AMRES TCS servis

Jovana Palibrk, AMRES

NA3 T4, Žabljak, februar 2013.

Uvod

- Teorijski uvod
  - Kriptografija
  - Infrastruktura javnih ključeva
- TERENA Certificate Service (TCS)
- AMRES TCS servis

Uvod

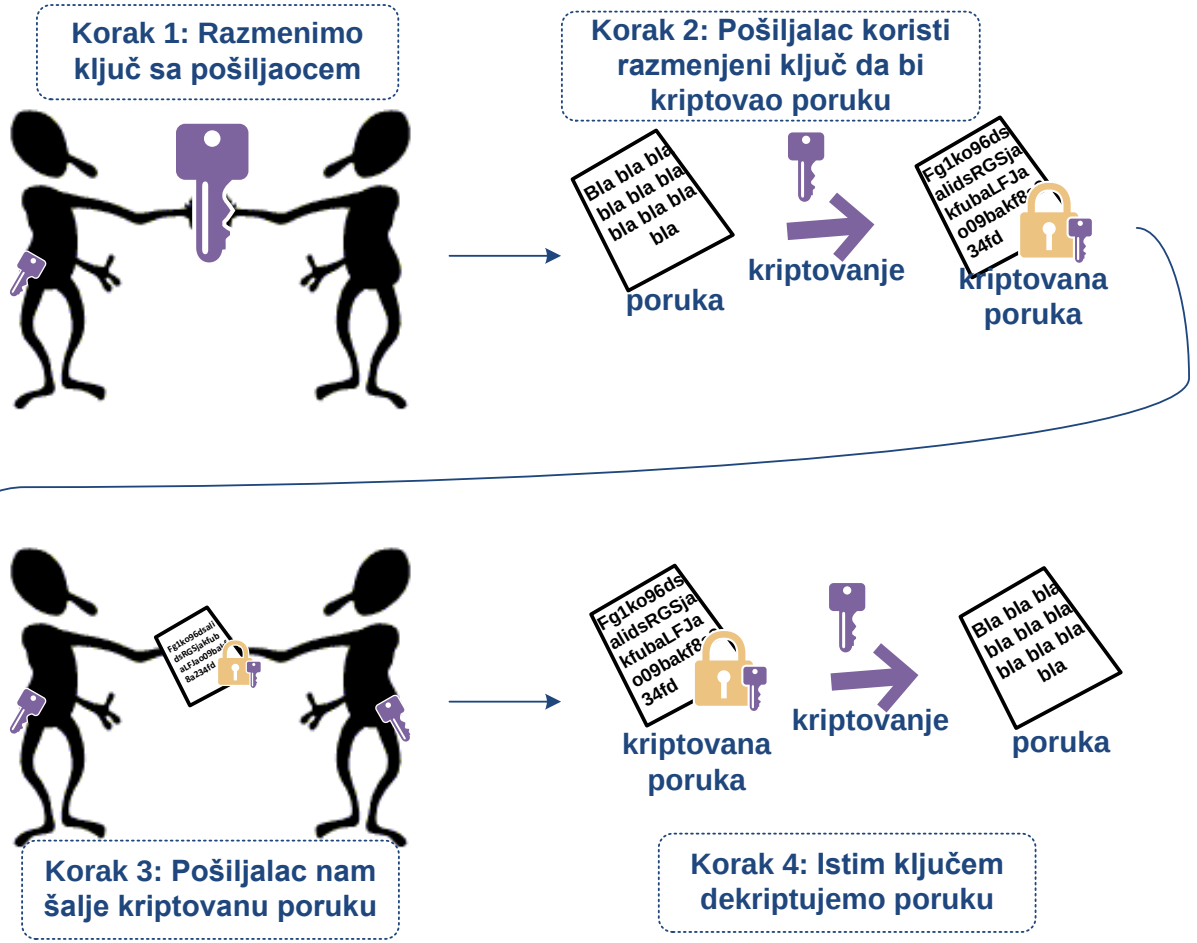
- Bezbedna komunikacija podrazumeva
  - Tajnost ili poverljivost – sistemi za šifrovanje
  - Autentifikaciju – digitalni potpisi
  - Integritet – hash funkcije

Kriptografija

- Samo učesnici u komunikaciji (pošiljalac i primalac) bi trebalo da razumeju komunikaciju u kojoj je očuvana tajnost ili poverljivost.
- Tajnost komunikacije postiže se šifrovanjem (enkripcijom) poruka.
- Sistemi za šifrovanje:
  - Sa simetričnim ključevima
  - Sa asimetričnim ključevima

Kriptografija – Sistemi za šifrovanje

- Sistemi za šifrovanje sa simetričnim ključevima - ključevi za šifrovanje i dešifrovanje isti i moraju se razmeniti pre početka komunikacije



Kriptografija – Sistemi za šifrovanje

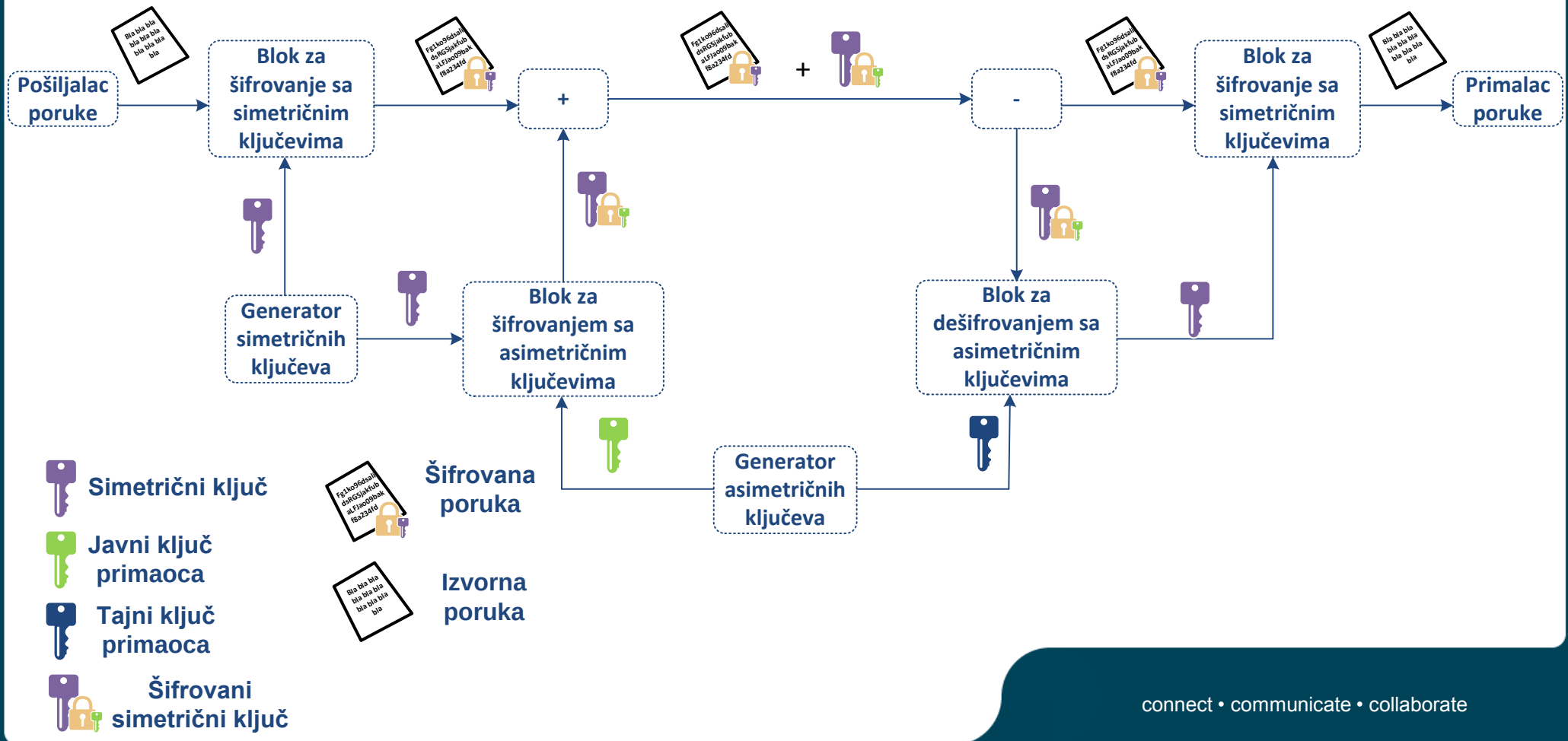
- Sistemi za šifrovanje sa asimetričnim ključevima
  - Svaki učesnik komunikacije poseduje par ključeva, privatni i javni ključ
  - Podaci šifrovani javnim ključem dešifruju se privatnim, i obrnuto

Kriptografija

- Primenom sistema za šifrovanje sa asimetričnim ključevima na poseban deo poruke, ključa ili nekog drugog važnog činioca u komunikaciji zainteresovanih strana nastali su servisi koji nude usluge:
  - efikasno šifrovanja,
  - digitalnog potpisa i
  - digitalnog sertifikata.

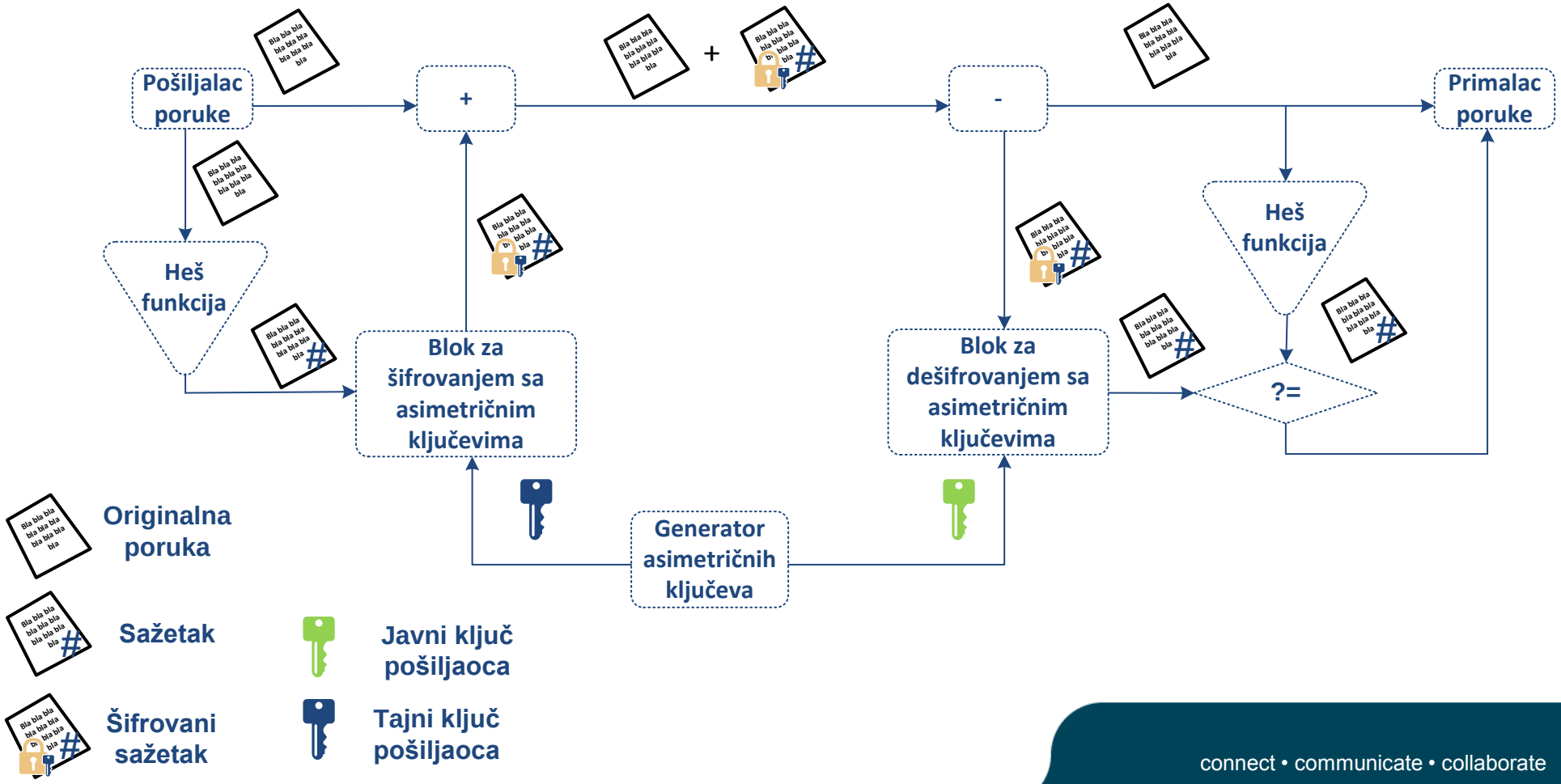
Kriptografija – efikasno šifrovanje

- Primene sistema za šifrovanje sa asimetričnim ključevima
  - Efikasno šifrovanje – kombinovani sistem za šifrovanje



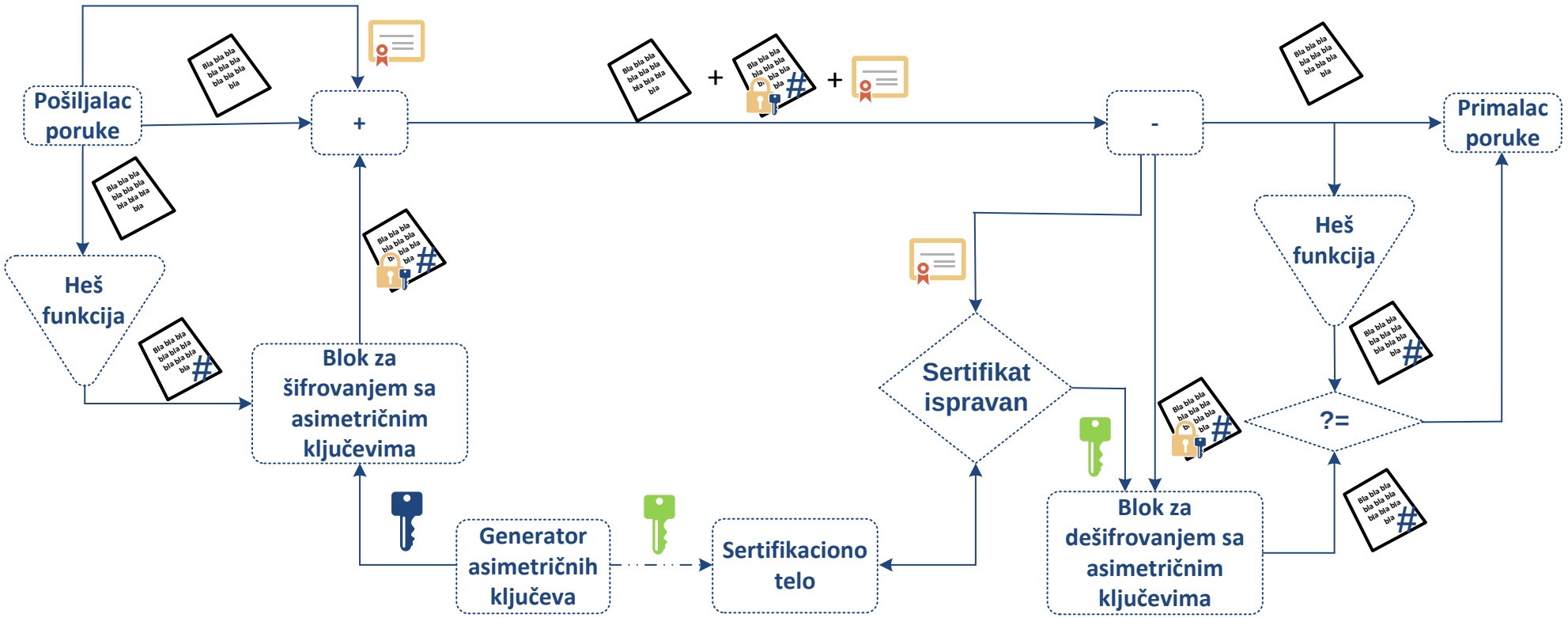
Kriptografija – digitalni potpis

- Primene sistema za šifrovanje sa asimetričnim ključevima
  - Digitalni potpis



Kriptografija – digitalni sertifikat

- Primene sistema za šifrovanje sa asimetričnim ključevima
  - Digitalni sertifikat



Public Key Infrastructure – PKI

- Potrebna infrastruktura koja omogućuje:
  - Prijavljivanje za dobijanje sertifikata
  - Provera identiteta prijavljenih korisnika
  - Izdavanje i objavljivanje sertifikata
  - Mehanizmi i protokoli za dopremanje sertifikata do korisnika
  - Proglašavanje sertifikata nevažećim
- Rešenje: infrastruktura javnih ključeva
- Infrastruktura javnih ključeva je okvir koji se sastoji od hardvera, softvera, polisa i procedura koji su neophodni za upravljanje, stvaranje, skladištenje i distribuciju ključeva i digitalnih sertifikata.

PKI – osnovne komponente

- Sertifikaciono telo – *Certification Authority* (CA) izdaje i opozivan digitalne sertifikate, a potom i upravlja svim aspektima životnog veka sertifikata nakon izdavanja

- Krajnji elementi - komponente infrastrukture koje koriste njene usluge, bilo kao predmeti sertifikovanja, bilo kao korisnici izdatog digitalnog sertifikata.

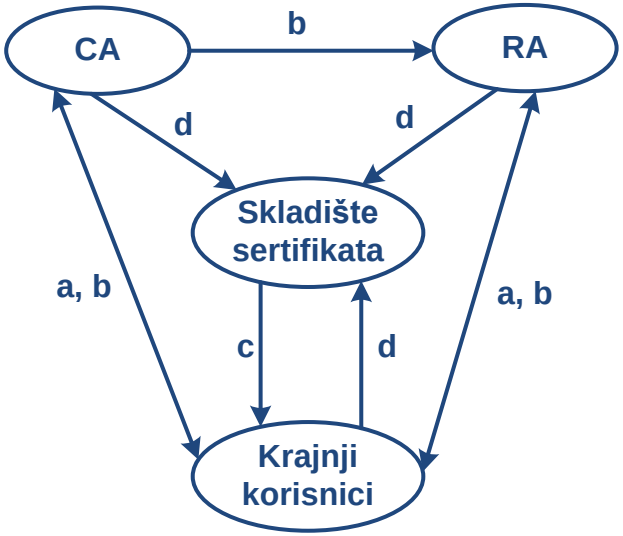
PKI – osnovne komponente

- Registraciono telo – *Registration authority* (RA), opciona komponenta infrastrukture javnih ključeva koja, ako je prisutna, služi da rastereti sertifikaciono telo administrativnih funkcija. Zadaci:
  - provera identiteta podnosioca zahteva za digitalnim sertifikatom
  - generisanje i distribuiranje deljenih tajnih podataka krajnjim korisnicima koji se koriste u procesu podnošenja zahteva za sertifikatom
  - započinjanje procesa sertifikovanja kod sertifikacionog tela u ime podnosioca zahteva
  - generisanje i distribuiranje para ključeva podnosiocu zahteva
  - iniciranje zahteva za opozivom sertifikata u ime krajnjeg korisnika.

- Skladište – *Repository*, komponenta infrastrukture javnih ključeva koja se koristi za skladištenje informacija vezanih za sertifikate i liste opozvanih sertifikata, *Certificate Revocation List* (CRL).

PKI – osnovne komponente

- Interakcije između komponenata PKI infrastrukture



a – inicijalna registracija/sertifikacija
b – obnova para ključeva
obnavljanje sertifikata
zahtevanje opoziva sertifikata
c – verifikacija sertifikata
d – obnavljanje sertifikata

PKI – osnovne funkcije

- Registracija – proces prijavljivanja institucije/krajnjih korisnika koji obuhvata proveru identiteta institucije/krajnjih korisnika i razmenu informacija sa za to zaduženom komponentom infrastrukture Registracionim telom (RA). Za svaki tip sertifikata je definisan odgovarajući nivo provere, dokumentom koji se naziva politika sertifikacije.

- Inicijalizacija – proces u okviru koga predstavnik institucije/krajnji korisnik i sertifikaciono telo razmenjuju neophodne informacije za dalju komunikaciju

- Sertifikacija – proces izdavanja i dostavljanja sertifikata predstavnicima institucija/krajnjim korisnicima i obavlja je CA

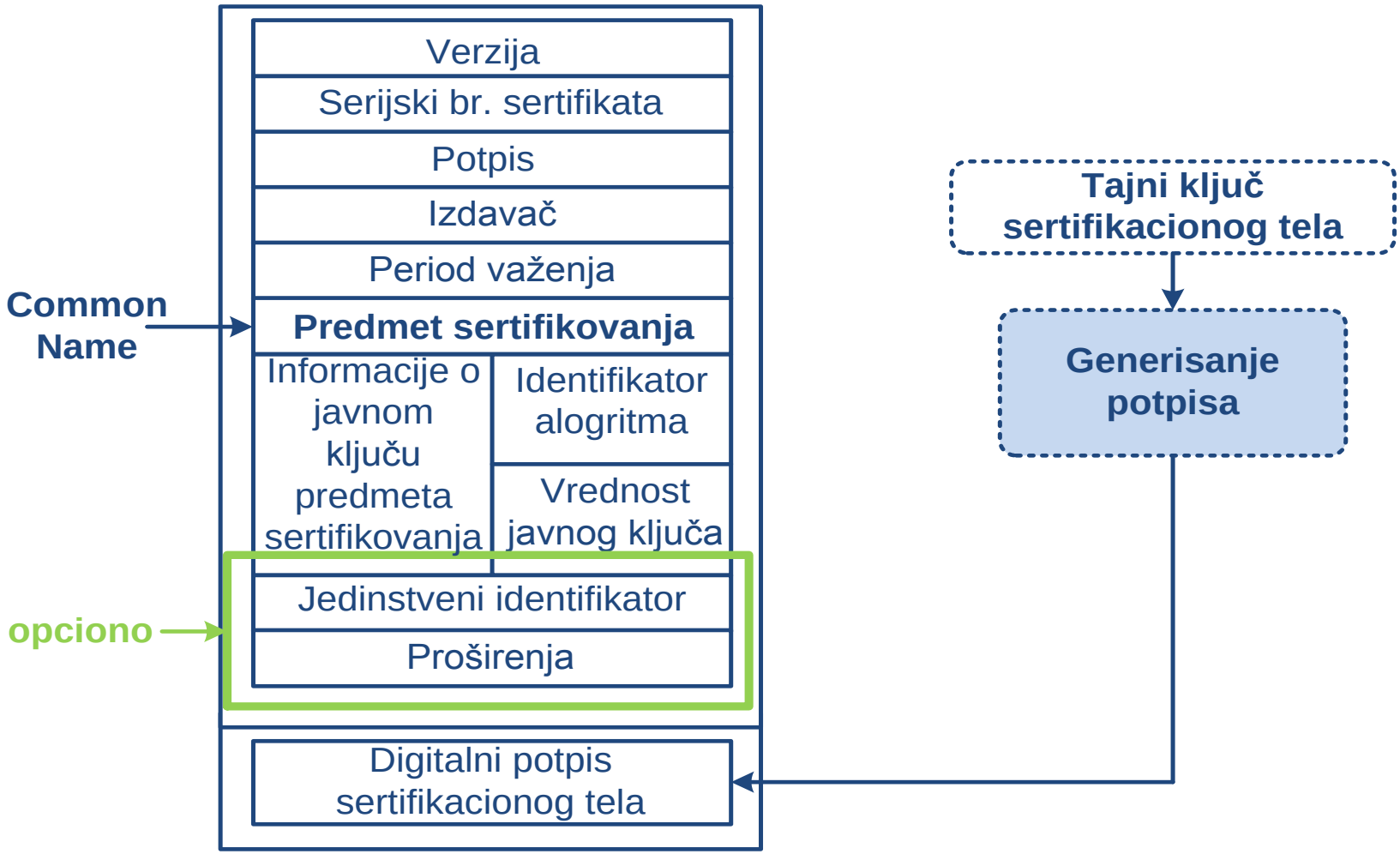
PKI – osnovne funkcije

- Opoziv sertifikata – Opozvani sertifikati se objavljuju preko lista opozvanih sertifikata (*Certificate Revocation List - CRL*) koje objavljuje sertifikaciono telo koje je izdalo sertifikat i te informacije smešta u repozitorijum

- Provera lanca poverenja – Potpisnik poruke može umesto jednog vlastitog sertifikati dati lanac sertifikata, u kome je svaki sertifikat potpisan sertifikatom nadređenog CA. To podrazumeva proveru lanca poverenja i validnosti svakog sertifikata u tom lancu. Da li postoji poverenje u dati sertifikat? Da li je sertifikat zaista potpisan od strane određenog CA?

- Provera validnosti sertifikata – Da li je sertifikat istekao? Da li je sertifikat važeći ili je opozvan?

Format digitalnog sertifikata



TCS – TERENA Certificate Service

TCS – TERENA Certificate Service

- TCS *predstavlja servis za izdavanje digitalnih sertifikata naučno-istraživačkim i* obrazovnim institucijama posredstvom njihovih matičnih akademskih mreža na koje su povezane
- TERENA – sertifikaciono telo
- AMRES – registraciono telo
- *Comodo CA Limited* izdaje sertifikate

TCS – TERENA Certificate Service

- TCS servis nudi pet različitih tipova digitalnih sertifikata :
  - **Serverski sertifikati –** SSL sertifikati, koriste se za autentifikaciju servera i uspostavljanje sigurne sesije sa krajnjim klijentima.
    - ***TERENA Single-Domain SSL Certificate***
    - ***TERENA Multi-Domain SSL Certificate***
    - ***TERENA Wildcard SSL Certificate***
  - e-Istraživački serverski sertifikati (*e-Science Server Certificate)*
  - Lični korisnički sertifikati (*Personal Certificate)*
  - e-Istraživački lični sertifikati (*e-Science Personal Certificate)*
  - Sertifikati za potpisivanje koda (*Code-signing Certificate)*

- Novina:
  - OV (Organization Validated) sertifikati
  - DV (Domain Validated) sertifikati

TCS – TERENA Certificate Service

- Sertifikati dobijeni preko TCS servisa su potpisani od strane **TERENA** sertifikacionog tela čiji **TERENA CA** sertifikat
  - je dalje potpisan od strane ***UserTrust***, prelaznog sertifikacionog tela, čiji sertifikat **UTN-USERFirst-Hardware**
    - je potpisan od strane **AddTrust External root** sertifikacionog tela, sertifikat **AddTrust External CA Root**

Servisi koje je potrebno obezbediti digitalnim sertifikatima

- Autentifikaciju servera
  - Web server
  - RADIUS server – eduroam
  - Email server
- Autentifikaciju krajnjih korisnika
- Sigurnu razmenu elektronske pošte
- Uspostavljanje IPsec/TLS VPN tunela
- Digitalno potpisivanje softvera

AMRES TCS servis

AMRES TCS servis

- Preko AMRES usluge izdavanja TCS sertifikata, institucijama članicama AMRES-a raspoloživi su serverski SSL sertifikati
  - **TERENA SSL sertifikati** - SSL sertifikati sadrže jedno DNS ime u Common Name polju.
  - **TERENA Multi-Domain SSL sertifikati** - Multi-Domain SSL sertifikati sadrže više (najviše 100) DNS imena.
  - **TERENA Wildcard SSL sertifikati** - Wildcard SSL sertifikat obezbeđuje SSL enkripciju svih poddomena domena za koji je zahtevan. Na primer, za domen rcub.bg.ac.rs Wildcard sertifikat (koji će biti izdat za *rcub.bg.ac.rs) možete da koristite za:
    - *mail.rcub.bg.ac.rs*
    - *www.rcub.bg.ac.rs*
    - *radius.rcub.bg.ac.rs*
    - *bilo-sta.rcub.bg.ac.rs*

AMRES TCS servis

- Omogućeno izdavanje sertifikati za ćirilični, ак.срб domen.
- Planirano je da se izdavanje ličnih korisničkih sertifikata uskoro uredi na sličan način, preko AMRES federacije identiteta koja je u razvoju.
- Izdavanje e-Istraživačkih tipovi sertifikata (serverskih i ličnih) za zaštitu i pristup GRID instalacijama, trenutno je uspostavljeno kroz AEGIS CA.

http://aegis-ca.rcub.bg.ac.rs/documents/AEGIS-CP-CPSv1-2.doc

AMRES TCS servis

- Registraciju institucije
- Prijavljivanje za korišćenje TCS servisa
- Kreiranje para ključeva i zahteva za sertifikatom
- Podnošenje zahteva

AMRES TCS servis – Registracija institucije

- Registracija institucije se obavlja preko portala Registra domena ac.rs.
- Smatra se da je institucija registovana u ac.rs kada ima registovan bar jedan domen na portalu Registra domena ac.rs.
- Registrovana institucija se može prijaviti za korišćenje TCS usluge
- Podaci o instituciji na portalu moraju biti tačni i ažurni

AMRES TCS servis – Prijavljivanje za korišćenje TCS servisa

- *Saglasnost za korišćenje TCS*

- Njegovim potpisivanjem, institucija imenuje osobu, koja će je kao administrativni kontakt zastupati u postupcima zahtevanja, dobijanja, obnavljanja i opozivanja digitalnih sertifikata.

- „Pravilnik korišćenja usluge izdavanja sertifikata“ - osnovni preduslovi korišćenja digitalnih sertifikata

http://www.amres.ac.rs/index.php?option=com_docman&task=doc_download&gid=87

AMRES TCS servis – Kreiranje asimetričnog para ključeva i zahteva za potpisivanje sertifikata

- CSR – *Certificate Signing Request*

- Kreiranju CSR zahteva, predhodi postupak generisanja asimetričnog para RSA ključeva, tj. privanog ključa i njemu odgovarajućeg javnog ključa, pomoću alata koji je raspoloživ na serveru.

- CSR zahtev sadrži:
  - Javni ključ
  - Informacije o identitetu servera
    - DNS ime servera
  - Informacije o instituciji

- BPD 106 – upustva za generisanje CSR zahteva:
  - Linux – OpenSSL
  - Microsoft IIS 4.x
  - Microsoft IIS 5.x / 6.x

AMRES TCS servis – Podnošenje zahteva

- AMRES TCS portal
  - DjangoRA – *open source* aplikacija za automatsko izdavanje sertifikata, razvijena u švedskoj akademskoj mreži, SUNET.
    - *Python, Django*
    - *MySQL baza*
    - *Linux*

- Svaka institucija ima profil – informacije o instituciji se preuzimaju iz baze registra domena ac.rs

- Svaki administrativni tehnički kontakt ima svoj nalog – isti nalog koji ima na portalu registra domena ac.rs

AMRES TCS servis – Procedura zahtevanja sertifikata

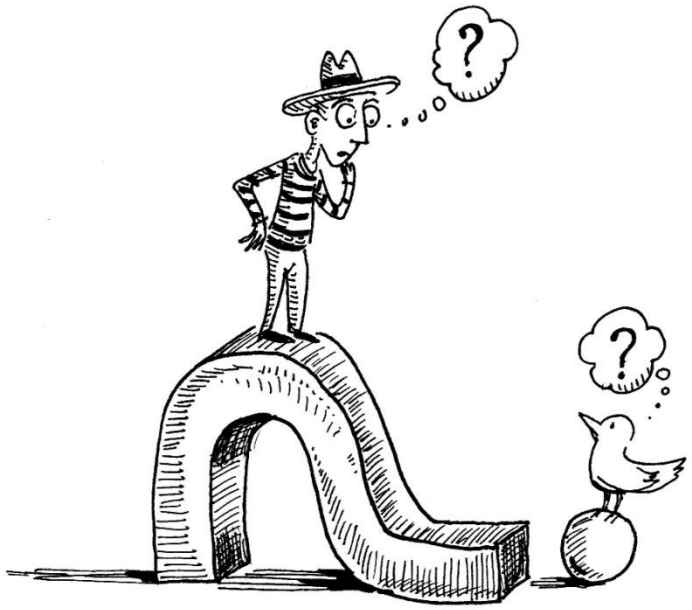
- AMRES TCS portal
  - Ovlašćeno tehničko lice se uloguje
  - Odabere profil svoje institucije i pošalje CSR zahtev
  - Prođe proceduru provere domena – DCV (Domain Control Validation)
    - šalje se email poruka na određenu email adresu koja se bira liste generičkih email adresa koje su sastavljene na osnovu FQDN (Fully Qualified Domain Name) imena sadržanih u zahtevu za sertifikat.
  - Potvrda slanja zahteva.
  - Na email administratora i tcs@amres.ac.rs se šalju obaveštenja
  - Povlačenje izdatog sertifikata može da izvrši samo ovlašćeni AMRES TCS administrator.

AMRES TCS servis – Procedura zahtevanja sertifikata

- AMRES Helpdesk
  - email obaveštenja se prosleđuju na AMRES tiketing sistem
  - Nakon poslatog zahteva automatski se kreira tiket sa predefinisanim poljima
  - Polja se popunjavaju informacijama iz email poruke dobijene od DjangoRA servera

- Informacije o sertifikatima se čuvaju i na DjangoRA serveru i u tiketing sistemu

Pitanja ?



Hvala na pažnji!