eduPKI Updates

Licia Florio

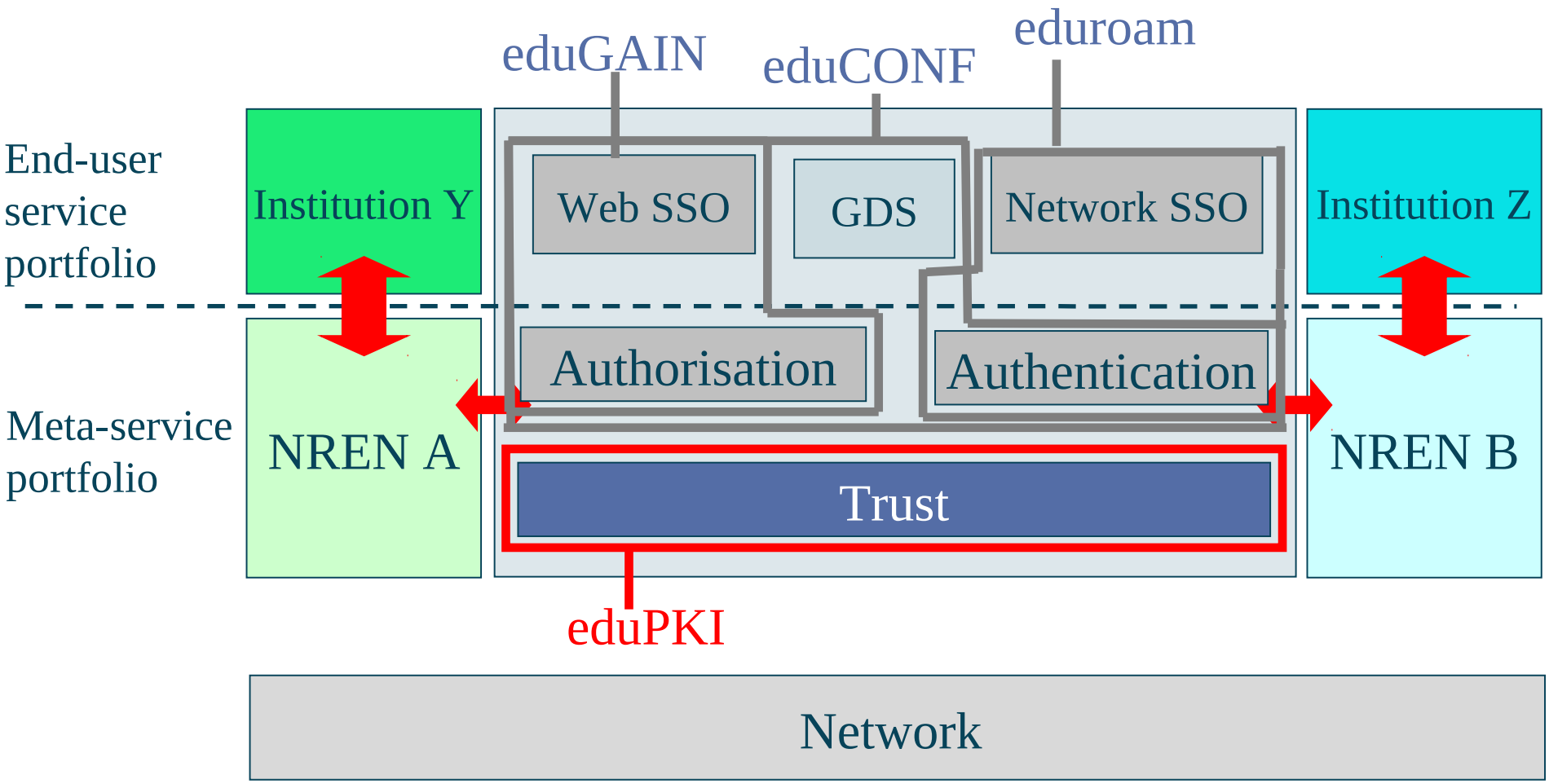
GN3 PR Network Meeting

Utrecht / NL, 09.02.2011

Outline

- eduPKI overview
- eduPKI as part of SA3
- What type of service are offered
- Main results

eduPKI and SA3 Service Portfolio



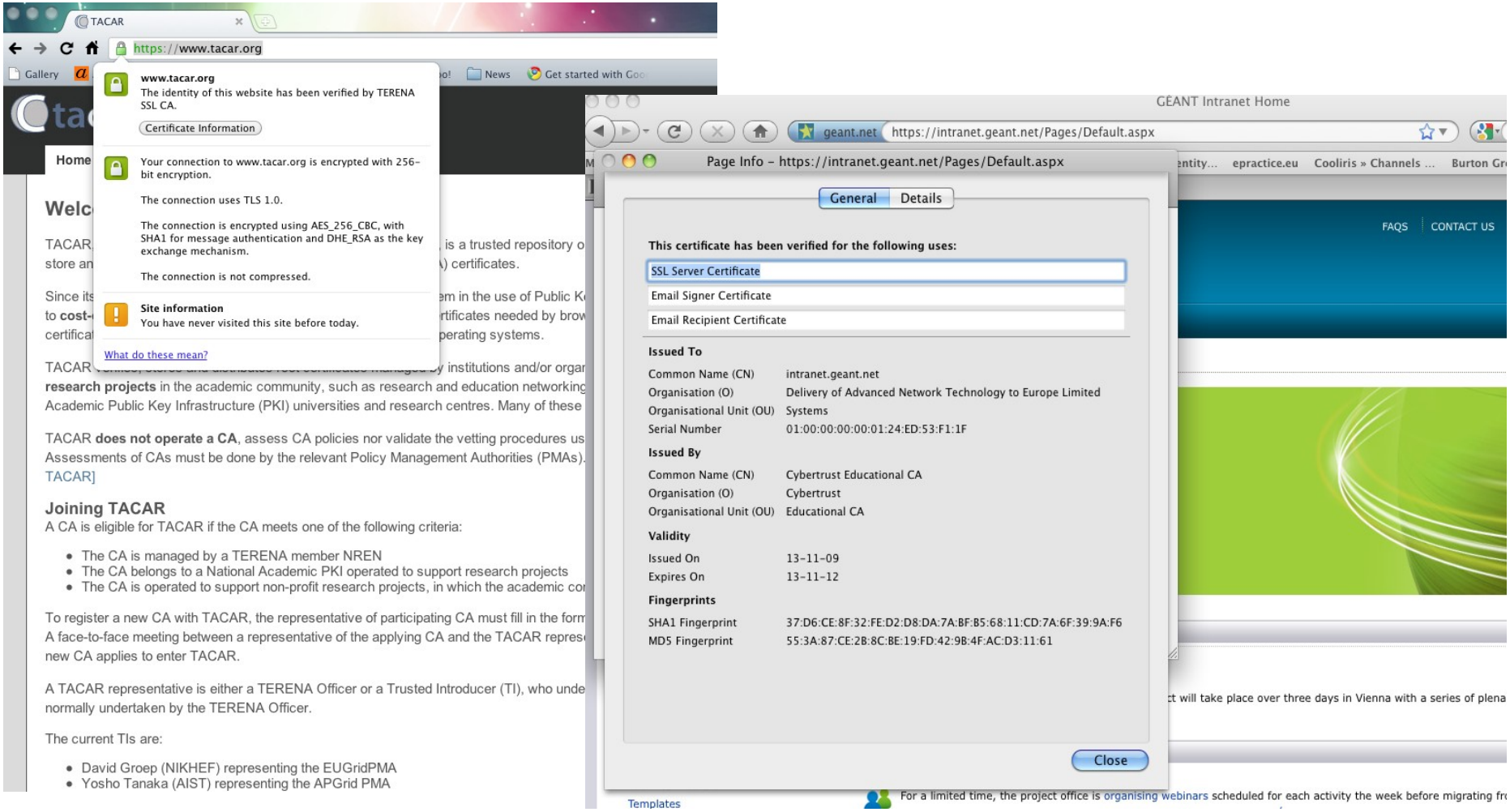
Josh Howlett's slide

eduPKI Objectives

- eduPKI enables trust establishment in GN3 services:
  - Trust allows users to rely on a service;
  - Trust facilitates **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


TACAR
https://www.tacar.org
www.tacar.org
The identity of this website has been verified by TERENA SSL CA.
Certificate Information
Your connection to www.tacar.org is encrypted with 256-bit encryption.
The connection uses TLS 1.0.
The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.
The connection is not compressed.
Site information
You have never visited this site before today.
What do these mean?
Home
Joining TACAR
A CA is eligible for TACAR if the CA meets one of the following criteria:
The CA is managed by a TERENA member NREN
The CA belongs to a National Academic PKI operated to support research projects
The CA is operated to support non-profit research projects, in which the academic co
The current TIs are:
David Groep (NIKHEF) representing the EUGridPMA
Yosho Tanaka (AIST) representing the APGrid PMA
GÉANT Intranet Home
geant.net
https://intranet.geant.net/Pages/Default.aspx
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
FAQS
CONTACT US
Templates

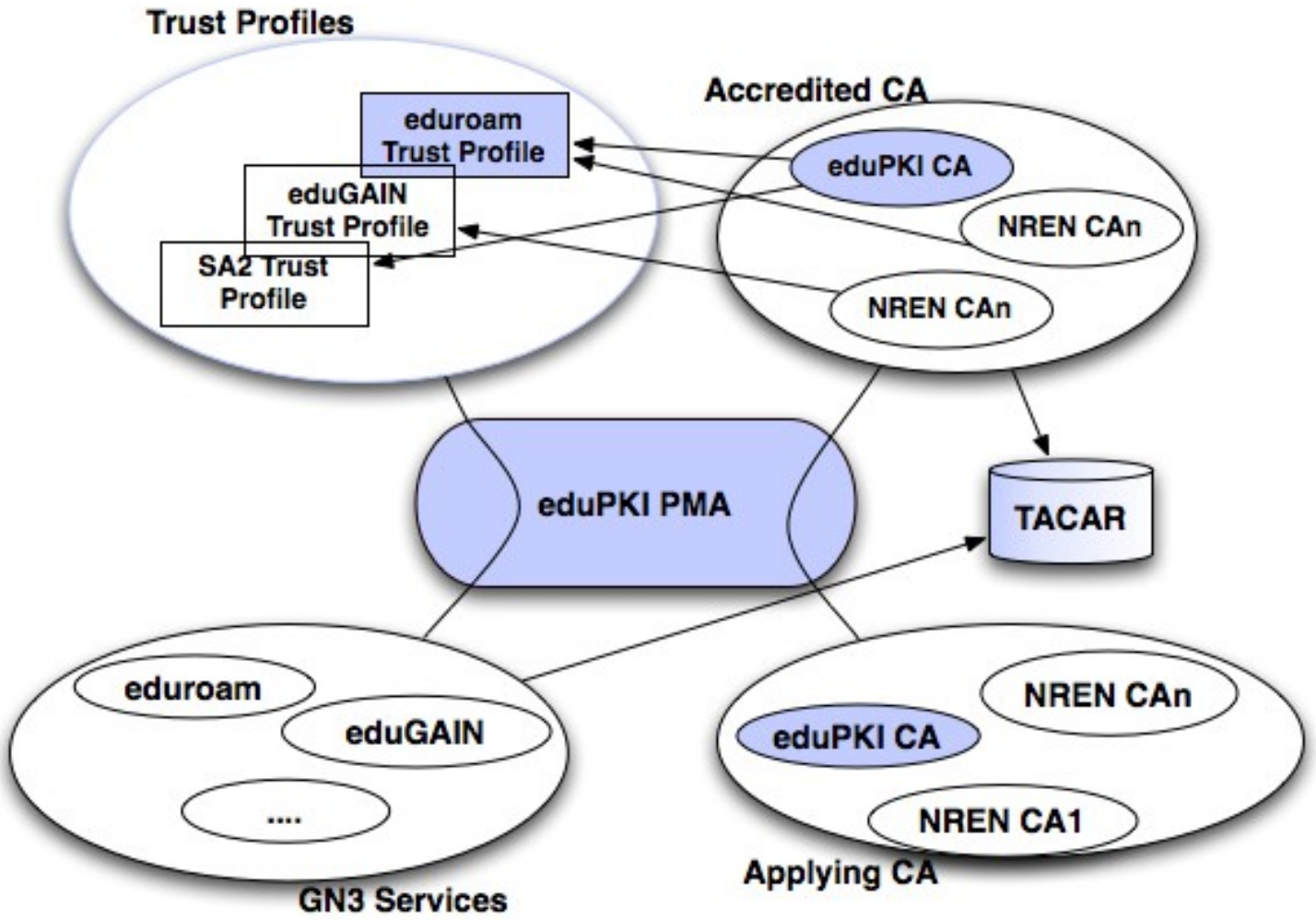
eduPKI Strategic Value

- 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 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;

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

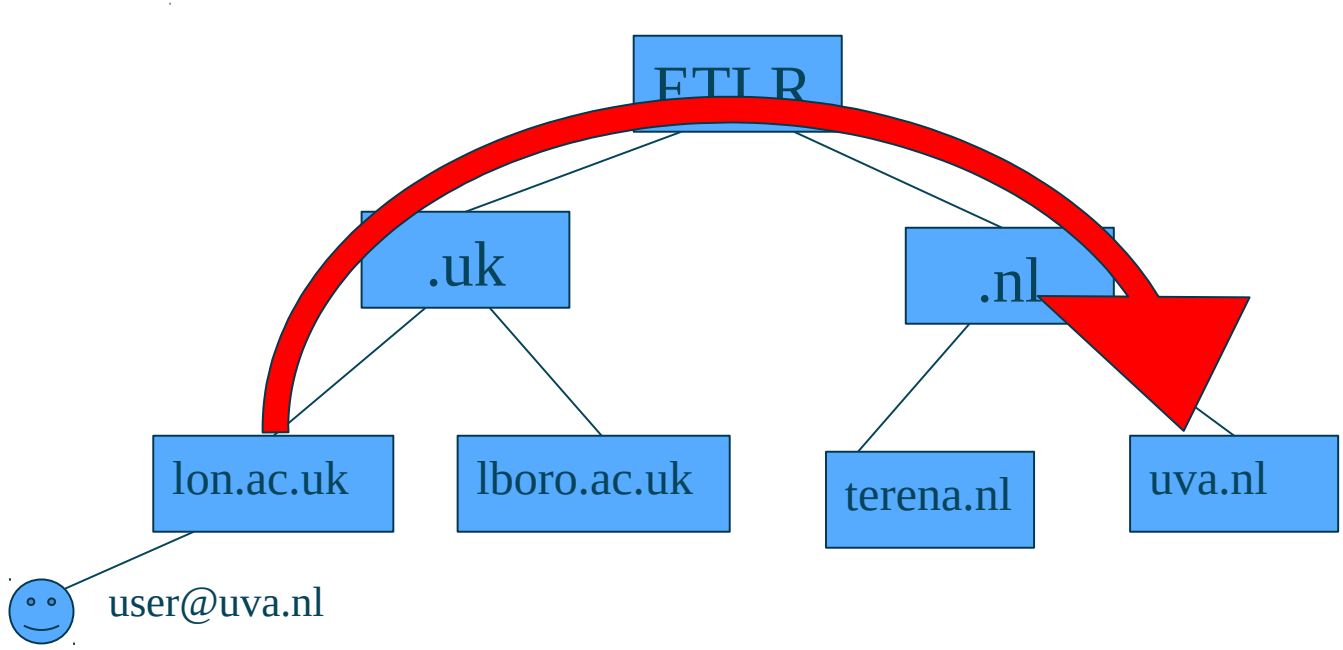
- eduPKI Business Case
  - Approved in May 2010;
- eduPKI governance and procedures in place;
  - Sept 2010;
- eduPKI cooperation with eduroam:
  - Very successful
- At the moment discussion initiated with SA2 and eduGAIN
- eduPKI Pilot phase:
  - Started in the summer 2010, ending in Feb 2011
- eduPKI 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 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;
  - Offer better security;
  - Change the trust model

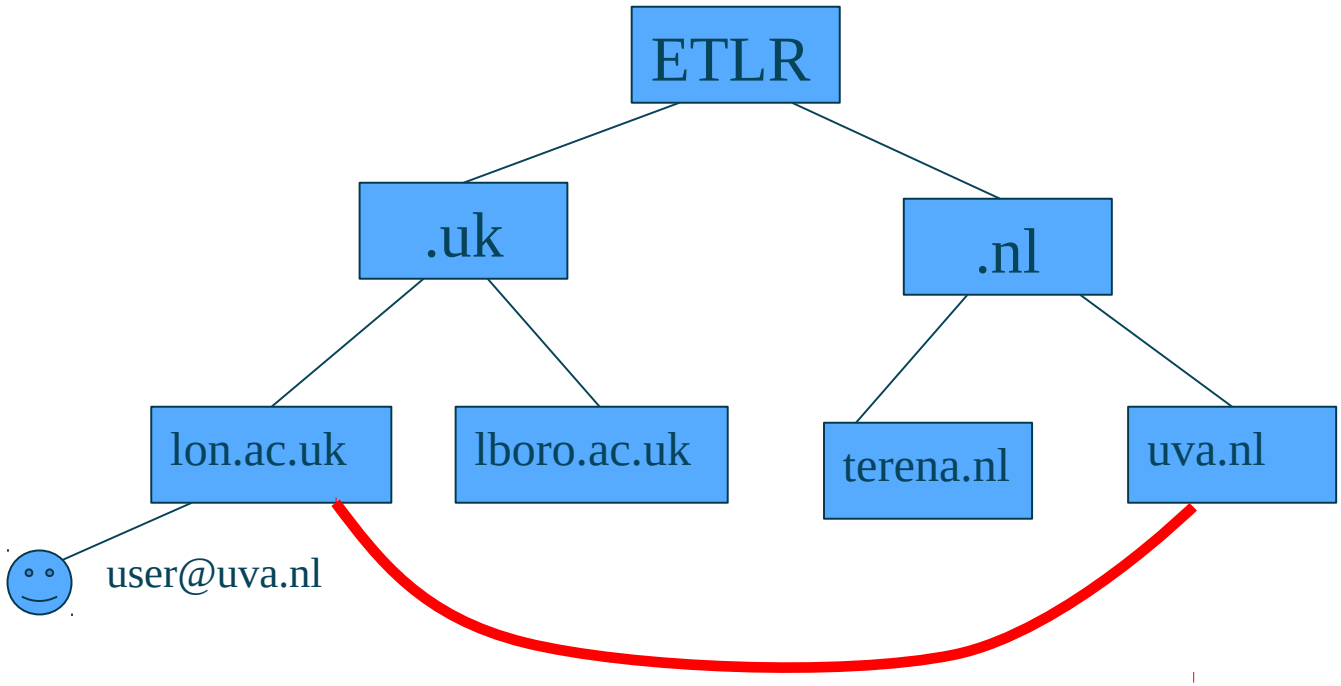
eduroam Trust Model Today

- eduroam's current trust model follows a "**transitive approach**":
  - Each node in the hierarchy trusts the ones it connects to;
  - Information travels through the whole hierarchy;



eduroam Trust Model Tomorrow

- The future eduroam trust model will follow a "**look-up approach**":
  - Nodes will be able to use the information in the certificates to establish direct connections with each others;



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/