Projektni zadatak 1.

Implementirati servis koji ima ulogu servera za logovanje (*Main Audit Service - MAS*). MAS je zadužen da na centralizovan način zapisuje događaje pristigle od različitih klijenata. Autentifikacija između MAS servera i njegovih klijenta je Windows, gde se za razmenu poruka korisnti digitalno potpisivanje.

MAS klijenti su XML Management (XMS) komponente koje svojim korisnicima pružaju usluge definisane interfejsom *IServices* za upravljanje XML datotekama. Postoje dve grupe XMS komponenti u zavisnosti od načina na koji loguju relevantne bezbednosne događaja: XMS koji zapisuje događaje u Windows Event Log i XMS koji zapisuju događaje u TXT fajl.

XMS komponente nude mogućnost kreiranja, čitanja i modifikovanja XML fajla. XML fajlovi predstavljaju malo bazu podataka u okviru koje se smeštaju liste studenata, predmeta i profesora. Takođe je neophodno implementirati proveru integriteta XML fajla.

XMS implementira ACL model kontrole pristupa tako da je za pristup svim metodama potrebno da korisnik ima Read privilegiju. Dodatno, za kreiranje xml fajla korisnik mora da ima privilegiju CreateFile, a za brisanje xml fajla korisnik mora da ima privilegiju DeleteFile. Za modifikaciju (pod modifikacijom se smatra dodavanje ili brisanje studenta, predmeta i/ili profesora) fajla korisnik mora da ima privilegiju Modify.

Dodatno, kao vlasnik datoteke (property Owner) mora da stoji ime klijenta koji je kreirao fajl.

Dodatno ograničenje jeste da ukoliko je korisnik Owner fajla može da vrši sve operacije nad fajlom ukoliko ima Read privilegiju (ostale mu nisu neophodne, a može da ih poseduje).

Autentifikacija izmedju klijenata i XMS je preko sertifikata.

Svaki XMS loguje događaj, i šalje notifikaciju MAS serveru o novom događaju, koje on zatim loguje u jedinstvenoj bazi podataka. Neophodno je voditi racuna da ukoliko MAS server nije pokrenut u momentu logovanje XMS cim uspostavi konekciju sa njim posalje sve one informacije koje do tada nije uspeo da prosledi.

Dodatno, MAS server vodi računa o nivou kritičnosti događaja na sledeći način:

- *Low level* su događaji niskog prioriteta, i tu spada detekcija neuspešnog pokušaja bilo kakve manipulacije nad određenim fajlom.
- *Medium level* su događaji kada se u periodu od S (konfigurabilno) sekundi detektuje N (konfigurabilno) puta neuspešan pokušaj pristupanja istom fajlu bez obzira koji MAS klijent da je prijavio događaj.

- *Critical level* su događaji kada se u periodu od S (konfigurabilno) sekundi detektuje N +1 neuspešan pokušaj pristupanja istom fajlu bez obzira koji MAS klijent da je prijavio događaj.