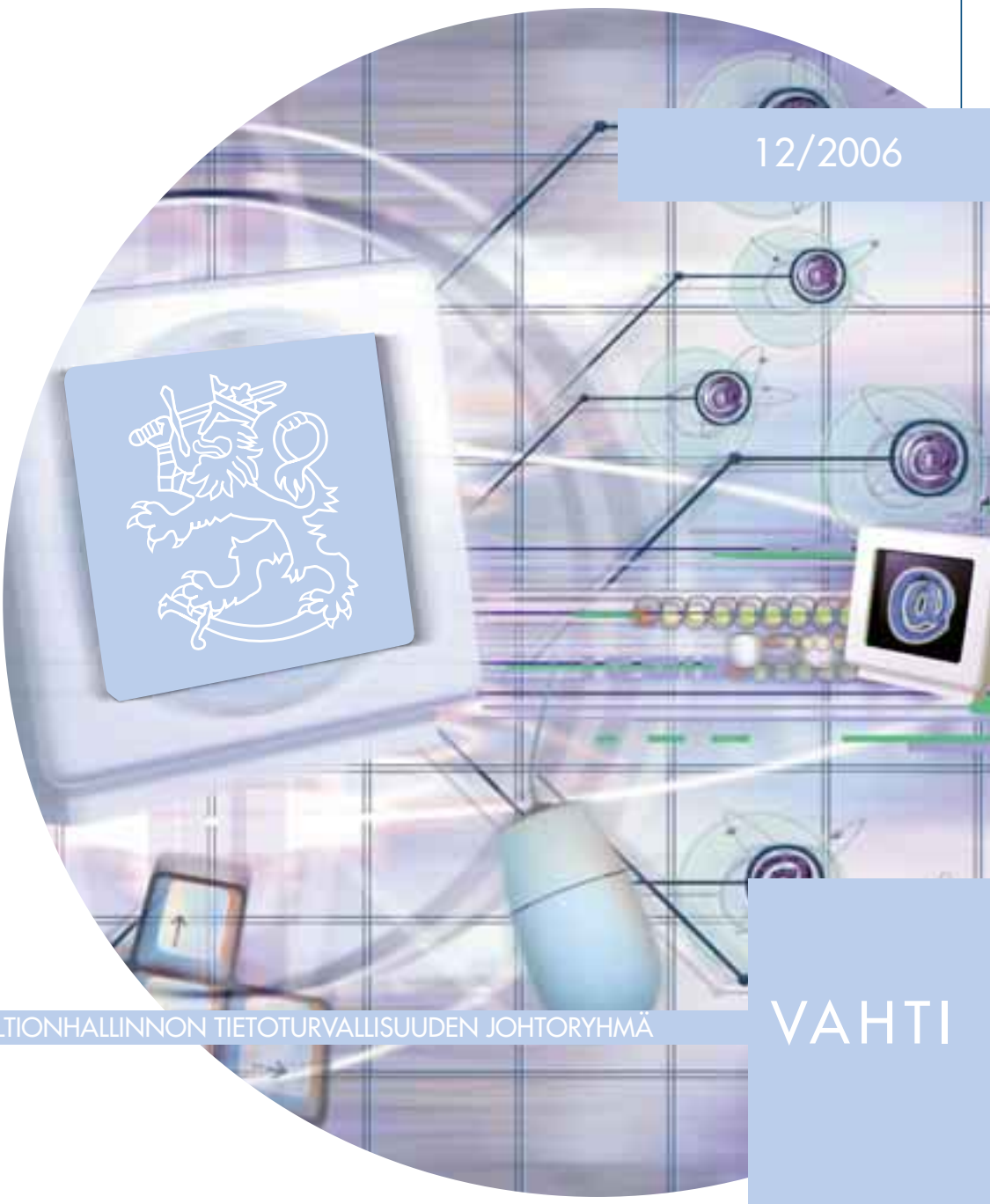
VALTIOVARAINMINISTERIÖ

TUNNISTAMINEN JULKISHALLINNON VERKKOPALVELUISSA



12/2006

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

TUNNISTAMINEN JULKISHALLINNON VERKKOPALVELUISSA

12/2006

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
asiakaspalvelu.prima@edita.fi
Puh. (09) 160 33287

ISSN 1455-2566
ISBN 951-804-668-9 (nid.)
ISBN 951-804-669-7 (pdf)

Edita Prima Oy
HELSINKI 2006

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 40/01/2006

OHJE
4.12.2006

Ministeriöille, virastoille ja laitoksille

TUNNISTAMINEN JULKISHALLINNON VERKKOPALVELUISSA

Oheisen hallinnon verkkopalveluja koskevan ohjeen (jäljempänä ohje) tavoitteena on tukea hallinnon organisaatioita laadukkaiden ja tietoturvallisten verkkopalvelujen kehittämisessä ja ylläpitämisessä. Ohje on tarkoitettu hallinnon organisaatioiden johdolle, tietohallinnolle, tietoturvavastaaville sekä verkkopalvelujen suunnittelijoille.

Ohje on laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI ohjauksessa ja alaisuudessa osana valtion tietoturvallisuuden kehitysohjelmaa (VAHTI-julkaisu 1/2004) ja se korvaa VM:n aiemmin antaman ohjeen tunnistamisesta valtionhallinnon verkkopalveluissa (VM 6/01/2003). Ohje on viimeistelty valtionhallinnon ja kunnallishallinnon yhteistyössä laajan lausuntokierroksen pohjalta. Ohje soveltuu koko julkishallinnon käyttöön.

Perustettaessa verkkopalvelua arvioidaan toimintaprosessien pohjalta ensimmäiseksi, tarvitaanko sen käyttäjiltä ylipäänsä tunnistamista. Kansalaisille suunnatuissa verkkopalveluissa käyttäjän tunnistamistarve vaihtelee palvelutyypin mukaan. Tiedottamispalveluissa käyttäjää ei tule tunnistaa.

Vahvaa tunnistamista tarvitaan luottamuksellisessa vuorovaikutteisissa asiointipalveluissa sekä tietojärjestelmien välisessä tietojenvaihdossa. Tunnistamisessa tulee ensisijaisesti käyttää valtionhallinnossa hyväksyttäviä vahvoja tunnistamismenetelmiä tukevia yleisiä tunnistamispalveluja. Luotettavuudeltaan parhaita tunnistamisratkaisuja ovat laatuvarmenteisiin perustuvat ratkaisut ja pankkien TUPAS-tunnistus.

Ohje tulee VAHTIn Internet-sivuille *www.vm.fi/vahti*. Opasta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää sekä neuvotteleva virkamies Seppo Kurkinen ja neuvotteleva virkamies, VAHTIn puheenjohtaja Mikael Kiviniemi (sähköpostit: etunimi.sukunimi@vm.fi).

Toinen valtiovarainministeri Ulla-Maj Wideroos

Ylijohtaja Jorma Karjalainen

Liite *Tunnistaminen julkishallinnon verkkopalveluissa (VAHTI 12/2006)*

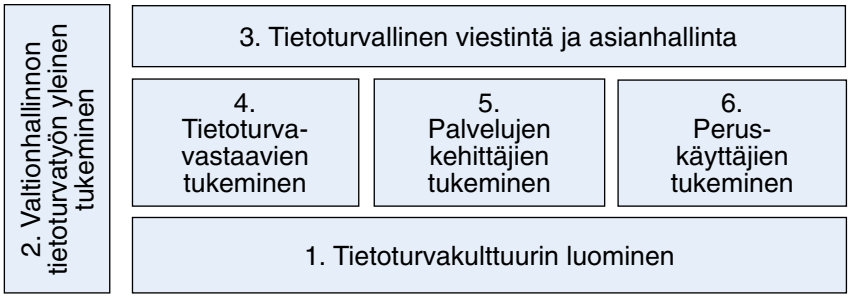
TIEDOKSI Kunnat

ESIPUHE

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) on yli kymmenvuotisen toimintansa aikana vakiinnuttanut asemansa hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimenä.

Valtiovarainministeriön johtamalla ja Valtion tietoturvallisuuden johtoryhmän VAHTI koordinoimalla valtion tietoturvallisuuden kehitysohjelmalla (VAHTIn julkaisu 1/2004) kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Seuraavassa kuvassa esitetyissä kuudessa kehitysohjelman osa-alueessa on yhteensä 29 laajaa kehittämiskohdetta.

Kaavio valtion tietoturvallisuuden kehitysohjelmasta ja sen hankealueista



Kehitysohjelman aikana merkittävää kehitystyötä on toteutunut kaikilla ohjelman hankealueilla ja yhteensä 26:ssa kehittämiskohteessa. Toteuttamiseen osallistuvat laajasti kaikki hallinnonalat ja osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä muita asiantuntijoita. Valtionhallintotasolta nimettyjä osallistujia hankkeissa on ollut yli 300.

Tämä ohjeen on laatinut VAHTIn alainen tunnistaminen ja käyttövaltuudet- työryhmä. Ohjeen luonnos oli laajalla lausuntokierroksella keväällä 2006. Ohje viimeisteltiin lausuntojen pohjalta valtion- ja kunnallishallinnon yhteistyössä.

Ohje hyväksyttiin VAHTIn kokouksessa marraskuussa 2006. Ohje korvaa VM:n aiemmin antaman ohjeen Tunnistaminen valtionhallinnon verkkopalveluissa (VM 6/01/2006).

Sisällysluettelo

JOHDON YHTEENVETO 9

1 JOHDANTO 11

2 SÄÄDÖSTEN ASETTAMIA RAJOITTEITA/VELVOLLISUUKSIA 13

3 YLEISET LINJAUKSET 15

4 VERKKOPALVELUJEN JA NIIDEN KÄYTÖN LUOKITTELUA 17
4.1 Verkkopalvelujen tyyppiluokittelu 17
4.2 Käyttäjien tunnistamisen luotettavuus 18
4.2.1 Käyttäjäidentiteetin luotettavuus 18
4.2.2 Käyttäjäidentiteetin todentamisen luotettavuus 20
4.3 Palvelutyyppien edellyttämä käyttäjän tunnistamisen luotettavuus 21
4.4 Tietojen luottamuksellisuustasoluokittelu 21

5 KÄYTTÄJIEN TUNNISTAMINEN VERKKOPALVELUISSA 23
5.1 Yleistä 23
5.2 Organisaation tunnistaminen 23
5.2.1 TUPAS 24
5.2.2 KATSO 24
5.3 Järjestelmä-tyyppisten käyttäjien tunnistaminen 25
5.4 Käyttäjien tunnistaminen eri tyyppisissä verkkopalveluissa 25
5.4.1 Tietopalvelut ja tiedottaminen 26
5.4.2 Asiakaspalaute ja kansalaisten osallistuminen 26
5.4.3 Ei-luottamuksellinen vuorovaikutteinen asiointi 27
5.4.4 Vireillepano 27
5.4.5 Luottamuksellinen vuorovaikutteinen asiointi 28
5.4.6 Tietojärjestelmien välinen tietojenvaihto 28
5.4.7 Viranomaispalvelut 29

6 VIRANOMAISEN TUNNISTAMINEN VERKKOPALVELUISSA 31

7 TUNNISTAMINEN SÄHKÖPOSTIASIOINNISSA 33

LIITE 1: Sanasto 35

LIITE 2: Voimassa olevat VAHTI-julkaisut 41

JOHDON YHTEENVETO

Tämä ohje koskee asiointia viranomaisten kanssa.

Tämä ohje on tarkoitettu virastojen johdolle, tietohallinnolle, tietoturvavastaaville sekä verkkopalvelujen suunnittelijoille. Ohjeessa ei käsitellä tunnistamiseen liittyviä oheispalveluita, kuten salausta, tekniikkaa eikä tuotteita.

Valtionhallinnon kansalaisille suunnatuissa verkkopalveluissa käyttäjän tunnistamistarve vaihtelee palvelutyypin mukaan. Tiedottamispalveluissa käyttäjää ei tarvitse eikä tule tunnistaa. Vahvaa tunnistamista tarvitaan luottamuksellisessa vuorovaikutteisissa asiointipalveluissa sekä tietojärjestelmien välisessä tietojenvaihdossa (sovellus-sovellus -asiointi). Verkkopalveluita rakennettaessa on aina arvioitava vaatiiko palvelu käyttäjän tunnistamista, ja jos vaatii, niin minkä tasoista.

Kansalaisella ei yleensä ole pitkäaikaista säännöllistä tarvetta vuorovaikutteiseen asiointiin valtionhallinnon kanssa. Jotta palvelujen käyttö olisi riittävän helppoa myös satunnaiselle käyttäjälle, valtion virastojen ja laitosten on vältettävä omien tunnistamispalvelujen rakentamista. Tunnistamisessa tulee ensisijaisesti käyttää valtionhallinnossa hyväksyttäviä vahvoja tunnistamismenetelmiä tukevia yleisiä tunnistamispalveluja.

Valtionhallinnon sisäisissä, viranomaiskäyttöön tarkoitetuissa verkkopalveluissa käyttäjät tulee aina tunnistaa. Tarvittava tunnistamisen vahvuus riippuu käsiteltävien tietojen luottamuksellisuustasosta. Myös viranomaispalveluissa voidaan käyttää em. yleisiä tunnistamispalveluja silloin, kun se nähdään tarkoituksenmukaiseksi.

Perustettaessa verkkopalvelua arvioidaan ensimmäiseksi, tarvitaanko sen käyttäjiltä ylipäänsä tunnistamista. Arvioinnissa on syytä ottaa huomioon koko se toimintaprosessi, johon verkkopalvelu liittyy.

Verkkosivuja tuottavan viranomaisen on huolehdittava sivujen eheydestä ja siitä, että asiakas voi aina varmistautua sivujen aitoudesta.

Viranomainen voi allekirjoittaa päätöksiä sähköisesti virkaan liittyvää varmennetta käyttäen. Tarvittaessa viranomainen voi tunnistautua myös asiakkaan kanssa asioidessaan, eli vahvistaa asiakkaalle olevansa se viranomainen, joka sanoo olevansa.

Sähköpostin lähettäjä on luotettavasti tunnistettavissa vain sähköisestä allekirjoituksesta. Sähköinen allekirjoitus takaa sekä viestin eheyden että lähettäjän luotettavan tunnistamisen. Tämä pätee sekä viranomaisten ja kansalaisten väliseen että viranomaisten keskinäiseen sähköpostiliikenteeseen.

Sähköposti soveltuu kohtuullisen hyvin kansalaisten ja viranomaisten väliseen ei-luottamukselliseen asiointiin. Samoin viranomaisten välillä sähköposti soveltuu normaaliin päivittäisasiointiin. Kriittisten ja/tai nopeaa toimintaa edellyttävien sähköpostiviestien perillemeno tulee vahvistaa joko sähköpostiviestin kuittauspyynnöllä tai erillisellä puhelinsoitolla. Luottamuksellisessa asioinnissa tulee sähköisen allekirjoituksen lisäksi käyttää tapauskohtaisen harkinnan mukaisesti sähköpostiviestin ja/tai sen liitteiden salausta.

Sähköpostiasioinnissa on suositeltavaa käyttää organisaatio-osoitetta henkilökohtaisen osoitteen sijasta. (*Valtionhallinnon sähköpostien käsittelyohje*, VAHTI 2/2005)

1 JOHDANTO

Tämä ohje koskee asiointia viranomaisten kanssa. Ohje korvaa valtionvarainministeriön vuonna 2003 antama ohjeen *Tunnistaminen valtionhallinnon verkkopalveluissa* (VM 6/01/2003). Ohjetta on täydennetty, ajanmukaistettu ja sen jäsentelyä on muutettu. Kokonaan uutta ohjeessa on liitteenä oleva sanasto, verkkopalvelujen käyttäjien tunnistamisen luotettavuustarkastelu, käyttöön tulleiden yleisten tunnistamispalvelujen sekä sovellus-sovellus -asioinnin ja viranomaispalvelujen huomioonottaminen sekä osapuolten tunnistamista sähköpostiasioinnissa käsittelevä osuus.

Tämä ohje on tarkoitettu virastojen johdolle, tietohallinnolle sekä verkkopalvelujen suunnittelijoille. Ohjeessa ei käsitellä tunnistamiseen liittyviä oheispalveluita, kuten salausta, tekniikkaa eikä tuotteita.

Taulukko 1

	Organisaation johto	Tietohallinto	Verkkopalvelujen suunnittelija
Luku 1	x	x	x
Luku 2	x	x	x
Luku 3	x	x	x
Luku 4	x	x	x
• 4.1			x
• 4.2			x
• 4.3			x
• 4.4			x
Luku 5		x	x
Luku 6	x	x	x
Luku 7	x	x	x

Lukuohje tähän ohjeeseen. Rasti ruudussa tarkoittaa ”Luettava”.

OECDltä on valmistumassa tunnistamista koskeva suositus. Suomen hallinto hyödyntää sitä soveltuvin osin omassa toiminnassaan.

Mobiili- ja biometriikkatunnistamisen menettelyt ja ratkaisut kehittyvät tällä hetkellä nopeasti, minkä takia niihin liittyviä tarkkoja linjauksia ei ohjeessa esitetä.

2 SÄÄDÖSTEN ASETTAMIA RAJOITTEITA/VELVOLLISUUKSIA

Tiedot, joiden perusteella henkilö voidaan tunnistaa ja yhdistää koskemaan tiettyä yksilöityä henkilöä, ovat henkilötietoja, joiden käsittelyssä tulee ottaa huomioon henkilötietolainsäädännön vaatimukset. Tunnistettavalle on ilmoitettava tunnistustietojen käsittelystä pääsääntöisesti ennen kuin tunnistus tapahtuu. Käsiteltävien henkilötietojen tulee olla käsittelyn tarkoituksen kannalta tarpeellisia ja tarkoituksenmukaisia (HetiL 9§). Tunnistustieto saa kertoa tunnistettavasta vain sen, mitä tunnistus edellyttää. Henkilötietoja ei saa luovuttaa tarkoituksiin, jotka eivät ole yhteensopivia tietojen alkuperäisen tarkoituksen kanssa (HetiL 8§). Tunnistamisen yhteydessä on varmistettava sekä tunnistamistietojen käsittelyn turvallisuus että tunnistustapahtuman osapuolten aitous. Lisätietoa henkilötietolain soveltamisesta löytyy tietosuojavaltuutetun kotisivuilta (www.tietosuoja.fi).

Sähköisen viestinnän tietosuojalain (516/2004) 7 §:ssä on säädetty evästeiden käyttöä koskevista edellytyksistä. Laki sähköisistä allekirjoituksista (14/2003) taas sääntelee varmenteiden tarjontaa ja niiden käyttöä allekirjoitus ja tunnistamistarkoituksiin.

Laki viranomaisten toiminnan julkisuudesta (Julkisuuslaki, 621/1999, uudistukset mm. 495/2005) määrittelee vaatimukset hyvälle tiedonhallintatavalle, joita täsmennetään lain nojalla annetussa asetuksessa (1030/1999).

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) säädetään viranomaisen ja hallinnon asiakkaan oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa. Lisäksi siinä säädetään henkilön sähköiseen tunnistamiseen liittyvistä keskeisistä vaatimuksista.

3 YLEISET LINJAUKSET

Valtionhallinnon kansalaisille suunnatuissa verkkopalveluissa käyttäjän tunnistamistarve vaihtelee palvelutyypin mukaan. Tiedottamispalveluissa käyttäjää ei tarvitse eikä tule tunnistaa. Vahvaa tunnistamista tarvitaan luottamuksellisessa vuorovaikutteisissa asiointipalveluissa sekä tietojärjestelmien välisessä tietojenvaihdossa (sovellus-sovellus -asiointi). Verkkopalveluita rakennettaessa on aina arvioitava vaatiiko palvelu käyttäjän tunnistamista, ja jos vaatii, niin minkä tasoista.

Kansalaisella ei yleensä ole pitkäaikaista säännöllistä tarvetta vuorovaikutteiseen asiointiin valtionhallinnon kanssa. Jotta palvelujen käyttö olisi riittävän helppoa myös satunnaiselle käyttäjälle, valtion virastojen ja laitosten on vältettävä omien tunnistamispalvelujen rakentamista. Tunnistamisessa tulee ensisijaisesti käyttää valtionhallinnossa hyväksyttäviä vahvoja tunnistamismenetelmiä tukevia yleisiä tunnistamispalveluja, jollaisia ovat tunnistus.fi sekä VETUMA[1].

Valtionhallinnon sisäisissä, viranomaiskäyttöön tarkoitetuissa verkkopalveluissa käyttäjät tulee aina tunnistaa. Tarvittava tunnistamisen vahvuus riippuu käsiteltävien tietojen luottamuksellisuustasosta. Myös viranomaispalveluissa voidaan käyttää em. yleisiä tunnistamispalveluja silloin, kun se nähdään tarkoituksenmukaiseksi.

Luotettavuudeltaan parhaita tunnistamisratkaisuja ovat laatuvarmenteeseen perustuvat PKI-ratkaisut ja Tupas-tunnistaminen. Laatuvarmenteilla on normipohja ja kumpaakin em. ratkaisuista valvotaan, laatuvarmenteiden toteutusta valvoo Viestintävirasto ja pankkien tunnistusratkaisuja Rahoitustarkastus.

[1] VETUMA -hanke on tuottanut yleisen kansalaisen tunnistamis- ja maksamispalvelun julkishallinnon verkkopalveluja varten.

4 VERKKOPALVELUJEN JA NIIDEN KÄYTÖN LUOKITTELUA

Verkkopalvelun käytön haluttu luottamustaso eli varmuus käyttäjän todellisesta identiteetistä on suoraan verrannollinen siihen, miten suuria riskejä palvelun väärinkäyttöön liittyy tai miten luottamuksellisia palvelussa käsiteltävät tiedot ovat. Käyttäjien tunnistamistaso pitää aina suhteuttaa edellä mainittuihin seikkoihin.

4.1 Verkkopalvelujen tyyppiluokittelu

Verkkopalvelut voidaan jakaa sisältönsä ja luonteensa mukaan karkeasti seuraavassa esiteltyihin seitsemään päätyyppiin. Jaottelu on suuntaa-antava. Sen tarkoituksena on auttaa palveluntarjoajaa käytännön verkkopalvelujen tunnistamiselle asetettavan vaatimustason määrittämisessä. Se ei ole mikään ehdoton luokittelu, johon käytännön verkkopalvelut pitää väkisin sovittaa.

A. Tietopalvelut ja tiedottaminen, jossa asiakkaalle tarjotaan tietoa hallinnosta ja hallinnon palveluista

B. Asiakaspalaute ja kansalaisten osallistuminen, jossa kansalaiset voivat antaa palautetta viranomaiselle palveluista tai osallistua keskusteluun, jolla pyritään kehittämään yhteiskunnan toimintaa

C. Ei-luottamuksellinen vuorovaikutteinen asiointi, joka koskee muuta kuin asiakkaan luottamuksellisia henkilökohtaisia tietoja

D. Vireillepano, jossa asiakkaalle tarjotaan mahdollisuus täyttää hakemuslomake sähköisesti ja lähettää se sähköisesti viranomaiselle

E. Luottamuksellinen vuorovaikutteinen asiointi, jossa käsitellään asiakkaan luottamuksellisia henkilökohtaisia tietoja

F. Tietojärjestelmien välinen tietojenvaihto, jossa tietojärjestelmäsovellukset keskustelevat automaattisesti keskenään. Esimerkiksi tietojen haku toisen viranomaisen

rekisteristä, verkkomaksutapahtumat, viranomaisten keskinäiset tai asiakkaiden ja viranomaisten väliset tietojen siirrot

G. **Viranomaispalvelut**, jolla tarkoitetaan kaikenlaisia yksinomaan viranomaisten sisäiseen käyttöön tarkoitettuja verkkopalveluja sekä eri viranomaisten välisen virkamieskäytön kuten virkamies virastosta A käyttää viraston B palvelua

4.2 Käyttäjien tunnistamisen luotettavuus

Verkkopalveluissa saavutettavissa olevaa käyttäjien tunnistamisen luotettavuutta voidaan tarkastella kahdesta näkökulmasta:

1. Käytetyn **käyttäjäidentiteetin** luotettavuus
2. Käytetyn **käyttäjäidentiteetin todentamisen** luotettavuus.

Keskimäärin voidaan lähteä siitä, että näiden luotettavuustekijöiden tulee olla suunnilleen samantasoisia, mutta aina tämä lähtökohta ei päde. Esimerkiksi[2] voidaan ajatella lääketieteellistä testauspalvelua, jota voidaan käyttää nimimerkillä (ts. alhaisen luotettavuustason käyttäjäidentiteetillä), mutta jonka tulosten tulee pysyä luottamuksellisina, eli käyttäjältä tulee vaatia vahvaa tunnistamista. Vastaavasti voi olla järkevää mahdollistaa ei-luottamuksellisten palvelujen käyttö myös korkean luotettavuustason käyttäjäidentiteetillä kuten kansalaisvarmenteella, jos käyttäjällä sellainen jo on, vaikka palvelun käyttö ei käyttäjiltään sellaista muuten edellytäkään.

4.2.1 Käyttäjäidentiteetin luotettavuus

Käyttäjäidentiteetillä tarkoitetaan palveluntarjoajan tiedossa olevia käyttäjän henkilöllisyyttä yksilöiviä ja kuvaavia tietoja. Käyttäjäidentiteetti luodaan palvelujärjestelmään silloin, kun käyttäjä rekisteröidään järjestelmän käyttäjäksi. Käyttäjäidentiteetin luotettavuus riippuu siten rekisteröintiprosessista. Jos käyttäjä antaa rekisteröinnin yhteydessä itse tietonsa, joita ei mitenkään tarkisteta, käyttäjäidentiteetin luotettavuus on alhainen. Vastaavasti jos käyttäjän henkilöllisyys selvitetään luotettavasti kasvotusten, rekisteröinnin tuloksena syntyy käyttäjäidentiteetti, jonka luotettavuus on maksimaalinen.

Joissain tapauksissa henkilön identiteetti ei ole tärkeää, vaan se kuuluuko henkilö johonkin ryhmään (esimerkiksi kuntalaisuus) ja onko näin oikeutettu esim. jonkin palvelun käyttöön. Käyttäjän ilmoittamat tiedot, kuten nimi ja osoite, riittävät monissa palveluissa sellaisenaan tunnistukseksi. Tarvittaessa voidaan tietojen luotettavuus varmistaa vertailemalla ilmoitettuja tietoja palvelun tarjoajan omissa tietojärjestelmissä oleviin tietoihin.

[2] Esimerkki on dokumentista "Interchange of Data between Administrations (IDA), Authentication Policy" (European Commission Directorate General Enterprise, 8.7.2004)

Aina todentamista ei tarvita, vaan esim. riittää että palvelun käyttäjä suorittaa palvelusta aiheutuvan maksun, maksajan henkilöllisyyttä ei tarvitse tietää.

Käyttäjäidentiteetin luotettavuuden kuvaamiseen voidaan käyttää seuraavaa nelitasoista luokittelua.

Taso 0: Anonyymikäyttäjät

Käyttäjiä ei rekisteröidä, eivätkä he ole palvelujen eri käyttökerroilla erotettavissa toisistaan.

Taso 1: Yksilöitävissä olevat käyttäjät

Käyttäjillä on rekisteröity käyttäjäidentiteetti, jonka perusteella he ovat yksilöitävissä. Käyttäjäidentiteetti ei kuitenkaan välttämättä paljasta käyttäjän todellista henkilöllisyyttä, asuinpaikkaa tms., koska rekisteröinnin yhteydessä annettujen käyttäjätietojen paikkansapitävyyttä ei ole tarkistettu.

Käyttäjä voi olla yksilöitävissä myös teknisesti ilman rekisteröintiä, palvelun käyttäjän työasemalle tallettaman evästeen perusteella. Yksilöinti kohdistuu tällöin tarkkaan ottaen käyttäjän päätelaitteeseen eikä itse käyttäjään. Henkilötietolain mukaan kuitenkin nämäkin yksilöintitiedot voitaisiin katsoa henkilötiedoiksi. Yhteiskäyttöiseltä koneelta luettava eväste aiheuttaa identiteettien sekaantumisen eli evästeeseen luottava sovellus ymmärtää kaksi peräkkäistä konetta käyttävää samaksi henkilöksi.

Taso 2: Kevyesti todennetut käyttäjät

Käyttäjillä on käyttäjäidentiteetti, jonka rekisteröintiprosessin yhteydessä on varmistauduttu siitä, että ainakin jotkut annetuista käyttäjätiedoista (puhelinnumero, osoite, luottokortin numero tms.) pitävät paikkansa, jolloin käyttäjäidentiteettiä voidaan pitää moniin tarkoituksiin riittävän luotettavana.

Taso 3: Vahvasti todennetut käyttäjät

Käyttäjien henkilöllisyys on selvitetty luotettavasti, esimerkiksi henkilökohtaisella tapaamisella rekisteröintitilanteessa. Henkilön identiteetin varmistaa valtuutetun organisaation edustaja. Henkilön on todistettava henkilöllisyytensä virallisella henkilökortilla, ajokortilla tai passilla.

4.2.2 Käyttäjäidentiteetin todentamisen luotettavuus

Todentamisen luotettavuus riippuu tunnistamisessa käytettävästä todentamismenetelmästä. Käyttäjäidentiteetin todentaminen perustuu johonkin seuraavista kolmesta vaihtoehdosta:

A) johonkin mitä käyttäjä tietää
B) johonkin mitä käyttäjällä on hallussaan
C) johonkin mitä käyttäjä on.

A-vaihtoehto on sähköisessä asioinnissa perinteisesti eniten käytetty todentamistapa ja tarkoittaa salasanaa tai salalausetta, jonka käyttäjä joutuu antamaan tunnistetietonsa eli käyttäjätunnuksensa yhteydessä. Käyttäjän tulee olla aiemmin sitoutunut olemaan luovuttamatta tietoa kenellekään muulle.

B-vaihtoehto tarkoittaa tunnistusvälinettä, jonka sisältämän tiedon perusteella käyttäjäidentiteetti pystytään määrittämään. Esimerkkejä tunnistusvälineistä: sirukortti, tietyllä SIM-kortilla varustettu matkapuhelin.

C-vaihtoehto tarkoittaa käytännössä jotain käyttäjän biometristä ominaisuutta: sormenjälkeä, kasvojen muotoa, silmän iiristä tms.

Tunnistamista sanotaan **kevyeksi tunnistamiseksi**, jos se nojautuu vain yhteen todentamistapaan. Esimerkkejä kevyestä tunnistamisesta:

- käyttäjätunnus + salasana
- pelkkä varmenteellisen sirukortin esittäminen tai pelkkä puhelinsoitto matkapuhelimesta/-een
- pelkkä biotunnistaminen.

Vahva tunnistaminen nojautuu kahteen tai useampaan todentamistapaan. Tällaisia tunnisteita ja tunnistamismenetelmiä ovat:

- verkkopankkitunnuksiin ja vaihtuviin salasanalistoihin perustuva TUPAS-tunnistus
- käyttäjätunnus + salasana + puhelinsoitto matkapuhelimesta/-een
- varmenteellinen sirukortti + salasana (PIN-koodi)
- varmenteellinen sirukortti + biotunnistus
- laatuvarmenteellinen sirukortti + salasana (PIN-koodi)
- laatuvarmenteellinen sirukortti + biotunnistus.

Biometrinen tunnistaminen ei yksinään takaa vahvaa tunnistamista. Tekniikat ovat kehitysvaiheessa, tunnisteet ja niihin liittyvät haavoittuvuudet muuttuvat tekniikan kehittyessä.

4.3 Palvelutyyppien edellyttämä käyttäjän tunnistamisen luotettavuus

Taulukossa 1 esitetään edellä kuvattujen palvelutyyppien ja käyttäjien tunnistamiselta edellytettävän luotettavuuden väliset lähtökohtaiset ohjeelliset riippuvuudet.

Huomattakoon kuitenkin, että kohdassa 4.2 esitetyn esimerkin mukaisesti voi olla tapauksia, joissa on syytä poiketa taulukon oletusarvoista. Siksi aina tulee viime kädessä tapauskohtaisesti arvioida, minkä tasoista luotettavuutta käyttäjäidentiteetiltä ja käyttäjän todentamiselta vaaditaan.

Taulukko 2

käyttäjäidentiteetti	**ano-nyymi**	**yksilöitävissä**		**kevyesti todennettu**		**vahvasti todennettu**	
käyttäjän tunnistamistapa (todentamisen luotettavuus)	–	kevyt	vahva	kevyt	vahva	kevyt	vahva
Tietopalvelut ja tiedottaminen	x	x					
Asiakaspalaute ja kansalaisten osallistuminen	x	x					
Ei-luottamuksellinen vuorovaikutteinen asiointi		x		x			
Vireillepano	x	x		x	x		x
Luottamuksellinen vuorovaikutteinen asiointi					x		x
Tietojärjestelmien välinen tietojen vaihto							x
Viranomaispalvelut						x	x

Rasti ruudussa tarkoittaa, että sarakkeen luotettavuustaso on käyttökelpoinen rivin asiointipalvelussa
Harmaa ruutu tarkoittaa, että sarakkeen luotettavuustaso ei ole mielekäs tai riittävä rivin asiointipalvelussa

4.4 Tietojen luottamuksellisuustasoluokittelu

Tietojen luokittelussa on parhaillaan käynnissä VM:n johtama ja VAHTIssa koordinoitava kokonaisuudistus, joka tulee osin muuttamaan nykyohjeissa vahvistettuja luokituksia ja niiden ohjeistamista.

Tähän liittyen on käynnissä myös julkisuuslain nojalla annetun hyvää tiedonhallintatapaa koskevan asetuksen uudistaminen siten, että tietoaineistojen luokittelun säännökset ja käsittelyn vaatimukset selkiytetään.

VAHTI-ohjeessa 2/2000 *”Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje”*, jota täydentää VAHTI-ohje 4/2002 *”Arkaluonteiset kansainväliset tietoaineistot”*, esitetään tietojen **luottamuksellisuustasoluokittelu**.

Kansainvälisten tietoaineistojen osalta luokittelu ja käsittely on ohjeistettu Laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sekä VAHTI-ohjeessa 4/2002 *”Arkaluonteiset kansainväliset tietoaineistot”*,

Verkkopalvelun käytön haluttu luottamustaso eli varmuus käyttäjän todellisesta identiteetistä on suoraan verrannollinen siihen, miten suuria riskejä palvelun väärinkäyttöön liittyy tai miten luottamuksellisia palvelussa käsiteltävät tiedot ovat.

Viranomaisten julkisten asiakirjojen ja tietojen käsittelylle ei aseteta erityisvaatimuksia; tietojen tulee periaatteessa olla kenen tahansa saatavilla ilman tunnistamisvaatimusta.

5 KÄYTTÄJIEN TUNNISTAMINEN VERKKOPALVELUISSA

5.1 Yleistä

Perustettaessa verkkopalvelua arvioidaan ensimmäiseksi, tarvitaanko sen käyttäjiltä ylipäänsä tunnistamista. Arvioinnissa on syytä ottaa huomioon koko se toimintaprosessi, johon verkkopalvelu liittyy. Jos esimerkiksi prosessin myöhempään vaiheeseen liittyy aina käyttäjän henkilökohtainen tapaaminen, käyttäjän muodollinen tunnistaminen ei vireillepanovaiheessa ole tarpeen. Tällöin ei palvelun käyttäjältä (asiakkaalta) tule myöskään vaatia rekisteröintiä eikä teknisin keinoin tule millään tavalla rekisteröidä käyttäjän tietoja. Käyttäjän anonymiteetin säilyminen on voitava taata (käyttäjäidentiteetin **luotettavuustaso 0** *taulukossa 1*).

Tunnistusta vaatimalla voidaan varmistaa myös, että tunnistettu henkilö voi käyttää palvelua vain kerran, mikäli se asiointitapahtuman kannalta on tärkeää. Tällaisia voivat olla mm. äänestykseen tai muuhun mielipiteen ilmaisuun liittyvät tapahtumat. Äänestystapahtumissa on kuitenkin tärkeä varmistaa, että käyttäjän identiteettiä ei voida teknisesti yhdistää annettuun mielipiteeseen.

Jos kuitenkin päädytään siihen, että käyttäjien tunnistamista tarvitaan, määritellään seuraavaksi tunnistamiselta edellytettävä luotettavuustaso. Vaadittava luotettavuustaso riippuu ennen kaikkea palvelussa käsiteltävien tietojen luottamuksellisuudesta. Tarpeellista palvelun käyttäjän tunnistaminen on silloin, kun käyttäjä pääsee käsiksi suojattaviin tietoihin (esim. salassa pidettävät henkilötiedot) tai käyttäjä voi laittaa vireille asioita, joilla on oikeudellista tai huomattavaa taloudellista merkitystä. Joskus myös lainsäädäntö voi vaatia käyttäjän tunnistamista. Luotettavuustasoa määriteltäessä otetaan kantaa siihen, miten luotettavaa käyttäjäidentiteettiä käyttäjiltä vaaditaan ja minkä tasoisesti käyttäjät todennetaan palvelun käyttötilanteessa. Näissä tapauksissa (käyttäjäidentiteetin **luotettavuustasot 1–3**) käyttäjän tulee rekisteröityä vaaditun luotettavuustason edellyttämällä tavalla.

5.2 Organisaation tunnistaminen

Organisaation tunnistaminen poikkeaa henkilön tunnistamisesta. Palvelua käyttävän henkilön tunnistaminen ei yksinään riitä organisaation tunnistamiseksi, vaan lisäksi on varmistettava henkilön yhteys organisaatioon. Jos henkilö tunnistautuu palveluun omalla henkilökohtaisella käyttäjäidentiteetillään, on varmistettava henkilön oikeus toimia palvelun käyttäjänä organisaation puolesta.

Organisaation ja henkilön samanaikaiseen tunnistamiseen voidaan käyttää rooli- tai työvarmennetta. Tällä tarkoitetaan tässä yhteydessä sellaista varmennetta, jossa on henkilötietojen lisäksi tieto organisaatiosta, jossa henkilö työskentelee.

Henkilökohtaista käyttäjäidentiteettiä kuten sähköistä henkilövarmennetta ei yksinään voi käyttää organisaation tunnistamiseen, koska sellaisen avulla voidaan tunnistaa vain henkilö. Organisaation edustajana toimiminen henkilökohtaista käyttäjäidentiteettiä käyttäen edellyttää kaksivaiheista rekisteröimisprosessia. Ensimmäisessä vaiheessa henkilöt hankkivat itselleen palvelussa tarvittavan henkilökohtaisen käyttäjäidentiteetin. Sen jälkeen organisaatio ilmoittaa luotettavalla tavalla palvelun tarjoavalle viranomaiselle ne henkilöt (käyttäjäidentiteetit), joilla on valtuus käyttää organisaation nimissä palvelua.

Palvelua käytettäessä käyttäjä tunnistetaan ensin henkilökohtaisen käyttäjäidentiteettinsä avulla ja sen jälkeen varmistetaan henkilön ja organisaation rekisteröidyn yhteyden olemassaolo.

5.2.1 TUPAS

Silloin kun henkilö käyttää organisaatiolle rekisteröityä käyttäjäidentiteettiä, organisaatio on tunnistettavissa. Etenkin pienillä ja keskisuurilla organisaatioilla on käytössään organisaatiokohtaisia verkkopankkitunnuksia. TUPAS-tunnistusmenetelmää tukevasta tunnistamispalvelusta viraston verkkopalvelu saa organisaation Y-tunnuksen, jonka avulla asioiva organisaatio voidaan suoraan yhdistää viraston asiakasrekisteriin. Organisaatiokohtaisilla TUPAS-tunnisteilla ei pääsääntöisesti tunnisteta asiointiin oikeutettua organisaatiota edustavaa henkilöä, vaan tunnistaminen kohdentuu organisaatioon yleisemmällä tasolla.

5.2.2 KATSO

Katso-organisaatiotunnistus on Verohallinnon ja Kansaneläkelaitoksen rakentama sähköisen tunnistamisen palvelu. Katso mahdollistaa joko vahvan tai kevyen tunnistamisen. Vahvassa tunnistamistavassa käytetään kahta todentamismenetelmää: käyttäjätunnusta, salasanaa ja vaihtuvaa salasanaa (OTP). Kevyessä tunnistamistavassa käytetään yhtä todentamismenetelmää: käyttäjätunnusta ja salasanaa (PWD).

Vahvasti todennettu Katso -tunniste liittää yhteen henkilön identiteetin sekä hänen

roolinsa organisaation toimivaltaisena edustajana. Tunniste muodostetaan organisaation aloitteesta tai avustuksella mutta tunniste myönnetään viranomaisen henkilö- ja organisaatiotarkistusten kautta.

Yksilöivä Katso -alitunniste on ainoastaan haltijansa nimeen sidottu. Yksiselitteistä henkilökytkentää ei ole. Tunniste muodostetaan organisaation toimesta. Alitunnisteita ei voi muodostaa oman organisaation (Y-tunnuksen) ulkopuolisille henkilöille.

Käyttäjän oikeudet määräytyvät tunnisteelle annettujen roolien perusteella.

Organisaatio itse antaa tarvittavat valtuudet organisaationsa puolesta toimiville, esimerkiksi yrityksen tilitoimistolle antama oikeus veroilmoituksen lähettämiseen.

5.3 Järjestelmä-tyyppisten käyttäjien tunnistaminen

Laajeneva trendi hallinnossa on se, että viraston tietojärjestelmäpalveluja käyttävät henkilökäyttäjien lisäksi suoraan toisen viraston tai asiakasyrityksen tietojärjestelmät/sovellukset. Sovellus-sovellus -käyttö vaatii *taulukon 1* mukaan oletusarvoisesti vahvasti todennettua käyttäjäidentiteettiä sekä vahvaa käyttäjätunnistusta. Käyttäjäsovelluksen vahva todentaminen voi tapahtua implisiittisesti käytettäessä järjestelmien välillä kiinteää yhteyttä. Yleisten verkkojen kautta kommunikoitaessa sovellusten välillä tulee käyttää salattua yhteyttä ja käyttäjäsovelluksen tulee pääsääntöisesti tunnistautua sähköistä varmennetta tai muuta vahvaa tunnistamistapaa käyttäen.

Katso-tunnisteita voidaan käyttää järjestelmätyyppisten käyttäjien tunnistamiseen. Katso tarjoaa tunnistusrajapinnan (-rajapinnan) sovellus-sovellus -käyttöä varten. Jos tunnistusmenetelmänä käytetään Katson vaihtuvaa salasanaa, täytetään vahvan tunnistamisen vaatimukset.

Verohallitus on luonut viranomaisille Katso-tunnisteet, joita voi käyttää myös tietojärjestelmien välisessä kommunikoinnissa.

5.4 Käyttäjien tunnistaminen eri tyyppisissä verkkopalveluissa

Valtionhallinnon verkkopalveluissa tarvittava tunnistaminen suositellaan toteutettavaksi käyttäen tarjolla olevia tunnistuspalveluja (*tunnistus.fi, Vetuma, KATSO*). Tällöin palveluntarjoajan ei tarvitse huolehtia erilaisten tunnistusmenetelmien vaatimasta teknisestä toteutuksesta ja infrastruktuurista, joka TUPAS-tunnistuksen ja varmennepohjaisen tunnistuksen tapauksessa voi olla huomattava rasite. Tunnistuspalvelut antavat käyttäjille mahdollisuuden valita käyttämänsä tunnistustavan palveluntarjoajan sallimissa puitteissa. Niiden voidaan olettaa tukevan jatkossa myös uusia tunnistamistapoja kuten biometrista tunnistamista.

5.4.1 Tietopalvelut ja tiedottaminen

Tieto- ja tiedottamispalvelut ovat oletusarvoisesti anonyymisti käytettäviä, joten niiden käyttäjiä ei pidä koskaan velvoittaa rekisteröitymään järjestelmään eikä käyttäjätietoja saa myöskään rekisteröidä teknisin keinoin. Jokaisella on julkisuuslain (laki viranomaisten toiminnan julkisuudesta 621/1999) nojalla oikeus saada tietoa viranomaisen toiminnasta ja julkisista asiakirjoista.

Käyttäjien yksilöitävyyttä voidaan käyttää hyväksi mahdollistamaan

- käyttäjälle personoitu näkymä palveluun
- yhteydenpito käyttäjän kanssa tämän antaman yhteysosoitteen kautta
- palveluntarjoajalle seurantatietojen kerääminen esim. palvelun kehittämistä varten.

Yhteydenpito palveluntarjoajan ja käyttäjän välillä sekä seurantatiedon kerääminen edellyttää käyttäjältä rekisteröitymistä, jossa voidaan yhteysosoitteen lisäksi (tai sijasta) kysyä käyttäjästä joitain yleisiä demografisia tietoja kuten ikä, sukupuoli tai asuinseutu/-paikka. Tietojen antaminen tulee pitää käyttäjälle vapaaehtoisena, eikä niiden oikeellisuutta yhteysosoitetta lukuun ottamatta tarvitse tarkistaa. Jos/kun yhteysosoitetta pyydetään, sen toimivuus ja valtuus sen käyttöön tulee varmistaa lähettämällä käyttäjän antamaan osoitteeseen (useimmiten sähköpostiosoite) ilmoitus palvelun aktivoinnista ja pyytää käyttäjää ilmaisemaan suostumuksensa tähän vastaamalla viestiin.

Mikäli käyttäjätietoja halutaan kerätä vaikkapa tietystä aihealueesta kiinnostuneista käyttäjistä kohdistetun tiedotusmateriaalin toimittamiseksi esimerkiksi postituslistojen avulla, on rekisteröintitietoja kysyttäessä selkeästi ilmaistava, että rekisteröinti on tarpeellinen ainoastaan silloin, kun käyttäjä haluaa tämän ylimääräisen postituspalvelun. Jos palvelun käytöstä kerätään seurantatietoa esim. järjestelmän kehittämistä varten, on palvelussa selkeästi kerrottava mitä tietoa kerätään ja miten sitä käsitellään. Evästeiden käytöstä palvelussa on kerrottava käyttäjälle ymmärrettävästi ja kattavasti. Käyttäjän on halutessaan voitava asioida ilman evästeitä ja käyttäjätietojen keräämistä aina silloin kun se on teknisesti mahdollista.

Rekisteröidyille käyttäjille tarkoitetuissa tieto- ja tiedottamispalveluissa käyttäjän todentamiseen voidaan käyttää kevyttä tunnistamista, esimerkiksi käyttäjätunnus-salasana -menetelmää.

5.4.2 Asiakaspalaute ja kansalaisten osallistuminen

Asiakaspalautetta kerättäessä ja kansalaisten osallistuessa kansalaiskeskusteluun ei tunnistamista pidä vaatia eikä käyttäjiä pidä rekisteröidä teknisin keinoin, ellei rekisteröinnille ole painavia syitä, esimerkiksi palveluun kohdistuva jatkuva häiriköinti. Käyttäjät voivat halutessaan antaa tietoja itsestään, mikäli he haluavat esiintyä omalla nimellään tai haluavat saada henkilökohtaista palautetta virkamiehiltä.

Asiakaspalautteen vastaanotossa ja kansalaisten osallistumiseen tarkoitetuissa palve-

luissa käyttäjien tunnistamiselle asetetut vaatimukset ovat siten samanlaisia kuin edellisessä alakohdassa kuvattujen tieto- ja tiedottamispalvelujen tapauksessa. Lähtökohtaisesti palvelut ovat anonyymisti käytettäviä. Jos käyttäjiltä pyydetään rekisteröitymistä, luotettavuustason 1 käyttäjäidentiteetti riittää, ja käyttäjien tunnistamisessa voidaan käyttää kevyttä tunnistamista, esimerkiksi käyttäjätunnus-salasana -menetelmää.

Käyttäjille on syytä tiedottaa, että asiakaspalautejärjestelmä ei ole oikea kanava välittää luottamuksellisia henkilökohtaisia tietoja.

5.4.3 Ei-luottamuksellinen vuorovaikutteinen asiointi

Ei-luottamuksellisessa vuorovaikutteisessa asioinnissa, jossa ei käsitellä asiakkaan omia tai muita luottamuksellisia tietoja, palvelun käyttäjä tulee pystyä yksilöimään, mutta vahva todentaminen ei ole tarpeen.

Palvelujen käyttäjät tulee rekisteröidä. Useimmiten voidaan käyttäjiltä edellyttää ainakin todennettua yhteysosoitetta (luotettavuustason 2 käyttäjäidentiteetti), mutta on mahdollista, että joissain tapauksissa pärjätään käyttäjän ilmoittamilla tarkistamattomilla identiteettitiedoillakin (luotettavuustasolla 1) tai käyttäjän kuulumisella johonkin ryhmään. Käyttäjän tunnistamisessa riittää kevyt tunnistaminen kuten käyttäjätunnus-salasana -menetelmä.

5.4.4 Vireillepano

Asia voidaan aina panna vireille sähköisesti siten kuin laissa sähköisestä asioinnista viranomaistoiminnasta (13/2003) on säädetty. Lain 5 §:n mukaan *”Viranomaisen, jolla on tarvittavat tekniset, taloudelliset ja muut valmiudet, on niiden rajoissa tarjottava kaikille mahdollisuus lähettää ilmoittamaansa sähköiseen osoitteeseen tai määriteltyyn laitteeseen viesti asian vireille saattamiseksi tai käsittelemiseksi. Tällöin on lisäksi kaikille tarjottava mahdollisuus lähettää sähköisesti viranomaiselle sille toimitettavaksi säädettyjä tai määrättyjä ilmoituksia, sen pyytämiä selvityksiä tai muita vastaavia asiakirjoja taikka muita viestejä.”*

Vireillepanoasioissa voidaan asiakkaalle tarjota usean tasoisia tunnistautumisvaihtoehtoja. Kansalaisaloitteen tyyppisissä valtionhallinnolle tehdyissä vireillepanoasioissa asiakas voi toimia anonyymisti. Muuten voidaan edellyttää käyttäjän tunnistautumista asian luonteesta riippuvalla luotettavuustasolla. Vahvasti todennettu käyttäjäidentiteetti ja vahva tunnistaminen ovat tarpeen vain silloin, kun nähdään, että mahdolliset väärinkäytökset aiheuttavat merkittävää haittaa ja riski väärinkäytöksiin on suuri.

Vahvaa tunnistamista ja sähköistä allekirjoitusta voidaan edellyttää vain silloin, kun vireillepanoasiakirja on säädösten mukaan henkilökohtaisesti allekirjoitettava. Näitä nimenomaisia allekirjoitusvaatimuksia on lainsäädännössä verrattain vähän. Sähköistä asiointia viranomaistoiminnassa koskevan lain (13/2003, 9 §) ja hallintolain (434/2003, 22§) mukaan viranomaisen ei tarvitse pyytää asiakirjaa täydennettäväksi allekirjoituksella, mi-

käli asiakirjassa on tieto lähettäjästä eikä viranomaisella ole erityistä syytä epäillä viestin eheyttä ja lähettäjän henkilöllisyyttä.

5.4.5 Luottamuksellinen vuorovaikutteinen asiointi

Luottamuksellisissa vuorovaikutteisissa sähköisissä asiointipalveluissa vaaditaan asiakkaan vahvaa tunnistamista. Myös asiakkaan käyttäjäidentiteetin tulee normaalisti olla vahvasti todennettu (luotettavuustasoa 3), mutta joskus myös tason 2 osittain todennettu käyttäjäidentiteetti voi olla mahdollinen. Jos kyseessä on toiselle organisaatiolla suunnattu asiointipalvelu, myös organisaation/ vahvaa tunnistamista suositellaan.

Em. vaatimukset täyttävät tunnisteet ja tunnistamismenetelmät on lueteltu kohdassa 4.2.2.

Vuorovaikutteisissa organisaatioille suunnatuissa sähköisissä asiointipalveluissa organisaatio on aina tunnistettava. Mikäli palvelussa käsitellään henkilötietolain (523/1999) tarkoittamia arkaluontoisia tietoja tai organisaation salassa pidettäviä tietoja, organisaation edustajan on käytettävä vahvasti todennettua (luotettavuustaso 3) käyttäjäidentiteettiä, joka on kytketty ao. organisaatioon viranomaisen järjestelmässä.

5.4.6 Tietojärjestelmien välinen tietojenvaihto

Tietojärjestelmien välisessä tietojenvaihdossa suositellaan, että osapuolet tunnistautuvat toisilleen varmenteiden avulla. Tunnistettavien sovellusten käyttäjäidentiteettien voidaan olettaa käytännössä aina olevan vahvasti todennettuja eli perustuvat sovellukset omistavien organisaatioiden sopimukseen. Yhteyskumppanisovelluksen tunnistaminen voi olla oletuksena kiinteätä yhteyttä käytettäessä, mutta yleisiä verkkoja käytettäessä on nojauduttava selkeään tunnistamiseen mieluiten sähköistä allekirjoitusta käyttäen.

Palvelinvarmenteiden käyttö takaa ns. perustason tunnistuksen palveluiden välillä. Jos palvelussa välitetään salassa pidettävää aineistoa, niin voidaan vaatia lisätunnistusta.

Organisaatio voi valtuuttaa toisen organisaation hoitamaan puolestaan tietojenvaihtoa viranomaisten kanssa. Toimeksiantopalvelun tuottajaorganisaation tietojenvaihtoa hoitava järjestelmä on tällöin tarvittaessa voitava todentaa toimeksiantajaorganisaation valtuuttamaksi samaan tapaan kuin henkilökäyttäjä tulee voida todentaa organisaationsa valtuutetuksi edustajaksi.

Mikäli viranomaiselle välitettävät tiedot sisältävät arkaluonteisia tai muuten salassa pidettäviä organisaation tietoja, on tiedonsiirtoyhteys salattava, ja vastaanottavan viranomaisen tai tämän puolesta tietoja keräävän tahon (esim. TYVI-palvelun tarjoaja) tulee olla palvelinvarmennetta käyttäen luotettavasti tietoja luovuttavan organisaation tunnistettavissa.

5.4.7 Viranomaispalvelut

Viranomaispalvelujen käyttäjiä ovat heille työtehtäviensä puolesta annettua vahvasti todennettua käyttäjäidentiteettiä käyttävät virkamiehet ja toimihenkilöt. Viranomaispalvelun luonteesta ja ennen kaikkea siinä käsiteltävien tietojen luottamuksellisuustasosta (vrt. *kohta 4.4*) riippuu palveluun tunnistauduttaessa tarvittavan todentamisen vahvuus. Toimittaessa viranomaisten sisäisissä verkoissa kuten virastojen lähiverkoissa vahvaa todentamista ei välttämättä tarvita. Toisaalta käytettäessä luottamuksellisia viranomaispalveluja turvattomista verkoista, esimerkiksi etäyhteydellä Internetin kautta tai langattomalla mobiiliyhteydellä, käyttäjät on aina vahvasti tunnistettava ja yhteyden tulee muutenkin olla vahvasti suojattu (*Turvallinen etäkäyttö turvattomista verkoista*, VAHTI 2/2003)

Virastorajat ylittävässä viranomaispalvelujen käytössä tulee soveltaa kohdassa 5.2 kuvattuja menettelyjä käyttäjän organisaation ja hänen toimintavaltuuksiensa määrittämisessä.

Viranomaispalveluissa tunnistautuminen on suositeltavinta ratkaista virkakortin tai muun viranomaisten yleisessä käytössä olevan tunnistautumisvälineen avulla. Yhdenmukainen tunnistamistapa helpottaa viranomaisten välisen luottamusverkoston luomista.

Salassa pidettävien tietojen suhteen on erikseen huomattava julkisuuslaissa (621/1999 sekä lainmuutokset 495/2005) ja sitä täydentävässä asetuksessa annetut määräykset.

6 VIRANOMAISEN TUNNISTAMINEN VERKKOPALVELUISSA

Verkkosivuja tuottavan viranomaisen on huolehdittava sivujen eheydestä ja siitä, että asiakas voi aina varmistautua sivujen aitoudesta. Sivujen aitouden osoittaminen tapahtuu palvelujärjestelmän palvelinvarmenteeseen nojautuen. Palvelinvarmenteen avulla palvelu voidaan tunnistaa asianomaisen viranomaisen omistamaksi.

Viranomainen voi allekirjoittaa päätöksiä sähköisesti virkaan liittyvää varmennetta käyttäen. (Sisäasiainministeriön ohje 3.10.2000 nro SM 0527:00/03/02/1999). Tarvittaessa viranomainen voi tunnistautua myös asiakkaan kanssa asioidessaan, eli vahvistaa asiakkaalle olevansa se viranomainen joka sanoo olevansa.

Viranomaisen sähköisten asiointipalvelujen osoitteiden ja tietojen asiointipalveluihin liittyvistä varmenteista ja varmentajista tulee olla asiakkaiden saatavilla. Ao. tiedot on julkaistava viranomaisen Internet-sivuilla ja niiden julkaisemista suositellaan myös julkisen hallinnon hakemistopalvelu JULHAssa (*www.julha.fi*). Lisäksi on suositeltavaa linkittää viranomaisen sähköiset palvelut valtakunnallisiin portaaleihin kuten *suomi.fi, yrityssuomi.fi, lomake.f*i jne.

7 TUNNISTAMINEN SÄHKÖPOSTIASIOINNISSA

Selainpohjaisten verkkopalvelujen rinnalla sähköposti on kätevä ja monikäyttöinen asiointikanava, jonka käyttöön liittyy kuitenkin ongelmia käyttäjien luotettavan tunnistamisen näkökulmasta.

Sähköpostin lähettäjätiedot ovat nykyisissä sähköpostijärjestelmissä helposti väärennettävissä. Sähköpostiosoitteen haltijan tunnistaminen on usein epäluotettavaa ilman lähettäjätietojen väärentämisriskiäkin. Sähköpostikäyttäjien rekisteröinti kansalaisten laajalti käyttämissä ilmaisissa sähköpostipalveluissa tapahtuu yleensä ilman minkäänlaista käyttäjätietojen tarkistamista. Sähköpostipalveluja maksullisesti tarjoavien operaattorien käytännöt vaihtelevat. Työnantajien ja oppilaitosten myöntämät sähköpostitunnukset ovat pääsääntöisesti luotettavia, mutta niiden luotettaviksi osoitteiksi tunnistaminen ei ole yksinkertaista.

Sähköpostin lähettäjä on luotettavasti tunnistettavissa vain sähköisestä allekirjoituksesta. Sähköinen allekirjoitus takaa sekä viestin eheyden että lähettäjän luotettavan tunnistamisen. Tämä pätee sekä viranomaisten ja kansalaisten väliseen että viranomaisten keskinäiseen sähköpostiliikenteeseen.

Sähköpostin lähettäjän tunnistamisen periaatteellisesta epäluotettavuudesta huolimatta sähköpostiasioinnin epäluotettavuutta ei ole syytä liioitella, koska aivan vastaava periaatteellinen epäluotettavuus pätee myös perinteisiin asiointimuotoihin, puhelin- ja kirjeasiointiin. Laissa sähköisestä asioinnista todetaan: *”Viranomaiselle saapunutta sähköistä asiakirjaa ei tarvitse täydentää allekirjoituksella, jos asiakirjassa on tiedot lähettäjästä eikä asiakirjan alkuperäisyyttä tai eheyttä ole syytä epäillä”*.

Sähköposti soveltuu kohtuullisen hyvin kansalaisten ja viranomaisten väliseen ei-luottamukselliseen asiointiin. Samoin viranomaisten välillä sähköposti soveltuu normaaliin päivittäisasiointiin. Kriittisten ja/tai nopeaa toimintaa edellyttävien sähköpostiviestien perillemeno tulee vahvistaa joko sähköpostiviestin kuittauspyynnöllä tai erillisellä puhelinsoitolla. Luottamuksellisessa asioinnissa tulee sähköisen allekirjoituksen lisäksi käyttää

tapauskohtaisen harkinnan mukaisesti sähköpostiviestin ja/tai sen liitteiden salausta. Sähköinen allekirjoitus varmistaa vastaanottajalle viestin lähettäjän aitouden ja viestin eheyden, viestin ja/tai sen liitteen salaus estää sen sisällön paljastumisen sivullisille.

Sähköpostiasioinnissa on suositeltavaa käyttää organisaatio-osoitetta henkilökohtaisen osoitteen sijasta. (*Valtionhallinnon sähköpostien käsittelyohje*, VAHTI 2/2005)

SANASTO

suomenkielinen termi	englanninkielinen vastine	määritelmä
aikaleima	time stamp	tapahtumatietoon tai viestiin liitetty tieto lähetys-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista Varmennetulla aikaleimalla saadaan aikaan viestin lähettämisen tai vastaanottamisen **kiistämättömyys**
allekirjoitus	signature	asiakirjaan, viestiin tai muuhun tekstiin liitetty henkilön omakätinen nimikirjoitus tai muu tieto, jonka vain kyseinen henkilö on voinut tuottaa, osoituksena siitä, että teksti vastaa hänen tahtoaan tai aikomustaan
anonyymikäyttö	anonymous use	tietoverkon käyttö, jossa **käyttäjän** henkilöllisyyttä ei **tunnisteta**
biotunnistus; biotunnistaminen	biometric identification	ihmisen fyysiseen ominaisuuteen (esimerkiksi kasvojen muoto, sormenjälki, kämmenen verisuonisto, ääni tai silmän iiris) perustuva **tunnistus**
digitaalinen allekirjoitus	digital signature	**sähköinen allekirjoitus**, jonka tuottamiseen on käytetty **varmennetta** Viestiin tai asiakirjaan liitetty digitaalinen allekirjoitus yksilöi lähettäjän ja on todiste viestin ja lähettäjän aitoudesta, ja yleensä myös viestin eheydestä
eväste	cookie	web-palvelimesta verkkoaseman web-selaimeen palvelimen lähettämä tietue, jonka avulla palvelin ja selain voivat pysyä yhteydessä toisiinsa, vaikka fyysinen yhteys välillä katkeaisikin Evästeissä käytettävät tiedot vaihtelevat web-palvelinkohtaisesti, mutta tyypillisiä evästeissä välitettäviä tietoja ovat personointi- ja pääsynvalvontatiedot.
haastemenetelmä haaste-vaste -menetelmä;	challenge-response method	**todennuksen** menetelmä, jossa kutsuttu palvelin tai viestin saaja pyrkii varmistumaan kutsujan tai lähettäjän aitoudesta ottamalla tähän uuden yhteyden tai esittämällä tälle kysymyksen, johon vain oikea taho voi vastata oikein
henkilökohtainen tunnusluku	personal identification number; PIN	ks. **tunnusluku**
henkilötunnus (HETU)	person identification number	luonnollisen henkilön pysyvästi yksilöivä tunnus Tunnus voi olla pysyvä, jos se ei sisällä muuttuvaa tietoa henkilöstä. Suomen henkilötunnus sisältää tiedon syntymäajasta ja sukupuolesta, jolloin, jos sukupuoli vaihtuu, henkilötunnus joudutaan vaihtamaan

suomenkielinen termi	englanninkielinen vastine	määritelmä
henkilövarmenne	personal certificate	vahvistaa yksityisen henkilön henkilöllisyyden
identiteetti	identity	joukko ominaisuuksia, jotka kuvaavat **käyttäjää** ja joiden avulla **käyttäjä** voidaan **tunnistaa**
kansalais-varmenne		kansalaisvarmenteilla tarkoitetaan esimerkiksi poliisin myöntämällä henkilökortilla tai vastaavan turvatason tarjoamalla kortilla olevia Väestörekisterikeskuksen myöntämiä **varmenteita** Kansalaisvarmenne on sijoitettavissa myös muille korteille, esimerkiksi pankkien maksukorteille tai matkapuhelimessa olevalle liittymäkortille (SIM)
KATSO		Katso-organisaatiotunnistus ja valtuutushallinta on verohallinnon sekä Kelan yhteinen maksuton palvelu organisaatioiden tunnistamiselle viranomaisasioinnissa Katso-tunniste liittyy aina organisaatioon ja se on henkilökohtainen
kertakirjaus: kertakirjautuminen	single sign-on; SSO	menettely, joka mahdollistaa pääsyn useisiin palveluihin samalla **sisäänkirjauksella**
kertatunnus	one-time password	**tunnussana** tai **salasana**, joka kelpaa vain yhtä käyttökertaa varten
kevyt tunnistus	weak identification weak authentication;	kevyellä **tunnistuksella** tarkoitetaan **tunnistamismenetelmää**, jossa **käyttäjän todentaminen** tapahtuu käyttäen vain yhtä seuraavista kolmesta tekijästä (mitä henkilö on, mitä henkilöllä on tiedossaan, mitä henkilöllä on hallussaan).
kiistämättömyys	non-repudiation	tietoverkossa eri menetelmin saatava varmuus siitä, että tietty **käyttäjä** on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi Luovutukseen tai käsiteltäväksi jättämiseen voidaan liittää **aikaleima**, joka todistaa viestin saapumisajankohdan.
käyttäjä	user; principal (Liberty Alliance)	tietojärjestelmäpalveluja käyttävä henkilö, ryhmä tai ohjelmisto
käyttäjäidentiteetti	user identity; principal identity (Liberty Alliance)	**käyttäjätilin** yksilöivä **käyttäjän** ilmentymä verkkopalvelussa
laatuvarmenne	quality certificate	laatuvarmenne täyttää **sähköisistä allekirjoituksista** annetussa laissa säädetyt vaatimukset ja sen on myöntänyt säädetyt vaatimukset täyttävä **varmentaja**
luotettu taho; luotettu kolmas osapuoli	trusted (third) party; TTP	taho, johon viestinnän varsinaiset osapuolet tai järjestelmän käyttäjät luottavat Esimerkiksi viranomainen tai yritys voi luotettuna kolmantena osapuolena **todentaa** asioinnin osapuolet tai jonkun osapuolista. Vrt. **todentaminen**.
mobiilitunnista-minen	mobile identification	matkapuhelimen SIM-kortin avulla tapahtuva **tunnistaminen** Tunnistaminen voi tapahtua muutamaa vaihtoehtoista tekniikkaa käyttäen: – tunnistetaan matkapuhelinliittymä puhelinsoiton tai lähetetyn tekstiviestin perusteella – tunnistetaan SIM-kortilla oleva tai siihen liitetty **varmenne**
nimimerkki	pseudonym	käyttäjäidentiteetti, joka ei välttämättä paljasta käyttäjän todellista identiteettiä

suomenkielinen termi	**englanninkielinen vastine**	**määritelmä**
organisaatio-varmenne	organisation certificate	organisaatiolle luotu **varmenne**, jonka avulla voidaan osoittaa, että **käyttäjä** kuuluu organisaatioon ja jossa voidaan kertoa lisätietoja hänen roolistaan ja valtuuksistaan
palvelinvarmenne	server certificate	palvelimelle myönnetty **varmenne**, jonka avulla **käyttäjä** voi varmistua siitä, asioiko oikean palvelimen kanssa
palvelujärjestelmä	service system	tietojärjestelmä, joka tarjoaa käyttäjille sovelluspalveluja
palveluntarjoaja; palveluntuottaja	service provider	**palvelujärjestelmän** omistaja ja ylläpitäjä
PIN-koodi; PIN	PIN code; PIN	ks. **tunnusluku**
rekisteröinti	registration	prosessi, jossa **käyttäjälle** perustetaan **käyttäjäidentiteetti** ja annetaan siihen liittyvät **tunnistetiedot** ja **-välineet**
roolivarmenne	role certificate	vahvistaa sekä henkilön henkilöllisyyden että oikeuden toimia jossakin roolissa kuten tietyssä työtehtävässä
salalause	passphrase	yleensä kielen sanoista muodostettu lause, jota käytetään **salasanana**
salasana	password	vain **käyttäjän** tiedossa oleva merkkijono, jonka avulla tietojärjestelmä voi **todentaa käyttäjän tunnistuksen**
salasanatunnistus	password identification	**tunnistus** ja **todennus salasanan** perusteella
SAML; Security Assertions Markup Language		XML-pohjaisia standardeja kehittävän OASIS-standardointijärjestön standardi, jossa määritellään tapa välittää järjestelmien välillä **tunnistamis-** ja **todentamis**tietoja
sirukortti; toimikortti; älykortti	chip card; smart card	mikropiirin sisältävä kortti Sirukortti voi olla vain muistia sisältävä muistikortti tai prosessorikortti, joka voi sisältää muistin lisäksi erilaisia sovelluksia. Sirukortti toimii vain erityisen lukulaitteen yhteydessä, joka voi olla irrallinen tai kytkettynä esimerkiksi tietokoneeseen, verkko-asemaan tai puhelimeen. Kortin käyttö vaihtelee siihen ohjelmoitujen toimintojen mukaan. **Sähköinen allekirjoitus** edellyttää salausprosessorin sisältävää sirukorttia.
sisäänkirjaus; sisäänkirjautuminen	log-in; login; sign-on	**käyttäjän** ilmoittautuminen järjestelmään käytön aloittamiseksi
sähköinen allekirjoitus	electronic signature	sähköisellä allekirjoituksella tarkoitetaan sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan **identiteetin todentamisen** välineenä
sähköinen asiointitunnus (SATU)	electronic client identifier	numeroista ja tarkistusmerkeistä muodostettu tietojoukko, jonka avulla yksilöidään Suomen kansalaiset ja kotikuntalain mukaisesti Suomessa vakituisesti asuvat ulkomaalaiset, jotka on merkitty Väestötietojärjestelmään
sähköinen tunnistus; sähköinen tunnistaminen	electronic identification	**käyttäjän tunnistaminen** ja **todentaminen** tietokoneessa tai tietoverkossa
todennus; todentaminen	authentication; verification	**käyttäjän** aitoudesta varmistuminen halutulla luottamustasolla Todentamisessa nojaudutaan johonkin jota a) käyttäjä tietää, b) käyttäjällä on tai c) käyttäjä on.
todentaa	authenticate; verify	ks. **todennus**

suomenkielinen termi	englanninkielinen vastine	määritelmä
toimikortti	smart card; chip card	ks. **sirukortti**
tunnistaa	identify	ks. **tunnistus**
tunnistaja; tunnistuspalvelu	authenticator	verkkopalvelun komponentti tai osapuoli, joka huolehtii **käyttäjien tunnistamisesta** ja **todentamisesta**
tunnistautuminen	identification	menettely, jossa **käyttäjä** esittää tunnistetietonsa
tunniste; tunnistetiedot	identifier; identification data	tiedot, joiden avulla **käyttäjäidentiteetti** on **tunnistettavissa** ja **todennettavissa**
tunnistus; tunnistaminen	identification	menettely, jolla yksilöidään joku tai jokin, esimerkiksi tietojärjestelmän **käyttäjä** Sähköiseen tunnistamiseen liittyy normaalisti aina myös käyttäjän **todentaminen**. Tunnistaminen voi perustua **tunnistautumiseen** tai olla passiivista tunnistamista, joka ei edellytä tunnistettavalta toimintaa ja jossa tunnistettava ei välttämättä tiedä tulevansa tunnistetuksi.
tunnistus.fi		Tunnistus.fi on Kansaneläkelaitoksen, työministeriön ja verohallinnon yhteinen sähköisen asioinnin tukipalvelu. Palvelu tuottaa luotettavan henkilö- ja organisaatiotunnistuksen
tunnistusväline	token	sähköisen **tunnisteen** käyttämiseen ja suojaamiseen tarkoitettu väline Tunnistusvälineitä ovat esimerkiksi sirukortti tai matkapuhelimen SIM-kortti.
tunnusluku; PIN; PIN-koodi; henkilökohtainen tunnusluku	personal identification number; personal identity number; PIN; PIN code	**salasana**, joka on muodoltaan lyhyt numerosarja Tunnuslukua käytetään yleensä yhdessä jonkin **tunnistusvälineen** kanssa
TUPAS		Tupas on suomalaisten pankkien yhteinen tunnistamispalvelu Tupas-palvelu on Suomen Pankkiyhdistyksen määrittelemä tapa tunnistaa verkkopalvelujen käyttäjiä pankkien verkkopalvelutunnuksilla
vahva tunnistus; vahva tunnistaminen	strong identification	**käyttäjän tunnistaminen käyttäen** vähintään kahta eri todennustapaa Vahvaa tunnistamista on esimerkiksi se, kun pankkikortilla maksettaessa maksajalta vaaditaan sekä pankkikorttia että siihen liittyvän **tunnusluvun** tietämistä.
varmenne	certificate	sähköinen todistus, jolla vahvistetaan, että todistuksen haltija on tietty henkilö, organisaatio tai järjestelmä Varmenne on yleensä ulkopuolisen **varmentajan** myöntämä. Varmenne voi sisältää muun muassa **käyttäjän** julkisen avaimen, henkilötiedot, varmenteen voimassaolopäiväyksen sekä varmenteen myöntäjän **sähköisen allekirjoituksen**.
varmentaja	certification authority	taho joka myöntää **varmenteen**

suomenkielinen termi	englanninkielinen vastine	määritelmä
varmentaminen	certification	julkisen avaimen todistaminen tietylle **käyttäjälle** kuuluvaksi liittämällä siihen **varmenne** Varmentamistoimintaa Suomessa säätelee laki **sähköisistä allekirjoituksista** (14/2003).
Vetuma-palvelu		kansalaisille tarkoitettu verkkotunnistus- ja maksamisjärjestelmä, joka mahdollistaa yhtenäisen tunnistautumisen ja verkkomaksamisen kaikkiin järjestelmään liitettyihin julkishallinnon tarjoamiin kansalaisten asiointipalveluihin
virkakortti		Valtion- ja kunnallishallinnon sähköisessä asioinnissa virkamiesten, viranhaltijoiden tai vastaavien tunnistamiseen, salaukseen ja sähköisen allekirjoituksen tuottamiseen käytettävä asiointikortti
älykortti	smart card; chip card	ks. **sirukortti**

LIITE 2: VOIMASSA OLEVAT VAHTI-JULKAISUT

VAHTI 12/2006 Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006 Tietoturvakouluttajan opas
VAHTI 10/2006 Henkilöstön tietoturvaohje
VAHTI 9/2006 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006 Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006 Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006 Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006 Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006 Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006 Electronic-mail Handling Instruction for State Government
VAHTI 1/2006 VAHTIn toimintakertomus vuodelta 2005
VAHTI 3/2005 Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005 Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005 Information Security and Management by Results
VAHTI 5/2004 Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004 Datasäkerhet och resultatstyrning
VAHTI 3/2004 Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004 Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004 Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 7/2003 Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 5/2003 Datasäkerhetsanvisning för användaren
VAHTI 5/2003 User´s Information Security Instruction

VAHTI 4/2003 Valtionhallinnon tietoturvakäsitteistö
VAHTI 3/2003 Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003 Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003 Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002 Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002 Etätyön tietoturvaohje
VAHTI 1/2002 Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001 Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001 Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2001 Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001 Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001 Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 3/2000 Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000 Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta (*www.vm.fi/vahti*) ja ohjeita saa myös tilattua painotalo Editasta.

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

12/2006
TUNNISTAMINEN JULKISHALLINNON VERKKOPALVELUISSA

ISBN 951-804-668-9 (nid.)
ISBN 951-804-669-7 (PDF)
ISSN 1455-2566