

## Sigurna komunikacija

### Što je to

Prilikom korištenja interneta (npr. našeg web sitea), prijenos podataka odvija se između vašeg računala i nekog drugog računala na internetu. Na tom putu mogu se nalaziti i mnoga druga računala i specijalizirani mrežni uređaji. Sama temeljna tehnologija koja to omogućava između ostalog omogućava i bilo kome (sa određenim znanjima i alatima) da može „prislušivati“ tu komunikaciju praktički sa bilo kojeg mjesta u svijetu.

Dakle od ključne je važnosti na neki način osigurati privatnost komunikacije između vas i našeg računala.

Pojednostavljeno rečeno, računala za pregledavanje web stranica koriste tzv. „**http**“ protokol koji ne osigurava potrebnu privatnost (informacije su čitljive svima). Http protokol nije problematičan za sadržaje koji ne predstavljaju povjerljive informacije (npr. naziv proizvoda, cijene i slično), no u koliko je riječ o vašim osobnim podacima tada http ostavlja mogućnost zlonamjernim pojedincima da ih iskoriste.

Tako je standardizirana inačica http protokola nazvana „**https**“ protokol. Https osigurava nečitljivost podataka dok putuju internetom između vašeg i našeg računala. Dakle, kad vaše računalo šalje bilo kakav upit (podatke i slično) na naše računalo, prije nego što podaci napuste vaše računalo, oni se kriptiraju, te tako kriptirani putuju do našeg računala. Naše računalo ih zaprima kriptirane, te ih dekriptira i obrađuje. Isto se događa kad naše računalo šalje podatke vašem.

Mogućnost dekripcije (čitanja sa razumijevanjem) podataka od strane trećih osoba negdje na internetu je zanemariva. Dekripcija bi zahtijevala izuzetno snažna računala i trebalo bi jako puno vremena da se kodiranje uspije razotkriti.

***Internet preglednici i web poslužitelji imaju mogućnost korištenja https protokola za sigurnu komunikaciju.***

Da bi web poslužitelj mogao koristiti https protokol, on mora imati instaliran tzv. certifikat. Taj certifikat je u stvari potvrda da ste zaista posjetili web site koji ste upisali kao adresu u internet pregledniku. Vaš internet preglednik vas obaviještava ako ima nekih sumnji u autentičnost certifikata. Sumnje mogu biti razne naravi ali se u principu svode na:

- Izdavatelj certifikata nije na popisu onih kojima vaš preglednik trenutno vjeruje (svaki preglednik ima unaprijed definiranu listu izdavatelja certifikata koje smatraju vjerodostojnim)
- Postoji neki konfiguracijski problem sa poslužiteljom

- Neki drugi poslužitelj se pretvara da je naš poslužitelj (certifikat sadrži informaciju za koje je računalo izdan, npr: www.telebit.hr; ako u adresnoj liniji preglednika piše jedno, a certifikat glasi na nešto drugo, tada je bolje odustati osim ako niste sigurni da je sve u redu).

Druga dva razloga su potencijalno problematična i trebate dobro promisliti da li nastaviti dalje.

Prvi razlog ukratko znači slijedeće: postoje tvrtke koje se bave izdavanjima certifikata. Izdavanje certifikata od strane takve tvrtke vama kao korisniku trebalo bi značiti da smo mi zaista mi. Dakle ako npr. poznata američka tvrtka kaže da je Telebit iz Hrvatske zaista Telebit iz Hrvatske onda vi to trebate vjerovati, zato jer je ta ista tvrtka platila drugoj tvrtci da ih stave na listu izdavatelja kojoj trebate vjerovati. To bi trebalo ostaviti dojam da ste sigurni kad ostavljate svoje podatke na na stranicama tvrtke kojoj je certifikat izdala tvrtka za koju je odlučeno da po predzadanoj vrijednosti trebate vjerovati.

Naš stav je da sve dok ne postoji konkretna materijalna odgovornost izdavatelja certifikata za eventualne zloupotrebe korisnika certifikata, nema potrebe za korištenje usluga izdavatelja sa liste onih kojima se vjeruje.

*Bez obzira na izdavatelja certifikata sigurnost komunikacije je potpuno identična uz korištenje istih parametara komunikacije (oni su manje više stalni). Protokol za sigurnu komunikaciju implementiran je u vašem internet pregledniku/operativnom sustavu.*

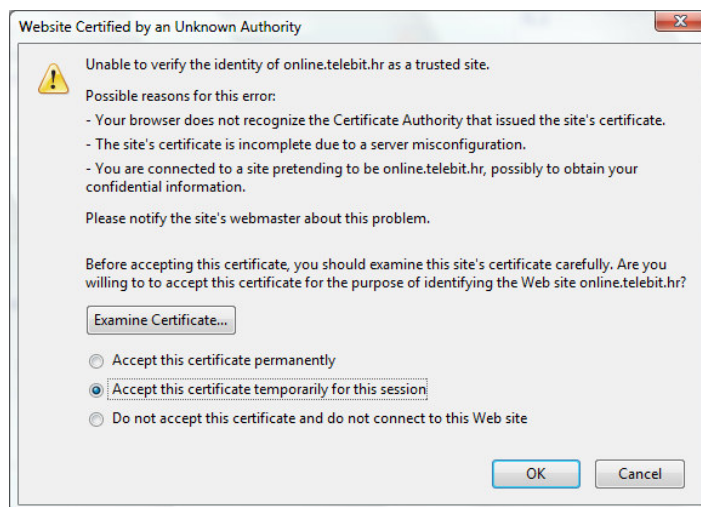
Na svu sreću, moguće je certifikate poslužitelja kojem pristupate, i/ili certifikate izdavatelja certifikata dodati na liste onih kojima vjerujete, te na taj način izbjeći upozorenje od strane preglednika.

## Instalacija certifikata

### Firefox

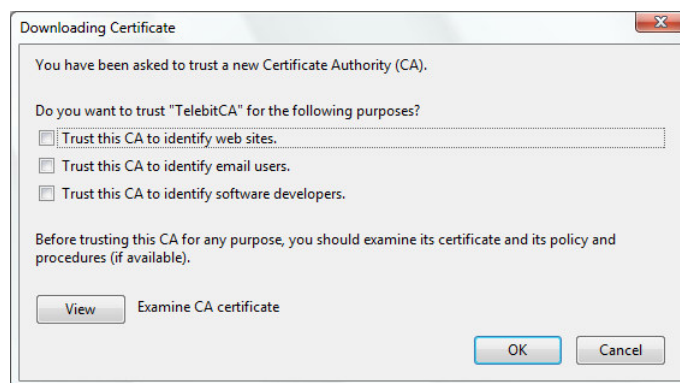
U nastavku su upute koje se odnose na Firefox 2.0 te Windows Vista Business. Instalacija na drugim kombinacijama može izgledati nešto drugačije.

Kad pokušate pristupiti stranicama za koje je zahtijevano koristiti https protokol, firefox omogućava dodavanje samo certifikata našeg internet site-a na listu te vas više neće upozoravati. Prije dodavanja dobro proučite certifikat te odlučite o samom trajnom dodavanju (Accept this certificate permanently)

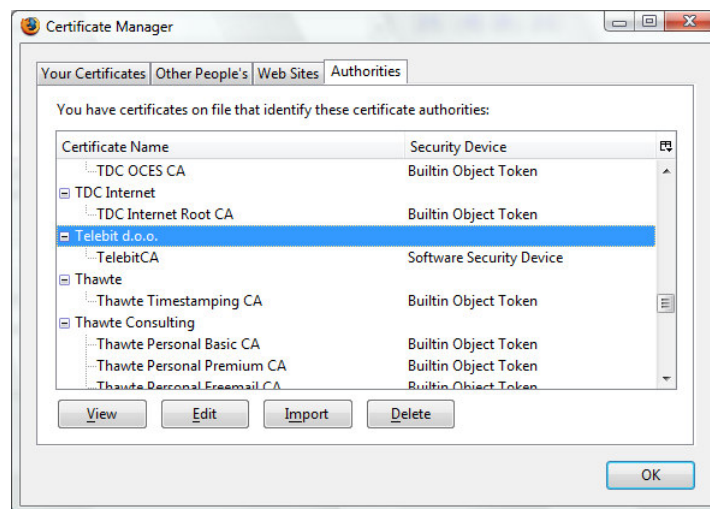


Ako želite možete certifikat izdavatelja dodati na listu root certifikata klikom na link na stranici <https://www.telebit.hr/shop/secure/certifikati.aspx>

Klikom se otvara prikaz kao na slici



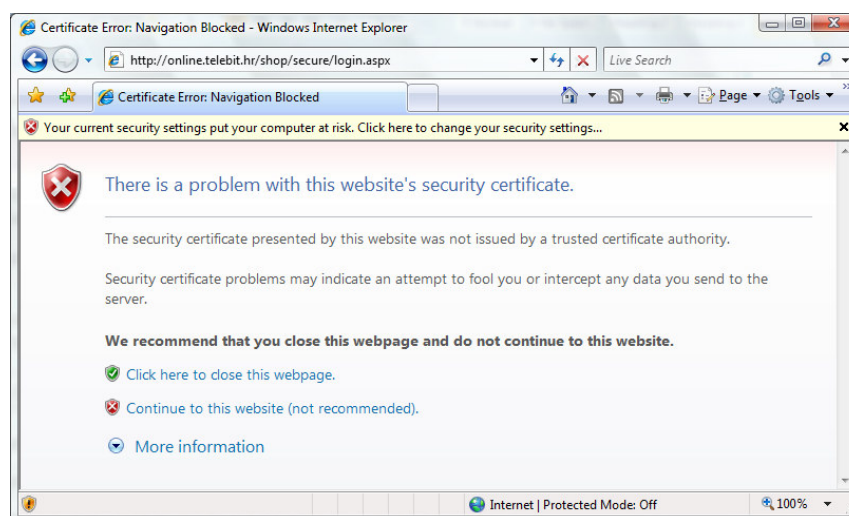
Potrebno je odabrati opciju „Trust this CA to identify web sites.“ Ovo će uvesti certifikat i staviti ga na odgovarajuće mjesto. Provjeru ispravnosti instalacije možete vidjeti na Tools-Options-Advanced-Encryption – View Certificates - Authorities.



## Internet explorer

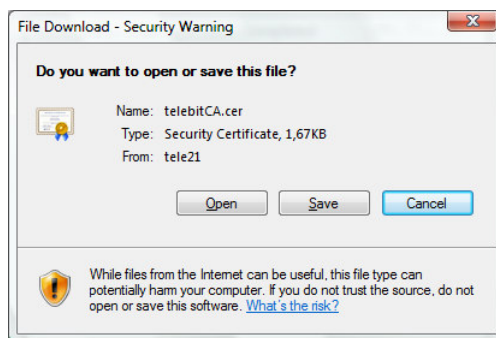
U nastavku su upute koje se odnose na Internet explorer 7 te Windows Vista Business. Instalacija na drugim kombinacijama može izgledati nešto drugačije.

Internet explorer omogućava privremeno povjerenje našem certifikatu (pojednostavljeno: povjerenje traje do slijedećeg posjeta stranicama) na način da kliknete na „Continue to this website (not recommended).“



Za trajno suzbijanje ovog upozorenja prilikom posjeta našim stranicama potrebno je dodati certifikat našeg izdavalca certifikata (Central authority /CA/) – to je naš interni odjel IT Services - na listu izdavalca certifikata kojima vjerujete.

Dodavanje certifikata se može napraviti na razne načine, ali smatramo da je najjednostavniji klikom na link <https://www.telebit.hr/shop/secure/certifikati.aspx> te odabirom „Instaliraj TelebitCA certifikat“.

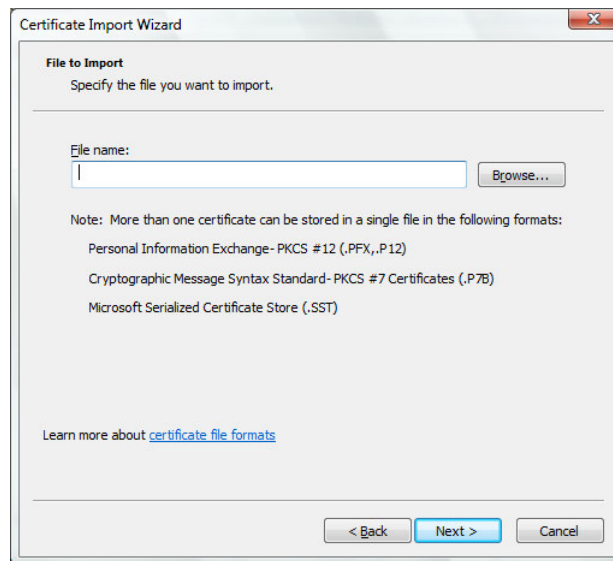


Klikom na link otvara se prozor kao na slici gore; odaberite „Save“

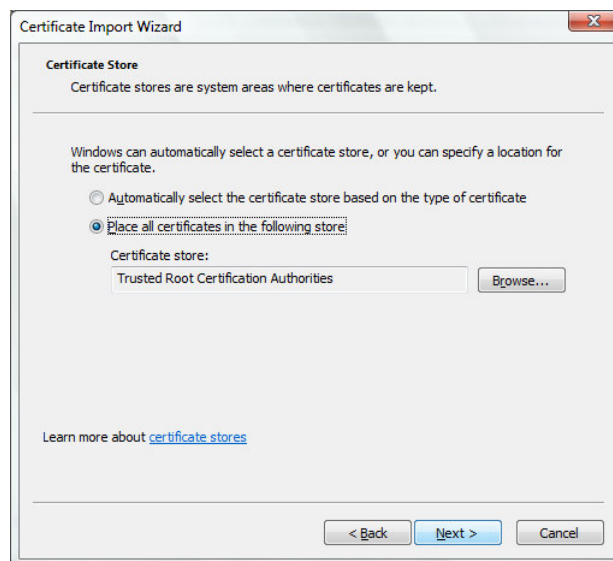
Tada u Internet exploreru odaberite Tools-Internet Options-Content-Certificates-Trusted Root Certification Authorities, kliknite na „Import“ što vas vodi do



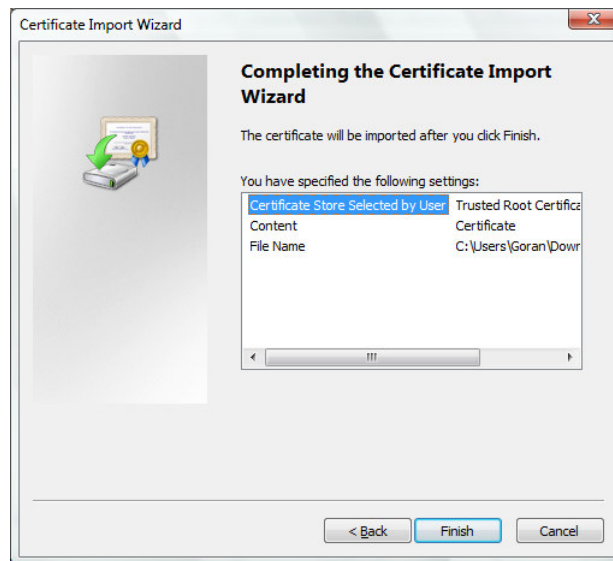
Kliknite na „Next“ što otvara slijedeći prozor



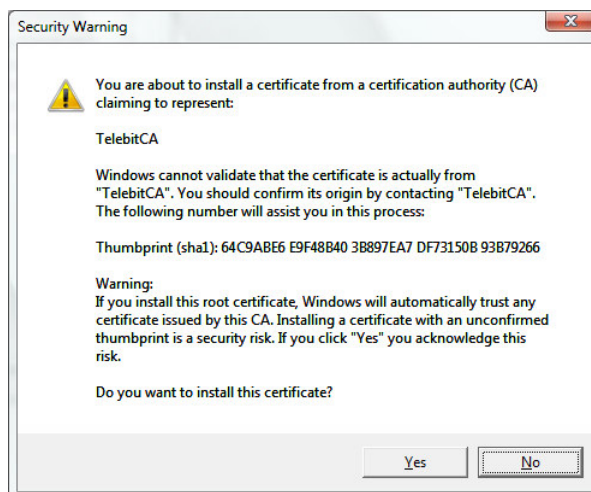
Sa browse odaberite certifikat koji ste snimili na svoje računalo u prethodnim koracima. Kliknite „Next“ što vas vodi do sljedeće slike



Važno je uočiti da je zabilježeno upravo kao na slici, jer spremanje certifiakata u neko drugo mjesto neće dati dobre rezultate. Ako je sve kako treba kliknite na „Next“ što vas vodi do

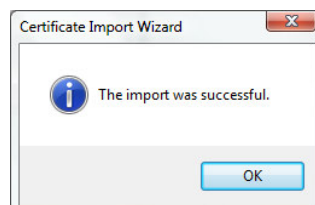


Klikom na „Finish“ certifikat idete na sljedeći ekran



Sada morate donijeti odluku da li želite dodati naš CA u vašu listu onima kojima se vjeruje. Mišljenja smo da kako ste sam certifikat preuzeli sa naših stranica koristeći https protokol mala je mogućnost da ne netko uspio podvaliti drugi certifikat kao svoj. Autentičnost (Thumbprint broj) možete provjeriti pozivom na naše telefone gdje ćemo usmeno razmijeniti brojeve koji bi morali odgovarati (na slici navedeni broj ne mora biti ono što ćete vi vidjeti na svom ekranu).

Klikom na „Yes“ odlazite na konačni završetak



Na kraju uvoza bi trebali dobiti obavijest da je sve prošlo u redu (slika gore).

Postoji teoretska mogućnost i potpuno automatske instalacije, no pokazalo se da odluka kuda staviti certifikat može na različitim verzijama IE rezultirati različitim mjestima postavljanja što nije dobro. Predloženi put je malo zahtjevniji ali s predvidivim ishodom.

Verzija dokumenta: 1.0