Sveučilišta

NOVE GENERACIJE

PULA **6. - 8. 11. 2024.**

CARNET znanje povezuje
e-Sveučilišta
Financira Europska unija NextGenerationEU

Elektronička certifikacija (TCS)

Sadržaj

- O elektroničkim certifikatima
- Usluga elektroničkih certifikata (TCS)
  - Inicijalna prijava
  - ~~Sectigo sustav~~
  - **ACME i automatizacija**
- Praktični primjer(i)
- Pitanja i kontakt podaci

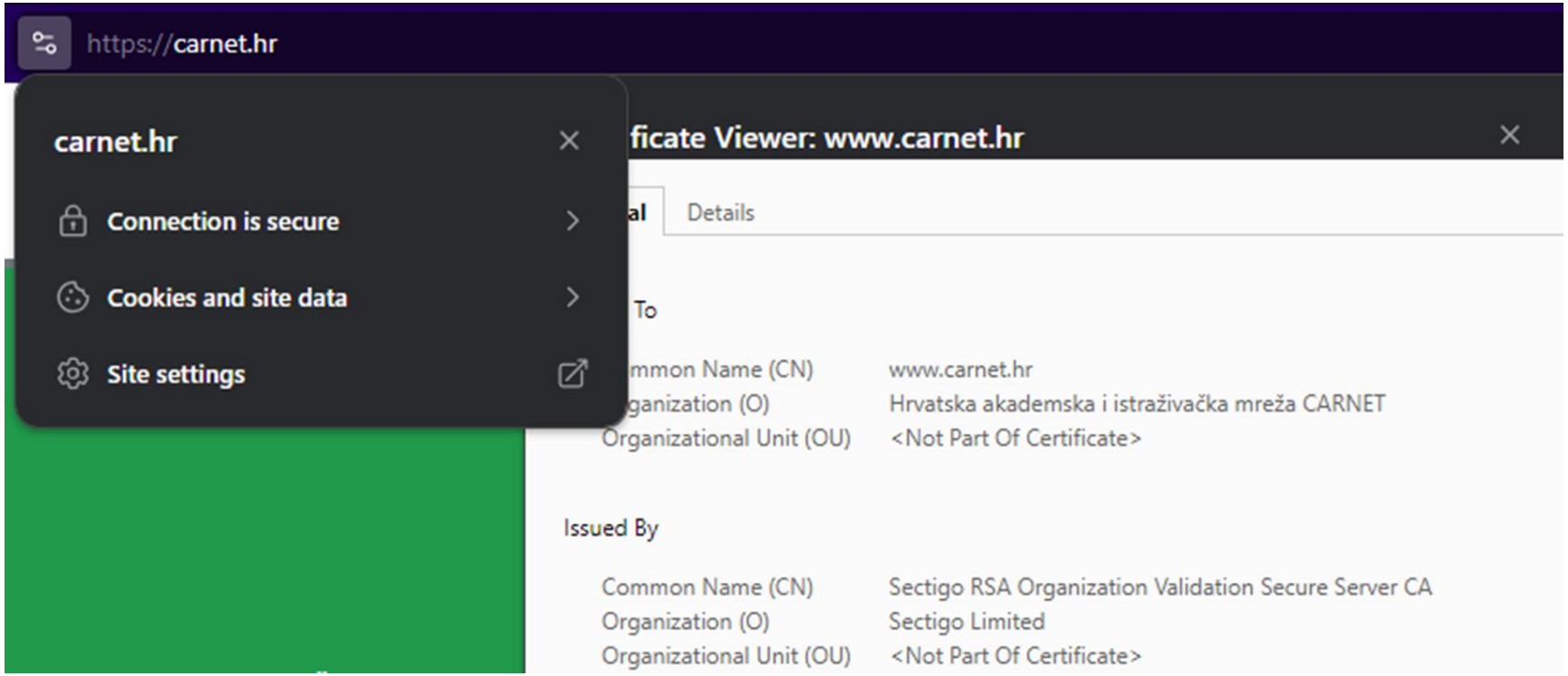
O elektroničkim certifikatima

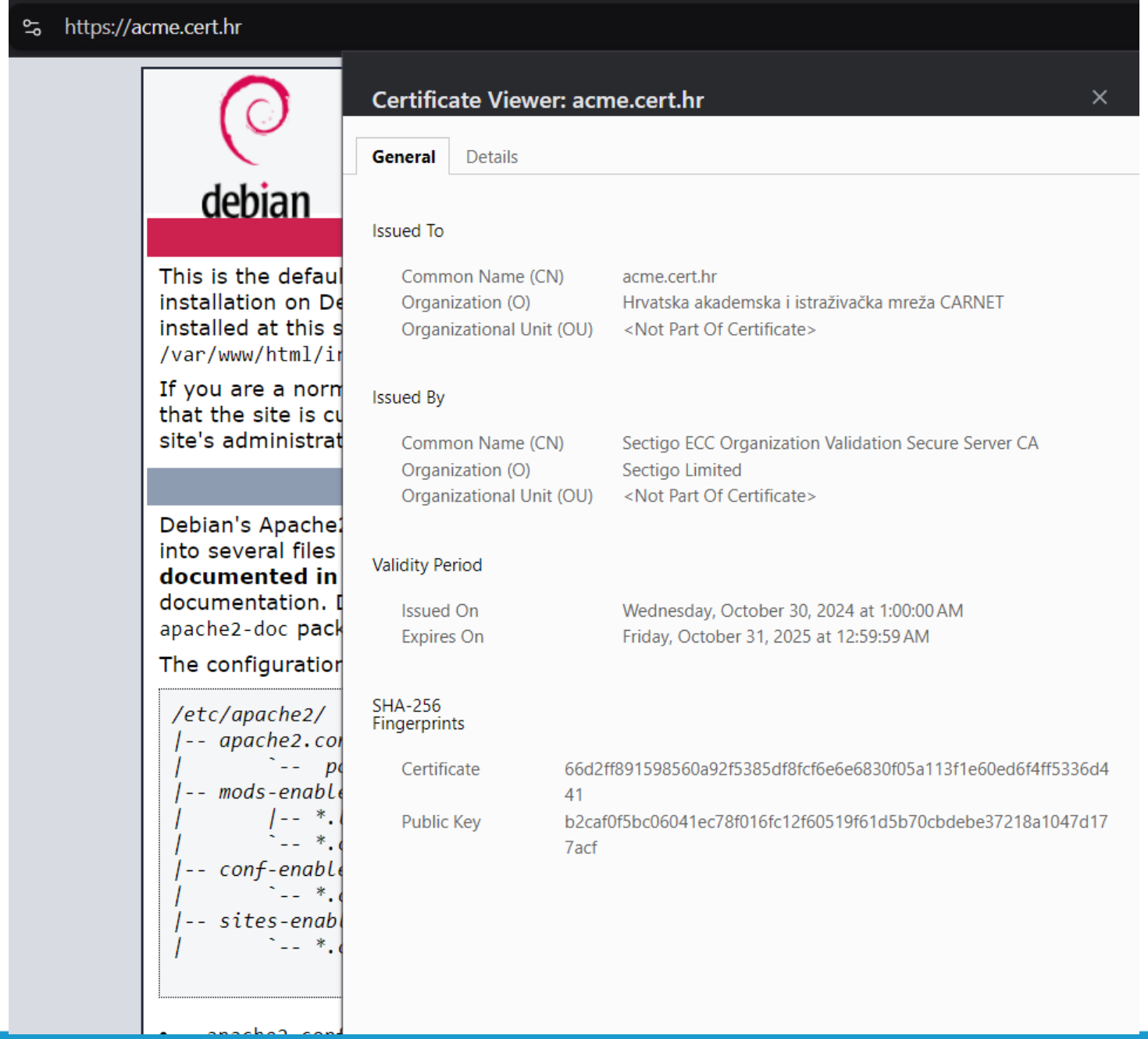
- datoteka povezana s kriptografskim parom ključeva
  - identifikacijski i potpisni dio
- autentifikacija identiteta i sigurna enkripcija
  - web stranice, osobe/korisnika, organizacije, uređaja ili servera
- temelj PKI-a
- povjerenje temeljeno na posredniku (Sectigo, Digicert i sl.)

O elektroničkim certifikatima

- namjene/vrste:
  - poslužiteljski (SSL), klijentski (S/MIME), Code Signing itd.

- prepoznati u svim mrežnim preglednicima
  - Google Chrome, Firefox, Microsoft Edge (Internet Explorer), Safari, Opera


https://carnet.hr
carnet.hr
Connection is secure
Cookies and site data
Site settings
ficate Viewer: www.carnet.hr
al
Details
To
mmon Name (CN) www.carnet.hr
ganization (O) Hrvatska akademska i istraživačka mreža CARNET
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) Sectigo RSA Organization Validation Secure Server CA
Organization (O) Sectigo Limited
Organizational Unit (OU) <Not Part Of Certificate>


https://acme.cert.hr
debian
This is the defaul
installation on De
installed at this s
/var/www/html/ir
If you are a norm
that the site is cu
site's administrat
Debian's Apache2
into several files
documented in
documentation. D
apache2-doc pack
The configuration
/etc/apache2/
|-- apache2.co
|-- mods-enable
|-- conf-enable
|-- sites-enab
Certificate Viewer: acme.cert.hr
General
Details
Issued To
Common Name (CN) acme.cert.hr
Organization (O) Hrvatska akademska i istraživačka mreža CARNET
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) Sectigo ECC Organization Validation Secure Server CA
Organization (O) Sectigo Limited
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Wednesday, October 30, 2024 at 1:00:00 AM
Expires On Friday, October 31, 2025 at 12:59:59 AM
SHA-256 Fingerprints
Certificate 66d2ff891598560a92f5385df8fcf6e6e6830f05a113f1e60ed6f4ff5336d441
Public Key b2caf0f5bc06041ec78f016fc12f60519f61d5b70cbdebe37218a1047d177acf

Usluga elektroničkih certifikata (TCS)

- **T**rusted **C**ertificate **S**ervice
  - https://certifikati.carnet.hr/
  - sve CARNET članice
  - registracija ustanove putem online obrasca
  - upute i procedure za administratore
  - prijava u **Sectigo** sustav

Radionica?

- SSL certifikat ~~395~~ 90 dana (vjerojatno početkom iduće godine)

- automatizacija upravljanja certifikatima
  - **ACME** protokol
    - Automatic Certificate Environment
    - CA (npr. Sectigo) i kor. server
    - autom. postavljanje PKI-a i HTTPS servera (pomoću CMA)

ACME

1. CMA dokazuje CA-u da web server zaista kontrolira domenu.
    1. Validacija domene (pomoću para ključeva prema CA).
    2. CA provjerava CMA (DNS zapis ili HTTP resurs pod poznatim URI-em).
    3. CA zadaje primjer na potpisivanje CMA-u kao potvrdu kontrole para ključeva.

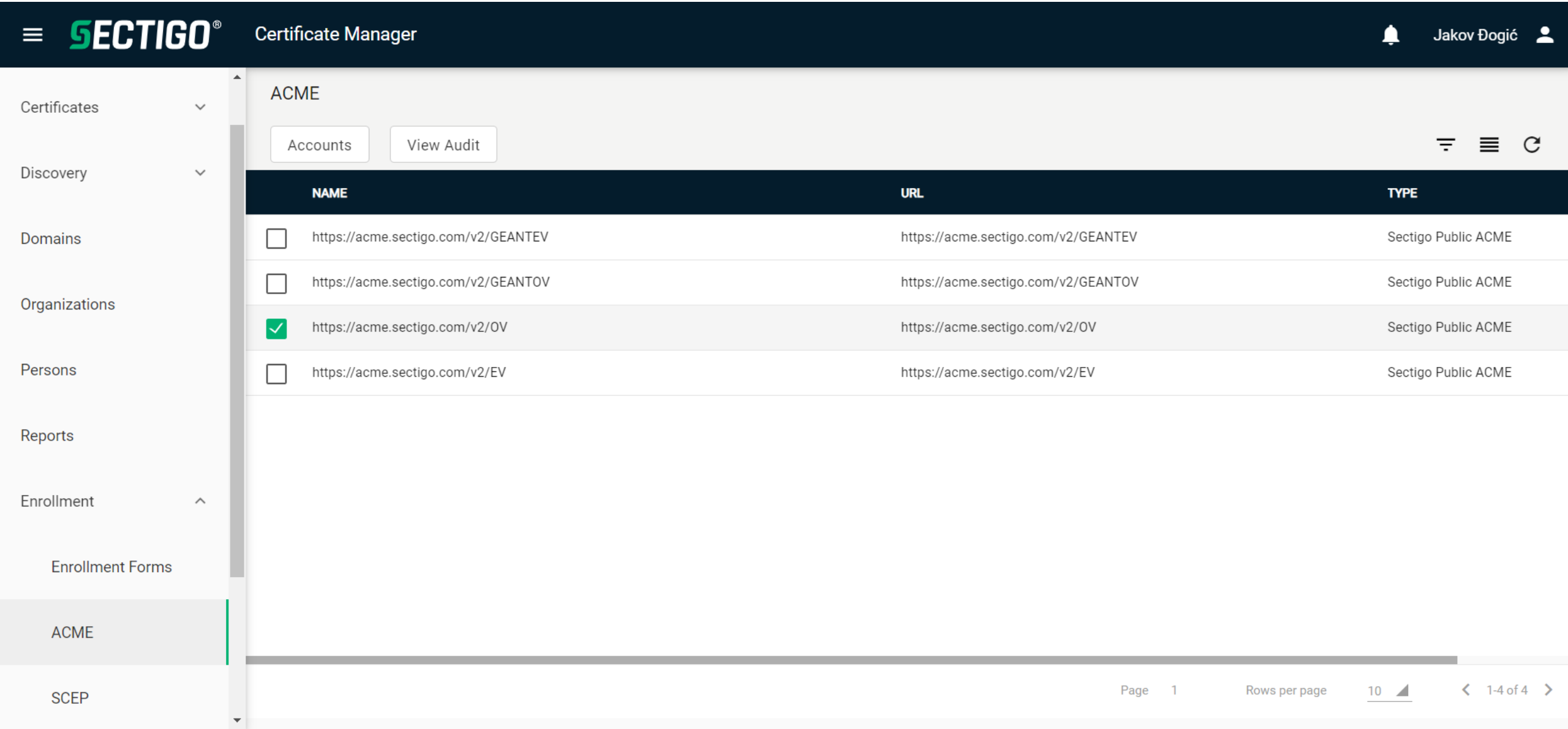
2. CMA traži, obnavlja i miče certifikate za navedenu domenu.

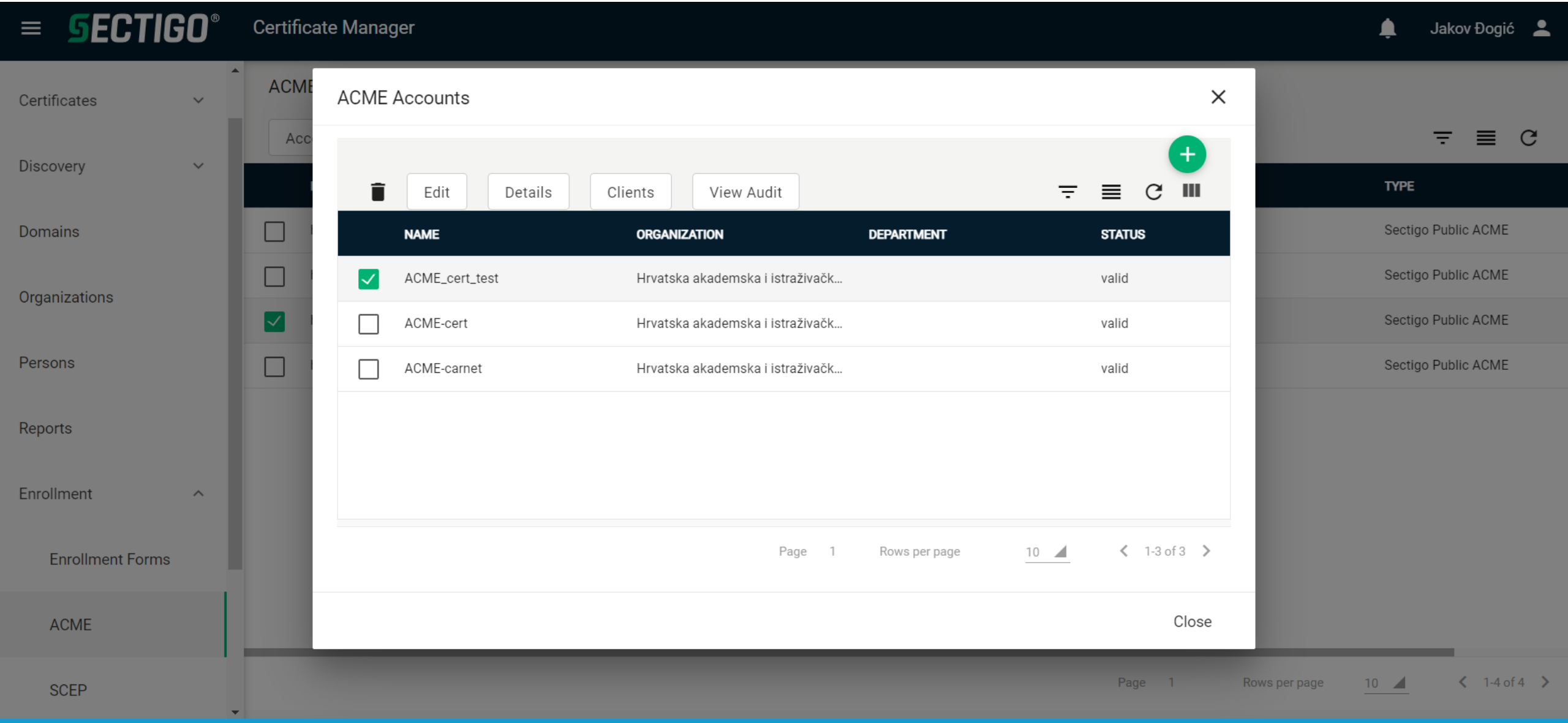
Praktični primjer(i)

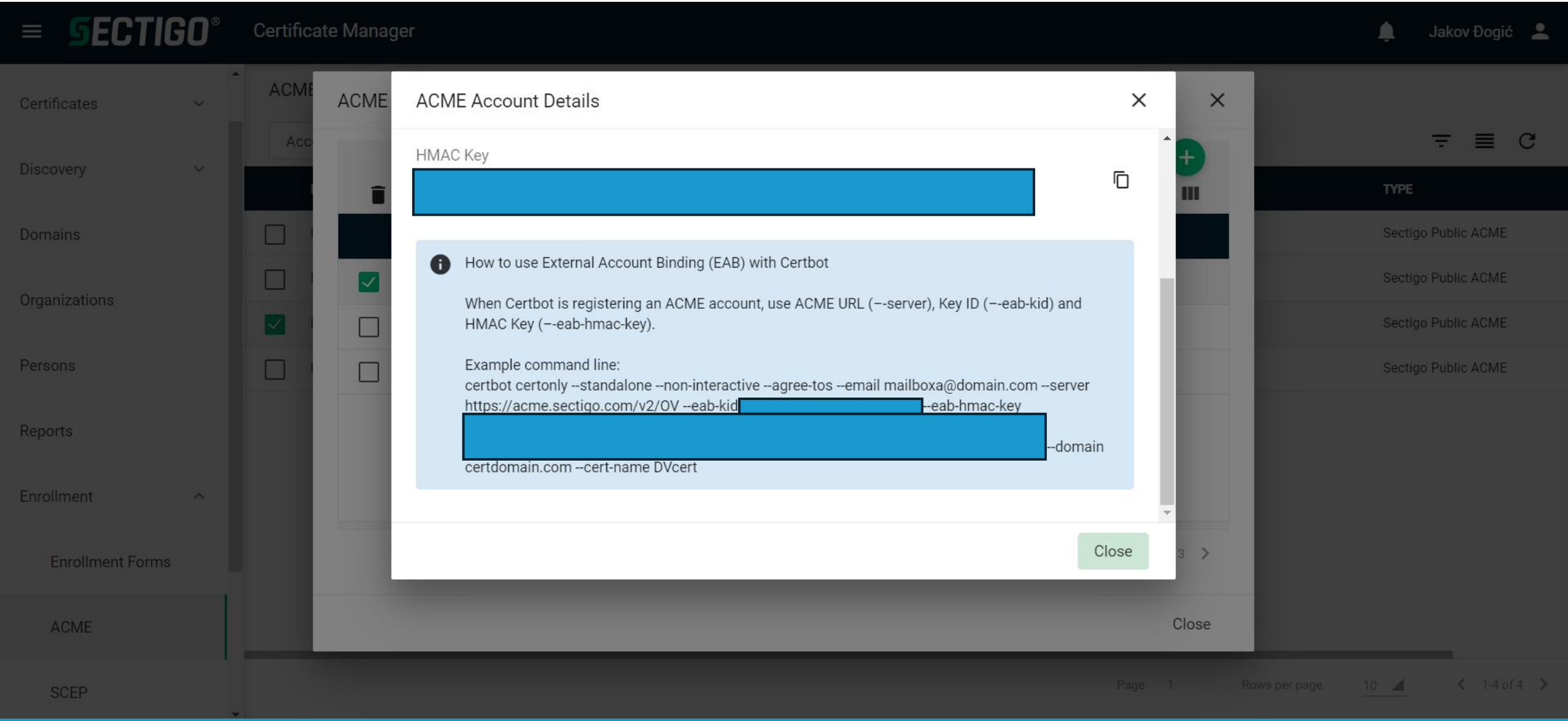
- instalacija certbota
  - `sudo apt install certbot`
  - symlink za systemd timer
    - `Created symlink /etc/systemd/system/timers.target.wants/certbot.timer → /lib/systemd/system/certbot.timer.`
  - instalacija dodatnih python3 paketa
    - `sudo apt install python3-certbot-apache`
    - `sudo apt install python3-certbot-nginx`

ACME profil na Sectigu

- Menu > Enrollment > ACME > https://acme.sectigo.com/v2/OV > Accounts > *odabir profila* > Details > How to use polje




SECTIGO
Certificate Manager
Jakov Đogić
Certificates
Discovery
Domains
Organizations
Persons
Reports
Enrollment
Enrollment Forms
ACME
SCEP
ACME Accounts
Edit
Details
Clients
View Audit
NAME
ORGANIZATION
DEPARTMENT
STATUS
ACME_cert_test
Hrvatska akademska i istraživačk...
valid
ACME-cert
Hrvatska akademska i istraživačk...
valid
ACME-carnet
Hrvatska akademska i istraživačk...
valid
Page 1
Rows per page 10
1-3 of 3
Close
TYPE
Sectigo Public ACME
Page 1
Rows per page 10
1-4 of 4


SECTIGO
Certificate Manager
Jakov Đogić
Certificates
Discovery
Domains
Organizations
Persons
Reports
Enrollment
Enrollment Forms
ACME
SCEP
ACME
ACME Account Details
HMAC Key
How to use External Account Binding (EAB) with Certbot
When Certbot is registering an ACME account, use ACME URL (--server), Key ID (--eab-kid) and HMAC Key (--eab-hmac-key).
Example command line:
certbot certonly --standalone --non-interactive --agree-tos --email mailboxa@domain.com --server https://acme.sectigo.com/v2/OV --eab-kid [redacted] --eab-hmac-key [redacted] --domain certdomain.com --cert-name DVcert
Close
Close
TYPE
Sectigo Public ACME
Sectigo Public ACME
Sectigo Public ACME
Sectigo Public ACME
Page 1
Rows per page 10
1-4 of 4

Korištenje certbota

- sudo certbot certonly --apache --non-interactive --agree-tos --email sysadm@carnet.hr --server https://acme.sectigo.com/v2/OV --eab-kid ~~REDACTED~~ --eab-hmac-key ~~REDACTED~~ --domain acme.cert.hr --cert-name acme.cert.hr
- Saving debug log to /var/log/letsencrypt/letsencrypt.log
- Plugins selected: Authenticator standalone, Installer None
- Requesting a certificate for acme.cert.hr

- IMPORTANT NOTES:
- - Congratulations! Your certificate and chain have been saved at:
- /etc/letsencrypt/live/acme.cert.hr/fullchain.pem
- Your key file has been saved at:
- /etc/letsencrypt/live/acme.cert.hr/privkey.pem
- Your certificate will expire on 2024-10-31. To obtain a new or
- tweaked version of this certificate in the future, simply run
- certbot again. To non-interactively renew *all* of your
- certificates, run "certbot renew"
- - If you like Certbot, please consider supporting our work by:

- Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
- Donating to EFF: https://eff.org/donate-le

dry-run provjera

- sudo certbot renew --dry-run

- Saving debug log to /var/log/letsencrypt/letsencrypt.log
- -
- Processing /etc/letsencrypt/renewal/acme.cert.hr.conf
- -
- Cert not due for renewal, but simulating renewal for dry run
- Plugins selected: Authenticator apache, Installer None
- Simulating renewal of an existing certificate for acme.cert.hr
- Performing the following challenges:
- http-01 challenge for acme.cert.hr
- Waiting for verification...
- Cleaning up challenges
- -
- new certificate deployed without reload, fullchain is
- /etc/letsencrypt/live/acme.cert.hr/fullchain.pem
- -
- Congratulations, all simulated renewals succeeded:
- /etc/letsencrypt/live/acme.cert.hr/fullchain.pem (success)

Provjera (i brisanje) certifikata

- `sudo certbot certificates`
- `sudo certbot delete --cert-name acme.cert.hr`

Pitanja publike @THECUC2024

- *cerbot* verzija/alternativa za Windows servere?
  - postoji verzija, **ALI** nije više podržana: https://certbot.eff.org/instructions?ws=other&os=windows
  - https://community.letsencrypt.org/t/certbot-discontinuing-windows-beta-support-in-2024/208101

  - alternative:
    - **win-acme**
      - https://www.win-acme.com/ (službeno podržava Win Server 2016 i iznad za .NET7)
    - popis ostalih preporuka: https://letsencrypt.org/docs/client-options/

Pitanja publike @THECUC2024

- Automatizacija certifikata za AOSI web servise? - Moguće
  1. Centralizirani *renew* certifikata
     - ACME klijent (npr. certbot)
  2. Sigurna pohrana certifikata u alatima za pohranu tajni
     - npr. HashiCorp Vault, AWS Secrets Manager, Azure Key Vault, Google Cloud Secret Manager, Kubernetes Secrets
  3. Distribucija certifikata prema AOSI node-ovima
     - koristeći sigurne API-eve (*ACME API, HashiCorp API, AWS* itd.) ili orkestracijske alate (Ansible, Kubernetes Operators
  4. Automatizirana nadogradnja
     - pokretanje automatskog ponovnog učitavanja konfiguracije ili ažuriranja vremena izvođenja u AOSI uslugama
  5. Validacija
     - alatima za nadzor provjerava se sve node-ove/servise za obnovljenim certifikatima

Kontakt:

tcs-ra@carnet.hr

certifikati.carnet.hr

ncert@cert.hr

CARNET

CERT.hr

Sektor Nacionalni CERT

Josipa Marohnića 5

10000 Zagreb

Hrvatska