Outline

- eduPKI overview
- eduPKI as part of SA3
- What type of service it offers
- Main results
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*;
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 assess 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;
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:

- eduPKI governance documents:
  - https://www.edupki.org/documents/pma-related-documents/