GÉANT eduPKI
Basics: The Building-Blocks for eduPKI

GN3 SA3 T1 – eduPKI
Reimer Karlsen-Masur, DFN-CERT Services GmbH
2nd GN3 Symposium, Vienna / AT, 25.11.2010

Slides & Related Materials @
https://www.edupki.org

Overview

- eduPKI Task overview
- eduPKI Policy Management Authority (PMA)
- eduPKI Certification Authority (CA)
- eduPKI Trust Anchor Repository (TACAR)
- Status summary & future plans

Slides & Related Materials @

https://www.edupki.org

eduPKI Task Overview

The Building-Blocks of eduPKI are

- eduPKI PMA
  which sets the coordinating frame and quality standards with its governing documents
- eduPKI CA
  which supplies X.509 certificates for GÉANT Services
- TERENA Academic CA Repository (TACAR)
  which provides a trustworthy download service for CA certificates, etc.

eduPKI PMA

- Policy Management Authority (PMA)
  - Management of Policies of Public-Key-Infrastructures (PKIs) and their Certification Authorities (CAs)
- Quality Assurance for GÉANT Services as Relying Parties of a PKI
  - Defines service requirements (called Trust Profiles) for PKIs
    - *Input from Relying Parties, i.e. GÉANT Services*
  - Assesses CAs of applying PKIs in regards to chosen Trust Profile
    - *compliant CAs will be accredited under the chosen Trust Profile*
- Publishes Trust Profiles and a list of accredited CAs in TACAR
- eduPKI PMA is a service for GÉANT Services

eduPKI PMA: Trust Profiles

A Trust Profile represents requirements and trust characteristics of identity assertions based on X.509 digital certificates.

- eduPKI PMA supports interested GÉANT Services to write up their Trust Profile.
- eduPKI PMA collects a set of Trust Profiles from interested GÉANT Services

eduPKI PMA: GÉANT Services Registration

- Registration of a GÉANT Service with the eduPKI PMA helps to
  - define and formalize its trust characteristics and requirements for identity assertions
  - provide a central GÉANT-wide DB of these requirements to interested CAs
  - find CAs that already support these requirements / get CAs to support these requirements
  - be able to use TACAR to download all suitable CA Certificates
- Registration of GÉANT Services with the eduPKI PMA includes the development of its Trust Profile
- Procedure for registering GÉANT Services is specified by eduPKI PMA's GÉANT Services registration guideline

eduPKI PMA: Registration of *eduroam*

- Trust characteristics and requirements for identity assertions of eduroam have been defined
- Based on that the eduPKI Trust Profile for eduroam Certificates has been developed
- GÉANT Service *eduroam* is registered with the eduPKI PMA as Relying Party

eduPKI PMA: CA accreditation (1)

- Accreditation of a CA under a Trust Profile of a GÉANT Service
  - states the compliance of that CA with the requirements stated in that Trust Profile
  - helps that GÉANT Service to find compliant CAs using TACAR
- Prerequisites and requirements for CAs wishing to get accredited are specified in
  - eduPKI PMA's CA accreditation guideline
  - at least one eduPKI Trust Profile document (only the ones that are supported by the applying CA)
- Procedure for the accreditation of CAs is specified by eduPKI PMA's CA accreditation guideline

eduPKI PMA: CA accreditation (2)

- eduPKI PMA is currently accrediting the eduPKI CA
- further CAs supporting eduPKI Trust Profiles can be accredited
- accredited CAs get an "Accredited under Trust Profile <NAME>" tag in their TACAR listing

eduPKI CA (1)

Certification Authority issuing x.509 certificates

- Governed by its policy documents, i.e. Certificate Policy (CP) and Certification Practice Statement (CPS)
- Certificate Policy (CP)
  - defines standards and requirements for the operation of the CA and Registration Authorities (RAs)
  - implements the "*eduPKI Trust Profile for eduroam Certificates*"
- Certification Practice Statement (CPS)
  - describes how the CP gets implemented in the daily CA / RA operations / work

eduPKI CA (2)

The eduPKI CA is

- an online CA, i.e. connected to a network
  - private CA key secured in nCypher Hardware Security Module (FIPS-140-2 Level 3 evaluated) → can't get out of HSM unencrypted
- running in established DFN-PKI trust centre providing the environment for its secure operation
  - strict physical access controls
  - secure network connection: firewalls, network segmentation / DMZ
  - monitored network

eduPKI CA: Obligations of the RA (operator)

RAs

- receive Certificate Requests from the Requester
- check authenticity of the Request
- check identity of the Requester
- check the Requester's authorisation to request and get the certificate

If all checks have been successfully passed

- approve Certificate Requests.

eduPKI CA: Obligations of the RA (operator) - in detail

Before an RA operator approves a Certificate Application he / she checks that:

- Certificate Application form (PDF) matches the certificate application in DB
- Certificate Application form (PDF) is submitted by a known Requester
- Requester's organisation exists
- Requester belongs to that organisation
- Requester is authorized to request certificate for that organisation
- Requester is authorized to use all requested names (FQDNs, IP#, email addresses) that are to be included in the issued certificate

Special checks for eduroam Certificates:

- Check with national eduroam operation centre that Requester is authorized to get eduroam Certificates for the requested eduroam servers

eduPKI CA: Obligations of the Subscriber

The Certificate Requester (later Subscriber) must adhere to the CP / CPS, especially:

- Submit only correct and truthful data in the Certificate Application
- Protect the private key
- Not share the private key with persons not authorized to have it
- Request revocation of the Certificate
  - if the private key and / or its password got compromised or exposed; or
  - if the data included in the Certificate got outdated or wrong

TACAR – eduPKI's CA Repository

Revamped secure & trustworthy Trust Anchor Repository provides a central repository for Relying Parties to download

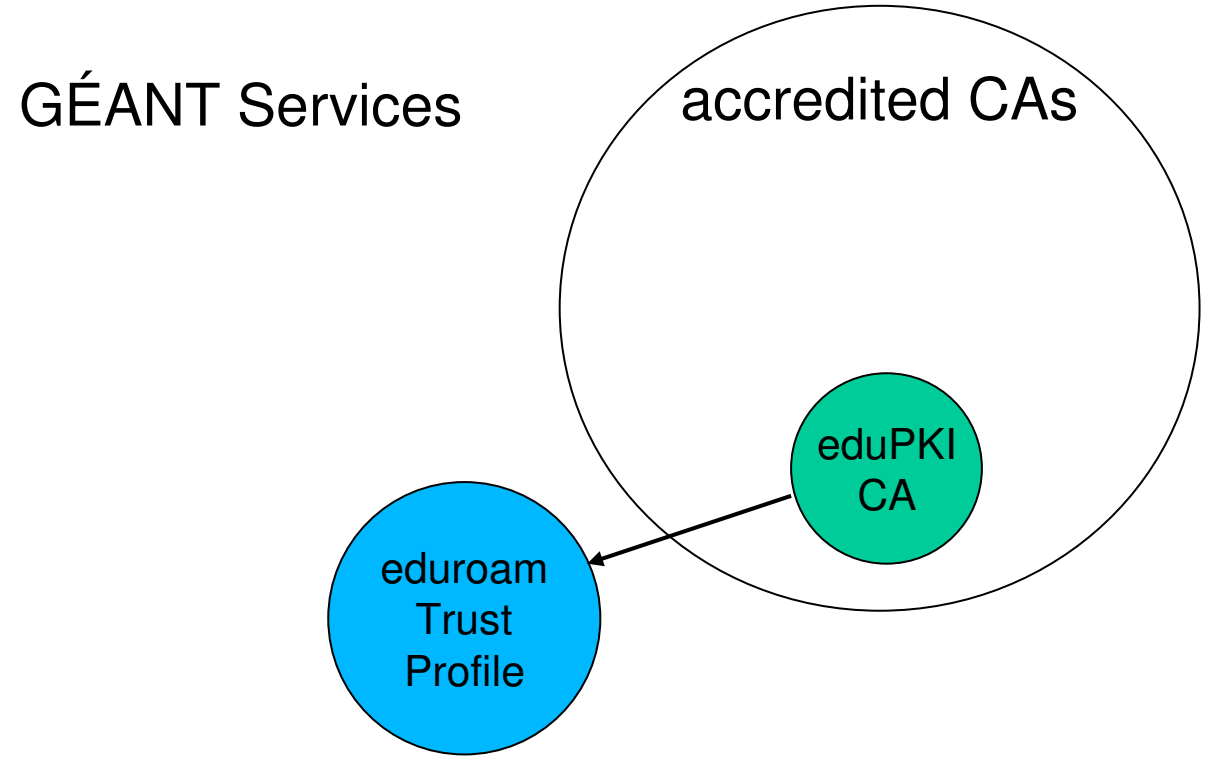
- CA Certificates
  - *CA Certificate bundles in various formats: PEM, DER, PKCS7, tgz*
- CA's policy documents
- CA's CRL download points
- CA's contact info

grouped by *TACAR Trust Category*, i.e. *eduPKI Trust Profile*

TACAR & eduPKI

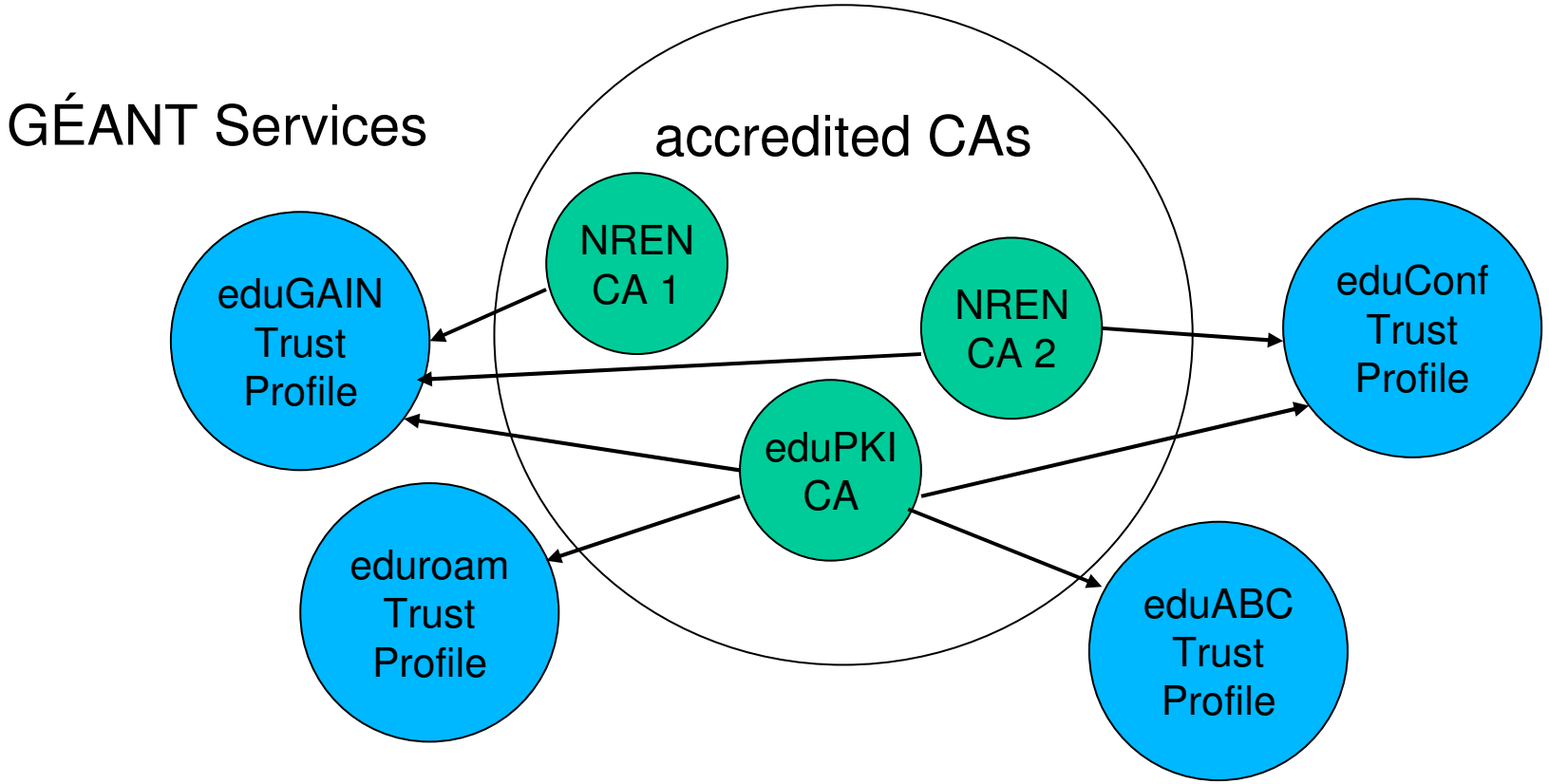
- TACAR provides a *TACAR Trust Category* per eduPKI Trust Profile
- TACAR lists accredited compliant CAs under the pertinent *TACAR Trust Category*
- Relying Parties can view / download all accredited CAs under a specific *TACAR Trust Category* with a view clicks

Current state: Now

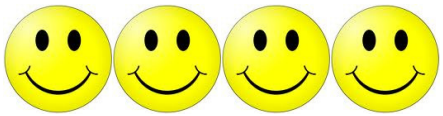


eduroam happy

Current state: Near future



more GÉANT Services happy



So, what's next?

- eduPKI is waiting for next GÉANT Service to do an eduPKI Trust Profile
- eduPKI is waiting for next CA applying for accreditation
- If you are interested contact GN3-SA3-T1 "eduPKI" at

  contact@edupki.org

Questions?

Thanks for your attention.

Questions?

Contact:

GN3 SA3 T1 – eduPKI
Reimer Karlsen-Masur, DFN-CERT Services GmbH
dfnpca@dfn-cert.de