eduPKI PMA
CA Accreditation Process

Version 1.1.2

05.02.2016

Abstract

This document describes how an X.509 end entity certificate issuing Certification Authority can obtain eduPKI PMA accreditation under a specific eduPKI Trust Profile.

Creation and maintenance of this document has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Change History

Version	*Author*	*Date*	*Changes*
1.0	RKM	23.08.2010	Init
1.1	RKM	19.04.2011	Updated section 5.4
1.1.1	RKM	17.06.2013	Transition from GN3 to GN3+
1.1.2	RKM	05.02.2016	Transition from GN3 to GN4 incl. new CD

Table of Contents

1 Introduction

This document describes how an identity assurer, i.e. an X.509 end entity certificate issuing Certification Authority (CA) as part of a Public Key Infrastructure (PKI), can obtain eduPKI PMA accreditation under a specific eduPKI Trust Profile. Such accreditation is awarded to a CA after being successfully reviewed by the eduPKI PMA.

This document also describes

- how an accredited CA is securing its accreditation and
- how accreditation of an accredited CA is suspended or withdrawn.

As a CA is the central part of a PKI from hereafter the term CA is referring to the CA itself as well as the PKI it is embedded in.

2 Identification of this document

Name: eduPKI PMA CA Accreditation Process

Version: 1.1.2

Date: 05.02.2016

2.1 Change procedure

Changes to this document must be voted on by the CA Evaluation and Accreditation 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 Initial Accreditation of an Identity Assurer

The identity assurer, i.e. the CA, chooses an eduPKI Trust Profile to be reviewed against and applies to be accredited under this eduPKI Trust Profile. The eduPKI PMA's CA Evaluation and Accreditation Team is managing the accreditation. A successful accreditation states that the applying CA's policies, practices and operations in regards to certificate issuance as documented by the CA are compliant to the requirements set forth in the applicable eduPKI Trust Profile.

After a successful review and thus accreditation the CA's trust anchor, i.e. its CA certificate, as published through the eduPKI Trust Anchor Repository (which is the TERENA Academic CA Repository (TACAR)) is tagged as being accredited under the applicable eduPKI Trust Profile.

The following steps – as shown in illustration 1 – need to be undertaken to accredit a new CA:

1. CA expresses interest to be accredited and

2. applies for accreditation providing input for its eduPKI Trust Profile selection.
3. eduPKI PMA reviews and evaluates the CA against the chosen eduPKI Trust Profile and
4. registers the CA with this eduPKI Trust Profile after successful review and evaluation (accreditation).
5. CA uploads (and maintains) its Policy, CA certificate and contact data onto the eduPKI Trust Anchor Repository (TACAR).
6. eduPKI PMA assigns the CA to the Trust Category corresponding to the chosen eduPKI Trust Profile.

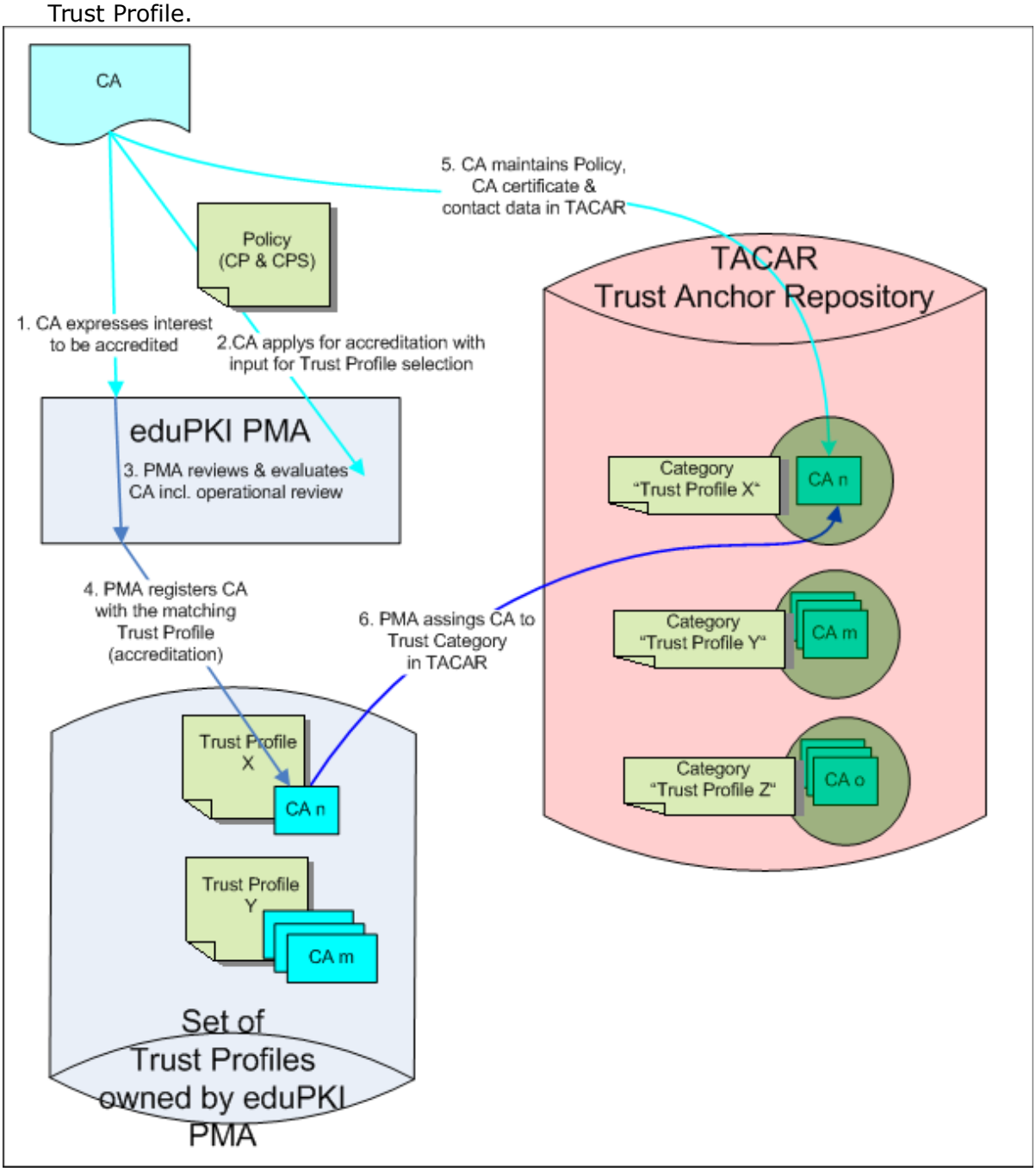

Illustration 1: CA requests accreditation under an eduPKI Trust Profile

4.1 Expressing interest

If a CA wants to get accredited under an eduPKI Trust Profile it needs to contact the eduPKI PMA in order to get the accreditation process started. The organisation owning the CA sends an official letter (signed by the upper management of the organisation owning the CA) of introduction to the eduPKI PMA naming two contact persons within the CA who will be responsible for the accreditation process on the side of the applying CA. All communication between the CA and the GÉANT eduPKI PMA is handled via the CA's named contact persons.

4.2 Application of a CA for accreditation

Once contact between the eduPKI PMA and the CA is established the eduPKI PMA checks if an accreditation of the interested CA is possible under the current GÉANT Charter, eduPKI PMA Charter [CHARTER] and by-laws.

The CA names the appropriate eduPKI Trust Profile it wants to be compliant with and sends to the eduPKI PMA

- policy documents, i.e. Certificate Policy (CP) and Certification Practice Statement (CPS), preferably formatted in RFC 3647 compliant style and
- any other documents deemed necessary to support the accreditation process

in English language as well as

- appropriate CA certificates (from the end entity certificate issuing CA up to the root CA),
- a selection of significant end entity certificates and
- Certificate Revocation Lists (CRLs)

if the CA is already in operation or accurate examples of these will look like.

4.3 Review of a CA for accreditation

eduPKI PMA's CA Evaluation and Accreditation Team is performing the review based on the eduPKI Trust Profile and the provided documents and materials. If necessary the Team will request clarifications or additional documents or files, etc., from the named contact persons.

An evaluation report is compiled by the Team and the findings are communicated to the CA's contact persons.

If there are deficiencies (based on the provided documents and materials) detected in the CA or its operations in regards to the chosen eduPKI Trust Profile or open questions arise, it is the responsibility of the CA's contact persons to provide the CA Evaluation and Accreditation Team with updated documents and answers. This process may go through several iterations until either the CA Evaluation and Accreditation Team is fully satisfied that the applying CA is compliant with the chosen eduPKI Trust Profile or the CA withdraws its application.

If the evaluation report states compliance with the chosen eduPKI Trust Profile the CA can be accredited.

4.4 Accreditation

If the outcome of the CA evaluation is successful the CA is registered and listed under the applicable eduPKI Trust Profile. The chair of the eduPKI PMA will inform the GÉANT management via its appointed contact persons about the accreditation.

The eduPKI PMA will inform Registered Relying Parties under the applicable eduPKI Trust Profile, i.e. registered GÉANT Services, see [SERV-REG-PROC], about the accreditation of the CA by email and publication on the eduPKI PMA website.

The CA certificate as published in the eduPKI Trust Anchor Repository is tagged with the applicable eduPKI Trust Profile's Trust Category.

4.5 Publishing in the eduPKI Trust Anchor Repository

Once a CA is successfully accredited under a specific eduPKI Trust Profile and the CA has published its trust anchors in the eduPKI Trust Anchor Repository (TACAR), the CA Evaluation and Accreditation Team assigns the relevant eduPKI Trust Profile's Trust Category tags to the accredited CA in the eduPKI Trust Anchor Repository.

5 Maintaining Accreditation

In order to keep its accreditation status a CA is obliged to perform updates, audits and resolve any detected deficiencies as described below.

Failure of any of these can result in suspension or withdrawal of the accreditation for the affected CA.

5.1 Update CA contact data

Accredited CAs are obliged to inform the eduPKI PMA about changes of their contact information and the appointed contact persons in a timely manner.

5.2 Update CA's Policies and Procedures

Accredited CAs are obliged to adjust their policies, procedures and operations according to updates and amendments of the applicable eduPKI Trust Profile as early as possible but within one year after the publication of the changed eduPKI Trust Profile. Ignoring changed requirements introduced by updates of the applicable eduPKI Trust Profile results in the suspension or withdrawal of the accreditation of affected CAs.

Whenever accredited CAs update their policy documents (other than layout, correcting spelling or unambiguous clarifications) they are obliged to notify the eduPKI PMA at least 30 days before its planned effective date providing the changed policy documents (or a download link to them) including a version highlighting the differences to the previous version as well as a short summary of the changes (all in English language).

5.3 Update CA's details published on the eduPKI Trust Anchor Repository

Accredited CAs are obliged to keep their information published on the eduPKI Trust Anchor Repository (TACAR) up-to-date.

5.4 Audits of accredited CAs

Accredited CAs are obliged to accept an audit request by the eduPKI PMA to check if their

- procedures and operations are in compliance with their policies and
- policies and such their procedures and operations are in compliance with the applicable eduPKI Trust Profile (per date at which the audit process is started).

An audit report (in English language) documenting the results of the requested audit and possibly detected deficiencies has to be compiled. If deficiencies are detected the completed audit report has to be sent to the eduPKI PMA immediately.

The eduPKI PMA may request the latest completed audit report (in English language) of their accredited CAs at their discretion. The CA Evaluation and Accreditation Team analyses the

requested audit report.

5.4.1 Auditor

The personnel performing the audit (auditor) of the CA may be external or internal to the CA. The auditor must have a sound understanding of PKIs, the involved standards, the applicable eduPKI Trust Profile and appropriate auditing practices.

5.5 Resolution of detected deficiencies

If any deficiencies in regards to the applicable eduPKI Trust Profile are detected an action plan and time-line is developed together with the affected CA to resolve the deficiencies in a coordinated way.

Depending on the severity of the detected deficiencies and its impact on the Relying Parties the affected CA may be suspended from accreditation until these deficiencies have been resolved.

The eduPKI PMA reserves the right to withdraw an accreditation of an affected CA that won't resolve detected deficiencies according to the negotiated plans.

6 Suspension / Withdrawal

The accreditation of a CA may be temporarily suspended or permanently withdrawn if deemed necessary by the eduPKI PMA to protect its Relying Parties or if the CA wishes to suspend or withdraw its accreditation.

If deficiencies in regards to a CA and

- its compliance with the applicable eduPKI Trust Profile or
- other security issues or
- trust related issues

with impact for the registered Relying Parties are detected, the severity of these is assessed and an action plan and time-line for their resolution is negotiated between the eduPKI PMA and the CA.

The affected CA must resolve the issues according to the agreed action plan and time-line. The eduPKI PMA will monitor the progress of the resolution of these issues in regards to the agreed action plan and time-line.

6.1 Suspension of Accreditation

The accreditation of a CA may be temporarily suspended if deficiencies are detected in regards to

- the compliance of the CA with the applicable eduPKI Trust Profile or
- other security or trust related issues that have a severe impact on the security of Relying Parties and the trust they put into the set of accredited CAs.

Other security and trust related issues may arise that prompt the temporary suspension of accreditation of an accredited CA.

The CA itself may ask the eduPKI PMA for temporary suspension.

When a CA is temporarily suspended from accreditation

- the CA is removed from the eduPKI Trust Anchor Repository, see section 6.3,
- the registered contact persons of the registered Relying Parties of the applicable eduPKI Trust Profile are notified by email,

- the CA is listed as '*suspended*' under the applicable eduPKI Trust Profile's registered CAs on the eduPKI PMA's web site, a reason for the suspension may be given and
- the registered contact persons of the affected CA are notified by email.

When the reasons for suspension of accreditation have been resolved

- the CA's accreditation status is restored,
- the registered contact persons of the applicable Relying Parties are notified by email,
- the affected CA is notified by email and
- the CA is listed as 'accredited' under the applicable eduPKI Trust Profile's registered CAs on the eduPKI PMA's web site.

6.2 Withdrawal of Accreditation

The accreditation of a CA is withdrawn if there are permanent deficiencies detected in regards to the compliance of the CA with the applicable eduPKI Trust Profile that have a severe impact on the security of Relying Parties and the trust they put into the set of accredited CAs and these deficiencies are not resolved according to the negotiated action plan and time-line.

When the accreditation of a CA is withdrawn

- the CA is removed from the eduPKI Trust Anchor Repository, see section 6.3,
- the registered contact persons of the registered Relying Parties of the applicable eduPKI Trust Profile are notified by email,
- the CA is listed as '*removed*' under the applicable eduPKI Trust Profile's registered CAs on the eduPKI PMA's web site for a period of time, a reason for withdrawal may be given and
- the registered contact persons of the affected CA are notified by email.

The CA can re-apply for accreditation following the outlined accreditation process, see section 4.

6.3 Removal from eduPKI Trust Anchor Repository

Once an accreditation of a CA is withdrawn or suspended in accordance with the eduPKI PMA accreditation process and the CA has published its trust anchors at the eduPKI Trust Anchor Repository (TACAR) the CA Evaluation and Accreditation Team removes the relevant eduPKI Trust Profile's Trust Category tags from the CA in the eduPKI Trust Anchor Repository in a timely manner.

Glossary

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

References

[CHARTER] The eduPKI PMA Charter document, eduPKI PMA, "eduPKI Policy Management Authority Charter", 2016

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

[SERV-REG-PROC] eduPKI PMA, description of the registration process and procedures for GÉANT Services, "eduPKI PMA GÉANT Services Registration Process", 2016