10_Autentifikacija - CAS

Centralni autentifikacijski servis (engl. *Central Authentication Service* – u daljem tekstu CAS) za Web je napravljen da radi s aplikacijama kojima se pristupa isključivo preko Web browsera. Svaki zahtev se presreće od strane interfejsa ili aplikacije, a neautentifikovani korisnici se ne propuštaju do traženog resursa. CAS je autentifikacijski servis razvijen na Univerzitetu Yale i pruža pouzdan način autentifikacije korisnika. CAS protokol je dostupan svima, a programski kod se može skinuti sa službenih stranica.

Usluge koje pruža CAS su:

• Olakšava SSO na višestrukim Web aplikacijama, kao i jezgru za servise koji nisu nužno bazirani na Webu, ali poseduju grafičko okruženje.

• Omogućava nepouzdanim aplikacijama autentifikaciju korisnika bez pristupa lozinkama.

• Pojednostavljuje procedure koje aplikacije moraju da slede da bi autentifikovali korisnika.

• Autentifikacija se lokalizuje na jednoj Web aplikaciji, čime se olakšava čuvanje i promena lozinki, bez izmena ostalih aplikacija.

CAS arhitektura

Centralni autentifikacijski servis je dizajniran kao samostalna Web aplikacija. Ostvaren je kao nekoliko Java apleta i koristi HTTPS protokol. Pristupa mu se kroz tri URL-a:

a) URL za prijavu,
b) URL za validaciju,
c) opcioni URL za odjavu.

Korisnik uobičajeno dolazi na jednu od Web aplikacija koje za autentifikaciju i SSO koriste CAS. U tom slučaju, aplikacija preusmerava korisnika na URL za prijavu. Tom URL-u se može pristupiti i direktno, ako se želi autentifikacija bez pozivanja bilo koje aplikacije. URL za prijavu obrađuje "primarnu" autentifikaciju, zapravo zahteva od korisnika unos imena i lozinke i proverava njihovu validnost. CAS sistem se može konfigurisati tako da vrši proveru korisničkog imena i lozinke pomoću bilo kojeg poznatog entiteta kao što su:

1. obična datoteka s lozinkama
2. kriptovana datoteka s lozinkama
3. baza podataka
4. LDAP server
5. ostalo

Kako bi se omogućila automatska ponovna autentifikacija, CAS šalje browseru "in-memory cookie" (koji se briše čim se browser isključi). Taj cookie se naziva cookie za dodelu ulaznica (engl. *ticket-granting cookie*), i identifikuje korisnika koji se već uspešno prijavio. Ako se on izostavi, korisnik će morati da unese ime i lozinku svaki put kada ga aplikacija preusmeri na CAS. Ako se ne izostavi, dobija se Single Sign-On za više Web aplikacija. Odnosno, korisnik unosi ime i lozinku samo jednom i dobija pristup svim aplikacijama koje koriste CAS. Prilikom odjave, cookie za dodelu ulaznica se

uništava, čime je potrebna ponovna prijava (odjava se izvršava odlaskom na URL za odjavu – *logout URL*).

Prilikom primarne autentifikacije, CAS pamti i aplikaciju kojoj je korisnik hteo da pristupi i sa koje je preusmeren. To je moguće, jer su aplikacije prilikom preusmeravanja korisnika dužne da predaju i svoj identifikator.

Ako je autentifikacija uspešna, CAS kreira ulaznicu – veliki slučajni broj. Tada se ta ulaznica povezuje sa korisnikom koji se uspešno autentifikovao i sa aplikacijom kojoj korisnik želi da pristupi. Kreirana ulaznica je namenjena samo za jednu upotrebu – jednom iskoristiva, validna je samo za tog korisnika i samo za tu aplikaciju u toj sesiji.

Po završetku primarne autentifikacije, CAS usmerava korisnika na aplikaciju sa koje je došao, odnosno kojoj je hteo da pristupi. To je moguće, jer već pomenuti identifikator aplikacije (engl. *serviceID*) deluje kao URL (engl. *callback URL*). To jest, identifikator mora da predstavlja URL same aplikacije. CAS usmerava korisnika na taj URL, dodajući kreiranu ulaznicu kao jedan parametar.