

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

SwissSign AG
Sägereistrasse 25
8152 Glattbrugg, Schweiz

für den Vertrauensdienst

SwissSign AG - EV/OV - SSL Gold
Certificate

die Erfüllung aller Anforderungen der Norm (EN)

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht
aus 4 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



Certificate ID: 67102.17

© TÜVIT - TÜV NORD GROUP - www.tuvit.de

18
Zertifikat gültig bis
30.11.2018

Essen, 30.11.2017

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de



Zertifikat

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH ist bei der „DAkkS Deutsche Akkreditierungsstelle GmbH“ für die Zertifizierung von Produkten in den Bereichen IT-Sicherheit und Sicherheitstechnik nach DIN EN ISO/IEC 17065 akkreditiert. Die Zertifizierungsstelle führt ihre Zertifizierungen auf Basis des folgenden akkreditierten Zertifizierungssystems durch:

- „Zertifizierungssystem (akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 2.0 vom 06.06.2016, TÜV Informationstechnik GmbH

Prüfbericht

- „Evaluation Report – Initial Certification – ETSI EN 319 411-1, TUVIT-CA67102, SwissSign AG – EV/OV – SSL Gold Certificate“, Version 1.0 vom 30.11.2017, TÜV Informationstechnik GmbH

Prüfanforderungen

Die Prüfanforderungen sind in der Norm ETSI EN 319 411-1 definiert:

- 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

Zusätzlich wurden folgende Kriterien bei dem Audit berücksichtigt:

- „Guidelines for the issuance and management of Extended Validation Certificates“, Version 1.6.6 vom 28.07.2017, CA/Browser Forum

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 1.5.1 vom 20.09.2017

Die anwendbare ETSI Zertifizierungspolitik ist:

- EVCP: Zertifizierungspolitik mit erweiterter Validierung
- OVCP: Zertifizierungspolitik mit Organisationsvalidierung

Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienst:

SwissSign AG - EV/OV - SSL Gold Certificate:

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = SwissSign Gold CA - G2 Zertifikatsseriennummer: 00 bb 40 1c 43 f5 5e 4f b0	
Name der CA (wie im Zertifikat)	Seriennummer des Zertifikates
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

Aussteller des CA-Zertifikats (Root CA oder Intermediate CA): CN = SwissSign Gold Root CA - G3 Zertifikatsseriennummer: 00 de c4 f2 44 f3 1d a6 fc	
Name der CA (wie im Zertifikat)	Seriennummer des Zertifikates
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

zusammen mit der Certificate Policy (CP) und mit dem Certification Practice Statement (CPS) des Betreibers:

- „Certificate Policy and Certification Practice Statement of the SwissSign Gold CA “ Version 2.5.0 vom 16.07.2018, SwissSign AG

Prüfergebnis

- Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien.
- Die im Zertifizierungssystem definierten Zertifizierungsvoraussetzungen sind erfüllt.

Zusammenfassung der Prüfanforderungen

ETSI EN 319 411-1 enthält Anforderungen für Vertrauensdiensteanbieter (VDA) bzgl. der Tätigkeit des VDAs unter folgenden Überschriften:

- 1 Verantwortlichkeiten bzgl. Veröffentlichung und öffentlichem Verzeichnis**
- 2 Identifizierung und Authentifizierung**
- 3 Betriebsanforderungen an den Zertifikatslebenszyklus**
- 4 Anforderungen an Einrichtung, Verwaltung und Betrieb**
- 5 Technische Sicherheitsanforderungen**
- 6 Zertifikats-, Sperrlisten- (CRL-) und OCSP-Profile**
- 7 Compliance-Audit und andere Bewertungen**
- 8 Sonstige geschäftliche und rechtliche Angelegenheiten**
- 9 Sonstige Maßnahmen**