Versio	Päivämäärä	Muutoshistoria
1.0	5.9.2011	
1.1	2.3.2012	Päivitetty metadataosoite

1 Virtu IdP-palvelimen testiohjeet

Virtuun liitettävää IdP-palvelinta voi testata operaattorin testipalveluiden kanssa. Testipalveluiden käyttö edellyttää IdP-palvelimen liittämistä operaattorin testipalveluun. Ohjeet palveluun liittämistä varten ovat operaattorin www-sivuilla: http://www.csc.fi/sivut/virtu/tekniikka/testipalvelimet

Testipalveluita käytettäessä tulee testaajan varmistua itse oman IdP-palvelimensa toiminnasta. Pelkkä palveluiden näennäinen toiminta testipalveluiden kanssa ei takaa IdP-palvelimen täyttävän kaikkia Virtun vaatimuksia.

SAML 2.0 on laaja määritys, joka sisältää lukuisia toiminnallisuuksia ja myös monia keskenään vaihtoehtoisia tapoja toteuttaa sama toiminnallisuus. Virtu on poiminut SAML2-määrityksestä varsin suppean osajoukon toimintoja (”Virtu SAML 2.0 profile”), millä pyritään varmistamaan mahdollisimman hyvä yhteentoimivuus eri tuotteiden välille. Lisäksi Virtu-luottamusverkostossa tarpeelliseksi katsotut kirjautuvan virkamiehen perushenkilötiedot (attribuutit) on määritelty Virtu-attribuuttimääritys -dokumentissa.

Organisaation Identity Provider -palvelua (IdP) testattaessa tavoitteena on siirtää testattavasta käyttäjästä henkilötietoja (attribuutteja) Virtu-operaattorin Service Provider -testipalveluun. Testauksella varmistetaan IdP:n noudattavan sovittua Virtun SAML2-profiilia sekä käytettävää attribuuttimääritystä. Osa SAML2-protokollan ominaisuuksista, jotka on määritetty Virtun SAML2-profiilissa, on vapaaehtoisia.

Osalla testipalveluista voi tulostaa IdP:n lähettämän kokonaisen SAML-viestin. Viestin sisällön vertaaminen Virtun SAML-profiilidokumenttiin on tarkin keino varmistua profiilin noudattamisesta.

1.1 Valmistelu

Ennen testauksen aloittamista varmista IdP:stä seuraavat asiat:

- Palvelimen kello on oikeassa ajassa, käytännössä saa aikansa ntp:n avulla.
- IdP on konfiguroitu noudattamaan Virtun SAML2-profiilia.
- Attribuutit on IdP:ssa lähtevissä viesteissä sitetty Virtun attribuuttiskeeman mukaisina.
- Testipalveluiden metadatat on lisätty IdP:iin ja IdP:n metadata on lähetetty testipalvelun ylläpidolle.
- Testipalvelut on konfiguroitu luotetuiksi palveluiksi IdP:ssä
- IdP on konfiguroitu luovuttamaan ainakin attribuuttiskeeman pakolliset attribuutit testipalveluille.

2 Testiympäristö

2.1 Testipalvelu 1

Testipalvelu 1 allekirjoittaa lähettämänsä viestinsä. Käytettynä ohjelmistona on Shibboleth 2.

Testipalvelu 1 tekemän LogoutRquest-viestin allekirjoituksen IdP:n tulee tarkistaa ja hyväksyä. LogoutResponse testipalvelu 1:lle tulee allekirjoittaa.

Autentikointitapana voidaan käyttää Virtun SAML2-profiilin mukaista strong-luokkaa tai määrittelemätöntä.

2.2 Testipalvelu 3

Testipalvelu 3:a voidaan käyttää esim. IdP:n viestin salaamiseen sekä Logout-toiminnon testaamisessa.

Autentikointitapana voidaan käyttää Virtun SAML2-profiilin mukaista strong-luokkaa tai määrittelemätöntä.

2.3 Testipalvelu 4

Testipalvelu 4 lähettää viestit allekirjoittamatta. IdP:n tulee autentikointipyyntöviestiä ei tule hyväksyä. Testipalvelun 4 lähettämää allekirjoittamatonta LogoutRequest-viestiä ei IdP:n tule hyväksyä.

Autentikointitapana voidaan käyttää Virtun SAML2-profiilin mukaista strong-luokkaa tai määrittelemätöntä.

2.4 Yhteenveto

Taulukko tuetuista ominaisuudet eri testipalveluissa:

	Testipalvelu 1	**Testipalvelu 3**	**Testipalvelu 4**
Ohjelmisto	Shibboleth 2	Shibboleth 2	Shibboleth 2
Signed *AuthnRequest*	X	X	
Unsigned *AuthnRequest*			X
Signed *LogoutRequest*	X	X	
Unsigned *LogoutRequest*			X
Encrypted Assertion		X	
Authentication Context Class: *undefined (tyhjä)*	X	X	X
Authentication Context Class: *http://www.valtiokonttori.fi/vip/virtu/AuthnContext/strong*	X	X	X
Force Authentication	X	X	X

3 Testitapaukset

3.1 Metatietojen päivittäminen

3.1.1 Kuvaus

Operaattori julkaisee www-sivuilla Virtu-luottamusverkoston kuvauksen SAML2-metatietoina. IdP:t ylläpitävät säännöllisesti palvelimiensa metatietoja.

3.1.2 Odotettu toiminta

Metatiedon sisältö saadaan tehokkaasti ja helposti lisättyä IdP:n luotettuihin palveluihin.

3.1.3 Suorittaminen

1. Ladataan testimetatieto osoitteesta https://virtu-ds.csc.fi/fed/virtu-test/CSC_Virtu_Test_Servers-metadata.xml
2. Otetaan metatieto käyttöön IdP:ssa.
3. Luottamussuhde testipalveluihin syntyy.

3.2 Palveluiden tarvitsemien attribuuttien päivittäminen

3.2.1 Kuvaus

Operaattori julkaiseen www-sivuilla Virtu-luottamusverkoston kuvaulsen SAML2-metatiedoissa kunkin palvelun tarvitsemat attribuutit. IdP:t ylläpitävät säännöllisesti luovutettavien attribuuttien listaa.

3.2.2 Odotettu toiminta

Attribuuttisäännöt saadaan tehokkaasti ja helposti lisättyä IdP:n konfiguraatioon.

3.2.3 Suorittaminen

1. Ladataan testimetatieto osoitteesta https://virtu-ds.csc.fi/fed/virtu-test/CSC_Virtu_Test_Servers-metadata.xml
2. Otetaan attribuuttisäännöt käyttöön IdP:ssa.
3. Attribuuttisäännöt testipalveluihin ovat käytössä.

3.3 Kirjautuminen, allekirjoitettu AuthnRequest

3.3.1 Kuvaus

Testissä varmistetaan että Virtun SAML2-profiilin mukainen kirjautuminen onnistuu ja attribuutit siirtyvät testipalveluun oikeassa muodossa, jolloin ne näytetään. Kirjautumisessa testipalvelu 1 ei pyydä mitään *authnContextClassRef* -arvoa, mutta SP allekirjoittaa autentikointipyynnön.

3.3.2 Odotettu toiminta

Kirjautuminen onnistuu ja käyttäjästä siirtyy IdP:stä käyttäjää koskevia attribuutteja palvelulle, joka tulostaa ne.

3.3.3 Suorittaminen

1. Siirry testipalveluun 1.
2. Käynnistä testipalvelussa kirjautuminen, jossa *authnContextClassRef* arvoa ei SP:ssä määritetä ja viesti allekirjoitetaan SP:ssa.
3. Kirjaudu testattavassa IdP:ssa. IdP:n ei tarvitse tarkistaa autentikointipyynnön allekirjoitusta.
4. Testipalvelun tulisi tulostaa ne attribuutit, jotka IdP on määritetty luovuttamaan SP:lle. Tähän joukkoon kuuluvat siis vähimmillään Virtun pakolliset attribuutit. Attribuutit näkyvät vain mikäli niiden NameFormat on "*urn:oasis:names:tc:SAML:2.0:attrname-format:uri*" ja Name on attribuutille oikea "*urn:oid...*".
5. Varmista IdP:n logien avulla SAML-viestin sisältö ja vertaa sitä testipalvelun tulostukseen erityisesti attribuuttien osalta.

3.4 Kirjautuminen, allekirjoittamaton AuthnRequest

3.4.1 Kuvaus

Testissä varmistetaan, että Virtun SAML2-profiilin mukainen allekirjoittamattamonta tunnistuspyyntöä ei hyväksytä. Tunnistuspyynnössä testipalvelu ei pyydä *authnContextClassRef* arvoa eikä SP allekirjoita autentikointipyyntöä.

3.4.2 Odotettu toiminta

Kirjautuminen ei onnistu IdP:ssa .

3.4.3 Suorittaminen

1. Siirry testipalveluun 4.
2. Käynnistä testipalvelussa kirjautuminen, jossa *authnContextClassRef* arvoa ei SP:ssä määritetä ja viestiä ei allekirjoiteta SP:ssa.
3. IdP:n ei tule sallia kirjautumista.

3.5 Attribuuttien toiminta-alue (”palo-osastointi”)

3.5.1 Kuvaus

Testissä varmistetaan että IdP:n tarjoama kotiorganisaatioattribuutin (virtuHomeOrganization) arvo sisältyy siihen joukkoon, jota kyseinen IdP-palvelin voi Virtu-metatietojen mukaan käyttää. Esimerkiksi vain valtioneuvoston kanslian IdP-palvelin voi väittää, että kirjautuva käyttäjä on (virtuLocalID=”mvanhanen”, virtuHomeOrganization=”vnk.fi”).

3.5.2 Odotettu toiminta

IdP luovuttaa virtuHomeOrganization-attribuuttina saman merkkijonon kuin on IdP:n metatiedoissa sille asetettu sallituksi. Merkkijono on määritetty IdP:tä liitettäessä testipalveluihin

3.5.3 Suorittaminen

1. Siirry testipalveluun.
2. Käynnistä testipalveluun kirjautuminen.
3. Kirjaudu testattavassa IdP:ssa.
4. Testipalvelu tarkistaa toimitetun kotiorganisaation ja vertaa sitä metatiedoissa oleviin sallittuihin.
5. Tulos näytetään *Identiteetin tila* kohdassa.

3.6 Pakotettu uudelleenkirjautuminen

3.6.1 Kuvaus

SP voi pyytää IdP:ltä käyttäjän tunnistusta vaikka käyttäjällä olisi jo istunto IdP:ssä. Tällöin IdP:n tulee suorittaa uusi käyttäjätunnistus.

3.6.2 Odotettu toiminta

IdP pyytää käyttäjää tunnistautumaan käyttäjän palatessa IdP:iin vaikka istunto on voimassa.

3.6.3 Suorittaminen

1. Siirry testipalveluun 1.
2. Käynnistä testipalveluun kirjautuminen.
3. Kirjaudu testattavassa IdP:ssa.

4. Varmista että istunto on muodostunut.
5. Kirjaudu testipalveluun 1 uudelleen käyttäen ForceAuthn-kirjautumistoimintoa samalla käyttäjällä sulkematta testipalvelua 1 selaimessa.
6. Tarkista että käyttäjätunnistus suoritetaan uudelleen vaikka käyttäjällä on olemassa oleva istunto IdP:ssä.

3.7 Vahvan tunnistuksen pyynnön testaus

3.7.1 Kuvaus

Vahvassa tunnistuspyynnössä SP pyytää IdP:tä tunnistamaan käyttäjän vahvasti. Testataan, miten IdP reagoi SP:n tekemään pyyntöön, jossa authnContextClassRef on
h*ttp://www.valtiokonttori.fi/vip/virtu/AuthnContext/strong*

3.7.2 Odotettu toiminta

IdP suorittaa vahvan tunnistuksen ja palauttaa siitä tiedon palvelulle. Mikäli IdP ei tue vahvaa tunnistusta, se palauttaa virheen.

3.7.3 Suorittaminen

1. Siirry testipalveluun 1.
2. Käynnistä testipalveluun kirjautuminen käyttäen vahvan tunnistamisen linkkiä.
3. Tarkista minkälaisen kirjautumisen IdP käyttäjälle tarjoaa.
4. Tarkista SP:n tulostaman authnContextClassRef:n sisältö.

3.8 Uloskirjautuminen yhdestä palvelusta

3.8.1 Kuvaus

Testillä varmistetaan SAML2 uloskirjautumisen toiminta yhden palvelun ja tunnistuslähteen välillä. Viestit allekirjoitetaan Virtu-profiilin mukaisesti.

3.8.2 Odotettu toiminta

Käyttäjä uloskirjautuu sekä testipalvelusta 1 että IdP:stä.

3.8.3 Suorittaminen

1. Siirry testipalveluun 1.
2. Käynnistä testipalveluun kirjautuminen (Kirjautuminen 1).
3. Kirjaudu testattavassa IdP:ssa.
4. Varmista että istunto on muodostunut.
5. Valitse testipalvelussa 1 uloskirjautuminen. SP lähettää allekirjoitetun uloskirjautumispyynnön.
6. IdP suorittaa uloskirjautumisen IdP:ssä, joka vastaa SP:lle uloskirjautumisen statusviestillä. Lähetetyt viestit ovat allekirjoitettuja.
7. Varmista että käyttäjän istunto on poistunut molemmista testipalveluista.

3.9 Uloskirjautuminen useasta palvelusta

3.9.1 Kuvaus

Testillä varmistetaan SAML2 uloskirjautumisen toiminta kahdesta palvelusta samanaikaisesti. Testissä kirjaudutaan kahteen palveluun, joista toisesta käynnistetään uloskirjautuminen. Lopputuloksena käyttäjä kirjautuu kerralla ulos molemmista palveluista.

3.9.2 Odotettu toiminta

Käyttäjä kirjautuu ulos kaikista palveluista sekä IdP:stä.

3.9.3 Suorittaminen

1. Siirry testipalveluun 1.
2. Käynnistä testipalveluun kirjautuminen (Kirjautuminen 1).
3. Kirjaudu testattavassa IdP:ssa.
4. Varmista että istunto on muodostunut.
5. Kirjaudu testipalveluun 3 samalla käyttäjällä kuin testipalveluun 1, sulkematta testipalvelua 1 selaimessa.
6. Valitse testipalvelussa 1 tai 3 uloskirjautuminen. SP lähettää allekirjoitetun uloskirjautumispyynnön.
7. IdP suorittaa uloskirjautumisen IdP:ssä sekä pyytää palvelulta 2 käyttäjän uloskirjaamista sekä palauttaa SP:lle tiedon uloskirjautumisen statuksesta IdP:ssä. Lähetetyt viestit ovat allekirjoitettuja.
8. Varmista että käyttäjän istunto on poistunut molemmista testipalveluista.