eduPKI Updates

Licia Florio

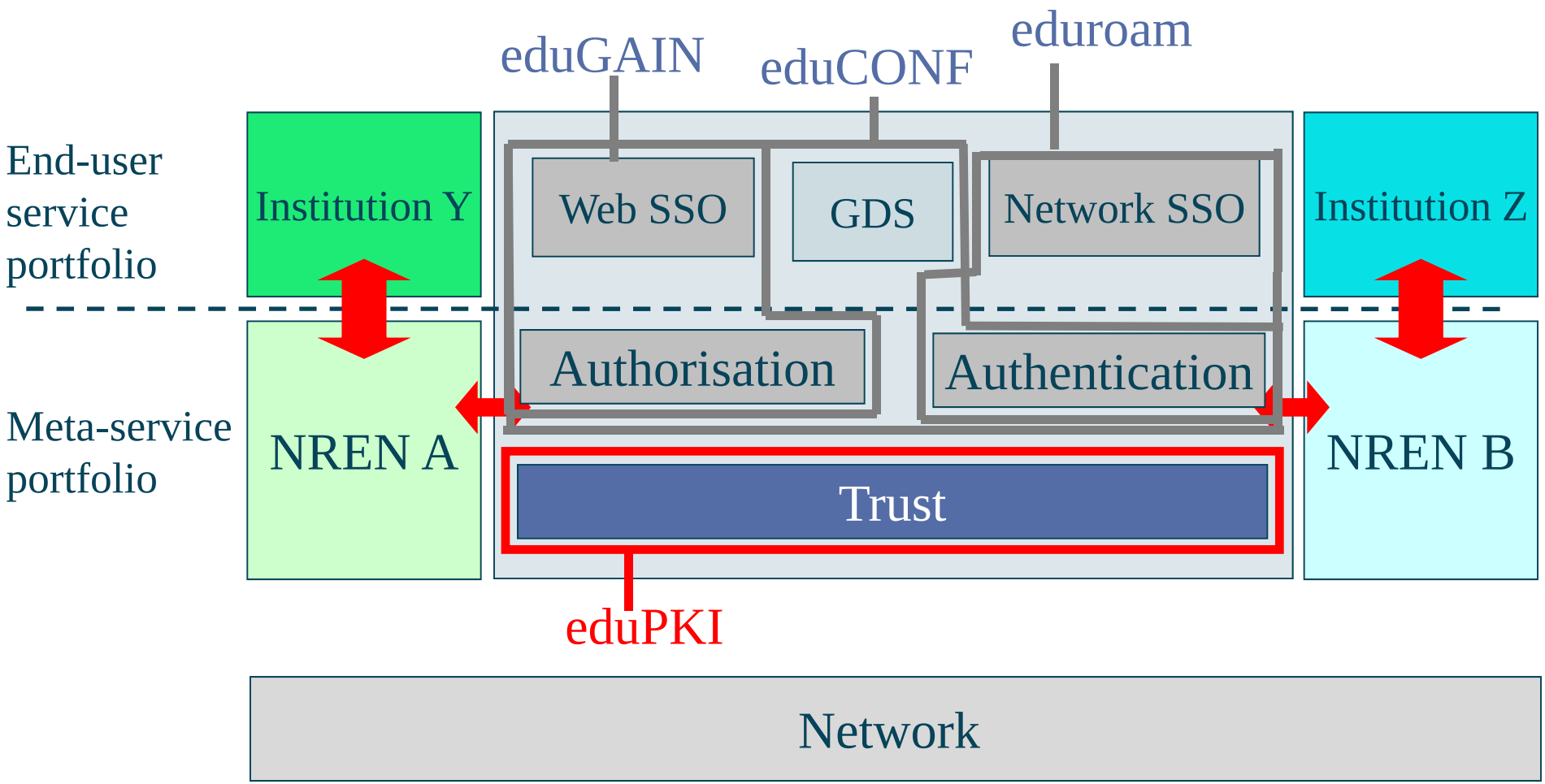
GN3 PR Network meeting

Utrecht, 9 Feb 2011

Outline

- eduPKI overview
- eduPKI as part of SA3
- What type of service it offers
- Main results

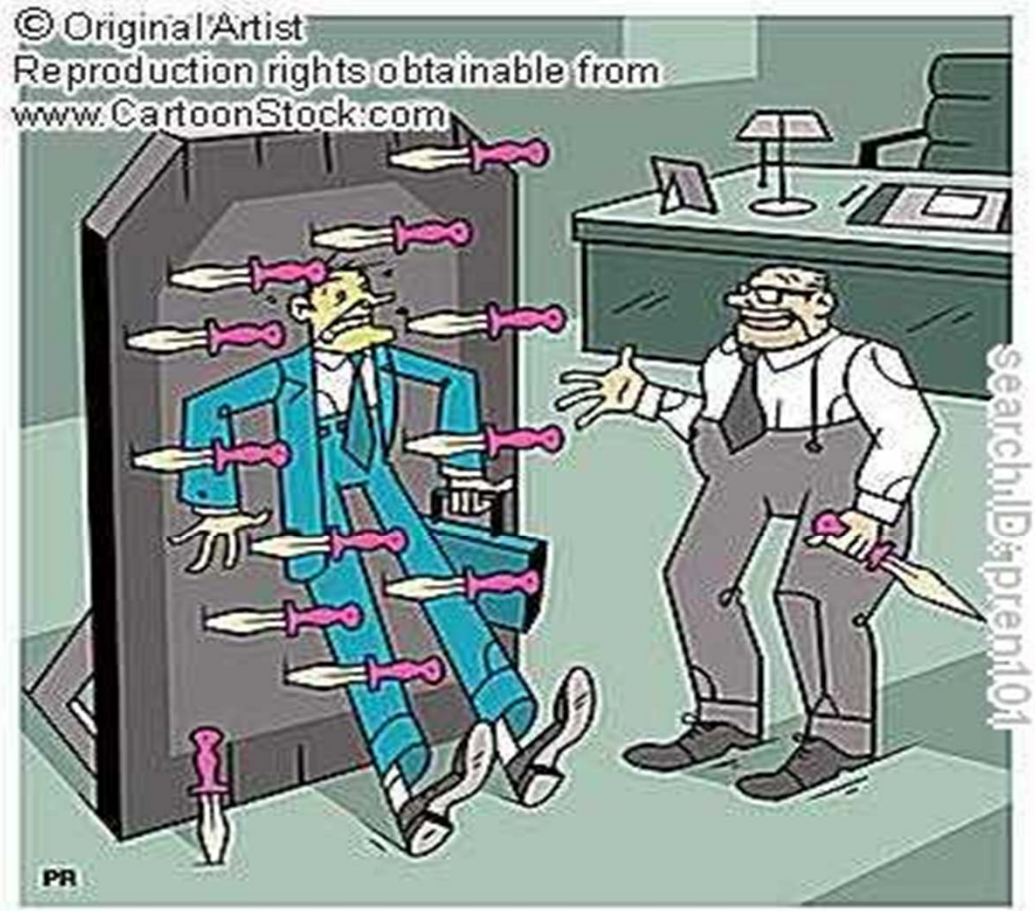
eduPKI and SA3 Service Portfolio



Josh Howlett's slide

It’s all about Trust

- Trust can be established in different ways….



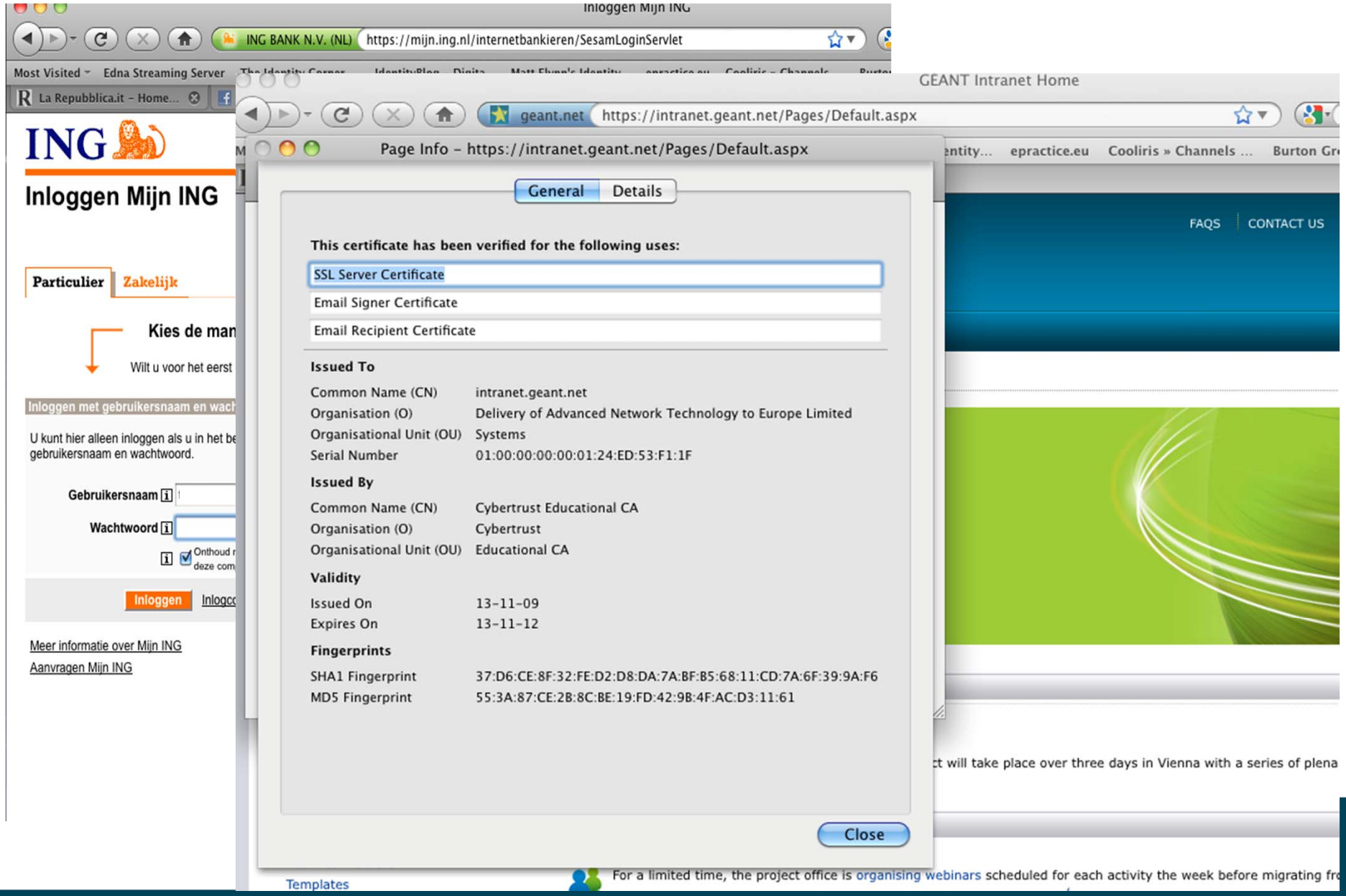
"Right, now that a relationship of trust has been established, let's get down to business, shall we? "

eduPKI Objectives

- eduPKI enables trust establishment in GN3 services:
  - Trust allows users to rely on a service;
  - Trust facilitate **confidence in the security and integrity of GN3 services**.

- eduPKI service objectives are to:
  - Support other of the project's services in defining their security requirements;
  - Provide them with digital certificates by **federating existing NRENs certificates services**;
    - *eduPKI defines how the certificates look like;*

Examples


Inloggen Mijn ING
ING BANK N.V. (NL)
https://mijn.ing.nl/internetbankieren/SesamLoginServlet
Most Visited
Edna Streaming Server
La Repubblica.it – Home...
ING
Inloggen Mijn ING
Particulier
Zakelijk
Kies de man
Wilt u voor het eerst
Inloggen met gebruikersnaam en wach
U kunt hier alleen inloggen als u in het be
gebruikersnaam en wachtwoord.
Gebruikersnaam
Wachtwoord
Onthoud
deze com
Inloggen
Inlogcc
Meer informatie over Mijn ING
Aanvragen Mijn ING
GEANT Intranet Home
geant.net
https://intranet.geant.net/Pages/Default.aspx
epractice.eu
Cooliris » Channels ...
Burton Gr
FAQS
CONTACT US
Page Info – https://intranet.geant.net/Pages/Default.aspx
General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Email Signer Certificate
Email Recipient Certificate
Issued To
Common Name (CN) intranet.geant.net
Organisation (O) Delivery of Advanced Network Technology to Europe Limited
Organisational Unit (OU) Systems
Serial Number 01:00:00:00:00:01:24:ED:53:F1:1F
Issued By
Common Name (CN) Cybertrust Educational CA
Organisation (O) Cybertrust
Organisational Unit (OU) Educational CA
Validity
Issued On 13-11-09
Expires On 13-11-12
Fingerprints
SHA1 Fingerprint 37:D6:CE:8F:32:FE:D2:D8:DA:7A:BF:B5:68:11:CD:7A:6F:39:9A:F6
MD5 Fingerprint 55:3A:87:CE:2B:8C:BE:19:FD:42:9B:4F:AC:D3:11:61
Close
t will take place over three days in Vienna with a series of plena
Templates
For a limited time, the project office is organising webinars scheduled for each activity the week before migrating fr

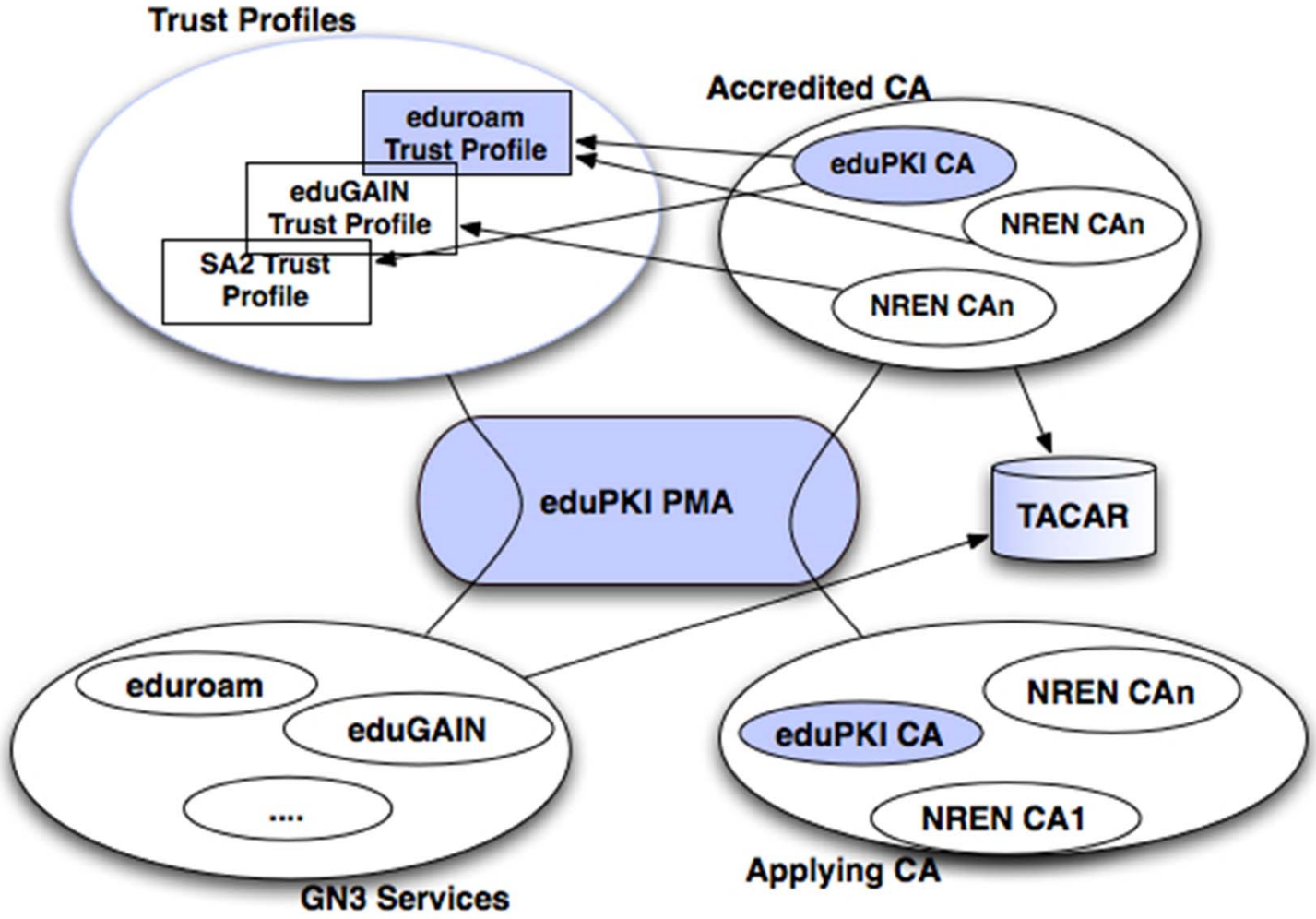
eduPKI Strategic Value

- By coordinating and harmonising trust across GN3 services, eduPKI :
  - Ensures efficiency as trust is dealt by a group of experts;
  - Facilitates implementation of a cohesive technical and policy infrastructure;
  - Avoids duplications of effort in different activities;
  - Will ease the transition from the current project to the next one;
  - Consequently improves the end-users experience;

eduPKI Service Elements

- **Policy Management Authority (PMA)**
  - Interacts with GN3 services to asses their security requirements;
    - *And offers solutions to address them (trust profiles);*
  - Interacts with NRENs CAs to engage them;
- **A dedicated Certification Authority (eduPKI CA)**
  - For test purposes and to support those NREN users that cannot rely on any national CA service;
- **An enhanced version of the existing TACAR** (TERENA Academic Certificate Authority Repository)
  - To list the CAs participating in eduPKI
  - Used by the services' operators;

eduPKI Service Provision



The coloured elements belong to eduPKI

eduPKI Target

- eduPKI targets GN3 (pilot) services:
  - Supporting them defining their trust requirements;
  - Facilitating access to digital certificates whenever needed;
- eduPKI targets NRENs:
  - NRENs are invited to participate by enabling their CAs to issue certificates in accordance with the eduPKI procedures.
  - This ensures continuity to users;
- eduPKI does not target end-users directly!

Main Results

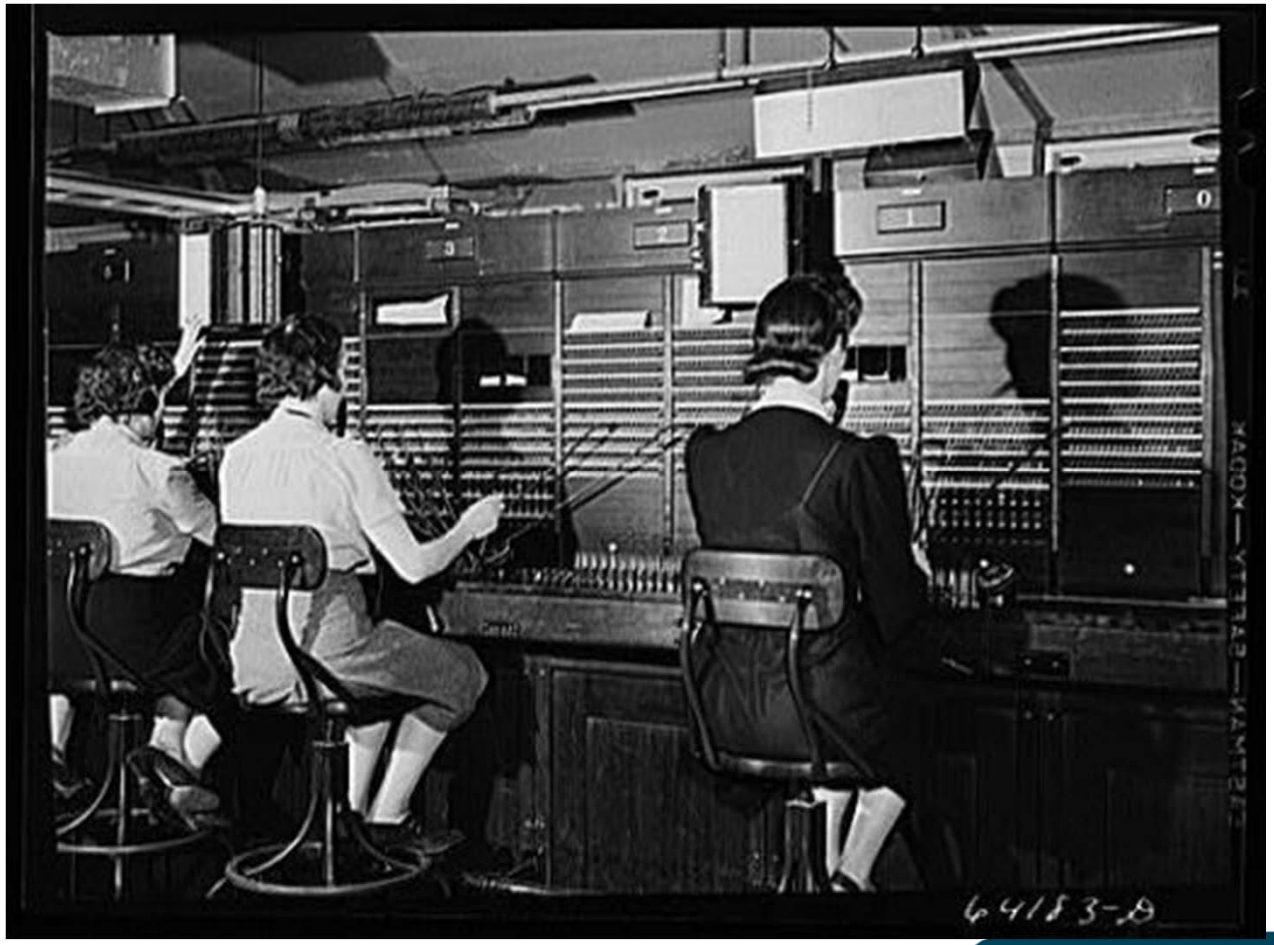
- eduPKI Business Case
  - Approved in May 2010;
- eduPKI governance and procedures in place;
  - Sept 2010;
- eduPKI cooperation with eduroam:
  - Very successful
- At the moment discussion initiated with SA2 and eduGAIN
- eduPKI Pilot phase:
  - Started in the summer 2010, ending in Feb 2011
- eduPKI service starts on 1 March 2011.

eduroam use-case

- eduPKI collaboration with the eduroam resulted in:
  - eduroam trust profile
    - *Hence new certificates for the eduroam hierarchy;*
  - To date only only eduPKI-CA issues these certificates:
    - *But discussion is started to engage TCS and DFN-PKI;*
- The process is completely transparent to end-users:
  - Only eduroam operators are involved;
- The usage of eduPKI certificates will:
  - Increase eduroam scalability;
  - Allow to change the trust model from a "**transitive approach**"

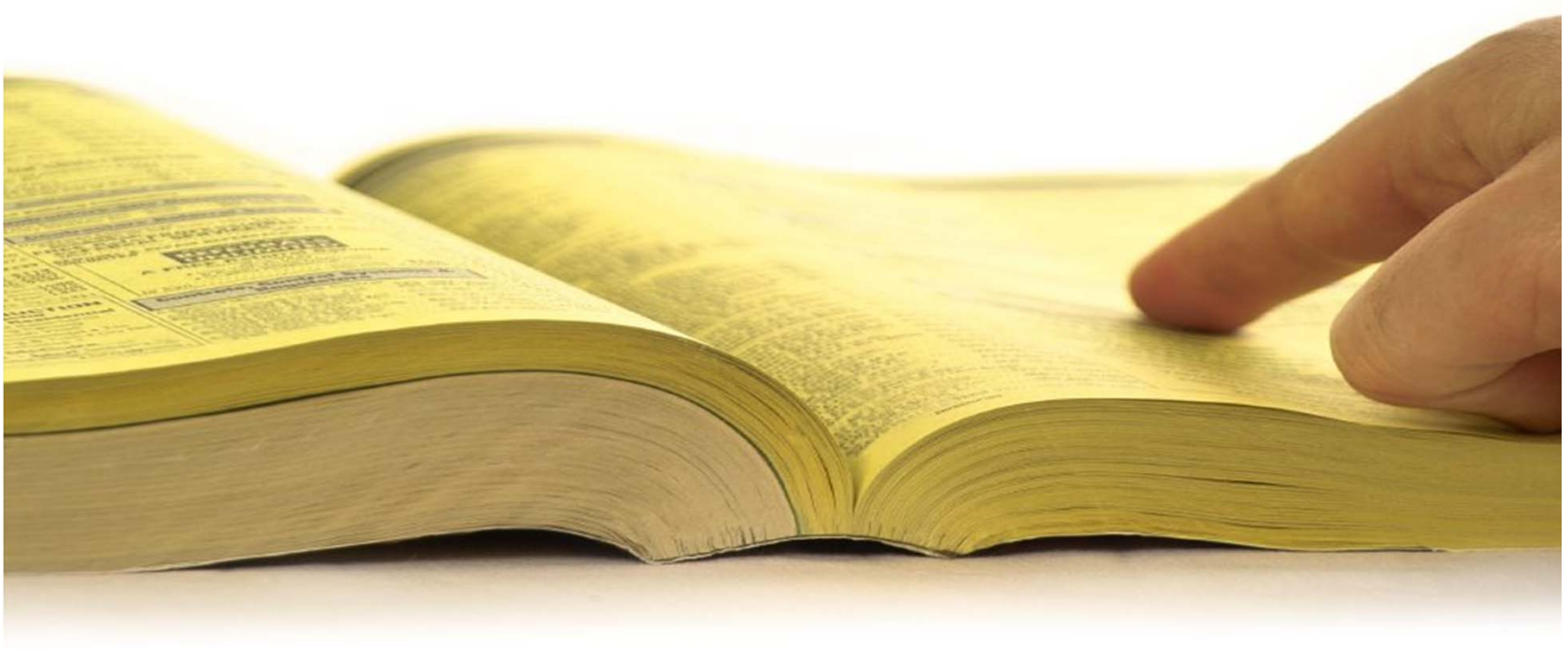
eduroam Trust Model

- The eduroam operational team….



eduroam Trust Model

- To a “look-up” approach:



References

- eduroam Trust Profile:
  - https://www.edupki.org/fileadmin/Documents/eduPKI-Trust-Profile-for-eduroam-certificates-1.0.pdf
- eduPKI governance documents:
  - https://www.edupki.org/documents/pma-related-documents/