Projektni zadatak 21.

Implementirati servis sa ulogom servera za skladištenje i upravljanje korisničkim nalozima (*CredentialsStore*). *CredentialsStore* server treba da obezbedi:

- Bazu korisničkih naloga (tip kredencijala je *username/password*), pri čemu se šifre ne smeju skladištiti u plaintext-u.
- Bazu pravila za upravljanje korisničkim nalozima (*Account Policy*). Pravilima se definiše:
    - Dozvoljeni broj neuspešnih pokušaja logovanja nakon čega se nalog zaključava.
    - Vreme nakon kojeg će zaključani nalog biti automatski otključan (nula znači da automatsko otključavanje naloga nije dozvoljeno).
    - Dozvoljeni period koji određeni nalog može biti neaktivan, nakon čega će automatski biti onemogućen.
- *CredentialsStore* pruža usluge definisane interfejsom *IAccountManagement* za administraciju podataka:
    - CreateAccount, DeleteAccount, LockAccount, EnableAccount, DisableAccount.
    - Prilikom implementacije ovih metoda voditi računa o pravilima za upravljanje politikama koje je potrebno uvažiti.
- *AuthenticationService* je komponenta za autentifikaciju korisnika u sistemu:
    - Login (...)
    - Logout(...)

Prilikom logovanja, korisnici šalju kredencijale, a *AuthenticationService* samo vodi evidenciju o ulogovanim korisnicima, dok se za validaciju kredencijala obraća *CredetialsStore* komponenti. U slučaju uspešne autentifikacije (nalog nije onemogućen, nalog nije zaključan i šifra je ispravna), *AuthenticationService* dodaje korisnika u listu ulogovanih. U slučaju neuspešne autentifikacije, potrebno je obezbediti upravljanje korisničkim nalozima u skladu sa definisanim pravilima za korisničke naloge.

CredentialsStore i *AuthenticationService* se međusobno autentifikuju preko sertifikata, a sa klijentima komuniciraju preko Windows autentifikacionog protokola.

Poruke koje se prosleđuju između CS i AS moraju biti kriptovane AES kriptografskim algoritmom u CBC modu i digitalno potpisane.

Postoje dve grupe korisnika:

1. *AccountUsers* koji komuniciraju sa *AuthenticationService* komponentom i mogu da koriste usluge *AuthenticationService* komponente. *Admins* nemaju pravo da izvršavaju ove metode.
2. *AccountAdmins* koji komuniciraju sa *CredentialsStore* servisom i koriste usluge *IAccountManagement* interfejsa. *AccountUser*s nemaju pravo da izvršavaju ove metode.