eduPKI Trust Profile for Generic Server- and Client-Machine-Certificates

Version 1.1

05.06.2014

Abstract

This is the eduPKI Trust Profile for Generic Server and Client-Machine-Certificates, specifying their minimum requirements in regards to digital Certificates and associated identity assertions used within these GÉANT Services.

Change History

Version	***Author***	***Date***	***Changes***
1.1	RKM	05.06.2014	Init

Table of Contents

1 Introduction

1.1 Overview

This eduPKI Trust Profile (TP) document defines the requirements on Public Key Infrastructures (PKIs) issuing public key digital Certificates to infrastructure nodes (network endpoints) such as Internet services (servers) or Internet clients (client machines).

This TP is formatted according to RFC 3647 [RFC3647].

Within this document the words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY' and 'OPTIONAL' are to be interpreted as in RFC 2119 [RFC2119].

1.2 Document name and identification

This document is the *eduPKI Trust Profile for Generic Server- and Client-Machine-Certificates* version 1.1*.* It is identified by the following Object Identifier (OID):

`1.3.6.1.4.1.27262.1.13.1.3.1.1`

The OID is constructed as follows: ISO assigned OIDs (1) . ISO Identified Organization (3) . US Department of Defense (6) . Internet (1) . Internet Private (4) . IANA-registered Private Enterprises (1) . DANTE Ltd. (27262) . GÉANT (1) . eduPKI (13) . eduPKI Trust Profiles (1) . eduPKI Trust Profile for Generic Server- and Client-Machine-Certificates (3) . Major Version (1) . Minor Version (1)

1.3 PKI participants

This TP affects Certification Authorities (CAs) issuing Certificates to infrastructure nodes (i.e. servers and client machines) operated by or for the GÉANT community.

The Subscribers of these CAs are organisations operating infrastructure nodes (i.e. servers or client machines) within or for the GÉANT community.

The Relying Parties (RPs) are services and their operators as well as client machine owners within the GÉANT community relying on the trustworthy identification of network endpoints used for TLS-secured Internet traffic.

This TP is not applicable and does not apply to client certificates identifying persons, i.e. personal user certificates.

1.4 Certificate Usage

No stipulation.

1.5 eduPKI Trust Profile administration

This TP is maintained by the eduPKI Policy Management Authority (eduPKI PMA).

The eduPKI PMA may be contacted by email at pma@edupki.org. Further information about the eduPKI PMA is available at its web-site www.edupki.org.

Suitability of a CA's policy documents for this TP is collectively determined by the eduPKI PMA in accordance with the GÉANT eduPKI CA Accreditation Process [CA-ACC-PROC].

A CA applying for accreditation under this TP MUST deliver its Certificate Policy (CP) and Certification Practice Statement (CPS) to the eduPKI PMA.

The eduPKI PMA SHALL evaluate the CP and CPS for its compliance with this TP. In case of any discrepancies, the eduPKI PMA MAY propose changes to the CA's procedures or other measures to reach the compliance. When all stipulations of this TP are satisfied to the best knowledge of the eduPKI PMA, the eduPKI PMA SHALL inform the CA that it has been accredited to issue Certificates under this TP.

The eduPKI PMA MAY at its own discretion refuse to process any CA application.

The eduPKI PMA MAY at its own discretion require a compliance audit of any applying or accredited CA.

1.6 Definitions and acronyms

Certification Authority (CA)

A Certification Authority issues X.509 Certificates and publishes revocation and status information about the issued Certificates.

Conforming CA

A Certification Authority acting in compliance with this TP.

eduPKI Trust Profile (TP)

Definition of minimum requirements of a GÉANT Service in regards to the quality of identity assertions and vetting procedures as well as the supporting assertion infrastructure.

Transport Layer Security (TLS)

A protocol defined by the Internet Engineering Task Force (IETF) in “The Transport Layer Security (TLS) Protocol” [RFC5246].

Definitions and acronyms are also available in an online glossary [GLOSSARY].

2 Publication and repository responsibilities

A Conforming CA SHALL make information needed for using its services publicly available, namely:

- the issuing CA Certificate and all Certificates required to verify an end-entity Certificate chain up to a self-signed root;
- the current Certificate Revocation List (CRL) issued by the issuing CA and all CRLs required to verify all Certificates in the end-entity Certificate chain;
- the CP and CPS documents;
- an official email address for enquiries and fault reporting.

The information SHALL be published in the CA's official repository as well as in the TERENA Academic CA Repository (TACAR) which is used as the eduPKI Trust Anchor Repository.

3 Identification and authentication

3.1 Naming

A Conforming CA SHALL assign each infrastructure node, that it issues a Certificate to, a unique Subject Name. The Subject Name MUST be a valid X.500 Distinguished Name.

Any Subject Name MUST be assigned to one and only one infrastructure node and MUST never be assigned to a different node.

Certificates issued under this TP MUST contain the fully qualified domain name(s) of the infrastructure node as *dNSName* in the *SubjectAltName* Certificate extension.

Certificates issued under this TP MAY contain the IP address(es) of the infrastructure node included as *iPAddress* in the *SubjectAltName* Certificate extension.

Certificates issued under this TP MAY contain one or more email address(es) of the infrastructure node's administrator(s) included as *rfc822Name* in the *SubjectAltName* Certificate extension.

All names SHALL be interpreted as defined in RFC 5280 [RFC5280].

3.2 Initial identity validation

A Conforming CA MUST verify that the Requester is authorised to use all names (O-attribute value, FQDNs, email addresses, IP addresses) contained in the requested Certificate under this TP.

A Requester SHALL be identified by his/her email address verified and asserted by the pertinent GÉANT partner. Certificate Applications MUST be authenticated by applying a (digital) signature to it (which is based on a key) that is known to be bound to the well-known Requester/Requester's pre-registered email address.

The RA (Registration Authority) MUST consult the pertinent GÉANT partner to confirm that a Requester is authorised to receive the requested Certificate for all included names.

The authorisation MUST be approved by the pertinent GÉANT partner applicable. The RA MUST check the authorisation by requesting authorisation information from the pertinent GÉANT partner with a secured call-back procedure, i.e. validating a digital signature of an authorisation statement against a pre-registered public key and email address of the pertinent GÉANT partner; or validating a handwritten signature on an authorisation statement against well-known pre-registered signatures of staff members of the pertinent GÉANT partner; or checking with the pertinent GÉANT partner by phone if the voice of the GÉANT partner's staff member is well-known to the RA staff performing the validation.

3.3 Identification and authentication for re-key requests

A Conforming CA SHALL NOT support Certificate re-keying. Any application for a Certificate renewal of any kind is treated like an initial Certificate Application.

3.4 Identification and authentication for revocation request

Requests for Certificate revocation made by Subscribers, RAs and the CA MUST be properly authenticated. Other entities MAY request Certificate revocation if they can prove compromise or exposure of the corresponding private key.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

A Certificate Application SHALL contain the public key and all the names to be certified.

Certificate Applications MUST be delivered to the CA using a secure and authenticated method.

4.2 Certificate Application processing

Upon receiving a Certificate Application, the RA SHALL:

1. verify the identity of the Requester
2. verify the authorisation of the Requester
3. verify all requested names in the application

Only if all steps above are successful, the application SHALL be relayed to the CA to issue the Certificate.

4.3 Certificate issuance

No stipulation.

4.4 Certificate acceptance

No stipulation.

4.5 Key pair and Certificate usage

The Certificate and the corresponding key pair MUST be used only in compliance with the relevant CP and for purposes indicated in the Certificate, primarily for authenticating infrastructure nodes to each other.

4.6 Certificate renewal

A Conforming CA SHALL NOT support Certificate renewal for Certificates issued compliant to this TP. Any application for a Certificate renewal of any kind is treated like an initial Certificate Application.

4.7 Certificate re-key

A Conforming CA SHALL NOT support Certificate re-keying for Certificates issued compliant to this TP. Any application for a Certificate renewal of any kind is treated like an initial Certificate Application.

4.8 Certificate modification

A Conforming CA SHALL NOT support Certificate modification for Certificates issued compliant to this TP. Any application for a Certificate renewal of any kind is treated like an initial Certificate Application.

4.9 Certificate revocation and suspension

A Certificate MUST be revoked if any of the following circumstances occurs:

1. The private key associated with the Certificate has been compromised or exposed.
2. The content of the Certificate is not representing the truth.
3. The Subscriber has breached its obligations.

Revocation MAY be requested by the Subscriber, by an RA, by the CA or by any entity that can prove a circumstance for revocation.

The entity detecting that a circumstance for revocation has occurred MUST request the Certificate revocation immediately, but not later than within one working day.

Revocation requests SHALL be submitted to an RA or to the CA.

The RA or CA MUST react to the submitted revocation request immediately, but not later than within one working day.

RPs MUST check the revocation status of a Certificate before relying on it.

A Conforming CA SHALL issue CRLs. A new CRL SHALL be issued after a Certificate revocation or not later than 24 hours before the time stated in the *nextUpdate* field in the current CRL. The *nextUpdate* field MUST NOT be set to a time later than 30 days after the time of the CRL issuance.

A Conforming CA SHALL NOT support Certificate suspension for Certificates compliant to this TP.

4.10 Certificate status services

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

A Conforming CA SHALL NOT support key escrow for Certificates compliant to this TP.

5 Facility, management, and operational controls

5.1 Physical Controls

The CA system SHALL be located in a secure location. Physical access to the location SHALL be monitored and enabled only to the CA personnel.

5.2 Procedural controls

No stipulation.

5.3 Personnel controls

The CA personnel SHALL be trained in using PKI technologies and in the CA procedures.

5.4 Audit Logging Procedures

A Conforming CA SHALL keep logs of the following events:

- initialization of the CA systems
- CA private key activation and deactivation
- access to the CA systems
- Certificate issuance
- Certificate revocation
- CRL issuance

The logs SHALL be secured against unauthorized access.

The logs SHALL be available to the CA personnel and to auditors.

5.5 Records archival

A Conforming CA SHALL keep the following types of records:

- the CA Certificate
- all issued Certificates
- all issued CRLs
- all CPs applied to issue Certificates
- all CPSs applied to issue Certificates

- all audit logs

A record SHALL be retained for at least one year after the relevant Certificates pertaining to that record have expired.

The record archive SHALL be protected against unauthorized access.

The records SHALL be accessible only to the CA personnel and to the auditors.

A Conforming CA SHOULD keep backup copies of the archived records. The backup SHOULD be stored in a secure off-site location. The backup MUST be protected against unauthorized access.

5.6 Key changeover

During a CA signing key changeover, the CA MUST provide for a transition period when only the new key is being used to sign new Certificates and the old key is being used to issue CRLs for the old Certificates. The old key MUST be available as long as all Certificates signed by it have not expired.

5.7 Compromise and disaster recovery

If the key material of a Conforming CA is compromised, the CA SHALL

- immediately inform all PKI participants,
- stop accepting Certificate Applications,
- revoke all issued Certificates,
- publish the CRL with the *nextUpdate* field set to a time after the expiration dates off all issued Certificates,
- request the revocation of all pertinent CA Certificates if signed by an other CA,
- stop operations,
- start analysis of the events leading to the key compromise,
- remove the cause of the key compromise,
- generate new keys,
- restart operations.

In case of a disaster not involving a CA key compromise, the system and the keys SHOULD be recovered from backups.

5.8 CA or RA Termination

A Conforming CA SHALL announce its intent to cease operation at least three months before the termination.

At the date of termination, the CA SHALL:

- revoke all issued Certificates
- publish the CRL with the *nextUpdate* field set to a time after the expiration dates off all issued Certificates,
- destroy the CA keys,
- stop the operation.

A terminating RA SHALL relay all its documentation to the CA or the RA's organisation MUST keep the RA's documents according to the defined retention periods. The CA SHALL disable access of the RA to the CA systems.

6 Technical security controls

6.1 Key pair generation and installation

The CA keys MUST be generated by authorised CA personnel. The CA RSA keys SHALL be at least 2048 bits long.

End-entities' RSA keys in Certificates compliant to this TP SHALL be at least 2048 bits long.

6.2 Private key protection and cryptographic module engineering controls

Private keys of a Conforming CA SHALL be protected with a pass-phrase of at least 15 characters when stored in a software security token. Private keys of a Conforming CA stored in a hardware security module (HSM) SHALL be protected to achieve similar or better key protection.

Backups of the CA private keys MUST be protected at the same level as the operational copies.

The CA private key SHALL be activated only by authorised CA personnel.

The end-entity private key MAY be stored unencrypted on the infrastructure node's file-system. In that case, the operating system MUST be set to prevent unauthorised access to the key.

Backups of end-entity private keys MUST always be encrypted using a key known only to authorized personnel.

6.3 Other aspects of key pair management

No stipulation.

6.4 Activation data

The pass-phrase protecting a CA private key SHALL be known only to authorised CA personnel.

6.5 Computer security controls

The computer hosting the Conforming CA system MUST run only software required to operate the CA.

6.6 Life cycle technical controls

No stipulation.

6.7 Network security controls

When a Conforming CA uses its private key from a software security token, the CA system MUST be kept disconnected of any network.

The CA system MAY be accessible from the Internet or other public network only if all the following conditions are met:

- The CA uses a HSM certified to at least FIPS 140-2 level 3 or equivalent to protect its private keys.
- The access to the CA system is limited only to the CA services.
- The access to the CA system is monitored.

6.8 Time-stamping

No stipulation.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate Profile

Certificates and CRLs issued by a Conforming CA SHALL follow the PKIX Certificate Profile as defined in RFC 5280 [RFC5280]. The following text further profiles the PKIX profile for use by infrastructure nodes.

All Certificates SHALL be X.509 version 3.

End-entity Certificates SHALL contain the following extensions:

a) Authority Key Identifier

the identifier of the key of the issuer in the *keyIdentifier* field

b) Subject Key Identifier

the identifier of the certified key

c) Basic Constrains

`false` in the *cA* field

d) Key Usage

bits *digitalSignature* and *keyEncipherment* set

e) Extended Key Usage

TLS server authentication and/or *TLS client authentication*

f) Certificate Policies

This extension SHOULD contain only *policyIdentifiers.* Their value SHALL be:

- the full OID of the TP applicable when issuing the Certificate, i.e. **1.3.6.1.4.1.27262.1.13.1.3.1.1**
- the OID of the base arc of this TP, i.e. **1.3.6.1.4.1.27262.1.13.1.3**
- the OID of the CP applied when issuing the Certificate

Further *policyIdentifiers* MAY be included.

g) Subject Alternative Name

- DNS name(s) of the infrastructure node in the *dNSName* field
- (optionally) IP address(es) of the infrastructure node in the *iPAddress* field

- (optionally) email address(es) of the infrastructure node's administrator(s) in the *rfc822Name* field

h) **CRL Distribution Point**

- at least one HTTP URL where the current DER encoded CRL for the Certificate is published in the *URI* field

End-entity Certificates SHOULD contain the following extensions:

a) **Authority Information Access**

- at least one HTTP URL where the issuer's DER encoded Certificate is published in the *URI* field for the *cAIssuers* access method
- (optionally) the OCSP locator in the *URI* field for the *OCSP* access method

The Certificate extensions listed MAY contain other additional values at the discretion of the CA.

Certificates MAY contain other additional extensions at the discretion of the CA.

7.2 CRL Profile

All CRLs SHALL conform to CRL version 2 as specified by the X.509 recommendation.

All CRLs SHOULD contain the following extensions:

a) **CRL Number**

- a sequential number of the CRL

CRLs MAY contain other extensions at the discretion of the CA.

7.3 OCSP Profile

No stipulation.

8 Compliance audit and other assessment

A Conforming CA SHALL enable a compliance audit by an entity appointed by the eduPKI PMA.

9 Other business and legal matters

No stipulation.

References

[RFC3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, RFC 3547, November 2003.

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, RFC 2119, March 1997.

[CA-ACC-PROC] eduPKI PMA, *eduPKI PMA CA Accreditation Process*, eduPKI PMA Governing Document, April 2013.

[RFC5246] T. Dierks, E. Rescorla, *The Transport Layer Security (TLS) Protocol*, RFC 5246, August 2008.

[GLOSSARY] eduPKI, *Glossary*, https://www.edupki.org/documents/glossary, August 2010.

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 5280, May 2008.