eduPKI - Supporting Trust Requirements in Europe's Research Networks

eduPKI is a response to the need for better coordination to address security requirements of the services being developed in GÉANT. eduPKI's main goal is the coordination of GÉANT-wide trust that is build on X.509 certificates and Public Key Infrastructures (PKI). eduPKI organizes provisioning of digital certificates to GÉANT Services from national Public Key Infrastructures (PKI) and supports GÉANT Services in defining their trust requirements (Trust Profiles) in regards to digital certificate based identity assertions. In addition, an eduPKI CA is established to meet those requirements of GÉANT Services that cannot be (easily or timely) covered by existing (national) Certification Authorities.

Text: **Reimer Karlsen-Masur** (DFN-CERT Services GmbH), **Dr. Ralf Gröper** (DFN-Verein), including material from the eduPKI Task on www.edupki.org and geant.net

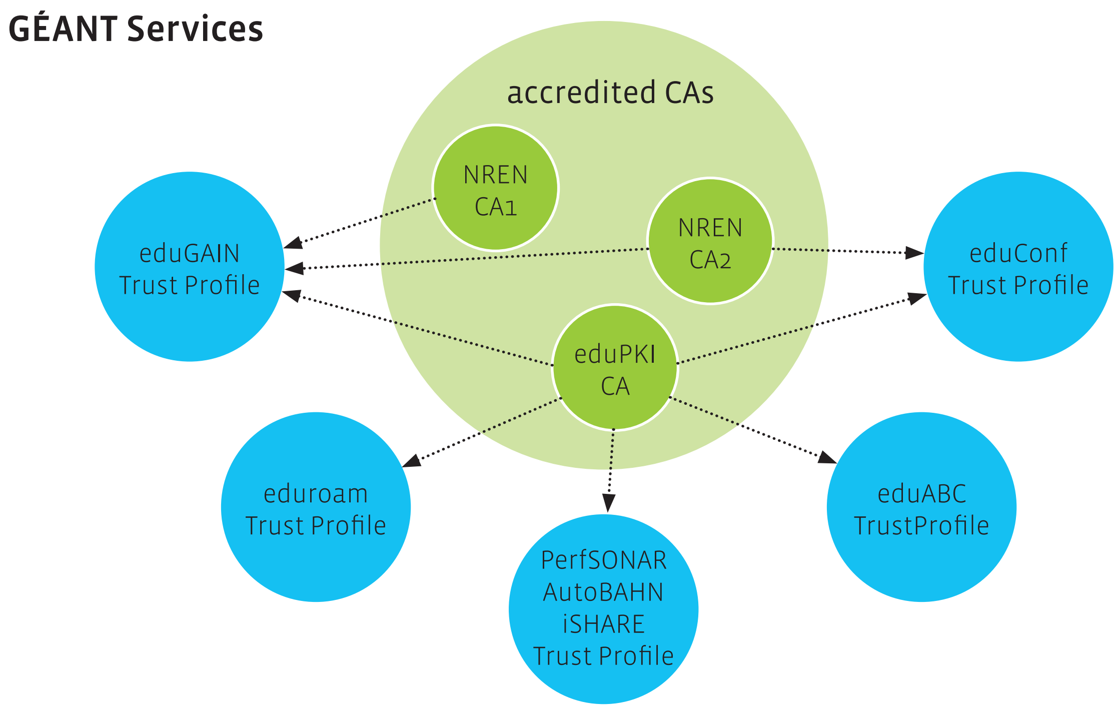

Abb. 1: Accredited CAs of the eduPKI PMA with their supported registered Trust Profiles of GÉANT Services

Background

Digital certificates are issued by Certification Authorities (CAs) and are widely used to guarantee secure and reliable communication between servers, users, or between a user and a server. One example for this are the authentication servers participating in the eduroam radius hierarchy, enabling researchers and students to access the Internet from all participating institutions.

eduPKI will build on top of existing CA services by National Research and Education Networks (NREN) such as DFN-PKI, federating them to make all participating CAs available to other services such as eduroam. A federated approach brings increased efficiency since a number of national CAs are already well-established and used within the NREN environment.

eduPKI aims to enable GÉANT services to obtain digital certificates from CAs operated by NRENs participating in the project, that meet those services' requirements. Thus Europe's NRENs are encouraged to join the federated eduPKI service. Whilst eduPKI will rely on existing national CAs whenever possible, it will also operate a dedicated CA for users belonging to an NREN that does not provide any CA service itself.

Why will eduPKI be beneficial to users?

By allowing existing CAs to issue certificates for those GÉANT project services that require them, eduPKI will permit users to deal with their NREN, following familiar procedures which will reduce the burden of using new services. So thanks to the federated approach, users will be able to obtain all necessary certificates from either the CA managed by their own NREN (or equivalent service) or via the eduPKI CA.

eduPKI structure

To achieve its goal eduPKI offers three main facilities:

Foto: © Marcus Lindström - istockphoto.com

- A Policy Management Authority (PMA), which will define procedures to assess GN3 services' requirements and categorise them into profiles; as well as procedures to assess existing national CA operations against the agreed profiles.
- A dedicated Certification Authority (eduPKI CA), operated by DFN 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 store and distribute root certificates of Certificate Authorities participating in eduPKI (including the eduPKI CA root) in a secure manner.

The role of eduPKI PMA to coordinate trust
The eduPKI PMA acts as the heart of the eduPKI Service. It is the body where GÉANT Services can register their trust and certificate requirements as Trust Profiles and Certification Authorities can get accredited as CAs serving these Trust Profiles in a compliant way.

The eduPKI PMA has published a number of documents describing its work and procedures. The eduPKI PMA Charter describes how the PMA is set up and operated, its scope, objectives and responsibilities, membership and voting processes.

The GÉANT Services Registration Process describes how a GÉANT Service can register as a Relying Party under one or more Trust Profiles, the CA Accreditation Process defines how a CA is obtaining accreditation under a specific Trust Profile by getting reviewed by the eduPKI PMA. It also describes how a CA is securing its accreditation by adopting changes to the relevant Trust Profiles, performing audits, delivering audit reports, and how an accreditation can be withdrawn.

The eduPKI PMA members support the GÉANT Services in writing their Trust Profiles and the CAs that wish to be accredited in performing the necessary procedures. TACAR is then used to publish sets of CAs that are compliant to a specific Trust Profile and such providing a central source for CA certificate download and information about compliant and fitting CAs to the GÉANT Services.

Why an eduPKI CA?
As described above, GÉANT Services can

obtain certificates that meet their Trust Profile from any CA that fulfils their respective requirements. Nevertheless experience has shown that some users have difficulties to get the certificates they need. The eduPKI CA is established to serve those users of GÉANT Services who cannot obtain certificates from a local or national CA and it can also be used for testing new Trust and Certificate Profiles before these profiles are made generally available. The eduPKI CA will adapt all Trust Profiles that are registered under the eduPKI PMA.

TACAR

TACAR is the central repository for administrators to download bundles of CA certificates used as local trust anchors that are compliant to selectable Trust Profiles. CA managers can upload their CA certificates including policy and revocation information onto TACAR where the information gets validated and depending on information provided by the eduPKI PMA gets assigned an eduPKI Trust Profile category. System administrators of Relying Parties can use the TACAR web site to select and download a single CA certificate or set of CA certificates compliant to a Trust Profile in a bundle for local installation as a trust anchor.

Key Benefits of the approach

The key benefits of the eduPKI approach are scalability and flexibility. This ensures sustainable results beyond the GN3 project, within which eduPKI is funded by the European Commission.

Scalability of eduPKI's approach is achieved by separating different trust and certificate requirements into different Trust Profiles. Trust Profiles can be used by several GÉANT Services if the requirements fit, if not, additional Trust Profiles can be defined. They can be defined at the pace GÉANT Services are ready to more formally define their requirements of trust and certificates. CAs can choose to support all, a subset or just one of the available Trust Profiles, depending on their infrastructure and on the local demand of their nearby GÉANT constituency. Furthermore, CAs can be accredited at the pace CAs become compliant with specific Trust Profiles.

eduPKI's approach is flexible as Trust Profiles can be added, updated or abandoned as demand and requirements by the pertinent GÉANT Services may change. CAs can be added or dropped as they are able or not or no longer able to support the GÉANT Services' requirements. eduPKI CA is a long-term effort to secure GÉANT Services the access and availability to certificates even if no other CA is able to fulfil the GÉANT Services' trust and certificate requirements or if participants of GÉANT Services can't get certificates from local or national CAs. ediPKI's approach abates the set-up and operation of ad-hoc or task specific CAs which often multiplies the effort and, if such an ad-hoc CA is abandoned, it leaves the relying GÉANT Services and tasks without a reliable source of working certificates. Additionally, eduPKI enables local or national (NREN) CAs to operate in a coordinated fashion.

Current Status

Trust Profiles for GÉANT Services

eduroam is the first GÉANT Service that has registered its Trust Profile under the eduPKI PMA and obtains certificates from the eduPKI CA which is in operation since mid November 2010.

Another Trust Profile that has been registered under the eduPKI PMA covers certificates for GÉANT's Multi-Domain Network Services such as perfSONAR, autoBAHN, cNIS and I SHARe.

It is expected that more GÉANT Services will write up their Trust Profile and register it with the eduPKI PMA in order to give interested CAs an overview about the GÉANT Services' trust and certificate requirements.

Accredited CAs

Currently the eduPKI CA and the CESNET CA from the Czech Republic's NREN are accredited under the eduroam service's Trust Profile. By accrediting eduPKI's own CA, the defined accreditation processes and procedures underwent a real life test which lead to optimised processes and procedures, resulting in the successful accreditation of the CESNET CA. It is expected that more local or national (NREN) CAs will express their compliance with one or (soon) more Trust Profiles and will then be accredited by the eduPKI PMA. Under the Trust Profile for GÉANT's Multi-Domain Network Services currently only the eduPKI CA is accredited.

The next steps for eduPKI

In the future, eduPKI will help more GÉANT Services to define their trust and certificate requirements in Trust Profiles and register these Trust Profiles with the eduPKI PMA. Furthermore, more local or national (NREN) CAs will be accredited under the existing Trust Profiles to express compliance with specific Trust Profiles and such provide a set of compliant CAs to the GÉANT Services. Framing these efforts, eduPKI will continue to provide consulting services to GÉANT Services for all aspects concerning X.509 digital certificates, Public Key Infrastructures, and building Trust Profiles.

Conclusion

eduPKI operates key services such as the Policy Management Authority and the eduPKI CA, but also helps other GÉANT services and projects by offering consulting services regarding all aspects of Public Key Infrastructures and X.509 certificates. By these means eduPKI helps to ease the adoption of X.509 digital certificates within GÉANT in an efficient way, maximizing the effective usage of PKI in Europe's research network environment and thus increasing the overall security level therein. ◆