Certifikati u službi zaštite prijenosa podataka

22.11.2019, Zagreb, Dubravko.Penezic@srce.hr

Sadržaj

- Što je certifikat i kako se koristi?
- Vrste certifikata
- Vjerodostojnost certifikata
- Gdje se praktično koriste certifikati

Zaštita prijenosa podataka

- Komunikacija između poslužitelja i klijenta
- Uporaba mehanizma asimetričnih ključeva
  https://www.ssl2buy.com/wiki/diffie-hellman-rsa-dsa-ecc-and-ecdsa-asymmetric-key-algorithms
- Implementirani putem TLS(SSL) protokola
  https://www.ssl2buy.com/wiki/ssl-vs-tls
- Digitalni poslužiteljski certifikat – ovjereni javni ključ poslužitelja
- CA – autoriteti koju ovjeravaju digitalni certifikat

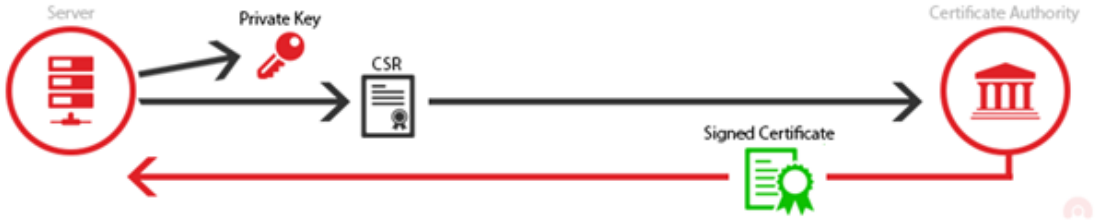
Kako se uspostavlja sigurna komunikacija

http://www.exabytes.ma/

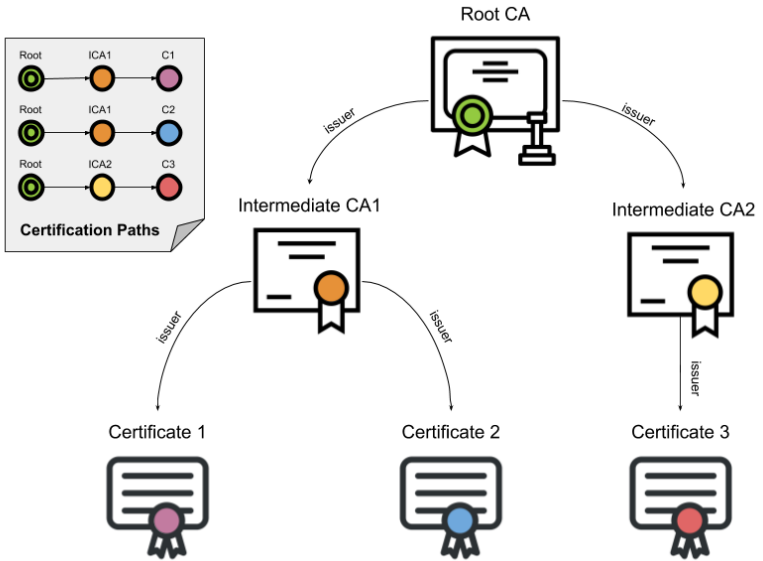
Digitalni certifikat

- Set od nekoliko datoteka (tekstualnih ili digitalnih)
- Zahtjev za izdavanjem certifikata
- Privatni ključ
- Certifikat
- CA Root certifikat
- Povezni CA certifikati (intermediate chain)

Tijek dobivanja certifikata



CA intermediate chain



http://ssl.com/

Vrste CA

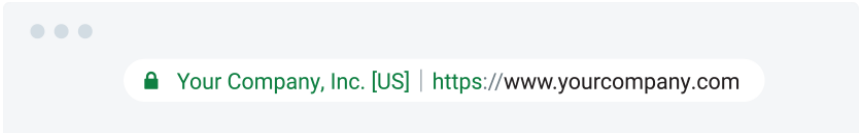
- **Self-signed** – vlastiti CA , vlastita pravila, nije automatski podržan od strane klijenata

- **Komercijalni CA** – naplaćuju izdavanje certifikata, automatski su podržani od strane klijenata
- **Besplatni CA** – Let's encrypt, besplatan, kratkotrajan certifikat, automatski podržan

Let's Encrypt

Vrste certifikata

- Osnovni SSL certifikat
  - povezan s jednim DNS zapisom
  - bilo koji CA
- EV SSL certifikat
  - Povezan s jednim DNS zapisom
  - Komercijalni CA
  - Dodatan prikaz pripadnosti ustanovi

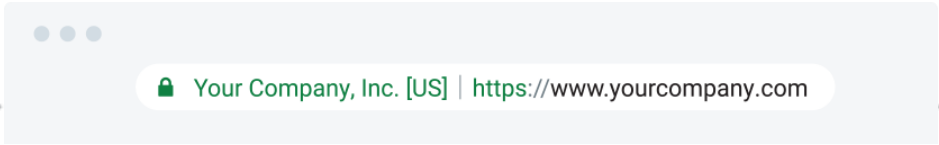


Vrste certifikata (2)

- Više-domenski SAN certifikat
  - Povezan s nekoliko DNS zapisa
  - Neki puta postoje ograničenja u broju DNS zapisa
  - Dostupan kroz komercijalne i self-signed CA
  - Subject **A**lternative **N**ame

Vrste certifikata (3)

- EV više-domenski SAN certifikat
  - Povezan s nekoliko DNS zapisa
  - Neki puta postoje ograničenja u broju DNS zapisa
  - Dostupan kroz komercijalne CA
  - Subject **A**lternative **N**ame
  - Dodatan prikaz pripadnosti ustanovi



Vrste certifikata (4)

- Wildcard certifikat
  - Povezan s jednom domenom
  - Dostupan kroz komercijalne i self-signed CA
- Kombinacije certifikata
  - Više-domenski i wildcard certifikat

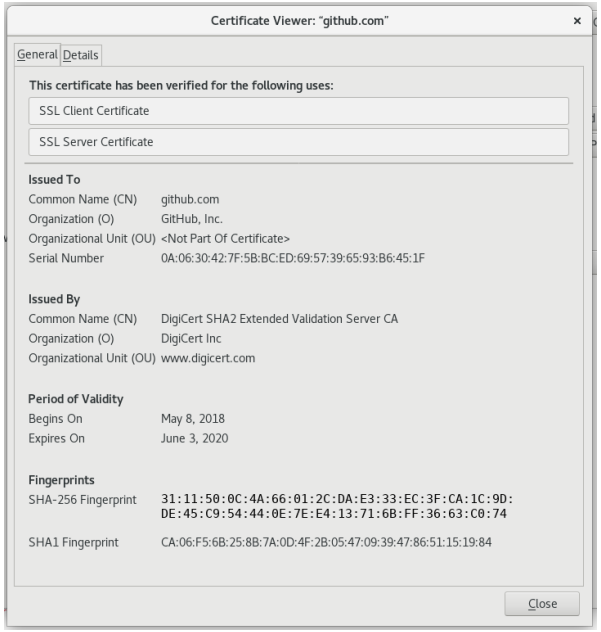
Vjerodostojnost certifikata

- CA autoritet
  - Globalni
  - Lokalni
- Vrijeme trajanja certifikata
  - Vrijedi samo od – do
  - Pokušava se smanjiti vrijeme maksimalnog trajanja certifikata

Vjerodostojnost certifikata (2)

- Pripadnost ustanovi
  - EV certifikati
- Lista povlačenja (revocation list)
- Format certifikata
  - Zadovoljava RFC 5280, X.509 v3 format
  - Zapis samog certifikata je obično DER i PEM

Vjerodostojnost certifikata (3)



Vjerodostojnost certifikata (4)

- Alati za provjeru
  - https://www.sslshopper.com/ssl-checker.html
  - https://www.digicert.com/help/
  - https://www.ssllabs.com/ssltest/
  - Openssl linux naredba

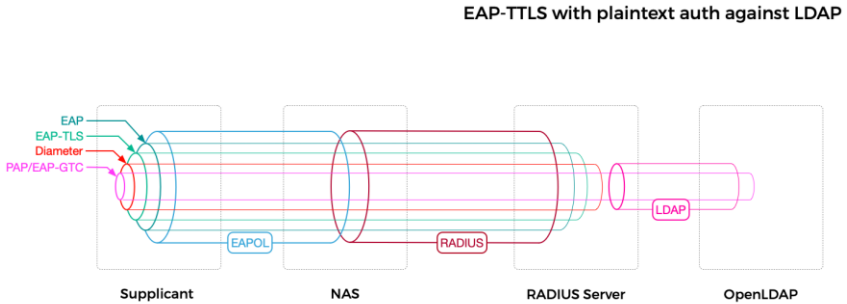
Gdje se praktično koriste certifikati

- Web sadržaji (HTTPS)

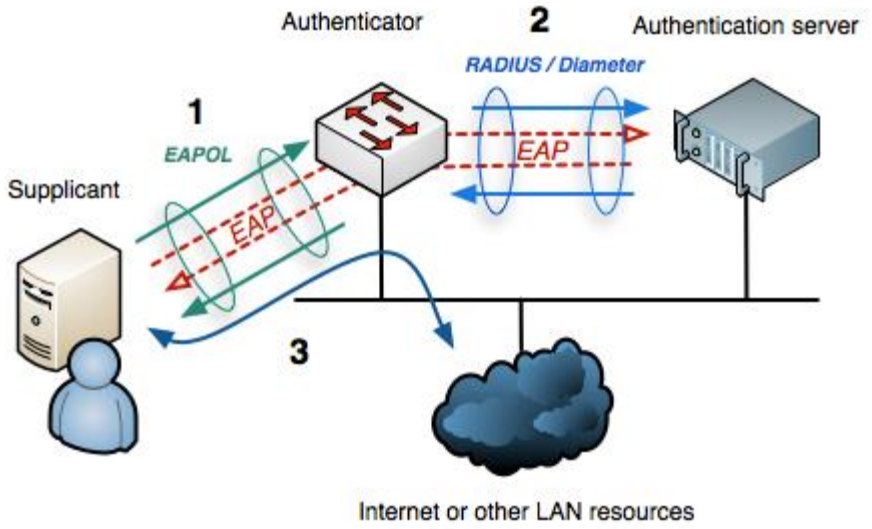
- email komunikacija (SSL/TLS)
  - IMAP, POP, SMTP
  - Autentikacija korisnika
  - nije SMIME/PGP

Gdje se praktično koriste certifikati (2)

- RADIUS
  - EAP (802.1x)
  - RADIUS/TLS (RadSec)



Gdje se praktično koriste certifikati (3)



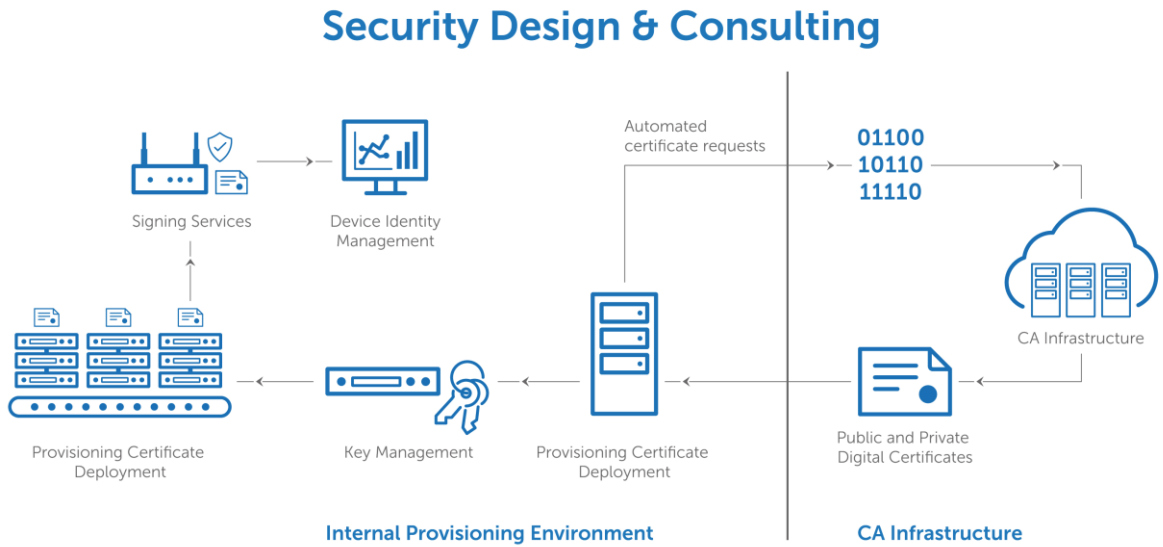
Gdje se praktično koriste certifikati (4)

- News (NNTP)
- LDAP (LDAPS)
- FTP

IoT i certifikati

- Mobilnost
- Potreba za sigurnom komunikacijom
- Nekontrolirani uvjeti
- Automatski dohvat certifikata

IoT i certifikati (2)



DigiCert

Certifikati u službi zaštite prijenosa podataka

Hvala na pažnji!

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

www.srce.unizg.hr

Srce politikom otvorenog pristupa široj javnosti osigurava dostupnost i korištenje svih rezultata rada Srca, a prvenstveno obrazovnih i stručnih informacija i sadržaja nastalih djelovanjem i radom Srca.

www.srce.unizg.hr/otvoreni-pristup

srce
otvoreni pristup