

GÉANT eduPKI
Serving GÉANT Services

GN4-2 SA2 Kick-Off Meeting – Amsterdam/NL – 30/31.05.2016

Reimer Karlsen-Masur, DFN-CERT Services GmbH

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

- The 3 building-blocks of eduPKI (Policy Management Authority, eduPKI CA, TACAR)
- So what's the service then and who's using it?
- Service Operations

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

So what's the service then?

- PKI policy coordination & expertise (kind of consulting)
- X.509 certificates by the eduPKI CAs
- Preventing unmanaged wild grass root PKI across GN4

Have *you* been using eduPKI?

Have *you* been using eduPKI?

Probably: Are you using eduroam?

And who's using it?

It's a service for GN *services*.

eduPKI is used by

- eduroam – certs for RADsec
- GN's MDNS – certs for autoBAHN
- GN-IT – certs
- CESNET - accredited CA

And who's using it?

18 NRENs using the eduPKI service directly:

ACONET, BELNET, CARNET, CESNET, DFN, FCCN, GEANT, GRNET, HEANET, HUNGARNET, JANET/JISC, NORDUNET, PIONIER, redIRIS, RENATER, RESTENA, SURFNET, SWITCH.

These NRENs and/or their constituency organisations got certificates of the eduPKI CA.

All NRENs (worldwide) that participate in eduroam are using eduPKI CA certificates indirectly by using the eduroam infrastructure which uses eduPKI CA certificates.

What for?

Need SSL certs

- with special cert extensions / policy OIDs; or
- for legacy software with SHA-1 signatures; or
- for testing/dabbling; or
- for internal domain names or private IP#

?

Service Operations (i'structure)



Infrastructure:

PMA: Wordprocessing writing documents and talking to people.

eduPKI CA: Just 2 more CAs which run on DFN-PKI systems (high availability)

TACAR: Using existing TACAR operated by GÉANT AMS office

Service Operations (team)



Team:

PMA: Jan (CESNET), Reimer (DFN-PKI)

eduPKI CA: Reimer & in the background IT-service group and user support (7pki+network)

TACAR: Licia & Christian and GÉANT IT staff (not part of GN4)

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)

- 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.~~ (failed within GN4-2 – due to oversubscription on man power, maybe with PMA work)



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. 731122 (GN4-2).