Käyttöönottosuunnitelma Virtu-palveluntarjoajalle

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	4.1.2011	Mikael Linden			VAHTI 2/2010. Lisää yksilöivästä tunnisteesta lukuun 6. Uusi luku 8 uloskirjautumisesta
1.2.	11.2.2011	Mikael Linden			Lisätty kustannusarvioihin VIP:n perimä palvelumaksu
1.3.	7.10.2011	Mikael Linden			Poistettu kustannustaulukosta vanhentunut tieto, jonka mukaan SP ei vaadi VRK:n palvelin-varmennetta

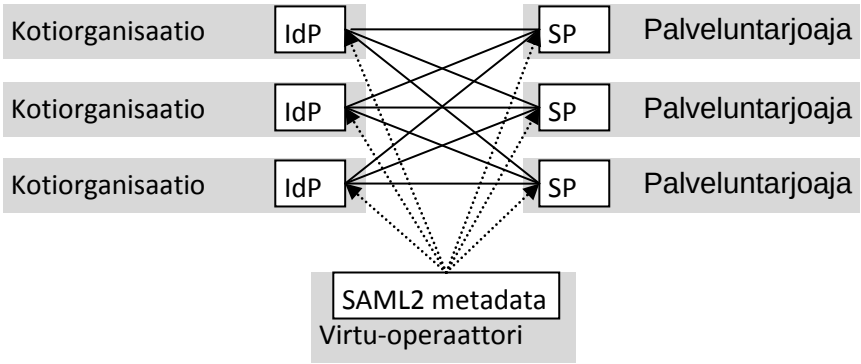
Jakelu

Nimi	Organisaatio

Käyttöönottosuunnitelma Virtu-palveluntarjoajalle

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 ohje on yksityiskohtainen käyttöönottosuunnitelma organisaatiolle, joka haluaa rekisteröidä palvelun (Service Provider) Virtu-käyttäjätunnistusjärjestelmään.

Käyttöönotto koostuu seuraavista askeleista:

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

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. Tunnista palvelusi tietoturvataso

Tunnista palvelusi VAHTI 2/2010 -ohjeen tarkoittamaksi suojattavaksi kohteeksi, ja määrittele sille tietoturvataso. Palvelusi tietoturvatasosta seuraa, mitä tietoturvatasoa Virtu-kotiorganisaatioilta (Identity Provider) edellytetään; esimerkiksi korotetulla tietoturvatasolla olevaan palveluun voi kirjautua vain vähintään korotetulle tietoturvatasolle yltävästä Virtu-kotiorganisaatiosta.

Voi olla, että suojattavaksi kohteeksi on tarkoituksenmukaista tunnistaa vain pieni osa suurempaa kokonaisuutta. Esimerkiksi valtionhallinnon perusrekisteri voidaan kokonaisuudessaan tunnistaa

korotetun tason suojattavaksi kohteeksi, mutta toiminto, jonka kautta kirjautuva virkamies voi pelkästään selata yksittäisiä perusrekisterin tietueita, voidaan tunnistaa perustason suojattavaksi kohteeksi. Tällöin perusturvatason täyttyminen Virtu-kotiorganisaatiossa mahdollistaisi selailukäyttäjän Virtu-kirjautumisen.

Virtu-käyttäjätunnistusjärjestelmään liittyminen ei sinällään edellytä, että palvelu myös auditoidaan Tietoturvatasot-käsikirjaa vasten. Auditointivaatimus voi kuitenkin seurata jostain muualta, esimerkiksi palvelun omistavan viraston toimintakäytännöistä.

Tunnista palvelusi edellyttämä käyttäjätunnistuksen vahvuus: tuleeko loppukäyttäjä tunnistaa vahvasti, vai riittääkö tavanomainen, salasanaan perustuva tunnistus.

3. Kartoita palvelusi loppukäyttäjät ja heitä koskevat rajaukset

Selvitä, ovatko palvelusi loppukäyttäjät Virtu-käyttäjätunnistusjärjestelmän piirissä. Kohdassa 1. esitettiin, minkälaiset organisaatiot ylipäätään voivat liittyä Virtuun. Lisäksi on tarpeen selvittää, ovatko loppukäyttäjien kotiorganisaatiot myös käytännössä rekisteröineet Virtuun Identity Provider –palvelimen, ja onko loppukäyttäjillä siihen käyttäjätunnus.

Ratkaise, miten mahdolliset Virtu-tunnistuksen ulkopuolelle jäävät loppukäyttäjät tunnistetaan. Onko mahdollista, että palvelussasi on käytössä kaksi rinnakkaista tunnistustapaa, jossa Virtu-tunnistamisen rinnalla on käytössä palvelun kannalta paikallisia käyttäjätunnuksia niille, jotka eivät voi kirjautua Virtun kautta? Vai onko tarkoituksenmukaista, että paikalliset käyttäjätunnukset siirretään palvelusta ulos sen yhteydessä olevaan erilliseen Identity Provider –palvelimeen, jolloin palvelussa tarvitsisi ylläpitää vain yhdenlaista pääsynvalvontamekanismia?

Käytetäänkö palveluasi www-selaimella? Onko palvelullasi ehkä myös client/server-käyttäjiä? Virtu ja sen käyttämä SAML-profiili on tarkoitettu lähtökohtaisesti www-ympäristöön. Jos osa käyttäjistä (esim. pääkäyttäjät) käyttävät palvelua muulla tavalla, on heitä varten todennäköisesti säilytettävä myös vanha kirjautumistapa.

Onko palvelullasi sellaisia käyttäjiä, joilla on palveluun useita eri käyttäjätunnuksia, esimerkiksi yksi käyttäjätunnus per rooli? Normaalisti käyttäjällä on kotiorganisaationsa Identity Provider –palvelimessa vain yksi käyttäjätunnus. Tällaiset käyttäjät täytyy joko rajata Virtu-kirjautumisen ulkopuolelle tai heitä varten tarvitaan palvelussa normaalista poikkeavia järjestelyjä.

4. Päätä, mihin asioihin haluat Virtua hyödyntää

Virtu-luottamusverkostoa voidaan käyttää kolmeen asiaan

1. **Käyttäjän tunnistus** (autentikointi), joka on SAML-tekniikan tyypillisin käyttötapa: loppukäyttäjän Identity Provider –palvelin suorittaa käyttäjän henkilöllisyyden todentamisen, ja ojentaa Service Provider –palvelimelle SAML-tunnistusselosteen (SAML assertion), joka sisältää käyttäjän yksilöivän tunnisteen ja tiedon tunnistustavasta.

2. **Käyttäjätilien ja -tietojen ylläpito** palvelussa (provisiointi), jolloin SAML-tunnistusseloste sisältää käyttäjän yksilöivän tunnisteen lisäksi myös muita käyttäjän attribuutteja, joita palvelu tarvitsee. Kun loppukäyttäjä kirjautuu palveluun ensimmäistä kertaa, hänen käyttäjätilinsä palveluun perustetaan ”lennosta” tunnistusselosteesta saatavien attribuuttien avulla.

3. **Käyttövaltuuksien välittäminen** (auktorisointi), jolloin käyttäjän käyttövaltuudet palvelussa perustuvat tunnistusselosteesta saataviin attribuutteihin (katso seuraava kohta).

5. Tunnista, mihin palvelusi käyttövaltuus perustuu

Palvelun käyttövaltuuksien hallinta Virtu-luottamusverkostossa voidaan tehdä ainakin kolmella tavalla:

1. Käyttövaltuutta ylläpidetään kokonaan palvelussa (esimerkiksi palvelussa ylläpidetään tieto, että käyttäjä "tammi03",kotiorganisaationa "virastoy.fi" on oikeutettu palvelun käyttöön selailuoikeuksin). Tällöin Virtua käytetään pelkästään käyttäjän tunnistukseen, mutta hänen käyttövaltuutensa hallitaan Virtun ohi.

2. Käyttövaltuutta ylläpidetään kokonaan kotiorganisaatiossa. Kirjautumishetkellä kotiorganisaation Identity Provider –palvelin ojentaa palvelulle attribuutin, jonka perusteella palvelu antaa hänelle käyttöoikeuden (esimerkiksi palveluun on konfiguroitu, että jokainen käyttäjä, jolla on attribuutti ”virtuPersonEntitlement=http://valtiokonttori.fi/rondo/TTY/1234/hyvaksyja” on oikeutettu TTY:n ostolaskujen hyväksyntään vastualueessa 1234)

3. Käyttövaltuus perustuu rooliin, jonka kotiorganisaatio ylläpitää ja ojentaa kirjautumishetkellä palveluun (esim. palveluun on konfiguroitu, että jokainen käyttäjä, jolla on attribuutti "virtuHomeOrganizationType=valtionhallinto" on oikeutettu palvelun käyttöön).

Paitsi palvelun pääsynvalvontaratkaisulta, yllä olevat vaihtoehdot vaativat erilaisia valmiuksia myös kotiorganisaatioilta. Vaihtoehto 1 on suoraviivainen, mutta edellyttää pääsääntöisesti loppukäyttäjien käyttövaltuuksien ylläpitoa palvelussa käsin. Vaihtoehto 2 mahdollistaa palvelun käyttäjähallinnon syvän integroinnin kotiorganisaation prosesseihin ja tietojärjestelmiin, mutta edellyttää käytännössä, että kotiorganisaatiolla on käytössä edistynyt identiteetinhallintajärjestelmä, johon sisältyy joko täysin automaattinen tai sähköisesti kierrätettäviin lomakkeisiin (workflow- eli työnkulkujärjestelmät) perustuva käyttövaltuuksien hallintajärjestelmä. Vaihtoehto 3:n keskeinen ongelma on tarkoitukseen sopivan sanaston löytäminen roolitukselle, mutta malli saattaa riittää jos pääsynvalvonta tapahtuu karkealla perusteella (esimerkiksi palvelu avautuu kaikille virkamiehille tietyltä hallinnonalalta).

Parhaassa tapauksessa sama palvelu pystyisi mukautumaan eri valmiustasolla oleviin kotiorganisaatioihin; aloittava organisaatio toimisi palvelussa mallin 1. mukaan, kun taas edistynyt organisaatio toimisi mallin 2. mukaan.

6. Mitä tietoja palvelu tarvitsee kirjautuvasta käyttäjästä

Virtu-luottamusverkostossa käytetyt yhteiset attribuutit on esitetty Virtu-skeema –dokumentissa. Kaikki kotiorganisaatiot eivät välttämättä pysty populoimaan jokaista attribuuttia (so. antamaan attribuutille arvoa), mutta ainakin pakollisiksi kirjatut attribuutit on saatavilla jokaiselle loppukäyttäjälle. Tarkista Virtu-operaattorin www-sivuilta, mitä attribuutteja kukin kotiorganisaatio kykenee tarjoamaan. Lisäksi voit määritellä palveluasi varten omia attribuuttejasi ja pyytää kotiorganisaatioita populoimaan ne.

Jos palvelusi tarvitsee käyttäjästä yksilöivän tunnisteen, päätä mitä attribuuttia tarkoitukseen käytetään. Virtu-skeema määrittelee erityisesti attributtiparin (virtuLocalID, virtuHomeOrganization), jonka arvot (esim. tammi03, virastoy.fi) yksilöivät käyttäjän ja ovat yhdessä ikuisesti uniikki tunniste. virtuHomeOrganization-attribuuttiin sisältyy myös Service Providerissa tehtävä tietoturvaa lisäävä tarkistus, joka varmistaa että vain Virasto Y:n Identity Provider voi antaa sille arvon virastoy.fi.

Vaihtoehtoisesti myös SAML 2.0 –määrityksen mukaista Persistent NameID –tunnistetta voi käyttää käyttäjän yksilöimiseen, mutta haittapuolena on sen arvojen mahdollinen rikkoutuminen virastojen Identity Provider –järjestelyjen muuttuessa. Virtu-skeema sisältää attribuutin myös mm. sähköiselle asiointitunnukselle ja henkilökuntanumerolle, mutta kannattaa huomioida että niitä ei välttämättä ole olemassa kaikille käyttäjille.

Henkilötietolain mukaan henkilötietojen tarpeeton käsittely on kiellettyä. Vaikka kotiorganisaatiolla olisi loppukäyttäjistään tarjolla runsaastikin erilaisia attribuutteja, palvelu voi pyytää kirjautuvasta käyttäjästä vain palvelun kannalta tarpeellisia attribuutteja.

7. Miten tunnistuslähteen päättelypalvelu toteutetaan

Tunnistuslähteen päättelypalvelu (Identity Provider Discovery) tarkoittaa mekanismia, jolla palvelu (Service Provider) päättelee, mihin Identity Provider –palvelimeen kirjautuva käyttäjä ohjataan tunnistettavaksi. Virtussa tunnistuslähteen päättely voi tapahtua esimerkiksi

- tukeutumalla Virtu-operaattorin tarjoamaan keskitettyyn Identity Provider Discovery –palveluun (katso Virtu SAML-määritys), joka tyypillisesti antaa loppukäyttäjän valita pudotusvalikosta oman Identity Provider –palvelimensa.
- upottamalla edellä mainittu pudotusvalikko tai vastaava toiminto suoraan palveluun, jolloin se voidaan räätälöidä palvelun kannalta tarkoituksenmukaisella tavalla.
- sijoittamalla tarkoitusta varten muotoiltu kirjautumislinkki suoraan kotiorganisaation Intranet-sivustoon (ns. IdP first –skenaario).

8. Tuetaanko uloskirjautumista

Sisäänkirjautumisen yhteydessä käyttäjälle syntyy selainistunto sekä Identity että Service Provider –palvelimeen. Kun käyttäjä kirjautuu ulos Service Provider –palvelimesta (esim. painamalla ”logout” tai ”kirjaudu ulos”-nappia), tulee Service Provider –ympäristön lisäksi istunto purkaa myös Identity Provider –palvelimesta. Jos Identity Provider –istunnon purkaminen laiminlyödään, pääsee uloskirjautunut käyttäjä uudelleen sisälle palveluun ilman autentikoitumista, mitä voidaan pitää tietoturvaongelmana tai ainakin palvelun kirjautumisen epäjohdonmukaisena toimintana.

Tavallisesti selaimen sulkeminen on varmin tapa päättää selainistunto, mutta SAML 2.0 -standardi sisältää myös vapaaehtoisen uloskirjautumistoiminnon (SAML 2.0 Single Logout). Kun loppukäyttäjä painaa ”logout”-nappia Service Providerissa, se lähettää Identity Providerille pyynnön purkaa käyttäjän istunto myös siellä. Vastavuoroisesti Identity Provider voi lähettää Service Providerille pyynnön purkaa käyttäjän istunto (esimerkiksi koska käyttäjä on painanut Logout-nappia jossain toisessa Service Providerissa).

Virtun SAML-profiilissa tuki uloskirjautumiselle on vapaaehtoinen sekä Identity että Service Provider –palvelimille. Niinpä Service Provider –palvelimella on seuraavat vaihtoehdot:

1. Service Provider ei tue lainkaan uloskirjautumista. Kun käyttäjä painaa ”logout” –nappia palvelussa, hänelle tulostetaan sivu, jossa kehotetaan sulkemaan selain.
2. Service Provider tukee uloskirjautumista (minkä tunnusmerkkinä se rekisteröi SingleLogoutService –osoitteensa Virtun SAML 2.0 -metadataan), mikä tarkoittaa että se osaa sekä lähettää että vastaanottaa uloskirjautumispyyntöjä. Tällöin tulee huomioida lisäksi, että
    a. Kaikki Identity Provider –palvelimet eivät välttämättä tue uloskirjautumista (minkä tunnusmerkkinä Identity Providerilla ei ole SingleLogoutService-osoitetta Virtu-

metadatassa). Näiden Identity Provider –palvelinten kohdalla jäänee vaihtoehdoksi 1-kohdan mukainen toiminta.

b. Vaikka Identity Provider –palvelin tukisikin uloskirjautumista, voi olla että uloskirjautuminen ei juuri tämän käyttäjän kohdalla ole mahdollinen (esimerkiksi siksi, että käyttäjä on kirjautunut toimikortilla, jonka istuntoa ei voi purkaa muuten kuin vetämällä kortin lukijasta). Tällöin Identity Provider –palvelin vastaa uloskirjautumispyyntöön virhesanomalla. Service Provider –palvelimen vaihtoehdoksi jää jälleen 1-kohdan mukainen toiminta.

9. Hanki ja ota käyttöön SAML 2.0 Service Provider -palvelin, ja yhdistä se palvelusi pääsynhallintaan

Vaihtoehtonasi on ainakin Service Provider –moduulin tai -kirjaston integrointi suoraan palveluun, tai erillisen pääsynvalvontaa suorittavan edustapalvelimen hankkiminen palvelun eteen. Tällöin edustapalvelimella voidaan ratkaista myös sellaisten käyttäjien tunnistaminen, joiden kotiorganisaatiolla ei ole Identity Provider –palvelinta (katso kohta 3).

Tarjolla on erilaisia kaupallisia ja avoimen lähdekoodin SAML 2.0 Service Provider -toteutuksia. Service Provider -palvelimen tulee tukea Virtun SAML 2.0 –profiilia. VIP ei erityisesti anna tuotteille "Virtu-yhteensopiva" –leimoja, mutta Virtu-operaattorille kertyy kuitenkin erilaisten tuotteiden Virtu-yhteensopivuudesta kokemusta, jota kotiorganisaatiosi voi tiedustella.

Virtu-operaattori tarjoaa organisaatiosi käyttöön testipalvelimen (Identity Provider), jota vasten voit testata Service Provider -palvelimesi 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 Service Provider -tuotteen toimittajan tarjoamaan tukeen.

10. 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).

11. Rekisteröi Service Provider -palvelimesi Virtuun

Rekisteröimisen yhteydessä Virtu-operaattori tiedustelee luetteloa attribuuteista, jotka ovat tarpeellisia palvelun kannalta. Voit nojautua joko Virtu-skeemassa määriteltyyn valmiiseen luetteloon attribuuteista, tai noudattaa skeeman ohjeita omien attribuuttien määrittelemisestä.

Rekisteröimisen yhteydessä Service Provider -palvelimen tekninen toimivuus varmistetaan vielä Virtu-operaattorin testipalvelimia vasten.

12. Kerro tarpeen mukaan Virtu-kirjautumiseen siirtymisestä Virtussa mukana oleville kotiorganisaatioille

Olemassaolevaan palveluun tarvitaan tyypillisesti konfiguraatiomuutoksia ja muunnosajo, jossa organisaatiosi olemassa olevat käyttäjätunnukset kuvataan Virtun käyttäjistä käyttämiin tunnisteisiin. Yksinkertaisimmissa palveluissa muutoksia ei tarvita.

Lisäksi kotiorganisaatioiden tulee tarpeen mukaan opastaa ja tukea loppukäyttäjiä uuden kirjautumistavan käyttöönotosta.

Arvioita Service Provider –käyttöönoton kustannuksista

Seuraavassa vedetään yhteen kustannuksia, jotka syntyvät Service Provider –palvelimen käyttöönotosta, integroimisesta palveluun ja rekisteröimisestä Virtuun. Tämä dokumentti on vain ohjeellinen ja laadittu lähinnä helpottamaan Virtu-palveluntarjoajia 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
Service Provider –lisenssi	0 e	Olettaen, että erillistä lisenssiä ei tarvita tai voidaan käyttää Open Source –tuotteita.
Service Provider –käyttöönotto ja –integrointi palveluun	20 000 – 50 000 e	Sisältää mahdollisesti myös olemassa olevien käyttäjätilien muunnosajon Virtun käyttämiin yksilöiviin tunnisteisiin.
Palvelinvarmenne VRK:lta	250 e/vuosi	
Auditointi	0 e	Virtu ei edellytä, että Service Providerit auditoidaan (vaatimus voi toki tulla muuta kautta).
VIP:n Virtu-palvelumaksu	2000 e/vuosi	