Tieto Oyj
Tietokarhu Oy
Markus Virolainen

v. 1.0E
Luottamuksellinen
8.1.2010

Tunnistus.fi & Katso – konnektorituotteen valintaopas

1 Yleistä

Tässä dokumentissa on ohjeistusta konnektorituotteen, josta käytetään myös termiä agentti, valintaan. Tällä ohjelmistokomponentilla asiointipalvelu saa käyttöönsä Tunnistus.fi-tunnistuksenohjauspalvelun (Identity Provider, IDP) tarjoamat tunnistusmenetelmät, kuten Katso-organisaatiotunnistuksen ja Tupas-pankkitunnistuksen.

Dokumentissa opastetaan sopivan konnektorin valintaa mm. käytettävien tunnistusmenetelmien ja asiointipalvelun toteutusteknologioiden/ajoympäristön näkökulmasta.

2 Konnektoritarjonta

Konnektoritarjonta on suhteellisen laaja ja niitä on tarjolla usealta toimittajalta. Ubisecuren tarjoamat konnektorit ovat ensimmäinen vaihtoehto, mutta myös muita SAML 2.0 -standardin toteuttavia SAML SP (Service Provider) -toteutuksia on mahdollista käyttää.

2.1 Ubisecuren konnektorivaihtoehdot

Ubisecurella on laaja valikoima konnektoreja eri ympäristöihin:

Konnektori	**Ympäristö**	**Protokolla**	**Tunnistus**	**Roolikysely**	**€**
Ubilogin Web Agent for .NET	.NET	Ubilogin	Kyllä	Ei	Ei*
Ubilogin Web Agent for Java	Java	Ubilogin	Kyllä	Ei	Ei*
Ubilogin Web Agent for IIS	MS IIS	Ubilogin	Kyllä	Ei	Ei*
Ubilogin Web Agent for Apache	Windows ja Linux	Ubilogin	Kyllä	Ei	Ei*
Ubilogin Web Agent for Lotus Domino	Domino	Ubilogin	Kyllä	Ei	Ei*
Ubilogin SAML SP for ASP.NET	ASP.NET	SAML 2.0	Kyllä	Kyllä	Ei*
Ubilogin SAML SP for Java	Java	SAML 2.0	Kyllä	Kyllä	Ei*
Ubilogin SAML SP for BEA WebLogic Server	BEA WebLogic 9.x	SAML 2.0	Kyllä	Kyllä	Kyllä

Taulukko 1. Ubisecuren konnektoritarjonta

Katve-konsortion jäsenille Web Agent -tyyppisten konnektorien käyttö (merkitty taulukkoon 1 tähdellä) sisältyy sopimukseen, SAML SP -konnektorien (ASP.NET

ja Java) käytöstä on tehty konsortiolaajuinen sopimus, jolloin yksittäisestä SAML SP -konnektorista ei tarvitse maksaa erillistä maksua.

Muiden kuin konsortion jäsenten osalta taulukon 1 konnektorien käyttöoikeus sisältyy Logican veloittamaan TFI/Katso-liittymismaksuun. Käyttöoikeuden voi ostaa joko yhtä asiointipalvelua varten tai rajoittamattomaan määrään asiointipalveluita.

2.2 Muut konnektorivaihtoehdot

SAML SP -konnektoreita löytyy mm. Fujitsulta, jota eräs Katso-hyödyntäjä on palvelussaan käyttänyt. Ilmaisia SAML SP -toteutuksia on myös olemassa (Tanskan OIO SAML ja Shibboleth), mutta näistä ei ole vielä käyttökokemuksia.

Verohallinto tarjoaa Katso-sivustolta ladattavaksi roolikyselykomponentteja, joita voi käyttää esimerkiksi yhdessä Ubisecuren Web Agent -konnektorien kanssa toteutettaessa Katso-roolikyselyä.

Komponentti	**Ympäristö**	**Protokolla**	**Tunnistus**	**Roolikysely**	**€**
VH:n roolikyselykomponentti	Java	SAML 2.0	Ei	Kyllä	Ei
VH:n roolikyselykomponentti	.NET 2.0	SAML 2.0	Ei	Kyllä	Ei

Taulukko 2. Verohallinnon tarjoamat roolikyselykomponentit

3 Konnektorin valintaperusteet

Käytettävän konnektorin valintaperusteita on lähinnä kaksi:

1. Tarvitaanko asiointipalvelussa Katso-roolikysely?

2. Mikä on asiointipalvelun web-kerroksen toteutustekniikka ja käytettävä sovelluspalvelinalusta?

Jos asiointipalvelu tarvitsee Katso-roolikyselyn, on syytä käyttää SAML SP -konnektoreja. Ubisecuren SAML SP -konnektorit sisältävät roolikyselytoiminnallisuuden, jolloin sitä ei tarvitse toteuttaa erillisenä. Ubisecuren SAML SP:t on saatavissa Java- ja .NET-ympäristöihin.

Yleensäkin uusien asiointipalveluiden osalta suositellaan käytettävän SAML SP -konnektoreja, koska ne käyttävät SAML 2.0 -protokollaa ja ovat siten kansainvälisiä standardeja noudattavia toisin kuin Web Agent -konnektorit, jotka käyttävät Ubisecuren Ubilogin-protokollaa.

Vanhojen, Ubisecuren omaa protokollaa käyttävien Web Agent -konnektorien käyttöä ei suositella kuin niissä tilanteissa, joissa esimerkiksi käytettävän sovelluspalvelimen (esim. Apache tai Lotus Domino) vuoksi ei ole mahdollista käyttää SAML SP -konnektoreja tai niitä ei ole saatavilla. Jos tällaisessa ympäristössä tar-

vitaan Katso-organisaatiotunnistamista, roolikysely voidaan toteuttaa käyttäen verohallinnon tarjoamia Katso-roolikyselykomponentteja.

Seuraavassa taulukossa on yhteenveto siitä, mitä konnektoria kannattaa käyttää missäkin tapauksessa.

Asiointipalvelun toteutusteknologia tai käytettävä sovelluspalvelin	**Käytettävä konnektori**
Microsoft ASP.NET (.NET FW 2.0)	SAML SP for ASP.NET
Java (Java 5.0 & servlet 2.3)	SAML SP for Java
Apache web server	Web Agent for Apache
Lotus Domino	Web Agent for Lotus Domino
Microsoft SharePoint Services 2003/2007	Web Agent for WSS
BEA WebLogic 9.x	SAML SP for Java tai Ubilogin Web Agent for BEA WebLogic Server

Taulukko 3. Suositeltavat konnektorit ympäristöittäin

3.1 Erityishuomioitavaa

Jos asiointipalvelun testiympäristössä on tarpeen siirtää web-palvelinkerroksen palvelimien kelloja, silloin SAML SP -agenttien käyttö muodostuu haasteelliseksi. SAML-protokolla ei käytännössä siedä pieniäkään aikaeroja IDP:n ja SAML SP:n välillä.

4 Linkkejä ja lisätietoja

Ubilogin Web Agents (25.7.2009): Web Agent.pdf

Ubilogin SAML SP for Java Installation Guide: Ubilogin SAML SP for Java.pdf

Ubilogin SAML SP for ASP.NET Installation Guide: Ubilogin SAML SP for ASP.NET.pdf

Verohallinnon Katso-sivut asiointipalveluiden kehittäjille: http://www.vero.fi/katso > asiointipalveluiden kehittäjät