Bosna i Hercegovina
Federacija Bosne i Hercegovine
Kanton Sarajevo
Zavod za informatiku i statistiku

Uputstvo
za korištenje sigurnog protokola i certifikata
za uspostavu zaštićene veze između servera i klijentskog računara

Uvod

Pod pojmom zaštićena komunikaciona veza podrazumijeva se veza preko koje se podaci prenose u šifriranom obliku, tako da on nije čitljiv za neovlaštenu osoba koja bi eventualno presrela komunikaciju. Tipično, šifriranje se obavlja preko jednog – istog ključa (šifre) koji je poznat i klijentu i serveru i koji se računarski generiše za svaku sesiju posebno, a njegova razmjena se obavlja putem mehanizma infrastrukture javnog ključa (engl. *Public Key Infrastructure*, PKI). Tipično PKI obuhvata certifikate za klijente, servere i ovlaštenu treću stranu kojoj vjeruju i klijenti i serveri (engl. *Certificate Authority*, CA). Za pružanje javnih usluga preko Interneta, veza se tipično štiti uz posredovanje javnih certifikacijskih agencija i njihovih ovlaštenih zastupnika, dok se u internoj mreži može koristiti i vlastiti CA.

Vezu između servera i klijentskog računara možemo svrstati u tri kategorije:

1. nezaštićena veza, podaci čitljivi na komunikacionom kanalu
2. veza zaštićena, dokazana vjerodostojnost servera
3. veza zaštićena, dokazana vjerodostojnost i servera i klijenta

1. HTTP osnovni način pristupa – nezaštićena komunikacija

Podaci između klijenta i servera prenose se nezaštićenom (nešifriranom) komunikacijom (HTTP protokol), podaci u mreži su čitljivi, postoji mogućnost njihovom pristupu.
Za pristup do aplikacije potrebna kombinacija “korisničko ime & šifra”, što znači da serveru može pristupiti i bilo koji drugi korisnik koji zna tuđe korisničko ime i njegovu šifru. **Ime i šifra se prenose nezaštićeno**, te ih neovlašteni korisnik iz iste mreže može otkriti.
Kada su u pitanju zloupotrebe, server nema način da dodatno provjeri da li se iza korisničkog imena stvarno nalazi ovlašteni korisnik. Također, niti korisnik ne može sa sigurnošću znati da li pristupa stvarnom ili lažnom serveru.

Upotreba: HTTP se treba koristiti samo za pregled i čitanje stranica.

2. HTTPS jednostruka provjera (korisnik prihvata vjerodostojnost servera)

Komunikacija sa serverom je zaštićena – šifrirana (HTTPS protokol), a podaci u mreži nečitljivi za druge. Internet preglednik korisničkog računara preuzima sa servera njegov javni ključ - certifikat, i koristi ga za uspostavu zaštićene komunikacije sa serverom.

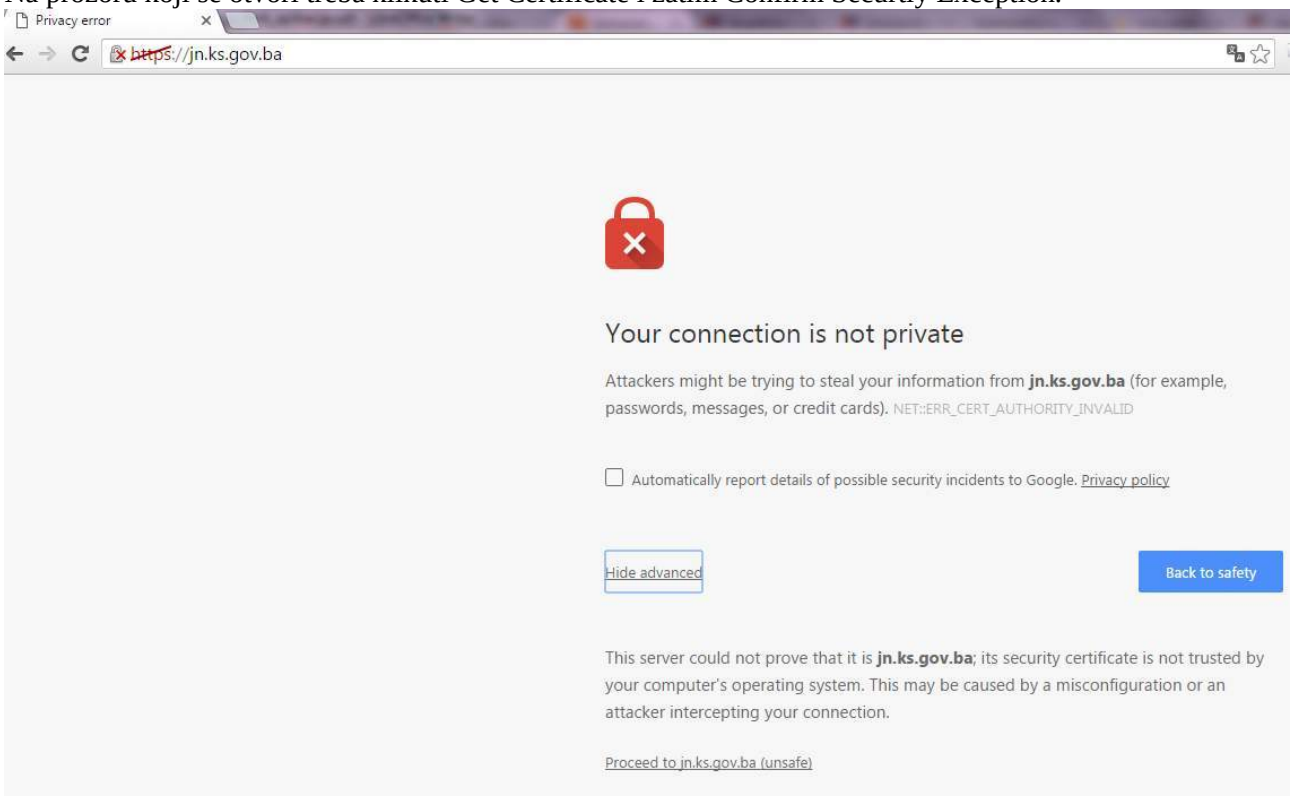
Za pristup do aplikacije su **potrebni korisničko ime i šifra**, što znači da serveru može pristupiti i bilo koji korisnik koji zna tuđe korisničko ime i njegovu šifru, ali ime i šifra se prenose zaštićeno.

Ukoliko je certifikacijsko tijelo (*Certificate authority*) jedna od zvanično priznatih agencija koje su automatski upisane u svaki Web preglednik pri instalaciji (pogledati Preferences > Advanced > Certificates > View certificates > Authorities), ili agencija unijeta naknadno od strane korisnika, tada preglednik ne prijavljuje upozorenje prilikom preuzimanja serverskog certifikata (javnog ključa), zato što se podrazumijeva da vjeruje svim certifikatima koje je izdala ovlaštena certifikacijska agencija.
U suprotnom, ukoliko server nema certifikat izdat od ovlaštene certifikacijske agencije (Certificate authority), ili je on istekao ili poništen iz bilo kog razloga (npr. radi toga što je kompromitiran), tada prilikom pristupanja HTTPS konekciji dobivamo upozorenje da je na nama da odlučimo da li da vjerujemo ili ne jer se ne može potvrditi vjerodostojnost servera.
Kada su u pitanju zloupotrebe, server nema način da dodatno provjeri da li se iza korisničkog imena stvarno nalazi ovlašteni korisnik, ali korisnik zna da pristupa stvarnom serveru.

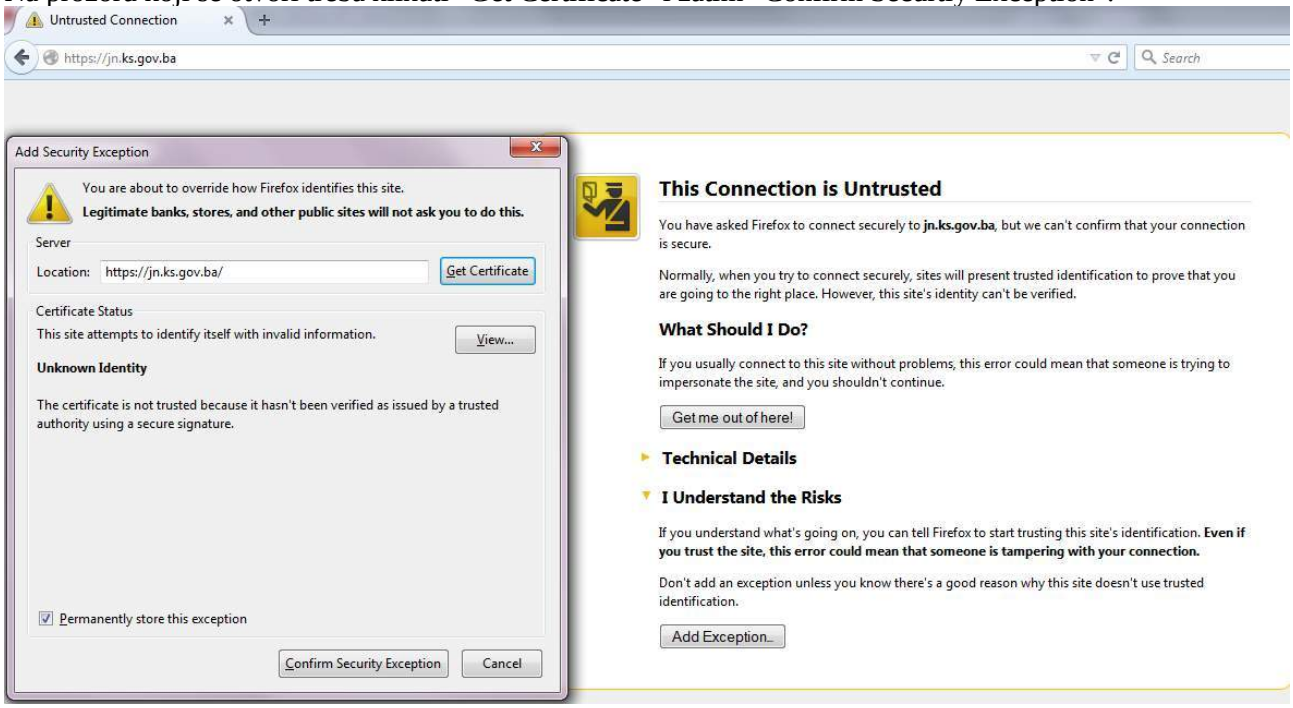
Upotreba: HTTPS se koristi za zaštićenu prijavu i unos podataka.
Primjer: U Kantonu Sarajevo je ovo slučaj za neke aplikacije koje održava Zavod za informatiku i statistiku KS, kao što su https://mail.ks.gov.ba/ ili https://jn.ks.gov.ba/.

HTTPS protokol koristi certifikat a ako ga preglednik ne prepoznaje, treba ga **zapamtiti ali samo za provjerene stranice** koje ne koriste komercijalne certifikate, obično stranice svoje firme.

U programu **Google Chrome** nakon dobivanja poruke "Your connection is not private" treba kliknuti "Advanced" i onda "Proceed to jn.ks.gov.ba (unsafe)"
Na prozoru koji se otvori treba klikuti Get Certificate i zatim Confirm Securtiy Exception.



U programu **Mozilla Firefox** nakon dobivanja poruke "This Connection is Untrusted" treba kliknuti "I Understand the Risks" i "Add Exception..."
Na prozoru koji se otvori treba klikuti "Get Certificate" i zatim "Confirm Securtiy Exception".



U programu **Internet Explorer** nakon dobivanja poruke “There is a problem with this website’s security certificate.” treba kliknuti “Continue to this website (not recommended).”

Upozorenje: Vjerodostojnost servera je važna kako bi se izbjegle zloupotrebe i gubici novca, povjerljivih podataka i sl. Npr. želimo obaviti kupovinu putem Interneta na stranici http://www.amazon.com/. Prilikom iniciranja kupovinu ulazimo na zaštićenu lokaciju https://www.amazon.com/ap/signin ...., a u redu za unos URL adrese u web pregledniku pojavljuje se slika malog ključa i katanca kao indikator uspostave zaštićene veze. Kada pređemo mišem preko te sličice pojavljuje se tekst: *Verified by: VeriSign, Inc.* što je potvrda da vjerodstojnost servera garantuje priznata certifikacijska agencija *VeriSign, Inc.* Web preglednik ne prijavljuje upozorenje zato što je certifikat servera izdala priznata certifikacijska agencija.
Ukoliko je naš računar zaražen, moguće je da budemo usmjereni na lažni server koji izgleda identično. Na tom lažnom serveru unosimo podatke o svojoj kartici za plaćanje i na taj način otkrivamo ih zlonamjernim osobama i tako gubimo novac s kartice.
U slučaju da smo pokušali pristupiti lažnom serveru, dobili bi upozorenje da server nije vjerodostojan, zato je veoma **važno obratiti pažnju** na takve poruke!

3. HTTPS dvostruka provjera (korisnik prihvata vjerodostojnost servera, server prihvata vjerodostojnost klijenta)

Komunikacija sa serverom je zaštićena – šifrirana (HTTPS protokol), a podaci u mreži nečitljiviza druge. Internet preglednik korisničkog računara preuzima sa servera njegov javni ključ - certifikat i koristi ga za uspostavu zaštićene komunikacije sa serverom. Također i server provjera klijenta i samo ukoliko on ima certifikat izdat od ovlaštene agencije, dozvoljava pristup.

Za pristup do aplikacije i dalje su **potrebni korisničko ime i šifra, ali i klijentski certifikat** (elektronski fajl zaštićen šifrom), što znači da serveru ne može pristupiti korisnik koji nema svoj certifikat iako može znati tuđe korisničko ime i njegovu šifru.
Na ovaj način server vjeruje da se iza korisničkog imena stvarno nalazi ovlašteni korisnik, jer je u upotrebi klijentski certifikat (korisnik je odgovoran za čuvanje svog certifikata, jer je to njegova elektronska legitimacija), a s druge strane korisnik zna da pristupa stvarnom serveru.

Upotreba: HTTPS se koristi za zaštićenu prijavu i unos podataka, tamo gdje je firma za koju se unosi izdala elektronski certfikat.
Primjer: aplikacije koje je pravio Zavod za informatiku i statistiku KS, te za aplikacija Porezne uprave FBIH