CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

SAML - Security Assertion Markup Language

CCERT-PUBDOC-2009-10-279

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Gotovo svi korisnici Interneta su se susretali s različitim web stranicama koje od korisnika zahtijevaju autentikaciju (korisničko ime i lozinku). Međutim, ljudi uglavnom koriste drugačije podatke za pristup pojedinim web servisima i programima, što u konačnici rezultira velikim brojem različitih identiteta. Budući da neke od njih korisnici s vremenom zaborave, moraju ponovno popunjavati pristupne prijave te na taj način gomilaju brojne korisničke račune. Način da se to riješi je uvođenje sustava jedinstvene autentikacije na webu, a SAML standard ima za cilj uspostavu takvog sustava.

SAML je XML standard za razmjenu autentikacijskih i autorizacijskih informacija putem Interneta. Smisao spomenutog standarda leži u međusobnoj komunikaciji različitih sigurnosnih sustava, a ne na uvođenju novog pristupa autorizaciji i autentikaciji.

Kroz ovaj dokument opisan je nastanak spomenutog standarda te koji su faktori utjecali na njegovo korištenje. Također, dan je pregled osnovnih elemenata SAML jezika te načini njihovog povezivanja i korištenja. Navode se informacije o programima, ali i standardima, koji koriste SAML. I naposljetku, dio teksta se odnosi na mehanizme koje primjenjuje ovaj standard u svrhu zaštite i sigurnosti podataka koji se prenose mrežom.

2. SAML standard

SAML (eng. *Security Assertion Markup Language*) je XML standard za sigurnu razmjenu identifikacijskih informacija između poslovnih partnera (organizacija, tvrtki, vlasnika pojedinačnih aplikacija) putem Interneta. SAML ne definira nove mehanizme niti pristupe za autentikaciju i autorizaciju, već samo određuje strukturu dokumenta kojim se informacije prenose između neovisnih servisa i programa. Drugim riječima, SAML omogućava stvaranje i razmjenu autentikacijskih i/ili autorizacijskih podataka, ali ne odlučuje na koji način se one provode na sustavima.

2.1. Razlozi nastanka SAML standarda

Postoje četiri osnovna razloga za razvoj SAML standarda:

1. Uvođenje standarda za razmjenu podataka na Internetu

   Prije usvajanja SAML standarda, uobičajeni način ostvarivanja jedinstvene sjednice na webu bila je uporaba kolačića (engl. cookie) koji se zadržavaju u Internet preglednicima. Međutim, oni se ne mogu prenositi između različitih domena, odnosno kolačić koji se koristi za autentikaciju na stranicu *www.abc.com* nije moguće iskoristiti za stranicu *www.xyz.com*. Pojavom SAML standarda, istu informaciju koju se spremalo u kolačićima, moguće je na standardizirani način spremiti u XML strukturu SAML izjava (više riječi o tome bit će rečeno u narednom poglavlju).
2. Interoperabilnost različitih sustava

   Kroz SAML je omogućena razmjena podataka i dijeljenje informacija između različitih sigurnosnih domena, neovisno o operacijskom sustavu i/ili proizvođaču. Sigurnosna domena uključuje skup računala i poslužitelja koji korisnicima omogućuju dostupnim informacije i aplikacije određene tvrtke, organizacije i sl. Pomoću sigurnosne domene mogu se definirati tehnologije, standardi i sigurnosne politike koji su potrebni kako bi se tvrtka (i njezini resursi) zaštitila od neovlaštenog pristupa. Na Internetu izraz domena (engl. domain) označava aplikacije i podatke označene nekim zajedničkim imenom (npr. poslovniforum.hr).
3. Sniženi administrativni troškovi za otvaranje i održavanje korisničkih računa
4. Pojednostavljena usluga za krajnje korisnike

   Korištenjem jedinstvenog mehanizma za autentikaciju osigurava se brži pristup uslugama i smanjuje broj podataka (npr. korisničko ime i pristupna lozinka) koje korisnik mora pamtiti za pristup različitim stranicama.

2.2. Povijesni razvoj

Spomenuti je standard razvila organizacija OASIS (eng. *Organization for Advancement of Structured Information Standards*). Radi se o globalnom konzorciju koji potiče razvoj i globalnu primjenu normi za elektroničko poslovanje.

OASIS skupina broji preko 5000 članova koji predstavljaju gotovo 600 organizacija u više od 100 zemalja diljem svijeta. Neki od najpoznatijih članova su IBM, Microsoft, Nokia, AOL, Sun, Novell, Hewlett-Packard i dr. Više informacija o ovoj organizaciji moguće je pronaći na službenoj stranici:

www.oasis-open.org

Ova je organizacija nastala 1993. godine pod imenom *SGML Open* s ciljem promoviranja SGML jezika kao standarda za specificiranje, definiranje i upotrebu oznaka u dokumentima.

SGML (eng. *Standard Generalized Markup Language*) je 1996. objavljen kao ISO norma (ISO-8879). SGML je uveo standardizaciju u načinu formatiranja i održavanja dokumenata kako bi isti bili razumljivi različitim poslovnim sustavima, neovisno o operacijskom sustavu, programu ili organizaciji. Međutim, spomenuti je standard bio pretjerano opširan, izuzetno složen i skup za upotrebu pa se kao takav mogao koristiti samo u velikim tvrtkama i institucijama. 1996. se pojavila ideja o stvaranju novog jezika, koji bi imao jednake mogućnosti kao i SGML, ali bi omogućio prijenos podataka preko Interneta (što nije bilo moguće korištenjem SGML-a).

Iz tog je razloga *SGML Open* 1998. promijenio naziv u *OASIS Open*, uključujući u svoje projekte razvoj različitih standarda koji se temelje na XML-u. Kao i SGML, XML (eng. *EXtensible Markup Language*) predstavlja jezik za označavanje podataka, s razlikom da se može izvoditi u web pregledniku. Danas je XML jezik vrlo raširen i koristi se za različite namjene: odvajanje podataka

od prezentacije, razmjenu i pohranu podataka, povećanje njihove dostupnosti te razvitak novih jezika za označavanje. U siječnju 2001. OASIS započinje s radom na razvoju standarda (SAML) koji bi omogućio razmjenu autentikacijskih i autorizacijskih podataka preko Interneta.

Prva inačica (SAML 1.0) je proglašena OASIS standardom u studenom 2002. godine. Ono što se njom željelo postići bila je mogućnost razmjene autentikacijskih i autorizacijskih informacija u različitim transakcijama. Osim toga, namjera je bila uvesti mehanizam za jedinstvenu autentikaciju koji korisnicima omogućuje da se prilikom pristupanja web aplikacijama autentificiraju jednom i nakon toga se neko vrijeme (dok traje sjednica) više ne moraju ponovo prijavljivati za pristup svakoj pojedinačnoj aplikaciji.

Nova inačica - SAML 1.1 je ratificirana u listopadu 2003., a naglasak je stavljen na unaprjeđenje interoperabilnosti između različitih sustava te korištenje XML potpisa zbog zaštite podataka. U to se vrijeme ovaj standard počeo primjenjivati u obrazovnim institucijama te financijskom, državnom i industrijskom sektoru.

Posljednja inačica (2.0) je službeno odobrena u ožujku 2005. Nastala je konvergencijom specifikacija SAML 1.1 i ID-FF (eng. *the Liberty Identity Federation Framework*). ID-FF je razvila organizacija Liberty Alliance za omogućavanje federativnog identiteta između različitih organizacija/tvrtki putem web servisa. Federativni pristup označava mogućnost povezivanja podataka o korisniku s raznim pružateljima pojedinih usluga (više o ovoj temi može se pročitati u poglavlju 4).

Ova je inačica nekompatibilna sa svojim prethodnicima, ali donosi niz novih značajki:

- korištenje pseudonima (nasumičnih identifikatora koji identificiraju korisnika),
- meta podatke – za pojednostavljivanje SAML imlementacije,
- enkripcija - omogućuje enkripciju cijele SAML izjave,
- podrška za mobilne uređaje,
- automatska odjava sa svih stranica na koje je korisnik prijavljen i dr.

2.3. Primjena ostalih standarda i protokola

SAML se temelji na korištenju nekih specijaliziranih jezika za označavanje i protokola komunikacije:

Standardi i protokoli	Pojašnjenje
XML (eng. *EXtensible Markup Language*)	Razmjena SAML podataka izražava se standardiziranim XML dijalektom, što je i logično budući da je nastao iz navedenog jezika
XML shema	SAML izjave i protokoli se definiraju korištenjem XML shema. Riječ je o jeziku koji opisuje strukturu XML dokumenata (tj. određuje skup pravila koja prikazuju što se može, a što ne može nalaziti u određenim dijelovima XML podatkovne datoteke).
XML potpis	SAML 1.1 i 2.0 koriste XML digitalne potpise. XML potpis je preporuka W3C (eng. *World Wide Web Consortium*) organizacije koja se bavi standardizacijom tehnologija korištenih na webu. Koristi se za uspostavu identiteta sudionika u elektroničkom poslovanju i osigurava integritet podataka.
XML enkripcija	Korištenjem ovog standarda u SAML 2.0 jeziku je moguće kodirati razne strukture koje prenose informaciju (SAML 1.1 nema tu mogućnost)
HTTP protokol (eng. *HyperText Transfer Protocol*)	SAML definira korištenje HTTP protokola budući da se radi o najčešće korištenoj metodi za prijenos podataka na Internetu.
SOAP (eng. *Simple Object Access Protocol*)	Riječ je o protokolu koji omogućuje komunikaciju između aplikacija preko HTTP protokola. SAML ga koristi radi povećanja sigurnosti i privatnosti podataka.

Tablica 1. Standardi i protokoli koje koristi SAML

3. Komponente SAML jezika

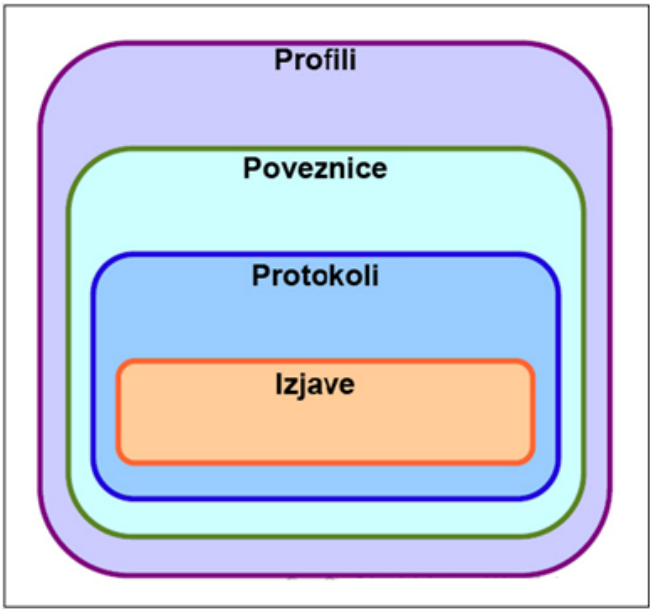
3.1. Strane u komunikaciji

Primjena SAML standarda se temelji na razmjeni izjava slanjem odgovarajućih poruka. Strane koje pritom sudjeluju u toj komunikaciji su:

1. **Korisnik** – osoba koja želi pristupiti određenom resursu (stranici, programu, servisu)
2. **Pružatelji usluge**: njihova se konfiguracija odvija putem programa koji implementira SAML
   a) **Davatelj elektroničkog identiteta** (eng. ***Id****entity* ***P****rovider*, **IdP**) – poslužitelj koji stvara, održava i upravlja korisničkim identitetima kod određene tvrtke/organizacije. Podatke o korisnicima prosljeđuje vlasniku resursa
   b) **Vlasnik resursa** (eng. ***S****ervice* ***P****rovider*, **SP**) – nadzire pristup resursima koje zahtijeva korisnik. Odluku o pravu pristupa za korisnike donosi na temelju izjava koje šalje IdP.

3.2. Struktura podataka SAML jezika

Osnovni elementi SAML jezika se izražavaju izjavama, protokolima, poveznicama i profilima. Termin „jezgra“ (eng. *core*) SAML-a se odnosi na općenitu sintaksu i semantiku SAML izjava i protokola. Protokoli su vezani uz ono što se prenosi (izjave) između različitih domena, a ne kako se prenosi (to određuju poveznice). Profili definiraju točno određeni slučaj korištenja navedenih komponenti.



Slika 1. Osnovne komponente SAML jezika

Izvor: OASIS

3.2.1. Izjava ili tvrdnja

Osnova SAML-a je izjava (eng. *assertion*) koja se prenosi između pružatelja usluga (IdP-a i SP-a), a sadrži informacije o nekom subjektu (korisniku ili kodu tj. programu). Na temelju njih SP donosi odluku o pravu pristupa željenoj usluzi/aplikaciji.

SAML definira tri različita tipa tvrdnji:

1. **Autentikacijske** – ovu izjavu oblikuje IdP kako bi potvrdio da je korisnik autenticiran korištenjem određene metode autentikacije (pametne kartice, biometrije, korisničkog imena, itd.) u određeno vrijeme
2. **Atributne** – koriste se za povezivanje subjekta s pojedinim atributima (npr. da je korisnik član neke organizaije, adresa, nadimak, itd.)

3. **Autorizacijske** – odgovor vlasnika resursa na zahtjev IdP-a da pristupi željenom resursu (dozvola ili zabrana pristupa)Slijedi primjer izjave (slika 2).

```
 1 <Assertion ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
 2    IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
 3    xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
 4    <Issuer>
 5       example.com
 6    </Issuer>
 7    <Subject>
 8       <NameID
 9         Format=
10         "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
11         Alice@example.com
12       </NameID>
13       <SubjectConfirmation
14         Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
15    </Subject>
16    <Conditions NotBefore="2003-04-17T00:46:02Z"
17                NotOnOrAfter="2003-04-17T00:51:02Z">
18       <AudienceRestriction>
19          <Audience>
20             example2.com
21          </Audience>
22       </AudienceRestriction>
23    </Conditions>
24    <AttributeStatement>
25       <saml:Attribute
26    xmlns:x500=
27      "urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
28    NameFormat=
29      "urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
30    Name="urn:oid:2.5.4.20"
31    FriendlyName="telephoneNumber">
32          <saml:AttributeValue xsi:type="xs:string">
33                +1-888-555-1212
34          </saml:AttributeValue>
35       </saml:Attribute>
36    </AttributeStatement>
37 </Assertion>
```

Slika 2. Primjer izjave
Izvor: IdentityMeme.org

Pojašnjenje slike 2:

- Linije 4-5 određuju tko je IdP (example.com)
- 7-15 definiraju korisnika (Alice@example.com)
- 16-23 postavljaju uvjete pod kojima se ova izjava smatra valjanom (vrijeme trajanja izjave za navedeni IdP)
- 24-36 navode atribute za korisnika (npr. broj telefona)

3.2.2. Protokol

SAML protokoli određuju kako se razmjenjuju SAML izjave između pružatelja usluge na temelju slanja zahtjev/odgovor poruka.

SAML 2.0 specificira moguće protokole:

- *Authentication Request protokol*
- *Single Logout protokol*
- *Assertion Query and Request protokol*
- *Artifact Resolution* protokol
- *Name Identifier Management* protokol
- *Name Identifier Mapping* protokol

Ovim se protokolima osigurava: slanje zahtjeva i odgovora za jednu ili više izjava, slanje zahtjeva za simultanom odjavom s različitih sustava, za određenom izjavom da je korisnik registriran kod IdP-a i za identifikaciju korisnika koji je registriran kod oba pružatelja usluge (IdP-a i SP-a),

U nastavku slijede primjeri zahtjeva, odnosno odgovora koji se razmjenjuju između pružatelja usluga (slike 3 i 4).

```
POST /SamlService HTTP/1.1
Host: www.example.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:AttributeQuery xmlns:samlp:="…"
xmlns:saml="…" xmlns:ds="…" ID="_6c3a4f8b9c2d" Version="2.0"
IssueInstant="2004-03-27T08:41:00Z"
            <ds:Signature> … </ds:Signature>
            <saml:Subject>
            …
            </saml:Subject>
        </samlp:AttributeQuery>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Slika 3. Primjer zahtjeva
Izvor: Sveučilište Santa Barbara (UCSB)

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Body>
        <samlp:Response xmlns:samlp="…" xmlns:saml="…" xmlns:ds="…"
ID="_6c3a4f8b9c2d" Version="2.0" IssueInstant="2004-03-27T08:42:00Z">
            <saml:Issuer>https://www.example.com/SAML</saml:Issuer>
            <ds:Signature> … </ds:Signature>
            <Status>
              <StatusCode Value="…"/>
            </Status>

            <saml:Assertion>
                <saml:Subject>
                …
                </saml:Subject>
                <saml:AttributeStatement>
            …
                </saml:AttributeStatement>
             </saml:Assertion>
        </samlp:Response>
    </SOAP-Env:Body>
```

Slika 4. Primjer odgovora
Izvor: Sveučilište Santa Barbara (UCSB)

3.2.3. Poveznice

Poveznice (eng. bindings) određuju na koji se način SAML protokoli povezuju s ostalim protokolima i prenose mrežom. Najvažnije SAML poveznice su:

- SAML SOAP– određuje kako SAML poruku enkapsulirati u SOAP omotnicu
- POST – enkapsulacija poruka u HTTP POST poruku
- HTTP Artifact – kada se SAML zahtjev ili odgovor prenosi putem URL adrese ili u HTML formatu
- HTTP Redirect – prijenos SAML poruka putem HTTP GET poruka
- PAOS (eng. *Reverse SOAP*) – određuje razmjenu SAML izjava kod mobilnih uređaja koji pristupaju određenim servisima i aplikacijama na web stranicama SAML URI (*eng. uniform* resource identifier) – ukoliko se SAML poruka prenosi putem URI identifikatora

3.2.4. Profili

Profili određuju konkretne slučajeve u kojima se koriste kombinacije ranije spojenih protokola i poveznica. Odnosno, oni omogućuju korištenje SAML standarda za izmjenu informacijskih podataka između različitih programa i uređaja.

Najvažniji SAML profil je *Web Browser SSO (eng. Single Sign-On) profil* koji pruža podršku za web SSO (jednostruka autentikacija na Internetu). Ovim se profilom definira korištenje SAML zahtjev/odgovor poruka s različitim kombinacijama HTTP Redirect, SOAP i HTTP POST poveznica. Više detalja o ovoj temi bit će rečeno u sljedećem poglavlju.

Osim navedenog, SAML 2.0 sadrži profile:

- ECP (eng. *Enhanced Client and Proxy*) – određuje kako koristiti SAML na mobilnim uređajima
- Otkrivanje pružatelja usluge (eng. *Identity Provider Discovery*) – koristi se za definiranje metode na koji način SP otkriva tko je IdP
- *Single Logout* profil – za automatsku odjavu sa svih sustava
- *Artifact Resolution* –definira kako koristiti *Artifact Resolution* protokol s određenom poveznicom
- *Assertion Query/Request* – kako koristiti istoimeni protokol (za slanje zahtjeva i odgovora koji sadrže SAML izjavu s pojedinim poveznicama
- *Name Identifier Management* – određuje kako koristiti *Name Identifier Management* protokol sa SOAP, HTTP Redirect, HTTP POST i HTTP Artifact poveznicama
- *Name Identifier Mapping* – definira kako koristiti *Name Identifier Mapping* protokol s različitim poveznicama

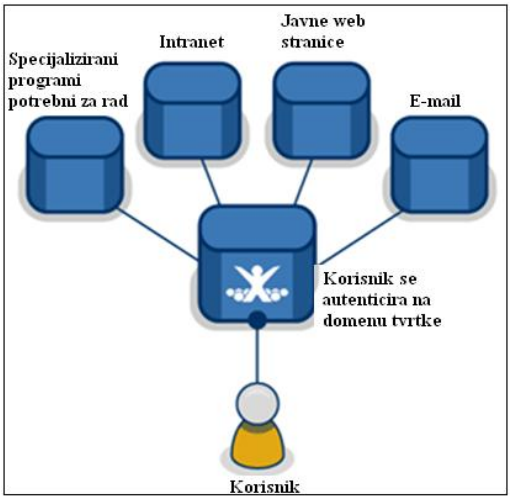
  Name Identifier Management i *Name Identifier Mapping* protokoli se odnose na slučaj kada je korisnik „od ranije“ registriran na obje domene (kod SP-a i IdP-a). Pojam „od ranije“ se odnosi na vrijeme prije nego je između pružatelja usluge uspostavljen ugovor o međusobnoj suradnji. Ovim se protokolima pružateljima usluge omogućava raspoznavanje da se radi o jednom korisniku koji je na različitim domenama prijavljen s različitim korisničkim imenom

4. Primjene SAML standarda

4.1. Web SSO

Najvažnija primjena SAML standarda je omogućavanje postupka jednostruke prijave i uspostave federativnog identiteta.

Jednostruka prijava (eng. *Single Sign-On*, SSO) predstavlja proces identifikacije koji korisnicima omogućuje predočenje svojih akreditacijskih podataka samo jednom kako bi mogli pristupiti različitim resursima. Tako korisnik ima osjećaj da u aplikacije ulazi bez dodatne autentikacije, čime se povećava ugodnost rada.



Slika 5. Postupak jednostruke prijave

Najprihvatljivije ostvarenje SSO-a je uporabom malih količina informacije koje poslužitelj pohranjuje na klijentsko racunalo preko preglednika i kojima kasnije može pristupati. Jedna takva informacija se naziva kolačić (engl. cookie). Kod prve prijave na pojedini poslužitelj, jedan kolačić sa zapisanim korisničkim imenim, se pohranjuje na klijentsko računalo. Prilikom svakog sljedećeg zahtjeva, poslužitelj može dohvatiti korisničko ime iz pohranjenog kolačića i odlučiti o daljnjim akcijama. Međutim, kolačići se ne mogu prenositi između računala unutar različitih domena. Noviji pristup ostvarenja SSO-a za web aplikacije je tzv. federativni pristup. Njime se želi postići povezivanje različitih korisničkih računa od jednog korisnika s pružateljima različitih usluga. Federacija kao takva predstavlja skupinu organizacija koje su dogovorile međusobnu suradnju prema određenim uvjetima i pravilima.

Što se time postiže? Uzmimo za primjer da je korisnik registriran na web stranici za rezervaciju avio leta. Slijedeći poveznice (eng, link) korisnik se upućuje na ostale stranice preko kojih može rezervirati sobu u hotelu, iznajmiti auto i slično, ali se na njih ne mora zasebno autenticirati niti prijavljivati s nekim novim korisničkim imenom.

Upotrebom SAML web SSO profila postiže se jednostruka autentikacija za različite sigurnosne domene. To u stvari znači da se korisnik prijavi na jednoj web stranici i zatim može pristupiti resursima na drugim web stranicama (na drugoj domeni) bez potrebe za ponovnom prijavom. SAML omogućuje SSO kroz komunikaciju izjavama. Stranica na kojoj se korisnik prijavio, šalje izjavu drugoj stranici. Na temelju informacija dobivenih izjavom (o identitetu korisnika) stranica koja je na različitoj domeni (od one odakle je izjava poslana) može tada propustiti korisnika kao da se izravno prijavio.

Postoje dva osnovna slučaja iniciranja SSO postupka prijave:

1. **IdP šalje podatke** - Korisnik se prijavljuje na web stranicu (npr. airline.example.com). Sa te stranice slijedi poveznicu na novu stranicu (cars.example.co.uk). Za pretpostaviti je pritom da je između njih uspostavljen federativni identitet i da je airline.example.com pružatelj usluge elektroničkog identiteta. Također, pretpostavka je da je korisnik već prijavljen na stranici airline.example.com. Kada korisnik klikne na poveznicu, IdP putem web preglednika šalje SAML izjavu prema SP-u. SP (cars.example.co.uk) na temelju izjave „propušta“ korisnika do traženog resursa, odnosno web stranice bez dodatne

prijave. U ovom slučaju korisnik ne mora upisivati svoje korisničke podatke kako bi pristupio stranici cars.example.com
prijave

2. **SP zahtijeva identifikaciju korisnika** - Mnogo češća je situacija u kojoj korisnik u web pregledniku izravno upisuje cars.example.co.uk. Korisnika se u tom slučaju putem web preglednika preusmjerava na stranicu airline.example.com (koja je definirana kao IdP). IdP potom šalje SAML izjavu prema SP-u. Za ovaj slučaj SAML definira poseban Identity Discovery profil kako bi SP mogao pronaći IdP i poslati mu zahtjev.

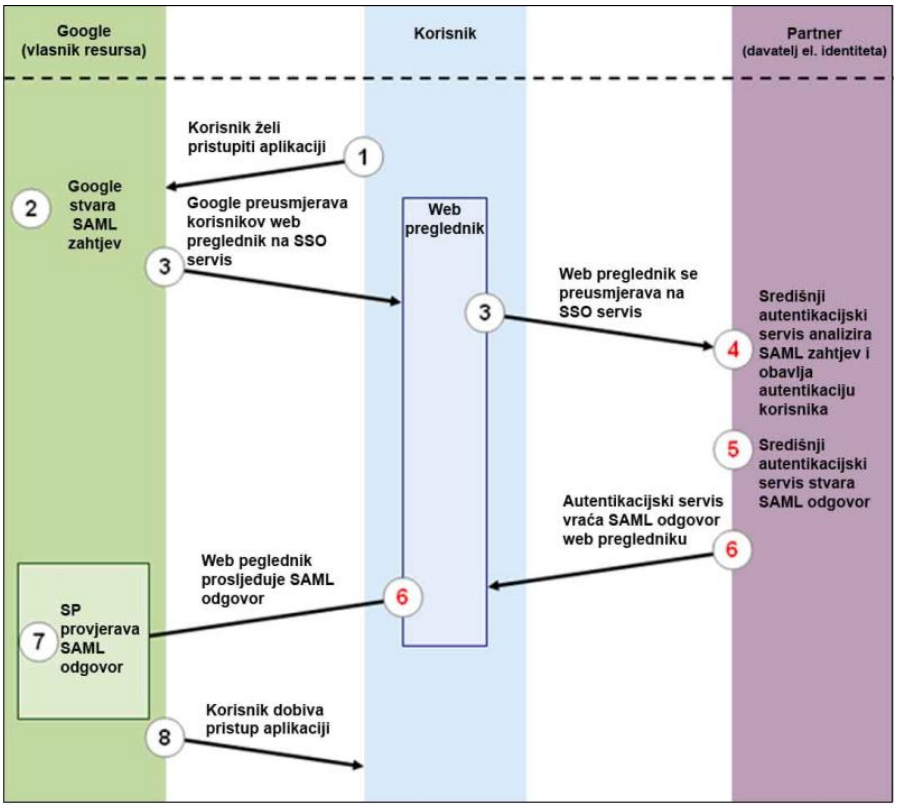
4.1.1. SAML SSO za Google Apps

U nastavku teksta je pikazan konkretan primjer komunikacije, tj. razmjena zahtjeva i odgovora prilikom pristupanja Google Apps aplikaciji.

Google Apps je servis koji korisniku omogućuje da na vlastitoj Internet domeni koristi Google alate za komunikaciju i suradnju, od kojih su najpoznatiji Gmail, Google kalendar, Gtalk, Google dokumenti i Google Sites.

Google Apps koristi SAML 2.0 specifikaciju na način da tvrtkama omogućuje autentikaciju i autorizaciju korisnika koji žele koristiti neke od maloprije spomenutih aplikacija. U ovom je slučaju Google Apps SP, dok je tvrtka davatelj elektroničkog identiteta. Pritom partnerska tvrtka mora Google-u prijaviti URL adresu svog SSO servisa kao i javni ključ koji će Google koristiti za potvrđivanje SAML zahtjeva.

Slika 5. prikazuje prijavu korisnika za korištenje Google aplikacija.



Slika 6. Prijava korisnika prilikom korištenje Google aplikacija

Izvor: Google

Pojašnjenje slike 5.

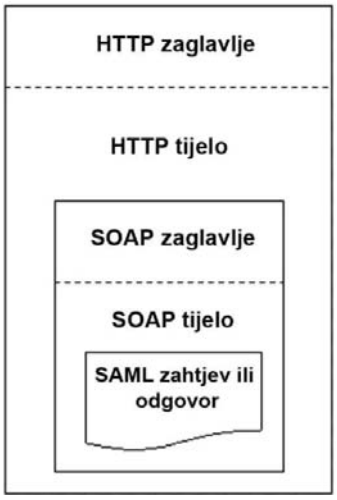
1. Korisnik pokušava pristupiti nekoj Google aplikaciji, npr. Gmail servisu za razmjenu elektroničke pošte
2. Google Apps (njihov SSO servis) obavještava web preglednik o potrebi provjere identiteta korisnika i stvara SAML autentikacijski zahtjev
3. Web preglednik se preusmjerava na IdP (korištenjem URL adrese)
4. SSO servis tvrke zatim provjerava je li korisnik već autenticiran (npr. kod korisnika provjerom kolačića za postojeću sjednicu) i provjerava dobiveni SAML zahtjev
5. IdP šalje povratni SAML odgovor (koji sadrži odgovarajuće izjave i atribute o korisniku) preko web preglednika do aplikacije koja je zatražila spomenutu provjeru
6. Nakon što Google servis za autentikaciju ovjeri dobivene podatke, korisnik dobiva pristup željenoj aplikaciji

4.2. Web servisi

Web servisi omogućuju integraciju različitih sustava i aplikacija putem standardiziranog načina komunikacije. Web servisi zapravo predstavljaju web aplikacije koje pružaju određenu funkcionalnost udaljenim programima.

Temeljni standard za razmjenu podataka u infrastrukturi Web servisa je SOAP. SOAP (eng. *Simple Object Access Protocol*) je aplikacijski protokol koji se koristi za razmjenu XML poruka između računala. SOAP poruke mogu biti razmijenjene preko različitih protokola (npr. HTTP i SMTP), ali uglavnom se koristi HTTP jer ga podržava većina internetskih poslužitelja i preglednika.

SAML je također moguće vezati uz različite komunikacijske i transportne protokole pa je tako moguće poslati SAML poruku korištenjem SOAP protokola preko HTTP veze. Ova je primjena određena SAML SOAP poveznicom koja određuje način na koji se SAML poruke enkapsuliraju u SOAP omotnice. U tom se slučaju SAML zahtjev/odgovor nalazi u tijelu SOAP poruke koja je smještena u HTTP omotnicu (slika 6).



Slika 7. Enkapsulacija poruke
Izvor: Wikipedia

Slika 7. prikazuje SAML poruku koja se prenosi u SAML omotnici:

```
1.  <?xml version="1.0" encoding="UTF-8"?>
2.  <env:Envelope
3.    xmlns:env="http://www.w3.org/2003/05/soap/envelope/">
4.    <env:Body>
5.      <samlp:AttributeQuery
6.        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
7.        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
8.        ID="aaf23196-1773-2113-474a-fe114412ab72"
9.        Version="2.0"
10.       IssueInstant="2006-07-17T20:31:40Z">
11.       <saml:Issuer>http://example.sp.com</saml:Issuer>
12.       <saml:Subject>
13.           <saml:NameID
14.           Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
15.           C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
16.           </saml:NameID>
17.       </saml:Subject>
18.       <saml:Attribute
19.           NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
20.           Name="urn:oid:2.5.4.42"
21.           FriendlyName="givenName">
22.       </saml:Attribute>
23.     </samlp:AttributeQuery>
24.   </env:Body>
25. </env:Envelope>
```

Slika 8. SAML poruka u SOAP omotnici
Izvor: OASIS

5. Sigurnost

Sigurnosni mehanizmi koje koristi SAML standard ovise o profilu koji se koristi u pojedinom slučaju kao i o okruženju u kojem se koristi. Tako se primjerice koriste drugačiji sigurnosni mehanizmi ako se SAML izjave prenose preko Interneta ili preko VPN veze. Također, nije potrebna enkripcija SAML poruke ukoliko se ona prenosi u SOAP omotnici koja se digitalno potpisuje.

5.1. Osnovne sigurnosne značajke

SAML specifikacija opisuje općenite zahtjeve za sigurnošću koji se moraju poštivati u svakom slučaju, bez obzira na vrstu okruženja ili profila koji se koristi:

- **Povjerljivost podataka** – podatke koji se šalju mogu pročitati samo one strane kojima su ti podaci namijenjeni. Kako bi se to postiglo koristi se uglavnom 3DES ili AES enkripcija
- **Integritet podataka** – nemogućnost izmjene (slučajno ili namjerno) podataka koji se prenose. U ovu se svrhu koriste digitalni potpisi koji se stvaraju pomoću RSA algoritma.
- **Autentikacija** – je vezana uz proces utvrđivanja identiteta korisnika razmjenom izjava
- **Autorizacija** – odnosi se na primjenu sigurnosne politike (npr. tvrtke) zbog utvrđivanja ovlasti pristupa pojedinim dijelovima sustava za korisnike na temelju SAML izjava
- **Povjerenje između strana koje komuniciraju** – odnosi se na povjerenje između IdP-a i SP-a, a temelji se na razmjeni X.509 certifikata. X.509 je standard digitalnog certifikata, u kojem se navodi struktura certifikata. Najvažnija polja u certifikatu su ID, naziv nositelja certifikata, datum isteka, javni ključ i CA potpis. O certifikatima brine nadležna CA (eng. certification authority) institucija. Za više detalja o ovoj temi preporuča se pogledati dokument „Metode povlačenja digitalnih certifikata“ raspoloživog na web adresi:

  http://www.cert.hr/documents.php?lang=hr

5.2. Primjena sigurnosnih mehanizama

5.2.1. Sigurnost komunikacijskog kanala

Kao što je spomenuto, korištenje pojedinih sigurnosnih mehanizama ponajviše zavisi o okruženju. Ako se SAML poruka prenosi preko zaštićenog kanala, onda ju nije potrebno kriptirati

Kako bi se ostvarila zaštićena komunikacija preko HTTP veze koriste se protokoli SSL i TLS.

SSL (eng. *Secure Sockets Layer*) i TLS (eng. *Transport Layer Security*) su transportni protokoli unutar TCP/IP stoga. Omogućuju sigurnu komunikaciju preko Interneta za razne aplikacije kao što su Internet bankarstvo, web pristup e-pošta itd.

SAML standard definira poželjne i opcionalne kombinacije načina kodiranja. Oni predstavljaju kombinaciju parametara kao što su odabir sigurnosnog algoritma, veličina ključa korištenog za autentifikaciju, dogovor o ključu, način kodiranja i način zaštite cjelovitosti poruke. Spomenute kombinacije su:

- TLS_RSA_WITH_3DEC_EDE_CBC_SHA – poželjan za SOAP preko HTTP-a
- TLS_RSA_AES_128_CBC_SHA – opcionalan za SOAP preko HTTP-a
- SSL_RSA_WITH_3DES_EDE_CBD_SHA - poželjan za web SSO profil preko SSL veze
- TLS_RSA_WITH_3DES_EDE_CBC_SHA - opcionalan za web SSO profil preko TLS veze

5.2.2. Zaštita poruka

Ukoliko se SAML poruke ne prenose preko sigurnog komunikacijskog kanala, mogu se koristiti i druge sigurnosne postavke. To su:

a) XML potpis

XML potpis je u stvari digitalni potpis, ali je prilagođen upotrebi u XML dokumentima. Digitalno XML potpisivanje koristi standard *XML Signature* koji opisuje XML sintaksu za predstavljanje i povezivanje kriptografskih potpisa i podataka u XML dokumentima.
XML potpis moguće je koristiti za zaštitu izjava i protokola

```
<element name = "Assertion" type = "saml:AssertionAbstractType"/>
   <complexType name = AssertionAbstractType = "true">
      <sequence>
         <element ref = "saml:Conditions" minOccurs = "0"/>
         <element ref = "saml:Advice" minOccurs = "0"/>
         <element ref = "ds:Signature" minOccurs="0" maxOccurs="1"/>
      <sequence>
      <attribute name = "MajorVersion" use = "required" type = "integrer"/>
      <attribute name = "MinorVersion" use = "required" type = "integrer"/>
      <attribute name = "AssertionID" use = "required" type = "saml:IDType"/>
      <attribute name = "Issuer" use = "required" type = "string"/>
      <attribute name = "IssueInstant" use = "required" type = "timeInstant"/>
   </complexType>
```

Slika 9.
Zaštita izjave korištenjem XML potpisa
Izvor: OASIS

b) XML enkripcija

XML enkripcija je W3C standard pomoću kojeg se XML sadržaj kodira i tako postaje vidljiv (dostupan) samo za određenog primatelja, a nevidljiv za sve ostale. Osim kriptiranja cijelog dokumenta, moguće je zaštititi i pojedinačne dijelove XML dokumenta.

Slika 10. Osnovna struktura XML kriptiranja

SAML shema uključuje razne elemente za enkripciju dijelova podataka koji trebaju biti povjerljivi. Neki od elemenata koji se primjenjuju za izjave i protokole su:

- <EncryptedId>
- <EncryptedAssertion>
- <EncryptedAttribute>

c) WS-Security

Za zaštitu SOAP poruka koriste se sigurnosne značke koje definira WS-Security standard. Sigurnosna značka (engl. *security token*) je oznaka koja se umeće u SOAP poruku, a služi kao sigurnosna propusnica, odnosno iskaznica identiteta koju treba pokazati ako se želi pristupiti u domenu zaštićenog sustava. Tako se za zaštitu SAML poruke u SOAP omotnici koristi SAML značka koja je zapisana u binarnom obliku

```
<S12:Envelope>
  <S12:Header>
    <wsse:Security>
      <saml:Assertion
        AssertionID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer="www.opensaml.org"
        MajorVersion="1"
        MinorVersion="1"
          . . .
      </saml:Assertion>
      <wsse:SecurityTokenReference wsu:Id="STR1">
        <wsse:KeyIdentifier wsu:Id="…"
          ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-
token-profile-1.0#SAMLAssertionID">
          _a75adf55-01d7-40cc-929f-dbd8372ebdfc
        </wsse:KeyIdentifier>
     </wsse:SecurityTokenReference>
    </wsse:Security>
  </S12:Header>
  <S12:Body>
    . . .
  </S12:Body>
</S12:Envelope>
```

Slika11. Zaštita SAML poruke u SOAP omotnici
Izvor: OASIS

5.3. Najčešće vrste napada

Ovisno o pojedinoj primjeni standarda SAML, zlonamjerni korisnici mogu izvesti napade vezane uz određene komponente SAML jezika (izjave, protokole, poveznice i profile). Najčešće vste napada su:

- **Prisluškivanje** – odvija se ako se podaci šalju kao „čisti tekst“ (eng. *plain text*)
- **Krađa informacija o korisniku**
- **Napad ponavljanjem slanja poruka** (eng. R*eplay Attack*)
- **Napad uskraćivanjem usluga** (eng. *Denial of Service*) – osnovni cilj ovakvog napada je učiniti sustav ili mrežu nedostupnom
- **MITM (eng. *man-in-the-middle*) napad** – napadač se nalazi na kanalu između strana koje komuniciraju. Na taj način uljez presreće povjerljive informacije (ima mogućnost nadgledanja, spremanja kopija dokumenata i njihove izmjene)
- **Lažiranje identiteta** – koristi se u svrhu lažiranja IP adrese pri čemu je moguće zaobići zaštitne mehanizme i dobiti pristup zaštićenim resursima

Najpoznatiji slučaj ranjivosti SAML standarda je u primjeni SAML SSO sustava za Google Apps servis. Radilo se o pogrešci koja je omogućila lažiranje IdP-a, što su napadači mogli iskoristiti kako bi saznali valjana korisnička imena (i lozinke). Više detalja o ovoj temi moguće je pronaći na stranici:

http://www.ai-lab.it/armando/pub/fmse9-armando.pdf

6. SAML primjene i budući razvoj

Na tržištu postoje različiti programi koji omogućuju uspostavu federativnog identiteta. Pozitivna strana njihovog korištenja je međusobna sukladnost, ali uz obavezan uvjet da su prilagođeni SAML standardu (inačicama 1.1 i 2.0).

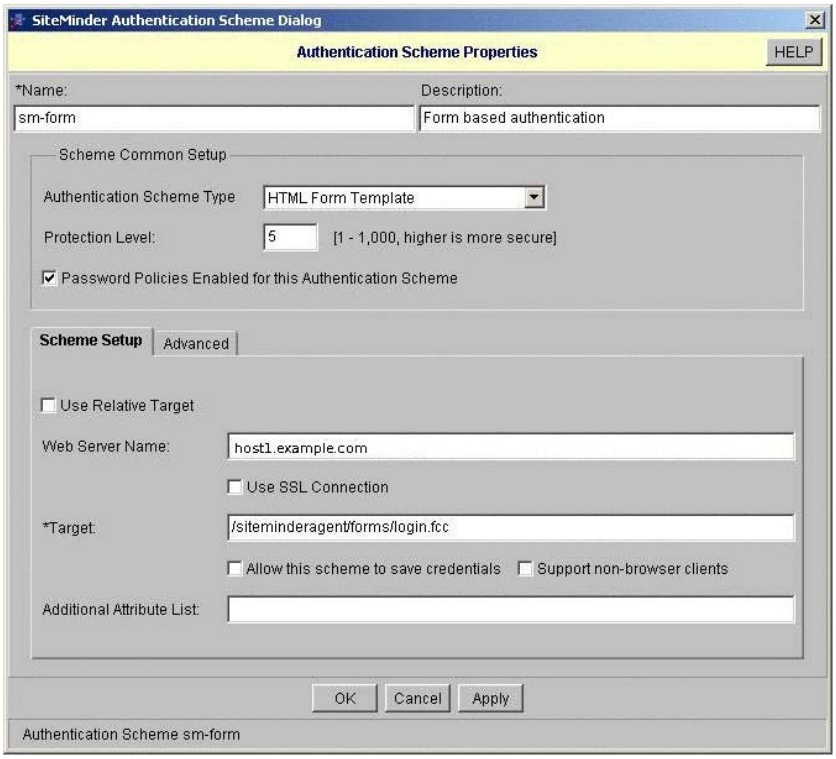
Najpoznatiji od tih programa su navedeni u tablici 2. :

Programi	Opis
OpenSAML	Riječ je o skupu C++ i Java biblioteka koji pružaju podršku programerima koji rade sa SAML-om (definiranje izjava, protokola i poveznica). Spomenute biblioteke ne mogu se iskoristiti za korištenje SAML profila
Shibboleth	Radi se o projektu otvorenog programskog koda koji omogućuje konfiguriranje SSO sustava između različitih domena. U svom radu koristi OpenSAML. Orijentiran je na mogućnost razmjene podataka u obrazovnim i akademskim institucijama.
OpenSSO	Ovaj je program otvorenog koda razvila tvrtka Sun Microsystems. Napisan je u Javi, a radi se o poslužiteljskoj plaformi za uvođenje sustava za identifikaciju korisnika i upravljanje ovlastima pristupa različitim resursima. Postoji i komercijalna inačica pod nazivom OpenSSO Enterprise. Podržava sljedeće operacijske sustave: Red Hat Enterprise Linux, Ubuntu, Windows 2003/Vista, IBM AIX i Sun Solaris.
SiteMinder	Program je razvila tvrtka Computer Associates (CA). Namijenjen je poslovnim korisnicima za provjeru pristupa web aplikacijama za djelatnike, klijente i poslovne korisnike. Podržan je na UNIX, Linux i Windows platformama.
RSA Federated Identity Manager	Program koji je razvila tvrtka RSA Security kao rješenje za uspostavu federativnog identiteta između poslovnih korisnika. Cijena programa zavisi o broju partnera s kojima se tvrtka želi povezati (osnovna cijena za jednog partnera je $25,000). Podržani operacijski sustavi su Microsoft Windows 2003 EE, Sun Solaris 9 i 10, te Red Hat Linux.

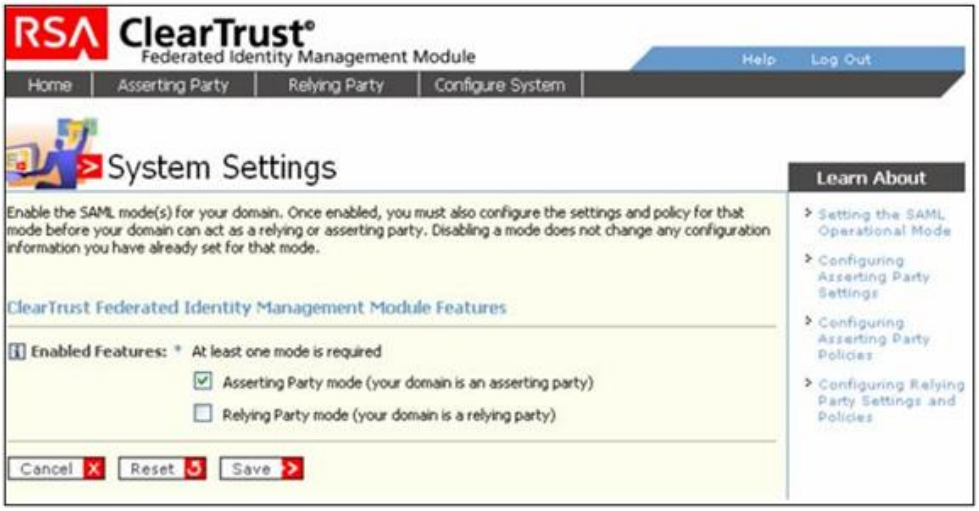
Tablica 2. Programi za korištenje SAML standarda

Kako ti programi izgledaju u primjeni moguće je vidjeti na narednim slikama.

Slika 12. OpenSSO
Izvor: Sun Microsystems



Slika 13. SiteMinder
Izvor: CA Software Systems



Slika 14. RSA Federated Identity Manager

Izvor: RSA

Određeni postojeći standardi su u svoje specifikacije već unijeli načine kako koristiti SAML u svom radu. Najpoznatiji od njih su:

- XACML (eng. *XML* Access *Control Markup Language*)

  Riječ je o OASIS standardu koji se može koristiti za provjeru pristupa XML dokumentu. Obično modeli provjere pristupa uključuju zahtjev korisnika za pristup XML dokumentu, a sustav mu to dozvoli ili odbije. Moguće je nadgledati pristup cijelom XML dokumentu ili samo nekim dijelovima. Ovaj standard u svojoj specifikaciji sadrži način primjene SAML podataka: od načina njihove obrade pa do korištenja kao mjerila na temelju kojeg se donosi odluka o pravima pristupa.

- WS-Security (eng. *Web Services Security*)

  Protokol su razvili IBM, Microsoft i VeriSign, a objavljen je kao OASIS standard. Riječ je o komunikacijskom protokolu koji osigurava sigurnost primjene web servisa. Protokol definira kako pripojiti elektronički potpis i zaglavlja enkripcije na SOAP. Osim toga, uključuje i detalje u korištenju SAML jezika, Kerberos sustava (za autentikaciju i autorizaciju) i digitalnih certifikata.

Upotreba SAML-a (kao samostalnog standarda ili u sklopu nekog drugog) kao osnove za osiguranje jednostruke autentikacije između različitih proizvođača se do sada pokazala kao vrlo uspješna i učinkovita. Za očekivati je kako će se taj trend nastaviti i u budućnosti jer bi se time osigurao centraliziran mehanizam za provođenje i upravljanje sigurnosnom politikom za pristup aplikacijama i servisima. U međuvremenu, stručnjaci iz OASIS skupine rade na definiranju novih, dodatnih komponenti za povezivanje s drugim komunikacijskim i transportnim protokolima koji nisu obuhvaćeni dosadašnjim specifikacijama. Te komponente ponajviše ovise o potrebama tvrtki i organizacija koje žele primijeniti SAML za svoje programe.

7. Zaključak

U posljednje vrijeme je sve više uočljiv trend povezivanja različitih sustava i aplikacija preko web portala, servisa i integriranih aplikacija. Stoga je nastala potreba za razvijanjem XML standarda koji bi omogućio prijenos autorizacijskih i autentifikacijskih podataka između tih sustava. Upravo SAML standard omogućuje takvu razmjenu informacija, čime se ujedno omogućuje uspostava jedinstvenog identiteta u raspodijeljenim sustavima.

Budući da se radi o standardu koji se počeo učestalo primjenjivati, moguće je da potencijalni napadači pokušaju doći u posjed podataka koji se razmjenjuju. Međutim, SAML standard detaljno opisuje koje je sve metode moguće koristiti u svrhu zaštite te se stoga korisnicima preporuča njihova primjena.

8. Reference

[1] Demystifying SAML, Harold Lockhart, http://www.oracle.com/technology/pub/articles/dev2arch/2005/11/saml.html, rujan 2005.

[2] Google, http://code.google.com/apis/apps/sso/saml_reference_implementation.htm, rujan 2009

[3] Krešimir Pavić: Sloboda za sve, http://www.bug.hr/mreza/tekst/liberty-alliance/51466.aspx, travanj 2004.

[4] Oasis Security Services TC, http://www.oasis-open.org/committees/security/faq.php, siječanj 2006.

[5] IBM: Debunking SAML myths and Misunderstandings, http://www.ibm.com/developerworks/xml/library/x-samlmyth.html, lipanj 2003.

[6] Wikipedia: SAML, http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language, listopad 2009.

[7] Univerzitet Sarajevo: Web servisi, http://209.85.129.132/search?q=cache:eQrYAVz4I2IJ:subversion.assembla.com/svn/WebServisi/WebServis.doc+internet+problem+nestandardiziranost&cd=3&hl=hr&ct=clnk&gl=hr, svibanj 2004.

[8] OASIS, http://xml.coverpages.org/SAML-ImplementationGuidelinesV01-8958.pdf, kolovoz 2004.

[9] FER Zagreb: Nadziranje pristupa računalnim sustavima zasnovanim na uslugama, http://bib.irb.hr/datoteka/277854.Magistarski_MiroslavPopovic.pdf, 2006.

[10] OASIS, http://209.85.129.132/search?q=cache:1jrRpwUw3ugJ:docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf+saml+security+consideration&cd=1&hl=hr&ct=clnk&gl=hr&client=firefox-a, ožujak 2005.