

**Certification authority (CA)**

**SEMINARSKI RAD**

**Predmet: Sigurnost informacionih sistema**

**Profesor: Muharem Redžibašić**

**Student: Samed Mujkanović**

**Indeks: 299**

**Studij: Softversko inženjerstvo Zenica, 14.04.2023**

Sadržaj

[Šta je certifikacijski organ (CA)? 3](#_Toc132385090)

[Šta je lanac povjerenja? 4](#_Toc132385091)

[Šta je to sidro povjerenja? 5](#_Toc132385092)

[Šta je srednji certifikat? 6](#_Toc132385093)

[Šta je certifikat krajnjeg entiteta? 7](#_Toc132385094)

[Zašto je važan lanac povjerenja? 8](#_Toc132385095)

[Šta je CA/Browser Forum? 8](#_Toc132385096)

[Vrste digitalnih Certifikata 8](#_Toc132385097)

[Primjeri upotrebe Certification Authority 9](#_Toc132385098)

[Zaključak 10](#_Toc132385099)

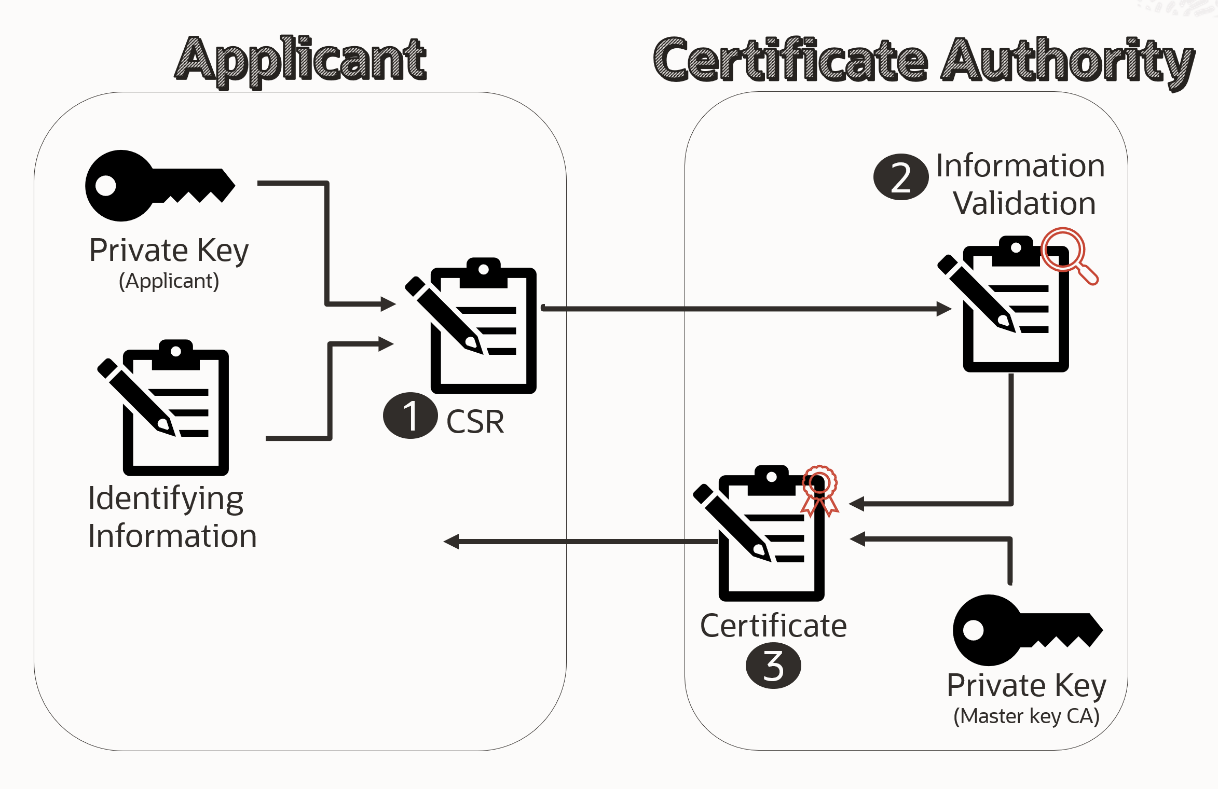
[Literatura 10](#_Toc132385100)

# Šta je certifikacijski organ (CA)?

Autoritet za izdavanje certifikata (CA), koji se također ponekad naziva certifikacijski organ, je kompanija ili organizacija koja djeluje na provjeravanju identiteta entiteta (kao što su web stranice, adrese e-pošte, kompanije ili pojedinačne osobe) i vezuje ih za kriptografske ključeve putem izdavanja elektronskih dokumenata poznatih kao digitalni potvrde.

Digitalna potvrda omogućava:

* Provjera autentičnosti, služeći kao akreditiv za potvrđivanje identiteta entiteta kojem je izdana.
* Enkripcija, za sigurnu komunikaciju preko nesigurnih mreža kao što je Internet.
* Integritet dokumenata potpisanih certifikatom tako da ih treća strana ne može mijenjati u tranzitu.



Tipično, podnositelj zahtjeva za digitalni certifikat će generirati par ključeva koji se sastoji od privatnog i javnog ključa, zajedno sa zahtjevom za potpisivanje certifikata (CSR). CSR je kodirana tekstualna datoteka koja uključuje javni ključ i druge informacije koje će biti uključene u certifikat (npr. naziv domene, organizacija, adresa e-pošte itd.). Par ključeva i generisanje CSR-a obično se obavljaju na serveru ili radnoj stanici na kojoj će biti instaliran certifikat, a vrsta informacija uključenih u CSR varira u zavisnosti od nivoa validacije i namjeravanoj upotrebi certifikata.

Za razliku od javnog ključa, privatni ključ podnositelja zahtjeva da se čuva na sigurnom i nikada se ne smije pokazati CA (ili bilo kome drugom).

Nakon generisanja CSR-a, aplikant ga šalje CA-u, koji samostalno provjerava da li su informacije koje sadrži ispravne i, ako je tako, digitalno potpisuje certifikat privatnim ključem koji izdaje i šalje ga podnosiocu zahtjeva.

Kada se potpisani certifikat predstavi trećoj strani (npr. kada ta osoba pristupi web stranici vlasnika certifikata), primalac može kriptografski potvrditi digitalni potpis CA putem javnog ključa CA.

Također, primalac može koristiti certifikat da potvrdi da je potpisani sadržaj poslao neko ko posjeduje odgovarajući privatni ključ, te da informacija nije promijenjena od kada je potpisana. Ključni dio ovog aspekta certifikata je nešto što se zove lanac povjerenja.

# Šta je lanac povjerenja?

U SSL/TLS, S/MIME, potpisivanju koda i drugim aplikacijama X.509 certifikata, koristi se hijerarhija certifikata za provjeru valjanosti izdavaoca certifikata. Ova hijerarhija je poznata kao lanac povjerenja. U lancu povjerenja, certifikati se izdaju i potpisuju certifikatima koji žive više u hijerarhiji.

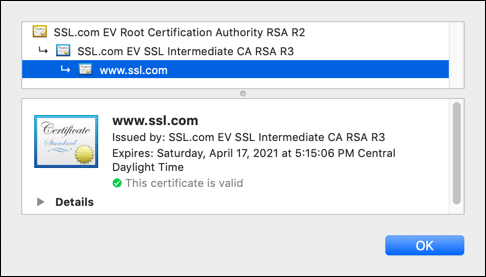
Lanac povjerenja sastoji se od nekoliko dijelova:

* Sidro povjerenja, koje je izvorno tijelo za izdavanje certifikata (CA).
* Najmanje jedan srednji certifikat, koji služi kao "izolacija" između CA i certifikata krajnjeg entiteta.
* Certifikat krajnjeg entiteta koji se koristi za provjeru identiteta entiteta kao što je web stranica, biznis ili osoba.

Lahko sami mozete vidjeti lanac povjerenja ako pregledate certifikat HTTPS web stranice. Kada provjerite SSL/TLS certifikat u web pretraživaču, naći ćete raščlambu lanca povjerenja tog digitalnog certifikata, uključujući sidro povjerenja, sve međucertifikate i certifikat krajnjeg entiteta.

Ove različite tačke verifikacije su potkrijepljene valjanošću prethodnog sloja ili "linka", vraćajući se na sidro povjerenja.

Primjer u nastavku prikazuje lanac povjerenja s web-mjesta SSL.com, koji vodi od certifikata web-mjesta krajnjeg subjekta natrag do korijenskog CA-a, preko jednog međucertifikata:

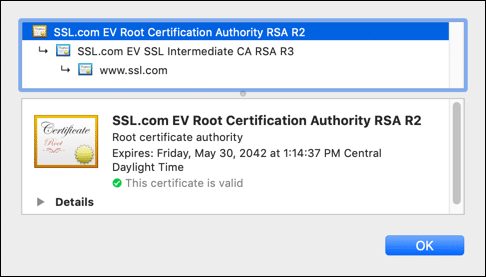


# Šta je to sidro povjerenja?

Korijenski autoritet za izdavanje certifikata (CA) služi kao sidro poverenja u lancu poverenja. Valjanost ovog sidra povjerenja je od vitalnog značaja za integritet lanca u cjelini. Ako je CA javno vjerodostojan (kao što je SSL.com), glavne softverske kompanije uključuju korijenske CA certifikate u svoj softver preglednika i operativnog sistema. Ovo uključivanje osigurava da će softver vjerovati certifikatima u lancu povjerenja koji vodi natrag do bilo kojeg od korijenskih certifikata CA.

Ispod možete vidjeti sidro povjerenja sa web stranice SSL.com

(SSL.com EV Root Certification Authority RSA R2):



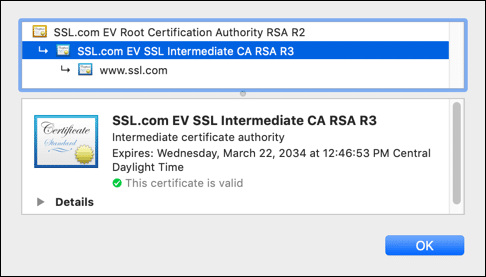
# Šta je srednji certifikat?

Korijenski CA ili sidro povjerenja ima mogućnost potpisivanja i izdavanja posrednih certifikata. Srednji certifikati (također poznati kao srednji, podređeni ili izdavajući CA) pružaju fleksibilnu strukturu za dodjelu valjanosti sidra povjerenja dodatnim posrednim i krajnjim certifikatima u lancu.

U tom smislu, srednji certifikati služe administrativnoj funkciji; svaki međuprodukt se može koristiti za određenu svrhu — kao što je izdavanje SSL/TLS ili certifikata za potpisivanje koda — i čak se može koristiti za prenošenje povjerenja korijenskog CA drugim organizacijama.

Srednji certifikati također pružaju međuspremnik između certifikata krajnjeg entiteta i korijenskog CA, štiteći privatni korijenski ključ od kompromisa. Za javne pouzdane CA-ove (uključujući SSL.com), Osnovni zahtjevi foruma CA/Browser zapravo zabranjuju izdavanje certifikata krajnjeg entiteta direktno iz korijenskog CA, koji se mora čuvati sigurno van mreže. To znači da će lanac povjerenja bilo kojeg javno pouzdanog certifikata uključivati barem jedan srednji certifikat.

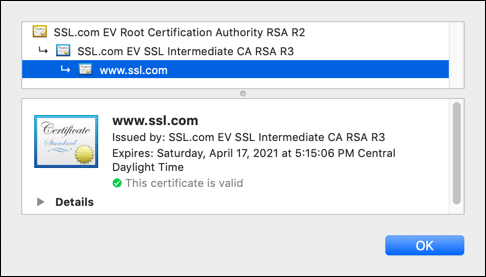
U primjeru prikazanom ispod, (SSL.com EV SSL Intermediate CA RSA R3) je jedini srednji certifikat u lancu povjerenja web stranice SSL.com. Kao što naziv certifikata sugerira, koristi se samo za izdavanje EV SSL/TLS certifikata:



# Šta je certifikat krajnjeg entiteta?

Certifikat krajnjeg entiteta je konačna karika u lancu povjerenja. Certifikat krajnjeg entiteta (ponekad poznat kao list certifikata ili certifikat pretplatnika) služi za dodjelu povjerenja korijenskog CA, putem bilo kojeg posrednika u lancu, entitetu kao što je web stranica, kompanija, vlada ili pojedinačna osoba.

Certifikat krajnjeg entiteta razlikuje se od sidra povjerenja ili posrednog certifikata po tome što ne može izdati dodatne certifikate. To je, na neki način, poslednja karika što se lanca tiče. Primjer ispod prikazuje SSL/TLS certifikat krajnjeg entiteta sa web stranice SSL.com:



# Zašto je važan lanac povjerenja?

Lanac povjerenja osigurava sigurnost, skalabilnost i usklađenost sa standardima za CA. Također osigurava privatnost, povjerenje i sigurnost za one koji se oslanjaju na certifikate krajnjeg entiteta, kao što su operateri web stranica i korisnici.

Važno je da vlasnici web lokacija i drugi korisnici certifikata krajnjeg entiteta shvate da je potpuni lanac povjerenja neophodan da bi njihov certifikat uspješno prenio povjerenje CA.

# Šta je CA/Browser Forum?

Forum CA/Browser (CA/B) održava smjernice za sve aspekte kreiranja, distribucije i upotrebe digitalnih certifikata, uključujući politike za istekom i opozivom certifikata. Na ovom forumu obično učestvuju javni servisi za izdavanje certifikata.

Većina članova su ili CA ili dobavljači web pretraživača. Međutim, učestvuju i organizacije potrošača certifikata.

Prema pravilima CA/B Foruma, CA mora ugovorno zahtijevati od svih RA da se pridržavaju i dokumentuju njihovu usklađenost sa ovim pravilima. CA su i sami podložni opsežnim pravilima i operativnim revizijama.

Bilo kakve povrede mogu izazvati dodatne revizije i druge posljedice koje bi mogle oštetiti reputaciju CA i smanjiti povjerenje u njegove operacije i pouzdanost.

​

# Vrste digitalnih Certifikata

CA-ovi ne izdaju samo SSL/TLS certifikate. Oni mogu izdati druge vrste certifikata za različite slučajeve upotrebe, uključujući sljedeće:

* Certifikate za potpisivanje koda koriste izdavači softvera i programeri za potpisivanje svojih distribucija softvera. Krajnji korisnici ih zatim mogu koristiti za provjeru autentičnosti i validaciju preuzimanja softvera od dobavljača ili programera.
* Certifikati za potpisivanje e-pošte omogućavaju entitetima da potpišu, šifriraju i autentifikuju e-poštu pomoću protokola Secure/Multipurpose Internet Mail Extensions za sigurne priloge e-pošte.
* Certifikati za potpisivanje objekata omogućavaju potpisivanje i provjeru autentičnosti bilo koje vrste softverskog objekta.
* Certifikati za potpisivanje korisnika/klijenta ili certifikati za verifikaciju potpisa pomažu pojedincima u rješavanju raznih potreba za autentifikacijom.

# Primjeri upotrebe Certification Authority

Postoje brojni primjeri upotrebe Certification Authority u svakodnevnom životu. Ovdje su neki primjeri:

* SSL certifikati za web stranice - Certification Authority izdaje digitalne certifikate za web stranice koji potvrđuju autentičnost identiteta web stranice i omogućuju enkripciju komunikacije između korisnika i web poslužitelja. SSL certifikati koriste se za sigurnu razmjenu osjetljivih informacija kao što su podaci o kreditnoj kartici, lozinke i drugo.
* Elektronički potpisi - Certification Authority izdaje digitalne certifikate za elektroničke potpise, koji potvrđuju autentičnost identiteta osobe koja je potpisala dokument i osiguravaju integritet dokumenta. Elektronički potpisi koriste se u različitim pravnim transakcijama, uključujući ugovore, financijske transakcije i druge.
* Identifikacijske kartice - Certification Authority može izdati digitalne certifikate za identifikacijske kartice, koje potvrđuju autentičnost identiteta nositelja. Ovo se koristi u mnogim državama u svrhu izdavanja službenih dokumenata, kao što su putovnice i osobne iskaznice.
* Sigurnost elektroničke pošte - Certification Authority izdaje digitalne certifikate koji omogućuju enkripciju i digitalno potpisivanje e-pošte. Ovo pomaže u sprječavanju neovlaštenog pristupa vašoj e-pošti i potvrđuje autentičnost poruka koje šaljete.
* Mobilne aplikacije - Certification Authority izdaje digitalne certifikate za mobilne aplikacije koji potvrđuju autentičnost identiteta programera i osiguravaju da je aplikacija autentična i nije bila modificirana nakon izdavanja certifikata.

Ovo su samo neki primjeri upotrebe Certification Authority u životu. Općenito, Certification Authority igra ključnu ulogu u osiguravanju sigurnosti i autentičnosti digitalnih dokumenata i transakcija.

# Zaključak

U ovom seminarskom radu sam istražili koncept Certification Authority (CA), koji je osnova za sigurnost kriptografskih komunikacija na internetu. Razmotrili smo ulogu CA u izdavanju digitalnih certifikata, koji se koriste za provjeru autentičnosti identiteta web stranica, uređaja i korisnika. Također smo razmotrili proces stvaranja ključeva, digitalnih potpisa i potpisivanja certifikata, kao i pristupačne alate za upravljanje CA infrastrukturom.

Istakli smo da je osiguravanje povjerenja u digitalne certifikate ključno za sigurnost korištenja interneta, te da je važno da korisnici i tvrtke razumiju ulogu CA u zaštiti od prijevara i napada na internetu.

Uz brzi razvoj tehnologije i sve veću količinu podataka koji se prenose preko interneta, sigurnost na internetu postaje sve važnija.

Certification Authority igra ključnu ulogu u zaštiti digitalnih komunikacija i osiguravanju integriteta i povjerenja u mrežu. Važno je da kompanije i korisnici shvate važnost korištenja digitalnih certifikata i pouzdanih CA, te da se pridržavaju sigurnosnih praksi kako bi se izbjegli sigurnosni propusti i napadi na internetu.

# Literatura

* D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF, June 2008.
* M. Ristic. Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications. Feisty Duck Ltd., 2014.

Web izvori:

* <https://wpmudev.com/blog/ssl-certificate-authorities-reviewed/>
* <https://www.entrust.com/resources/faq/what-is-certificate-authority>
* <https://www.digicert.com/blog/what-is-a-certificate-authority>
* <https://www.techtarget.com/searchsecurity/definition/certificate-authority>
* <https://www.thesslstore.com/blog/what-is-a-certificate-authority-ca-and-what-do-they-do/>