Securing Service Access with Digital Certificates

Jovana Palibrk, AMRES

NA3 T2, Tbilisi, December 2013.

Agenda

- Theory
  - Cryptographic Protocols and Techniques
  - Public Key Infrastructure
- TERENA Certificate Service (TCS)
- AMRES Certificate Service

Secure communication

- Confidentiality of data – Cryptographic Systems

  ensures that the data or the content of a message is only available to the intended recipients

- Integrity of data – Hash Functions

  guarantees that there has been no change to the data or the content of a message on its way from the source to the destination

- Authentication – Digital Sugnatures

  process of establishing the identity of the end users in communication

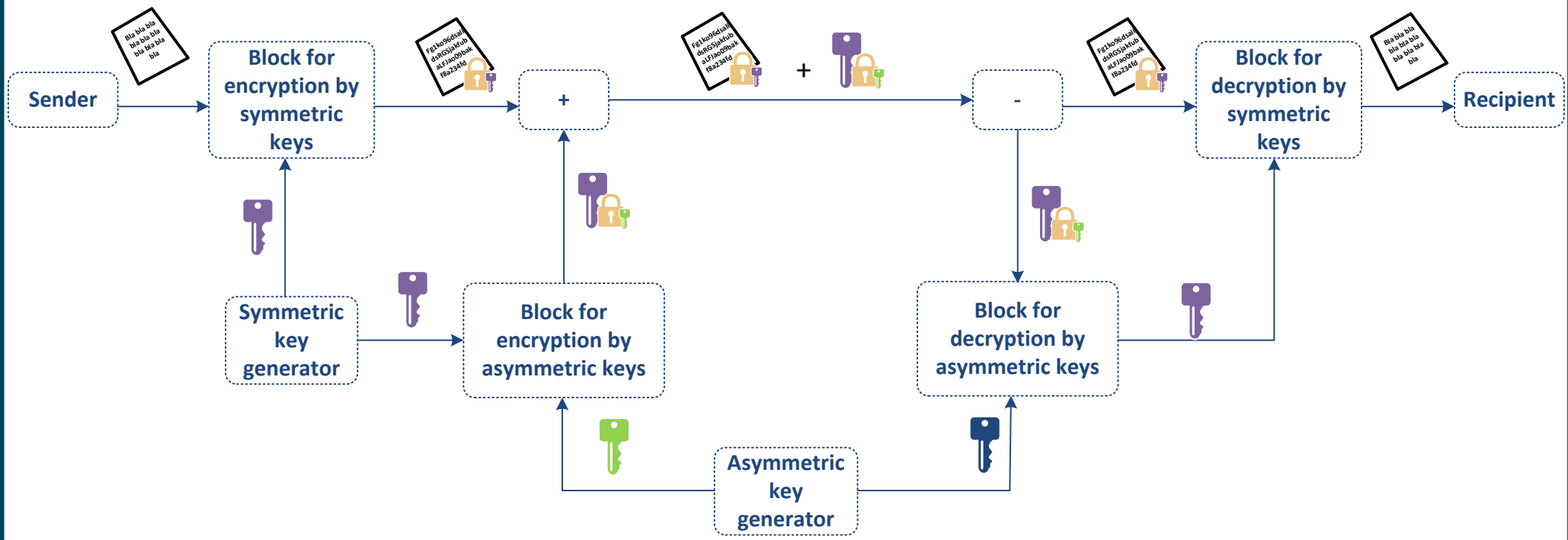
Cryptographic Systems

- Only the participants in the communication (the sender and the recipient) should be able to understand a communication whose confidentiality or integrity is preserved.
- The confidentiality of communication is achieved by way of encryption of the messages.
- Cryptographic systems:
  - Symmetric-key encryption systems
  - Asymmetric-key encryption systems

Cryptographic Systems

- New systems are established by applying asymmetric key-encryption system on specific part of the message, on a key or another important part of communication :
  - Combined encryption systems
  - Digital signatures
  - Digital certificates

Cryptographic Systems
Combined Encryption Systems



Symmetric key

Recipient's public key

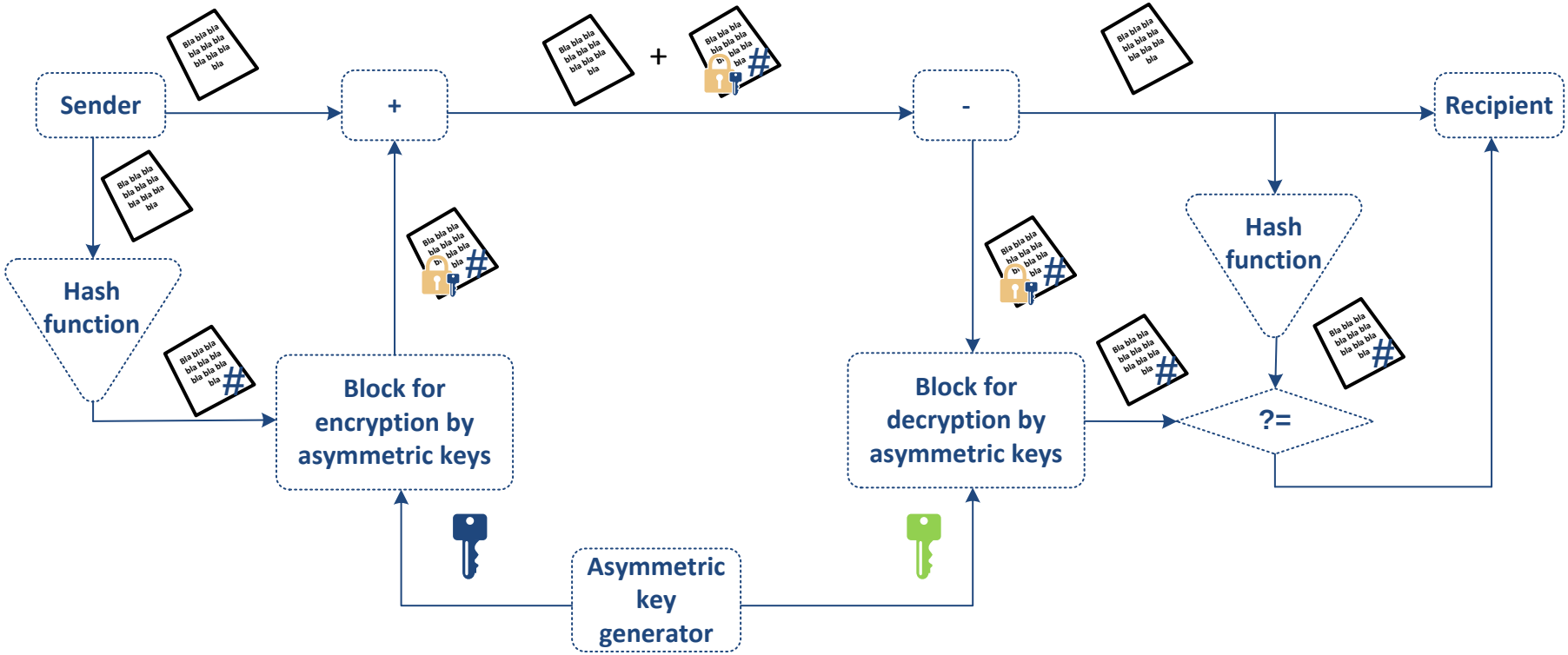
Recipient's private key

Encrypted symmetric key

Encrypted message

Original message

Cryptographic Systems
Digital Signature



Original message

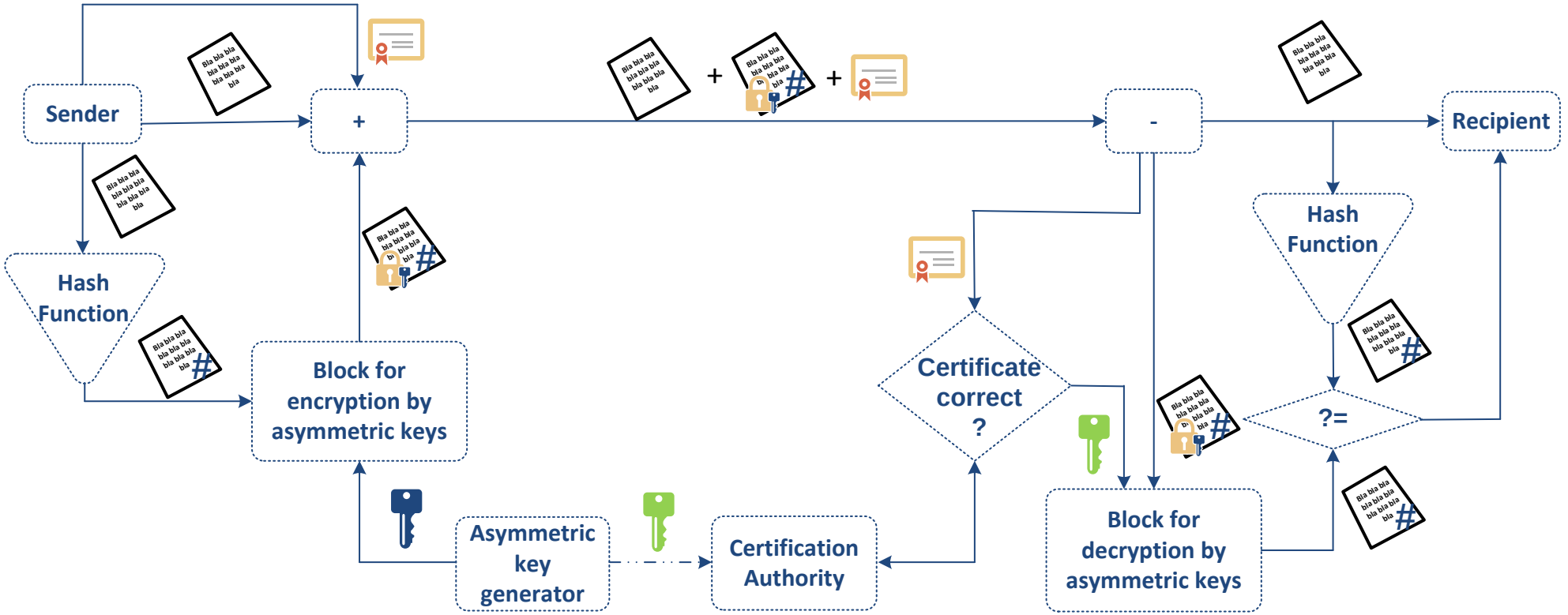
Hash of the message

Encrypted hash

Sender's public key

Sender's private key

Cryptographic Systems
Digital Certificates



Digital certificate

Public Key Infrastructure – PKI

- Infrastructure with following elements was needed:
  - Registration and application process for certificate issuing
  - Verification of registered user's identity
  - Issuance and renewal of the certificate
  - Delivery of certificates
  - Revocation of certificates
- Solution: public key infrastructure
- The PKI is comprised of the hardware, software, policies and procedures needed to manage, generate, store, distribute, use and revoke cryptographic keys and digital certificates.

PKI – Components

- **Certification Authority (CA)** – a trusted authority, that issues and revokes digital certificates and undertakes a complete check of the data of the owner/end entity for whom the request for issuing the certificate has been submitted

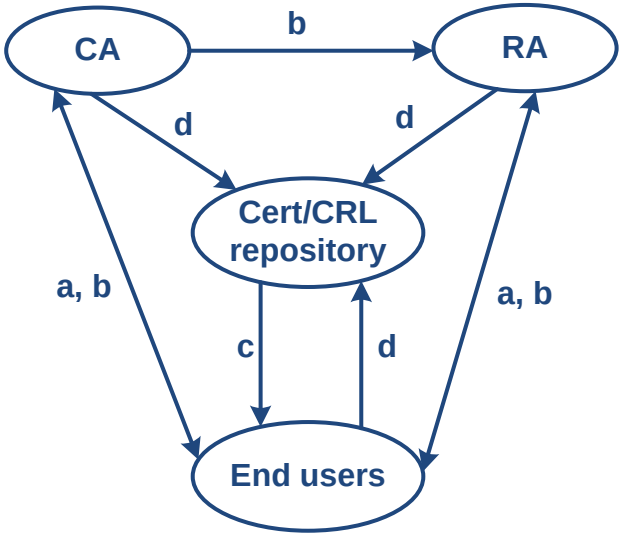
- **End entity** – end user (an individual) or legal entities that request the certificates using PKI infrastructure

- **Registration authority (RA)** – responsible for identification and authentication of subjects of digital certificates

- **Repository** – a database and/or folder that contains basic documents on the work of the specific CA, i.e. information related to certificates and Certificate Revocation List (CRL).

PKI – Components

- The relationship between the PKI elements



a – initial registration/certification
b – renewal of the key pair
renewal of the certificate
request for revoking the certificate
c – verification of the certificate
d – publication of the certificate

PKI – Basic function

- **Registration** – institutions/end users first need to go through a process of application that includes verification of their identity and exchange of information with the appropriate component of the infrastructure – the Registration Authority (RA). The appropriate level of verification is defined for each type of certificate by a document called the certificate policy

- **Initialisation** – The representative of an institution/end user and the CA exchange the information necessary for further communication

- **Certification** – The certification process involves the issuance and delivery of certificates to the representatives of an institution/end user and is conducted by the CA

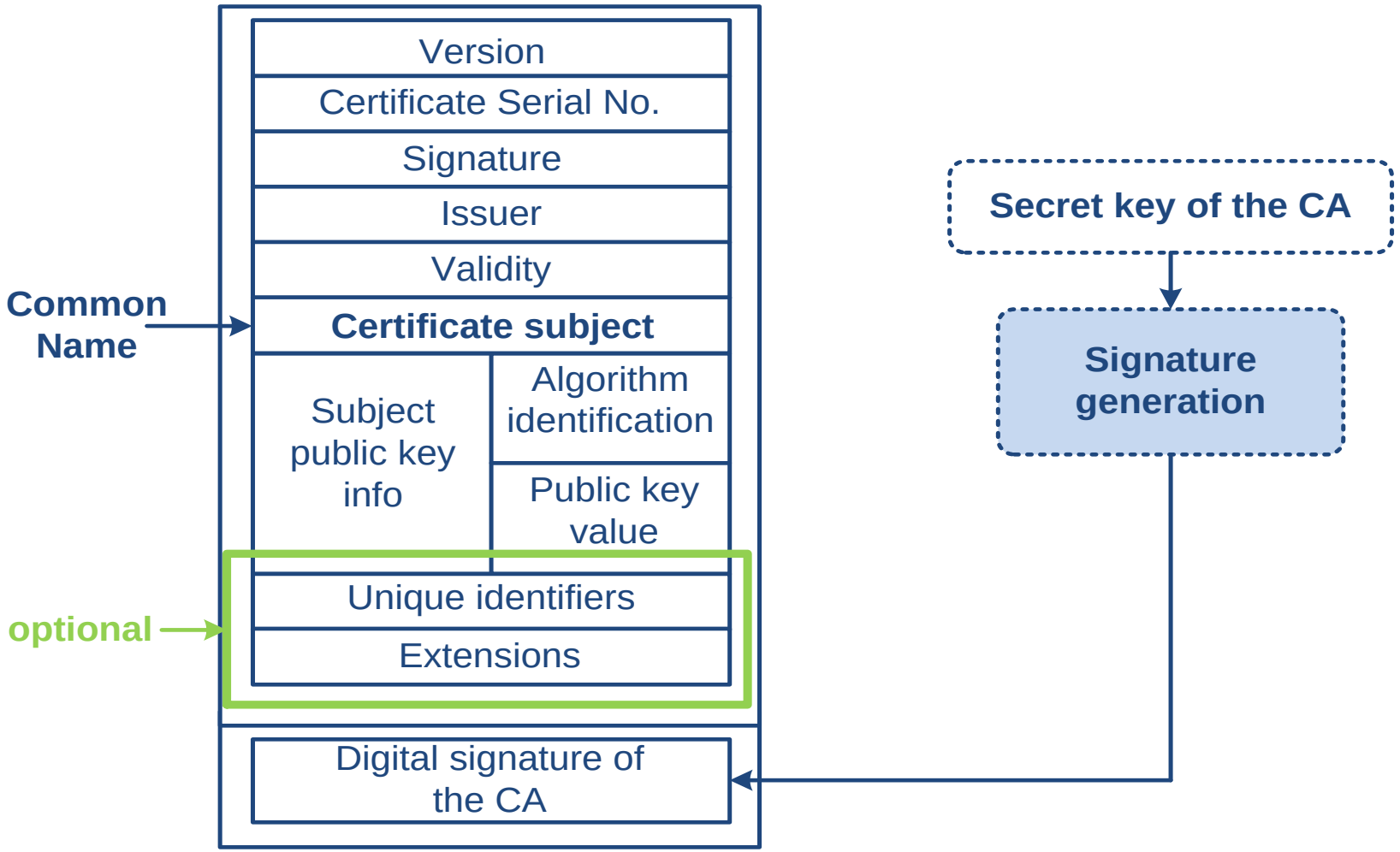
PKI – Basic function

- **Revocation of a certificate** – The revoked certificate is included in the Certificate Revocation Lists (CRLs) published by the CA that issued the certificate. The revoked certificate is listed in repository.

- **Verification of the chain of trust** – the signatory of a message may provide a chain of certificates, where each certificate is signed by the certificate of the superior CA. This requires verification of the chain of trust and the validity of each certificate contained in the chain. Is the given certificate trusted? Is the certificate actually signed by the specific CA?

- **Verification of the validity of a certificate** – Verification of the validity of each individual certificate needs to provide answers on whether the specific certificate has expired and whether the certificate is still valid or has been revoked.

The format of digital certificate



TCS – TERENA Certificate Service

TCS – TERENA Certificate Service

- TCS issues digital certificates to scientific, research and education institutions through their National Research and Education Networks (NRENs).
- TERENA – certification authority
- NREN – registration authority
- TCS certificates are issued by Comodo CA Limited

TCS – TERENA Certificate Service

- TCS offers five different types of digital certificates:
  - **Server SSL Certificate –** an SSL certificate for authenticating servers and establishing secure sessions with end clients
    - ***Single-Domain SSL Certificate*** *– this type of certificate is linked to only one registered DNS name of the server, which is included in the certificate as the value in the CN (Common Name) attribute*
    - ***Multi-Domain SSL Certificate*** *– this type of certificate secures more than one (maximum 100) registered DNS name s of the server*
    - ***Wildcard SSL Certificate*** *– one certificate allows for an unlimited number of subdomains located on different physical machines (servers). For instance, Wildcard certificate for amres.ac.rs (*amres.ac.rs in certificate) can be used for:*
      - *mail.amres.ac.rs*
      - *www.amres.ac.rs*
      - *radius.amres.ac.rs*
      - *anything.amres.ac.rs*

TCS – TERENA Certificate Service

- TCS offers five different types of digital certificates:
  - *Personal Certificate*
  - *e-Science Server Certificate*
  - *e-Science Personal Certificate*
  - *Code-signing Certificate*

- From 1 February 2013:
  - DV (Domain Validated) certificates
  - OV (Organization Validated) certificates

TCS – TERENA Certificate Service

- The certificates obtained using the TCS are signed by the **TERENA CA** certificate,
  - which is further signed by **UserTrust**, an intermediate CA, certificate **UTN-USERFirst-Hardware,**
    - which in turn is signed by the **AddTrust External Root CA.**

AMRES Certificate Service

AMRES Certificate Service

- Using TERENA Certificate Service AMRES offers following types of certificates to its users:
  - **Server SSL Certificate**
    - ***TERENA Single-Domain SSL certificate***
    - ***TERENA Multi-Domain SSL certificate***
    - ***TERENA Wildcard SSL certificate***
  - **Certificates for Cyrillic domain, ак.срб domain**

AMRES Certificate Service

- AMRES certificate service offers following types of certificates to its users:
  - **Personal certificates** – we are working on infrastructure for issuing personal certificates:
    - *AMRES identity federation*
    - *Confusa, open source application for handling personal certificates, developed by UNINET*

- Separate infrastructure for issuing e-science server and e-science personal certificates for protection and access to GRID infrastructure, established through AEGIS CA, University of Belgrade Computing Center.

  http://aegis-ca.rcub.bg.ac.rs/documents/AEGIS-C

Services that need to be secured with digital certificates

- Authenticating servers
  - Web server
  - RADIUS server – eduroam
  - Email server
- Authenticating end users
- The secure exchange of e-mails
- Establishing an IPsec/TLS VPN tunnel

AMRES Certificate Service

- Registering an institution
- Application for using AMRES certificate service
- Creating a pair of keys and a certificate signing request
- Submitting the request

AMRES Certificate Service – Registering an institution

- Registration is performed through the ac.rs Domain Registry portal
- An institution is considered registered with the ac.rs if it has at least one domain registered with the ac.rs Domain Registry
- The registered institution can, apply for using the AMRES certificate service
- The data about the institution must be accurate and up-to-date - state registries of companies

AMRES Certificate Service – Application for using AMRES certificate service

- **Certificate Practice Statement** - basic preconditions for the use of digital certificates
- **TCS Terms of Use Agreement -** filled in and signed by the authorized person
- When signing the document, the institution appoints a person who needs to be familiar with *Certificate Practice Statement* and who will act as its administrative contact for the procedures of requesting, obtaining, renewing and revoking digital certificates

AMRES Certificate Service – Creating a pair of keys and a certificate signing request

- CSR – *Certificate Signing Request*

- The creation of the CSR is preceded by the procedure of generating an asymmetric pair of RSA keys, i.e., a private key and a corresponding public key, using available tools

- CSR contains:
  - Public key
  - Identity of the server
    - DNS name(s)
  - Information about institution (OV certificates)

- BPD 106 – how to generate CSR:
  - Linux – OpenSSL
  - Microsoft IIS 4.x
  - Microsoft IIS 5.x / 6.x

AMRES Certificate Service – Submitting the request

- AMRES TCS portal
  - DjangoRA – *open source* application for handling TCS server, TCS e-Science server and code-signing certificates developed by SUNET.
    - *Python, Django*
    - *MySQL database*
    - *Linux*

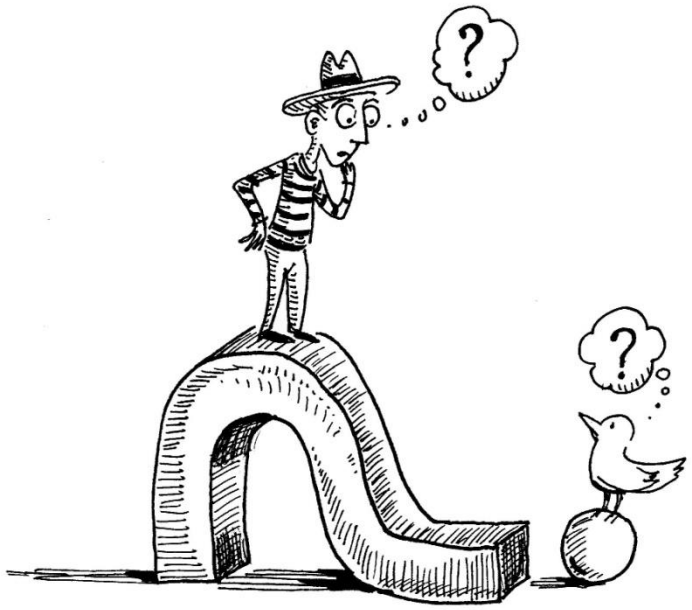
- Profile for each institution – information is copied from *ac.rs Domain Registry portal*

- Profile for administrative contact of institution – information is copied from *ac.rs Domain Registry portal*

AMRES Certificate Service – Number of issued certificates

2011	
TERENA Multi-domain SSL	26
TERENA Single-domain SSL	49
TERENA Wildcard SSL	1
Totally	**76**
2012	
TERENA Multi-domain SSL	30
TERENA Single-domain SSL	24
TERENA Wildcard SSL	2
Totally	**56**
2013	
TERENA Multi-domain SSL	12
TERENA Single-domain SSL	33
TERENA Wildcard SSL	3
Totally	**48**

Questions?



Thank you!