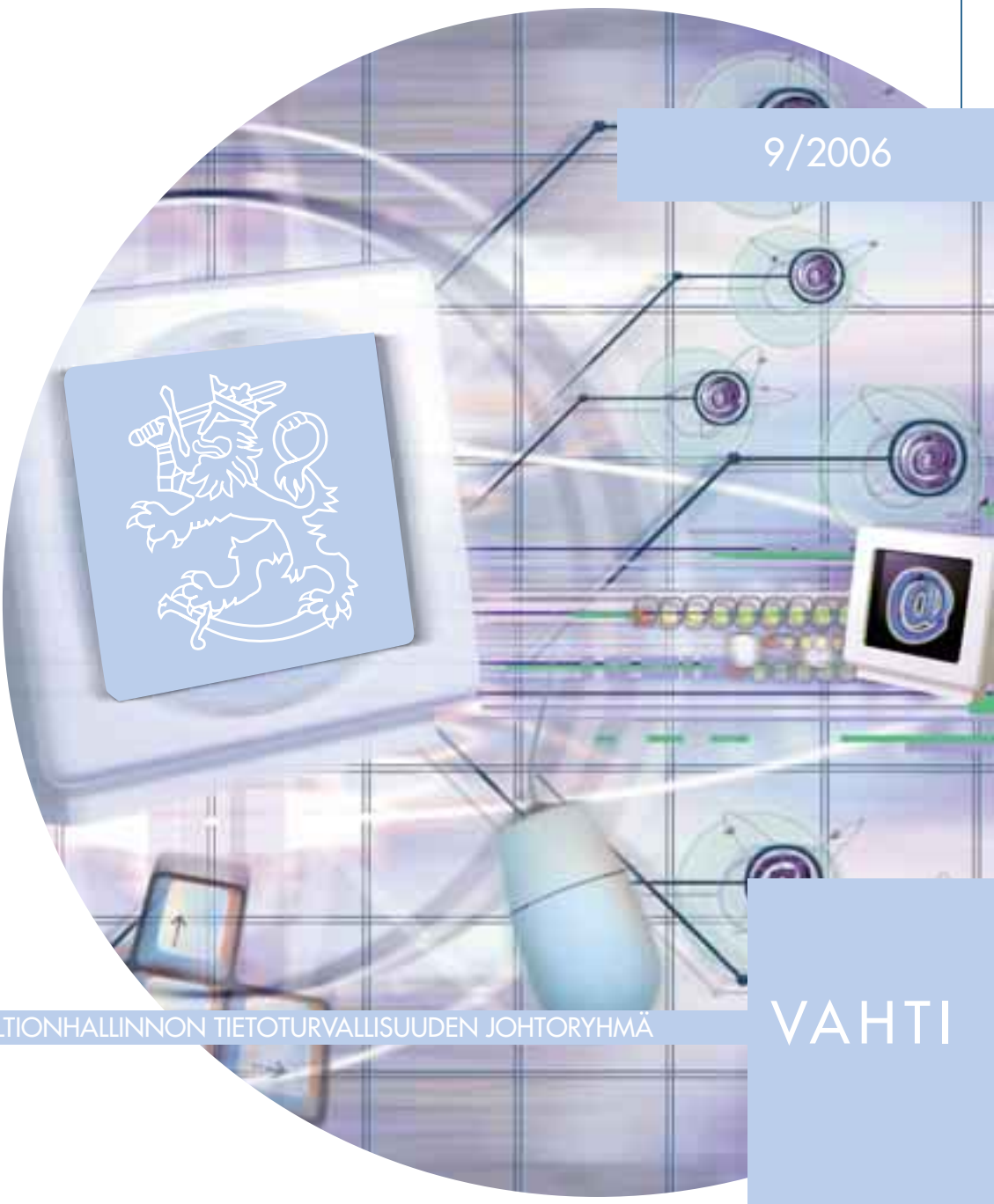
VALTIOVARAINMINISTERIÖ

KÄYTTÖVALTUUSHALLINNON PERIAATTEET JA HYVÄT KÄYTÄNNÖT



9/2006

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

KÄYTTÖVALTUUSHALLINNON PERIAATTEET JA HYVÄT KÄYTÄNNÖT

9/2006

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
Sähköposti:
asiakaspalvelu.prima@edita.fi
Puh. (09) 160 33287

ISSN 1455-2566
ISBN 951-662-X (nid.)
ISBN 951-804-663-8 (pdf)

Edita Prima Oy
HELSINKI 2006

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 37/01/2006

OHJE
22.11.2006

Ministeriöille, virastoille ja laitoksille

KÄYTTÖVALTUUSHALLINNON PERIAATTEET JA HYVÄT KÄYTÄNNÖT

Valtiovarainministeriön ohessa antaman tietoturvaohjeen (jäljempänä ohje) tavoitteena on kehittää käyttövaltuuksien hallintaa ja luoda perusta hyvän käyttövaltuushallinnon toteutukselle. Ohje on laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI ohjauksessa ja alaisuudessa osana valtion tietoturvallisuuden kehitysohjelmaa (VAHTI-julkaisu 1/2004) ja se täydentää laajaa VAHTI-ohjeistoa.

Ohje on tarkoitettu organisaatioiden johdolle, tietoturvavastaaville, henkilöstö- ja tietohallinnosta vastaaville sekä tietojärjestelmien omistajille ja niiden toiminnasta vastaaville. Ohjeessa kuvataan hyvän käyttövaltuushallinnon edellytykset ja hyvää hallintokäytäntöä tukevan käyttövaltuuksien hallintaympäristön arkkitehtuuri. Laaja-alainen ja jatkuva tietoturvatyö on hyvän käyttövaltuushallinnon keskeinen edellytys.

Organisaation tulee huolehtia käyttöoikeuksien hallinnoinnista sekä määritellä käyttövaltuushallinnon periaatteet. Jokaisen organisaation käytössä olevan tietojärjestelmän, sovelluksen ja henkilörekisterin osalta tulee määritellä ja hallinnoida järjestelmän käyttöön oikeutetut henkilöt, käyttöoikeuden sisältö ja laajuus sekä käyttöoikeuden päättyminen.

Vastuu käyttövaltuuksien periaatteiden määrittelystä on organisaation johdolla, jonka tehtävänä on nimetä käytännön käyttövaltuushallinnosta vastaavat henkilöt, määritellä heidän tehtävänsä sekä järjestää toiminnan edellyttämät resurssit, ratkaisut ja seuranta.

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

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää, erityisasiantuntija Olli-Pekka Rissanen ja neuvotteleva virkamies, VAHTIn puheenjohtaja Mikael Kiviniemi (sähköpostit: etunimi.sukunimi@vm.fi).

Toinen valtiovarainministeri — Ulla-Maj Wideroos

Neuvotteleva virkamies — Mikael Kiviniemi

Liite Käyttövaltuushallinnon periaatteet ja hyvät käytännöt (VAHTI 9/2006)

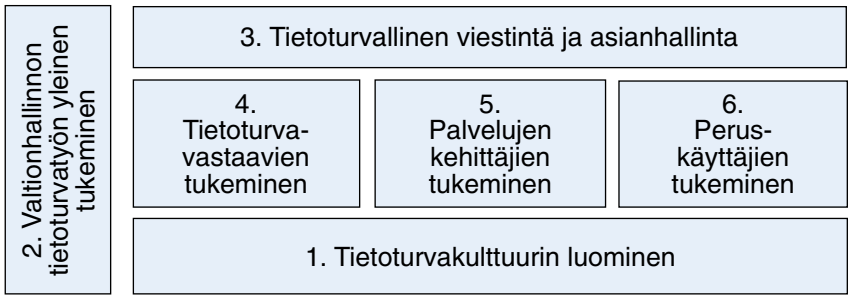
ESIPUHE

Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset ja toimenpiteet. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on tunnettu muun muassa tietoturvajulkaisuista ja –ohjeista sekä tietoturvahankkeistaan (www.vm.fi/vahti).

Valtion tietoturvallisuuden kehitysohjelma on julkaistu VAHTI-julkaisusarjassa nimellä Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006, VAHTI 1/2004. Kehitysohjelmalla kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Kehitysohjelmaan sisältyy kaikkiaan 29 laajaa kehittämiskohdetta, joista osaa toimeenpannaan työryhmien tai jaostojen valmistelussa ja osaa muilla toimenpiteillä. Kehitysohjelmaan osallistuvat laajasti kaikki hallinnonalat ja lisäksi osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä ulkopuolisia asiantuntijoita. Virallisesti asetetut hankkeet löytyvät valtioneuvoston hankerekisteristä (http://www.hare.vn.fi/) VAHTIn (VM166:00/2003) alahankkeina. Seuraavassa kuvassa on esitettyinä kehitysohjelman osa-alueet.

Kaavio valtion tietoturvallisuuden kehitysohjelmasta ja sen hankealueista



Tämän ohjeen on laatinut VAHTIn alainen tunnistaminen ja käyttövaltuushallinta- ryhmä osana valtion tietoturvallisuuden kehitysohjelmaa. Ohjeessa on otettu huomioon laajan lausuntokierroksen kommentit 2006. Ohjeen julkaisemisesta päätettiin VAHTIn kokouksessa lokakuussa 2006.

Sisällysluettelo

1 JOHDANTO

1.1 Ohjeen tarkoitus ja kohderyhmä

Tämän ohjeen tarkoituksena on luoda perusta hyvän käyttövaltuushallinnon toteutukselle. Siinä kuvataan ne periaatteet ja käytännöt, joita tarvitaan käyttövaltuushallinnon menettelyjä suunniteltaessa ja käyttöön otettaessa.

Ohje on tarkoitettu organisaatioiden johdolle, henkilöstö- ja tietohallinnosta vastaaville sekä tietojärjestelmien omistajille ja niiden toiminnasta vastaaville.

Tässä ohjeessa keskitytään käyttövaltuushallinnon periaatteisiin erityisesti isoja tietojärjestelmiä käyttävien organisaatioiden kannalta. Ohjeessa käsitellään organisaation sisäisen käyttäjätiedon hallintaa. Organisaatiorajat ylittävään käyttäjätietojen hallintaan on olemassa vaihtoehtoisia tapoja, mutta ne ovat vielä kehitysvaiheessa ja osin vakiintumattomia. Erilaisia toteutustapoja ei ole kuvattu tässä ohjeessa, mutta liitteessä 1 on kuvattu yksi tapa toteuttaa organisaatiorajat ylittäviä käyttövaltuuksia.

Käyttövaltuuksien hallinnointi muodostuu sitä haastavammaksi tehtäväksi, mitä isompi organisaatio on ja erityisesti mitä enemmän järjestelmiä sillä on käytössään. Vaativuus lisääntyy vielä, jos tietojärjestelmiä ylläpitää ulkopuolinen palvelujen tuottaja toimeksiantosopimuksen perusteella. Uudenlainen näkökulma käyttövaltuushallintoon liittyy, jos tietojärjestelmien tietoja luovutetaan esimerkiksi katseluoikeuksien avulla toisen organisaation palveluksessa olevalle henkilölle.

Ohjeen luvussa 1 käsitellään nykytilaa ja siihen liittyviä ongelmia, luku 2 käsittelee käyttövaltuushallinnon lainsäädännöllistä perustaa, luvussa 3 esitetään hyvän käyttövaltuushallinnon edellytykset, luvussa 4 käyttövaltuushallinnon arkkitehtuuria ja luku 5 esittelee käyttöönottoon liittyviä suosituksia. Liitteinä ovat esimerkki organisaatiorajat ylittävästä käytöstä, rekisteriselostemallit, aihepiirin käsitteitä ja terminologiaa yhteen vetävä sanasto sekä lähdeluettelo ja lista voimassaolevista VAHTI-julkaisuista.

1.2 Nykytilan ongelmia

Perinteinen, nykyään vallitseva tapa hoitaa käyttövaltuushallintoa perustuu löyhästi määriteltyihin hallintaprosesseihin ja vastuisiin. Toiminnoista ja niihin liittyvistä järjestelmistä

ja tiedoista substanssivastuussa olevat hallintoyksiköt ovat usein käytännössä delegoineet käyttövaltuushallinnon ja jopa niihin liittyvän omistajanvastuunsa täysin tietohallinnolle. Käyttövaltuuksien myöntämistä ei kontrolloida asianmukaisesti, vaan henkilöille saatetaan antaa ”varmuuden vuoksi” tarpeettoman laajat käyttövaltuudet. Palveluksesta poistuneiden tai toisiin tehtäviin siirtyneiden henkilöiden vanhat käyttövaltuudet saattavat jäädä voimaan vuosikausiksi, kun hallintaprosessit ovat tältä osin puutteelliset ja kun voimassa olevien valtuuksien asianmukaisuutta ei valvota. Käytännössä tämä johtaa tilanteeseen, jossa riskit vakaville väärinkäytöksille kasvavat vähitellen merkittäviksi.

Hallinnollisen epämääräisyyden ja siitä johtuvien riskien lisäksi perinteinen käyttövaltuushallinto on erittäin työvaltainen ja virhealtis, kun valtuushallinnon tapahtumat tehdään käsityönä monilukuisen järjestelmävastaavien joukon toimesta. Valtuuksien myöntämis-, muutos- ja poistotapahtumista sekä niiden alullepanijoista ja hyväksyjistä ei useinkaan jää kunnollisia dokumentteja, joiden avulla tekijät voitaisiin jäljittää ongelmatilanteissa tai riskien toteutuessa.

Liikkeelle lähdetään organisaatioille välttämättömien periaatteellisten ja toiminnallisten valmiuksien luomisesta. Sen jälkeen kuvataan suositeltavaa hallintokäytäntöä tukevan hallintajärjestelmän toiminnallinen arkkitehtuuri sekä annetaan joitain järjestelmän hankintaan ja käyttöönottoon liittyviä suosituksia.

	Organisaation johto	Henkilöstö-hallinnosta vastaava	Tieto-hallinnosta vastaava	Tieto-järjestelmän omistaja	Tieto-järjestelmästä vastaava
Luku 1	x	x	x	x	x
Luku 2	x	x	x	x	x
Luku 3	x	x	x	x	x
• 3.1	x	x	x	x	x
• 3.2	x	x	x	x	
• 3.3			(x)	x	
• 3.4	x		(x)	x	x
• 3.5				x	x
• 3.6		x	(x)	x	x
• 3.7			(x)	x	x
• 3.8		(x)	(x)	x	x
• 3.9	x	(x)	x	x	x
• 3.10		x	x	x	x
• 3.11			x	x	x
Luku 4		x	x	x	x
Luku 5	x	x	x	x	x

Taulukko 1.1 Lukuohje tähän ohjeeseen. Rasti ruudussa tarkoittaa ”Luettava”, suluissa oleva rasti ”Suositellaan luettavaksi”.

2 TIETOTURVALLISUUS JA LAINSÄÄDÄNTÖ

Jokaisen organisaation tulee huolehtia käyttöoikeuksien hallinnoinnista sekä siihen liittyen määritellä käyttövaltuushallinnon periaatteet. Jokaisen organisaation käytössä olevan tietojärjestelmän, sovelluksen ja henkilörekisterin osalta tulee määritellä myös ne henkilöt, joilla on oikeus käyttää ko. tietojärjestelmää, tieto siitä, mitä käyttöoikeudet sisältävät, sekä milloin käyttöoikeus päättyy.

Organisaatiossa tulee olla myös määriteltyinä asiaan liittyvät vastuut; kuka käyttöoikeudet eri järjestelmiin myöntää, sekä ketkä vastaavat oikeuksien ajan tasalla pidosta. Työ- tai palvelussuhteen päätyttyä käyttöoikeudet tulee poistaa välittömästi. Vastuu käyttövaltuushallinnon periaatteiden määrittelystä on johdolla, jonka asiana on nimetä käytännön toiminnasta vastaavat henkilöt ja määritellä heidän tehtävänsä.

Vastuiden määrittely tehdään organisaatiokohtaisesti. Käyttöoikeuksien myöntäminen on kuitenkin aina sidoksissa myös palvelussuhteeseen ja siihen liittyvään tehtävänkuvaukseen. Sen voidaan siten katsoa kuuluvan henkilöstöhallinnon tehtäviin. Käytännössä vastuu on usein jaettu asianomaiselle toiminnalliselle yksikölle ja käyttöoikeuden toteuttaa yleensä kunkin järjestelmän pääkäyttäjä. On tärkeää, että organisaatiossa on määritelty ja koordinoitu ko. tehtävien hoito siten, että käyttöoikeuksien hallinnointi tulee aukottomasti hoidettua.

2.1 Käyttövaltuushallintoa koskeva lainsäädäntö

Laki viranomaisten toiminnan julkisuudesta (Julkisuuslaki, 621/1999) sääntelee hyvän tiedonhallinnan vaatimuksesta, jota täsmennetään lain nojalla annetussa asetuksessa. Asetuksen uusiminen on parhaillaan käynnissä.

Henkilötietojen käsittelyä sääntelevä henkilötietolaki (523/1999) edellyttää henkilötietojen suojaamista, tietojen tarpeellisuus- ja virheettömyysvaatimuksen, sekä käyttötarkoitussidonnaisuuden vaatimuksen huomioon ottamista. Lisäksi käsittelyssä tulee ottaa huo-

mioon muutkin henkilötietolain henkilötietojen käsittelyä koskevat vaatimukset.

Kaikkien em. vaatimusten noudattaminen ja noudattamisen valvonta ja siten suojaamisvelvoitteesta huolehtinen edellyttää, että käyttöoikeudet eri järjestelmiin on määritelty asianmukaisesti ja että käyttöä voidaan myös jälkikäteen valvoa. Käytännössä se merkitsee, että käyttöoikeudet ja niiden sisältö on määriteltävä henkilötasolla.

2.2 Käyttövaltuusrekisterin suunnitteluvaatimus

Käyttövaltuuksista muodostuu henkilötietolain tarkoittama henkilörekisteri, jonka tietojen käsittelyssä tulee ottaa huomioon henkilötietolain vaatimukset. Käyttäjärekisteriä koskevat siten myös henkilötietolain suojaamis- ja huolellisuusvelvoitteet.

Käyttövaltuusrekisteri on suunniteltava etukäteen, jossa yhteydessä on kuvattava

- sen käyttötarkoitus
- sen tietosisältö
- mistä tiedot säännönmukaisesti hankitaan
- mihin niitä säännönmukaisesti luovutetaan
- millä tavalla ja miten pitkään rekisteritietoja säilytetään
- miten ne hävitetään
- miten tarpeellisuusvaatimus huomioidaan
- miten huolehditaan tietojen virheettömyydestä ja ajan tasalla pidosta
- miten huolehditaan henkilöiden informoinnista
- miten huolehditaan tarkastusoikeudesta ja virheellisen tiedon oikaisusta

Jokaisesta eri käyttötarkoitukseen perustetusta henkilörekisteristä tulee laatia rekisteriseloste. Samaan rekisteriselosteen voidaan merkitä organisaation omassa käytössä olevien tietojärjestelmien ja henkilörekisterien käyttäjäoikeudet. Tällöin rekisteriselosteesta tulee ilmetä, että käyttöoikeudet määritellään erikseen eri tietojärjestelmiin ja eri henkilörekistereihin. Nämä on tarpeen eritellä rekisteriselosteessa. Mallit rekisteriselosteesta (tietosuojaselosteesta) ovat tämän ohjeen liitteinä 2 ja 3. Lisätietoja asiasta saa Tietosuojavaltuutetun toimiston sivuilta.

Silloin kun järjestelmän käytöstä jää merkintä siitä, kuka ko. järjestelmää tai sen tietoja on käyttänyt, myös nämä lokit muodostavat henkilörekisterin, josta tulee myös laatia rekisteriseloste.

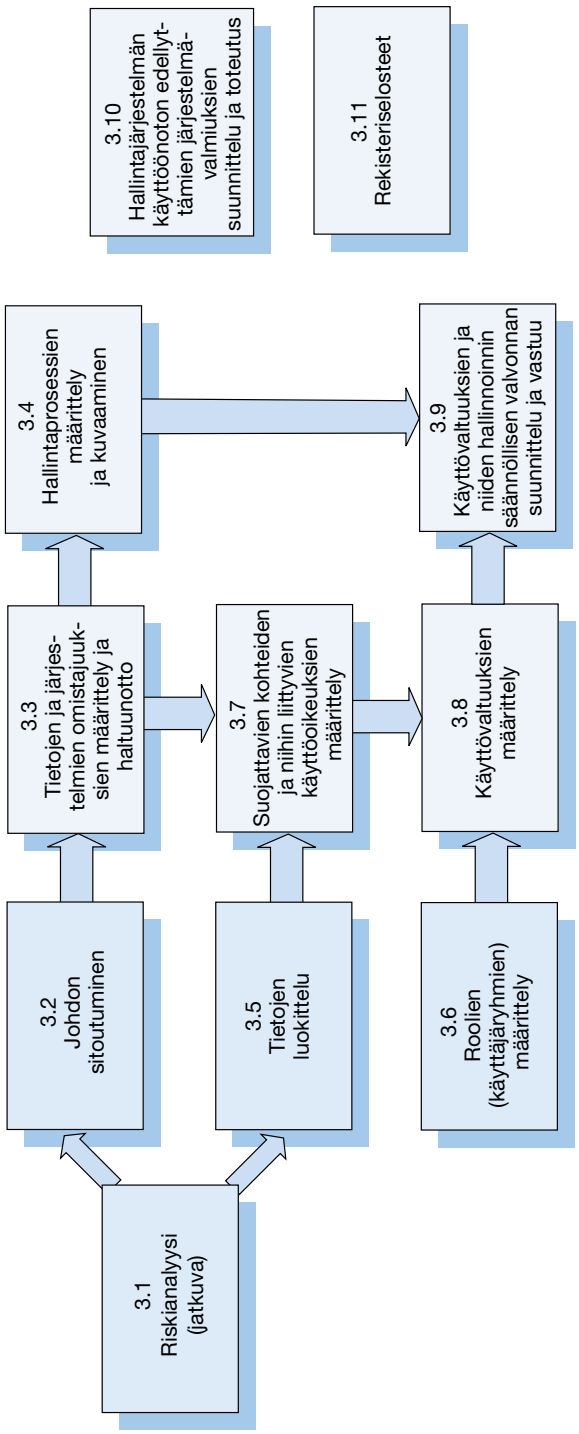
Rekisteriselosteet tulee pitää kaikkien rekisteröityjen saatavilla.

3 HYVÄN KÄYTTÖVALTUUSHALLINNON EDELLYTYSTEN LUOMINEN

Hyvän käyttövaltuushallinnon edellytyksenä on, että organisaation tietoturvallisuudesta huolehditaan asianmukaisesti. Tietoturvallisuuden hallintajärjestelmän perusdokumentti on organisaation johdon määrittelemä ja läpi organisaation jalkautettu tietoturvapolitiikka. Tietoturvapolitiikan mallina voidaan käyttää esimerkiksi ISO 17799 standardin mukaista politiikkaa.

Kuvassa 1 esitetään kaavion muodossa toimenpiteet, joiden läpivieminen on välttämätön edellytys hyvin toimivalle käyttövaltuushallinnolle. Toimenpiteet on numeroitu sen kohdan mukaan, missä ne tässä luvussa esitellään.

Osa kaaviossa esitetyistä toimenpiteitä on hyvän tiedonhallintatavan ja tietoaineistojen käsittelystä annettujen ohjeiden mukaisia perusvalmiuksia, joiden tulisi olla lähtökohtaisesti kunnossa organisaatioissa. Käytännössä valmiudet eivät silti useinkaan ole riittävät, joten käyttövaltuushallinnon kehittämistä suunniteltaessa on syytä vähintään tarkistaa, että kuvassa 1 näkyvien toimenpiteiden avulla luotavat valmiudet ovat olemassa ja ajan tasalla. Ilman kunnossa olevia perusvalmiuksia, kuten riskianalyysia, tietojen luokittelua tai tietojen ja järjestelmien omistajuuksien määrittelyä, käyttövaltuushallinto ei seiso vakaalla pohjalla.



Kuva 1 Hyvän käyttövaltuushallinnon edellytysten luomisessa tarvittavat toimenpiteet

3.1 Riskianalyysi

Johdolla tulee olla oikea kuva organisaation toimintaan kohdistuvista tietoriskeistä ja tietoturvallisuuden tasosta. Toimintaan ja palvelujen tietoturvallisuuteen kohdistuvien riskien arviointiin tarvitaan järjestelmällinen riskianalyysimenettely. Riskianalyysin tarkoituksena on (VAHTI 1/2001, kohta 4.3.1, s. 25):

- Selvittää toiminnan ja palvelujen tietoturvatarpeet ja vaatimukset
- Arvioida ulkoiset ja sisäiset riskit
- Selvittää säädöksistä ja määräyksistä johtuvat vaatimukset
- Arvioida toiminnan ja tietotekniikan muutoksien vaikutukset tietoturvallisuuteen
- Selvittää sidosryhmien odotukset
- Edellä mainittujen perusteella määritellä tietoturvallisuuden tarpeet, periaatteet ja toteutustapa.

Listan viimeisen kohdan mukaisesti myös käyttövaltuushallinnon tarpeet, periaatteet ja toteutustapa tulee viime kädessä johtaa riskianalyysin tuloksista.

Riskianalyysi ei ole kertatoimenpide, vaan se on toistettava säännöllisesti tai/ja tehtävä suurten organisaatiota tai sen toimintaympäristöä koskevien muutosten yhteydessä. Riskianalyysissä tunnistetaan suojattavat kohteet sekä määritellään riskien hyväksyttävä taso ja sen pohjalta tarvittavat suojaustasot, luottamuksellisuus-, eheys- ja käytettävyysvaatimukset.

3.2 Johdon sitoutuminen

Tietoturvallisuus on osa organisaation johtamistoimintaa. Jokaisen organisaatiotason tehtävänä on huolehtia oman organisaationsa toiminnan ja hankkimiensa palvelujen tietoturvallisuudesta, määritellä tarvittavat periaatteet sekä laatia ja antaa tarvittavat ohjeet. Tietoturvaratkaisujen valinnassa tulee riskianalyysien perusteella ottaa huomioon ratkaisujen taloudellisuus ja tarkoituksenmukaisuus. Ylimmän johdon päätöksiä tarvitaan erityisesti silloin, kun ratkaisut on valittava taloudellisuusvaatimuksista poiketen (VAHTI 1/2001, s. 8). Linjajohdon on tarpeellista omaksua riskienhallinnan toimintamallit ja viedä ajattelua eteenpäin kaikilla organisaatiotasoilla. Riskienhallinta ei toimi riittävän tehokkaasti, jos se jätetään vain riskienhallinnan ammattilaisten hoidettavaksi.

Organisaation johdon on ymmärrettävä riskianalyysin tulokset ja otettava vastuu valitusta riskitasosta. Johdon on myös huolehdittava, että suojausten edellyttämät organisaation toimintaprosessit ja tekniset järjestelmät toimivat niiltä edellytettävällä tavalla. Huolehtiminen ei tarkoita ainoastaan toimeenpanon valvontaa vaan myös sitä, että toiminnalle, kuten tässä tapauksessa käyttövaltuushallinnolle, on osoitettu resurssit, jotka mahdollistavat siltä edellytettyjen tehtävien hoidon.

3.3 Tietojen ja järjestelmien omistajuuksien määrittely ja haltuunotto

Hyvän tiedonhallintatavan asettama perusvaatimus on, että kaikilla organisaation tiedoilla ja tietoja hallinnoivilla järjestelmillä on vastuullinen omistaja. Omistaja on yksikkö, jonka toimintaan tiedot lähinnä liittyvät tai/ja jonka toimintaa tiedot ensisijaisesti tukevat ja/tai jonka vastuulle ao. prosessi kuuluu ja joka käyttää niihin liittyvää määräysvaltaa. Tietojen (ja järjestelmän) omistajan vastuulla on riskianalyysiin perustuva tietojen suojaamistarpeen määrittely sekä suojausten ja niihin liittyvien kontrollien toimeenpano. Toimeenpanoon liittyvät tekniset seikat voidaan delegoida tietohallinnolle, mutta vastuu ja valvontavelvollisuus eivät ole delegoitavissa.

Käyttövaltuushallinnon tapauksessa tietojen omistajan velvollisuutena on päättää ja valvoa, ketkä ja millä ehdoilla pääsevät tietoihin ja niitä hallinnoiviin järjestelmiin käsiksi. Omistaja määrittelee tietoihin liittyvät käyttöoikeudet ja käyttäjäroolit, joille voidaan myöntää valtuus tietojen käyttöön. Omistaja ottaa kantaa myös siihen millainen on prosessi, jolla käyttövaltuuksia hallinnoidaan. Omistajalla tulee olla ajan tasalla oleva luettelo tietojensa käyttövaltuuksien haltijoista, ja omistajan tulee huolehtia säännöllisistä tietojen ja niihin liittyvien käyttövaltuuksien käytön auditoinneista.

3.4 Hallintaprosessien määrittely ja kuvaaminen

Käyttövaltuushallinnon hallintaprosesseilla tarkoitetaan toimintoja, jotka liittyvät tietojärjestelmien käyttäjä- ja käyttöoikeustietojen sekä käyttövaltuuksien ylläpitoon.

Organisaatiolla tulee olla olemassa käyttövaltuuksien hallintapolitiikka, jossa määritellään organisaation käyttövaltuusperiaatteet ja toimintatavat. Tämä politiikka on osa organisaation tietoturvapolitiikkaa.

Prosessit tulee suunnitella niin, että ne kattavat aukottomasti sekä käyttövaltuuksien että suojattavien kohteiden elinkaaret ja ne ovat riittävän turvallisia. Prosesseista tulee ylläpitää ajan tasalla olevia kuvauksia ja ohjeistuksia. Prosesseilla ja niihin liittyvillä hallinnollisilla (tieto-) kohteilla tulee olla nimetyt vastuuhenkilöt. Kaikkien prosesseihin osallistuvien organisaatioyksiköiden ja henkilöiden vastuiden, velvollisuuksien ja valtuuksien tulee olla selkeästi määriteltyjä.

Suojattavien kohteiden omistaja on taho, joka päättää valtuuksien myöntämisestä ja poistamisesta. Omistajan velvollisuutena on siksi myös osallistua myöntämis- ja poistamisprosessien määrittelyyn. Prosessien yleinen toteutustapa ja niihin liittyvät osapuolet on kuitenkin syytä pyrkiä sopimaan mahdollisimman yhdenmukaisiksi koko organisaatiossa.

Prosessien tulee olla jäljitettäviä niin, että kaikkiin lupien myöntämis-, muutos- ja poistamistapahtumiin osalliset ja heidän roolinsa voidaan haluttaessa jälkeenpäin selvit-

tää. Kaikista käyttövaltuuksien muutoksista pitää siten löytyä dokumentti, joka mahdollistaa tapahtumien jäljitettävyyden.

Erityistä huomiota hallintaprosessien toteutuksessa tulee kiinnittää tilanteisiin, joissa käyttäjä poistuu tai hänen työroolinsa muuttuu tavalla, joka vaikuttaa käyttövaltuuksiin. Tällöin on huolehdittava siitä, että poistuneen käyttäjän käyttäjätiedot ja kaikki siihen liittyneet käyttäjätilit ja käyttövaltuudet tai käyttäjän aikaisempaan rooliin liittyvät uutta tilannetta vastaamattomat käyttövaltuudet poistetaan. Vastaavasti tulee huolehtia, että käytöstä poistuneisiin tietoihin/järjestelmiin liittyvät käyttöoikeudet poistetaan. Irrallisiksi jääneet vanhentuneet tiedot rapauttavat järjestelmäympäristöä ja voivat aiheuttaa arvaamattomia tietoturvariskejä.

Parhaiten käyttövaltuushallinnon prosessien määrämuotoisuus- ja jäljitettävyysvaatimukset voidaan täyttää mahdollisimman pitkälle automatisoiduilla hallintaprosesseilla.

3.5 Tietojen luokittelu

Hallinnossa käsiteltävät tiedot tulee luokitella luottamuksellisuutensa suhteen tietoaineistojen käsittelystä annettujen ohjeiden mukaisesti. Tiedon/tietoaineiston luottamuksellisuus sekä riskianalyysissä selvitetty tietojen väärinkäyttöön liittyvien riskien suuruus määrää, mihin luottamuksellisuusluokkaan tieto/tietoaineisto kuuluu. Tietojen suojaustarpeet, eli esimerkiksi tarve rajoittaa tietojen käyttötapoja ja mahdollisia käyttäjiä, ovat lähtökohtaisesti johdettavissa luottamuksellisuusluokittelusta. Tietoaineiston ja joskus jopa yksittäisen tiedon kohdalla voi kuitenkin esiintyä erityisiä, em. luokittelua hienojakoisempia suojaustarpeita, jotka voivat vaikuttaa tietoja koskeviin käyttövaltuuksiin. Tietoaineistojen suojaamista on parhaillaan kehittämissä VAHTIn ryhmä, jonka työn tuloksena luokittelut ja käsittelysäännöt yhdenmukaistetaan kansallisten ja kansainvälisten aineistojen osalta.

Luottamuksellisuus on vain yksi luokittelunäkökulma, tietoja voidaan luokitella myös muilla perusteilla. Henkilötietolain mukaisesti myös tietojen käyttötarkoitus on huomioitava käyttövaltuuksia myönnettäessä.

3.6 Roolien (käyttäjäryhmien) määrittely

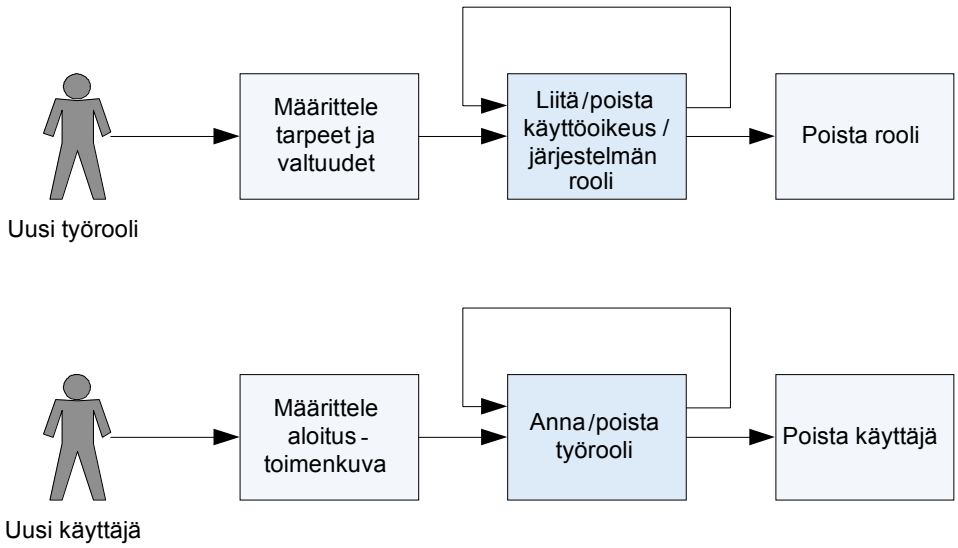
Käyttövaltuuksia määriteltäessä ei ole käytännöllistä eikä järkevää tarkastella käyttäjiä yksilötasolla, vaan tulee pyrkiä löytämään käyttäjäryhmiä, joiden jäsenillä samantyyppiset työtehtävät. Näin ollen heillä on samanlaiset tietotarpeet ja toimintavaltuudet eli samanlainen toiminnallinen rooli, jota tässä kutsutaan työrooliksi.

Perinteisesti käyttövaltuuksia on hoidettu niin, että palvelujärjestelmissä on määritelty joukko erilaisia lupa-/käyttöoikeusyhdistelmiä, joita on kutsuttu ao. järjestelmien käyttäjä-

rooleiksi. Yksittäiset käyttäjät on sitten sijoitettu näihin käyttäjärooleihin. Yksilöiden (ja organisaatioiden) tarpeiden muuttuessa rooleja on jouduttu määrittelemään yhä lisää ja tyypillisesti vielä erikseen kussakin palvelujärjestelmässä, mistä on seurannut jatkuva iso ylläpitotyökuorma palvelujärjestelmien vastuuhenkilöille.

Käyttövaltuushallinnon kannalta tehokkaampaan ja joustavampaan lopputulokseen voidaan päästä erottamalla toisistaan käyttäjien **työroolit** ja palvelujärjestelmien mahdollistamat käyttäjäroolit. Käyttövaltuuksien määrittely (kohta 2.8) tarkoittaa tällöin työroolien kytkemistä järjestelmien rooleihin, mikä on käytännössä yksi suuri kertaponnistus. Sen jälkeen ylläpitotarvetta on ainoastaan tilanteissa, joissa jonkun työroolin sisältö muuttuu tai lanseerataan kokonaan uusi työrooli. Palvelujärjestelmien jatkuva ylläpitotarve korvaantuu näin silloin tällöin esiintyväksi tarpeeksi ylläpitää työrooli / käyttäjärooli -matriisia. Yksittäisen käyttäjän toimenkuvassa tapahtuvat muutokset eivät normaalisti aiheuta muita toimenpiteitä käyttövaltuuksien hallintajärjestelmässä kuin käyttäjän työroolitietojen päivittämisen. Kuva 2 havainnollistaa työroolien ja käyttäjien toimenkuvan ja niihin liittyvien valtuuksien hallinnan elinkaaria.

Edellä kuvattu tapa kuvata työroolien ja järjestelmien roolien väliset riippuvuudet matriisina, on käyttökelpoinen pienissä toimintaympäristöissä. Työroolien ja järjestelmien lukumäärän kasvaessa menettelystä tulee helposti liian raskaasti ylläpidettävä.



Kuva 2 Työroolien ja käyttöoikeuksien elinkaaret

Työrooli on käyttäjäryhmä, jossa on yksi tai useampia jäseniä. Henkilöllä voi olla yksi tai useampia työrooleja. Hän voi esimerkiksi olla 1) organisaatio A:n jäsen, 2) yksikön A1 johtoryhmän jäsen ja 3) projekti P:n jäsen, eli hänellä on kolme työroolia, joihin kaikkiin liittyy ainakin osittain erilaiset tietotarpeet ja toimintavaltuudet. Työroolit ovat jotain, mitä ei voida eikä pidä kytkeä mekaanisesti henkilöiden työnimikkeisiin tai organisaatioihin. Niihin voi myös liittyä sääntöjä, jotka esimerkiksi sitovat roolin vain tiettyihin tilanteisiin. Esimerkiksi toimiessaan henkilön N.N. sijaisen roolissa henkilö M.M. voi käyttää N.N:n valtuuksia vain tietyissä ennalta määrätyissä tilanteissa. Henkilön työroolit voivat olla eri tavoin riippuvaisia toisistaan sekä esim. henkilön työsuhteesta, joka on myös eräänlainen rooli.

Rooleissa ja niiden jäsenyyksissä tapahtuvien muutosten hallinta on kriittinen osa käyttövaltuuksien hallintaa. Käyttövaltuushallinnon prosessit tulee rakentaa niin, että tietojärjestelmien käyttäjien työrooleissa tapahtuvat ja niiden seurauksena tehtävät käyttövaltuuksien muutokset noteerataan ajantasaisesti. Tämä edellyttää kiinteää kytkentää mm. henkilöstöhallinnon järjestelmien ja käyttövaltuuksien hallintajärjestelmän välillä.

Niin kuin tiedoilla ja järjestelmillä myös rooleilla tulee olla omistaja, joka määrittelee roolin, ylläpitää sen sisältöä ja pitää lukua roolissa toimivista käyttäjistä. Hienojakoisimmat työroolit kannattaa määritellä toimintayksikkötasolla, jossa roolin sisältö eli siihen liittyvät tarpeet ja vastuut tunnetaan parhaiten. Karkeampi perusroolitus sen sijaan on syytä tehdä koko organisaation kattavana. Tarpeettomiksi jäävät roolit ja niihin liittyvät käyttövaltuusmääritykset tulee aina poistaa järjestelmistä.

3.7 Suojattavien kohteiden ja niihin liittyvien käyttöoikeuksien määrittely

Käyttövaltuushallinnon viitekehyksessä suojattavia kohteita voivat olla mitkä tahansa tiedot, toiminnot tai fyysiset kohteet, joiden käyttöä halutaan rajoittaa ja valvoa. Yksilöllisesti suojattavia kohteita voi olla tietojärjestelmäarkkitehtuurin kaikilla tasoilla: sovellukset, sovellustoiminnot, tietokannat, tiedostot, tietojoukot ja yksittäiset tiedot ja dokumentit, käyttöliittymät, järjestelmien liittymistavat, erilaiset käyttöjärjestelmä- ja middleware-tason kohteet ja toiminnot.

Suojattavan kohteen omistajan tehtävä on määritellä, millaisia erilaisia käyttöoikeuksia ja niitä mahdollisesti täsmentäviä sääntöjä kohteelle annetaan. Johonkin käyttöoikeuteen voi esimerkiksi liittyä vaatimus, että käyttäjän tulee olla vahvasti tunnistettu, että suojattavan kohteen käyttöä ei sallita yleisen verkon kautta yhteydessä olevalle käyttäjälle, tai että käyttöoikeus on voimassa vain tiettynä aikana tai tietyssä käyttötilanteessa. Erityisesti järjestelmätason pääsyoikeuksia määriteltäessä on pidettävä huolta siitä, että käyttäjäistunnoille määritellään enimmäispituus, millä estetään päiväkausia tai vielä pitempään kestävät istunnot, jotka ovat huomattava tietoturvariski.

Omistaja vastaa siitä, että suojattaviin kohteisiin liittyvät määritykset poistetaan järjestelmistä samalla kun kyseinen suojauksen kohde poistuu käytöstä.

3.8 Käyttövaltuuksien määrittely

Käyttövaltuuksien määrittely tarkoittaa käyttöoikeuksien kytkemistä käyttäjien työrooleihin. Palvelujärjestelmien käyttöoikeudet tai osa niistä saattaa olla koottu joukoksi järjestelmän rooleja, joihin työroolit kytketään siten, että halutut käyttövaltuudet syntyvät. Jos rooleja ei ole määritelty järjestelmään, niin työrooleihin kytketään asianmukaiset yksittäiset käyttöoikeudet.

Tiedon tai muun kohteen omistaja määrittelee ja viime kädessä hyväksyy kenelle ja millä ehdoilla käyttövaltuuksia myönnetään. Hallintajärjestelmässä, jossa käyttövaltuudet ovat työroolikohtaisia, työroolin omistajan tehtävänä on hankkia työroolille sen edellyttämät käyttövaltuudet sopimalla asiasta ao. kohteen omistajien kanssa. Pääperiaatteena työroolin käyttövaltuuksien määrittelyssä tulee pitää todellista tarvetta, ts. rooliin ei tule kiinnittää ”kaiken varalta” laajempia valtuuksia kuin mitä rooli käytännössä edellyttää. Tilapäiset laajemmat tietotarpeet tai muut käsittelyvaltuudet tulee hoitaa käyttäjälle esimerkiksi määräajaksi aktivoitavalla työroolilla, johon on liitetty tarvittavat valtuudet.

Käyttäjän kannalta käyttövaltuuksien määrittely palautuu käyttäjän työroolien ylläpitoon. Organisaatioon liittyessään käyttäjä liitetään aloitustoimenkuvaansa vastaaviin työrooleihin, joiden joukkoa työuran aikana sitten tarpeen mukaan ylläpidetään liittämällä käyttäjä uusiin rooleihin ja/tai irrottamalla käyttäjä entisistä rooleista, jotka eivät enää vastaa hänen uusiutuneen toimenkuvansa tarpeita ja valtuuksia.

Kaikki käyttövaltuuksien muutokset tulee tehdä ennalta määritellyn prosessin mukaisesti niin, että muutokset ovat myöhemmin jäljitettävissä. Työroolin kytkentä palvelujärjestelmän rooliin tai yksittäiseen käyttöoikeuteen edellyttää asianomaisen kohteen omistajan hyväksyntää. Käyttäjän liittäminen työrooliin edellyttää vastaavasti työroolin omistajan hyväksyntää. Jos työrooliin kuuluu käyttövaltuuksia, joihin liittyy erityisehtoja kuten käyttäjän tietynlainen rekisteröintitapa tai tietynlaisten tunnistusvälineiden käyttö, nämä on otettava huomioon kytkettäessä käyttäjää ao. työrooliin.

Työrooleja, joihin liittyy erityisen laajoja käyttövaltuuksia (esim. pääkäyttäjän tai järjestelmävastaavan oikeudet, käyttöjärjestelmä- ja middleware-tason käyttöoikeudet), tulee myöntää erityisen harkitusti ja niihin tulee liittää erityisehtoja kuten käyttäjän vahva tunnistaminen. Työrooleja tai työroolien yhdistelmiä, joihin sisältyy riskimielessä vaarallisia käyttövaltuusyhdistelmiä, tulee välttää. Jos niitä kuitenkin on pakko myöntää, niiden käyttöä tulee valvoa normaalia tarkemmin. Kriittisimpien tietojen/kohteiden käytössä voi olla tarpeen soveltaa menettelyä, jossa käyttövaltuus (omistajatahon käyttölupa) haetaan aina kertaluonteisesti käyttötilanteessa.

Tarpeettomiksi käyneet käyttövaltuudet eli kytkennät työroolien ja järjestelmän rooli en tai käyttöoikeuksien välillä tulee aina välittömästi poistaa.

3.9 Käyttövaltuuksien ja niiden hallinnoinnin säännöllisen valvonnan suunnittelu ja vastuutus

Hyvin organisoitu käyttövaltuushallinto edellyttää sovittujen prosessien ja niiden avulla hallinnoitavien käyttövaltuuksien jatkuvaa valvontaa. Valvonnan tarkoituksena on seurata, että sovittuja käytäntöjä noudatetaan, että käyttäjä- ja valtuustiedot ovat ajan tasalla, ja että hallinta- ja palvelujärjestelmiin ei kerry tarpeettomiksi käyneitä vanhoja määrityksiä. Valvonnan perustana ovat hallintajärjestelmän lokitiedot sekä hallinta- ja palvelujärjestelmissä olevat käyttäjä- ja käyttövaltuustiedot. Valvonnan välineitä ovat erilaiset raportointivälineet sekä säännölliset katselmoinnit. Valvonnan ovat velvollisia järjestämään ao. tietojen vastuulliset omistajat, eli työroolit omistavat organisaatioyksiköt sekä suojattavien kohteiden omistajat.

Säännöllisellä valvonnalla seurataan käyttäjä-, rooli-, käyttöoikeus- ja käyttövaltuustiedoissa tapahtuneita muutoksia. Kriittisimpien kohteiden käyttöä on hyvä säännöllisesti valvoa, samoin kuin erityisen laajat käyttövaltuudet omaavien henkilöiden toimintaa. Hallintajärjestelmän tulee mahdollistaa ajantasaisesti saatavilla olevat raportit

- käyttäjistä ja heidän työrooleistaan
- työrooleista ja niihin kytketyistä käyttövaltuuksista
- käyttäjistä ja heidän käyttövaltuuksistaan (edellisten yhdistelmä)
- käyttäjistä, joilla on tietty työrooli
- käyttäjistä, joilla on tietyn kohteen käyttövaltuus

Säännöllisesti, vähintään vuosittain järjestettävissä katselmoinneissa selvitetään

- onko järjestelmissä käyttäjiä, jotka eivät enää ole organisaation palveluksessa
- onko järjestelmissä työrooleja, jotka eivät ole enää käytössä
- onko järjestelmissä kohteita ja käyttöoikeuksia, jotka eivät ole enää käytössä
- onko järjestelmässä irrallisia käyttövaltuusmäärityksiä (ts. liittyen käytöstä poistettuihin kohteisiin tai poistuneisiin työrooleihin)
- onko käyttäjiä, joilla on vaarallisia työrooli- ja käyttövaltuusyhdistelmiä
- ovatko kohteisiin, rooleihin ja hallintaprosesseihin liittyvät omistajuudet ja niihin liittyvät toimeenpano- ja valvontavastuut hoidossa
- toimivatko hallinnointiprosessit sovitulla tavalla

Valvonnan organisointitavan ja siihen liittyvien vastuiden tulee olla sovittu viimeistään hallintajärjestelmän käyttöönottoon mennessä.

3.10 Hallintajärjestelmän käyttöönoton edellyttämien järjestelmävalmiuksien suunnittelu ja toteutus

Edellä kuvatut toimenpiteet rakentavat omalta osaltaan valmiuksia, jotka mahdollistavat seuraavassa luvussa kuvatun mukaisen hyvää käyttövaltuushallintoa tukevan hallintajärjestelmän käyttöönoton. Luonteeltaan periaatteellisten ja organisatoristen valmiuksien lisäksi tarvitaan joukko teknisiä valmiuksia, jotka valmistelevat hallintajärjestelmän käyttöönottoa. Tällaisia ovat

- henkilöstö- ja muiden lupaprosessien lähdetietojärjestelmien liittymien suunnittelu ja toteutus
- käyttäjätietovarastoliittymät
- provisiointiliittymät kohdejärjestelmiin.

3.11 Rekisteriselosteet

Organisaation tulee laatia käytössään olevista käyttäjä- ja lokirekistereistä liitteen mukaiset rekisteriselosteet (tietosuojaselosteet). Näitä koskevat velvoitteet on kuvattu luvussa 2.2.

4 HYVÄÄ HALLINTOKÄYTÄNTÖÄ TUKEVAN KÄYTTÖVALTUUKSIEN HALLINTAYMPÄRISTÖN ARKKITEHTUURI

Kuva 3 on toiminnallinen yleiskuva tavoitteellisesta, hyvää hallintakäytäntöä tukevasta käyttövaltuushallinnon järjestelmäympäristöstä.

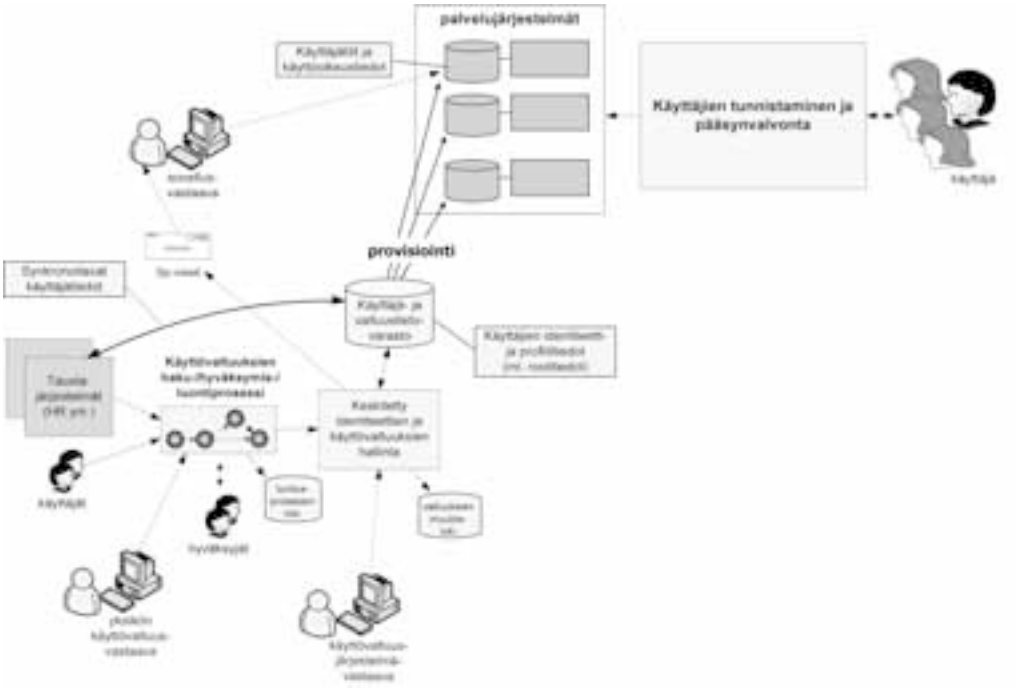
Kuva 3 Yleiskuva käyttövaltuushallinnon toimintaympäristöstä

4.1 Käyttäjäidentiteettien ja käyttövaltuuksien hallintajärjestelmä

Toimintaympäristön perustoiminnallisuudet toteuttaa käyttövaltuuksien hallintajärjestelmä ja siihen liittyvä keskitetty käyttäjä- ja valtuustietovarasto (kuva 4).

Hallintajärjestelmän muodostavat

- automaattisen luvitusprosessin eli käyttövaltuuksien haku-, hyväksymis- ja luontiprosessin toteuttava osajärjestelmä, johon on liittymät käyttäjätietoja tuottavista lähdetietojärjestelmistä ja jota palvelujärjestelmien käyttäjät ja käyttövaltuuksien hyväksyjät itsepalveluna käyttävät
- keskitetty käyttäjä- ja käyttövaltuustietovarasto
- automaattinen käyttövaltuustietojen provisiointijärjestelmä
- jäljitettävyys- ja raportointitoiminnot.



Kuva 4 Käyttövaltuuksien hallinta

4.1.1 Automaattisen luvitusprosessin toteuttava osajärjestelmä

Hallintajärjestelmän avulla toteutetaan automatisoitu käyttövaltuuksien haku-, hyväksymis- ja luontiprosessi, joka saa syötteensä

- henkilötietoja ja niissä tapahtuvia muutoksia tuottavilta taustajärjestelmiltä
- muutostietoja itsepalveluna syöttäviltä käyttäjiltä

Vara- ja poikkeusjärjestelynä tietoja järjestelmään voivat syöttää manuaalisesti myös organisaatioyksiköiden käyttövaltuusvastaavat ja/tai hallintajärjestelmän järjestelmävastaavat.

Käytännössä hallintaprosessien automatisointi tarkoittaa työnkulkujen määrittely ja automatisointi -toiminnallisuutta, jonka ohjaamana valtuuksien määrittely- ja hyväksymisprosessit tapahtuvat. Prosessien yhteyteen määritellään myös kaikki jäljitettävyysvaatimusten edellyttämät lokikirjoitustoiminnot. Automatisointiin voi liittyä laaja itsepalvelu, jossa käyttäjät, heidän esimiehensä ja kohteiden omistajat operoivat määriteltyjen hallintaprosessien mukaisesti hallintajärjestelmää suoraan ilman välikäsiä.

Organisaatioon työsuhteessa olevien käyttäjien perustietojen ja käyttöoikeuksien elinkaaren hallinta karkealla tasolla toteutetaan synkronoimalla organisaation henkilöstöhallinnon (HR) järjestelmä käyttövaltuuksien hallintajärjestelmään. Henkilöstöhallinnon järjestelmästä saadaan suoraan tiedot uusista käyttäjistä ja päättyvistä työsuhteista samoin kuin perusroolituksen mahdollistavat toimenkuvatiedot. Kytkentä ei kuitenkaan saa olla liian mekaaninen, koska esim. työsuhteen ja käyttövaltuuksien päättymisajankohta eivät välttämättä ole aina samat.

Henkilöstöhallinnon järjestelmän kautta ei saada tietoja käyttäjistä, jotka eivät ole organisaatioon työsuhteessa, mutta jotka silti tarvitsevat pääsyn joihinkin organisaation tietojärjestelmäpalveluihin. Näiden osalta lähdetietojärjestelmänä voi toimia esim. projektinhallintajärjestelmä tai jokin muu erillisrekisteri.

Valtionhallinnon organisaatioilla yleisessä käytössä oleviin potentiaalisiin lähdetietojärjestelmien, kuten yleisesti käytössä oleviin henkilöstöhallinnon järjestelmien, ja käyttövaltuuksien hallintajärjestelmien välille kannattaa määritellä ja teettää yhteinen, standardoitu liitäntämekanismi.

4.1.2 Keskitetty käyttäjä- ja käyttövaltuustietovarasto

Hallintajärjestelmän ytimen muodostaa keskitetty tietovarasto, jossa hallinnoidaan järjestelmän piirissä olevien käyttäjien ja heidän eri palvelujärjestelmissä olevien käyttövaltuuksiensa tietoja. Tietovarasto voi olla käytännössä yhdistetty useista eri lähteistä: käyttäjähakemistoista, tietokannoista tai tiedostoista. Tietovaraston tietoja pidetään yllä lähdetietovarastoihin synkronoimalla sekä ennen kaikkea käyttövaltuuksien hallintaprosessien kautta.

4.1.3 Käyttövaltuustietojen provisiointi kohdejärjestelmiin

Hallintajärjestelmän tämä osa huolehtii uusien ja muuttuneiden käyttäjä- ja käyttövaltuustietojen automaattisesta siirrosta eli provisioinnista kohdejärjestelmiin, ts. organisaation palvelujärjestelmiin. Hallintajärjestelmän luvitusprosessien läpi kulkeneet käyttövaltuustapahtumat (uudet käyttäjät/roolit, uudet käyttövaltuudet, käyttövaltuuksien poistot jne.) siirretään automaattisesti kohdejärjestelmiin heti niiden synnyttyä tai ajastettuna esim. saman vuorokauden sisällä. Vara- ja poikkeusjärjestelynä hallintajärjestelmä voi välittää muutostiedot esim. salattuna ja sähköisesti allekirjoitettuna sähköpostina palvelujärjestelmien järjestelmävastaaville, jotka sitten syöttävät tiedot manuaalisesti kohdejärjestelmään. Tämä on mahdollinen tilapäisjärjestely myös esim. silloin, kun kohdejärjestelmän automaattinen provisiointiliittymä ei ole vielä käytettävissä.

Valvonnan kannalta on hyvä siirtää tietoa myös toiseen suuntaan eli tietojärjestelmästä käyttövaltuuskantaan. Vertaamalla käyttövaltuuskannan ja tietojärjestelmissä olevan valtuustiedon tilannetta voidaan havaita nopeasti sekä yritykset antaa käyttöoikeuksia ohi virallisen prosessin että myös provisioinnissa tapahtuneet tekniset virheet.

Ongelmana käyttövaltuustietojen automaattisessa provisioinnissa on se, että tietojen kohdejärjestelmiin syöttämiseen tarvittavia rajapintoja ei ole standardoitu ei sellaisia välttämättä ole aina edes valmiina olemassa. Kansainvälinen standardointityö näyttäisi jatkossa tuottavan tässä käyttökelpoisia avoimia standardeja kuten SPML (Service Provisioning Markup Language). Käytännössä kuitenkin vielä hyvän aikaa provisiointiliitäntöjä täytyy räätälöidä, mikä valtionhallinnossa yleisesti käytössä oleviin palvelujärjestelmiin kannattaisi tehdä laajana yhteistyönä samalla tavalla kuin lähdetietojärjestelmien liitännätkin.

Myös provisioinnissa on otettava huomioon, että käyttövaltuustietoihin sisältyvät käyttäjäidentiteettitiedot ovat henkilötietoja.

4.1.4 Jäljitettävyys- ja raportointitoiminnot

Käyttövaltuuksien hallintajärjestelmän keskeinen vaatimus on, että kaikkien sen piirissä olevien tietojen ja tehtyjen tapahtumien tulee olla raportoitavissa. Käyttövaltuuksiin ja niihin vaikuttaviin määrityksiin, kuten käyttäjien rooleihin ja suojattavien kohteiden käyttöoikeuksiin, tehdyt muutokset tulee olla jäljitettävissä siten, että kaikki muutostapahtumiin osalliset (alullepanijat, hyväksyjät, asianomaiset) käyvät selville. Käytännössä tämä toteutuu siten, että luvitusprosessin kaikki tapahtumat samoin kuin kaikki hallintajärjestelmään suoraan tehdyt tapahtumat ja kohdejärjestelmiin välitetyt tapahtumat kirjataan lokitiedostoihin, joiden perusteella käyttäjätietojen ja käyttövaltuuksien muutoksia voidaan seurata.

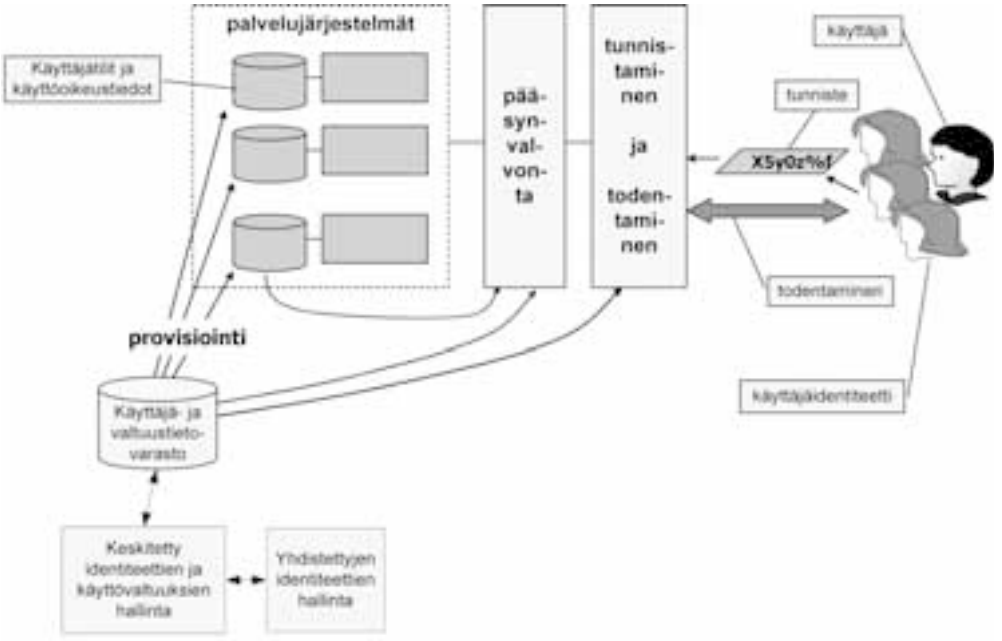
Hallintajärjestelmän kautta tulee olla mahdollista saada milloin tahansa ajantasainen raportti toimintaympäristössä käytössä olevista käyttäjäidentiteeteistä, niiden haltijoista ja niihin liittyvistä käyttövaltuuksista samoin kuin palvelujärjestelmissä määritellyistä suojattavista kohteista ja niihin liittyvistä käyttövaltuuksista. Raportointivälineet mah-

dollistavat myös yksittäisten käyttäjien, kuten erityislaajat valtuudet omaavien käyttäjien, käytön seurannan. Järjestelmän tulee osata varoittaa ei-aktiivisista käyttäjätunnuksista ja käyttöoikeuksista sekä valvoa määritysten eheyttä niin, että irralleen jäävät määritykset eivät ole mahdollisia tai ovat helposti havaittavissa ja poistettavissa.

4.2 Käyttäjien tunnistaminen ja pääsynvalvonta

Palvelujärjestelmien pääsynvalvonta voi nojautua keskitettyihin käyttäjä- ja käyttövaltuustietoihin. Pääsynvalvonta on mahdollista toteuttaa eri tavoin. Kertakirjausjärjestelmä on tässä yhteydessä luonteva ja käyttäjäystävällinen ratkaisu, mutta myös enemmän tai vähemmän hajautettu keskitettyihin valtuustietoihin nojautuva pääsynvalvonta on mahdollinen. Pääsynvalvonnan hienojakoisin taso voidaan jättää palvelujärjestelmätasolla tehtäväksi.

Käyttäjien luotettava tunnistaminen on sitä tärkeämpää mitä hienojakoisempia käyttövaltuuksia – ja siten suojaustarpeita – palvelujärjestelmässä on. Käyttäjien tunnistaminen ja todentaminen voi tapahtua keskitetyssä järjestelmäympäristössä tai ulkoistetun palve-



Kuva 5 Käyttäjien tunnistaminen ja pääsynvalvonta keskitetyn käyttövaltuushallinnon toimintaympäristössä

lun toimesta. Kaikissa tapauksissa pääsynvalvonta saa tunnistusjärjestelmältä todennetun käyttäjän tiedot joko standardinmukaisena tunnistusselosteena (esim. SAML-standardin mukaisesti) tai järjestelmäkohtaisesti sovitussa muodossa.

Jokaisella käyttäjällä tulee olla yksilöivä tunniste kaikissa käyttövaltuushallintoon liittyvissä tietovarastoissa.

Kuva 5 on tarkennettu esitys kuvien 3 ja 4 esittämän toimintaympäristön ”käyttäjien tunnistaminen ja pääsynhallinta” sekä ”yhdistettyjen identiteettien hallinta ” -osuuksista.

5 KESKITETYN KÄYTTÖVALTUUKSIEN HALLINTAJÄRJESTELMÄN KÄYTTÖÖNOTTOON LIITTYVIÄ SUOSITUKSIA

Tässä dokumentissa kuvatun kaltaisen keskitetyn käyttövaltuuksien hallintajärjestelmän käyttöönotto on täydessä laajuudessaan sekä toiminnallisilta vaikutuksiltaan että teknisesti mittava hanke, johon on syytä suhtautua asiaankuuluvalla vakavuudella. Olennaista hankkeen onnistumiselle on kunnollinen ennakkosuunnittelu ja valmistautuminen luvussa 3 kuvatun mukaisesti. Hankkeeseen tulee kytkeä ja sitouttaa alusta alkaen mukaan kaikki osapuolet: organisaation johto, järjestelmien omistajat, henkilöstöhallinto, tietohallinto ja käyttäjät. Järjestelmän ja sen tukemien prosessien toimintaedellytykset ja jatkuva ylläpito ja valvonta käyttöönoton jälkeen on järjestettävä ja turvattava etukäteen.

Vaiheittainen eteneminen on välttämätöntä samoin kuin se, että hanke on riittävästi resursoitu. Tavoitteena tulee pitää toimintojen mahdollisimman kattavaa automatisointia. Tähän pitäisi päästä suhteellisen helposti luvitusprosessin osalta. Sen sijaan automaattisen provisioinnin suhteen on realistista olettaa tavoitetilan toteutuvan vähitellen. Kokonaisjärjestelmän toteutuksessa tulisi käyttää mahdollisimman paljon valmiita ratkaisukomponentteja ja mahdollisimman vähän räätälöintiä. Järjestelmäratkaisun tulee tukea avoimia standardeja ja rajapintoja, ihanneratkaisuna voidaan pitää modulaarista tuotekokonaisuutta. Harkinnan arvoinen voisi olla yhteisin ponnistuksin määriteltävä valtionhallinnon vaatimuksiin perustuva järjestelmäratkaisukehikko, jossa on hoidettu mm. yleisimmin tarvittavat liitännät lähde- ja kohdetietojärjestelmiin sekä käyttäjätietovarastoihin. Hallintajärjestelmän tulee olla liitettävissä myös valtionhallinnon yleisiin tunnistamispalveluihin.

Teknisessä mielessä tärkeimpiä vaatimuksia hallintajärjestelmälle ovat

- jatkuvatoimintaisuuden takaava järjestelmäarkkitehtuuri (24/7-käyttö) ja sen mahdollistamat toimivat varajärjestelyt myös poikkeustilanteissa
- korkeinta luokkaa oleva sisäinen tietoturvallisuus
- skaalautuvuus sekä määrällisesti (käyttäjät, liitännäisjärjestelmien määrä, käyttövolyymit) että maantieteellisesti.

Käyttövaltuushallintoon liittyvien tietojen ja asiakirjojen sekä järjestelmän lokitietojen säilytysajat on määriteltävä arkistolain (831/94) säännösten mukaisesti. Määräajan säilytettävät tiedot on hävitettävä niille vahvistetun säilytysajan jälkeen siten, että tietosuoja ja tietoturvallisuus on varmistettu.

LIITE 1 ORGANISAATIORAJAT YLITTÄVÄT KÄYTTÖVALTUUDET

Käyttövaltuuksien hallinnan edellyttämät toimenpiteet

Yhdistettyjen identiteettien hallinta (federointi) on yksi mahdollinen tapa toteuttaa organisaatiorajat ylittävä palvelujärjestelmien käyttö. Identiteettien yhdistäminen edellyttää luottamusverkoston muodostamista, jossa

- osapuolet ovat määritelleet yhteiset toimintaperiaatteet
- osapuolet ovat katselmoineet ja hyväksyneet toistensa toimintaprosessit, muun muassa käyttäjien rekisteröintitavan ja käyttäjien tunnistustavan
- osapuolet ovat muodollisin sopimuksin sitoutuneet yhteisesti sovittujen toimintatapojen noudattamiseen

Ulkopuolisen organisaation käyttäjille annettavien työroolien sisällöstä, erityisesti niihin liittyvistä käyttövaltuuksista, tulee sopia käyttäjän tarpeet määrittelevän kotiorganisaation ja tarvittavat resurssit omistavien organisaatioiden kesken. Ulkopuolisen organisaation tulee tiedottaa palveluntarjoajaosapuolelle välittömästi verkostokäyttäjiinsä liittyvistä muutoksista, erityisesti työsuhteen päättymisestä sekä tarpeettomiksi käyneistä työrooleista.

Yhdistettyjen identiteettien hallinta

Organisaatiorajat ylittävän palvelujärjestelmien käytön toteutustapa perustuu organisaatioiden muodostaman luottamusverkoston piirissä suoritettavaan identiteettien yhdistämiseen (federointiin). Lähtötilanteessa kullakin organisaatiolla on oma, organisaatiokohtainen käyttäjätietojen sisältö, ts. attribuutit, joista organisaation käyttäjäidentiteetit muodostuvat. Tyypillisesti osa näistä attribuuteista on kaikkien osapuolten jossain muodos-

sa käyttämiä, osa täysin organisaatiokohtaisia. Identiteettien yhdistäminen tarkoittaa sopimista luottamusverkostossa käytettävistä yhteisistä attribuuteista eli verkostoidentiteetistä ja sen muodosta sekä tavasta, jolla identiteettitietoja välitetään organisaatioiden välillä. Yhteisesti sovittu verkostoidentiteetti toimii avaintietona, jonka perusteella organisaatio pystyy päättelemään, mihin heidän omaan käyttäjäidentiteettiinsä se kuvautuu. Käyttäjätietojen välittämisessä organisaatioiden välillä on otettava huomioon henkilötietojen käsittelyä koskeva lainsäädäntö.

Tietoja voidaan välittää erämuotoisesti etukäteen esimerkiksi kaikista niistä käyttäjistä, jotka ovat potentiaalisia toisen organisaation palvelujen käyttäjiä. Mahdollista on myös toimintatapa, jossa käyttäjän tiedot välitetään palveluntarjoajaorganisaatiolle vasta käyttötilanteessa. Lähtökohtana on periaate, että käyttäjän tunnistaa hänen kotiorganisaationsa, joka sitten välittää tunnistamansa käyttäjän identiteettitiedot tunnistusselosteena palveluntarjoajaorganisaatiolle ja tämän pääsynvalvonnalle. Palveluntarjoajaorganisaation pääsynvalvonnan kannalta ulkoiset käyttäjät eivät erotu omista käyttäjistä muuten kuin mahdollisesti erilaisten roolitietojensa puolesta. Käyttäjien kannalta yhdistettyjen identiteettien luottamusverkostoon kuuluvien palvelujärjestelmien käyttökokemus on kuin laajennettu kertakirjausympäristö, jossa käyttäjä tunnistautuu vain kerran omassa kotiorganisaatiossaan.

Valtionhallinnon piirissä esimerkiksi yliopistot ovat toteuttaneet yhdistettyjen identiteettien hallinnan. Lisätietoa toteutuksesta löytyy http://www.csc.fi/suomi/funet/middleware/projektit/index.phtml.

LIITE 2 KÄYTTÄJÄHALLINTA-REKISTERIN REKISTERISELOSTE, MALLI ISOILLE ORGANISAATIOILLE

XXXXXX VIRASTON KÄYTTÖOIKEUKSIEN HALLINNAN REKISTERISELOSTE JA INFORMOINTIASIAKIRJA

(= tietosuojaseloste)

MALLI ON LAADITTU ERITYISESTI VIRASTOA VARTEN, JOSSA PIDETÄÄN SUURIA, JOPA VALTAKUNNALLISIA HENKILÖREKIS-TEREITÄ JA TIETOJÄRJESTELMIÄ

1. Rekisterin nimi	**xxxxxxxxx VIRASTON KÄYTTÖOIKEUSHALLINNON REKISTERI (KÄYTTÄJÄREKISTERI)** Käyttäjärekisteri on henkilöstöhallinnon osarekisteri, jossa eritellään viraston eri henkilörekisterien ja niitä ylläpitävien tietojärjestelmien käyttäjät. Käyttäjärekisteri jakaantuu organisaatiosta riippuen eri osarekistereihin, esim. • organisaation varsinaiseen toimintaan kuuluvien henkilörekisterien/tietojärjestelmien käyttäjärekisteri (esim. ajoneuvohallintakeskuksen ajoneuvoliikennerekisterin käyttäjät, väestörekisterikeskuksen väestörekisterin/väestötietojärjestelmän käyttäjät, valtiokonttorin eläkeasioiden rekisterien/tietojärjestelmän käyttäjät) • henkilöstöhallinnon rekisterin/tietojärjestelmän käyttäjät • ym. *Käyttäjärekisterin rekisteri-/tietosuojaseloste voidaan laatia myös erikseen eri henkilörekisterin / tietojärjestelmien osalta*

MALLI ON LAADITTU TIETOSUOJAVALTUUTETUN TOIMISTOSSA 27.9.2006

2. Rekisterinpitäjä	**VIRASTO XXXX** Postiosoite: Käyntiosoite: Puhelin/vaihde: Rekisteri on perustettu xx virastoa varten ja sillä on oikeus määrätä rekisterin käytöstä.
3. Rekisterin vastuuhenkilö	**Vastuuhenkilönä toimii** xx viraston xx xxx virassa oleva henkilö xx (nimi: _____ (esim. hallintoyksikön päällikkö, IT-käytönhallintayksikön vastuuhenkilö XX tai vastaava) *Käytännössä vastuu voidaan delegoida organisaatiokohtaisesti toiminnalliset vastuut huomioiden* ***Ohje*** Vastuuhenkilön tehtävänä on määritellä käyttöoikeuksien hallinnan ja käytön periaatteet ja huolehtia siitä, että rekisterinpito on suunniteltu ja hoidetaan koordinoidusti, virheettömästi ja että rekisterintiedot ovat ajantasaisia. Rekisterin vastuuhenkilön tehtäviin kuuluu yleisesti huolehtia siitä, että rekisteritoiminnot suunnitellaan ja toteutetaan ja sitä käytetään säännösten ja määräysten mukaisesti. Vastuuhenkilö antaa asiaan liittyvät ohjeet sekä määrittelee tarkemmin käytännön rekisterinpitoon liittyvät vastuut ja tehtävät sekä määrittelee seuraamukset lain ja ohjeiden vastaisesta menettelystä.
4. Rekisterin yhteyshenkilö	**Yhteyshenkilönä toimi**i xxxxx Yhteystiedot: - Postiosoite: - Sähköposti-osoite - puhelin: Rekisterin yhteyshenkilö antaa rekisteristä ja siihen liittyvästä henkilötietojen käsittelystä tarkempia tietoja sekä huolehtii tarvittaessa siitä, että rekisteröityjen tarkastusoikeutta ja virheen oikaisua koskevat ja vastaavat pyynnöt ohjataan asiasta päättäville henkilöille
5. Rekisterin käyttötarkoitus	Käyttöoikeushallinnossa ylläpidetään ajantasaista luetteloa (henkilörekisteriä) viraston xx henkilöstölle myönnetyistä käyttöoikeuksista, käyttöoikeuden kestosta ja käyttöoikeuksien sisällöstä. Erillinen osarekisteri muodostetaan viraston lukuun toimivien sen tietojärjestelmää xx käyttävien ulkopuolisten palvelujen tuottajien palveluksessa olevista työntekijöistä, (käyttäjistä). Rekisteriseloste laaditaan eri tietojärjestelmien ja eri henkilörekisterien osalta eriteltynä. Käyttäjähallinnan tarkoituksena on 1. mahdollistaa xxxx rekisteriin talletettujen henkilötietojen suojaaminen siten kuin henkilötietolain (523/1999) 32 §:ssä säädetään; 2. huolehtia yksityisyyden suojasta työelämässä annetun lain (759/2004) mukaisten työsuhteen osapuolten oikeuksien ja velvollisuuksien täyttämisestä ja 3. mahdollistaa puuttuminen käyttöoikeuden vastaiseen xx rekisterin tietojen käyttöön, luovutukseen ja muuhun käsittelyyn. Valvonnassa kerättävistä tiedoista (lokeista) muodostetaan eri henkilörekisteri

6. Rekisterin pitämisen peruste	**Rekisterinpitäjän oikeus pitää käyttäjärekisteriä perustuu** 1. rekisterinpitäjän ja rekisteröidyn välillä olevaan palvelussuhteesta tai siihen verrattavasta suhteesta johtuvaan asialliseen yhteyteen (8 §:n 1 momentin 5 kohta, HetiL 523/2006) 2. rekisterin tiedot on suojattava henkilötietolain 32 §:n edellyttämällä tavalla; 3. viranomaisena rekisterinpitäjän on huolehdittava xxxx rekisteriä koskevien tietojärjestelmien suojaamisesta, eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä hyvän tiedonhallintatavan mukaisesti siten kuin laissa viranomaisten toiminnan julkisuudesta (621/1999) 18 §:ssä säädetään
7. Rekisterin tietosisältö	**Käyttäjän ja hänen käyttöoikeuksiensa yksilöimiseksi tarvittavat tiedot (ml. järjestelmän ylläpitäjien käyttäjätiedot)** • nimi, • henkilötunnus • virasto, jossa työskentelee ja • Tehtävä/tehtäväryhmä ja työskentely-yksikkö (toimipiste) • tieto siitä kuka /mikä yksikkö käyttöoikeudet antaa • tieto siitä, toimiiko henkilö viraston lukuun toimivan palvelun tuottajan lukuun; asiaa koskevan toimeksiantosopimuksen yksilöinti ja muut sopimukseen liittyvät tarvittavat tiedot • tieto käyttäjä- ja vaitiolositoumuksen antamisesta rekisterinpitäjälle **Käyttöoikeuden myöntämistä ja voimassaoloa koskevat tiedot Eriteltynä tarpeen mukaan eri tietojärjestelmien ja rekisterien osalta** • käyttöoikeuden myöntämistä koskevat tiedot • käyttöoikeuden kesto • käyttöoikeuden päättymistä koskeva tieto • käyttäjätunnus **Tietojärjestelmä(t) ja henkilörekisteri(t) jonka/joiden käyttöä varten käyttöoikeus myönnetään** • tietojärjestelmä(t) • henkilörekisteri(t) • Käyttöoikeutta koskevat tarkemmat tiedot (tehtävään kuuluvat käyttöoikeudet) - tehtävä, jonka hoitamiseksi käyttöoikeus on annettu - käyttöoikeuden sisältöä koskevat tarkemmat tiedot o oikeus rekisterin käyttöön (esim. luku, päivitys, tulostus yms.) o oikeus rekisterin tietojen luovuttamiseen • tieto käyttöoikeuteen tehdyistä muutoksista, muutosajankohta ja muutoksen tekijä • muita mahdollisia välttämättömiä tietoja, yksilöitynä Muita tietoryhmiä ovat käyttöjärjestelmän keräämät lokitiedot palvelimien ja palveluiden käytöstä sekä muut käyttöjärjestelmiin kuuluvat tarvittavat käyttöoikeudet mahdollistavat määrittelytiedostot.
8. Säännönmukaiset tietolähteet	• henkilöstöhallinnon rekisteristä/ tietojärjestelmästä (viraston ao. vastuuhenkilöltä) saadut palvelussuhdetta, tehtävää ja sijaintipaikkaa ym. koskevat tarpeelliset tiedot • asianomaisilta henkilöiltä käyttöoikeuslupahakemuksen ym. yhteydessä saadut tiedot (hakemukset kuuluvat loogiseen käyttäjärekisteriin) • työnantajan ao. toiminnon vastuuhenkilön määrittelemät käyttöoikeuden myöntämistä, käyttäjätunnusta, käyttöoikeuden kestoa tai sisältöä sekä käyttöoikeuden päättymistä koskevat tiedot. Jos virasto on hankkinut sopimuksen perusteella tietojenkäsittelypalveluja ulkopuoliselta palvelujen tuottajalta, tiedot käyttäjistä saadaan sopimusosapuolelta ja virasto myöntää ko. käyttäjäluvat (sopimukseen ao. määräys)

9. Rekisterissä olevien tietojen luovutus	Rekisterin ja sen tiedot ovat sisäiseen käyttöön tarkoitettuja. Tiedot ovat salassa pidettäviä siltä osin kun kysymys on tietojärjestelmien turvajärjestelyistä ja niiden toteuttamisesta (laki viranomaisten toiminnan julkisuudesta, JulkL 24.1 § kohta 7). Käyttöoikeushallinnon rekisterin tietoja ei pääsääntöisesti luovuteta sivullisille, ellei siihen ole lakiin oikeuttavaa perustetta. Asianosaisella eli henkilöllä, jonka tietoja ko. henkilörekisteriin/järjes-telmään on talletettu voi olla oikeus saada tietoja käyttäjärekisteriin merkityn henkilön tiedoista viranomaisten toiminnan julkisuudesta annetun lain 11 § mukaisesti ja sinä säädetyin edellytyksin.
10. Rekisterin suojaaminen	Rekisteriä säilytetään ulkopuolisilta suojattuna. Luetteloa niiden käyttöön oikeutetuista henkilöistä säilytetään xxxxx (esim. manuaalinen lukitussa kaapissa yms., atk:lla käsiteltävä aineisto ulkopuoliselta ja sivullisilta suojattuna) Rekisterin tietoja saa nähtäväkseen vain sen hallinnoinnin edellyttämiin tehtäviin osallistuvat henkilöt (nimet ja virka-asema). Rekisteriin pääsy on rajoitettu siten, että muutoksia siihen voi tehdä vain ennalta määritellyiltä ylläpitäjien työasemilta. Ylläpitäjät tunnistetaan henkilökohtaisten käyttäjätunnusten ja salasanojen avulla. Rekisterinmuutos- ja lukuoikeudet annetaan erikseen määriteltyjen oikeuksien (pääsylistojen) avulla. Jokaisen käyttäjän edellytetään allekirjoittavan käyttäjä- (ja salassapitositoumus)
11. Rekisterissä olevien tietojen tarkastusoikeus henkilötietolain perusteella	Käyttäjärekisteriin merkityillä henkilöillä (rekisteröidyillä) on oikeus saada tarkastaa itseään koskevat rekisteriin talletetut tiedot sekä tällöin ilman eri pyyntöä saada tiedot rekisterin säännönmukaisista tietolähteistä ja säännönmukaisista tietojen luovutuksista. Sen, joka haluaa tarkastaa itseään koskevat em. tiedot, on esitettävä pyyntö xx:lle. Nimi: xx yhteystiedot Pyyntö esitetään kirjallisesti omakätisesti allekirjoitetulla kirjeellä tai henkilökohtaisesti. Tarkastusoikeus on maksutonta kerran vuodessa toteutettuna Mikäli tarkastuspyyntö evätään, rekisteröidyllä on oikeus saada kirjallinen kieltäytymistodistus. Rekisteröity voi tällöin saattaa epäämisen tietosuoja-valtuutetun toimiston käsittelyyn. Tietosuojavaltuutetun toimiston osoite: PL 315, 00181 Helsinki Käyntiosoite Albertinkatu 25 , 3 krs

12. Virheellisen tiedon korjaaminen	Rekisteröity voi vaatia käyttäjä rekisteriin merkitys virheellisen tiedon korjaamista Oikaisupyyntö osoitetaan xx:lle Nimi : xx Yhteystiedot: xx Mikäli tietoa ei korjata, rekisteröidyllä on oikeus saada kirjallinen kieltäytymistodistus. Rekisteröity voi saattaa epäämisasian tietosuojavaltuutetun toimiston käsiteltäväksi. Tietosuojavaltuutetun toimiston osoite: PL 315, 00181 Helsinki Käyntiosoite Albertinkatu 25 , 3 krs.
13. XX Rekisteriin merkityn (rekisteröidyn) tiedonsaantioikeus omien tietojen käytöstä	Henkilöllä, jonka tietoja on talletettu tietojärjestelmään/henkilörekisteriin (rekisteröity), jonka tietoihin tässä tarkoitettu käyttäjä saa käyttöoikeudet, ei ole henkilötietolain mukaista tarkastusoikeutta käyttäjärekisterin tietoihin. Sen sijaan hänellä voi olla oikeus Julkisuuslain 11 §:ssä tarkoitetun asianosaisaseman perusteella saada tietoja käytönhallintarekisteristä, säädetyin edellytyksin.
14. Rekisterin yhdistäminen muihin rekistereihin	Rekisteritietoja yhdistetään lokirekisteriin HetiL:n 32 §:n perusteella suojaamisvelvoitteen noudattamiseksi
15. Rekisterin arkistointi ja hävittäminen	Rekisteriin talletetaan tiedot niistä henkilöistä, joilla on voimassa oleva(t) käyttöoikeudet. Rekisteristä poistettuja tietoja voidaan säilyttää poistamisen jälkeen jos se on tarpeellista toiminnan tai valvonnan kannalta tai siihen on laissa säädetty oikeus. *- viranomaisten tulee määritellä säilyttämisaika arkistolain mukaisesti (arkistonmuodostamissuunnitelma)* *- Tietoja lienee säilytettävä ainakin sen ajan kuin lokitietojakin säilytetään (vähintään kahden vuoden ajan, jos käyttäjän toimintaa joudutaan arvioimaan jälkikäteen ko. selvityksen edellyttämän ajan. Tiedot on syytä siirtää eri tiedostoon.*
16. Henkilötietojen käsittely yhteistoimintamenettelyssä ja henkilötietojen käsittelystä informointi (Työelämän tietosuojalaki, TyTSL)	Henkilötietojen käsittelyn tarkoitus, peruste, kerättävät tiedot, tietojen säännönmukaiset luovutukset ja rekisteröityjen tarkastus- ja virheen oikaisuun liittyvät oikeudet sekä niiden toteuttamistapa on käsitelty yhteistoimintamenettelyssä henkilöstön ao. edustajien kanssa xx.xx.xxxx Rekisteriin merkityn henkilön tulee varmistaa, että on tutustunut tähän selosteeseen ennen kuin hän allekirjoittaa XX tietojärjestelmien/henkilörekisterin käyttöoikeuden saamisen edellytyksenä olevan käyttäjä- ja/tai salassapitositoumuksen. Lisäksi tämä seloste on kaikkien xx tietojärjestelmien käyttöön oikeutettujen luettavissa (sisäisen verkon) kotisivuilla kohdassa xx sekä saatavilla xx viraston kirjaamossa. Huom. Salassapitositoumus tarvitaan, jos käsitellään salassa pidettäviä tietoja, muutoin riittää käyttäjäsitoumuksen tekeminen. Tutustu käyttäjä- ja salassapitositoumusmalliin tietosuojavaltuutetun toimiston verkkosivuilla www.tietosuoja.fi).

LIITE 3 KÄYTTÄJÄHALLINTA-REKISTERIN REKISTERISELOSTE, MALLI PIENILLE ORGANISAATIOILLE

REKISTERISELOSTE JA INFORMOINTIASIAKIRJA

(Tietosuojaseloste)
Henkilötietolaki (523/99) 10 §
Laatimispvm:

MALLI VIRASTOA VARTEN, JOLLA ON KÄYTÖSSÄÄN VAIN PIENIÄ JA OMAAN KÄYTTÖÖN TARKOITETTUJA HENKILÖREKISTEREITÄ JA TIETOJÄRJESTELMIÄ

1. Rekisterinpitäjä	Nimi virasto xx
	Yhteystiedot (osoite, puhelin…) Käyntiosoite: Postiosoite:
2. Rekisteriasioista vastaava henkilö ja/ tai yhteyshenkilö	Nimi Vastuuhenkilö, esim. hallintopäällikkö xxxx Yhteyshenkilö esim. osastosihteeri xxxx
	Yhteystiedot (osoite, puhelin…) puh. xxxxx / vastuuhenkilö xx puh. xxxx /yhteyshenkilö xx
3. Rekisterin nimi	Henkilöstön käyttöoikeusrekisteri (Käyttäjärekisteri)

MALLI ON LAADITTU TIETOSUOJAVALTUUTETUN TOIMISTOSSA 27.9.2006

4. Henkilötietojen käsittelyn tarkoitus / rekisterin käyttötarkoitus	Virasto xx henkilöstölle eri henkilörekistereihin /tietojärjestelmiin myönnettävien käyttöoikeuksien ylläpito ja hallinta (HetiL 32 §, TyTSL xx §) esim. - diaari/diaarijärjestelmä - asianhallintajärjestelmä - sähköpostijärjestelmä - henkilöstöhallinnon tietojärjestelmä - taloushallintojärjestelmä - yms.
5. Rekisterin tietosisältö	- Käyttäjän nimi - käyttäjän yksikäsitteinen tunniste - tieto henkilörekisteristä ja tietojärjestelmästä, johon käyttöoikeus on myönnetty - käyttöoikeuden sisältö eri rekisterien/tietojärjestelmien osalta eriteltynä (esim. luku, muuttaminen, muokkaus yms.) - käyttöoikeuden alkaminen - käyttöoikeuden päättyminen - käyttöoikeuden kesto - käyttöoikeuden muuttaminen - käyttäjätunnus Muita tietoryhmiä ovat käyttöjärjestelmän keräämät lokitiedot palvelimien ja palveluiden käytöstä sekä muut käyttöjärjestelmiin kuuluvat tarvittavat käyttöoikeudet mahdollistavat määrittelytiedostot.
6. Säännönmukaiset tietolähteet *	Tiedot saadaan henkilöstöasioiden hoitajalta ja käyttöoikeuksien myöntäjältä
7. Säännönmukaiset tietojen luovutukset ja tietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle	Rekisteri on laadittu sisäistä käyttöä varten - Tietoja ei luovuteta ulkopuolisille
8. Rekisterin suojauksen periaatteet	Tietoja ylläpidetään - manuaalisesti / word-tiedostona - Rekisterin tietoja käyttävät vain ne joiden tehtäviin käyttöoikeuksien määrittely, hallinta ja ylläpito kuuluu - tiedot suojataan ulkopuolisilta

9. Rekisterissä olevien tietojen tarkastusoikeus henkilötietolain perusteella	Käyttäjärekisteriin merkityillä henkilöillä (rekisteröidyillä) on oikeus saada tarkastaa itseään koskevat rekisteriin talletetut tiedot sekä tällöin ilman eri pyyntöä saada tiedot rekisterin säännönmukaisista tietolähteistä ja säännönmukaisista tietojen luovutuksista. Sen, joka haluaa tarkastaa itseään koskevat em. tiedot, on esitettävä pyyntö xx:lle. Nimi: xx yhteystiedot Pyyntö esitetään kirjallisesti omakätisesti allekirjoitetulla kirjeellä tai henkilökohtaisesti Tarkastusoikeus on maksutonta kerran vuodessa toteutettuna Mikäli tarkastuspyyntö evätään, rekisteröidyllä on oikeus saada kirjallinen kieltäytymistodistus. Rekisteröity voi tällöin saattaa epäämisen tietosuoja-valtuutetun toimiston käsittelyyn. Tietosuojavaltuutetun toimiston osoite: PL 315, 00181 Helsinki Käyntiosoite Albertinkatu 25, 3 krs.
10. Virheellisen tiedon korjaaminen	Rekisteröity voi vaatia käyttäjärekisteriin merkitys virheellisen tiedon korjaamista Oikaisupyyntö osoitetaan xx:lle Nimi : xx Yhteystiedot: Xx Mikäli tietoa ei korjata, rekisteröidyllä on oikeus saada kirjallinen kieltäytymistodistus. Rekisteröity voi saattaa epäämisasian tietosuojavaltuutetun toimiston käsiteltäväksi. Tietosuojavaltuutetun toimiston osoite: PL 315, 00181 Helsinki Käyntiosoite Albertinkatu 25, 3 krs.
11. rekisteriin/tietojärjes- telmään merkityn (rekisteröidyn) tiedonsaantioikeus omien tietojen käytöstä	Henkilöllä, jonka tietoja on talletettu tietojärjestelmään/henkilörekisteriin (rekisteröity), jonka tietoihin tässä tarkoitettu käyttäjä saa käyttöoikeudet, ei ole henkilötietolain mukaista tarkastusoikeutta käyttäjärekisterin tietoihin. Sen sijaan hänellä voi olla oikeus Julkisuuslain 11 §:ssä tarkoitetun asianosaisaseman perusteella saada tietoja käyttäjärekisteristä säädetyin edellytyksin
Huom. Henkilötietojen käsittelyn tarkoitus, peruste, kerättävät tiedot, tietojen säännönmukaiset luovutukset ja rekisteröityjen tarkastus- ja virheen oikaisuun liittyvät oikeudet sekä niiden toteuttamistapa on käsitelty yhteistoimintamenettelyssä henkilöstön ao. edustajien kanssa xx.xx.xxxx	

LIITE 4 SANASTO

Termi	englanninkielinen vastintermi	määritelmä
identiteetin eriyttäminen	identity defederation; defederation	**käyttäjäidentiteetin** irrottaminen **yhdistetystä verkko-identiteetistä**
identiteetti	identity	joukko ominaisuuksia, jotka kuvaavat **käyttäjää** ja joiden avulla **käyttäjä** voidaan **tunnistaa**
identiteetti- ja käyttövaltuushallinto	identity and access management (IAM)	toimintaprosessit, säännöt, organisaatio ja välineet, joiden avulla hallinnaidaan tietojärjestelmien asianmukaista käyttöä
identiteettien yhdistäminen/federointi	identity federation	**käyttäjän** erillisten **käyttäjäidentiteettien** kytkeminen toisiinsa
jäljittäminen	auditing	tietojärjestelmän käyttötietojen selvittäminen
kotiorganisaatio	identity provider	**yhdistettyjä identiteettejä** käyttävässä toimintaympäristössä osapuoli, joka vastaa **käyttäjän tunnistamisesta** ja välittää **tunnistusselosteen palveluntarjoajalle**
käyttäjä	user; principal (Liberty Alliance)	tietojärjestelmäpalveluja käyttävä henkilö, ryhmä tai ohjelmisto
käyttäjähallinta	user management; identity management	k**äyttäjäidentiteetti-** ja **käyttäjätilitietojen** ylläpito
käyttäjäidentiteetti	user identity; principal identity (Liberty Alliance)	**käyttäjätilin** yksilöivä **käyttäjän** ilmentymä verkkopalvelussa
käyttäjäprofiili	user profile	**palvelujärjestelmässä** ylläpidettävät **käyttäjätiliin** liittyvät ominaisuudet, mm. **käyttäjärooli** Käyttäjäprofiilin avulla voidaan ohjata palvelujen käyttöä

Termi	**englanninkielinen vastintermi**	**määritelmä**
Käyttäjärooli	user role	joukko **käyttäjän** ominaisuuksia, jotka liittyvät hänen tietotarpeittensa ja/tai toimintavaltuuksiensa määrittelyyn Käyttäjäroolia voidaan katsoa joko **käyttäjän** toimenkuvan näkökulmasta (työrooli) tai hänellä **palvelujärjestelmissä** olevien valtuuksien näkökulmasta
Käyttäjätili	user account	**käyttäjän** ja **palveluntarjoajan** välinen sopimus, joka mahdollistaa verkkopalvelujen käytön
Käyttäjätunnus	user identifier; user name; user ID	**tunnistamista** varten annettu **käyttäjätilin** yksilöivä **tunniste**
Käyttövaltuushallinto	usage rights management; access management	**käyttöoikeus-** ja **käyttäjien valtuustietojen** ylläpito
käyttövaltuus; käyttöoikeus	usage right; access right	tietojärjestelmän **käyttäjälle** tai esimerkiksi tietyn **käyttäjäroolin omaavalle** käyttäjäryhmälle myönnetty yksilöity oikeus nimetyn **palveluelementin** tai muun kohteen käyttöön Käyttövaltuus määrittelee, miten ja millaisilla edellytyksillä **käyttäjällä** on oikeus käyttää ao. **palveluelementtiä**
Luottamusverkosto	circle of trust, trust circle	joukko **palvelutarjoajia** ja **tunnistajia**, joiden kanssa **käyttäjät** voivat asioida turvallisesti kuin yhdessä ympäristössä
Palveluelementti	service element	**palvelujärjestelmän** toiminto tai tieto, jonka käyttöä halutaan erikseen valvoa
Palvelujärjestelmä	service system	tietojärjestelmä, joka tarjoaa **käyttäjille** sovelluspalveluja
palveluntarjoaja; palveluntuottaja	service provider	**palvelujärjestelmän** omistaja ja ylläpitäjä
provisiointi	provisioning	**käyttäjä-** ja **käyttövaltuus**tietojen välittäminen **palvelujärjestelmiin**
pääsynvalvonta	access control	tiedot, toiminnot ja menettelyt, joiden avulla **palvelujärjestelmän** tai sen **palveluelementtien** käyttö mahdollistetaan vain valtuutetuille **käyttäjille**
rekisteröinti	registration	prosessi, jossa **käyttäjälle** perustetaan **käyttäjäidentiteetti** ja annetaan siihen liittyvät **tunnistetiedot** ja **-välineet**
rooliperustainen pääsynvalvonta	role-based access control	**käyttäjärooleihin** ja niihin liitettyihin **käyttövaltuuksiin** perustuva **pääsynvalvonta**politiikka

Termi	**englanninkielinen vastintermi**	**määritelmä**
SAML;	Security Assertions Markup Language	XML-pohjaisia standardeja kehittävän OASIS-standardointijärjestön standardi, jossa määritellään tapa välittää järjestelmien välillä **tunnistamis-** ja **todentamistietoja**
SPML;	Service Provisioning Markup Language	XML-pohjaisia standardeja kehittävän OASIS-standardointijärjestön standardi, joka kuvaa palvelumääritysten siirrossa järjestelmästä toiseen sovellettavia käytäntöjä
todennus; todentaminen	authentication; verification	k**äyttäjän** aitoudesta varmistuminen halutulla luottamustasolla Todentamisessa nojaudutaan johonkin jota a) käyttäjä tietää, b) käyttäjällä on tai c) käyttäjä on.
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.
tunnistusseloste; seloste	assertion	**tunnistajan palvelujärjestelmälle** toimittama selvitys, joka sisältää todennettua **käyttäjäidentiteettiä** vastaavia tietoja ao. **käyttäjästä** Esimerkkejä tunnistusselosteista ovat **SAML**-selosteet ja evästeet.
Tunnistusväline	token	sähköisen **tunnisteen** käyttämiseen ja suojaamiseen tarkoitettu väline' Tunnistusvälineitä ovat esimerkiksi sirukortti tai matkapuhelimen SIM-kortti.
Työrooli	business role	**käyttäjän** toimenkuvaan kuuluvat tietotarpeet ja toimintavaltuudet

Termi	**englanninkielinen vastintermi**	**määritelmä**
vahva tunnistus; vahva tunnistaminen	strong identification	**käyttäjän tunnistaminen** käyttäen vähintään kahta eri **todennus**tapaa Vahvaa tunnistamista on esimerkiksi se, kun pankkikortilla maksettaessa maksajalta vaaditaan sekä pankkikorttia että siihen liittyvän tunnusluvun tietämistä.
valtuustieto/-tiedot	credential(s)	todiste valtuuksien omaamisesta tai viestin lähettäjän aitoudesta
valtuutus	authorisation; authorization	**todennetulle käyttäjälle** annettu lupa tietyn tiedon, suojattavan kohteen tai muun **palveluelementin** käyttöön voimassa olevien **pääsynvalvontatietojen** perusteella
verkostoidentiteetti; yhdistetty identiteetti	network identity, federated identity	**käyttäjän yhdistettyjen käyttäjäidentiteettien** yhdessä määrittelemä joukko käyttäjän ominaisuuksia
XACML;	Access Control Markup Language	XML-pohjaisia standardeja kehittävän OASIS-standardointijärjestön standardi, jonka avulla voidaan määritellä ja esittää **käyttövaltuuksia**

LIITE 5 LÄHTEITÄ

Riskianalyysiin liittyviä ohjeita:

- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management

Hyvään tiedonhallintatapaan, tietoturvallisuuteen ja tietoaineistojen luokitteluun ja käsittelyyn liittyviä ohjeita:

- Hyvän tiedonhallintatavan määritys, VM:n työryhmämuistio 11/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002

Muita VAHTI:n ohjeita ja suosituksia (Tähän lista kaikista ohjeista)

- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003
- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003

Muita kotimaisia lähteitä

- Hyvän tiedonhallintatavan määritys, VM:n työryhmämuistio 11/2000
- Kartoitus tietojärjestelmien käyttäjähallinnasta korkeakouluissa, KATO-projekti 15.10.2002
- Korkeakoulujen HAKA-projektin tulokset 2002-2004 (http://www.csc.fi/suomi/funet/middleware/projektit/haka/index.phtml)
- Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt, STAKES 24.8.2005

Lisäksi työryhmän jäsenorganisaatioiden ei-julkisia aineistoja.

Ulkomaisia lähteitä

- Registration and Authentication, Office of the e-Envoy UK 2002
- HMG's Minumum Requirements for the Verification of the Identity of Individuals, Office of the e-Envoy UK 2003
- Identity Management Business Scenario, The Open Group 2002
- Identity Management White Paper, The Open Group 2004
- Liberty Alliancen (http://www.projectliberty.org/) tuottamat spesifikaatiot ja esitys-aineistot

Lisäksi lukuisia käyttövaltuushallintojärjestelmätoimittajien aineistoja.

VOIMASSA OLEVAT VAHTI-JULKAISUT

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

9/2006

KÄYTTÖVALTUUSHALLINNON
PERIAATTEET JA HYVÄT KÄYTÄNNÖT

ISBN 951-804-662-X (nid.)
ISBN 951-804-663-8 (PDF)
ISSN 1455-2566