Projektni zadatak za predmet

Bezbednost u sistemima elektronskog poslovanja

verzija 1.0

20.04.2016.

U okviru projektnog zadatka iz BSEP-a potrebno je definisati i implementirati bezbednosne mehanizme u projektnom zadatku "Informacioni sistem Skupštine Grada Novog Sada" iz predmeta XML i web servisi.

1. Identifikacija učesnika

1.1 Identifikacija Skupštine Grada Novog Sada

Skupštine Grada Novog Sada (SGNS) treba da obezbedi izdavanje digitalnih sertifikata. SGNS se u tom slučaju posmatra kao najviše sertifikaciono telo (root CA) i ona objavljuje svoj samopotpisan (selfsigned) digitalni sertifikat u X.509v3 formatu. Ovaj root CA izdaje sertifikat za subordinate CA koji takođe pripada SGNS. Subordinate CA se kasnije koristi za izdavanje sertifikata svim potrebnim učesnicma u sistemu.

1.2. Identifikacija odbornika

Svaki odbornik dobija svoj digitalni sertifikat u X.509v3 formatu od strane subordinate CA SGNS.

1.3. Identifikacija Istorijskog arhiva Grada Novog Sada

Istorijski arhiv Grada Novog Sada (IAGNS) dobija svoj digitalni sertifikat u X.509v3 formatu od strane subordinate CA SGNS.

1.4. Generisanje sertifikata

Za registraciju učesnika i izdavanje sertifikata realizovati aplikaciju na Java platformi sa grafičkim korisničkim interfejsom koji koristi Swing biblioteku (ili neki drugi programski jezik i odgovarajuće GUI biblioteke).

2. Model pretnji

Potrebno je napraviti model pretnji sistema što uključuje sve od baze podataka do klijentske aplikacije. U sklopu modeliranja pretnji nije neophodno formirati abuse case dijagrame, ali treba napraviti data flow dijagrame, kao i sve propratne tabele. Za sistem kategorizacije pretnji koristiti STRIDE.

3. Bezbednost komunikacije

3.1. Browser-server

Sva komunikacija između web čitača i back end aplikacije treba da bude osigurana upotrebom HTTPS protokola.

3.2. Potpisivanje i šifrovanje poruka

Digitalno potpisivanje XML poruka

Svi učesnici kada formiraju XML poruku koja predstavlja odgovarajući dokument koji se koristi u sistemu (predlog akta, amadmana, finalni akti i sl.) moraju taj dokumenti i potpisati. Digitalni potpis se

formira prema XML Signature standardu i mora biti sastavni deo poruke, smešten kao dete korenskog elementa poruke (Enveloped stil).

Enkripcija
U komunikacija SGNS i IAGNS potrebno je obezbediti i poverljivost poruka. Poverljivost poruka se obezbeđuje tako što se poruke šifruju simetričnim algoritmom i jednokratnim simetričnim ključem. Jednokratni simetrični ključ se šifruje asimetričnim algoritmom i javnim ključem primaoca poruke. Za formiranje šifrata i podataka o korišćenom jednokratnom simetričnom ključu koristi se XML Encryption standard. U svim slučajevima šifruje se sadržaj korenskog elementa poruke.

CRL

Autentifikacija učesnika u komunikaciji obuhvata i proveru da li se sertifikat nalazi u listi povučenih sertifikata (CRL). SGNS kao CA održava svoju listu povučenih sertifikata. CRL liste se čuvaju u X509 formatu (standardan način) ili u obliku namenski formiranog XML dokumenta potpisanog od strane nadležnog CA.

Replay napad
Svaka poruka treba da sadrži timestamp i redni broj poruke kako bi se sprečio replay napad.

4. Bezbednost aplikacija

4.1. Bezbednosnih mehanizmi

Implementirati sigurne bezbednosne mehanizme i ispoštovati najbolje prakse koje su pređene na vežbama. Ovo uključuje validaciju korisničkog unosa, enkodiranje serverskog odgovora, upotrebu centralizovanog sistema za autentifikaciju, autorizaciju, loging, itd.

4.2. Zaštita od poznatih propusta

Sistem treba da bude osiguran protiv svih propusta koji su odrađeni na vežbama, od nepravilnog rukovanja greškama do injection napada. Iako su određeni propusti manje relevantni za naveden sistem, prilikom odbrane tim treba da pokaže šta je uradio da se osigura da njihov sistem nije podložan određenim eksploatacijama.

5. Kontrola pristupa

5.1. RBAC

Kontrola pristupa treba da je bazirana na RBAC standardu. Potrebno je definisati korisničke uloge u sistemu, objekte, operacije i privilegije. Korisničke uloge se mogu definisati na osnovu različitih učesnika navedenih u projektnom zadatku iz XWS-a: *građanin*, *odbornik* i *predsednik skupštine.*
Kontrola pristupa treba da bude implementirana kako na serveru, tako i na klijentu.

5.2. Lozinke

Lozinke treba čuvati upotrebom hash & salt metoda.

6. Korišćeni algoritmi i formati

6.1. Simetrično šifrovanje

Za simetrično šifrovanje koristi se AES, sa dužinom ključa od 128 bita.

6.2. Heš funkcije

Kao heš funkcija koristi se SHA-1.

6.3. Asimetrično šifrovanje

Za asimetrično šifrovanje koristi se RSA algoritam sa dužinom ključa od 1024 bita.

6.4. Digitalno potpisivanje

Za digitalno potpisivanje koristi se RSA algoritam (ključ dužine 1024 bita) i SHA-1 heš funkcija.

6.5. Digitalni sertifikati

Digitalni sertifikati se formiraju prema X.509v3 standardu.

7. Test scenario

Test slučajevi treba da pokriju situacije kada je razmena poruka uspešna i kada je razmena poruka neuspešna (npr. neispravan potpis, povučen sertifikat, istekao sertifikat, timestamp/redni broj ponovljen, poruka nije potpisana/šifrovana).