

Ladattavan koodin luokittelu ja ominaisuudet perustuvat tilanteeseen keväällä 2001.

2 LADATTAVAN KOODIN KÄYTTÖ TUNNISTETTUJEN RISKIEN PERUSTEELLA

2.1 Luokka 1: Soveltamisessa on merkittäviä riskejä, joista vain osaa voidaan hallita

1. Kyseessä on runsaasti toiminnallisuutta mahdollistava ladattava koodi, joka voi aiheuttaa tietoturvallisuusriskejä työasemissa tai palvelimissa. Riskit tunnetaan, mutta koodin suoritusvaiheessa niihin ei voida juurikaan vaikuttaa, joten asiakkaan on päätettävä suoritetaanko koodi sellaisenaan vai jätetäänkö se suorittamatta.
2. Soveltaminen voi aiheuttaa riskejä organisaation palveluihin. Joissakin toteutuksissa tähän voidaan kuitenkin vaikuttaa esim. koodin allekirjoituksella, jolloin estetään allekirjoittamattoman koodin suoritus ja suoritetaan vain luotetun tahon allekirjoittama koodi.
3. Koodi voidaan suorittaa turvallisesti vain, jos se on hyväksytyn varmentajan antaman varmenteen avulla allekirjoitettu ja allekirjoittaja on luotettu.
4. Koodi, joka ei täytä kohdan 3 vaatimuksia voidaan hyväksyä suoritettavaksi vain, mikäli tämä on toiminnan kannalta välttämätöntä ja koodin käyttämiselle on saatu tietoturvallisuudesta vastaavalta taholta ja johdolta erillinen hyväksyntä.
5. Mikäli tämän luokan koodia hyväksytään suoritettavaksi kohtien 3 ja 4 perusteella jossain laitteessa tai ohjelmassa, on tietoturvallisuusriskit arvioitava paitsi kyseisten laitteiden tai ohjelmistojen kannalta, myös koko muun laite- ja palveluympäristön kannalta. Kokonaisuuteen sisältyvät myös järjestelmät, joilla on liittymiä siihen laite- ja palveluympäristöön, jossa tämän luokan koodin suorittaminen sallitaan.

Luokkaan 1 on tunnistettu kuuluviksi seuraavia teknologioita, kun ne siirretään palvelun käyttötilanteessa palvelimelta asiakkaan koneelle suoritettavaksi:

- ActiveX (ei kuitenkaan, jos se on luotettavasti allekirjoitettua)
- Windows Scripting
- Unix Shell skriptit
- DOS komentojonot

2.2 Luokka 2: Soveltamisessa on hallittavissa oleva kohtuullinen riski

1. Kyseessä on runsaasti toiminnallisuutta mahdollistava mobiili koodi, joka voi aiheuttaa tietoturvallisuusriskejä. Riskit tunnetaan, ja niihin voidaan koodin suoritusvaiheessa varautua yksityiskohtaisin turvatoimin. Nämä toimet tulee pitää ajan tasalla jatkuvalla.
2. Koodi voi aiheuttaa riskejä organisaation palveluihin tai toimintoihin. Voidaan kuitenkin arvioida, että hyötyihin nähden riskit ovat kohtuulliset, ja että riskit voidaan hallita tietoturvallisuusmenettelyiden avulla.
3. Koodia voidaan käyttää, kun se saadaan luotettavasta lähteestä suojatun tietoliikennekanavan kautta. Lisäksi voidaan käyttää kaikkea muuta allekirjoittamatonta koodia, joka ei voi aiheuttaa muutoksia paikallisessa ympäristössä.
4. Työasema pyritään konfiguroimaan (mm. ohjeistamalla) siten, että koodi suoritetaan vasta asiakkaalta saadun hyväksynnän jälkeen.
5. Uudet järjestelmäkehityshankkeet, joissa tähdätään tämän luokan mukaisen koodin hyödyntämiseen, on erikseen arvioitava kokonaisuutena tietoturvallisuusriskien hallitsemiseksi.

Luokkaan 2 on tunnistettu kuuluviksi seuraavia teknologioita:

- Java-appletit ja muu siirrettävä Java-koodi
- VisualBasic for Applications (VBA)
- Lotus Script ja PerfectScript
- Postscript

2.3 Luokka 3: Soveltamisessa on vähäinen riski

1. Kyseessä on vain rajattua toiminnallisuutta mahdollistava ladattava koodi, joka ei voi aiheuttaa muutoksia paikallisessa työasemassa tai verkkoympäristössä. Koodilla voi olla tietoturvallisuusriskejä sisältävä historia, mutta riskit voidaan hallita.
2. Koodi ei voi aiheuttaa riskejä organisaation palveluihin tai toimintoihin. Huolellisella toiminnalla voidaan nähdä hyötyjen olevan merkittävästi suuremmat kuin riskit.
3. Voidaan yleisesti hyväksyä koodin käyttö palveluissa.
4. Ennen tämän luokan mukaisen koodin hyödyntämistä on arvioitava tietoturvallisuusriskit ja tehtävä suunnitelma niiden hallitsemiseksi.

Luokkaan 3 on tunnistettu kuuluviksi seuraavia teknologioita:

- JavaScript variaatioineen
- VBScript
- PDF-muotoiset tiedostot
- Shockwawe ja Flash
- ActiveX (luotettavasti allekirjoitettua)

Esimerkki: Ladattava ja suorituskelpoinen koodi sähköpostissa. 1) Kaiken ladattavan koodin suorittaminen sähköpostissa ja sen liitteissä tulee ohjeistaa estettäväksi asiakaspäässä. 2) Asiakaspäässä tiedostoliitteitten avaaminen tulee konfiguroida siten, että asiakas saa vähintään mahdollisuuden tehdä itse päätöksen liitteen avaamisesta tapauskohtaisesti, mikäli on olemassa mahdollisuus, että liite sisältää ladattavaa koodia.

2.4 Luokka 4: Soveltaminen sisältää ratkaisuja, joiden riskejä ei osata arvioida

1. Kyseessä on uudenlaista toiminnallisuutta mahdollistava koodi, jonka tietoturvallisuusriskejä ei riittävästi tunneta.
2. Koodin lataus ja suoritus asiakaspäässä tulee oletusarvoisesti estää, eikä sitä tule käyttää missään normaaleissa palveluissa.
3. Koodin käyttöönottoa voidaan harkita, mikäli koodista on saatavissa riittävästi tietoa, jotta sen tietoturvallisuusominaisuudet voidaan selvittää. Tietoturvallisuusominaisuuksien selvitykseen ja testaukseen on varattava aikaa vähintään 3 kuukautta.
4. Koodia ei tule hyödyntää sovelluksissa, ennen kuin se on ollut kaupallisesti saatavilla kohtuullisen ajan.

Luokkaan 4 on tunnistettu kuuluviksi seuraavia teknologioita:

- WPKI-koodin käyttö (Langattomassa ympäristössä ladattava PKI-koodi)
- Eräitä muita ovat WML, SyncML

3 OHJEEN ULKOPUOLISET ASIAT JA RAJOITUKSET

Tämä tarkastelu ei koske mm. seuraavia teknologioita, joita ei luokitella ladattavaksi koodiksi:

- XML
- VRML ja sen avulla tehtyihin ympäristöihin liitetyt appletit ja skriptit (mutta rajoitukset koskevat kuitenkin VRML:ään liittyvää Java- tai JavaScript-koodia)
- QuickTime, Streaming-protokollat (musiikki, video jne.)

Tarkastelu ei koske seuraavia sovellusten käyttötilanteita:

- WWW-sivuilla olevat skriptit ja appletit, jotka suoritetaan palvelinympäristössä: Java servletit, Java Server Pages, Java RMI, Java Jini, CGI, Active Server Pages, CFML, PHP, SSI, server-side JavaScript, server-side LotusScript
- Paikalliset sovellukset ja komentojonot: suorituskelpoiset ohjelmat, komentotulkkiskriptit, eräjonot, Windows Scripting Host (WSH), Perl-skriptit
- Käyttäjän itsensä aktivoimat ohjelmistojen eräajot, päivitykset, itsepurkautuva pakattu koodi: Windows Update, Linux, Netscape Plug-Ins.
- Hajautetut olioteknologiasovellusympäristöt: CORBA, DCOM

LIITE 5: AUDITOINNIN TARKISTUSLISTA

Auditoinnissa tulee kiinnittää erityistä huomiota seuraaviin kohtiin:

- Palvelu: käytettävyys, vikasietoisuus, vaatimukset asiakkaalle
- Tunnistaminen: ovatko tunnistusmenetelmät riittävän vahvoja ja toimivia
- Palomuuri: konfigurointi, ohjelmiston ajantasaisuus ja palomuurista vastaavan henkilön ammattitaito, varakonejärjestelyt
- Verkon ja palvelun valvonta: seurannan reaaliaikaisuus, reagointi ongelmatilanteisiin, hälytysten seuranta ja dokumentointi, ohjelmien ajantasaisuus
- Lokitietojen sisältö, käsittely ja arkistointi
- Henkilöstö ja tietoturvallisuus: koulutuksen laatu ja ajantasaisuus, yleinen ammattitaito ja asenne, johdon suhtautuminen
- Tietokannat ja liittymät: järjestelmien välisten liittymien hallinta, tietokantojen suojaustapa
- Käytettävyys: varakonejärjestelyt, varmuuskopiointi ja näiden harjoittelu, laitteiden kapasiteetti ja kahdennukset, toipumissuunnitelma ja varautuminen ongelmatilanteisiin sekä näiden harjoittelu
- Sopimukset ja kumppanit: ovatko sopimukset selkeitä ja ovatko niissä määritellyt vastuut selkeitä ja molempien tiedossa, ja onko kumppanit auditoitu luotettavasti

LIITE 6: TIETOTURVALLISUUS SÄHKÖISTEN PALVELUIDEN ELINKAAREN AIKANA

Elinkaariajattelussa tarkastellaan tietoturvallisuuden kannalta keskeisiä asioita alkaen palvelun esitutkimuksesta ja päättyen palvelun lopettamiseen. Lähestymistavassa korostuu kaksi asiaa:

- Tietoturvallisuuden on oltava mukana palvelun kehittämisen alusta alkaen.
- Tietoturvallisuus on palveluun kiinteästi kuuluva asia. Se ei saa olla irrallinen osuus, joka liitetään mukaan elinkaaren ensimmäisten vaiheiden jälkeen.

1 TOTEUTUSPROJEKTI

1.1 Esitutkimus

- Onko sähköinen palvelu säädösten ja ohjeiden mukainen? Onko palvelu organisaation strategian mukainen?
- Mitkä ovat palvelun jäljitettävyys- ja kiistämättömyysvaatimukset sekä palvelun tarjoajan että asiakkaan kannalta?
- Onko karkea riskianalyysi tehty? Onko organisaation tietotekniikka-arkkitehtuurin tietoturvallinen? Puuttuko siitä palvelun toteutuksen kannalta keskeisiä komponentteja?
- Mitä odotuksia palvelun asiakkailla tai muilla sidosryhmillä on palvelun suhteen? Mitä sellaisia seikkoja on, jotka vaikuttavat mielikuvaan palvelun tietoturvallisuudesta?
- Ovatko tietoturvallisuuden perustamis- ja ylläpitokustannukset selvitetty? Onko organisaatiossa resursseja ja tietotaitoa toteuttaa ja valvoa sähköisten palveluiden toteutusta ja tuotantovaiheessa olevaa palvelua?

1.2 Määrittely

- Onko riskianalyysiä tarkennettu? Onko palvelun asiakas- ja tapahtumavolyymit arvioitu?
- Ymmärretäänkö oikein sähköisen palvelun suhde muihin palveluihin? Miten toteutetaan sähköisen palvelun vaatimien järjestelmien eriyttäminen muista järjestelmistä?
- Onko palveluketjuun osallistuvien osapuolten vastuurajat selvitetty ja tästä tiedotettu asiakkaille ja muille sidosryhmille?
- Onko tietoturvallisuusvastuulliset nimetty? Onko laadittu alustava toimintasuunnitelma tietoturvallisuuden pettämisen varalle?
- Onko tietoturvallisuusnäkökohdat huomioitu toteutuksen vaatiman tekniikan valinnassa? Millaista laitekapasiteettia ja muita ratkaisuja haluttu käytettävyystaso edellyttää? Toteutetaanko sellaisia palveluita, joiden tietoturvallisuuden implementointi on hankalaa?
- Onko selvitetty palvelun vaatiman salauksen ja tunnistamisen taso?

1.3 Suunnittelu

- Onko tietoturvallisuussuunnitelmat dokumentoitu riittävästi?
- Onko selvitetty asiat, joiden tietoturvallisuus pitää arvioida ennen palvelun toteutusta?
- Mitä komponentteja tai komponenttiarkkitehtuureja voidaan käyttää? Mitä tietoturvallisuusongelmia komponentteihin saattaa liittyä? Miten käyttöliittymän lisäosia voidaan tietoturvallisesti käyttää? Hallitaanko toteutusvälineiden tietoturvallisuuskysymykset?
- Onko kokonaisuuden tietoturvallisuus riittävästi suunniteltu? Onko liittymät perusjärjestelmiin suunniteltu hyvin?

- Onko asiakkaiden osaamistaso ja ohjelmistovalinnat riittävästi huomioitu?
- Onko tietoturvallisuuden testaus suunniteltu? Onko kumppanit valittu oikein ja ovatko vastuut selvät? Onko sopimukset laadittu selkeiksi ja tietoturvallisuuden huomioiviksi?

1.4 Toteutus

- Onko tietoturvallisuuden testaus toteutettu?
- Onko käytössä uusin tieto toteutusvälineiden tietoturvallisuudesta?

1.5 Käyttöönotto

- Onko tietoturvallisuutta testattu riittävästi? Pystytäänkö vakuuttamaan asiakkaat tietoturvallisuuden tasosta?
- Poikkeaako tuotantoympäristö olennaisesti testiympäristöstä? Kyetäänkö tietoturvallisuuden "tuotantotaso" saamaan aikaan heti?
- Ollaanko varauduttu siihen, että uuden palvelun tietoturvaa vastaan saatetaan tietoisesti hyökätä heti sen tultua tuotantokäyttöön?

2 PALVELUN TUOTANTO

2.1 Tuotantovaihe

- Miten on varauduttu toiminnan rutinoitumiseen "kun kaikki menee hyvin"? Harjoitellaanko toimia tietoturvallisuuden rikkoontumisen varalle?
- Onko palvelun uudenlainen ajallinen ja maantieteellinen saatavuus huomioitu henkilöstö- ja muissa järjestelyissä? Onko selvitetty, mitkä ovat järjestelyt tärkeä apupalvelun toiminnan häiriintyessä?
- Pidetäänkö ajan tasalla tietoa teknisten komponenttien tietoturvallisuudesta? Miten on järjestetty ympäristön muutosten seuranta?

2.2 Palvelun lopettaminen

- Onko palvelun lopettaminen suunniteltu riittävästi? Miten varmistutaan siitä, ettei tietoturvallisuuden ylläpitotoimia lopeteta ennenaikaisesti?
- Huolehditaanko tietoaineistojen arkistoinnista ja hävittämisestä asianmukaisesti? Miten varmistetaan tiedotus sidosryhmiin?

3 ELINKAAREEN LIITTYVIÄ ERILAISIA TOIMIA

- Ymmärretäänkö muutosten laajuus ja niiden sidokset riittävästi?
- Miten on varauduttu uusien työntekijöiden, asiakkaiden ja partnereiden mukaan tuomiin tietoturvallisuusongelmiin? Sopivatko uudet tekniset ratkaisut ja palvelut kokonaisuuteen? Onko niiden tietoturvallisuus testattu?
- Toimiiko tiedotus ja yhteistoiminta palvelun muuttuessa? Aiheuttaako palvelun kehittäminen muutoksia vastuissa tai sopimuksissa? Onko toimittajan tietoturvallisuus arvioitu? Ovatko toimittajanvaihdoksen tietoturvallisuuskysymykset selvillä?
- Onko tietoturvallisuuden kehittäminen ja testaus hyvin hoidettu ja ajan tasalla? Kuka vastaa muutoksista? Onko testausaineiston ja testausmenettelyjen tietoturvallisuus hyvin hoidettu?
- Tehdäänkö auditointeja riittävän usein ja onko ne dokumentoitu?

LIITE 7: TARJOUSTYÖSKENTELY JA SOPIMINEN

Tämä tarkistuslista sisältää tarjouspyyntö-, tarjous- ja sopimisvaiheeseen liittyviä edellytyksiä sähköisten palveluiden kehityshankkeissa. Ohjeita on noudatettava valikoiden ja soveltaen. Tässä ei esitetä palvelutuotantoon tai ulkoistukseen liittyviä näkökohtia.

1 TARJOUSPYYNTÖVAIHE

- Tilaajan on varattava käyttöönsä tietoturvallisuusosaamista jo tarjouspyynnön tekemiseen
- Tilaajan on selvitettävä, että kyseessä on toiminto, jota voi säädösten ja ohjeitten perusteella tarjota sähköisenä palveluna. Tähän on tarvittaessa käytettävä ulkopuolisia asiantuntijoita joko julkisen hallinnon sisältä tai yrityksistä.

1.1 Tarjouspyyntöön liitettävä materiaali

- Yleiset valtiohallinnon tietoturvallisuusohjeet (luettelo, viittaukset), omat tietoturvallisuusvaatimukset, -ohjeistot ja tietoturvallisuuspolitiikka.
- Kehitettävän palvelun tietoturvallisuusvaatimukset, ajantasaiset ja mahdollisimman kattavat kuvaukset palveluun liittyvistä prosesseista ja tietotekniikasta sekä palveluun liittyvät säädökset ja ohjeet.
- Tuotantoympäristön kuvaus ja yleiset vaatimukset. Tilaajan ja toimittajan välinen työnjako.

1.2 Tarjoajalle asetettavia vaatimuksia

- Referenssiasiakkaat, tietoturvallisuuspolitiikka ja valtionhallinnon tietoturvallisuusohjeistojen tuntemus.
- Toimittajan tuntemus ja kuvaukset järjestelmään liittyvien valmiiden komponenttien ja osapuolten tietoturvallisuusominaisuuksista, projektiin nimettyjen henkilöiden osaamisprofiilit ja käytettävyys.
- Kuvaus, miten palvelun tietoturvallisuus aiotaan ratkaista, ml. järjestelyt yleisimpien ongelmatilanteiden varalle.
- Kuvaus muista sitoumuksista kolmansiin osapuoliin palvelun tuotannossa.
- Viraston omistusoikeudet ja oikeudet tuotetun ratkaisun jatkokehitykseen, toimittajan takuut palveluiden saatavuudesta sekä toimittajan hyväksymismenettely ja sitoutuminen sanktioihin.

2 TARJOUSVAIHE

Tarjousvaiheessa korostetaan tietoturvallisuuteen liittyvien vaatimusten täyttymistä ehdoksi jatkokäsittelyyn pääsylle. Dokumentoidaan huolellisesti oma tarjousarviointiprosessi. Tarjousarviointiin otetaan mukaan myös tilaajan tietoturvallisuuden osaajia.

Palveluiden kehityksessä käytettävien toimittajien valintaan on kiinnitettävä erityistä huomiota. Tarjousten laatua parannetaan liittämällä tarjouspyyntöön toimittajakandidaattien arvioinnin kriteerit, erityisesti toimittajan osaamisen, heidän yhteistyöverkoston ja tietoturvallisuuden osalta.

2.1 Tarjouksen arvioinnin kriteeristöä

Tarjouksissa vaadittavia arvioinnin peruskriteerejä ovat:

- Toimittajan tietoturvallisuuspolitiikka, säädösten ja valtionhallinnon ohjeiden tuntemus.
- Ratkaisun tietoturvallisuustaso, komponenttien tietoturvallisuusominaisuudet, yleisyys ja arvio niiden jatkuvuudesta.

- Tarjouspyynnössä esitettävät saatavuuden, käytettävyyden ja eheyden vaatimukset.
- Tilaajan oikeus auditoida tulokset ja niiden tietoturvallisuus, sekä toimittajan sitoutuminen auditoinnissa mahdollisesti ilmeneviin muutostarpeisiin.

2.2 Palvelutoimittajan arviointi

Tarkasteltavia asioita ovat:

- Referenssit yleensä ja kokemukset vastaavista kohteista. Toimittajan kumppanuudet ja yhteistyöverkosto.
- Tarjotun kokonaisuuden ja sen osien sopivuus toimittajan kehittymisvisioon.
- Toimittajan laatuohjelma ja toimittajan tarjoaman henkilöstön laadun varmistaminen. Toimittajan välineosaaminen ja ohjelmistokehityksen välineiden yhteensopivuus organisaation käyttämiin kehitystyökaluihin.
- Toimittajan palvelumalli ja joustavuus jatkokehitystä ajatellen, tarvittaessa toimittajan 7x24 toimintamallin arviointi.

3 SOPIMINEN

3.1 Vaatimuksia virastolle

Tilaajan on huolehdittava, että a) määritykset tehdään huolella b) toimitusta valvotaan:

- Tilaajan on annettava riittävä tieto toimittajalle kohteeseen liittyvästä määräyksistä.
- Tilaajan on tehtävä suunnitellusta palvelusta tietoturvallisuusanalyysi, tarvittavat toimenpiteet ja ohjeet.
- On sovittava yhteistoiminnan periaatteista ja sanktiosta toimittajan kanssa.
- On varmistettava mahdollisuuden jatkokehitykseen ja toimittajan vaihtoon. Tämä sisältää käytettyjen ratkaisujen omistusoikeuden, dokumentoinnin ja yleisen tunnettuuden.
- On velvoitettava toimittaja testaamaan ratkaisun toimivuus tuotantoympäristössä.

3.2 Vaatimuksia tarjoajalle

Tarjoajan suunnitelmista tulee ilmetä, että toimittaja

- on tutustunut tietoturvallisuusvaatimuksiin ja sitoutuu noudattamaan niitä.
- kuvaa oman tietoturvallisuuspolitiikkansa, noudattamansa tietoturvallisuusohjeet ja projektiin osallistuvat henkilöt osaamisprofiileineen, sekä nimeää projektiin tietoturvallisuusvastuullisen henkilön.
- esittää takuut alihankkijoiden ja kolmansien osapuolten osuuksista. Hyväksyy kolmansien osapuolten tekemät auditoinnit ja niiden perustella toimittajan vastuulle tulevat toimenpiteet.
- sitoutuu dokumentoimaan tietoturvallisuuden toteutukseen ja suunnittelemaan audit trail -menettelyt eli kirjausketjut.
- panostaa kokonaisuuden testaukseen ja käyttöönottovaiheeseen.

LIITE 8: LÄHTEITÄ

1 VAHTI:N OHJEET JA SUOSITUKSET

- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/vahti12001.pdf)
- Tietokoneviruksilta ja muista haittaohjelmilta suojautumisen yleisohje, VAHTI 4/2000 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/vahti42000.pdf)
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/vahti32000.pdf)
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvaohje, VAHTI 2/2000 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/tiluraportti.pdf)
- Valtionhallinnon tietoturvallisuuskäsitteistö, VAHTI 1/2000 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/sanasto/sisallys.htm)
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, VAHTI 2/1999 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/vahti21999.pdf)
- Valtion etätyön tietoturvallisuussuositus, VAHTI 1/1999 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/etatyo.htm)
- Valtion Internetin käyttö- ja tietoturvallisuussuositus, VAHTI 1/1998 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/suositus.htm)
- Sähköpostin ja lokitiedostojen käsittely, VAHTI 3/1997 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/vahti397.pdf)

2 MUUT KOTIMAISET LÄHTEET

- Tarpeettomaksi tulleiden tietoaineistojen hävittäminen, VM, Hallinnon kehittämisosasto, 2000 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/21012000.pdf)
- Tietoturvallisuuden tulosohjaus ja kehittämisvälineet, Valtionhallinnon tietoturvallisuuden johtoryhmä, 1997 (http://www.vn.fi/vn/vm/kehittaminen/tietoturvallisuus/vahti/tulosohj.htm)
- Kohti verkkoasiointia, Vapsu, 1999 (http://www.intermin.fi/suom/vapsu/opas.htm)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, 1999 (http://www.vn.fi/vn/suomi/vnviikko/99vv45.htm#Liite)
- Virkamiesten asiointikortti, Sisäasianministeriö, 2000 (ISBN 951-734-366-3; http://www.intermin.fi/julkaisut/virkakortti.pdf).
- Kohti verkkoasiointia ja e-hallintoa, Sisäasianministeriö ja JUNA, 2001 (http://www.intermin.fi/suom/juna/julkaisut/verkkoasiointi_opas.pdf)
- Henkilön sähköinen tunnistaminen, VRK, 2000 (http://www.vaestorekisterikeskus.fi/hstetusivu2.htm)
- Varmennepalvelut ja sähköinen asiointi hallinnossa, VRK, (http://www.sahkoinenhenkilokortti.fi/download/dokumentit/varmpalv/Vtekstiosa.pdf)
- Verkkopalvelujen tekniset määritykset, VETURI, 1999 (http://www.intermin.fi/suom/veturi/tekninenraportti.html)
- Valmiudet verkkopalveluun - Veturi-projektin kyselytutkimus paikallishallinnon työntekijöille, 2000 (ISBN 951-734-364-7; http://www.intermin.fi/suom/julkaisut/veturi.pdf)

– WWW:n käyttö julkishallinnossa (JHS 129), 2000
(http://www.intermin.fi/juhta/suositukset/jhs129s.htm)

3 ULKOMAISET LÄHTEET

– Framework for Information Age Government - Security
(www.e-envoy.gov.uk/egovernment/iagc/guidelines/security/security.htm), Central IT Unit, (CITU), Iso-Britannia, 2000
– E-Government Strategy Framework Policy and Guidelines. Web Security, Draft
(www.e-envoy.gov.uk/egovernment/iagc/guidelines/webprofiles/webprof.htm), Central IT Unit, (CITU), Iso-Britannia, 2000
– Elektroniska signaturer och elekronisk identifiering för myndigheters e-tjänster, Statskontoret 2000:40, ISBN 91-7220-437-0
– The 24/7 Agency. Criteria for 24/7 Agecies in the Networked Public Administration, Statskonturet 2000:41, ISBN 91-7220-438-9
– Electronic Tax Administration – A Strategy for Growth, Internal Revenue Service (IRS), Publication 3187, Catalog Number 26634M, 2000
– Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology, United States General Accounting Office (GAO), GAO-01-277 Federal PKI Initiatives, 2001
– ECMA Protection Profile E-COFC Public Business Class, ECMA, ECMA Technical Report TR/78, 1999
– Policy Guidance for use of Mobile Code Technologies in Department of Defence (DoD) Information Systems, Department of Defence, 2000
– Securing Electronic Government, CIO Council, Security, Privacy and Critical Infrastracture Commitee, 2001
– EU:n sähköisen allekirjoituksen direktiivi 1999/93/EY
(http://www.europa.eu.int/eur-lex/fi/lif/dat/1999/fi_399L0093.html)