Käyttöönottosuunnitelma Virtu-kotiorganisaatiolle

Valtiokonttori
Statskontoret
State Treasury

VALTION IT-PALVELUKESKUS ▸ STATENS IT-SERVICECENTRAL ▸ STATE IT SERVICE CENTRE ▸ SILTASAARENKATU 18–20 A, HELSINKI, PL 100, 00054 VALTIOKONTTORI, PUH. (09) 77251, FAKSI (09) 7725 9301, WWW.VALTIOKONTTORI.FI ▸ BROHOLMSGATAN 18-20 A, HELSINGFORS, PB 100, 00054 STATSKONTORET, TFN. (09) 77251, FAX (09) 7725 9301, WWW.STATSKONTORET.FI ▸ SILTASAARENKATU 18–20 A, HELSINKI, P.O. Box 100, FI-00054 STATE TREASURY, TEL +358-9-77 251, FAX +358-9-7725 9301, WWW.STATETREASURY.FI

Asiakirjan muutoshistoria

versio	päiväys	tekijä	tarkastaja	hyväksyjä	Muutoshistoria
1.0	11.12.2009	Mikael Linden		Virtu-käyttöönotto-hankkeen ohjausryhmä	Lisätty Virtun yleiskuvauskappale ja julkaistu.
1.1	12.1.2010	Mikael Linden			Päivitetty VIP:n kilpailuttama uusi auditoija
1.2	4.1.2011	Mikael Linden			VAHTI 2/2010. Teknisiä asioita (mm. uloskirjautuminen) lukuun 5. Auditoinnin hinta-arvio.
1.2.1	12.1.2011	Tapani Puisto			Tarkistettu versio
1.2.2	19.1.2011	Tapani Puisto			Korjattu Virtu-palvelumaksu
1.3.	11.2.2011	Mikael Linden			Lisätty linkki VRK:n palvelinvarmenteisiin ja CSC:n IdP-rekisteröintisivuun

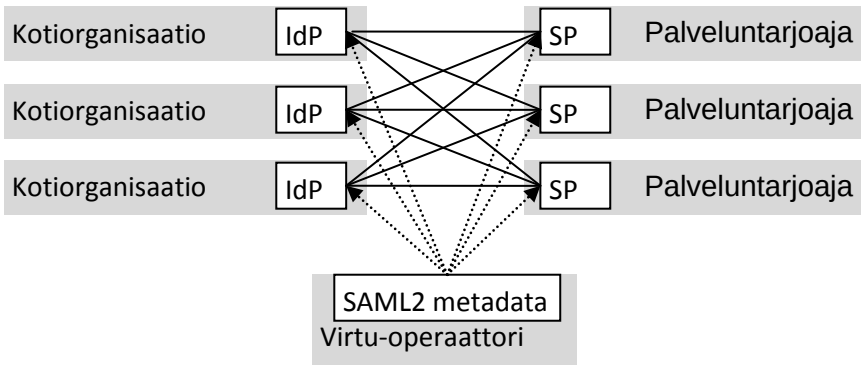
Jakelu

Nimi	Organisaatio

Käyttöönottosuunnitelma Virtu-kotiorganisaatiolle

Virkamiehen tunnistuspalvelu (Virtu) on valtionhallinnon yhteinen käyttäjätunnistusjärjestelmä, jota Valtion IT-palvelukeskus (VIP) tarjoaa organisaatiorajojen ylitse käytettävien palveluiden käyttäjätunnistukseen. Virkamiehen käyttäjätunnistuspalvelussa toteutetaan luottamusverkostomainen työnjako, jossa virkamiehen (tai muun palvelussuhteessa olevan henkilön) kotiorganisaatio (ministeriö, virasto, laitos ym.) vastaa virkamiehen käyttäjätietojen (identiteetin) ylläpidosta järjestelmissään ja kirjautumishetkellä todentaa (autentikointi) hänen henkilöllisyytensä.

Kotiorganisaatio kytkeytyy Virtu-käyttäjätunnistusjärjestelmään ottamalla käyttöön Identity Provider (IdP) –palvelimen ja rekisteröimällä se Virtuun. Vastaavasti palveluntarjoaja, joka haluaa tukeutua Virtu-käyttäjätunnistukseen, niveltää palvelunsa pääsynhallintaan Service Provider (SP) –palvelimen, ja rekisteröi sen Virtuun. VIP:n alihankkijana Virtu-luottamusverkoston päivittäisestä teknisestä toiminnasta vastaa Virtu-operaattori, joka ylläpitää luetteloa (SAML 2.0 metadata) Virtuun rekisteröidyistä Providereista. Tilannetta selkeyttää oheinen kuva.



Tämä dokumentti on yksityiskohtainen käyttöönottosuunnitelma organisaatiolle, joka haluaa rekisteröityä Virtu-käyttäjätunnistusjärjestelmään kotiorganisaationa (Identity Provider).

Käyttöönotto koostuu seuraavista askeleista:

1. **Voiko organisaatiosi VIP:n vallitsevan linjauksen puitteissa ylipäätään liittyä kotiorganisaationa Virtuun?**

   Valtiokonttoria koskeviin säännöksiin perustuva linjaus on, että Virtuun voivat liittyä valtion budjettitalouden piirissä olevat virastot. Tarkista voimassaoleva linjaus VIP:n Virtu-sivustolta www.valtiokonttori.fi/virtu

2. **Mihin Virtussa mukana oleviin palveluihin (Service Provider) organisaatiostasi todennäköisesti halutaan kirjautua?**

   Luettelo Virtuun rekisteröidyistä palveluista löytyy Virtu-operaattorin WWW-sivuilta www.csc.fi/sivut/virtu.

   Kiinnostavien palveluiden tunnistaminen antaa vastauksia mm. seuraaviin kysymyksiin:
   - kuinka korkeaa auditointitasoa kotiorganisaatiosi tietoturvallisuudelta edellytetään?

- mikä joukko organisaatiosi loppukäyttäjistä tulee olla kirjautumisen piirissä?
- mitä henkilötietoja eli attribuutteja palvelu odottaa saavansa kirjautuvasta käyttäjästä?
- kuinka tukevaa autentikointia (salasana vai vahva tunnistus) loppukäyttäjältä edellytetään?

Samalla kannattaa myös kartoittaa, kuinka suuria järjestelyjä palvelupäässä tullaan tarvitsemaan. Tarpeen saattaa esimerkiksi olla kuvata ("mäpätä") olemassaolevat käyttäjätunnukset Virtu-käyttäjätunnisteiksi.

3. Täyttääkö organisaatiosi Virtu-kotiorganisaatiolta vaadittavat auditointitasot?

Auditointi suoritetaan ennen kuin Identity Provider –palvelin rekisteröidään Virtuun (kohta 6). On tarkoituksenmukaista, että organisaatiosi arvioi auditointitason toteutumista (gap analysis) ja suorittaa tarpeen mukaan kohentavia toimenpiteitä jo etukäteen. Näin säästät auditointeihin ja uusinta-auditointeihin menevää aikaa ja rahaa. Auditointitason täyttäminen saattaa olla suurempi ponnistus kuin Virtun edellyttämän teknisen ympäristön rakentaminen.

Palvelun käyttöönotto edellyttää, että Asiakas on auditoitu VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta –ohjeen mukaista korotettua tasoa vastaan ja auditoinnissa havaitut vakavat (kriittiset) poikkeamat on hyväksytysti korjattu. Asiakkaan on laadittava toimenpidesuunnitelma muiden kuin vakavien (kriittisten) poikkeamien korjaamiseksi. Lisäksi viraston tulee esittää suunnitelma korotetun tason saavuttamisesta.

Vaatimusta tullaan nostamaan perustasolta korotetulle tasolle myöhemmin – aikaisintaan lokakuussa 2013, kun perusturvataso asetetaan valtionhallinnolle velvoittavaksi. Joillain Virtussa mukana olevilla palveluilla (Service Provider) voi olla kuitenkin tätä korkeammat vaatimukset kotiorganisaatioille.

4. Tunnista kotiorganisaatiostasi se käyttäjätietokanta, jota vasten kirjautuminen organisaatiosta Virtuun tapahtuisi

Käyttäjätietokannassa tulisi olla käyttäjätunnus kaikille loppukäyttäjille, joilla on tarve kirjautua Virtuun rekisteröityihin palveluihin (Service Provider). Edelleen käyttäjätietokannassa tulisi olla tarpeelliset attribuutit käyttäjistä. Jotkut Identity Provider -tuotteet tukevat myös attribuuttien keräilyä useastakin eri tietokannasta, mikä toki sekin edellyttää suunnitelmallisuutta.

Virtu-määrityksiin kuuluva Virtu-skeema määrittelee pakolliset attribuutit sekä muita attribuutteja. Pakollinen attribuutti tarkoittaa, että se tulee olla populoituna (so. sillä tulee olla annettuna arvo) jokaiselle loppukäyttäjälle Virtussa. Lisäksi yksittäisten palveluiden (Service Provider) käyttäminen saattaa edellyttää myös muiden attribuuttien populoimista. Lisätietoa eri palveluiden tarvitsemista attribuuteista on Virtu-operaattorin www-sivuilla (www.csc.fi/sivut/virtu).

Vahva autentikointi tulisi olla saatavilla, jos Virtussa mukana olevat palvelut (Service Provider) sitä edellyttävät.

5. Hanki ja ota käyttöön SAML 2.0 Identity Provider -palvelin, ja yhdistä se organisaatiosi käyttäjätietokantaan

Vaihtoehtona on ainakin oman SAML 2.0 -tuotteen lisenssin hankkiminen tai Identity Providerin hankkiminen palveluna (IdP SaaS). Markkinoilla on erilaisia IdP SaaS –palvelukonsepteja, esim.

- palveluntarjoajan IdP-palvelin kytketään kotiorganisaation LDAP-hakemistossaan ylläpitämiin käyttäjätietoihin
- palveluntarjoajan IdP-palvelimella on oma käyttäjähakemisto, jota replikoidaan kotiorganisaation LDAP-hakemistosta
- palveluntarjoajan IdP-palvelimella on oma käyttäjähakemisto, jossa käyttäjien tilejä ja attribuutteja ylläpitää kotiorganisaation nimeämä pääkäyttäjä.

Identity Provider -palvelimen tulee tukea Virtun SAML 2.0 –profiilia. Markkinoilla on runsaasti soveltuvia kaupallisia ja open source .-toteutuksia. VIP ei erityisesti anna tuotteille "Virtu-yhteensopiva" -leimoja. Virtu-operaattorille kertyy kuitenkin kokemusta erilaisten tuotteiden yhteensopivuudesta Virtussa, joita kotiorganisaatiosi voi tiedustella.

Identity Provider -palvelimen teknistä ympärstöä suunnitellessa kannattaa huomioida mm. seuraavaa

- Voit halutessasi kytkeä Identity Provider –palvelimen **organisaation kertakirjautumisjärjestelmään**, kuten työasemakirjautumiseen. Tällöin esimerkiksi riittäisi, että työntekijä kirjautuu aamulla työasemalleen, ja Virtu-palveluihin (Service Provider) mentäessä ei normaalisti enää kysyttäisi salasanaa. Jotkut palvelut saattavat kuitenkin eksplisiittisesti pyytää käyttäjän uudelleenautentikointia (SAML 2.0 Force Authentication).
- Sisäänkirjautumiseen nähden käänteinen toimenpide on **uloskirjautuminen** (SAML 2.0 Single Logout): käyttäjä painaa ”logout”-nappia palvelussa (Service Provider), mikä liipaisee uloskirjautumisen myös Identity Provider –ympäristöstä ja edelleen mahdollisesti muista palveluista, joissa käyttäjällä on istunto. Halutaanko Identity Provider –ympäristön tukevan uloskirjautumista, ja onko se teknisesti mahdollista? Uloskirjautumisen toteuttaminen voi olla haastavaa esimerkiksi tilanteessa, jossa sisäänkirjautuminen on kytketty työasemakirjautumiseen. Virtu-luottamusverkostossa tuki uloskirjautumiselle on vapaaehtoista sekä Identity että Service Providereille.
- Voit harkintasi mukaan sijoittaa Identity Provider -palvelimen kokonaan organisaatiosi **palomuurin sisäpuolelle**, jolloin se on paremmin suojassa ulkoverkosta tulevilta palvelunesto- ja muilta hyökkäyksiltä. Tällöin palomuurin ulkopuolelta kirjautuvan loppukäyttäjän tulee ensin ottaa VPN-yhteys organisaatiosi sisäverkkoon.

Virtu-operaattori tarjoaa organisaatiosi käyttöön testipalvelimen (Service Provider), jota vasten voit testata Identity Provider -installaatiosi toimintaa (http://www.csc.fi/sivut/virtu/tekniikka/testipalvelimet). Virheilmoitusten ja lokien avulla Virtu-operaattori voi olla avuksi virheen selvittämisessä, mutta ensisijaisesti organisaatiosi tulisi kuitenkin tukeutua Identity Provider –tuotteen toimittajan tarjoamaan tukeen.

6. Ota yhteyttä VIP:n Virtu-palveluun (virtu@valtiokonttori.fi) Identity Provider -ympäristön auditoinnin sopimista varten

Lisätietoa auditoinnista on kohdassa 3.

7. Allekirjoita Virtu-palvelusopimus

Virtu-palvelusopimus on liite organisaatiosi ja VIP:n väliseen puitesopimukseen VIP:n palveluista. Sopimuksen allekirjoittamista varten ota yhteyttä VIP:n Virtu-palveluun (virtu@valtiokonttori.fi)

8. Rekisteröi Identity Provider -palvelimesi Virtuun

Identity Provider rekisteröidään Virtu-luottamusverkostoon Virtu-operaattorin WWW-sivuilta (Lisätietoa: http://www.csc.fi/sivut/virtu/tekniikka/ohjeet_ja_suositukset). Rekisteröimisen yhteydessä

Identity Provider -palvelimen tekninen toimivuus varmistetaan vielä Virtu-operaattorin testipalvelimia vasten. Rekisteröitävältä Identity Provider -palvelimelta edellytetään Väestörekisterikeskuksen palvelinvarmennetta (lisätiedot Väestörekisterikeskuksesta: www.fineid.fi > Varmennepalvelut > Yhteisöille). Virtu-operaattori lisää Identity Provider -palvelimesi Virtu-käyttäjätunnistusjärjestelmän IdP Discovery Service -palveluun ja metadataan, joka julkaistaan operaattorin WWW-sivuilla.

9. Kerro tarpeen mukaan Virtu-kirjautumiseen siirtymisestä niille Virtussa mukana oleville palveluille, joissa haluat Virtu-kirjautumisen käyttöön.

Jos palvelu (Service Provider) noutaa päivitetyn Virtu-metatiedon Virtu-operaattorilta säännöllisesti, tunnistaa se myös uudet Identity Providerit automaattisesti.

Jos käyttöönottoon kuitenkin liittyy vanhan tunnistustavan korvaaminen Virtu-kirjautumisella, tarvitaan tyypillisesti muunnosajo, jossa organisaatiosi olemassa olevat käyttäjätunnukset kuvataan ("mäpätään") Virtun käyttäjistä käyttämiin tunnisteisiin (Lisätietoa Virtu-skeemassa). Edelleen kirjautumissivua tarvitsee usein muuttaa niin, että käyttäjätunnuksen kysymisen sijaan käyttäjä ohjataan Virtu-kirjautumiseen. On hyvä huomata, että palvelusta ja työn laajuudesta riippuen tästä saattaa syntyä palveluntarjoajalle kustannuksia, jotka se haluaa periä kotiorganisaatiolta. Tämä on tilanne mm. Valtiokonttorin ostolaskun hallinnan ja matkanhallinnan palveluissa.

Yksinkertaisimmissa palveluissa muutoksia ei tarvita.

10. Järjestä tuki ja koulutus loppukäyttäjille

Virtu-käyttäjätunnistusjärjestelmässä tukea loppukäyttäjille antaa aina hänen kotiorganisaationsa IT-tuki.

Arvioita Identity Provider –käyttöönoton kustannuksista

Identity Provider –palvelimen käyttöönotosta ja rekisteröimisestä Virtuun syntyviä kustannuksia on vedetty yhteen seuraavassa. Tämä dokumentti on vain ohjeellinen ja laadittu lähinnä helpottamaan Virtu-kotiorganisaatioita kokonaiskuvan saamisessa. Yksityiskohtainen hinnoittelu on aina syytä tarkistaa tapauskohtaisesti asianomaisesta lähteestä.

Virtu-luottamusverkoston kustannusanalyysi, joka sisältää myös Virtusta saatavat säästöt, on esitetty Virtu-esitutkimusraportissa http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070625Virkam/name.jsp

Kustannus	Suuruusluokka	Muuta
Identity Provider –lisenssi	20 e/käyttäjä/vuosi	Open Source –tuotteet ovat ilmaisia
Identity Provider –käyttöönotto	10 000 – 50 000 e	
Identity Provider –ylläpito	3 600 – 40 000 e/vuosi	
Vaihtoehtoisesti: IdP as a service	Markkina on syntymässä	Todennäköisesti kiinteä ja käyttäjämäärän mukaan muuttuva hintakomponentti
Identity Provider –ympäristön auditointi	5000-6000 eur	Lisäksi organisaationi saattaminen vaaditulle tietoturvatasolle voi vaatia paljonkin työtä organisaatiossa.
Palvelinvarmenne VRK:lta	250 e/vuosi	
VIP:n Virtu –palvelumaksu	2000 e/vuosi + 7 e/käyttäjä/vuosi	