GÉANT eduPKI - Certificates for eduroam

GN3 SA3 T1 – eduPKI
Gerti Foest, DFN-Verein
2nd GN3 Symposium, Vienna / AT, 25.11.2010

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

Overview

- Why does eduroam need certificates?
- What had to be done (by eduPKI and by eduroam)?
- How to get an eduroam certificate from eduPKI CA?

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

Why does eduroam need certificates?

eduroam needs

- Server Certificates for RADsec (RADIUS/TLS)
  - Certificates for securing communications between RADIUS infrastructure servers, i.e. eduroam Identity Provider and eduroam Service Provider

eduroam has

- Special requirements regarding certificate profile
  - e.g. OIDs (policy, eduroam Identity Provider, eduroam Service Provider)

What had to be done?
(by eduPKI and by eduroam)

Work of eduPKI / eduroam

eduroam

- Develop a Trust Profile for eduroam certificates
- Submit the Trust Profile to eduPKI PMA
- Set up a Registration Authority (RA) for eduroamers
  - eduroam task leader (Miro) appoints eduroam RA-operators (Milan, Stefan, Miro) by sending a signed paper to eduPKI CA
  - RA operators identify themselves in person towards eduPKI CA
  - RA operators request an RA operator certificate

eduPKI

- eduPKI CA includes the eduroam Trust Profile in eduPKI CA policy
- eduPKI CA issues RA operator certificate

Tasks of eduroam RA

- Define communication / identification procedures between Certificate Requesters and eduroam RA
- Distribute these procedures to potential Requesters
- Check identity, authenticity, and authorisation of certificate Requesters

How to get an eduroam certificate from eduPKI CA?

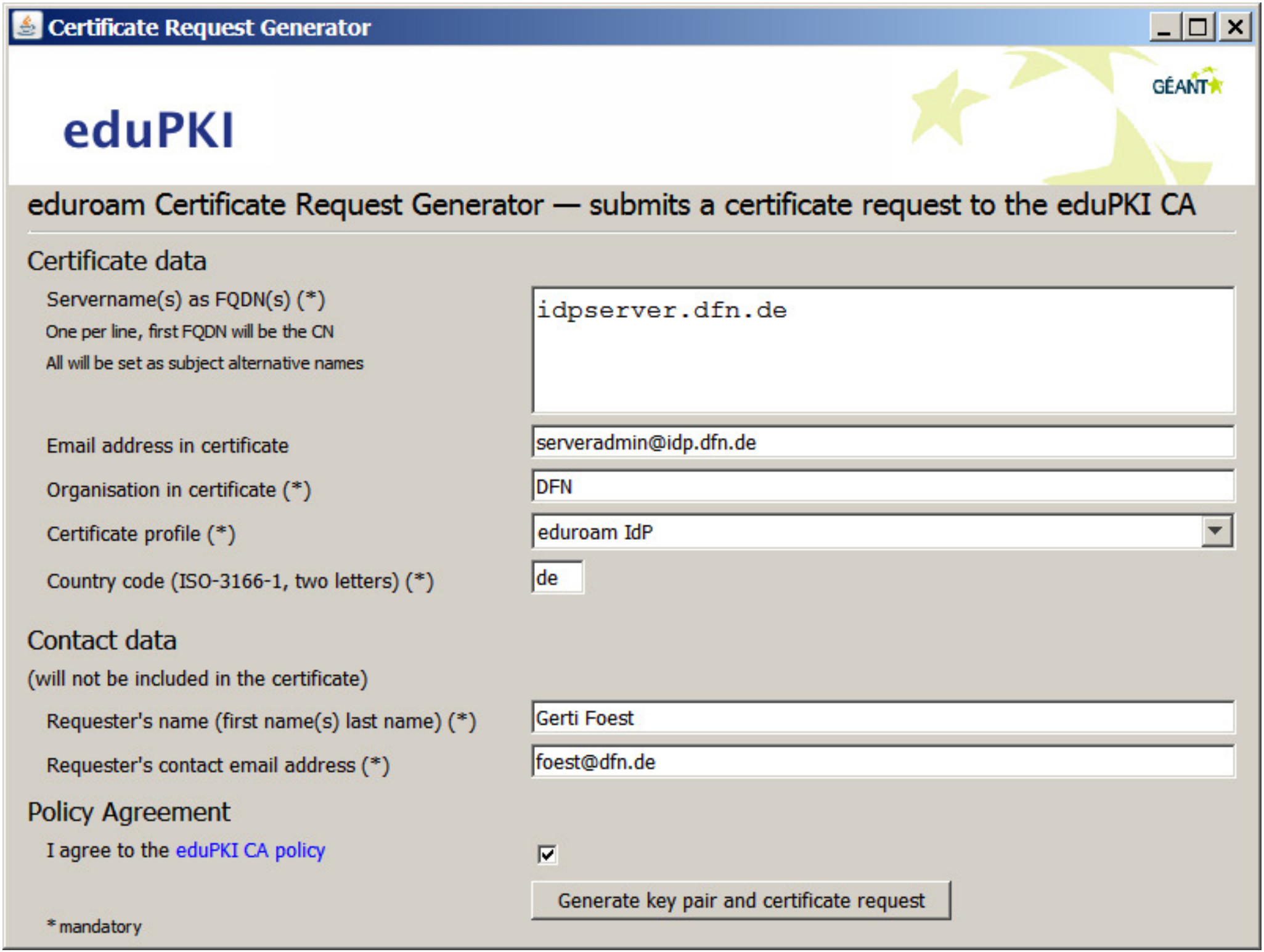
Requesting an eduroam certificate
Who – Where – What?

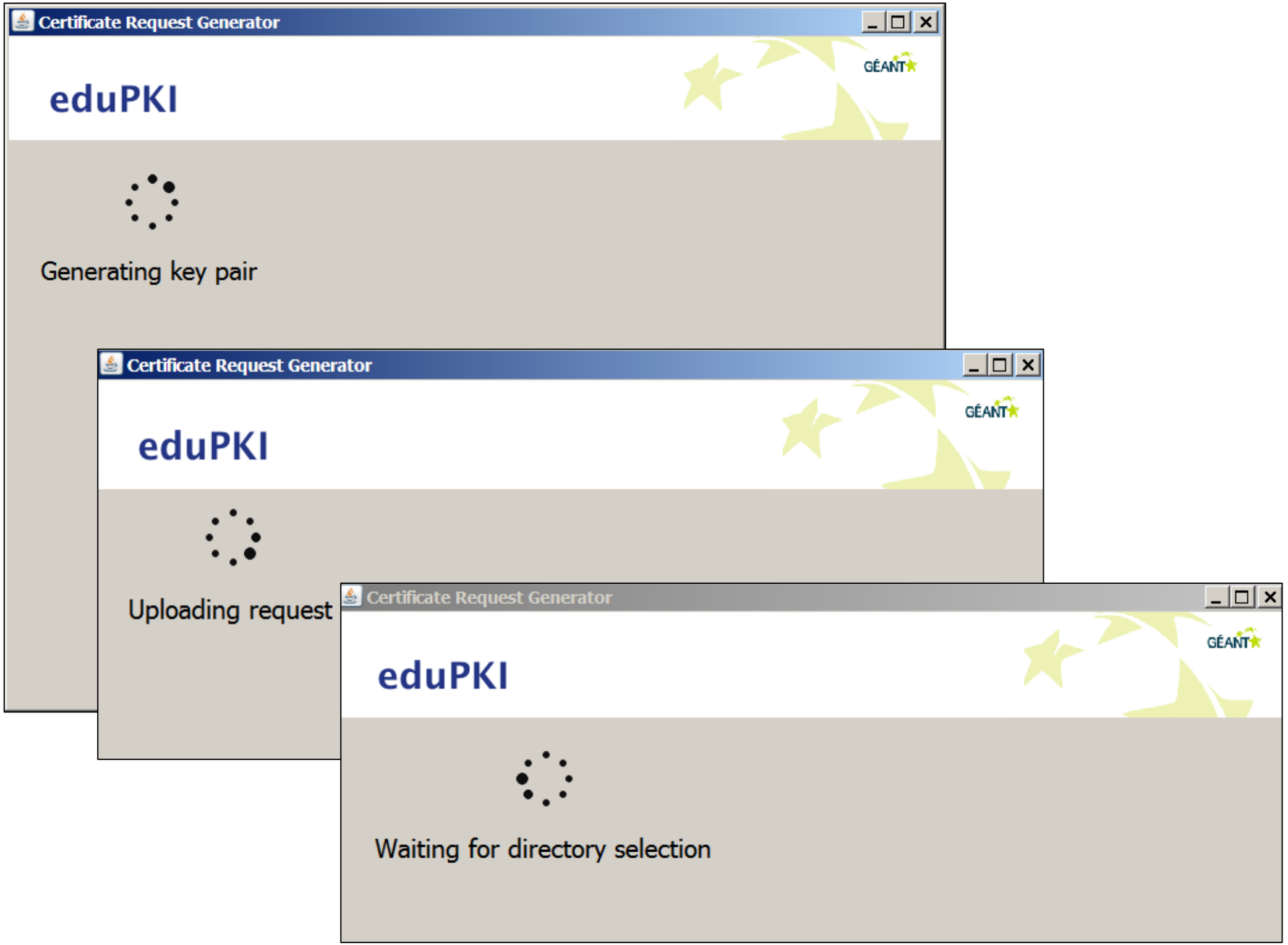
- **Who can request a certificate?**
  - eduroam server administrators
- **Where can the administrator request a certificate?**
  - https://www.edupki.org/
- **What is needed to request a certificate?**
  - Java JRE >= 1.6 (Java WebStart Application works in Browser or from java commandline)

Requesting an eduroam certificate
It's as easy as this!

You have to

- Start eduroam certificate request generator from https://www.edupki.org/edupki-ca/eduroam-certificates/
- Enter certificate and Requester data and the generator will …
  - generate a key pair and certificate signing request (CSR)
  - submit an electronic certificate application to the eduroam Registration Authority (eduroam RA) electronic certificate application
  - produce a certificate application form as PDF and ask you where to store the private key, the CSR and the PDF
- Send the signed PDF application form to eduroam RA as defined in the RA communication procedure


Certificate Request Generator
eduPKI
GÉANT
eduroam Certificate Request Generator — submits a certificate request to the eduPKI CA
Certificate data
Servername(s) as FQDN(s) (*)
One per line, first FQDN will be the CN
All will be set as subject alternative names
idpserver.dfn.de
Email address in certificate
serveradmin@idp.dfn.de
Organisation in certificate (*)
DFN
Certificate profile (*)
eduroam IdP
Country code (ISO-3166-1, two letters) (*)
de
Contact data
(will not be included in the certificate)
Requester's name (first name(s) last name) (*)
Gerti Foest
Requester's contact email address (*)
foest@dfn.de
Policy Agreement
I agree to the eduPKI CA policy
Generate key pair and certificate request
* mandatory


Certificate Request Generator
eduPKI
GÉANT
Generating key pair
Certificate Request Generator
eduPKI
GÉANT
Uploading request
Certificate Request Generator
eduPKI
GÉANT
Waiting for directory selection


Certificate Request Generator
eduPKI
GÉANT
Request successfully submitted:
The request has been generated.
The key pair has been generated and saved as idpserver.dfn.de-key.pem.
The request has been uploaded.
All files have been saved under C:\Dokumente und Einstellungen\Foest\Eigene Dateien\eduPKI\eduPKI CA.
Please note:
The private key file is not protected with a password!
The following things have to be done:
Ensure that the private key file is protected by proper access permission.
Print out the request pdf (idpserver.dfn.de.pdf) and send it to the Registration Authority (RA).
When you received the certificate by email (after approval of your request by the RA) install the private key (idpserver.dfn.de-key.pem) and the certificate on your server.
New Request
Close

How to send the signed form to eduroam RA?

The eduroam RA will define the communication procedure

Most probably it will be

- send the PDF application form by S/MIME or PGP signed email

Possible alternatives

- print the PDF application form, sign it and send it by traditional mail
- print the PDF application form, sign it and send it by fax

Approval of request by eduroam RA

eduroam RA

- Receives the signed PDF application form
- Visits eduroam RA interface of eduPKI CA using RA operator certificate
- Verifies certificate application / request data, especially authorisation of the Requester and authenticity of the request
- Approves certificate application

Details of request verification

eduroam RA checks / verifies

- Matching of PDF application form with the corresponding electronic certificate application in the eduroam RA interface including digital fingerprint of public key
- Home organisation
- Affiliation of Requester with home organisation
- Authorisation of Requester to use all names (FQDNs, IP#, email addresses) included in the certificate request (based on WHOIS and national roaming DB)

eduPKI CA issues certificate

When everything is ok

- eduroam RA approves request
- eduPKI CA delivers certificate via email to Requester

eduroam server admin is happy