Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

NICHT KLASSIFIZIERT

Checklist for approval of applications for SSL/TLS certification to Swiss Government PKI certificate authorities

1.0, 12.05.2016

Application number SG-PKI (reference): Approval_SSL_ _ CA III_

Applicant: **Dept/Office:** **FQDN:**

Check: **OV** ◯ **EV** ◯

DV certificates (SG PKI Policy OIDs …/…):

Domain validated or DV certficates are checked with the name of the domains applied for. Swiss Government PKI does not offer DV certificates.

OV certificates (SG PKI Policy OIDs 2.16.756.1.17.3.62.1/2.16.756.1.17.3.62.2)

Organisation validated or OV certificates require more validation steps than required for DV certificates. The organisation that applied for the certificate is checked for this type. The organisation's name is listed in the certificate. This provides greater assurance that both the website and the organisation are reputable. OVs are generally used by companies, governments and other establishments that want to offer their users an additional layer of trust.

EV certificates (SG PKI Policy OIDs 2.16.756.1.17.3.62.4/2.16.756.1.17.3.62.5):

Extended validation or EV certificates offer maximum assurance for users. Considerable effort is required from the CA to validate the application. To be able to issue an EV certificate, additional documentation must be made available in accordance with the rules of the CA/browser forum.

	Relevance	Check	Check criteria	Comment	OK/NOK
1	OV / EV	**Check that the applicant is not on lists of anti-phishing work groups or similar blocking lists.**	Compare with data sources: ➢ http://www.phishtank.com/ ➢ http://www.surbl.org/surbl-analysis	(See also: DV/OV-> [BR] Chap. 4.2.1 Performing Identification and Authentication Functions) EV -> [CAB] Chap. 11.12.2 Denied Lists and Other Legal Black Lists)	◯ ◯
2	OV / EV	**Verify telephone number and communication channel**	Call the company's main office about the information or look up the www.local.ch directory	Verified through a data source by third parties or through an online data source directly by a telecommunications provider. (See also: OV/DV-> [BR] Chap.3.2.2.1 Identity; EV -> [CAB] Chap. 11.5 Verified Method of Communication)	◯ ◯
3	OV / EV	**Verify the name, title and authorisation of the certificate applicant**	Compare with data sources: ➢ Admin directory (trusted source) ➢ Digital signature on the form ➢ Entry in SOGC (Swiss Official Gazette of Commerce) ➢ SG-PKI list of SSL-authorised users ➢ Identity document with passport photo	(See also: OV/DV-> [BR] Chap. Xxxxxx), EV -> [CAB] Chap. 11.9 Verification of Signature on Subscriber Agreement and EV Certificate Requests)	◯ ◯

	Relevance	Check	Check criteria	Comment	OK/NOK
4	OV / EV	**Verify domain authorisation**	➢ Compare with data sources: ▪ www.whoIs.com ▪ www.firestorm.ch ➢ Call domain owner ➢ Ask for confirmation email to the administrator address	Domain names are verified by the domain name registrar. The fully qualified domain names (FQDN) applied for must be within the authorised domains. Compare with data sources or by one of the following methods: ▪ Submitting a query to the domain name registrar to check if the applicant is the domain holder ▪ Communicating directly with the domain holder by means of an address, email or telephone number provided by the domain name registrar. ▪ Communicating directly with the domain holder using the details listed in the registrar's WHOIS dataset, i.e. the "technical" or "administrative" contact. Otherwise use generic email contacts such as the domain administrator with an address made up of the prefix "admin", "administrator", "webmaster", "hostmaster" or "postmaster" followed by "@" followed by the domain name of the final parts from the FQDN applied for. ▪ Using the domain authorisation documents as a basis ▪ Asking the applicant to make an agreed change to information on the website that is addressed as a uniform resource identifier by the FQDN applied for. ▪ Other confirmation methods on the condition that the CA provides documents showing that the applicant is the domain holder or controls the FQDN. This is at least as reliable as the methods described above. (See also: OV/DV-> [BR] Chap.3.2.2.4 Authorization by Domain Name Registrant), EV -> [CAB] Chap. 11.7 Verification of Applicant's Domain Name)	◯ ◯
5	OV / EV	**Signature certification**	➢ Verification of the digital signature ➢ Comparison of hand-written signature with previous applications, where available ➢ Call the domain owner and request a signed document	(See also: OV/DV-> [BR] Chap. Xxxxx), EV -> [CAB] Chap. 11.9 Verification of Signature on Subscriber Agreement and EV Certificate Requests)	◯ ◯

	Relevance	Check	Check criteria	Comment	OK/NOK
6	OV / EV	**Applicant's legal status and identity**	Compare with data sources: ➢ LDAP (Softerra LDAP Administrator) ➢ Admin directory ➢ SG-PKI list of SSL-authorised users ➢ Entry in SOGC ➢ UID register	This verification must be made where the applicant is registered and depends on the type of applicant. Verification of legal status, name (must be as it is in the certificate application), registration number and registration office for a •private organisation •government office •profit-making organisation •natural person •non-profit organisation (See also: OV/DV-> [BR] Chap. 3.2.2.1 Identity EV -> [CAB] Chap. 11.2 Verification of Applicant's Legal Existence and Identity)	◯ ◯
7	OV / EV	**Check DBA or trade names – assumed names**	Compare with data sources: ➢ Admin directory ➢ Entry in SOGC ➢ UID register ➢ https://www.swissreg.ch/srclient/faces/jsp/start.jsp	Is the common name (CN) or fully qualified domain name (FQDN) applied for under the applicant's legitimate control? (See also -> BR 1.3.4, Chap. 3.2.2.2) (See also: OV-> [BR] Chap. 3.2.2 DBA/Tradename; EV -> [CAB] Chap.11.3 Verification of Applicant's Legal Existence and Identity – Assumed Name)	◯ ◯
8	OV / EV	**Verify if the organisation exists physically (at the address provided)**	Compare with data sources: ➢ Telephone directory (www.local.ch) ➢ Admin directory ➢ Entry in SOGC ➢ UID register	(See also: OV-> [BR] Chap. 3.2.2.1 Identity; EV -> [CAB] Chap.11.4 Verification of Applicant's Physical Existence)	◯ ◯
9	EV	**Verify if the organisation is operating (at the address provided)**	➢ Call the company's main office ➢ Compare with data sources: ▪ Telephone directory ▪ Company's website	(See also: EV -> [CAB] Chap. 11.6 Verification of Applicant's Operational Existence)	◯ ◯
10	EV	**Verify the name, title and authorisation of the contracting party**	Compare with data sources: ➢ Admin directory ➢ Entry in SOGC ➢ Call the organisation's HR department	Call the human resources department of the applicant organisation. During the call, the authorisation of the person applying can be checked. (See also: EV -> [CAB] Chap. 11.8 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver)	◯ ◯
11	EV	**Letter of authorisation from the organisation**	Signed letter available: Compare with data sources: ➢ Admin directory ➢ Entry in SOGC ➢ Call the organisation's HR department	Is the letter available and are the signatures valid? Was the letter signed by the right person?	◯ ◯

References: [BR] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.3.4.pdf; and [CAB] https://cabforum.org/wp-content/uploads/EV-SSL-Certificate-Guidelines-Version-1.5.1.pdf

Application status: Accepted: ◯ **Returned to applicant for additional information:** ◯ **Rejected:** ◯ **/ Reason**

Check date: **Check performed by (dSig):**