eduPKI PMA
GÉANT Services Registration Process

Version 1.0

23.08.2010

Abstract

This document describes how a GÉANT Service can register with the eduPKI PMA as a Relying Party under one or more eduPKI Trust Profiles.

Change History

Version	*Author*	*Date*	*Changes*
1.0	RKM	23.08.2010	Init

Table of Contents

1 Introduction

This document describes how a GÉANT Service can register with the eduPKI PMA as a Relying Party of Public Key Infrastructures (PKIs) under one or more eduPKI Trust Profiles. In order to register the GÉANT Service it must either pick the appropriate eduPKI Trust Profiles or if none is available it must define its trust requirements and then together with the eduPKI PMA derive an eduPKI Trust Profile. This document also describes how an eduPKI Trust Profile is defined.

2 Identification of this document

Name: eduPKI PMA GÉANT Services Registration Process

Version: 1.0

Date: 23.08.2010

2.1 Change procedure

This document can only be changed following the documented change procedure.

Changes to this document must be voted on by the Trust Team according to the voting rules set down by the eduPKI PMA Charter [CHARTER].

3 Contact Information

The eduPKI PMA office can be contacted via various means:

Web-site: www.edupki.org

Email: pma@edupki.org

Mail: eduPKI PMA
c/o DFN-Verein
Alexanderplatz 1
10178 Berlin
GERMANY

4 Registration Procedure for GÉANT Services

The eduPKI PMA's Trust Team is responsible to define eduPKI Trust Profiles and to register interested GÉANT Services under one or more suitable eduPKI Trust Profiles.

Before a GÉANT Service can register under specific eduPKI Trust Profiles the Service and its trust requirements need to be mature, i.e. the Service's authentication architecture and trust requirements are well discussed and understood by the constituency providing and using the GÉANT Service and thus should only change within the parameters that the potentially chosen eduPKI Trust Profile allows.

New eduPKI Trust Profiles are only introduced if existing eduPKI Trust Profiles don't match and there is a sustainable demand and user base for the applying GÉANT Service.

4.1 Work-flow overview

The following steps need to be undertaken to accommodate a new GÉANT Service:

1. GÉANT Service defines its trust requirements

2. GÉANT Service announces its trust requirements to the Trust Team together with a request to become a Relying Party.
3. The trust requirements of the GÉANT Service may be input for a new eduPKI Trust Profile if no existing eduPKI Trust Profile fulfils the trust requirements.
4. The eduPKI PMA defines a (new) eduPKI Trust Profile that fulfils the GÉANT Service's trust requirements
5. The eduPKI PMA, registers the GÉANT Service as Relying Party of that eduPKI Trust Profile.
6. The eduPKI PMA establishes and maintains a Trust Category in the TERENA Academic CA Repository (TACAR) that is associated with the eduPKI Trust Profile and accredits PKIs with their CAs under it [CA-ACC-PROC].
7. Users and operators of the GÉANT Service download and install the CA certificates of the eduPKI Trust Profile the Service has registered with from TACAR and such become a Relying Party trusting the accredited CAs of that eduPKI Trust Profile.

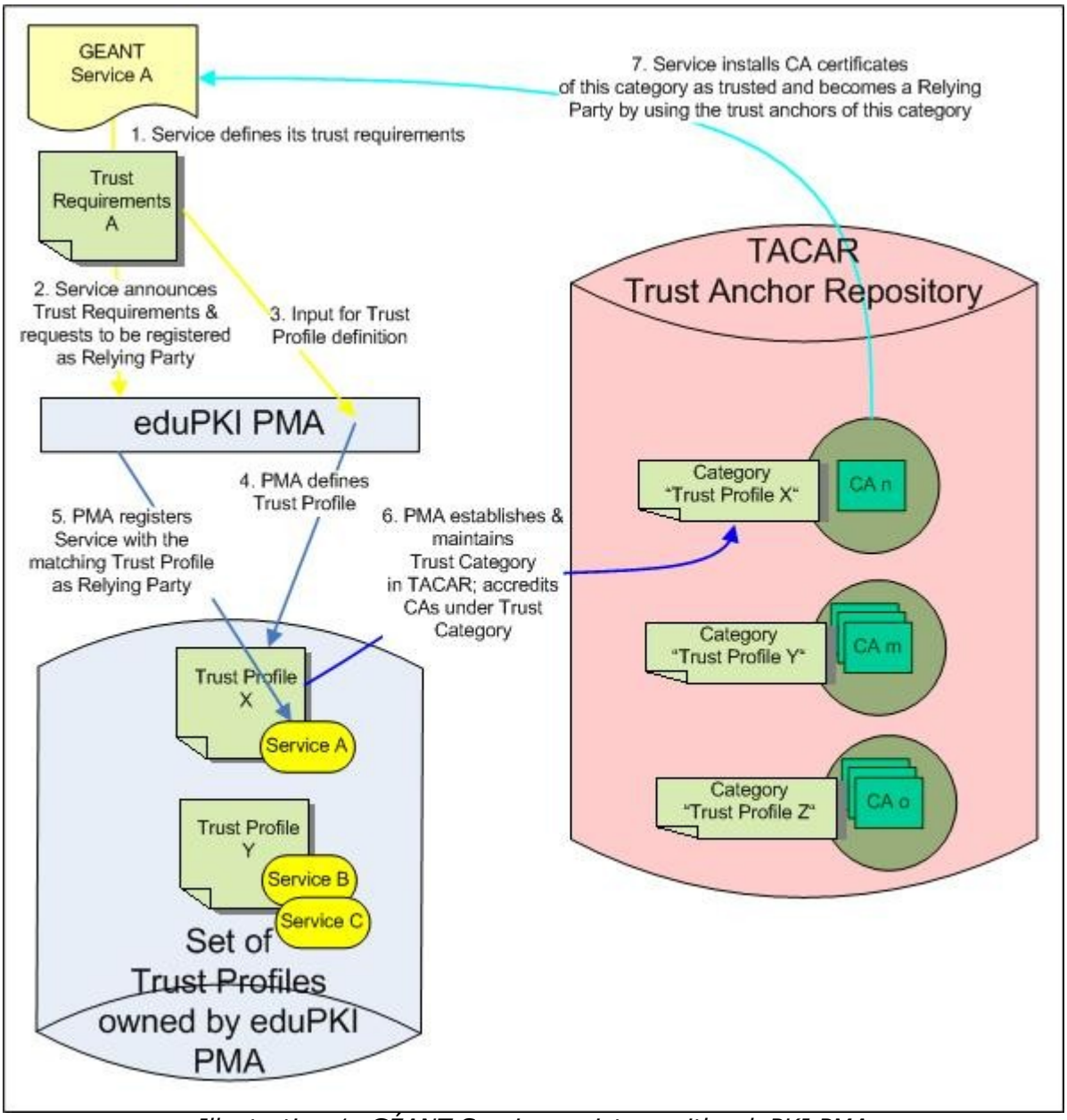

Illustration 1: GÉANT Service registers with eduPKI PMA

4.2 Expressing Interest

If a GÉANT Service including its infrastructure and users officially wants to rely on accredited trust anchors that are published by the eduPKI PMA Trust Anchor Repository it must register with the eduPKI PMA as a Relying Party. To get this registration process started a representative of the GÉANT Service needs to contact the eduPKI PMA chair with an supporting/endorsing letter of recommendation expressing the wish to register as Relying Party. The endorsing letter needs to be issued by organisations that support the applying GÉANT Service. The chair then initiates a direct contact between the GÉANT Service's representative and the Trust Team for further actions.

4.3 Assessing Trust Requirements

In order to become a Relying Party the trust fabric requirements, i.e. the requirements on the quality of identity assertions and vetting procedures as well as the supporting assertion infrastructure, of the GÉANT Service must be clear to find or define a matching eduPKI Trust Profile. The Trust Team is in charge of helping the GÉANT Service assessing its trust requirements and later choosing a suitable eduPKI Trust Profile on the base of the requirements.

4.4 eduPKI Trust Profiles

The Trust Team gathers trust fabric requirements from GÉANT Services that wish to deploy or use asserted identities based on X.509 digital certificates issued by a PKI for their authentication needs and – based on these requirements, best practices and standards – defines various sets of minimal criteria to be met and implemented by these PKIs. These sets of minimal criteria, called eduPKI Trust Profiles, represent the different requirements, trust characteristics and identity assertions that GÉANT Services have in regards to their authentication needs.

The Trust Team defines, publishes and maintains one or more common eduPKI Trust Profiles that are acceptable to GÉANT Services.

4.4.1 Choosing a suitable eduPKI Trust Profile

Once an applying GÉANT Service has stable and well defined trust requirements the Trust Team together with the GÉANT Service is choosing one or more eduPKI Trust Profiles that the GÉANT Service is going to be registered under as Relying Party.

The Trust Team evaluates the trust requirements and sees if they fit under an eduPKI Trust Profile. If a suitable eduPKI Trust Profile exists, the GÉANT Service is registered under this profile. If no suitable eduPKI Trust Profile exists, it needs to be decided if an existing eduPKI Trust Profile can be adjusted to meet the GÉANT Service's trust requirements without breaking trust between already registered Relying Parties and accredited identity assurers of the eduPKI Trust Profile or if a new eduPKI Trust Profile needs to be defined.

4.4.2 Defining eduPKI Trust Profiles

An eduPKI Trust Profile shall define and describe the minimal requirements in regards to PKI practices, operations and security that an identity assurer, i.e. a PKI with its CA, shall fulfil to be accredited under such eduPKI Trust Profile.

The outline of an eduPKI Trust Profile document is aligned with policy format described by RFC 3647 [RFC3647]. An eduPKI Trust Profile must specify its requirements in the relevant sections. An outline is provided below:

1. **INTRODUCTION**
2. **PUBLICATION AND REPOSITORY RESPONSIBILITIES**
3. **IDENTIFICATION AND AUTHENTICATION**
4. **CREDENTIAL LIFE-CYCLE OPERATIONAL REQUIREMENTS**
5. **FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**
6. **TECHNICAL SECURITY CONTROLS**
7. **CREDENTIAL, REVOCATION LIST, AND ONLINE CREDENTIAL STATUS PROTOCOL PROFILES**
8. **COMPLIANCE AUDIT AND OTHER ASSESSMENTS**
9. **OTHER BUSINESS AND LEGAL MATTERS**

A more detailed outline of an eduPKI Trust Profile is included in Appendix 1.

An eduPKI Trust Profile document must have a uniquely assigned Object Identifier (OID) under an eduPKI Trust Profile specific OID arc including the version number of the eduPKI Trust Profile document.

If an eduPKI Trust Profile defines that identities are assured by issuing X.509 certificates, the eduPKI Trust Profile must mandate that compliant end-entity certificates issued by accredited CAs under that eduPKI Trust Profile must contain at least three Policy OID certificate extensions:

- the OID of the base arc of the relevant eduPKI Trust Profile
- the full OID of the relevant eduPKI Trust Profile document that the issued certificate complies with
- the full OID of the relevant PKI CA policy document that the issued certificate complies with

Once an eduPKI Trust Profile is defined, the eduPKI PMA can accredit identity assurers under the eduPKI Trust Profile and creates an appropriate Trust Category within the TACAR under which the accredited identity assurers and their trust anchors can be listed [CA-ACC-PROC].

4.4.3 Updating eduPKI Trust Profiles

eduPKI Trust Profiles may be updated from time to time as needed e.g. to rephrase parts to clarify things or ambiguities, to correct errors or to include new technical or trust aspects into the eduPKI Trust Profile.

Any planned changes need to be communicated to the already registered GÉANT Services, i.e. Relying Parties, and to CAs already accredited or within the accreditation process under the eduPKI Trust Profile in order to consult with them that the planned changes are not breaking the trust of the Relying Parties nor breaking the compliance of the CAs. If the eduPKI PMA deems it necessary that an eduPKI Trust Profile needs an update, and the update is in effect, accredited CAs must update their practices and policies to comply with the updated eduPKI Trust Profile as soon as possible but within the next 12 months.

Whenever an eduPKI Trust Profile changes, its version number and thus the assigned OID of the eduPKI Trust Profile document must be changed.

4.5 Registering GÉANT Services

Once a GÉANT Service has chosen to become a Relying Party of a suitable eduPKI Trust Profile, the GÉANT Service name and contact person are registered by the eduPKI PMA under that eduPKI Trust Profile. Users and operators of a registered GÉANT Service can then download and use the accredited trust anchors of identity assurers (i.e. CA certificates) from the TACAR Trust Category associated with the chosen eduPKI Trust Profile. If the eduPKI Trust Profile under which a GÉANT Service is registered needs to be changed, the registered GÉANT Service will be consulted with in order to prevent the breaking of trust. Imminent changes to existing eduPKI Trust Profiles will be announced to all GÉANT Services registered under the changing eduPKI Trust Profile.

The eduPKI PMA may publish the information that a Service has registered as Relying Party under a specific eduPKI Trust Profile.

4.5.1 Maintaining GÉANT Services' contact data

Registered GÉANT Services are responsible to keep their contact data registered with the eduPKI PMA up-to-date.

4.6 De-registering GÉANT Services

If a registered GÉANT Service dissolves or does not want to be a registered Relying Party under a specific eduPKI Trust Profile for longer, the named contact person of the GÉANT Service informs the eduPKI PMA about this. In this case the GÉANT Service is no longer informed about (planned) changes to the eduPKI Trust Profile. And in due course trust matters might not fit the GÉANT Service's requirements no longer. Users and operators of the GÉANT Service should no longer base automated authentication decisions on trust anchors downloaded from the TACAR Trust Category.

The eduPKI PMA may publish the information about a GÉANT Service withdrawing from being registered as Relying Party under the specific eduPKI Trust Profile.

Glossary

The glossary is available online: https://www.edupki.org/documents/glossary

References

[CA-ACC-PROC] eduPKI PMA, description of the accreditation process and procedures for PKIs and their CAs, "eduPKI PMA CA Accreditation Process", 2010

[CHARTER] The eduPKI PMA Charter document, eduPKI PMA, "eduPKI PMA Charter", 2010

[GLOSSARY] The Glossary for eduPKI PMA documents. https://www.edupki.org/documents/glossary

[RFC3647] Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, IETF, Network Working Group, November 2003

Appendix 1 – Detailed eduPKI Trust Profile

More detailed outline of an eduPKI eduPKI Trust Profile:

1. INTRODUCTION
1.1 Overview
1.2 Document name and identification
1.3 Authentication Infrastructure participants
1.4 Credential usage
1.5 eduPKI Trust Profile administration
1.6 Definitions and acronyms
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES
2.1 Repositories
2.2 Publication of credential information
2.3 Time or frequency of publication
2.4 Access controls on repositories
3. IDENTIFICATION AND AUTHENTICATION
3.1 Naming
3.2 Initial identity validation
3.3 Identification and authentication for re-key requests
3.4 Identification and authentication for revocation request
4. CREDENTIAL LIFE-CYCLE OPERATIONAL REQUIREMENTS
4.1 Credential Application
4.2 Credential application processing
4.3 Credential issuance
4.4 Credential acceptance
4.5 Credential usage
4.6 Credential renewal
4.7 Credential re-generation
4.8 Credential modification
4.9 Credential revocation and suspension
4.10 Credential status services
4.11 End of subscription
4.12 Credential escrow and recovery
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS
5.1 Physical controls
5.2 Procedural controls
5.3 Personnel controls
5.4 Audit logging procedures
5.5 Records archival
5.6 Credential changeover
5.7 Compromise and disaster recovery
5.8 Credential Authority or Registration Authority termination
6. TECHNICAL SECURITY CONTROLS
6.1 Credential generation and installation
6.2 Credential Protection and Cryptographic Module Engineering Controls
6.3 Other aspects of Credential management
6.4 Activation data
6.5 Computer security controls
6.6 Life cycle technical controls
6.7 Network security controls
6.8 Time-stamping
7. CREDENTIAL, REVOCATION LIST, AND ONLINE CREDENTIAL STATUS PROTOCOL PROFILES
7.1 Credential profile