Sigurnost sustava FER e-račun

Luka Humski*, Zoran Skočir * i Boris Vrdoljak**
* Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva/Zavod za osnove elektrotehnike i električka mjerenja, Zagreb, Hrvatska
** Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva/Zavod za primijenjeno računarstvo, Zagreb, Hrvatska
{luka.humski, zoran.skocir, boris.vrdoljak}@fer.hr

Sažetak - U današnje vrijeme sve je važnije poslovne procese čim više automatizirati što se obavlja elektroničkim poslovanjem. Vrlo važan poslovni proces razmjena je elektroničkih računa (e-računa). Na FER-u je razvijen sustav za razmjenu elektroničkih računa *FER e-račun*. Sigurnost informacijskih sustava općenito pa tako i sigurnost sustava *FER e-račun* vrlo je važna. U ovom je članku opisano kako je u sustavu *FER e-račun* implementirana sigurnost. Ona je u ovom sustavu implementirana u pet osnovnih koraka: za pristup korisnika bilo kojoj od aplikacija od kojih se sustav sastoji potrebno je proći proces autentifikacije i autorizacije; sav korisnički unos provjerava se s ciljem zaštite od unosa zlonamjernog koda; veza između klijentskih računala i poslužitelja informacijskih posrednika provodi se korištenjem sigurnosne nadgradnje protokola HTTP, protokolom HTTPS koji koristi sigurnosni protokol SSL/TLS; komunikacija između informacijskih posrednika odvija se korištenjem *web*-usluga čija je sigurnost osigurana sigurnosnim proširenjem *WS-Security*; računi koji se kroz sustav razmjenjuju digitalno se potpisuju korištenjem FINA-ine pametne kartice.

I. UVOD

Elektroničko poslovanje (e-poslovanje) oblik je organizacije poslovanja koji obuhvaća poslovne transakcije i razmjenu informacija što se izvode uporabom informacijske i komunikacijske tehnologije u poduzeću, između poduzeća i njihovih kupaca ili između poduzeća i javne administracije [1]. Osnovna karika elektroničkog poslovanja dobavni je lanac, a osnovni poslovni procesi koje uključuje jesu: katalog, natjecanje, ugovor, narudžba, vremensko terminiranje isporuke, izdavanje računa, plaćanje te obavještavanje o plaćanju. Kako bi navedeni dobavni lanac te cjelokupni proces e-poslovanja bili ostvarivi, potrebno je ostvariti određene elektroničke isprave i postupke poput e-kataloga, e-narudžbenice, e-računa, registra korisnika e-računa, e-plaćanja, e-potpisa, e-identiteta te semantičke i tehničke interoperabilnosti. Cilj je elektroničkog poslovanja automatizirati (nužno i digitalizirati) poslovne procese u najvećoj mogućoj mjeri. Primjerice, u svijetu u kojem se ne koriste elektroničke isprave kupac bi napisao papirnatu narudžbu te je poštom, faksom ili elektroničkom poštom poslao prodavatelju. Prodavatelj bi ručno analizirao narudžbu te bi je, ako može isporučiti proizvode ili izvršiti usluge iz narudžbe, odobrio. Potom bi elemente iz narudžbe ručno prepisao na račun te bi istim medijem kojim je primio narudžbu izdao i račun. U svijetu koji koristi elektroničko poslovanje taj bi se isti postupak izveo slanjem računalno čitljive narudžbe (uobičajeno u formatu XML). Iz te narudžbe, nakon što je prodavatelj odobri, bilo bi moguće preuzeti elemente koje i račun sadrži te automatski (bez prepisivanja) generirati račun. Na opisani se način štedi vrijeme, papir (ekološka osviještenost), uklanja mogućnost pogrješaka pri prepisivanju što na koncu zajedno rezultira financijskim uštedama (prema [2], samo bi se u Hrvatskoj uštedjelo 6 milijardi kuna godišnje, od čega oko 350 milijuna kuna samo u državnoj upravi).

U današnje vrijeme elektroničko poslovanje sve više uzima maha. Mnogi procesi koji su se ranije vodili ručno danas se digitaliziraju i automatiziraju. U tom se procesu osim problema vezanih za funkcionalnost sustava javljaju i problemi vezani za sigurnosti sustava. Novi način organizacije poslovanja traži i provođenje novih sigurnosnih mjera. Bitno je omogućiti povjerljivu komunikaciju što se ostvaruje šifriranjem komunikacije, ali također i osigurati nadomjestak za vlastoručni potpis i pečat u papirnatom poslovanju. U tu je svrhu osmišljen digitalni potpis, tj. postupak kojim se dokumentu dodaje dodatak šifriran korištenjem podataka dostupnih samo osobi koja dokument potpisuje. Takav dodatak u potpunosti zamjenjuje vlastoručni potpis i pečat jer kao i spomenuti ima svojstvo da pripada samo jednoj osobi.

Ostatak članka organiziran je na sljedeći način: u poglavlju II opisan je sustav za razmjenu e-računa *FER e-račun*; u poglavlju III definirana je sigurnost mreža, usluga i aplikacija, pobrojani su osnovni sigurnosni zahtjevi te su opisane najvažnije sigurnosne norme za sustav *FER e-račun*; u poglavlju IV objašnjeno je kako je korištenjem ranije opisanih normi implementirana sigurnost u sustav *FER e-račun*; u poglavlju V ukratko je prikazana implementacija sigurnosti u sličnim sustavima; u poglavlju VI iznesene su smjernice za budući rad, a u poglavlju VII dan je zaključak.

II. OPIS SUSTAVA *FER E-RAČUN*

Na Fakultetu elektrotehnike i računarstva Sveučilišta u Zagrebu (FER) razvijen je pilotski sustav za razmjenu elektroničkih računa. Razmjena e-računa podrazumijeva oblikovanje, slanje, primanje, pohranjivanje i pretraživanje e-računa. Kao potpora sustavu za razmjenu e-računa razvijen je i prijedlog sustava registra korisnika e-računa. Korisnici koriste sustav kroz dvije osnovne pripremljene aplikacije: aplikaciju za razmjenu e-računa, sastavljenu od aplikacije za slanje e-računa i aplikacije za pristup arhivi e-računa, te aplikaciju za pristup registru

korisnika e-računa. Za registraciju novih korisnika koristi se posebna aplikacija (obrazac).

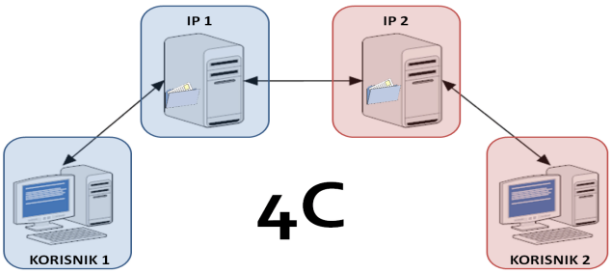
A. Arhitektura sustava

Arhitektura sustava *FER e-račun* temelji se na modelu 4 *corner* (4C – četiri kuta). Kao što i samo ime sugerira, sustav ima 4 osnovne komponente: korisnika pošiljatelja računa, informacijskog posrednika pošiljatelja, informacijskog posrednika primatelja te korisnika primatelja računa. Slika 1 prikazuje skicu modela 4C (korisnik 1 i 2 – primatelji/pošiljatelj računa, IP – informacijski posrednik).

Računi se šalju na način da korisnik-pošiljatelj oblikuje (ručno ili kroz aplikaciju) e-račun te ga proslijedi svom informacijskom posredniku. Informacijski posrednik pošiljatelja taj račun prosljeđuje informacijskom posredniku primatelja. Primatelj računa dobiva račune od svog informacijskog posrednika.

Podatke o korisnicima potrebno je negdje pohraniti zbog čega na svakom informacijskom posredniku postoji registar korisnika e-računa u kojem se pohranjuju svi važni podatci vezani za korisnike, klijente određenog informacijskog posrednika.

Bitna značajka ovakve arhitekture sustava jest činjenica da je središnji dio sustava potpuno decentraliziran. Središnji dio sustava sastoji se od skupa (moguće beskonačno mnogo) informacijskih posrednika. Međutim, što je veći broj informacijskih posrednika, teže je znati kojem informacijskom posredniku poslati račun kako bi on stigao do primatelja. Zbog toga je u sustav uveden središnji registar korisnika e-računa u kojem se pohranjuju osnovni podatci potrebni za usmjeravanje e-računa. Nakon što korisnik pošiljatelj računa preda račun koji želi poslati svom informacijskom posredniku, informacijski će posrednik iz računa dohvatiti OIB primatelja računa te od središnjeg registra zatražiti informaciju o tome kojem informacijskom posredniku treba proslijediti račun kako bi on stigao do primatelja. Skicu razvijenog sustava za razmjenu elektroničkih računa prikazuje Slika 2. Na slici su naznačene sastavnice sustava te *web*-usluge kojima te sastavnice komuniciraju.



Slika 1. Skica modela 4C

Sustav *FER e-račun* sastoji se od:

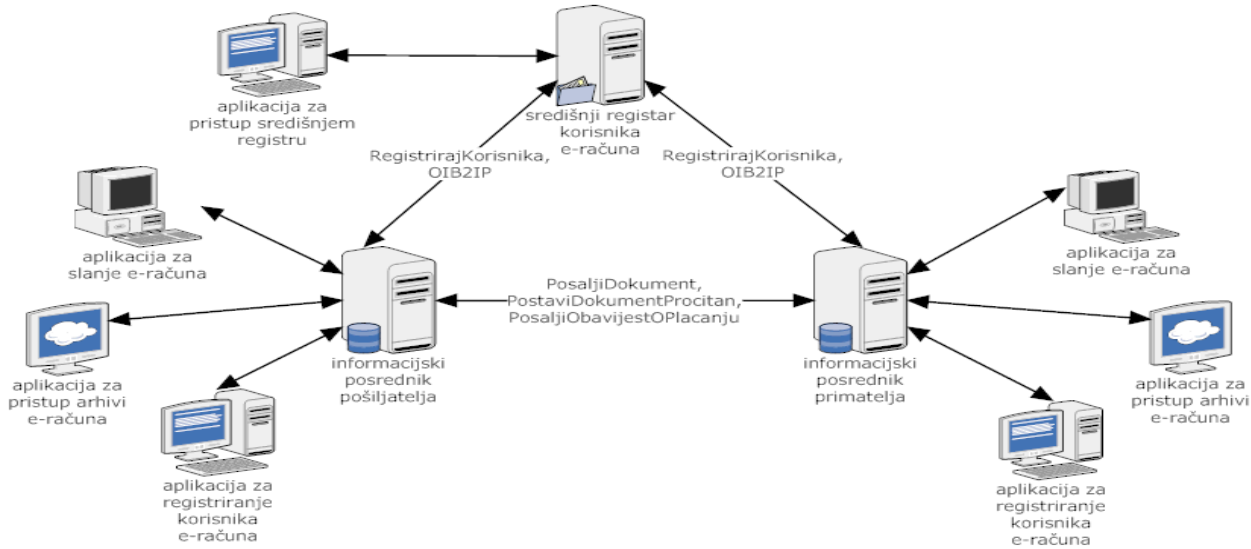
1. aplikacija koje omogućuju oblikovanje i slanje e-računa, pregledavanje arhive primljenih i poslanih e-računa te registriranje novih korisnika i pregledavanje podataka o postojećim korisnicima
2. informacijskih posrednika (s lokalnim registrima korisnika e-računa) koji omogućuju razmjenu oblikovanih računa
3. središnjeg registra korisnika e-računa
4. *web*-usluga korištenjem kojih se e-računi razmjenjuju.

III. PREGLED KORIŠTENIH SIGURNOSNIH NORMI

Nakon što je u prethodnom poglavlju opisan sustav *FER e-račun*, u ovom će poglavlju biti objašnjeno što je to sigurnost mreža, usluga i aplikacija te će biti opisane za taj sustav najvažnije sigurnosne norme, a sve s ciljem da se u sljedećem poglavlju objasni kako je korištenjem tih normi implementirana sigurnost u sustavu *FER e-račun*.

Sigurnost mreža, usluga i aplikacija može se promatrati kao sposobnost mreže i informacijskog sustava da se suprotstavi neočekivanim slučajnim događajima i neprijateljski usmjerenim akcijama [1]. Prema [1] osnovni sigurnosni zahtjevi svrstani su u sljedeće osnovne skupine:

1. **autentifikacija** – potvrda identiteta korisnika
2. **cjelovitost (integritet)** – jamstvo da su informacije poslane, primljene ili pohranjene u izvornom i nepromijenjenom obliku
3. **povjerljivost** – zaštita komunikacije ili pohranjenih podataka od presretanja i stavljanja na uvid neovlaštenim osobama



Slika 2. Skica sustava FER e-račun

4. **neporecivost** – sudionici ne mogu odbiti ili poreći akciju u kojoj su sudjelovali

5. **kontrola pristupa** – ograničenje pristupa informacijama i ograničenje provođenja akcija

6. **raspoloživost** – informacije moraju biti raspoložive, a sustavi i usluge u operativnom stanju, usprkos mogućim neočekivanim i nepredvidljivim događajima.

U nastavku ovog poglavlja dan je pregled sigurnosnih normi koje se u sustavu *FER e-račun* koriste za implementaciju sigurnosti, a u poglavlju IV objašnjeno je kako je korištenjem tih normi sigurnost sustava u konačnici i implementirana.

A. SSL/TLS

Protokol TLS (*Transport Layer Security*) [3] i SSL (*Secure Sockets Layer*) [4] kriptografski su protokoli koji osiguravaju sigurnu komunikaciju kroz nesigurnu komunikacijsku mrežu. Radi se o implementaciji sigurnosti povrh transportnog sloja komunikacijske mreže (internetski model komunikacijske mreže poznatiji i kao model TCP/IP opisan je u [5]). Za kriptiranje podataka koristi se simetrična kriptografija. Osnovna razlika između spomenuta dva protokola jest u tome što je SSL vlasnički protokol, dok je TLS otvoreni protokol.

Protokol TLS omogućuje aplikacijama zasnovanim na arhitekturi klijent – poslužitelj komuniciranje kroz mrežu na način da se onemogući prisluškivanje.

Prije no što se uspostavi sigurna veza koja čuva stanje komunikacije, klijent i poslužitelj pregovaraju o parametrima veze. Proces uspostave sigurne veze sljedeći je:

1. Postupak uspostavljanja sigurne veze započinje spajanjem klijenta na poslužitelj koji podržava protokol TLS i zahtjevom za uspostavom sigurne veze. Pri tome klijent poslužitelju predočava listu podržanih algoritama za šifriranje i računanje *hash*-koda.
2. Iz ponuđene liste algoritama poslužitelj odabire najjači algoritam šifriranja i računanja *hash*-koda koji ujedno i on podržava.
3. Poslužitelj se identificira prema klijentu slanjem svog digitalnog certifikata.
4. Klijent može kontaktirati izdavatelja digitalnog certifikata i provjeriti mu ispravnost.
5. Kako bi stvorio sjedničke (engl. *session*) ključeve koji se koriste za sigurnu komunikaciju, klijent šifrira slučajno odabrani broj s javnim ključem poslužitelja te ga šalje poslužitelju.
6. Iz slučajno odabranog broja koji je klijent poslao poslužitelju obje strane (klijent i poslužitelj) generiraju podatke potrebne za šifriranje i dešifriranje.

B. XML Signature

Današnje elektroničko poslovanje uglavnom se temelji na razmjeni XML-dokumenata. Zbog toga su razvijene posebne norme za sigurnost XML-dokumenata, tj. sigurnosne norme ugrađene u XML. Dakako, sigurnost XML-dokumenata može biti implementirana i korištenjem standardnih sigurnosnih protokola, ali u tom je slučaju problem što ti algoritmi koriste binarne datoteke koje onda mogu biti interpretirane samo korištenjem posebnih alata. U slučaju posebnih normi za sigurnost XML-a, sigurnosne mjere dodaju se dokumentu bez kršenja pravila XML-a. Takvi se dokumenti tada mogu pregledavati korištenjem standardnih alata za XML. Također, valja biti svjestan i razlike između implementiranja sigurnosti na razini dokumenta i na razini komunikacijske mreže. Primjerice, protokolima SSL i TLS moguće je osigurati povjerljivost prijenosa informacije kroz komunikacijsku mrežu. To znači da je dokument zaštićen samo dok putuje kroz mrežu. Povjerljivost dokumenta na računalu pošiljatelja kao ni povjerljivost dokumenta na računalu primatelja nije osigurana. Implementiranje sigurnosti na razini dokumenta osigurava povjerljivost dokumenta i nakon što stigne na odredište.

XML Signature [6] jest norma za digitalno potpisivanje korištenjem XML-a. Jednim potpisom moguće je potpisati više dokumenata. Dokumenti koji se potpisuju ne trebaju nužno biti u formatu XML, a onda kada jesu nije nužno potpisati cijeli XML-dokument. Moguće je potpisati samo dio XML-dokumenta. Na taj se način omogućuje da različite dijelove jednog XML-dokumenta potpisuju različiti ljudi. Norma *XML Signature* definira način na koji se digitalni potpis i informacije o njemu pohranjuju tako da su zadovoljena pravila XML-a. Standardom se ne definira algoritam za digitalno potpisivanje, ali se definira kako ugraditi digitalni potpis u XML.

XML-potpis može se pojaviti u tri različita osnova oblika:

1. **Omotani potpis** – potpis se nalazi unutar dokumenta koji se potpisuje
2. **Omotavajući potpis** – potpis omata dokument koji se potpisuje
3. **Odvojeni potpis** – potpis se nalazi u odvojenom dokumentu (dokument koji se potpisuje identificira se URI-jem).

XML-potpis ne mora nužno uvijek biti u osnovnom obliku. Moguće su različite kombinacije osnovna tri oblika, tj. hibridni oblik. Slika 3 prikazuje primjer omotanog potpisa u koji je dodana referenca na vanjski dokument koji se potpisuje. U ovom se slučaju jednim potpisom potpisuje dokument unutar kojeg je potpis (tamnije na slici) te dokument identificiran URI-jem (svjetlije na slici).

C. WS-Security

Norma za sigurnosno proširenje *web*-usluga *WS-Security* [7] zasnovana je na već postojećim tehnologijama kao što su to, primjerice, *XML-Signature* i *XML-Encryption* koje rješavaju problem šifriranja i digitalnog potpisivanja XML-poruka. Autentifikacija se rješava protokolima X.509 i Kerberos. *XML Canonicalization* [8] opisuje način pripreme XML-sadržaja za šifriranje i digitalno potpisivanje. Norma *WS-Security* postojećim specifikacijama dodaje mogućnost ugradnje spomenutih mehanizama u SOAP-poruke. Bitno je napomenuti da je sigurnost SOAP-poruka posve neovisna o sigurnosti transportnog sloja.

WS-Security definira element SOAP-zaglavlja koji nosi podatke vezane za sigurnost pri čemu format digitalnog potpisa ili format šifriranja nisu definirani.

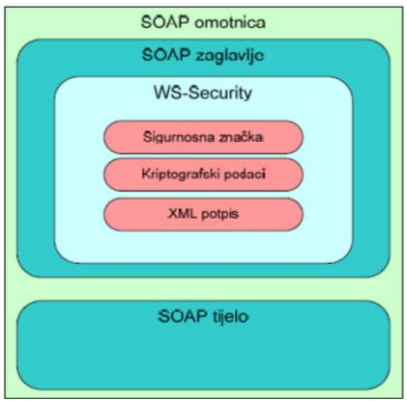
```
<Igrac xmlns="http://www.hou.hr/">
  <Ime>Antea</Ime>
  <Prezime>Tadic</Prezime>
  <Pozicija>Tehnicar</Pozicija>
  <Signature xmlns='http://www.w3.org/2000/09/xmldsig#'>
    <SignedInfo>
      <CanonicalizationMethod Algorithm=
        "http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm=
        "http://www.w3.org/2000/07/xmldsig#rsa-sha1" />
      <Reference URI=""> ovaj dokument
        <Transforms Algorithm=
          "http://www.w3.org/TR/2000/WD-xml-c14n-20000710" />
        <DigestMethod Algorithm=
          "http://www.w3.org/2000/07/xmldsig#sha1" />
        <DigestValue>
          jkhKJHHIhkklADKHj=dsfs34'FDE'?sdsa
        </DigestValue>
      </Reference>
      <Reference URI=
        "http://www.abccompany.com/news/2000/03 27 00.htm">
        <DigestMethod Algorithm=
          "http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
      </Reference> neki drugi dokument identificiran URI-jem
    </SignedInfo>
    <SignatureValue>DFSLK89sdf?sdasHK</SignatureValue>
    <KeyInfo>...</KeyInfo>
    <Object>...</Object>
  </Signature>
</Igrac>
```

Slika 3. Primjer hibridnog oblika XML-ovskog digitalnog potpisa

Specificira se kako se format, opisan nekom drugom specifikacijom, može ugraditi u SOAP-poruku. Slika 4 prikazuje na koji se način podatci vezani za sigurnost ugrađuju u SOAP-poruku.

IV. IMPLEMENTACIJA SIGURNOSTI U SUSTAVU *FER E-RAČUN*

U sustavu *FER e-račun* sigurnost je implementirana na način da je osigurana autentifikacija i autorizacija korisnika, podatci dobiveni od korisnika provjeravaju se radi zaštite od SQL-upada (engl. *SQL Injection*) i XSS-napada (engl. *Cross-Site Scripting*), aplikacijama koje su uključene u sustav pristupa se preko sigurnog protokola HTTP (HTTPS) korištenjem protokola SSL/TLS, a komunikacija između informacijskih posrednika odvija se korištenjem sigurnih *web*-usluga (*WS-Security*). Sustav omogućuje i digitalno potpisivanje izdanih računa, tj. cijelih XML-datoteka koje se kroz sustav *FER e-račun* razmjenjuju, a koje između ostalog sadrže i e-račun. XML-datoteke koje sadrže e-račune ne



Slika 4. Struktura sigurnosnih informacija u SOAP-poruci prema normi WS-Security [9]

šifriraju se prije arhiviranja jer se smatra da je njihovo pohranjivanje u bazu podataka kojoj se ne može pristupiti bez odgovarajućih korisničkih podataka dovoljna zaštita. Na taj način sustav ispunjava sljedeće sigurnosne zahtjeve: povjerljivost, cjelovitost, autentifikacija, neporecivost i kontrola pristupa. Zahtjev za raspoloživošću sustava nije razmatran, a njegova implementacija u značajnoj mjeri uvjetovana je i brojem korisnika realnog sustava koji će onda definirati potrebne performanse sustava. U svrhu bolje raspoloživosti, u sustavu treba implementirati redundantne ključne točke i usluge sustava.

U nastavku će po stavkama detaljnije biti opisano kako je implementirana sigurnost.

A. *Sigurnost aplikacija*

1) *Autentifikacija i autorizacija korisnika*

U postupku registracije u sustav korisniku se dodjeljuju podatci za pristup aplikacijama. Dodijeljeni pristupni podatci pohranjuju se u lokalnom registru korisnika e-računa koji održava svaki informacijski posrednik za sebe. Autentifikacija i autorizacija korisnika obavlja se korištenjem korisničkog imena i lozinke. Na taj se način određuje o kojem se korisniku radi te koje su njegove ovlasti u aplikaciji.

U bazi podataka bilježi se točno korisničko ime te *hash*-kod (SHA1 [10]) lozinke. Na taj se način osigurava njezina tajnost. Pri autentificiranju korisnika u bazi podataka traži se zapis koji sadrži uneseno korisničko ime. Za unesenu lozinku računa se njezin *hash*-kod i uspoređuje s onim koji je pohranjen u bazi podataka. Pronađe li se u bazi podataka korisnik s unesenim korisničkim imenom i odgovarajućim *hash*-kodom lozinke, autentifikacija je uspješno provedena, provjeravaju se ovlasti korisnika te se korisniku omogućuje korištenje sustava.

Tajnost lozinke temelji se na činjenici da iz *hash*-koda lozinke nije moguće rekonstruirati samu lozinku.

2) *Provjera ulaznih podataka, SQL-upadi i Cross-Site Scripting (XSS)*

Provjera ulaznih podataka temelj je sigurnosti *web*-aplikacija. Svaki podatak koji je dobiven od strane korisnika prije no što uđe u sustav mora biti provjeren na način da se eliminira mogućnost da se radi o zlonamjernom programskom kodu. Korisnik sustavu *FER e-račun* predaje podatke na način da ih unosi u odgovarajuća polja u HTML-obrascima ili ih prenosi kao parametre u upitnom dijelu URI-ja.

a) *SQL-upadi*

SQL-upadi [11] jesu način napada u kojem napadač unošenjem odgovarajućih podataka – SQL-koda umjesto traženih podataka (bilo kroz HTML-obrasce, bilo kroz parametre URI-ja) mijenja početni SQL-upit na način da dobije upit kakav on želi (naime, podatci dobiveni od korisnika uobičajeno se ugrađuju u SQL-upit). Za zaštitu od SQL-upada valja provjeriti sadrži li korisnički unos SQL-kod. Vrlo učinkovito rješenje jest i onemogućavanje istodobnog slanja više od jednog upita bazi podataka. Naime, SQL-upad često se izvodi na način da se na korisni SQL-upit zalijepi još jedan (zlonamjerni) upit.

Recimo, na SELECT-upit zalijepi se upit DELETE i obrišu se podatci iz baze podataka.

b) Cross-Site Scripting (XSS)

XSS-napadi [12] jesu napadi u kojima zlonamjerni korisnici umjesto regularnih podataka unose programski kod. Ovakvi napadi na *web*-aplikacije opasni su kada, primjerice, zlonamjerni korisnik unese zlonamjerni JavaScript-kod. Ako se unos ne provjerava, takav se zlonamjerni kod pohranjuje u bazu podataka i izvršava na računalu onih korisnika kojima se prikazuju podatci uneseni u bazu podataka. Na njihovim će se računalima izvršiti zlonamjerni kod umjesto da se prikažu podatci. Primjer takvog zlonamjernog koda može biti skripta koja napadaču šalje korisnička imena i lozinke pohranjena u korisničkom internetskom pregledniku.

Zaštita od ovakvih napada u funkcijama je koje programski kod pretvaraju u običan tekst. Primjerice, takve će funkcije znak „<“ pretvoriti u „&lt“. Naime, znak „<“ u HTML-u tretira se kao dio programskog koda, a za zapis „&lt“ na zaslonu će se ispisati znak „<“.

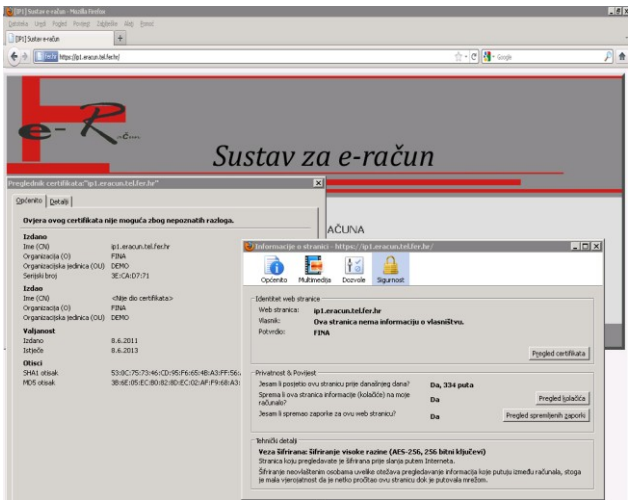
c) Zaštita skripti i konfiguracijskih datoteka od neovlaštenog pregledavanja i pokretanja

Datoteke unutar *web*-sjedišta bitno je organizirati tako da su javno dostupne (imaju globalni URL) samo one datoteke koje su za to pripremljene. Skripte koje se pišu da bi se na nekom mjestu uključile (engl. *include*) u postojeći kod, a same za sebe ne smiju se izvršiti valja smjestiti u posebne poslužiteljske mape koje nisu „izvana“ dostupne. Isto vrijedi i za konfiguracijske datoteke. Konfiguracijske datoteke ili ne smiju imati globalni URL ili treba biti osigurano da se uz poznavanje njihova URL-a ne može dohvatiti njihov sadržaj. Primjerice, ako se radi o jeziku PHP, na kraj naziva konfiguracijske datoteke može se staviti nastavak PHP. Na taj će način biti osigurano da će korisnik koji će pokušati dohvatiti konfiguracijsku datoteku vidjeti rezultat izvršavanja koda konfiguracijske datoteke (uglavnom bijeli ekran – konfiguracijske datoteke uglavnom su niz naredbi kojima se u određene varijable pohranjuju određene vrijednosti), a ne sam kod što mogu, primjerice, biti (tajni) pristupni podatci za bazu podataka.

B. *Pristup aplikacijama korištenjem HTTPS-a*

Aplikacijama sustava sigurno se pristupa korištenjem HTTPS-a [13], sigurnosne nadogradnje protokola HTTP. HTTPS koristi protokol SSL/TLS za šifriranje prometa povrh transportnog sloja. Informacije koje se korištenjem aplikacije razmjenjuju između klijenta i poslužitelja šifrirane su.

Za uspostavu sigurne sjednice koriste se demo poslužiteljski certifikati dobiveni od FINA-e. Certifikatima se također korisnicima jamči i da je sustav (*web*-aplikacija na koju se spajaju) onaj za kojeg se predstavlja. Slika 5 prikazuje pristup *web*-aplikacijama jednog od informacijskih posrednika uključenih u sustav *FER e-račun* preko HTTPS-a. Budući da se radi u demo-certifikatu, u certifikatu se ne nalaze točni podatci o sustavu *FER e-račun*, ali tehnički gledano demo-certifikat jednak je pravom certifikatu.



Slika 5. Pristup *web*-aplikaciji jednog od informacijskih posrednika preko HTTPS-a

C. *Sigurne web-usluge*

Sigurnost *web*-usluga osigurana je implementiranjem standarda *WS-Security*. Koriste se mehanizmi za autentifikaciju korisnika i šifriranje poruka.

Autentifikacija se obavlja uključivanjem korisničkog imena i lozinke u zaglavlje SOAP-zahtjeva. *Web*-usluge moguće je koristiti tek nakon uspješno provedenog procesa autentifikacije.

Poruke se šifriraju korištenjem asimetričnog kriptografskog algoritma DES [14].

D. *Digitalno potpisivanje*

Oblikovani sustav omogućuje digitalno potpisivanje datoteka koje se kroz njega razmjenjuju. Digitalni potpis pohranjuje se unutar posebnog elementa XML-datoteke koja se kroz sustav šalje. Za pohranjivanje digitalnog potpisa koristi se standard *XML Signature*. Digitalno potpisivanje e-računa nije obavezno, ali je omogućeno korisnicima koji žele jamčiti: autentičnost, cjelovitost i neporecivost u procesu razmjene e-računa.

Nakon što korisnik kroz aplikaciju popuni sve potrebne podatke i na taj način oblikuje novi račun ili preda gotov račun u formatu XML, taj se e-račun zajedno s možebitnim prilogom ugrađuje u XML-datoteku koja se šalje. Takvu datoteku korisnik može potpisati korištenjem korisničkog digitalnog certifikata koji je izdala FINA (jedini hrvatski CA – certifikacijsko tijelo, engl. *Certification Authority*). Digitalni certifikat pohranjen je na pametnoj kartici. Zahtjev za potpisivanjem šalje se pametnoj kartici iz JavaScripta korištenjem funkcija gotovog programskog međusloja koji je izradila FINA. Kao odgovor dobiva se digitalni potpis dokumenta koji se tada ugrađuje u spomenutu XML-datoteku.

Slika 6 prikazuje dio XML-datoteke koja se kroz sustav razmjenjuje, a prikazuje strukturu opisanog digitalnog potpisa dokumenta.

Slika 6. Dio XML-datoteke e-računa koji sadrži digitalni potpis

V. SIGURNOST U SLIČNIM SUSTAVIMA

U svrhu što bolje implementacije sigurnosti u sustav *FER e-račun* proučeni su još neki domaći i strani sustavi za razmjenu e-računa. U nastavku će biti objašnjeno kako je sigurnost implementirana u projektu Europske unije za elektroničku nabavu nazvanom e-Prior [15].

U projektu e-Prior za prenošenje poruka koristi se mreža PEPPOL. Sigurnost *web*-usluga u sustavu PEPPOL implementirana je korištenjem standarda *WS-Security*, *WS-Reliability*, *WS-Addressing* te *WS-Transfer*. Za prenošenje sigurnosnih informacija kroz mrežu koristi se protokol SAML 2.0. U sustavu e-Prior sigurnost se temelji na definiranim sigurnosnim procedurama te nadzoru (sva interakcija između korisnika i sustava bilježi se u *log*-datotekama). Sigurnost je implementirana na transportnom i aplikacijskom sloju te na razini poruke. Za zaštitu sigurnosti na transportnom sloju koristi se protokol SSL. Zaštita sigurnosti na aplikacijskom sloju implementirana je kroz pridjeljivanje korisničkih profila korisnicima. Na taj se način definiraju ovlasti pojedinog korisnika nad sustavom. Autentifikacija korisnika ostvarena je korištenjem običnih lozinki umjesto korištenjem klijentskih certifikata.

VI. BUDUĆI RAD

U budućem radu razmotrit će se implementacija normi *WS-Reliability*, *WS-Addressing* te *WS-Transfer* po uzoru na projekt PEPPOL, a sve s ciljem povećanja razine sigurnosti *web*-usluga. Također, po uzoru na projekt e-Prior valja omogućiti bilježenje informacija o svoj komunikaciji između korisnika i sustava u *log*-datoteke.

Kada bi se sustav *FER e-račun* počeo koristiti u praksi, bilo bi potrebno pomno analizirati raspoloživost sustava što do sada zbog nedostupnosti dovoljno kvalitetne računalne opreme nije učinjeno.

Spomenuto je da se za digitalno potpisivanje računa pametnim karticama koristi FINA-in programski međusloj za pristup pametnoj kartici. Programski međusloj koji se trenutno koristi radi isključivo u internetskom pregledniku Internet Explorer te samo na 32-bitnim računalima. Potrebno je kroz suradnju s FINA-om nabaviti noviju i fleksibilniju inačicu spomenutog međusloja ili izvesti vlastiti međusloj za pristup FINA-inoj pametnoj kartici.

U budućem radu razmotrit će se moguće ranjivosti sustava koje u dosadašnjem radu nisu uočene i razmatrane. Bitno je imati u vidu činjenicu da je sigurnost mjera, a ne karakteristika. Sigurnost sustava treba kontinuirano preispitivati i unaprjeđivati.

VII. ZAKLJUČAK

U članku je ukratko predstavljen sustav za razmjenu elektroničkih računa *FER e-račun*. Predstavljene su i opisane za sustav važne sigurnosne norme. Objašnjeno je kako je korištenjem tih normi implementirana sigurnost u sustavu *FER e-račun*. Na koncu je na primjeru europskog projekta e-Prior prikazano kako je problem sigurnosti riješen u tim sustavima te su dane smjernice za daljnji razvoj sustava *FER e-račun*a u domeni sigurnosti sustava.

LITERATURA

[1] A. Bažant , Ž. Car, G. Gledec, D. Jevtić, G. Ježić, M. Kunštić, I. Lovrek, M. Matijašević, B. Mikac, Z. Skočir, *Telekomunikacije – tehnologija i tržište*, Element, prvo izdanje, Zagreb, 2007.

[2] M. Bačelić, *E-račun: Država i dalje gubi jer ne mijenja Pravilnik o PDV-u,* Časopis Lider, Zagreb, 28. siječnja 2011.

[3] *RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2*, http://tools.ietf.org/html/rfc5246, 20. 1. 2012.

[4] *RFC 6101 – The Secure Sockets Layer (SSL) Protocol Version 3.0*, http://tools.ietf.org/html/rfc6101, 20. 1. 2012.

[5] A. Bažant, G. Gledec, Ž. Ilić, G. Ježić, M. Kos, M. Kunštić, I. Lovrek, M. Matijašević, B. Mikac, V. Sinković, *Osnovne arhitekture mreža*, Element, prvo izdanje, Zagreb, 2003.

[6] *XML Signature Syntax and Processing*, http://www.w3.org/TR/xmldsig-core/, 25. 4. 2011.

[7] *OASIS Web Services Security (WSS) TC|OASIS,* http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss, 23. 1. 2012.

[8] *Canonical XML*, http://www.w3.org/TR/xml-c14n, 23. 1. 2012.

[9] Mornar, V., Kalpić, D., Smokvina, R., Kovač, M., Hadjina, N., Skočir, Z., Bohaček, Z., Magdalenić, I., Vrdoljak, B. *Standardi i norme elektroničkog poslovanja*

[10] *SHA-1*, http://en.wikipedia.org/wiki/SHA-1, 23. 1. 2012.

[11] *SQL injection*, http://en.wikipedia.org/wiki/SQL_injection, 24. 1. 2012.

[12] *Cross-site scripting*, http://en.wikipedia.org/wiki/Cross-site_scripting, 24. 1. 2012.

[13] *HTTP Secure*, http://en.wikipedia.org/wiki/HTTP_Secure, 24. 1. 2012.

[14] *Data Encryption Standard*, http://en.wikipedia.org/wiki/Data_Encryption_Standard, 25. 1. 2012.

[15] *e-PRIOR Software Architecture Document*, https://joinup.ec.europa.eu/sites/default/files/Open%20e-PRIOR%20SAD%202%2001.pdf, 24. 2. 2011.