Date: May 2011

Author: Licia Florio

Version: 1.4

eduPKI solution for eduroam use-case

Introduction

Since the summer of 2010, GÉANT pilot and production service developers have been able to consult the eduPKI group to build security and trust mechanisms for their services. The eduPKI service, operated under the GN3 project, aims to assist GÉANT services in defining their trust procedures (with a special emphasis about the usage of digital certificates). The eduPKI service has been in production since 1 March 2011.

The eduPKI task (SA3/T1) has worked with the eduroam task (SA3/T2) to support the mutual authentication and authorisation of RADIUS nodes within the eduroam infrastructure by means of digital certificates. This document describes the joint collaboration between the eduPKI service, the eduroam service and the roaming task (JRA3/T1).

To get a more in depth view on the topics discussed in this document, please refer to:

https://www.geant.net/Media_Centre/Media_Library/Media%20Library/JRA3-T1-idp-discovery.pdf

https://www.edupki.org/fileadmin/Documents/GF-2010-11-GEANT-Symposium-certificates-for-eduroam.pdf

What is eduPKI?

By harmonising trust across GN3 services, eduPKI facilitates the effective development and maintenance of cohesive technical and policy infrastructure whilst avoiding duplication of effort.

eduPKI comprises the following components:

1. **Policy Management Authority** (PMA) which acts as 'the heart' of the service defining the governance and the procedures for eduPKI service as a whole; the eduPKI PMA has also defined procedures to analyse services' requirements and categorise them into trust profiles.

2. **eduPKI Certification Authority** (eduPKI CA) which supports the GN3 services, partners and users that cannot utilise a national CA service and/or

for test purposes.

TACAR [2], the TERENA Academic CA Repository is used as a support tool to register NREN CAs supporting eduPKI proposed solutions.

For more information on eduPKI, please visit:

https://www.edupki.org/

eduroam Requirements – The Challenges

eduroam is a global service that provides secure roaming connectivity to users at hundreds of participating institutions across Europe (and beyond), including universities, libraries and research institutes.

For more information about eduroam please visit: http://www.eduroam.org/

The eduroam architecture is currently based on two main principles:

- RADIUS servers exchange packets via the User Datagram Protocol (UDP);
- the original eduroam architecture is a static hierarchy of RADIUS nodes where all the trust is configured manually during setup; this model is also referred to as “transitive trust”, as each server trusts the next node in the hierarchy.

The development of Secure RADIUS (also known as RadSec or RADIUS/TLS) and the proposal under discussion in JRA3-T1 to move from the current static RADIUS hierarchy to a dynamic model (dynamic discovery) [1], requires certificate-based node authentication and authorisation.

During the initial tests with Secure RADIUS, carried out towards the end of the GÉANT2 project (2008), certificates were provided by RedIRIS via the “eduGAIN-SCA”.

In 2010, JRA3-T1 proposed a plan to roll out Secure RADIUS to the whole eduroam infrastructure; due to technical limitations affecting the certificates issued by the eduGAIN-SCA and the decision to discontinue this CA, it was felt that the time was ripe for involving eduPKI in proposing a suitable, scalable and standard-based solution for eduroam.

The main requirement for the new eduroam model was the need to encode the identity of a RADIUS node and its role (whether the node acts as a Service Provide (SPs) or as an Identity Provider (IdPs) into a certificate.

eduPKI Proposed Solution

The eduPKI PMA, based on the eduroam requirements, proposed a solution based on encoding the eduroam node properties into a digital certificate.

This solution is based on including two Object Identifiers (OIDs) into a certificate; each OID is assigned to identify eligible eduroam Service Providers (SPs) and eduroam Identity Providers (IdPs).

A document, the eduroam Trust Profile [3] defines the format of the eduroam certificates as well as the requirements on CAs issuing public key certificates to Secure RADIUS nodes participating in eduroam; the eduPKI PMA is responsible for maintaining the profile.

The procedures followed to verify that an entity is a legitimate eduroam IdP or SP and therefore can obtain an eduroam Trust Profile compliant certificate are defined by the eduroam community and detailed at:

http://www.eduroam.org/index.php?p=europe&s=edupki

eduPKI PMA will also keep track of the CAs that support the eduroam Trust Profile; this list will be made available via TACAR.

Current status and next step

The eduroam Trust Profile was released in November 2011 and has been tested with positive results. To date the eduPKI CA is the first CA to support this Trust Profile. Other NREN CAs are encouraged to support the eduroam Trust Profile; in this case the CA would need to be accredited [4] by the eduPKI PMA.

Potential NREN CA services that could support the eduroam Trust Profile are the TERENA Certificate Service (TCS) [5] and the DFN-PKI Service [6]; at the beginning of 2011 the eduPKI PMA approached these services to discuss the necessary steps to accredit them.

Key Benefits of the proposed approach

The major benefit of this approach is in concentrating expertise in the appropriate group.

The eduPKI group is focused on operations and procedures related to certificate management, which is handled in a single group (eduPKI) with the expertise and manpower for this task.

The eduroam group responsibility is in establishing the legitimacy of new eduroam

entities and defining which OID or OIDs it should be assigned.

The eduPKI-CA provides eduroam operators with an easy-to-use, reliable on-line CA which will be able to provide certificates in a quickly, efficient and scalable manner.

References

[1] **Dynamic discovery** allows moving from a model in which trust among the RADIUS servers follows a transitive model (each element in the RADIUS hierarchy trust the next one in the hierarchy) to a look-up model where nodes are able to establish direct trust among each other without using the whole eduroam hierarchy. The implementation of this model is based on Secure RADIUS. See also:

https://www.geant.net/Media_Centre/Media_Library/Media%20Library/JRA3-T1-idp-discovery.pdf

[2] TACAR:

http://www.tacar.org

[3] eduroam Trust Profile:

https://www.edupki.org/fileadmin/Documents/eduPKI-Trust-Profile-for-eduroam-certificates.pdf

[4] CA accreditation process:

https://www.edupki.org/fileadmin/Documents/eduPKI-PMA-CA-accreditation-process.pdf

[5] TCS:

http://www.terena.org/tcs/

[6] DFN-PKI

https://www.pki.dfn.de/