SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

SWITCHpki Identity Validation for User Certificate Requests

Version 2.0, May 2014

1. Roles and terminology

Applicant: The legal entity on behalf of which a SWITCHpki digital certificate is applied for.

CA Outsourcing Provider: The Certification Authority which is operating the technical infrastructure for issuing SWITCHpki user certificates.

Certification Authority (CA): An organization that is responsible for the creation, issuance, revocation, and management of certificates.

Certificate Holder: A natural person who is a holder of a SWITCHpki digital certificate. A Certificate Holder is (i) named in a digital certificate and (ii) holds a private key corresponding to the public key listed in that digital certificate.

Certificate Approver: A natural person who is employed by the Applicant and who has express authority to represent the Applicant to approve certificate requests submitted by other Certificate Holders.

Registration Authority (RA): An entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. SWITCH may act as an RA for other Applicants, in particular for carrying out steps on the technical level (such as initiating the issuance of a user certificate through a Web interface provided by the CA Outsourcing Provider).

Validation: This term is used to indicate a verification step in the procedure.

2. Scope

This document provides an overview of the validation procedures relating to a SWITCHpki user certificate request. The validation consists of two main parts:

1. an initial, pre-validation procedure
2. a per-certificate validation procedure

These validation procedures help provide reasonable assurance that:

- the organization (whose name will be included in the SWITCHpki user certificate) exists, has signed up for participation in the SWITCHpki program and has been subject to the required validation checks;
- the Certificate Holder for a SWITCHpki user certificate is affiliated with the organization;
- each certificate request is approved by a nominated Certificate Approver;
- for each certificate the Certificate Holder agrees with the relevant Certificate Holder Agreement of the CA Outsourcing Provider;
- for each certificate, the Applicant is authorized to request a SWITCHpki user certificate which includes e-mail addresses ending in the requested domain name(s)

The procedure operates within these limitations:

- The Registration Authority will only process SWITCHpki user certificate requests from Applicants and Personnel that have been pre-validated;

- All (pre-validation) registries and verification documents and proof of validation (paper or electronic) must be open to inspection and/or verification by the CA Outsourcing Provider.

3. Pre-validation procedure

The pre-validation phase only refers to the initial accreditation of the Applicant, not to individual certificate requests (see section 4).

3.1. Personnel and Organization Validation

The Applicant submits the “SWITCHpki RA Agreement” that has been completed, printed and signed by a legal representative of the Applicant. Signing this RA agreement binds the organization to the relevant Certificate Policy/Certification Practice Statement and Certificate Holder Agreement of the respective CA Outsourcing Provider. With the SWITCHpki RA Agreement the Applicant also submits its Articles of Association/Incorporation or any other official document proving the legal existence of the Applicant. SWITCH representatives will perform verification checks on the Applicant and confirm that the signature on the SWITCHpki RA Agreement is that of a legal representative.

The Applicant also submits the “SWITCHpki certificate applicant proxy” form to the Registration Authority. This proxy must be completed, printed out and signed by a legal representative of the Applicant. This proxy formally grants authority to the representatives who can approve certificate requests (“Certificate Approvers”) on behalf of the Applicant. SWITCH representatives will perform verification checks on the relevant representatives of the Applicant.

3.2. Domain Ownership Validation

The representatives of the Applicant must submit domain names to the Registration Authority for pre-validation. Upon receipt of such a request the Registration Authority will verify the ownership of each of the domain names, the appropriate official domain name registry for that particular domain name and maintain proper records of this verification. Pre-validated domain names must be re-validated every 39 months or when indications of change of ownership have been received.

4. Request Validation

4.1. Certificate Holder identity vetting procedure

The identity of every Certificate Holder must be validated by the relevant Registration Authority (RA) based on a nationally recognized identity document (identity card or passport, valid at the time the request is submitted). The Certificate Approver must check the presented identity document and make sure that a copy is archived. The completed and signed SWITCHpki User Certificate Application Form must be archived for at least 7 years after expiration or revocation of the relevant digital certificate; copies of ID documents may be destroyed 3 years after expiration or revocation of the relevant digital certificate.

For Grid user certificate requests, either a face to face meeting with a Certificate Approver or an identification via the Swiss Post’s “Yellow Identification” service (http://www.post.ch/gelbeidentifikation) is mandatory. For these types of requests, the identity vetting of a Certificate Holder will be considered valid for a maximum of three years, after which period the identity of the Certificate Holder will have to be reassessed as new i.e. the Certificate Holder will have to appear in person again.

4.2. Certificate request validation procedure

4.2.1. General procedure

In general each issuance of a SWITCHpki user certificate is initiated by the Registration Authority based on the submission of a duly signed user certificate application form.

Upon submission of the form, the Registration Authority verifies that:

- The Applicant is present in the appropriate pre-validation registry of the Registration Authority;
- A signed “SWITCHpki RA Agreement” is present that has been signed by a nominated Contract Signer and that binds the Applicant to the relevant Certificate Policy/Certification Practice Statement and Certificate Holder Agreement of the selected CA Outsourcing Provider;
- The Certificate Approver is one of the nominated Certificate Approvers for the Applicant;
- For digitally signed application forms: the Registration Authority will verify the correctness of the digital signature (signer certificate must represent one of the nominated Certificate Approvers);
- For application forms submitted in the form of a scan of a hardcopy document: the Registration Authority will verify that the signature of the Certificate Approver on the document scan is that of an authorized Certificate Approver.
- The ownership of each of the domain names in the request via an internal registry of pre-validated domain names.

Not all of these steps are necessarily carried out manually by an RA operator; some of them may be implemented via technical means (e.g. restricting the list of available domain names for e-mail addresses when initiating the issuance of a certificate).

The CA Outsourcing Provider must at any time and for each certificate request be able to cross check the verification steps described above i.e. asking for paper or electronic proof. The Registration Authority must therefore maintain evidence of the documents associated with the certificate request and related validation.

4.3. Digital signatures

Digital signatures can be provided in the form of S/MIME signed messages or signed PDF documents. The X.509 certificates used for signing need to have an assurance level matching the one of the Normalised Certificate Policy (NCP) described in ETSI TS 102 042 *(“Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”)*. The use of X.509 certificates issued by a third-party CA is subject to prior approval by the CA Outsourcing Provider.