Certificate

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

SwissSign AG
Sägereistrasse 25
8152 Glattbrugg, Switzerland

to confirm that its trust service

SwissSign AG – EV/OV - SSL Gold Certificate

fulfils all requirements defined in the standard (EN)

ETSI EN 319 411-1 V1.1.1 (2016-02), policy EVCP, OVCP.

The appendix to the certificate is part of the certificate and consists of 4 pages.

The certificate is valid only in conjunction with the evaluation report.

ETSI EN 319 411-1 2017 TÜViT® Trusted Site

Certificate ID: 67102.17

Certificate valid until 2018-11-30

Essen, 2017-11-30

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

DAkkS Deutsche Akkreditierungsstelle D-ZE-12022-01-01

Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- "Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH", version 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

Evaluation Report

- "Evaluation Report – Initial Certification – ETSI EN 319 411-1, TUVIT-CA67102, SwissSign AG – EV/OV - SSL Gold Certificate", Version 1.0 as of 2017-11-30, TÜV Informationstechnik GmbH

Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1:

- ETSI EN 319 411-1 V1.1.1 (2016-02): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements", Version 1.1.1, 2016-02, European Telecommunications Standards Institute

Additionally the following criteria were considered in the audit:

- "Guidelines for the issuance and management of Extended Validation Certificates", Version 1.6.6 as of 2017-07-28, CA/Browser Forum

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 1.5.1 as of 2017-09-20

The applicable ETSI Certificate Policy is:

- EVCP: Extended Validation Certificate Policy
- OVCP: Organizational Validation Certificate Policy

Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

SwissSign AG – EV/OV - SSL Gold Certificate:

Issuer of CA certificate (Root CA or intermediate CA): CN = SwissSign Gold CA - G2 Certificate Serial Number: 00 bb 40 1c 43 f5 5e 4f b0	
Name of CA (as in certificate)	**serial number of certificate**
CN = SwissSign EV Gold CA 2014 - G22 (EVCP)	00 81 08 38 3c c0 07 75 c4 0c 6d 73 6b e3 30 8b
CN = SwissSign Personal Gold CA 2014 - G22 (OVCP)	19 17 95 dc 22 74 1b 12 1d db 54 4c 5c cb dc
CN = SwissSign Server Gold CA 2014 - G22 (OVCP)	00 fa 1d aa ea c9 b3 a5 fa 57 98 0b 99 74 da 31

Issuer of CA certificate (Root CA or intermediate CA): CN = SwissSign Gold Root CA - G3 Certificate Serial Number: 00 de c4 f2 44 f3 1d a6 fc	
Name of CA (as in certificate)	**serial number of certificate**
CN = SwissSign Gold EV CA 2010 - G3 (EVCP)	00 c9 76 d2 aa dd 04 06 fb 67 df f3 3a 79 6d 90
CN = SwissSign Gold Personal CA 2010 - G3 (OVCP)	00 c4 20 cb 69 5e 71 d8 b6 72 b8 ba 1a ef 35 71
CN = SwissSign Gold Server CA 2010 - G3 (OVCP)	00 c7 34 35 d9 9e f4 bc 23 0f 6c d4 4e d0 20 0e

together with the Certificate Policy (CP) of the operator and the Certification Practice Statement (CPS) of the operator:

- ,,Certificate Policy and Certification Practice Statement of the SwissSign Gold CA " version 2.5.0 as of 2018-07-16, SwissSign AG

Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

Summary of the Evaluation Requirements

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

1 **Publication and repository responsibilities**

2 **Identification and authentication**

3 **Certificate Life-Cycle operational requirements**

4 **Facility, management, and operational controls**

5 **Technical security controls**

6 **Certificate, CRL, and OCSP profiles**

7 **Compliance audit and other assessment**

8 **Other business and legal matters**

9 **Other provisions**