

# AMRES usluga za izdavanje serverskih sertifikata



# AMRES

Akademski mreža Srbije

Jovana Palibrk

Sastanak administratora, Beograd, 12.12.2013.



# 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

---

- » 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**





# AMRES usluga za izdavanje serverskih sertifikata

---

AMRES

- » Registraciju institucije
- » Prijavljivanje za korišćenje TCS servisa
- » Kreiranje para ključeva i zahteva za sertifikatom (CSR zahtev)
- » **Podnošenje zahteva**





# Podnošenje zahteva

---

- ❧ Automatizovano izdavanje serverskih sertifikata - AMRES TCS portal
  - ❧ Svaka institucija ima profil - informacije o instituciji se preuzimaju iz baze registra domena ac.rs. U ime institucije mogu da se zahtevaju sertifikati isključivo za domene koji su registrovani.
  - ❧ Svaki administrativni i tehnički kontakt ima svoj nalog - informacije o korisniku se preuzimaju iz baze registra domena ac.rs. Za prijavljivanje na AMRES TCS portal korisnik koristi iste kredencijale koje ima na portalu registra domena ac.rs





# Podnošenje zahteva

---

- ❧ Ovlašćeno tehničko lice se uloguje na portal
- ❧ Odabere profil svoje institucije i pošalje CSR zahtev
- ❧ Prođe proceduru provere informacija iz CSR zahteva
- ❧ Na email tehničkog lica koje je podnelo zahtev šalje se potvrda slanja zahteva i linkovi za preuzimanje sertifikata.
- ❧ Povlačenje izdatog sertifikata može da izvrši samo ovlašćeni AMRES TCS administrator



# Vrste serverskih sertifikata (1)

---

- ❧ TERENA Single-Domain SSL sertifikati
- ❧ TERENA Multi-Domain SSL sertifikati
- ❧ **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
  - ❧ bilo-sta.rcub.bg.ac.rs
- ❧ **Sertifikati za ćirilčni, ак.срб domen**





## Vrste serverskih sertifikata (2)

---

- » DV (Domain Validated) sertifikati
- » OV (Organization Validated) sertifikati







## Vrste serverskih sertifikata (2)

---

- ❖ **DV (Domain Validated) sertifikati** - proverava se FQDN ime navedeno u CSR zahtevu putem Domain Control Validation (DCV) procedure:
  - ❖ Na osnovu FQDN imena iz CSR zahteva formira se lista generičkih email adresa. Primer liste generičkih email adresa:
    - ❖ administrator@fqdn.inst.bg.ac.rs
    - ❖ admin@fqdn.inst.bg.ac.rs
- Ili
  - ❖ administrator@inst.bg.ac.rs
  - ❖ admin@inst.bg.ac.rs





## Vrste serverskih sertifikata (2)

---

- ❖ **DV (Domain Validated) sertifikati** - proverava se FQDN ime navedeno u CSR zahtevu putem Domain Control Validation (DCV) procedure:
  - ❖ Na izabranu email adresu se šalje poruka sa jedinstvenim kodom i URL adresom do Comodo stranice na kojoj će biti izvršena provera
  - ❖ Unosom koda u označeno polje na navedenoj URL adresi izvršena je provera FQDN imena.
  - ❖ Svako FQDN ime iz zahteva za sertifikat treba da bude provereno na ovaj način





## Vrste serverskih sertifikata (2)

---

- » **OV (Organization Validated) sertifikati**
  - » Proverava se FQDN ime navedeno u zahtevu za sertifikat putem Domain Control Validation (DCV) procedure
  - » Proveravaju se podaci institucije putem procedure telefonske provere





# OV sertifikati - telefonska provera institucije

---

AMRES

- ❧ Registracija institucije u Poslovnom imeniku Telekomu Srbije, 11811.rs
- ❧ Prilikom podnošenja zahteva, između ostalog, navodi se broj telefona koji je registrovan u predhodnom koraku
- ❧ Putem email-a šalje se poruka sa URL adresom na Comodo serveru gde se nalazi uputstvo za dalje korake
- ❧ Putem telefona automat na engleskom jeziku diktira jedinstveni kod za proveru





# OV sertifikati - telefonska provera institucije

## Callback



### Callback Confirmation

Email Verification Code

We verified phone number "+38111 [redacted]" for your organisation.

Please provide your extension number (optional):

Note: Entering an extension may assist in ensuring that the callback makes it to you and can be completed.

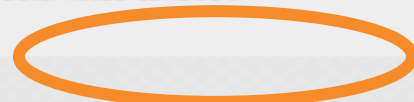
✓ This phone number is correct!

✗ This phone number is incorrect!

Note: This will initiate immediate automated callback.

Note: This will schedule automated callback for a later time.

Note: Use this option if you can't use automated callbacks.



Please initiate automated callback to continue.





# DV (Domain Validated) sertifikati

---

## ❖ Informacije:

- ❖ Common Name: fqdn2.amres.ac.rs
- ❖ Subject Alternative Names: fqdn2.amres.ac.rs
- ❖ Organization Unit: Domain Control Validated
- ❖ Valid From: December 10, 2013
- ❖ Valid To: December 10, 2016
- ❖ Issuer: TERENA SSL CA, TERENA
- ❖ Key Size: 2048 bit
- ❖ Serial Number: 123456abcdef





# OV (Organization Validated) sertifikati

---

## ❖ Informacije:

- ❖ Common Name: fqdn1.amres.ac.rs
- ❖ Subject Alternative Names: fqdn1.amres.ac.rs
- ❖ **Organization**: Akademska mreža Republike Srbije
- ❖ **Locality**: Beograd
- ❖ **State**: Srbija
- ❖ **Country**: RS
- ❖ Valid From: November 27, 2013
- ❖ Valid To: November 27, 2016
- ❖ Issuer: TERENA SSL CA, TERENA
- ❖ Key Size: 2048 bit
- ❖ Serial Number: abcdef123456





# Statistika

## 2011

TERENA Multi-domain SSL	26
TERENA Single-domain SSL	49
TERENA Wildcard SSL	1
Ukupno	76

## 2012

TERENA Multi-domain SSL	30
TERENA Single-domain SSL	24
TERENA Wildcard SSL	2
Ukupno	56

## 2013

TERENA Multi-domain SSL	12
TERENA Single-domain SSL	33
TERENA Wildcard SSL	3
Ukupno	48