Projektni zadatak 8.

Implementirati servis koji ima ulogu alata za nadzor softvera (*File Integrity Monitoring - FIM*). Servis se periodično (svakih N minuta ili sekundi) aktivira i validira digitalni potpis za unapred definisani skup fajlova. Za potpisivanje svih fajlova koristi je jedinstveni sertifikat čijem tajnom ključu pristup ima samo ovlašćena grupa korisnika.

Ukoliko FIM servis detektuje da je fajl neovlašćeno izmenjen, šalje alarm Intrusion Prevention System (IPS) komponenti – datum i vreme detekcije, naziv i lokacija fajla i nivo kritičnosti koji FIM određuje po sledećem pravilu:

- Information – ukoliko je prvi put detektovan fajl sa neovlašćenom izmenom
- Warning – ukoliko je drugi put detektovan fajl sa neovlašćenom izmenom
- Critical - ukoliko je treći put (ili veći broj puta) detektovan fajl sa neovlašćenom izmenom.

IPS sve pristigle događaje loguje u sopstveni Windows Event Log, a kada detektuje Critical događaj šalje *FileManager* komponenti zahtev za brisanjem fajla. FileManager je komponenta zadužena za upravljanje fajlovima i moguće je izvršiti sledeće operacije:

- Dodati novi fajl u sistem ili ažurirati postojeći, uključujući i ažuriranje FIM konfiguracije. Ova operacija treba da bude dozvoljena samo korisnicima koji su članovi *Management* grupe (ne i IPS komponenti) a koji imaju pravo pristupa sertifikatu za potpisivanje.
- Ispravno dodavanje fajla znači da je kreiran novi fajl, izračunat njegov digitalni potpis (koristeći sertifikat CN=FIMCert) i ažurirana FIM konfiguracija.
- Ažuriranje postojećeg fajla znači da je nakon modifikacije, ponovo izračunat njegov digitlani potpis i ažurirana FIM konfiguracija.
- Brisanje postojećeg fajla, i uklanjanje istog iz FIM konfiguracije. Ova operacija treba da bude dozvoljena samo korisnicima koji su članovi *Administration* grupe – korisnici koji pokreću IPS komponentu.

Autentifikacija između FIM i IPS komponente se vrsi putem sertifikata, dok za autentifikaciju izmedju IPS komponente i njenih klijenata koristi Windows autentifikacioni protokol.