AMRES usluga izdavanja personalnih digitalnih TCS sertifikata

AMRES

Akademska mreža Srbije

Miloš Kukoleča

Sastanak administratora, Beograd, 12.12.2013.

Hijerarhija AMRES TCS servisa

- TCS – TERENA Sertificate Service
- TERENA
  - TERENA originalno nudi TCS servis izdavanja serverskih i personalnih sertifikata
  - TERENA predstavlja sertifikaciono telo -Potpisuje personalne sertifikate korisnika
- AMRES
  - Uređuje proces izdavanja sertifikata u Republici Srbiji
  - Održava portal za izdavanje sertifikata
- Akademske institucije u Republici Srbiji
  - Moraju posedovati internu bazu svojih korisnika
  - Odgovorne su za sve podatke u svojoj bazi korisnika
  - Predstavljaju Registraciono telo – odlučuju ko od korisnika ima pravo na korišćenje servisa

AMRES digitalni personalni sertifikat

- Sertifikat podržava standard X.509 V3
- V3 podržava ekstenzije (dodatna polja u sertifikatu)

Polja u personalnom sertifikatu (1)

- „Valid From“/„Valid To“
  - Određuje period važenja sertifikata
  - AMRES personalni sertifikati traju 1 godinu
- Subject
  - Sadrži informacije o korisniku – korisničko ime, ime i prezime, ime matične institucije i ime države
  - Podaci potiču iz interne baze matične institucije
- Public Key
  - Sadrži javni ključ sertifikata
  - AMRES propisuje da ključevi moraju biti dužine 2048 bita

Polja u personalnom sertifikatu (2)

- Subject Alternative Name
  - Sadrži registrovane E-mail adrese korisnika
  - Može biti više registrovanih E-mail adresa u jednom sertifikatu
  - Prihvataju se samo adrese koje se nalaze u „ac.rs“ domenu
  - Podatak o E-mail adresama potiče iz interne baze matične institucije
- CRL Distribution Point
  - URL adresa na kojoj se nalazi lista povučenih sertifikata
  - Lista se ažurira u roku od jednog dana

AMRES TCS portal – personalni sertifikati

- Portal automatizuje proces izdavanja digitalnih personalnih sertifikata
- Svaka institucija nakon registracije ima svoju sekciju na portalu
- Razlikuju se 4 uloge (skup privilegija):
  - AMRES administrator
  - Administrator institucije
  - Podadministrator institucije
  - Krajnji korisnik

3 administratorske uloge

- Jedna osoba može imati samo jednu administratorsku ulogu !

AMRES TCS portal - Uloge (1)

- AMRES administrator
  - Registruje institucije
  - Postavlja administratore institucija
  - Ima mogućnost povlačenja bilo kog sertifikata

- Administrator institucije
  - Postavlja kolege administratore i podadministratore iz matične institucije
  - Ima mogućnost menjanja podataka o instituciji
  - Ima mogućnost povlačenja sertifikata u okviru matične institucije

AMRES TCS portal - Uloge (2)

- Podadministrator institucije
  - Samo ima mogućnost povlačenja sertifikata u okviru matične institucije
- Krajnji korisnik
  - Može da zahteva i dobija personalne sertifikate
  - Ima mogućnost povlačenja sopstvenih sertifikata

- VAŽNA NAPOMENA: Jedna osoba (administrator) može imati dve uloge – kao administrator i kao korisnik

Autentifikacija

- Institucija mora biti član iAMRES federacije da bi mogla da učestvuje u servisu izdavanja digitalnih personalnih sertifikata

- Institucija mora da obezbedi:
  - Internu bazu svojih korisnika
  - Povezivanje na RADIUS infrastrukturu AMRES-a

Autentifikacija na portal

AMRES

Korisnici

Interna baza institucije

RADIUS server institucije

Domen institucije

TCS Portal

RADIUS Proxy

Centralni portal za autentifikaciju

Domen AMRES-a

Autentifikacija na portal

KORAK 1

Korisnici

1. HTTPS

TCS Portal

Interna baza institucije

RADIUS server institucije

RADIUS Proxy

Centralni portal za autentifikaciju

AMRES TERENA Certificate Service TCS

KORAK 1

Sertifikati

*Moji sertifikati**

Pomoć

O NREN-u
O Portalu
Obaveštenje o privatnosti

Pomoć
CA Sertifikati

Prijavite se

Ovaj servis vam omogućava da pribavite ili deaktivirate personalne sertifikate.
Da biste koristili ovaj servis, prethodno je neophodno da se prijavite na portal.

Login >

FAQ

Kako ovaj servis radi?

Koliko jedan sertifikat ima period važenja?

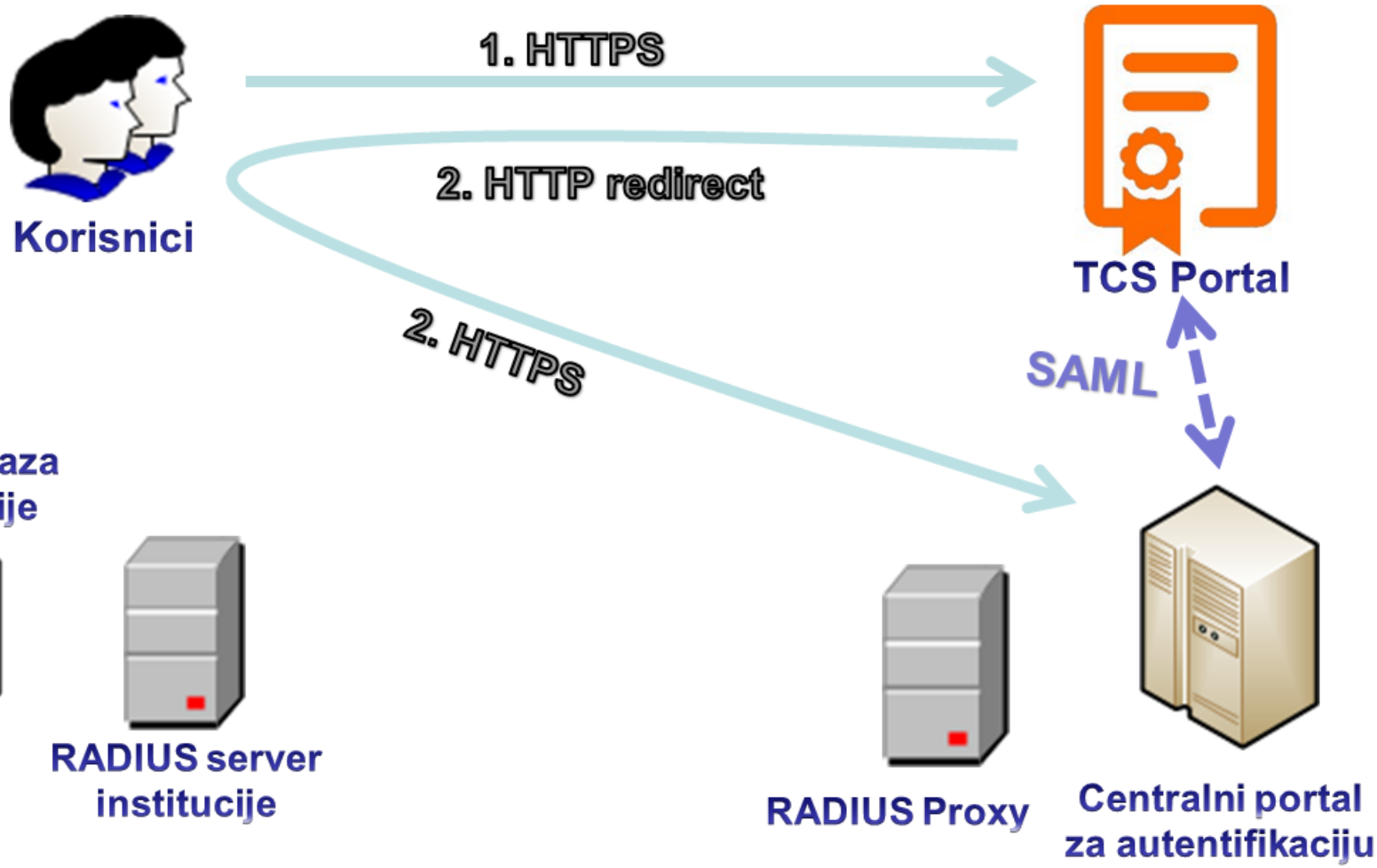
Zašto moram da se prijavim na portal?

Da li Confusa portal čuva moje lične podatke?

Šta znači ovo \'Confusa\' koje se pojavljuje svuda?

Autentifikacija na portal

KORAK 2



IAMRES
Portal za jedinstvenu prijavu na sistem

Unesite vaše korisničko ime i lozinku

Srpski | English

KORAK 2

Unesite vaše korisničko ime i lozinku

Servis zahteva od vas da se autentifikujete. Unesite vaše korisničko ime i lozinku u dole navedena polja.

Korisničko ime: korisnik

Lozinka: ••••••••••••

Matična institucija: AMRES

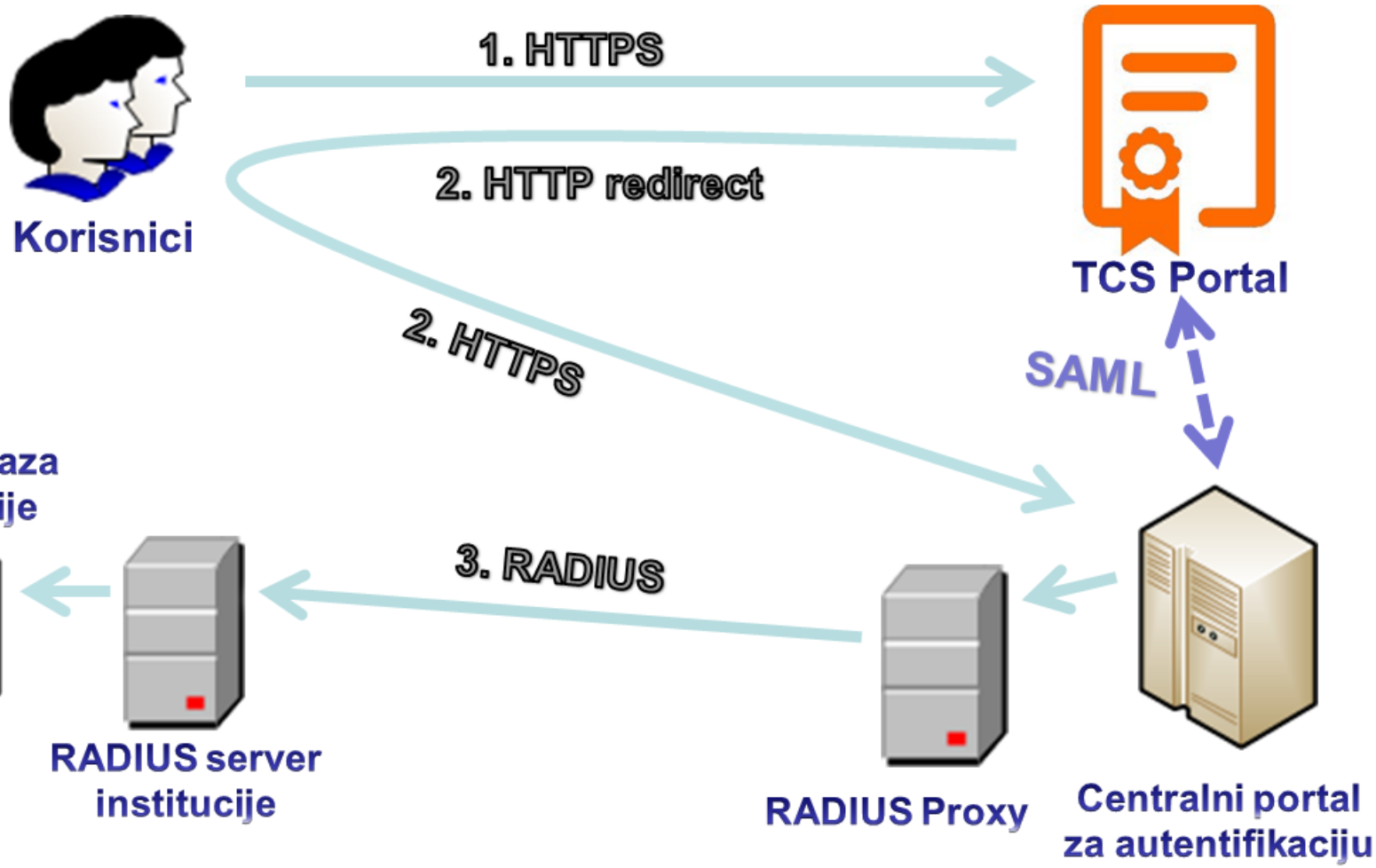
Prijavi

Upomoć! Zaboravio/la sam svoju lozinku.

Šteta! - Bez ispravnog korisničkog imena i lozinke ne možete pristupiti servisu. Da biste saznali vaše korisničko ime i lozinku obratite se vašoj matičnoj instituciji.

Autentifikacija na portal

KORAK 3



Autentifikacija na portal

KORAK 4

Korisnici

TCS Portal

Interna baza institucije

RADIUS server institucije

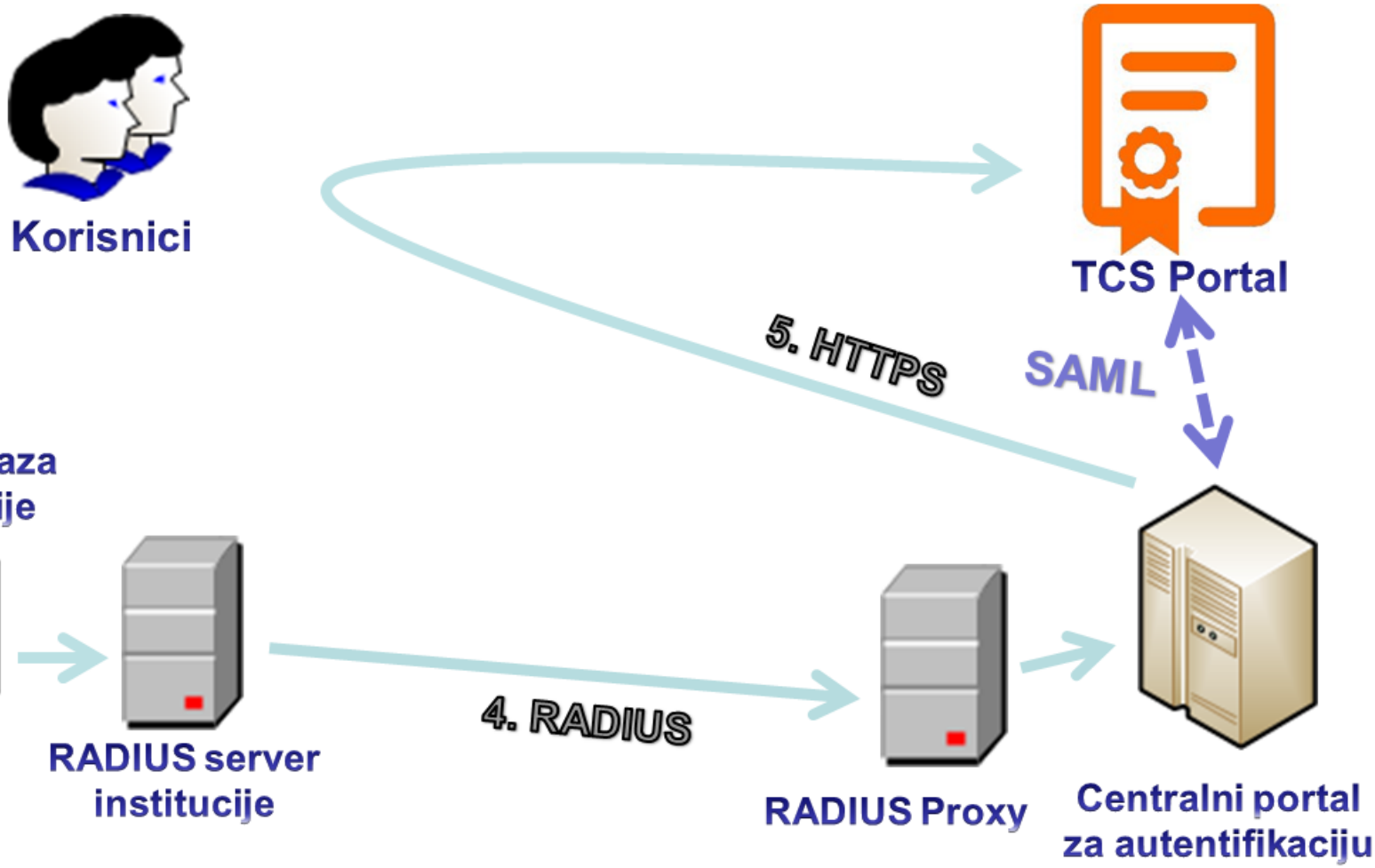
4. RADIUS

RADIUS Proxy

Centralni portal za autentifikaciju

Autentifikacija na portal

KORAK 5



AMRES TCS

TERENA Certificate Service

KRAJ

Sertifikati

Moji sertifikati

Pomoć

O NREN-u
O Portalu
Obaveštenje o privatnosti

Pomoć
CA Sertifikati

Prikaz menija

Korisnik
NREN-Admin

Odjavite se

Uspešno ste se prijavili na portal preko vaše matične institucije i sada možete koristiti ostale funkcije portala.

Molimo vas, NEMOJTE koristiti ovaj servis preko računara koji delite sa drugim ljudima. Vaš novi personalni sertifikat će biti smešten na ovaj računar.

Info about you

Ovo su informacije koje smo primili od vaše matične institucije u kombinaciji sa informacijama o vašem NREN-u (AMRES) i institucija (Akademska mreža Republike Srbije).

Ime:	Miloš Kukoleča
E-mail adresa:	milos.kukoleca@amres.ac.rs
Entitlement:	User
Jedinstveni identifikator:	kukolecha@amres.ac.rs
Matična organizacija:	Akademska mreža Republike Srbije
Zemlja:	SR
Org ID:	Akademska mreža Republike Srbije
NREN:	AMRES
Full-DN:	/C=SR/O=Akademska mreža Republike Srbije/CN=Miloš Kukoleča/unstructuredName=kukolecha@amres.ac.rs

Podaci u bazi institucije

- Jedinstveno korisničko ime
  - Forma korisničko_ime@domen_institucije.ac.rs
  - Primer mkukoleca@amres.ac.rs
  - Korisničko ime se upisuje u Subject polje sertifikata
- Ime institucije
  - Puno ime institucije
  - Primer „Akademska mreža Srbije“
  - Ime institucije se upisuje u Subject polje sertifikata

Podaci u bazi institucije (2)

- E-mail adrese
  - Jedan korisnik može imati više E-mail adresa
  - Servis ne prihvata mail adrese van „ac.rs“ domena
- Puno ime korisnika
  - Mora odgovarati imenu iz zvaničnog dokumenta izdatog od strane organa vlasti (lična karta, pasoš, vozačka dozvola)
  - Puno ime korisnika se upisuje u Subject polje sertifikata

Podaci u bazi institucije (3)

- Atribut dozvole pristupa
  - Skup karaktera koji definiše pravo korisnika da koristi servis izdavanja personalnih sertifikata
  - Atribut se dobija isključivo postupkom registracije !
  - Registracija: korisnik lično donosi administratoru ličnu kartu, pasoš ili vozačku dozvolu na uvid
  - Atribut administratora: „urn:mace:amres.ac.rs:amres:entitlemnt:confusa:Admin“
  - Atribut korisnika : „urn:mace:amres.ac.rs:amres:entitlemnt:confusa:User“
  - Jedna osoba (administrator) može imati oba atributa

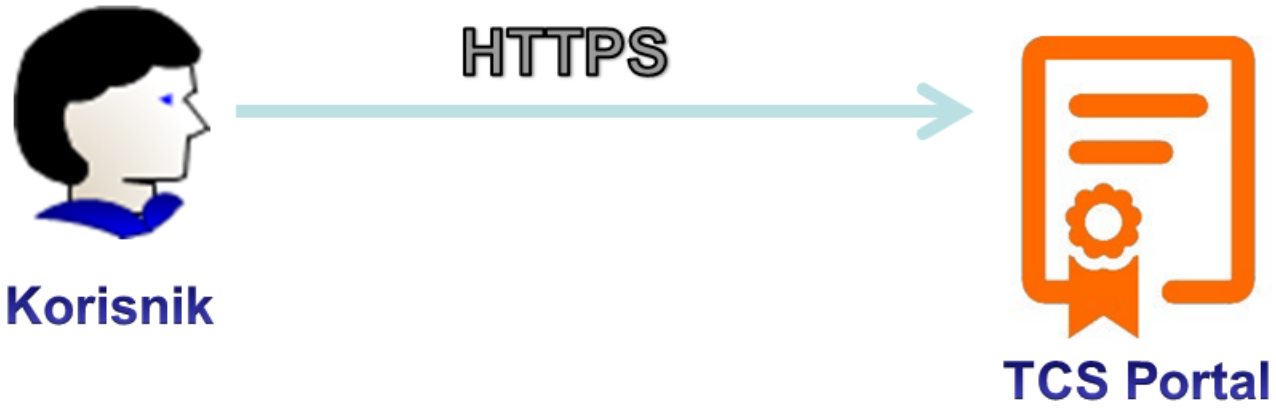
Proces izdavanja sertifikata

Korisnik

TCS Portal

Proces izdavanja sertifikata

KORAK 1



AMRES
TERENA Certificate Service
TCS

Sertifikati

*Moji sertifikati**

Pomoć

O NREN-u
O Portalu
Obaveštenje o privatnosti

Pomoć
CA Sertifikati

Prijavite se

KORAK 1

Ovaj servis vam omogućava da pribavite ili deaktivirate personalne sertifikate.
Da biste koristili ovaj servis, prethodno je neophodno da se prijavite na portal.

FAQ

Kako ovaj servis radi?

Koliko jedan sertifikat ima period važenja?

Zašto moram da se prijavim na portal?

Da li Confusa portal čuva moje lične podatke?

Šta znači ovo \'Confusa\' koje se pojavljuje svuda?

AMRES
TERENA Certificate Service
TCS

Sertifikati

Moji sertifikati

Pomoć

O NREN-u
O Portalu
Obaveštenje o privatnosti

Pomoć
CA Sertifikati

Prikaz menija

Korisnik
NREN-Admin

Odjavite se

KORAK 2

Uspešno ste se prijavili na portal preko vaše matične institucije i sada možete koristiti ostale funkcije portala.

Molimo vas, NEMOJTE koristiti ovaj servis preko računara koji delite sa drugim ljudima. Vaš novi personalni sertifikat će biti smešten na ovaj računar.

Info about you

Ovo su informacije koje smo primili od vaše matične institucije u kombinaciji sa informacijama o vašem NREN-u (AMRES) i institucija (Akademska mreža Republike Srbije).

Ime:	Miloš Kukoleča
E-mail adresa:	milos.kukoleca@amres.ac.rs
Entitlement:	User
Jedinstveni identifikator:	kukolecha@amres.ac.rs
Matična organizacija:	Akademska mreža Republike Srbije
Zemlja:	SR
Org ID:	Akademska mreža Republike Srbije
NREN:	AMRES
Full-DN:	/C=SR/O=Akademska mreža Republike Srbije/CN=Miloš Kukoleča/unstructuredName=kukolecha@amres.ac.rs

AMRES TCS
TERENA Certificate Service

Sertifikati

Moji sertifikati

Pomoć

O NREN-u
O Portalu
Obaveštenje o privatnosti

Pomoć
CA Sertifikati

Prikaz menija

Korisnik
NREN-Admin

Odjavite se

1. Slažem se sa pravilnikom o korišćenju (AUP)

KORAK 3

Pravilnik o korišćenju (AUP)

☑ ***Izjavljujem pod punom odgovornošću da ću poštovati sve obaveze korisnika koje su predočene u pravilniku ovog servisa i CPS dokumentu.***

manje informacija

AUP je deo CPS dokumenta koji propisuje skup uslova i obaveza koje korisnik treba da ispuni. Ovo uključuje:

- Zaštitite kredencijale naloga koje imate kod matične institucije (sekcija u CPS dokumentu 4.1.2)
- Zaštitite i čuvajte privatni ključ vašeg novog sertifikata na sigurnom mestu (sekcija u CPS dokumentu 4.1.2).
- Opozovite vaš sertifikat ukoliko je vaš privatni ključ kompromitovan (sekcija u CPS dokumentu 1.4.2).
- Ne koristite sertifikat na sistemu gde otkaz može dovesti do ozbiljne štete (sekcija u CPS dokumentu 1.4.2).
- Ne koristite sertifikat u bilo kojoj nezakonitoj transakciji (sekcija u CPS dokumentu 1.4.2).

< nazad dalje >

During this session, we had 11 individual DB-connections.

AMRES
TERENA Certificate Service
TCS

Sertifikati

Moji sertifikati

Pomoć

O NREN-u
O Portalu
Obaveštenje o privatnosti

Pomoć
CA Sertifikati

Prikaz menija

Korisnik
NREN-Admin

Odjavite se

3. Podnesite ili kreirajte vaš zahtev za sertifikat (CSR)

KORAK 4

više inforamcija

Generisanje preko Internet pregledača | Učitaj CSR | Kopiraj CSR

Generiši CSR u Internet pregledaču (*browser*)

*Pritisnite dugme "Dalje" **jedanput** kako biste generisali zahtev za sertifikat (CSR) u vašem Internet pregledaču (browser).*

Nekada je potrebno određeno vreme dok ne vidite reakciju vašeg Internet pregledača.

< nazad ***dalje >***

AMRES
TERENA Certificate Service
TCS

Sertifikati

Moji sertifikati

Pomoć

O NREN-u
O Portalu
Obaveštenje o privatnosti

Pomoć
CA Sertifikati

Prikaz menija

Korisnik
NREN-Admin

Odjavite se

4. Obrada zahteva za sertifikat koji je generisan preko Internet pregledača ('*browser*')

KORAK 5

Generiši CSR u Internet pregledaču (*browser*)

2048 (High Grade)

*Strogo je preporučeno da koristite veličinu ključeva **2048** bita. Molimo vas proverite veličine ključeva i kako su gradirani u vašem Internet pregledaču (browser)!*

Uzmite u obzir da ključevi kraći od 2048 bita će biti odbijeni od strane portala.

Polje 'Subject-DN' u sertifikatu će biti:

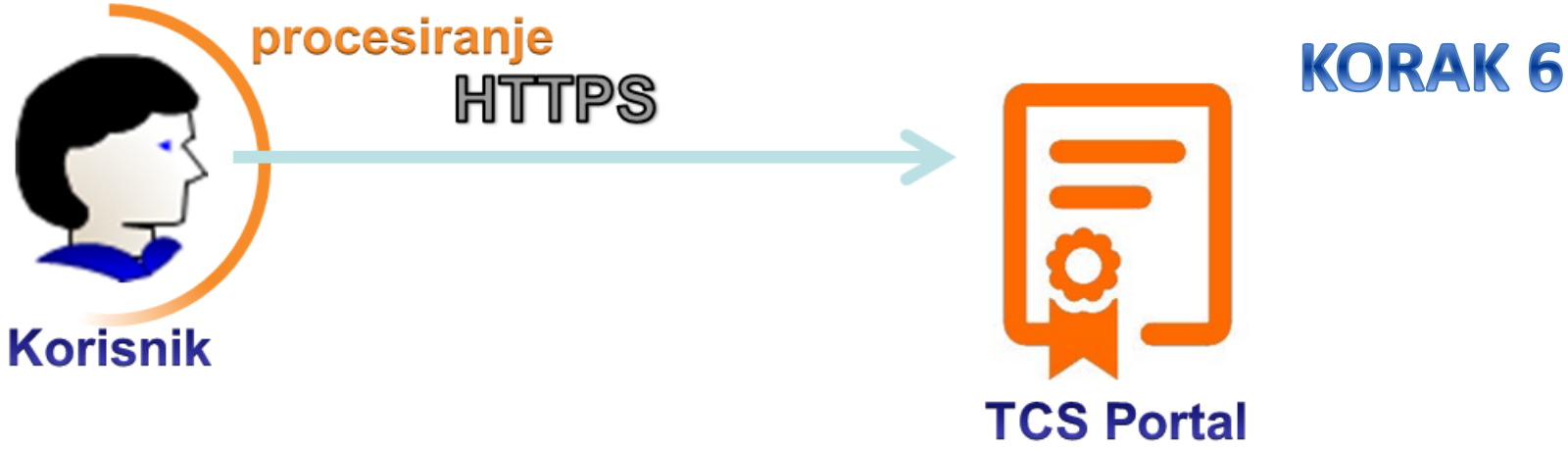
```
/C=SR/O=Akademska mreža Republike Srbije/CN=Miloš
Kukoleča/unstructuredName=kukolecha@amres.ac.rs
```

*Molimo vas pritisnite sledeće dugme samo **jedanput**.*

< nazad dalje >

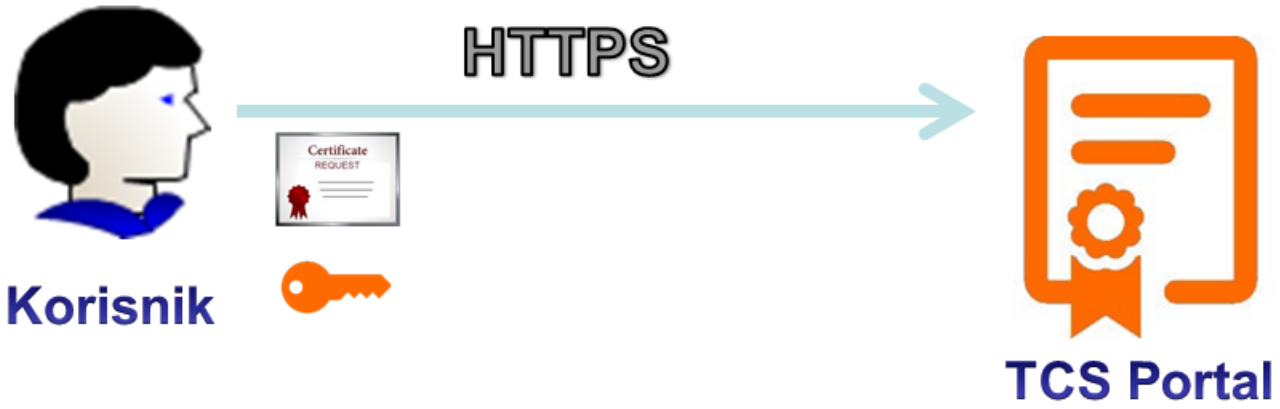
dalje

Proces izdavanja sertifikata



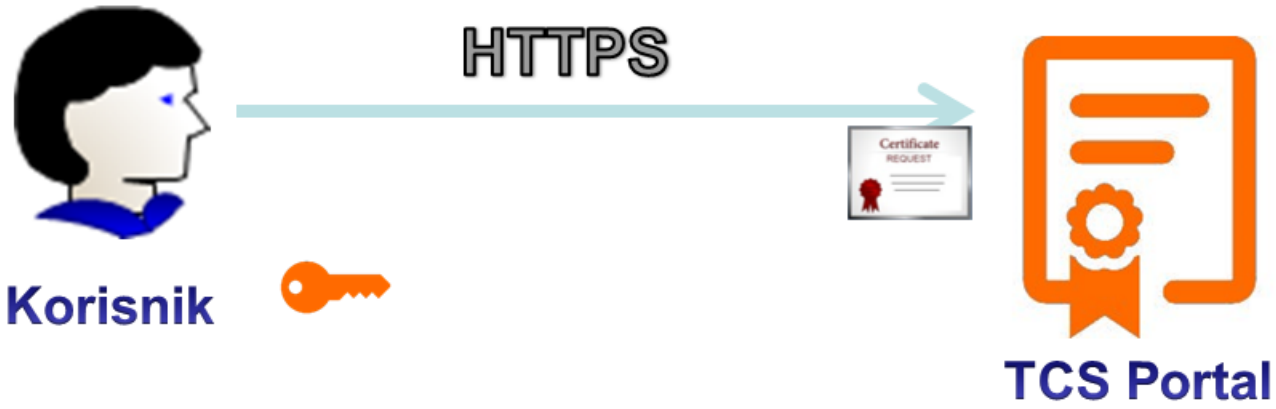
Proces izdavanja sertifikata

KORAK 6



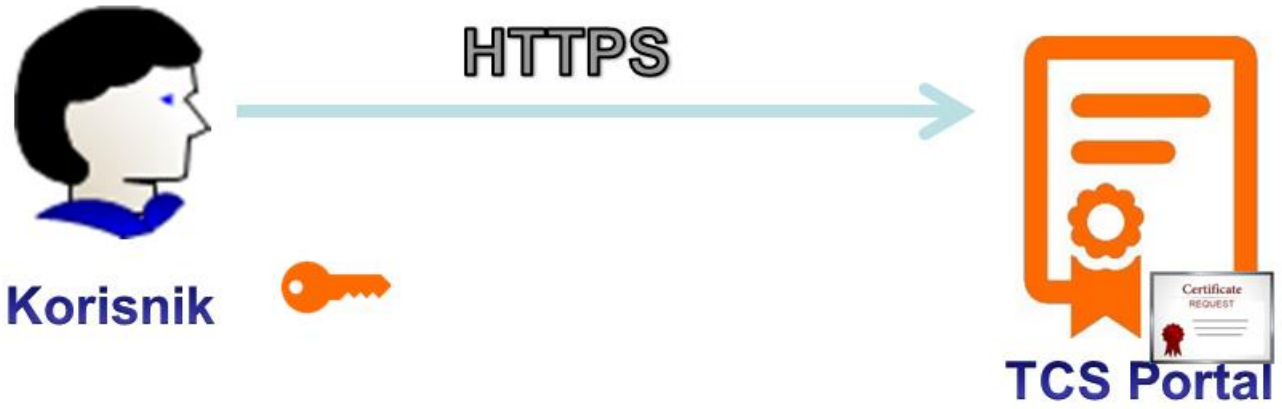
Proces izdavanja sertifikata

KORAK 7



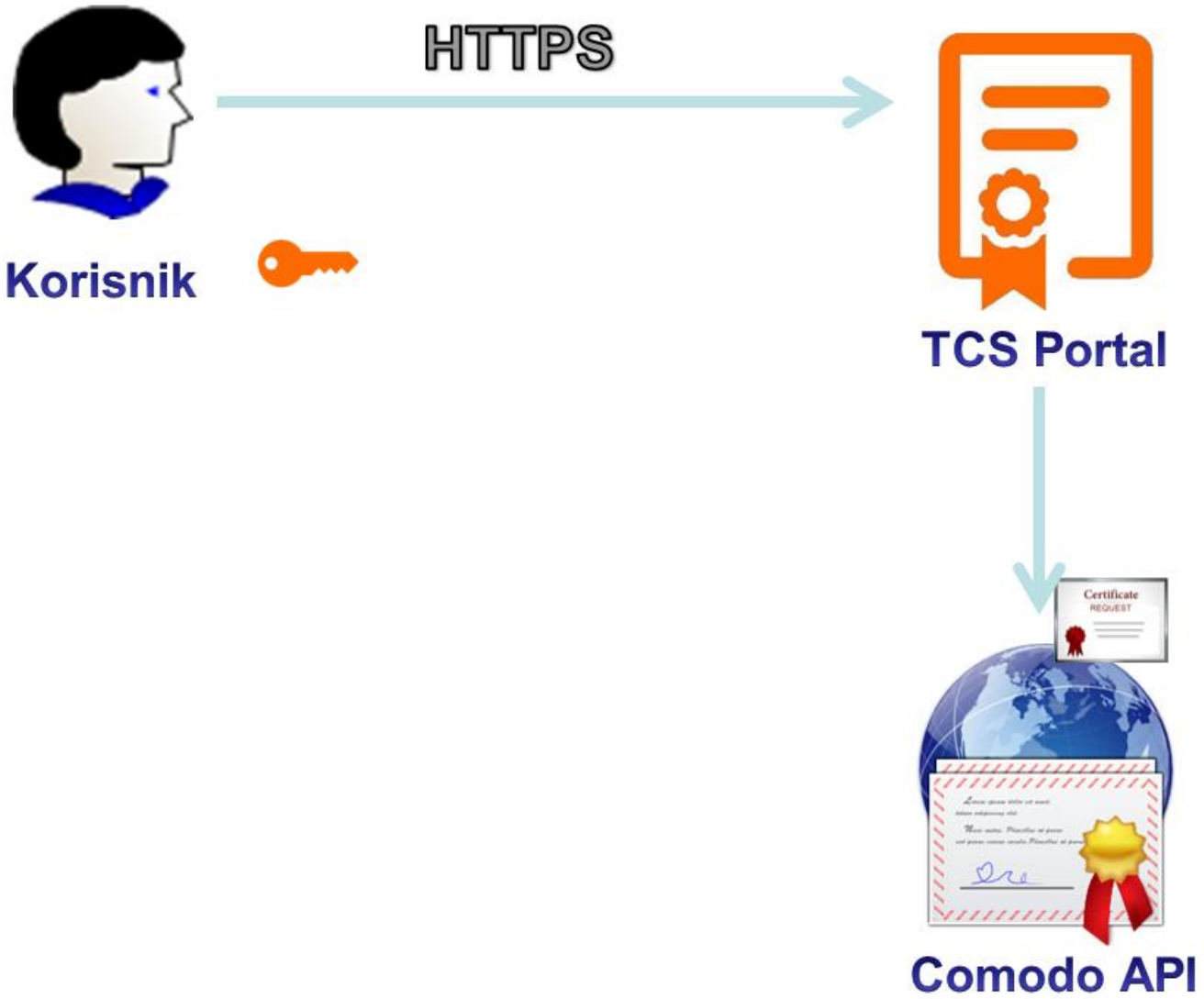
Proces izdavanja sertifikata

KORAK 7



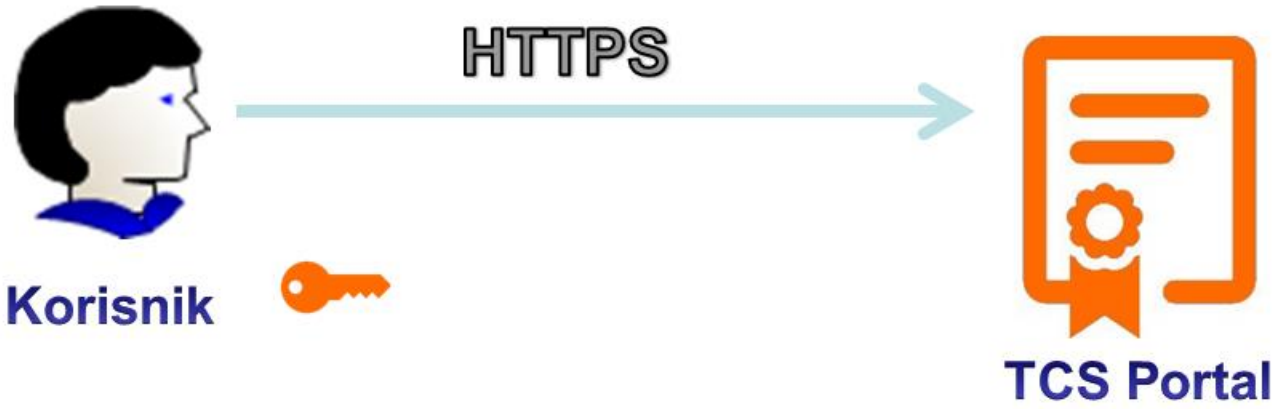
Proces izdavanja sertifikata

KORAK 8

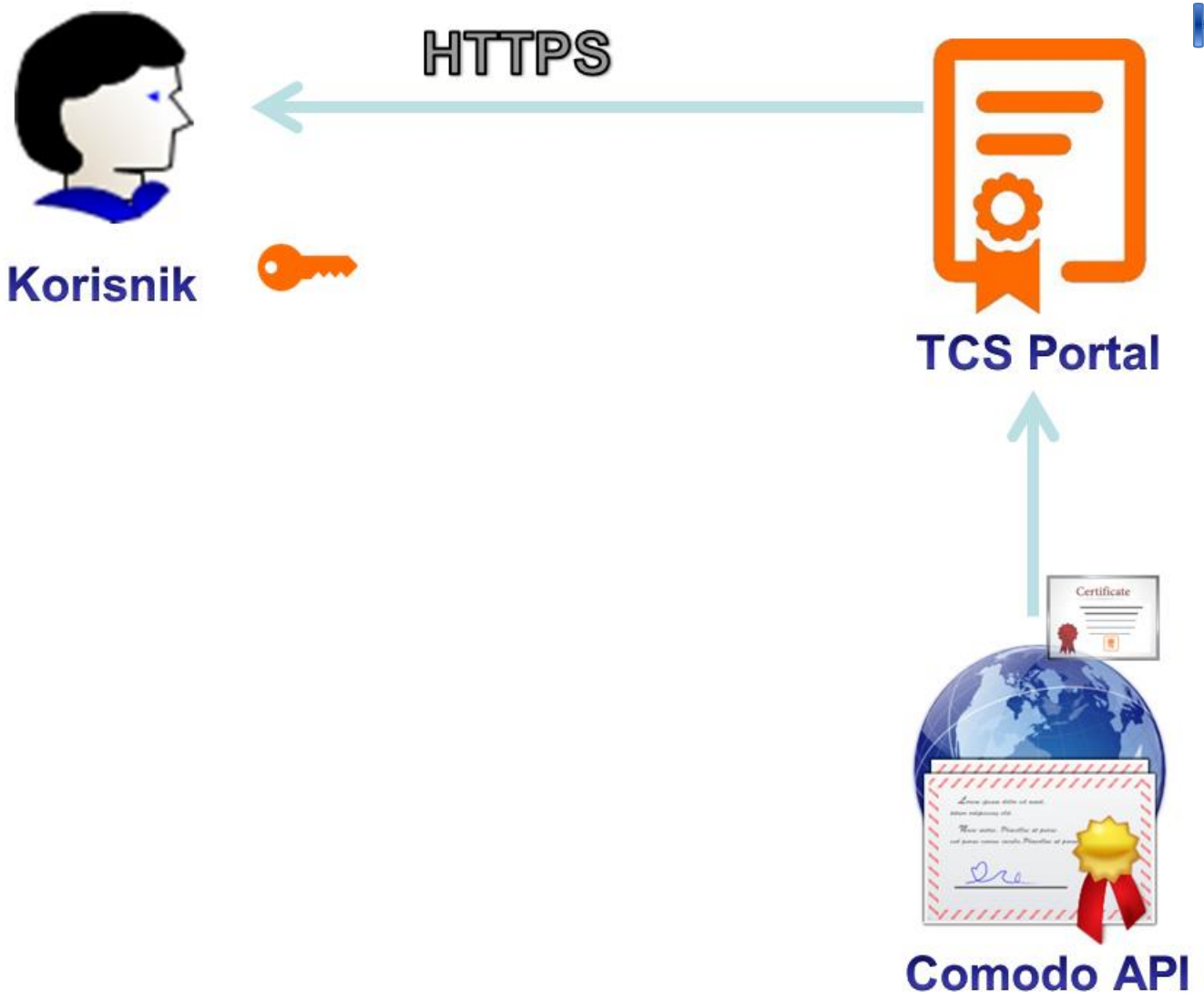


Proces izdavanja sertifikata

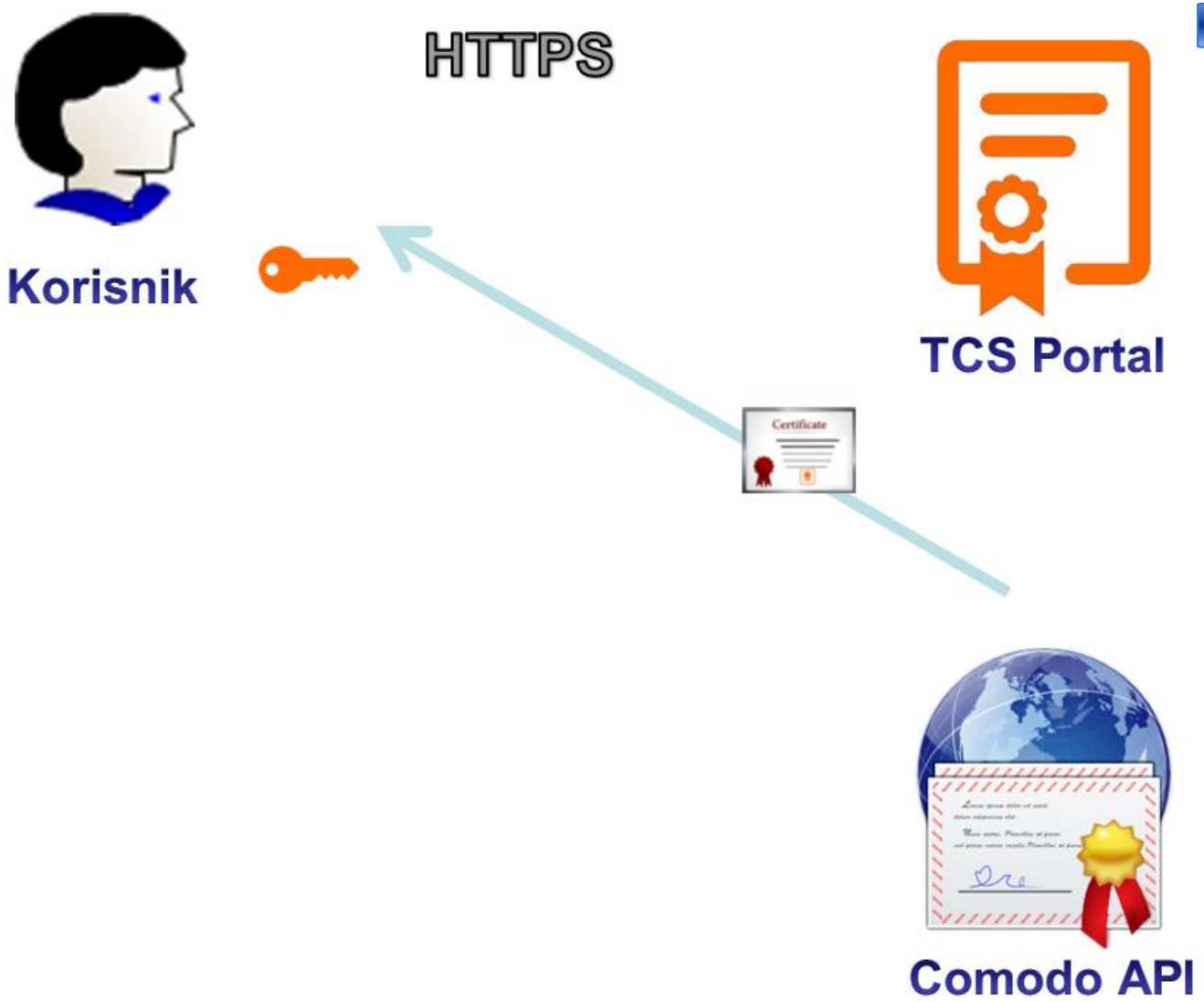
KORAK 9



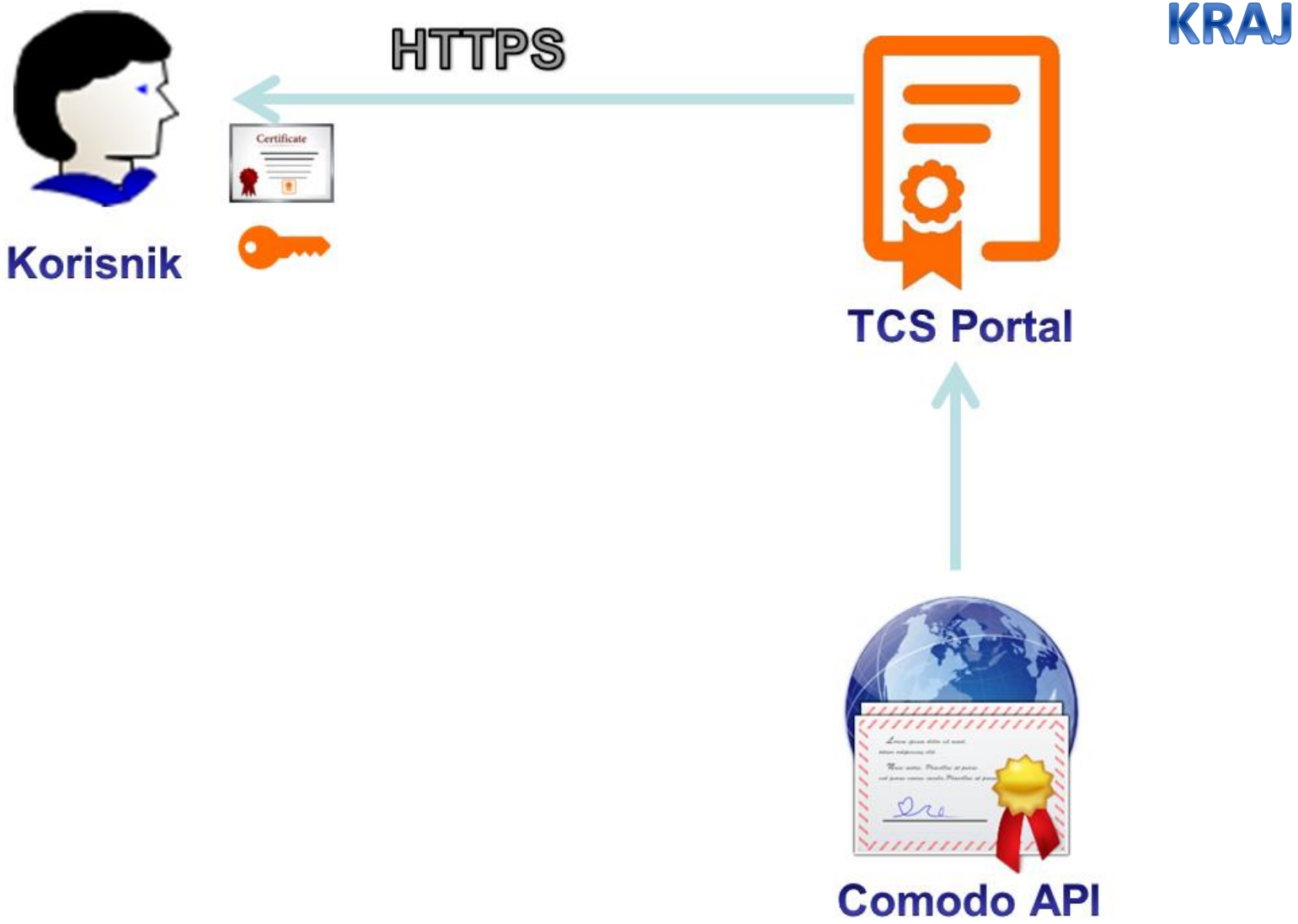
Proces izdavanja sertifikata



Proces izdavanja sertifikata



Proces izdavanja sertifikata



Pravilnik korišćenja servisa

- Prava institucije:
  - Institucija ima pravo da traži neograničen broj sertifikata za svoje korisnike
  - Administrator institucije ima pravo da opozove bilo koji sertifikat u okviru svoje institucije
- Obaveze institucije:
  - Institucija se obavezuje da neće koristiti sertifikat koji je istekao
  - Institucija se obavezuje da će povući sertifikat kada ustanovi da je došlo do kompromitovanja privatnog ključa
  - Sertifikat se ne sme koristiti za finansijske transakcije!

Povezivanje na servis

- Institucija mora postati deo iAMRES Federacije
- Institucija se mora upoznati sa Pravilnikom i pratećim TCS dokumentima
- Institucija mora potpisati, overiti i predati „Saglasnost za prijavu na servis izdavanja digitalnih personalnih sertifikata“
- AMRES kreira nalog administratora na portalu
- Institucija vrši registraciju korisnika za korišćenje servisa