

GÉANT eduPKI
in 5 Slides
Serving GÉANT Services

GN4 Symposium 2016 – Vienna

Reimer Karlsen-Masur, DFN-CERT Services GmbH

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

The 3 building-blocks of eduPKI are

- eduPKI Policy Management Authority – eduPKI PMA
which sets the coordinating frame and quality standards with its governing documents for eduPKI participants
- eduPKI Certification Authority – eduPKI CA
which supplies GÉANT Services with SSL certificates
- eduPKI's Trust Anchor Repository – TERENA Academic CA Repository (TACAR)
which provides a trustworthy download service for CA certificates for eduPKI participants

Policy Management Authority (PMA)

- manages Policies of Public-Key-Infrastructures (PKIs) and their Certification Authorities (CAs) – focus on SSL certificates
- interacts with GN services (the Relying Parties) to assess their PKI security requirements; if SSL certificates fit, offers solutions to address the requirements by defining requirements as Trust Profiles
- interacts with NREN CAs to engage them
 - CAs adopt Trust Profiles and get accredited by PMA
- publishes the Trust Profiles and a list of accredited CAs in TACAR

<https://www.edupki.org/edupki-pma/>

Certification Authority (CA)

- eduPKI's own CA issuing SSL certificates to GN services
 - for try-out, demo, test and proof-of-concept purposes
 - to support those providers and users of GN services that cannot use any NREN CA service for suitable SSL certificates for their GN service
- running in established DFN-PKI trust-centre which is providing the environment for its secure operation
- governed by its policy documents, i.e. Certificate Policy (CP) and Certification Practice Statement (CPS)
- accredited under the eduPKI Trust Profiles for “eduroam Certificates”, “Certificates for GÉANT's Multi-Domain Network Services” and “Generic Server- and Client-Machine-Certificates”
- 3 specific Registration Authorities (RAs) for GN services: eduroam, GN's Multi-Domain Network Services and GÉANT-IT

<https://www.edupki.org/edupki-ca/>

CA Certificate Repository

- utilizing TERENA's TACAR
- secure & trustworthy trust anchor repository provides a central repository for providers of GN services (the Relying Parties) to find / download
 - (Root-) CA certificates of mainly NREN / project PKIs
 - CA's policy documents & contact info
- TACAR provides one TACAR Trust Category per eduPKI Trust Profile
- TACAR lists all accredited compliant CAs under the pertinent TACAR Trust Category
- Relying Parties can find / download all accredited CA certificates under a specific TACAR Trust Category with a view clicks

<https://www.edupki.org/tacar/>

eduPKI's KPIs and Future Plans

KPIs	Target	Baseline	Measured
www.edupki.org (general info web-site) absolute availability (%)	99.9	99.4	99.42 (~51 hrs down/Y)
Certificate Status Check (CRL Download & OCSP) absolute availability (%)	99.99	99.9	100 (0 hrs down/Y)
RA Service (certificate application & approval) absolute availability (%)	99.9	99.7	99.93 (~6 hrs down/Y)
CA Service (certificate & CRL issuance) absolute availability (%)	99.9	99.7	99.67 (~29 hrs down/Y)

Future Plans:

Keep the availability KPIs high.

Continue to prevent grass root SSL PKI within GÉANT.

Relocating from GN4-1 SA4T2 to GN4-2 SA2T2.5.

Get involved with the Certificate Transparency work that GN4-2 JRA2T6 is doing.



Thank you

Slides available from
<https://www.edupki.org/documents/>

Contact:

GÉANT eduPKI

contact@edupki.org

Reimer Karlsen-Masur, DFN-CERT Services GmbH



Networks · Services · People
www.geant.org



This work is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).