Java Sun OpenSSO

Odprtokodni sistemi za enkratno prijavo v spletne aplikacije - Java Sun OpenSSO Enterprise 8

Sandi Holub, Bron d.o.o.

Potek predavanja

- Pregled najpogostejših problemov v zvezi s spletnimi aplikacijami
- Prednosti in slabosti SSO
- Pregled odprtokodnih rešitev za SSO
- Predstavitev Java Sun OpenSSO Enterprise 8
- Demonstracija

Tipični problemi spletnih aplikacij

- Vsaka aplikacija zahteva uporabnikovo prijavo
- Uporabnik ima lahko veliko uporabniških imen in gesel
- Potreben je nadzor dostopa do aplikacij in pravic uporabnikov znotraj posamezne aplikacije
- Partnerji potrebujejo dostop do naših zaščitenih aplikacij

Prednosti SSO

- Enkratna prijava v vse spletne aplikacije z isto metodo avtentikacije
- Prehod iz ene v drugo spletno aplikacijo brez ponovne prijave
- Manjša možnost napačne prijave
- Centraliziran nadzor
- Zmanjšana potreba po podpori uporabnikov

Slabosti SSO

- Če nekdo ukrade uporabniško ime in geslo ima dostop do vseh uporabnikovih aplikacij
- Če SSO sistem ne deluje se ni možno prijaviti v nobeno aplikacijo
- Razni napadi (replikacija, prestrezanje)

Odprtokodne rešitve SSO

- OpenSSO Enterprise 8 (Sun)
- JA-SIG CAS (Yale)
- JOSSO (Apache)

OpenSSO Enterprise 8

- Proizvod dolgoletnega razvoja Sun Microsystems, Inc.
- Odprtokodni spletni sistem za enkratno prijavljanje, ki zna rešiti vse probleme sodobne kontrole dostopa do spletnih aplikacij
- Kontrola dostopa (avtentikacija in avtorizacija) do spletnih aplikacij
- Kontrola dostopa do spletnih storitev
- Med domenska (cross domain) avtentikacija in avtorizacija
  - SAML 2.0
  - WS-Federation

Kdo uporablja OpenSSO

- Verizon wireless ima več kot 40 mio uporabnikov, 1 mio prijav na dan in največ 4000 prijav na minuto
- Audi UK ima OpenSSO za uporabnike njihovega portala (cca. 250 tisoč uporabnikov)

Prednosti OpenSSO

- Odlična podpora implementatorjem preko Sunovih svetovalcev
- Med domenska enkratna prijava
- “Site” način delovanja. Nameščena imamo dva sistema OpenSSO na različnih strežnikih, ki nista v isti gruči. Strežnika sama skrbita za pravilno nemoteno delovanje sistema v primeru izpada posameznega strežnika.
- Centralizirane konfiguracijske datoteke
- Podpira vse spletne aplikacije, ki poznajo protokol HTTP/1.1
- Razširljivost, modularnost, enostavno administriranje
- Podpira veliko aplikacijskih strežnikov npr. BEA WebLogic 10, Oracle IAS 10g 10.1.3.x, IBM WebSphere, Glassfish, Apache Tomcat, Jboss Application Server 4.x itd.

Prednosti OpenSSO

- V aplikacijah je potrebno spremeniti samo minimalen del kode v delu kjer se uporabnik prijavi v posamezno aplikacijo
- Izdelana rešitev za spletne java aplikacije
- Izdelana rešitev za vse ostale aplikacije ki poznajo HTTP protokol
- Enostavna vzpostavitev visoko zanesljive arhitekture
- Enostaven razvoj avtentikacijskih modulov za potrebe različnih načinov avtentikacije (SecurID, certifikati, Active Directory)

Prednosti OpenSSO

- Poglejmo koliko je potrebno spremeniti v eni javanski aplikaciji, katera sama kontrolira avtentikacijo

```
private String getAuthenticatedUser()
{
  FacesContext facesContext = FacesContext.getCurrentInstance();
  HttpServletRequest httpServletRequest =  (HttpServletRequest)
     facesContext.getExternalContext().getRequest();
       OrderedSet orderedSet = (OrderedSet)
     httpServletRequest.getAttribute("HTTP_REMOTE_USER");
       if(!orderedSet.isEmpty())
           return ""+orderedSet.get(0);
       return "Ni podatkov o uporabniku";
}  //Dodati je potrebno še ustrezne knjižnice
```

Prednosti OpenSSO

- Potrebno je dodati še filter za agenta v web.xml

```
<filter>
    <filter-name>Agent</filter-name>
    <filter-class> com.sun.identity.agents.filter.AmAgentFilter </filter-class>
  </filter>
  <filter-mapping>
    <filter-name>Agent</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
    <dispatcher>INCLUDE</dispatcher>
    <dispatcher>FORWARD</dispatcher>
    <dispatcher>ERROR</dispatcher>
  </filter-mapping>
```

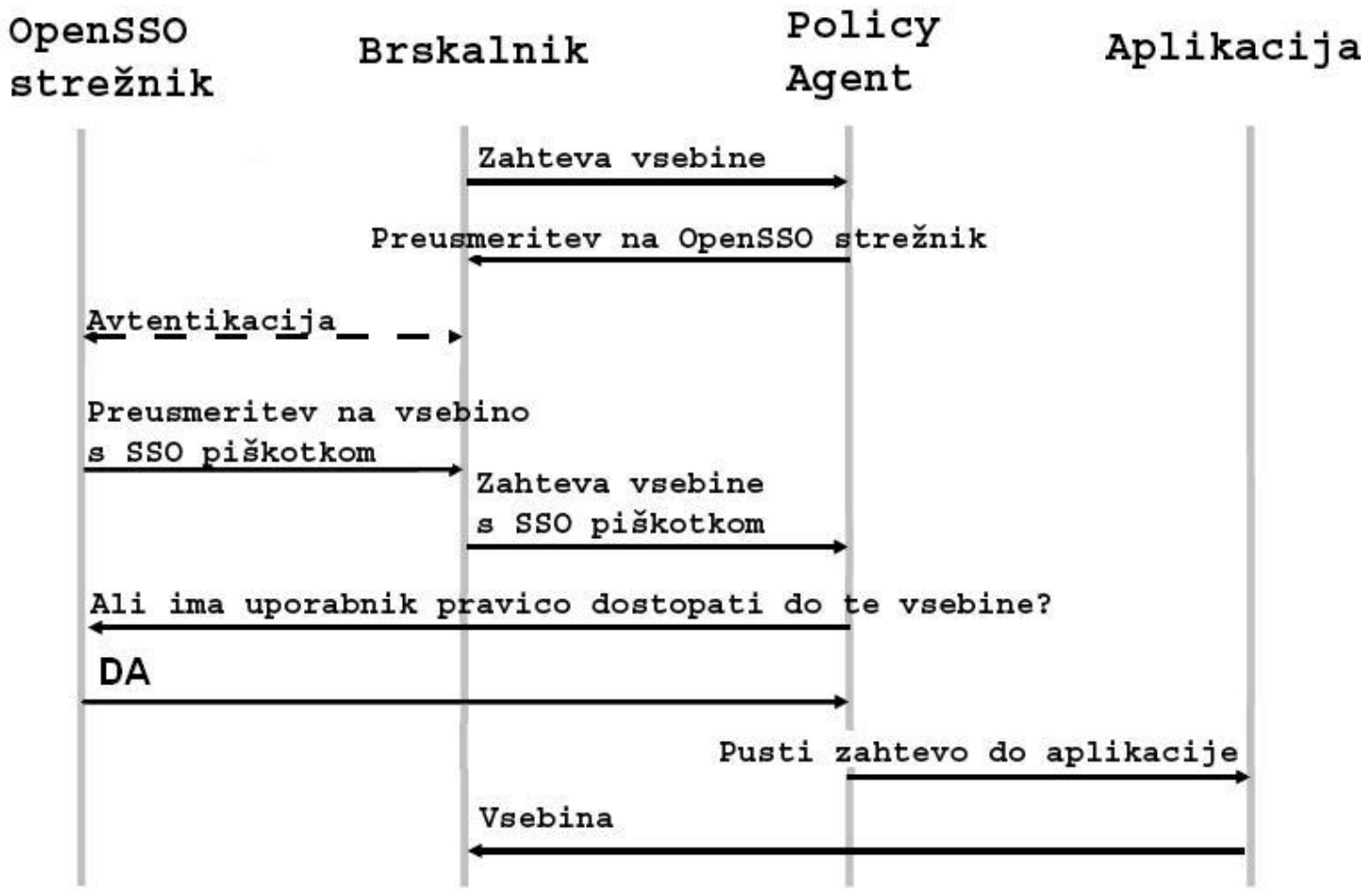
Oblike SSO z OpenSSO

- Avtentikacija in avtorizacija
- Samo avtentikacija
- Med domenska prijava

Avtentikacija

- Lažji način implementacije OpenSSO rešitve
- OpenSSO skrbi za avtentikacijo in ne tudi za avtorizacijo
- Podatki o avtorizaciji so shranjeni drugje
- OpenSSO aplikaciji v tem primeru poda uporabniško ime prijavljenega uporabnika
- Aplikacija sama poveže to uporabniško ime s pravicami uporabnika in se glede na te pravice ustrezno vede (administrator, navadni uporabnik)

Postopek avtentikacije



Avtorizacija

- Kompleksnejši način implementacije OpenSSO
- OpenSSO mora hraniti podatke o uporabniških pravicah
- Uporabniki morajo biti grupirani znotraj OpenSSO glede na njihove vloge
- OpenSSO mora pri komunikaciji z aplikacijo le tej podati tudi podatke o pravicah uporabnika
- Aplikacija mora znati interpretirati prejete podatke o avtorizaciji
- Kompleksna pravila v OpenSSO avtorizacijskem agentu

OpenSSO Policy agent

- Modul ki stoji na aplikacijskem strežniku zaščitene aplikacije
- Web in J2EE agenti
- Dostopni na OpenSSO strani
- Odprtokodni moduli katere lahko razširimo za svoje potrebe
- Centralizirana konfiguracija

OpenSSO Policy agent

Enter the Application Server Config Directory Path:

C:\Sun\AppServer\domains\domain1\config

Enter the URL where the OpenSSO server is running.

OpenSSO server URL:http://2andi.bron.si:9090/opensso

Enter the Agent URL.

Agent URL:http://2andi.bron.si:8080/agentapp

Enter the Agent Profile name

Profile name:glassfishagent

Enter the path to the password file:

D:\Java\j2ee_agents\appserver_v9_agent\passwordfile.txt

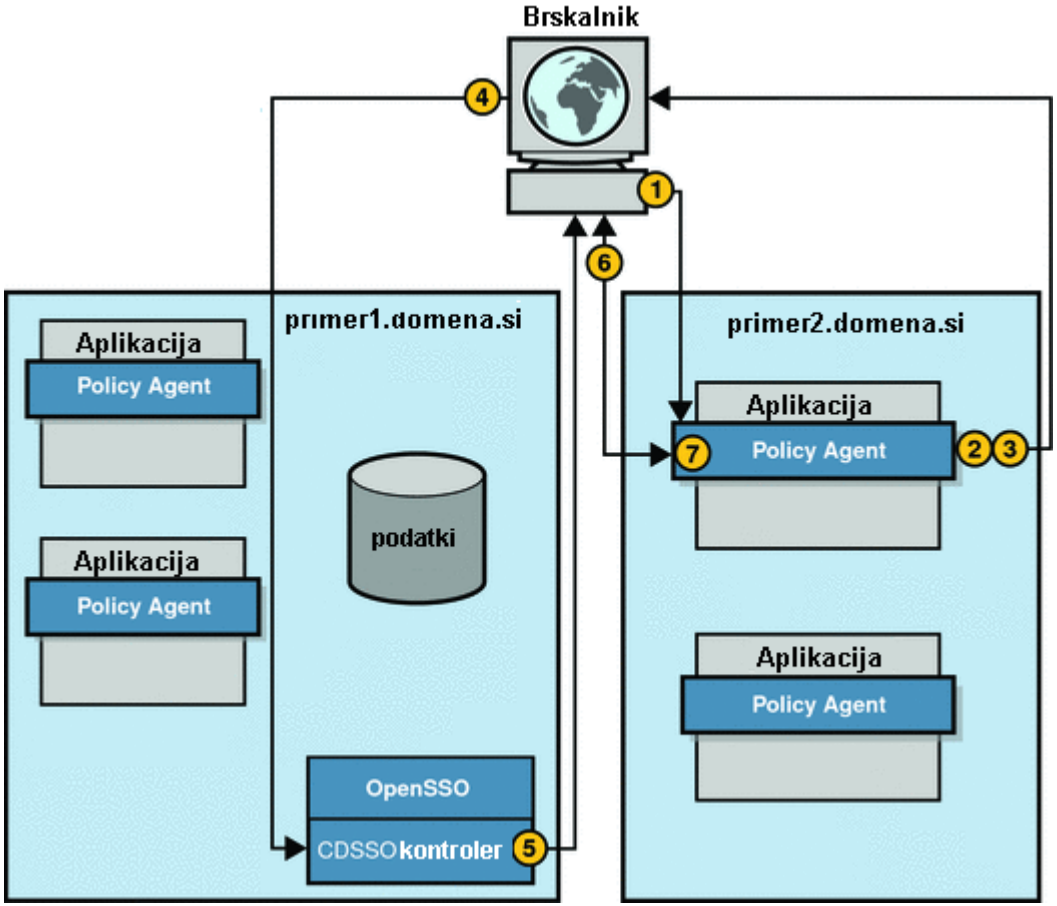
Avtorizacija ali avtentikacija ?

- Že obstoječe aplikacije, bazna avtorizacija -> avtentikacija
- Kompleksnejša pravila avtorizacije -> avtentikacija
- Veliko aplikacij v katerih je potrebno avtorizacijo zamenjati -> avtentikacija
- Centraliziran nadzor avtentikacije in avtorizacije -> avtentikacija in avtorizacija
- Nova zbirka spletnih aplikacij -> avtentikacija in avtorizacija

Med domenska prijava

- CDSSO kot lažja rešitev problema med domenske prijave
  - V nastavitvah agenta se določi, da bo prijava potekala preko CDSSO
  - Določimo v katerih domenah so veljavni piškotki
  - Namestitev CDC med domenskega kontrolerja
- Med domenska prijava s SAML v2 protokolom
  - Postavitev kroga zaupanja, service ter identity providerjev
  - Omejitev uporabe piškotkov
  - Skoraj obvezena varna SSL povezava zaradi XML

Med domenska prijava



Enostavna namestitev

- Namestimo OpenSSO Enterprise 8 na strežnik (npr. V Glassfish okolje)
- Na aplikacijski strežnik ali proxy strežnik namestimo veljavnega agenta
- V aplikaciji popravimo prijavno stran tako da sedaj dobi uporabniško ime in/ali pravice iz HTTP glave in ustrezno reagira
- Ni potrebna namestitev posebne uporabniške zbike podatkov

Demo

- Prikaz administracijskega vmesnika OpenSSO
- Prikaz delovanja OpenSSO

Vprašanja