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

SWITCHpki Identity Validation for Server Certificate Requests

Version 1.0, October 2008

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

1. Scope

This document provides an overview of the validation procedures relating to a SWITCHpki server 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 (on behalf of which a Certificate Requester requests a SWITCHpki server certificate) exists, has signed up for participation in the SWITCHpki program and has been subject to the required validation checks;
- the Certificate Requestor for a SWITCHpki server certificate is authorized to act on behalf of their organization;
- each certificate request is approved by a nominated Certificate Approver
- for each certificate the Applicant agrees with the relevant subscriber agreement of the CA Outsourcing Provider;
- for each certificate, the Applicant is authorized to request a SWITCHpki server certificate for the requested domain name(s); and
- Extended Validation (EV) Certificates are issued in accordance with the “Guidelines for the Issuance and Management of Extended Validation Certificates” (EV Guidelines) issued by the CA/Browser forum (http://www.cabforum.org).

The procedure operates within these limitations:

- The Registration Authority will only accept SWITCHpki server 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;
- EV certificates will only be issued once all of the relevant requirements of the EV guidelines have been met.

2. Roles and terminology

Applicant: The organization on behalf of which a SWITCHpki server certificate is requested.

CA Outsourcing Provider: The certification authority which is operating the technical infrastructure for issuing SWITCHpki server certificates.

Certificate Requester: A natural person who is employed by (or is an agent of) the Applicant and who completes and submits a certificate request on behalf of the Applicant.

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 Requesters.

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

Confirming Person: A person employed by the Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact.

Contract Signer: A natural person who is employed by the Applicant who has express authority to represent the Applicant and sign RA agreements and Subscriber Agreements.

Extended Validation (EV) Certificate: A certificate that contains information specified in the "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines) and that has been validated in accordance with these guidelines.

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

3. Extended Validation (EV) Certificates

An Extended Validation (EV) Certificate is a certificate that contains information specified in the "Guidelines for the Issuance and Management of Extended Validation Certificates" (EV Guidelines) and that has been validated in accordance with these guidelines, which are published by the CA/Browser Forum (http://www.cabforum.org).

EV Certificates are used for the following purposes:

(a) Primary purposes of an EV Certificate are to:
- Identify the legal entity that controls a website, with validated information in the EV Certificate including Name, Address, Jurisdiction, and Registration Number; and
- Enable/encrypted communications with a website.

(b) Secondary purposes of an EV Certificate are to provide reliable third-party verified identity and address information regarding the owner of a website that may be used to:
- Make it more difficult to mount phishing and other online fraud attacks using SSL certificates;
- Assist companies by providing them with a tool to better identify themselves and their legitimate websites to users; and
- Assist law enforcement in investigations of online fraud.

SWITCHpki EV SSL certificates will be issued in conformance with the latest version of the EV guidelines published at http://www.cabforum.org.

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

4. Pre-validation procedure

4.1. Personnel and Organization Validation

The Applicant submits the “SWITCHpki RA Agreement” that has been completed, printed and signed by a legal representative (Confirming Person) of the Applicant. Signing this RA agreement binds the organization to the relevant Certificate Policy/Certification Practice Statement and Subscriber 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. For organizations that will be requesting EV certificates these organization verification checks will be performed in accordance with the EV Guidelines. This will include verification checks on the legal existence, identity, physical existence, operational existence and telephone number.

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 (Confirming Person) of the Applicant. This proxy formally grants authority to the representatives who can approve certificate requests (“Certificate Approvers”) and sign RA Agreements/Subscriber Agreements (“Contract Signers”) on behalf of the Applicant. SWITCH representatives will perform verification checks on the relevant representatives of the Applicant. For organizations that will be requesting EV certificates, these verification checks will be performed in accordance with the EV Guidelines. In particular, one of the authorized Contract Signers has to submit a signed version of the subscriber agreement for EV certificates.

4.2. Domain Ownership Validation

4.2.1. Pre-validated domain names

The representatives of the Applicant can submit domain names to the Registration Authority to be pre-validated. 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 when indications of change of ownership have been received. To make sure ownership has not changed since pre-validation, the RA administrator must always perform a brief check of domain name ownership in the pre-validation registry before issuance of the server certificate.

4.2.2. Non pre-validated domain names

For domain names that have not been pre-validated the domain name ownership will be checked through querying the appropriate official registry:

- gTLD domain names can be verified using registries listed at http://www.icann.org/registries/listing.html
- ccTLD domain names can be verified using registries listed at http://www.iana.org/cctld/cctld-whois.htm

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

Registries not listed above need to be approved by the CA Outsourcing Provider.

4.2.3. Domain Names for Extended Validation Certificates

For organizations that will be requesting EV certificates, Domain verification checks will be performed in accordance with the relevant requirements of the EV Guidelines. This includes verifying that the domain name satisfies the following requirements:

1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);

2) The domain registration information in the WHOIS database should be public and should show the name, physical address and administrative contact information for the organization;

3) The Applicant is the registered holder of the domain name or has been granted exclusive right to use the domain name by the registered holder of the domain name;

4) The Applicant is aware of its registration or exclusive control of the domain name;

5) The domain or Applicant is not identified as likely to be “high risk” of being targeted for fraudulent attacks.

4.3. Request Validation

4.3.4. Per certificate validation procedure

Each SWITCHpki server certificate request results in an email challenge sent to the Certificate Approver, containing details of both the certificate request (such as the DN) and the Certificate Requester.

The Certificate Approver must sign and return this email challenge to the Registration Authority. The available methods are:

- by signed postal mail;
- a signed fax;
- an email with a scan of the signed form;
- a signed email.

Upon receipt of the signed email challenge, the Registration Authority verifies:

- 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 Subscriber Agreement of the selected CA Outsourcing Provider.
- The certificate request in the registration form is equal to the request online (crosscheck);
- The Certificate Approver is one of the nominated Certificate Approvers listed on the “SWITCHpki certificate applicant proxy” form;

- For challenges returned via signed email: the Registration Authority will verify the correctness of a digital signature (name, organization and certificate validity);
- For challenges returned with hardcopy signatures: the Registration Authority will verify that the signature of the Certificate Approver on the email challenge is that of a nominated Certificate Approver listed on the “SWITCHpki certificate applicant proxy” form. For EV Certificate requests, this verification will be performed in accordance with the acceptable verification methods listed in the EV Guidelines.
- The ownership of each of the domain names in the request via either the appropriate official domain name registry for that particular domain name or an internal registry of pre-validated domain names.
- For Extended Validation Certificates, the Registration Authority will check that all required personnel, organization and domain validation steps have been performed in accordance with the EV Guidelines.

The CA Outsourcing Provider must at any time and for each certificate request be able to check whether or not the verification steps described above have been performed (i.e. ask for paper proof or electronic proof).

4.3.5. Signed email

E-mail signatures can be provided as S/MIME messages using X.509 user certificates. The certificates need to have an assurance level matching the one of either SwissSign Silver or QuoVadis Standard Commercial certificates. The use of X.509 certificates which are issued by a third-party CA is subject to prior approval by the CA Outsourcing Provider.