Versio	Päivämäärä	Muutoshistoria
1.0	5.9.2011	
1.1	2.3.2012	Päivitetty metadataosoite

1 Virtu Service Provider -palvelimen testiohjeet

Virtuun liitettävää Service Provider (SP) -palvelinta voi testata operaattorin testipalveluiden kanssa. Testipalveluiden käyttö edellyttää SP-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 SP-palvelimensa toiminnasta. Pelkkä palveluiden näennäinen toiminta testipalveluiden kanssa ei takaa SP-palvelimen täyttävän kaikkia Virtun vaatimuksia.

Organisaation SP-palvelua testattaessa tavoitteena on siirtää operaattorin testitunnistuslähteestä käyttäjätunnistustiedot ja attribuutit testattavaan palveluun. Testauksella varmistetaan SP:n noudattavan sovittua SAML2-protokollaan profiilia sekä käytettävää attribuuttiskeemaa. Osa SAML2-protokollan ominaisuuksista, jotka on määritetty Virtun SAML2-profiilissa, ovat vapaaehtoisia.

1.1 Valmistelu

Ennen testauksen aloittamista varmista SP:stä seuraavat asiat:

- Palvelimen kello on oikeassa ajassa, käytännössä saa aikansa ntp:n avulla.
- SP on konfiguroitu noudattamaan Virtun SAML2-profiilia.
- Attribuutit otetaan vastaan Virtun attribuuttimääritysten mukaisina
- Testipalvelun metadata on lisätty SP:iin ja SP:n metadata on lähetetty testipalvelun ylläpidolle.
- Testipalvelut on konfiguroitu luotetuiksi palveluiksi SP:ssa

2 Testitapaukset

2.1 Metatietojen päivittäminen

2.1.1 Kuvaus

Operaattori julkaiseen www-sivuilla Virtu-luottamusverkoston kuvaulsen SAML2-metatietoina. SP:t ylläpitävät säännöllisesti palvelimiensa metatietoja.

2.1.2 Odotettu toiminta

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

2.1.3 Suorittaminen

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

2.2 Kirjautumisen testaaminen

2.2.1 Kuvaus

Testissä varmistetaan että Virtun SAML2-profiilin mukainen kirjautuminen onnistuu ja attribuutit siirtyvät palveluun oikeassa muodossa.

2.2.2 Odotettu toiminta

Kirjautuminen onnistuu käyttäen allekirjoitettua AuthnRequest-viestiä, jossa ei ole määritetty käyttäjätunnistustapaa ja käyttäjästä siirtyy IdP:stä käyttäjää koskevia attribuutteja palvelulle, joka tulostaa ne.

2.2.3 Suorittaminen

1. Siirry testattavaan palveluun.
2. Käynnistä kirjautuminen, joko ohjaten suoraan testi-IdP:iin tai DS:n kautta..
3. Kirjaudu IdP:ssa sovitulla testikäyttäjätunnuksella.
4. SP:iin siirtyy SAML-viesti, jossa tieto autentikoinnista ja käyttäjästä attribuutit, jotka oli sovittu siirrettäviksi. Attribuuttien NameFormat on "*urn:oasis:names:tc:SAML:2.0:attrname-format:uri*" ja Name on attribuutille oikea "*urn:oid...*".

2.3 Vahvan kirjautumisen testaaminen

2.3.1 Kuvaus

Testissä varmistetaan että Virtun SAML2-profiilin mukainen kirjautuminen onnistuu ja attribuutit siirtyvät palveluun oikeassa muodossa. Kirjautumispyynnössä määritetään *authnContextClassRef* arvoa, mutta SP allekirjoittaa autentikointipyynnön.

2.3.2 Odotettu toiminta

SP tekee allekirjoitetusu AuthnRequest-viestin, jossa pyydetään käyttäjän tunnistamistamista käyttäen tunnistustapana http://www.valtiokonttori.fi/vip/virtu/AuthnContext/strong.

SP vastaanottaa SAMLResponse-viestin, tarkistaa sen ja ottaa käyttöönsä AttributeStatement-osiossa olleet käyttäjäattribuutit.

2.3.3 Suorittaminen

1. Siirry testattavaan palveluun.
2. Käynnistä kirjautuminen, joko ohjaten suoraan testi-IdP:iin tai DS:n kautta. AuthnRequest-viestissä on määritetty *authnContextClassRef* arvoksi http://www.valtiokonttori.fi/vip/virtu/AuthnContext/strong
3. Kirjaudu IdP:ssa sovitulla testikäyttäjätunnuksella. IdP näyttää pyydetyn autentikointitavan.
4. SP:iin siirtyy SAML-viesti, jossa tieto autentikoinnista ja käyttäjästä attribuutit, jotka oli sovittu siirrettäviksi. Attribuuttien NameFormat on "*urn:oasis:names:tc:SAML:2.0:attrname-format:uri*" ja Name on attribuutille oikea "*urn:oid...*".

2.4 Uloskirjautuminen, yksi SP – IdP

2.4.1 Kuvaus
Testissä varmistetaan testattavan SP:n ja testi-IdP:n välinen uloskirjautuminen.

2.4.2 Odotettu toiminta
Testattavaan SP:iin kirjauduttua käyttäjän käynnistäessä uloskirjautumisen, palvelu poistaa mahdollisen oman istuntonsa ja tekee allekirjoitetun LogoutRequest-viestin IdP:lle. IdP vastaa LogoutResponse-viestillä SP:lle.

2.4.3 Suorittaminen
1. Siirry testattavaan palveluun.
2. Kirjaudu palveluun, jollain edellisten testien kuvaamalla tavalla
3. Käynnistä uloskirjautuminen, SP tekee allekirjoitetun LogoutRequest-viestin.
4. IdP vastaa allekirjoitetulla LogoutResponse-viestillä.
5. Istunto palveluun poistuu käyttäjältä.

2.5 Uloskirjautuminen, SP tekee aloitteen

2.5.1 Kuvaus
Testissä varmistetaan usean SP:n, mukaan lukien testattava SP, ja testi-IdP:n välinen uloskirjautuminen kun uloskirjautuminen käynnistetään testattavasta SP:stä.

2.5.2 Odotettu toiminta
Testattavaan SP:iin kirjauduttua käyttäjän käynnistäessä uloskirjautumisen, palvelu poistaa mahdollisen oman istuntonsa ja tekee allekirjoitetun LogoutRequest-viestin IdP:lle. IdP vastaa LogoutResponse-viestillä SP:lle.

2.5.3 Suorittaminen
1. Siirry testattavaan palveluun.
2. Kirjaudu palveluun, jollain edellisten testien kuvaamalla tavalla
3. Kirjaudu samalla käyttäjällä operaattorin testipalveluun.
4. Käynnistä uloskirjautuminen testattavasta palvelusta, SP tekee allekirjoitetun LogoutRequest-viestin.
5. IdP vastaa allekirjoitetulla LogoutResponse-viestillä.
6. Istunto kaikista palveluista poistuu käyttäjältä.

2.6 Uloskirjautuminen, SP vastaanottaa

2.6.1 Kuvaus
Testissä varmistetaan usean SP:n, mukaan lukien testattava SP, ja testi-IdP:n välinen uloskirjautuminen kun uloskirjautuminen on käynnistetty muualta kuin testattavasta SP:stä.

2.6.2 Odotettu toiminta
Testipalvelusta käyttäjän käynnistäessä uloskirjautumisen, testattava palvelu vastaanottaa uloskirjautumispyynnön ja suorittaa uloskirjautumisen.

2.6.3 Suorittaminen
1. Siirry testattavaan palveluun.

2. Kirjaudu palveluun, jollain edellisten testien kuvaamalla tavalla
3. Kirjaudu samalla käyttäjällä operaattorin testipalveluun.
4. Käynnistä uloskirjautuminen operaattorin testipalvelusta.
5. IdP lähettää allekirjoitetun uloskirjautumispyynnön testattavalle palvelulle
6. Istunto testattavasta palveluista poistuu käyttäjältä.

2.7 IdP:stä käynnistyvä kirjautuminen

2.7.1 Kuvaus

Testataan IdP:stä käynnistetty kirjautuminen SP-palveluun.

2.7.2 Odotettu toiminta

Testi-IdP:stä käynnistetään kirjautuminen testattavaan palveluun. IdP tekee AuthnResponse-viestin tunnistettuaan käyttäjän, josta puuttu InResponseTo-elementti. SP tarkistaa viestin ja mikäli luottamussuhde IdP:iin on tehty, käyttäjä päästetään palveluun.

2.7.3 Suorittaminen

1. Siirry testipalveluun 2.
2. Syötä testattavan palvelun entityid sille varattuun kenttään.
3. Käynnistä kirjautuminen luodusta palvelukohtaisesta linkistä.
4. Kirjaudu IdP:ssä.
5. Käyttäjälle luodaan istunto testattavassa palvelussa.

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

2.8.1 Kuvaus

Testissä varmistetaan että SP tarkistaa 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”).

2.8.2 Odotettu toiminta

Suoritetaan käyttäjätunnistus testi-IdP:n kanssa. Sallitun käyttäjän SP päästää palveluun. Virheellisen käyttäjän pääsyn palveluun SP estää.

2.8.3 Suorittaminen

1. Kirjaudu testattavaan SP:iin testi-IdP:ssä sallitulla käyttäjällä.
2. Istunto muodostuu sallitulle käyttäjälle.
3. Poista sallitun käyttäjän istunto testattavasta SP:stä.
4. Kirjaudu testattavaan SP:iin testi-IdP:ssä virheellisellä käyttäjällä.
5. Istuntoa ei tule muodostua virheelliselle käyttäjälle.