Ismo Kyrönlahti

Single Sign-On ja SAML

Tietotekniikan erikoistyö
28. lokakuuta 2006

Jyväskylän yliopisto

Tietotekniikan laitos

Jyväskylä

Tekijä: Ismo Kyrönlahti
Yhteystiedot: ispekyro@cc.jyu.fi
Työn nimi: Single Sign-On ja SAML
Title in English: Single Sign-On and SAML
Työ: Tietotekniikan erikoistyö
Sivumäärä: 25
Tiivistelmä: Tässä erikoistyössä käsitellään Single Sign-On -tekniikoita ja SAML-standardia. Lisäksi esitellään Shibboleth-ohjelmistoprojekti.
English abstract: In this study Single Sign-On techniques and the SAML Standard are discussed. The Shibboleth project is presented.
Avainsanat: tietotekniikka, erikoistyö
Keywords: Information Technology, Special Study

Sisältö

1 Single Sign-On

Tässä luvussa selvitetään Single Sign-On (*suom. kertakirjautuminen*) -käsitettä ja kuvataan erilaisia kertakirjautumisjärjestelmälle asetettavia tavoitteita. Lopuksi esitellään kertakirjautumista hyödyntäviä sovelluksia.

1.1 Johdanto

Tietojärjestelmien siirtyessä tukemaan yhä uusia liiketoiminnan prosesseja käyttäjien ja järjestelmänvalvojien työmäärä kasvaa järjestelmien monimutkaistumisen myötä. Käyttäjät joutuvat kirjautuaman useisiin järjestelmiin ja syöttämään kuhunkin omat käyttäjätunnukset ja käyttäjätietonsa. Järjestelmänvalvojat joutuvat ylläpitämään rinnakkaisten järjestelmien käyttäjätietoja yhtenäisyyden ja turvallisuuden varmistamiseksi [1].

Perinteinen hajautettu järjestelmä koostuu useista eri komponenteista, joista kukin vastaa oman alueensa (*engl. domain*) turvallisuudesta. Komponenteilla on omat alustansa (*engl. platform*) käyttöjärjestelmineen ja sovelluksineen. Komponentit toimivat itsenäisinä kokonaisuuksina siten, että käyttäjän tunnistautuminen vaaditaan erikseen aina, kun siirrytään toimimaan toiselle alueelle.

Käyttäjä aloittaa aluksi istunnon (*engl. session*) ensisijaisen alueen kanssa. Tällöin hän yleensä syöttää käyttäjätunnuksen ja salasanan. Ensisijaisen alueen istunnon aloittaa tavallisesti käyttöjärjestelmän istunnon kuori (*engl. session shell*), joka suoritetaan käyttäjän työasemassa käyttäjän ympäristön edustajan (*engl. environment representative*) (esim. prosessiattribuutit, ympäristömuuttujat ja kotihakemisto) sisällä. Tästä ensisjaisen alueen istunnon kuoresta käyttäjä voi siirtyä käyttämään muiden alueiden palveluita, kuten alustoja ja sovelluksia.

Toissijaisten alueiden palveluita käyttääkseen käyttäjän täytyy kirjautua kyseiselle toissijaiselle alueelle. Tämä vaatii taas uuden tunnistautumisen ja tunnistetietojen syötön. Toissijaisen alueen istunnon aloittaa tavallisesti käyttöjärjestelmän kuori tai sovelluksen kuori käyttäjän ympäristön edustajan sisällä. Ylläpidon kannalta edellä kuvaillun kaltainen käyttäjien tunnistaminen vaatii jokaisen alueen erillisen hallinnoinnin sekä monta käyttäjätilien hallinnan rajapintaa.

Käytettävyys- ja turvallisuussyiden vuoksi on syytä integroida saman organisaation sisällä eri alueiden käyttäjien kirjautumis- ja käyttäjätilien hallinnan toimintoja.

Tällöin voidaan saavuttaa ainakin seuraavia hyötyjä:

- Käyttäjän eri alueille kirjautumisiin käyttämä aika lyhenee.
- Käyttäjän tietoturva paranee, koska hänen ei enää tarvitse käsitellä useita käyttäjätunnuksia ja salasanoja.
- Järjestelmätuen ja -hallinnan toiminta nopeutuu, kun käyttäjien lisääminen ja käyttäjätietojen muuttaminen yksinkertaistuvat.
- Järjestelmän yleinen turvallisuus paranee käyttäjätilien ja käyttäoikeuksien hallinnan yhtenäistyessä ja yksinkertaistuessa.

Edellä kuvattua integroitua käyttäjien kirjautumismenetelmää kutsutaan nimellä Single Sign-On (*suom. kertakirjautuminen*). SSO-lähetymistavassa järjestelmän on ensisijaisen kirjautumisen yhteydessä saatava käyttäjältä myös kaikki mahdollisesti toissijaisisten alueiden tunnistautumisissa tarvittavat käyttäjätiedot. SSO-palvelut hyödyntävät ensisjaisen alueen käyttäjätietoja käyttäjän tunnistautuessa toissijaisille alueille.

Käyttäjän ensisijaisen kirjautumisen yhteydessä antamia tietoja voidaan hyödyntää toissijaisissa kirjautumisissa monin eri tavoin. Käyttäjän tietoja voidaan ensinnäkin suoraan välittää toissijaiselle alueelle. Käyttäjän tietojen avulla on mahdollista myös epäsuorasti noutaa muita käyttäjän tietoja SSO:n hallintatietokannasta ja käyttää noudettuja tietoja hyödyksi toissijaisissa kirjautumisissa. Tietoja voidaan myös käyttää välittömästi, jos aloitetaan istunto toissijaisen alueen kanssa osana ensimmäistä istuntoa. Tässä tapauksessa asiakkassovelluksia on kutsuttava ja yhteydet niihin muodostettava ensisjaisen kirjautumisen yhteydessä. Lisäksi on mahdollista väliaikaisesti varastoida käyttäjätiedot käytettäväksi myöhemmin toissijaisten alueiden kirjautumisisssa.

Hallinnoinnin kannalta SSO-malli tarjoaa yhtenäisen käyttäjätilien hallinnan rajapinnan, jonka kautta järjestelmän eri alueita hallitaan keskitetysti.

1.2 SSO:n kuvaus

Seuraavissa alaluvuissa kuvataan kertakirjautumisjärjestelmälle asetettavia toiminnaliisia, ei-toiminnallisia ja turvallisuustavoitteita sekä esitellään kertakirjautumisjärjestelmän sovelluksia.

1.2.1 Toiminnallisia tavoitteita

The Open Group [2] määrittää Single Sign-On -rajapintojen toiminnan määrittelevässä XSSO-spesifikaatiossaan seuraavia toiminnallisia tavoitteita käyttäjäkirjautumisen rajapinnalle [3]:

- Rajapinnan tulee toimia tunnistetiedon tyypistä riippumattomasti ja sen pitää tukea kaikkia tarkoituksenmukaisia vuorovaikutteisia kirjautumistapoja. Käyttäjätiedot voidaan lukea ensisijaisen kirjautumisen yhteydessä esimerkiksi älykortilta (*engl. smartcard*) tavanomaisen käyttäjäkirjautumisen syötön sijaan.
- Käyttäjän pitää voida muuttaa tunnistetietoja. Tämä tarkoittaa ainakin mahdollisuutta muuttaa salasanaa, mutta mahdollisesti muitakin käyttäjän tietoja.
- Vierailijan pitää voida muodostaa oletuskäyttäjäprofiili.
- Istunnon päättyessä tai uloskirjautumisen yhteydessä täytyy käynnistää järjestelmän siivoustoimiinnot (*engl. cleanup services*).
- Kaikkien kirjautumistoimintojen ei tarvitse tapahtua samanaikaisesti ensisijaisen kirjautumisen kanssa. Samanaikainen kirjautuminen aloittaa käyttäjän istunnon kaikkien mahdollisten palveluiden kanssa, vaikka käyttäjä ei palveluja käyttäisikään.
- Järjestelmän kirjautumissääntöjä (*engl. system sign-on policy*) pitää voida hallita.
- XSSO:n ohjelmointirajapintojen ei tule estää 16-bittisten merkkien käyttöä. Muut järjestelmän komponentit voivat kuitenkin estää niiden käytön erityistapauksissa.
- Kirjautumistapahtumissa käytettävien valtuutusten (*engl. credentials*) pitää päivittyä automaattisesti.
- Sekä ensisijaisen että toissijaisten kirjautumisten nimeämisjärjestelmiä pitää voida yhdistellä (*engl. mapping*) sekä hallinnollisesti että algoritmisesti.

The Open Group määrittää XSSO-spesifikaatiossaan [3] seuraavia toiminnallisia tavoitteita käyttäjätilien hallinnan rajapinnoille:

- Käyttäjätilejä pitää voida luoda, poistaa ja muokata.
- Yksittäisten käyttäjätilien ominaisuuksia pitää voida muokata.

1.2.2 Ei-toiminnallisia tavoitteita

The Open Group asettaa kertakirjautumisjärjestelmän toiminnalle seuraavia ei-toiminnallisia tavoitteita [3]:

- Järjestelmän pitää olla tunnistautumismenetelmistä riippumaton. Rajapinnann toiminnan ei tule perustua minkään tietyn tunnistaumistekniikan käyttöön, eikä myöskään mitään tarkoituksenmukaista tunnistautumistekniikkaa pidä poissulkea.
- Järjestelmän pitää olla alustoista ja käyttöjärjestelmistä riippumaton. Järjestelmän pitää voida yhdistää keskenään yleisimmin käytetyt tietokoneet, palvelimet sekä keskustietokoneet. Liitettävien laitteiden ei välttämättä tarvitse toimia järjestelmän kanssa suoraan ilman muutoksia.
- Kertakirjautumisjärjestelmään pitää voida liittää yleisesti käytettäviä sovelluksia, ja järjestelmän toimintojen pitää helpottaa liittämistä. Liitettäviin sovelluksiin saatetaan tosin joutua tekemään muutoksia ohjelmakoodin tasolla.
- Kertakirjautumisjärjestelmässä pitää voida kirjautua sekä paikallisilla että etäalustoilla olevien asikas-palvelinjärjestelmien asiakasosaan.

1.2.3 Turvallisuustavoitteita

The Open Group asettaa kertakirjautumisjärjestelmän toiminnalle seuraavia turvallisuustavoitteita [3]:

- Järjestelmän ei tarvitse raportoida järjestelmässä ilmenevän yksittäisen vian sijaintia.
- Järjestelmä ei vaikuta yksittäisten järjestelmän palvelujen saatavuuteen.
- Järjestelmän pitää tukea toiminta-alueellaan olevien sovellusten käyttämiä valtuutusmenetelmiä (*engl. authorization policies*). Henkilö voi saada järjestelmän kautta käyttäjätilistä (*engl. account*) tietoja vain sellaisesta sovelluksesta, jonka tarjoamiin palveluihin henkilöllä itsellään on käyttöoikeus.
- Järjestelmän sisäiset turvallisuuteen liittyvät tapahtumat pitää olla mahdollista tarkastaa.

- Järjestelmän pitää suojata kaikki järjestelmään syötettävät ja järjestelmässä olevat turvallisuuteen liittyvät tiedot siten, että muut palvelut voivat luottaa tietojen eheyteen ja alkuperään, kun tietoja siirretään niille toissijaisten kirjautumisten yhteydessä.

- Toteutuksen pitää suojata turvallisuuteen liittyviä tietoja, kun niitä vaihdetaan toteutuksen omien osien tai omien osien ja muiden palveluiden välillä.

1.3 SSO-ratkaisuja

Internet-sanakirja Wikipedia listaa Single Sign-On -termin määritelmän yhteydessä seuraavia kertakirjautumiseen perustuvia sovelluksia [4]:

- **The JA-SIG Central Authentication Service (CAS)** on avoin SSO-palvelu (alunperin kehitetty Yalen yliopistossa), jonka avulla web-sovellukset voivat suorittaa kaikki tunnistautumistoimintonsa yhdellä tai useammalla keskuspalvelimella.

- **CoSign** on avoimen lähdekoodin projekti, joka suunniteltiin alunperin Michiganin yliopiston Internet-SSO-järjestelmäksi. CoSign tunnistaa web-palvelimen käyttäjät ja tuottaa ympäristömuuttujan käyttäjien nimelle. Kun käyttäjä siirtyy käyttämään jotakin tunnistautumista vaativaa sivuston osaa, ympäristömuuttuja sallii käytön ilman uutta kirjautumista.

- **Enterprise Single Sign-On (E-SSO)** , josta käytetään myös nimeä **Legacy Single Sign-On** , tunnistaa ensimmäisen kirjautumisen jälkeiset toissijaisten sovellusten kirjautumiskehotteet ja täyttää automaattisesti niiden käyttäjätunnus- ja salasanakentät. E-SSO-järjestelmät mahdollistavat järjestelmien, jotka eivät voi ulkoistaa käyttäjien tunnistusta, yhteistoiminnan.

- **Web Single Sign-On (Web-SSO)** , josta käytetään myös nimeä **Web Access Management (Web-AM)** , toimii ainoastaan WWW-selaimilla käytettävissä sovelluksissa. Verkkoresurssien käyttöä tarkkaillaan joko välityspalvelimen avulla tai asentamalla jokaiselle kohdepalvelimelle erityinen lisäkomponentti. Tunnistautumattomat käyttäjät, jotka yrittävät käyttää resursseja, siirretään tunnistaumispalveluun ja palautetaan vain onnistuneen tunnistaumisen jälkeen. Käyttäjän tunnistautumisen tilan seuraamiseen käytetään keksejä (*engl. cookies*), joista Web-SSO erottaa käyttäjän tunnistetiedot ja välittää ne sitten eri resurssille.

- **Kerberos** on suosittu menetelmä, jota käytetään sovellusten autentikoinnin ulkoistamiseen. Käyttäjät kirjautuvat Kerberos-palvelimelle, jossa heille annetaan tunniste, jonka käyttäjien asiakassovellukset esittävät palvelimille yhteyttä muodostaessaan. Kerberos on saatavana Unixille, Windowsille, ja keskustietokonealustoille, mutta vaatii mittavia muutoksia asiakas-palvelin -sovellusten ohjelmakoodeihin.

- **Federation** on uusi lähestymistapa (myös WWW-sovelluksissa), joka käyttää standardeihin pohjautuvia protokollia käyttäjän henkilöllisyyden vakuuttamiseen toiselle käyttäjälle. Näin vältytään ylimääräisiltä tunnistautumisilta. Federatonia tukevat muun muassa SAML- ja WS-Federation -standardit.

- **Light-Weight Identity** ja **OpenID** tarjoavat YADIS-kattojärjestön alla hajautetun kertakirjautumisen, jossa henkilöllisyys sidotaan helposti käsiteltävään WWW-osoitteeseen. Henkilöllisyys voidaan tarkastaa millä tahansa palvelimella, joka käyttää jotakin osallisena olevaa protokollaa.

- **Windows Live ID** (aikaisemmat nimet .NET Passport ja Microsoft Passport Network) on Microsoftin kehittämä yhdistetyn kirjautumisen palvelu, jonka kautta käyttäjät voivat kirjautua useille WWW-sivustoille yhden käyttäjätilin avulla. Palvelu suunniteltiin aluksi kertakirjautumismenetelmäksi verkkokaupankäyntiin.

2 SAML

Tässä luvussa käsitellään SAML (Security Assertion Markup Language) -standardia. Aluksi kerrotaan yleisesti standardista. Sen jälkeen käydään läpi jokaisen standardin muodostavan spesifikaation sisältöä.

2.1 Mikä on SAML?

SAML (Security Assertion Markup Language) on OASIS Security Services Technical Committeen käyttäjätietojen, -oikeuksien ja -ominaisuuksien siirtoa varten kehittämä XML-metakieleen pohjautuva ohjelmistokehys. Nimensä mukaisesti SAMLin avulla voidaan vakuuttaa kohteiden (tavallisesti ihminen) henkilöllisyyksiä, ominaisuuksia tai oikeuksia [5].

SAML V1.0 OASIS -standardi julkaistiin syyskussa 2002 ja SAML V1.1 seurasi syyskuussa 2003. Standardia on siitä lähtien sovellettu yleisesti etenkin rahaliikenteen, yliopistojen, hallitusten ja yritysten erilaisissa järjestelmissä. Kaikki suurimmat WWW-hallintajärjestelmiä kehittävät yritykset ovat implementoineet SAMLin sovelluksissaan. Myös kaikki tunnetuimmat sovelluspalvelintuotteet tukevat SAMLia. SAML on käytössä useimpien Internetin tietoturvaratkaisuja tarjoavien yritysten tuotteissa. SAML-standardin viimeisin versio 2.0 rakentuu vahvasti aikaisempien versioiden pohjalle ja sisältää lisäksi monia uusia merkittäviä toiminnallisuuksia.

SAMLin käytöllä voidaan saavuttaa ainakin seuraavanlaisia hyötyjä:

- **Alustan neutraalius** - SAML erottaa turvarakenteet alustan arkkitehtuurista ja käytettävistä kaupallisista sovelluksista. Yksi palvelukeskeisen arkkitehtuurin tärkeitä tavoitteita on saada turvallisuus riippumattomaksi sovelluslogiikasta.

- **Heikko hakemistojen kytkentä** - SAML ei vaadi käyttäjätietojen ylläpitoa ja synkronointia hakemistojen välillä.

- **Parempi käytettävyys loppukäyttäjille** - SAML mahdollistaa kertakirjautumisen sallimalla käyttäjien tunnistautua ensin henkilöllisyyden tuottajapalvelussa ja sitten käyttää muita palveluita ilman uutta tunnistutumista.

- **Pienemmät palveluntarjoajan hallinnointikulut** - Käyttämällä SAMLin avulla uudelleen yksittäisiä tunnistautumistapahtumia (kuten sisäänkirjautuminen käyttjätunnuksella ja salasanalla) useiden palveluiden välillä, voidaan pienentää käyttäjätilien ylläpitokustannuksia.

- **Riskien siirto** - SAML voi siirtää henkilöllisyyksien hallinnan vastuuta henkilöllisyyksien tarjoajalle (*engl. identity provider*), joka on useammin yhteensopiva SAML:n toimintamallin (*engl. business model*), kuin palveluntarjoajan toimintamallin kanssa.

2.2 SAML V2.0 OASIS -standardi

Seuraavissa alaluvuissa käydään läpi SAML-standardin muodostavien spesifikaatioiden sisältöjä.

2.2.1 Johdanto

SAML-standardi määrittelee XML-pohjaisen ohjelmistokehyksen (*engl. framework*), jonka kautta välitetään turvallisuustietoja verkon kautta toisiinsa yhteydessä olevien tahojen välillä. Turvallisuustiedot ilmaistaan siirrettävillä SAML:n vakuutuksilla (*engl. assertion*), joihin sovellukset voivat luottaa toimiessaan turvallisuussalueen (*engl. security domain*) rajojen yli. OASIS SAML-standardi määrittelee tarkat säännöt vakuutusten pyynnöille, luonnille, välitykselle ja käytölle [6].

The OASIS Security Services Technical Committee (SSTC) on julkaissut lukuisia SAML V2.0:an liittyviä dokumentteja. Erilaisia dokumentteja ovat virallisen OASIS-standardin muodostavat dokumentit, SAML V2.0:n käyttöä tukevat dokumentit sekä useita laajennoksia, jotka mahdollistavat SAML:n käytön erityisissä ympäristöissä tai integroinnin muiden teknologioiden kanssa.

Seuraavissa alaluvuissa esitellään dokumentit, jotka yhdessä muodostavat SAML V2.0 OASIS -standardin.

2.2.2 Conformance Requirements

Conformance Requirements for the OASIS SAML V2.0 -spesifikaatiossa kuvataan ominaisuudet, jotka ovat pakollisia ja valinnaisia SAML V2.0:n kanssa yhdenmukaisille toteutuksille. Spesifikaatiossa esitellään myös dokumentit, joista SAML V2.0 koostuu [7].

Dokumentissa on viisi päälukua. Luvussa 1 kuvataan lyhyesti kaikki dokumen-

tit, jotka kuuluvat SAML V2.0 -standardiin. Lisäksi selvennetään eri dokumenteissa käytettäviä merkintöjä. Luvussa 2 listataan kaikki SAML Profiles -spesifikaatiossa määriteltävät profiilit. Jokaiselle profiilille kuvaillaan viestivuo (*engl. message flow*) protokollien välillä ja jokaista viestivuota kohden listataan asiaankuuluvat sidokset (*engl. bindings*). Luvussa 3 kuvataan SAML V2.0:n tekniset vastaavuusvaatimukset ohjelmistototeuksille. Luvussa 4 käsitellään XML:n digitaalista allekirjoitusta, jota SAML V2.0 käyttää yhtenäisen ja lähteen tunnistavan XML-kirjautumisen ja salauksen toteutuksessa. Lisäksi käsitellään XML:n salausta, jota SAML V2.0 käyttää tietosuojan, salattujen tunnusten (*engl. identifiers*), väittämien (*engl. assertions*) ja attribuuttien toteutuksessa. Luvussa 5 käsitellään SSL 3.0- ja TLS 1.0 -salausprotokollien käyttöä SAML V2.0:n yhteydesä.

2.2.3 Assertions and Protocols

Assertions and Protocols for the OASIS SAML V2.0 -spesifikaatiossa määritellään syntaksi ja semantiikka XML-koodatuille tunnistautumista (*engl. authentication*), ominaisuuksia (*engl. attributes*) ja valtuuttamista (*engl. authorization*) koskeville vakuutuksille, sekä protokollille, jotka kuljettavat näitä tietoja [8].

Dokumentissa on kahdeksan päälukua. Luvussa 1 selvennetään yleisesti dokumentissa käytettäviä merkintätapoja ja kuvaillaan XML:n nimiavaruuksien (*engl. namespaces*) käyttöä sekä SAMLin vakuutusten muodostamista. Lisäksi luvussa kuvaillaan SAMLissa käytettäviä tietotyypejä. Luvussa 2 käsitellään SAMLin vakuutusten muodostamista. Luvussa 3 käsitellään SAML:n protokollia ja kuvaillaan viestien luontia ja niiden välitystä eri protokollia käyttäen. Luvussa 4 käsitellään SAMLissa käytettäviä versiointitapoja (*engl. versioning*) ja kuvataan sääntöjä eri versioiden tunnistamiseen ja käsittelyyn. Lisäksi luvussa esitetään syitä milloin ja miksi versiointitietoja aiotaan muuttaa spesifikaatiossa tulevaisuudessa. Luvussa 5 kuvataan SAMLin ja XML:n allekirjoitusten (*engl. signature*) syntaksia ja käsittelyä. Luvussa 6 kuvataan SAMLin ja XML:n salausten syntaksia ja käsittelyä. Luvussa 7 käsitellään SAMLin laajennettavuutta (*engl. extensibility*) ja esitellään vakuutusten ja protokollien laajennosmahdollisuuksia. Luvussa 8 määritellään URI-pohjaisia tunnisteita yleisille resurssien käsittelytoiminnoille sekä aiheiden ja attribuuttien nimille.

2.2.4 Bindings

Bindings for the OASIS SAML V2.0 -spesifikaatiossa määritellään SAMLin protokollasidokset (*engl. protocol bindings*), joita käytetään SAML:n vakuutuksissa ja tiedosnsiirtoprotokollien request-response -viesteissä [9].

Dokumentissa on kolme päälukua. Luvussa 1 selitetään protokollasidoksen käsitettä sekä selvitetään dokumentissa käytettäviä merkintätapoja. Luvussa 2 annetaan ohjeita sellaisille kolmansille osapuolille, jotka haluavat määrittää uusia protokollasidoksia. Luvussa 3 kuvataan yleispiirteisesti kaikkia SAML-standardissa määriteltäviä protokollasidoksia.

2.2.5 Profiles

Profiles for the OASIS SAML V2.0 -spesifikaatiossa määritellään profiilit SAMLin vakuutusten ja request-response -viestien käytölle tiedonsiirtoprotokollissa ja kehyksissä. Lisäksi määritellään profiilit SAMLin attribuuttiarvojen syntaksille ja nimeämissäännöille [10].

Dokumentissa on kahdeksan päälukua. Luvussa 1 selitetään profiilin käsitettä sekä selvitetään dokumentissa käytettäviä merkintätapoja. Luvussa 2 annetaan ohjeita, kuinka voidaan määritellä uusia profiileja. Luvussa 3 kerrotaan vahvistusmetodien tunnistimista (*engl. confirmation method identifiers*). Luvussa 4 määritellään SAMLin profiilit, jotka tukevat kertakirjautumista WWW-selaimissa ja muissa asiakassovelluksissa. Luvussa 5 kuvataan Artifact Resolution -profiilin toimintaa ja käyttöä. Tätä protokollaa käytetään viittaamaan SAMLin kohteesta (*engl. artifact*) vastaavaan protokollaviestiin (*engl. protocol message*). Luvussa 6 käsitellään Assertion Query/Request -profiilia. Luvussa 7 käsitellään Name Identifier Mapping -profiilia. Luvussa 8 käsitellään SAMLin attribuuttiprofiileja (*engl. attribute profiles*).

2.2.6 Metadata

SAMLin profiilit edellyttävät sopimista yhteistyöstä tunnisteiden, sidosten alku- ja loppupisteiden, sertifikaattien, avainten jne. käytöstä järjestelmän eri kokonaisuuksien välillä. Metadata for the OASIS SAML V2.0 -spesifikaatiossa kuvataan näitä tietoja yhdenmukaistetulla tavalla. Dokumentissa määritellään SAML-järjestelmän osakokonaisuuksille laajennettava metadata-formaatti, joka on järjestetty SAML-profiileja kuvaavien tehtävien mukaan. Lisäksi dokumentissa määritellään profiilit metatiedon dynaamiselle vaihdolle (*dynamic exchange*) eri järjestelmän osien välillä, mikä voi olla hyödyllistä joissakin järjestelyissä [11].

Dokumentissa on neljä päälukua. Luvussa 1 esitellään dokumentin sisältöä ja selvitetään dokumentissa käytettäviä merkintätapoja. Luvussa 2 selvitetään SAMLin metadatan toimintaa ja annetaan esimerkkejä metadatan käytöstä. Luvussa 3 kerrotaan metadatan elementtien digitaalisesta allekirjoituksesta. Luvussa 4 käsitellään metadatan julkaisua ja metadata-dokumenttien paikannustarkkuutta (*engl. resolution*). Luvussa esitetään keinoja metadatan tarkkuuden ja pätevyyden (*engl. legitimacy*) varmistamiseksi.

2.2.7 Authentication Context

Authentication Context for the OASIS SAML V2.0 -spesifikaatiossa määritellään syntaksi tunnistautumiskontekstiin (*engl. Authentication Context*) liittyville määritelmille sekä luetellaan SAMLissa käytettäviä tunnistautumiseen liittyviä luokkia [12].

Dokumentissa on kolme päälukua. Luvussa 1 selitetään tunnistautumiskontekstin käsitteitä sekä selvitetään dokumentissa käytettäviä merkintätapoja. Luvussa 2 kuvataan tunnistautumiskontekstin määrittelyä ja listataan täydelliset tunnistautumiskontekstityyppien XML-koodit sekä itse tunnistautumiskontekstin XML-koodi. Luvussa 3 kuvataan tunnistautumiskontekstien luokittelun periaatteita sekä esitetään tunnistatumiskontekstien luokkien koodilistaukset.

2.2.8 Glossary

Glossary for the OASIS SAML V2.0 -spesifikaatiossa määritellään termit, joita käytetään OASIS SAML -spesifikaatiossa ja siihen liittyvissä dokumenteissa [13].

Termit esitetään dokumentin vasemmanpuoleisessa sarakkeessa allekkain listattuna. Oikeanpuoleisessa sarakkeessa esitetään termejä vastaavat määritelmät sekä mahdollisesti viitteitä dokumentteihin, joissa termejä käytetään.

3 Shibboleth

Tässä luvussa esitellään SAML-standardin toteuttavaa Shibboleth-projektia. Aluksi kuvataan projektia yleisesti. Sitten selitetään Shibbolethin toimintaa. Lopuksi esitellään joitakin Shibbolethin sovelluksia.

3.1 Projektin esittely

Shibboleth on standardeihin perustuva avoimen lähdekoodin projekti, jota kehittää Internet2, pääosin Yhdysvaltalainen voittoa tuottamaton verkkoyhtymä. Shibbolethin avulla voidaan toteuttaa kertakirjautuminen (*engl. Single Sign-On*) organisaation sisäisesti tai sen rajojen yli. Shibboleth mahdollistaa käyttäjän tietoihin perustuvan tunnistautumisen ja suojattujen resurssien käytön käyttäjän yksityisyyttä suojaten [14].

Shibboleth-ohjelmisto toteuttaa OASIS SAML V1.1 -spesifikaation ja mahdollistaa yhdistetyn kertakirjautumisen ja atribuuttien vaihdon. Shibbolethin avulla Internet-selaimen käyttäjä ja hänen kotisivustonsa voivat ohjata selaimen attribuuttien tietojen julkaisemista eri palveluntarjoajille. Shibbolethia tukevan yhteyden käyttäminen helpottaa sekä palveluntarjoajien (*Service Provider*) että identiteetintarjoajien (*Identity Provider*) henkilöllisyyksien ja käyttöoikeuksien hallintaa. Shibbolethia kehitetään yhteistyöprojektina, se on vapaasti saatavilla, ja se julkaistaan Apache-ohjelmistolisenssin alaisuudessa.

3.2 Kirjautumisprosessi

Shibboleth-järjestelmä koostuu kahdesta ohjelmistokomponentista: identiteetintarjoaja (*Identity Provider, IdP*) ja palveluntarjoaja (*Service Provider, SP*). Komponentit ovat erillisiä, mutta toimivat yhdessä mahdollistaen turvallisen verkkoresurssien käytön [15].

Seuraavassa kuvataan vaiheittain Shibbolethin kirjautumistapahtuman kulkua. Yksityiskohdat voivat vaihdella hieman toteutustavasta riippuen, mutta esitetyt vaiheet ovat hyvin tyypillisiä. Kirjautumisessa eri osapuolia ovat käyttäjä, joka haluaa käyttää suojattua verkkoresurssia sekä resurssin tarjoava palvelin ja käyttäjän kotiorganisaatio, jotka molemmat ovat asentaneet Shibboleth IdP -ohjelmiston.

1. Käyttäjä ottaa yhteyden selaimella verkkoresurssiin. Resurssin palvelin on suojattu, ja tästä johtuen se vaatii tietoa käyttäjästä, jotta voi tehdä päätöksen yhteyden sallimisesta.

2. Shibboleth SP-ohjlmisto ohjaa käyttäjän navigointisivulle (*engl. WAYF, "where are you from*), jolla käyttäjälle esitetään lista organisaatioista, joiden käyttäjät voivat käyttää resurssia.

3. Käyttäjä valitsee oman organisaationsa, jolloin hänen selain ohjataan kotiorganisaation sivulle, joka käyttää Shibboleth IdP-ohjelmistoa. Tämä sivu käyttää kotiorganisaation valitsemaa verkon kirjautumismenetelmää. Käyttäjä näkee nyt tutun kotiorganisaationsa kirjautumissivun, syöttää käyttäjätunnuksen, salasanan ja painaa kirjautumispainiketta.

4. Shibboleth IdP-ohjelmisto ohjaa selaimen takaisin alkuperäiseen resurssiin ja liittää viestiin vakuutuksen (*engl. assertion*), joka ilmaisee, että käyttäjä on kirjautuneena. Shibboleth SP -ohjelmisto vahvistaa vakuutuksen resurssin palvelimella ja pyytää sitten lisätietoja (attribuutteja, kuten "tiedekunta"tai "tietotekniikan opiskelija") käyttäjästä hänen kotiorganisaation Shibboleth IdP -palvelusta.

5. Palveluntarjoaja vastaanottaa käyttäjän attribuutit kotiorganisaation identiteetintarjoajalta ja välittää resurssintarjoajan verkkosovellukselle. Sovellus päättää attribuuttien ja omien sääntöjensä perusteella salliiko käyttäjän yhteyden. Jos yhteys sallitaan, käyttäjän pyytämä sivu näytetään.

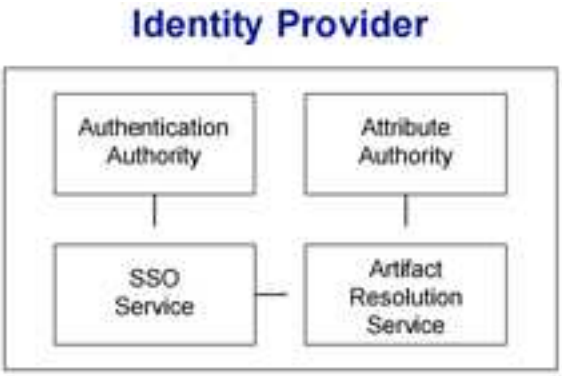
Usein monet edellä mainituista vaiheista voidaan sivuuttaa. Navigointisivu (WAYF) voi asettaa keksin (*engl. cookie*) käyttäjän selaimeen, jolloin käyttäjä ei näe kyseistä sivua seuraavalla kerralla. Jos kotiorganisaation tunnistautumispalvelu käyttää kertakirjautumista, ja käyttäjällä on jo istunto (*engl. session*) sen kanssa, kirjautumissivua ei näytetä. Usein käyttäjä pääseekin käyttämään resurssia niin, että yhtään välisivua ei näytetä.

3.3 Komponentit

Tässä alaluvussa esitellään Shibbolethin ohjelmistokomponentit.

3.3.1 Identity Provider

Identity Provider (*suom. identiteetintarjoaja*) ylläpitää käyttäjän valtuutuksia (*engl. credentials*) ja attribuutteja. Pyydettäessä identiteetintarjoaja (IdP) vakuuttaa autentikointeja tai attribuutteja luotettaville osapuolille, erityisesti palveluntarjoajille (SP). IdP:n alikomponentit esitetään kuvassa 3.1.



Kuva 3.1: Shibboleth Identity Provider.

Authentication Authority jakaa autentikointilausuntoja (*engl. Authentication Statements*) muille komponenteille. Authentication Authority on integroitu IdP:n autentikointipalveluun.

Single Sign-On Service on ensimmäinen IdP:n kontaktipiste. SSO-palvelu käynnistää autentikointiprosessin IdP:ssä ja pohjimmiltaan ohjaa käyttäjän välisivun siirtopalveluun (ellei SSO-palvelun ja välisivun siirtopalvelun toimintoja ole yhdistetty, mikä on suositeltavaa).

Inter-Site Transfer Service myöntää HTTP-vastauksia Browser/POST- ja Browser/Artifact -profiileita noudattaen. Välisivun siirtopalvelu on yhteydessä Aut-

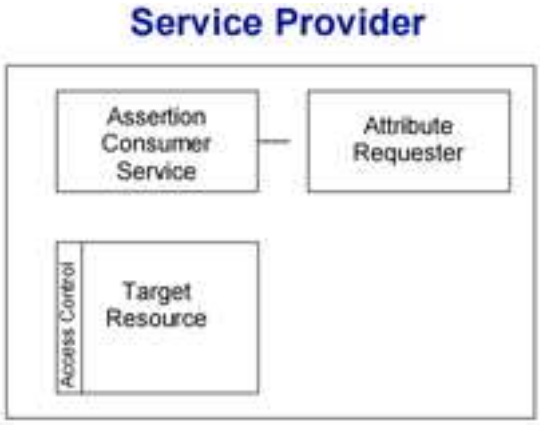
hentication Authorityyn tuottaakseen vaaditun autentikointivakuutuksen.

Jos Browser/Artifact -profiili on käytössä, IdP lähettää SP:lle artifaktin (*engl. artefact*) varsinaisen vakuutuksen sijaan (artifakti on viittaus autentikointivakuutukseen). SP lähettää sitten artifaktin sen ratkaisupalvelulle (***Artifact Resolution Service***). Vastauksena IdP lähettää vaaditun autentikointivakuutuksen SP:lle.

Attribute Authority käsittelee attribuuttipyynöt, eli siis myöntää attribuuttivakuutuksia. Attribuute Authority vahvistaa ja valtuuttaa kaikki saamansa pyynnöt.

3.3.2 Service Provider

Service Provider (*suom. palveluntarjoaja*) hallitsee suojattuja resursseja. Käyttäjän pääsy resursseihin perustuu vakuutuksiin, jotka palveluntarjoaja (SP) vastaanottaa identiteetintarjoajalta (IdP). SP:n alikomponentit esitetään kuvassa 3.2.



Kuva 3.2: Shibboleth Service Provider.

Assertion Consumer Service (*suom. vakuutusten kuluttajapalvelu*) on palveluntarjoajan päätepiste SSO:ssa. Se käsittelee autentikointivakuutukset, jotka SSO-palvelu palauttaa (tai Artifact Resolution Service, riippuen käytetystä profiilista), käynnistää valinnaisen attribuuttipyynnön, perustaa turvakontekstin SP:ssä, ja ohjaa asiakkaan haluamalleen kohderesurssille.

Attribute Requester (*suom. attribuutin pyytäjä*) SP:ssä ja Attribute Authority IdP:ssä voivat käynnistää paluukanavan attribuuttien vaihdon (*engl. back-channel attribute exchange*), kun turvakonteksti on perustettu SP:ssä. Tämä tarkoittaa, että SP ja IdP kommunikoivat keskenään suoraan, selaimen ohittaen.

3.3.3 WAYF Service

SP:stä ja IdP:stä erillään toimii vaihtoehtoinen WAYF-palvelu. SP voi käyttää WAYF:ää määrittääkseen käyttäjän ensisijaisen IdP:n, joko käyttäjän kanssa yhteistyössä tai itsenäisesti. WAYF on pohjimmiltaan autentikointipyynnön vakuutus, joka lähetetään SP:stä IdP:n SSO-palvelulle.

3.4 Käyttökohteita

Shibbolethin avulla saavutetaan pääasiassa kahdenlaisia hyötyjä. Ensinnäkin, Shibboleth-toteutuksissa vältytään monilta eri salasanoilta ja kirjautumisilta, mikä helpottaa käyttöä ja parantaa myös turvallisuutta. Toiseksi, vältytään tarpeettomalta käyttäjän henkilökohtaisten tietojen julkaisulta, jolloin käyttäjän yksityisyys säilytetään [14].

Seuraavana esitetään esimerkkinä joitakin tyypillisiä opiskelijan tietoverkon kautta käyttämiä toimintoja ja vertaillaan nykyisiä toteutustapoja mahdollisiin Shibboleth-toteutuksiin.

Toiminto 1: Opiskelija käyttää kampuksen ulkopuolella olevaa digitaalista kirjastoa.

Nykyinen toteutus:

- välityspalvelimia, jaetut salasanat tai ei palvelua

Ongelmat nykytoteutuksessa:

- välityspalvelimien ylläpito hankalaa
- ei yhteyttä kotoa
- IP-osoitteeseen pohjautuvat rajoitukset epäluotettavia
- yksityisyys voi vaarantua, jos henkilöllisyys välitetään epäasiallisesti kirjastolle

Shibboleth-toteutus:

- sallii pääsyn suoraan aineistoon ilman kampuksen välityspalvelinta

Toiminto 2: Opiskelija käyttää ulkopuolista kurssimateriaalia tai arvostelupalvelua.

Nykyinen toteutus:

- käyttäjätunnuksen ja salasanan syöttö

Ongelmat nykytoteutuksessa:

- uusi käyttäjätili
- käyttäjä valitsee usein jo aikaisemmin käyttämänsä salasanan
- ulkopuolisilla toimipaikoilla on rajoitetut varmennusmahdollisuudet

Shibboleth-toteutus:

- käyttää paikallisen kampuksen tunnistusta ja sallii kampuksen lähettää sopivan tunnistimen palvelulle
- vaatii etäresursseja, jotta voi luottaa kampuksen tunnistautumiseen

Toiminto 3: Opiskelija käyttää toisen yliopiston tutkimussivustoa tai ylläpitää jaettua mittausinstrumenttia.

Nykyinen toteutus:

- ryhmän käyttäjätilit tai uudet henkilökohtaiset käyttäjätilit

Ongelmat nykytoteutuksessa:

- uudet käyttäjätilit käyttäjille
- jaetut salasanat muodostavat tietoturvariskin

Shibboleth-toteutus:

- mahdollistaa paikallisten kampuksen käyttäjätilien käytön
- mahdollistaa käyttäjän rooliin perustuvat käyttöoikeudet
- vaatii aktiivisen käyttäjien yksityisyyden hallinnan

Toiminto 4: Opiskelija käyttää toisen yliopiston yhteisopetussivustoa.

Nykyinen toteutus:

- ryhmän käyttäjätilit tai uudet etäkäyttäjien henkilökohtaiset käyttäjätilit

Ongelmat nykytoteutuksessa:

- useita käyttäjätilejä
- henkilökohtaiset käyttäjätilit voivat olla turvallisuusriski
- suuret käyttäjätilien hallinnointikulut

Shibboleth-toteutus:

- mahdollistaa paikallisen kampuksen käyttäjätilien käytön
- säilyttää yksityisyyden
- sisällön omistajat voivat hallita kohdetta
- käyttäjiä voidaan vaatia julkistamaan attribuutteja

3.5 Käyttäjiä ja palveluita

Monet organisaatiot käyttävät nykyään Shibboleth-järjestelmää ratkaisuna organisaatioidenvälisiin verkko-ongelmiin. Monet muut sovellukset ovat pilottivaiheessa. Seuraavissa kappaleissa kerrotaan joitakin esimerkkejä Shibbolethin käytöstä [15].

Pennsylvania State Universityn järjestely tarjota opiskelijoille pääsy Napster-musiikkipalveluun sai aikanaan suurta huomiota julkisuudessa. Shibboleth-järjestelmä oli ratkaisevassa asemassa palvelun toteutuksessa, koska sen avulla voitiin toteuttaa sekä yliopiston että Napsterin turvallisuus- ja yksityisyysvaatimukset täyttävä järjestelmä.

Akateemiset tutkimusprojektit, erityisesti luonnontieteissä, käyttävät lisääntyvässä määrin kehittyneitä tietokonepohjaisia menetelmiä. Lisäksi projekteissa työskentelee ihmisiä eri laitoksista. Tällaiset virtuaaliset organisaatiot (VO), jotka on perustettu tutkimuksen tueksi, kärsivät samoista henkilöllisyyksien hallinnan ongelmista kuin yliopistojen kampukset. Tällaisia ongelmia ovat salasanojen jakelu ja vaihto, tietoturvan takaaminen ja oikeuksien hallinta. Lisäksi kyseisten organisaatioiden käyttäjät ovat fyysisesti laajalle alueelle jakautuneena ja heillä on yleensä järjestelmähallintaan käytössä vain vähän henkilöstöä. Käyttämällä Shibbolethia verkkoresurssien käytön hallintaan VO:t voivat sovittaa yhteen eri kampuksista tulevat, Shibboleth-yhteensopivia tunnistuspalveluja käyttävät jäsenet.

JSTOR on voittoa tuottamaton järjestö, joka ylläpitää luotettavaa arkistoa akateemisista julkaisuista ja tarjoaa pääsyn arkistoon mahdollisimman laajalle käyttäjäkunnalle. JSTOR tarjoaa valvotun pääsyn arkistoon tutkijoille, kirjastoille, tiedekunnille, ja valittujen laitosten henkilökunnalle. Kuten monet samankaltaiset palvelut, JSTOR toteuttaa käyttäjien hallinnan pääosin verkko-osoitteiden avulla. Jäsenlaitos ilmoittaa JSTORille verkko-osoiteavaruutensa, jolloin JSTORin palvelimet sallivat pääsyn palveluihinsa näistä verkko-osoitteista. Tällaisiin käyttäjien hallintamenetelmiin liittyy useita tunnettuja ongelmia, mutta järjestelmän toteutushetkellä valittu toteutustapa oli ainoa käytännöllinen vaihtoehto.

JSTOR oli varhain Shibboleth-projektiin osallistunut järjestö, joka piti Shibbolethia parhaana vaihtoehtona siirryttäsessä pois IP-osoitepohjaisesta käyttäjien hallinnasta. Paremman turvallisuuden lisäksi Shibboleth antaa JSTORille mahdollisuuden tarjota käyttäjille henkilökohtaista palvelua ilman, että tarvitsisi käyttää erillisiä käyttäjätilejä ja salasanoja.

Yliopistojen tietotekniikkaosastot tutkivat tapoja saada käyttöön uusia hallinnollisia sovelluksia edullisesti ja joustavasti. Tällöin yleensä todetaan isännöityjen palveluiden (*engl. hosted services*) olevan yleisesti käytettyjä ja houkuttelevia. Kirjautumisen hallinnan toiminta on tärkeä tekijä isännöidyn toimintatavan onnistumisessa. Uusien käyttäjänimen ja salasanojen käyttö ei ole houkuttelevaa, eikä myöskään yliopiston omien tunnusten käyttö etäpalveluissa. Toimittajat ymmärtävät yliopistojen kiinnostuksen kertakirjautumiseen, mutta tavallisesti tuottavat omat kirjautumisjärjestelmänsä, joiden turvallisuus on heikko ja tuki muille järjestelmille huono.

Shibboleth tarjoaa ratkaisun myös tällaisiin sovelluksiin. Eri kampukset vaativat toimittajien järjestelmiltä tukea omille kirjautumisjärjestelmilleen, mikä nostaa palveluiden kustannuksia ja lisää monimutkaisuutta. Jotkut toimittajat päätyvät käyttämään kaupallisia verkkokirjautumistuotteita, mutta yliopistot ovat monesti haluttomia lisensoimaan kaupallisia tuotteita tähän tarkoitukseen. Shibboleth tarjoaa yleisen, hyvin tuetun menetelmän, jonka käyttö yleistyy jatkuvasti. Lisäksi, Shibbolethin attribuuttien käyttö antaa yliopistoille mahdollisuuden ilmaista eri rooleja (kuten "ostava asiakas"tai "etuihin oikeutettu eläkeläinen") toimittajille kirjautumisen yhteydessä. Näin voidaan välttää aikaavieviä eräajoja kyseisten tietojen ylläpitämiseksi.

4 Yhteenveto

Kertakirjautuminen on autentikointimenetelmä, joka tarjoaa käyttäjälle mahdollisuuden yhdellä kirjautumisella käyttää kaikkia palveluita, joihin hänellä on käyttöoikeudet. Kertakirjautumisen käyttö on suotavaa, koska se parantaa tietoturvaa ja vähentää ihmisen tekemiä virheitä, jotka ovat syynä moniin järjestelmäongelmiin. Kertakirjautumisjärjestelmän toteuttaminen käytännössä on kuitenkin vaativaa.

Kertakirjautumisen suurimpana ongelmana voidaan pitää keskitettyä käyttätietojen hallintaa, jota juuri pidetään myös menetelmän vahvuutena. Jos murtautuja saa haltuunsa käyttäjän tunnukset, hänellä on nopasti pääsy kaikkiin käyttäjän toimintoihin. Käytännössä kaikki kertakirjautumisjärjestelmät tukevat useita turvalisuutta parantavia ratkaisuja, kuten tehokasta salausta ja älykorttien käyttöä käyttäjien tunnistuksessa. Lisäksi tulevaisuudessa uusien menetelmien, kuten biotunnisteiden käyttö, parantaa yhä turvallisuutta.

SAML on protokolla, jonka avulla voidaan turvallisesti vaihtaa autentikointi- ja valtuutustietoja identiteetintarjoajan (*engl. Identity Provider*) ja palveluntarjoajan (*engl. Service Provider*) välillä. SAMLin turvallisuustietojen vaihto perustuu erityisten vakuutusten (*engl. assertions*) siirtoon osapuolten välillä. SAMLin pääasiallisena tarkoituksena on tarjota ratkaisu luotettavan kertakirjautumisjärjestelmän toteuttamiseen verkoissa.

SAMLista on nopeasti tullut standardi, jota useimmat verkkopalveluita tarjoavat yritykset noudattavat kertakirjautumisratkaisuissaan. SAML on vielä varsin nuori standardi, sillä ensimmäinen versio julkaistiin syksyllä 2003. Lisäksi SAML perustuu XML-metakieleen, jonka historia on myös varsin lyhyt. Voidaankin ajatella, että SAMLin käyttöön saattaa liittyä vielä joitakin ongelmia. Kuitenkin, yhä laajenevasta käytöstä päätellen SAMLia pidetään jo ilmeisen luotettavana.

Shibboleth on Internet2-yhteisön avoimen lähdekoodin ohjelmistoprojekti, joka toteuttaa SAML-standardin. Shibboleth muodostaa yhdistetyn kertakirjautumis- ja attribuuttienvaihtokehyksen, jonka avulla voidaan turvallisesti vaihtaa tietoja käyttäjistä samaan Shibboleth-yhteisöön kuuluvien organisaatioiden välillä. Sibbolethia käyttävien toteutusten määrä lisääntyy kaiken aikaa. Shibboleth mahdollistaa uudenlaisten sovellusten ja palveluiden toteuttamisen.

Lähteet

[1] The Open Group, *Introduction to Single Sign-On*, saatavilla WWW-muodossa <URL: http://www.opengroup.org/security/sso/sso_intro.htm>

[2] The Open Group, *Enterprise Architecture Standards, Certification and Services*, saatavilla WWW-muodossa <URL: http://www.opengroup.org>

[3] The Open Group, *Scope of the Single Sign-On Standard*, saatavilla WWW-muodossa <URL: http://www.opengroup.org/security/sso/sso_scope.htm>

[4] Wikipedia, the free encyclopedia, *Single Sign-On*, saatavilla WWW-muodossa <URL:http://wikipedia.org/>

[5] OASIS, *SAML V2.0 Executive Overview*, saatavilla WWW-muodossa <URL: http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>

[6] SAML V2.0 Technical Overview, *Working Draft 9, July 2006*, saatavilla WWW-muodossa <URL: http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2 0-draft-10.pdf>

[7] Conformance Requirements, *OASIS SAML V2.0*, saatavilla WWW-muodossa <URL:http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>

[8] Assertions and Protocols, *OASIS SAML V2.0*, saatavilla WWW-muodossa <URL:http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

[9] Bindings, *OASIS SAML V2.0*, saatavilla WWW-muodossa <URL:http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf>

[10] Profiles, *OASIS SAML V2.0*, saatavilla WWW-muodossa <URL:http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>

[11] Metadata, *OASIS SAML V2.0*, saatavilla WWW-muodossa <URL:http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>

[12] Authentication Context, *OASIS SAML V2.0*, saatavilla WWW-muodossa <URL:http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>

[13] Glossary, *OASIS SAML V2.0*, saatavilla WWW-muodossa <URL:http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf>

[14] Shibboleth Project, *Internet2 Middleware*, saatavilla WWW-muodossa <URL:http://shibboleth.internet2.edu/>

[15] Federated Security: The Shibboleth Approach, *Volume 27, Number 4, 2004*, saatavilla WWW-muodossa <URL:http://www.educause.edu/apps/eq/eqm04/eqm0442.asp?bhcp=1>