

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

**SwissSign AG**  
**Sägereistrasse 25**  
**8152 Glattbrugg, Schweiz**

für den Zertifizierungsdienst

**SwissSign LI Qualified Platinum CA**

die Erfüllung aller Anforderungen der Spezifikation

**ETSI TS 101 456 V1.4.3 (2007-05),  
policy QCP public + SSCD.**

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht  
aus 7 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



**Certificate ID: 6782.16**

© TÜVIT - TÜV NORD GROUP - [www.tuvit.de](http://www.tuvit.de)

**17**  
Zertifikat gültig bis  
30.06.2017

Essen, 21.06.2016

Dr. Christoph Sutter  
Leiter Zertifizierungsstelle

**TÜV Informationstechnik GmbH**  
TÜV NORD GROUP  
Langemarckstraße 20  
45141 Essen  
[www.tuvit.de](http://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 TS 101 456, SwissSign LI Qualified Platinum CA“, Version 2.0 vom 21.06.2016, TÜV Informationstechnik GmbH

## Prüfanforderungen

Die Prüfanforderungen sind in der technischen Spezifikation ETSI TS 101 456 definiert:

- ETSI TS 101 456 V1.4.3 (2007-05): „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing qualified certificates“, Version 1.4.3, 2007-05, European Telecommunications Standards Institute

Die anwendbare ETSI Zertifizierungspolitik ist:

- QCP public + SSCD: Zertifizierungspolitik für (öffentlich angebotene) qualifizierte Zertifikate, welche die Verwendung sicherer Signaturerstellungseinheiten fordert.

## Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Zertifizierungsdienst:

### SwissSign LI Qualified Platinum G2:

<b>Aussteller des CA-Zertifikats (Root CA oder Intermediate CA):</b> <b>CN = SwissSign Platinum CA - G2</b> <b>Zertifikatsseriennummer: 4e b2 00 67 0c 03 5d 4f</b>	
<b>Name der CA (wie im Zertifikat)</b>	<b>Seriennummer des Zertifikates</b>
CN = SwissSign LI Qualified Platinum CA 2016 - G2	49 45 26 0c bf 0f 20 16 74 12 42 1f 09 5e 8d

### SwissSign LI Qualified Platinum G3:

<b>Aussteller des CA-Zertifikats (Root CA oder Intermediate CA):</b> <b>CN = SwissSign Platinum Root CA - G3</b> <b>Zertifikatsseriennummer: 22 3f a9 17 20 de 81 94</b>	
<b>Name der CA (wie im Zertifikat)</b>	<b>Seriennummer des Zertifikates</b>
CN = SwissSign LI Platinum Qualified CA 2016 - G3	22 3d 5e e8 58 66 06 6b 31 2a b9 da 41 5f 99

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

- „SwissSign Platinum CP/CPS“, Version 3.2.2 vom 25.11.2015, SwissSign

## Prüfergebnis

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

## **Zusammenfassung der Prüfanforderungen**

Die ETSI Spezifikation ETSI TS 101 456 enthält folgende Anforderungen:

### **1 Certification Practice Statement (CPS)**

Die CA stellt sicher, dass sie die erforderliche Zuverlässigkeit für die Bereitstellung von Zertifizierungsdiensten darlegt (siehe die Richtlinie 1999/98/EG, Anhang II (a)).

### **2 Public Key Infrastructure - Schlüsselmanagement-Lebenszyklus**

Die CA stellt sicher, dass CA Schlüssel unter kontrollierten Bedingungen erzeugt werden (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass private CA Schlüssel vertraulich bleiben und ihre Integrität beibehalten (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass die Integrität und Authentizität der (öffentlichen) CA Signaturprüfchlüssel und aller zugehörigen Parameter während ihrer Übermittlung an vertrauende Parteien (relying party) erhalten bleiben (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Private Signaturschlüssel von Inhabern (subject) dürfen nicht hinterlegt werden, dass eine (Reserve-)Entschlüsselungsmöglichkeit geboten wird, die es autorisierten Stellen unter bestimmten Bedingungen erlaubt, Daten unter Verwendung von Information, die durch einen oder mehrere Beteiligte bereitgestellt werden, zu entschlüsseln (gemeinhin als Key Escrow bezeichnet) (siehe die Richtlinie 1999/93/EG, Anhang II (j)).

Die CA stellt sicher, dass private CA Signaturschlüssel nicht unsachgemäß verwendet werden.

Die CA stellt sicher, dass private CA Signaturschlüssel nicht über das Ende ihres Lebenszyklus hinaus verwendet werden (siehe die Richtlinie 1999/93/EG, Anhang II (g) und Anhang II (f)).

Die CA stellt sicher, dass die Sicherheit der kryptografischen Hardware während ihres gesamten Lebenszyklus gewährleistet ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass jeder Schlüssel, den sie für Zertifikatsinhaber (subject) erzeugt, sicher generiert wird und die Geheimhaltung des privaten Schlüssels des Zertifikatsinhabers sichergestellt ist (siehe die Richtlinie 1999/93/EG, Anhang II (f) und Anhang II(j)).

Die CA stellt sicher, dass die Übergabe der sicheren Signaturerstellungseinheit sicher erfolgt, sofern diese Signaturerstellungseinheit der CA bereitgestellt wird (siehe die Richtlinie 1999/93/EG, Anhang III).

### **3 Public Key Infrastructure - Zertifikatsmanagement Lebenszyklus**

Die CA stellt sicher, dass Zertifikatsinhaber (subject) geeignet identifiziert und authentifiziert sind und dass Zertifikatsanträge vollständig, korrekt und ordnungsgemäß autorisiert sind (siehe die Richtlinie 1999/93/EG, Anhang II (d)).

Die CA stellt sicher, dass Zertifikatsanträge von Zertifikatsinhabern (subject), die zuvor bei der gleichen CA registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind. Dies beinhaltet Zertifikatsverlängerungen, erneute Schlüsselgenerierung (rekey) nach Sperrung oder vor Ablauf der Gültigkeit oder Aktualisierung aufgrund Attributsänderungen des Zertifikatsinhabers (subject) (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass Zertifikate sicher ausgegeben werden, so dass ihre Authentizität erhalten bleibt (siehe die Richtlinie 1999/93/EG, Anhang II (g)).

Die CA stellt sicher, dass die allgemeinen Geschäftsbedingungen den Teilnehmer (subscriber) und vertrauenden Parteien (relying party) zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (k)).

Die CA stellt sicher, dass Zertifikate den Teilnehmern (subscriber), Zertifikatsinhabern (subject) und vertrauenden Parteien (relying party) im erforderlichen Umfang zur Verfügung gestellt werden (siehe die Richtlinie 1999/93/EG, Anhang II (l)).

Die CA stellt sicher, dass Zertifikate kurzfristig anhand von autorisierten und überprüften Sperranfragen gesperrt werden (siehe die Richtlinie 1999/93/EG, Anhang II (b)).

#### **4 CA Management und Betrieb**

Die CA stellt sicher, dass Verwaltungs- und Management-Verfahren angewendet werden, die angemessen sind und anerkannten Normen entsprechen (siehe die Richtlinie 1999/93/EG, Anhang II (e), 2. Teil).

Die CA stellt sicher, dass ihre schützenswerte Objekte und Informationen einen angemessenen Schutz erhalten (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass das Personal und die Einstellungsverfahren die Vertrauenswürdigkeit des CA Betriebs verstärken und unterstützen (siehe die Richtlinie 1999/93/EG, Anhang II (e) 1. Teil).

Die CA stellt sicher, dass der physische Zugriff auf kritische Dienste kontrolliert wird und physische Risiken der schützenswerten Objekte minimiert werden (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass die CA Systeme sicher sind und ordnungsgemäß betrieben werden mit minimalem Ausfallrisiko (siehe die Richtlinie 1999/93/EG, Anhang II (e)).

Die CA stellt sicher, dass der Zugriff auf die CA Systeme auf geeignet autorisierte Personen beschränkt ist (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA soll vertrauenswürdige Systeme und Produkte verwenden, die vor Veränderungen geschützt sind (siehe die Richtlinie 1999/93/EG, Anhang II (f)).

Die CA stellt sicher, dass im Falle einer Katastrophe, einschließlich der Kompromittierung des privaten CA Signaturschlüssels, der Betrieb so schnell wie möglich wiederhergestellt wird (siehe die Richtlinie 1999/93/EG, Anhang II (a)).

Die CA stellt sicher, dass im Falle der Einstellung des Betriebs der CA potenzielle Störungen von Teilnehmer (subscriber) und vertrauenden Parteien (relying party) minimiert werden und dass der Forterhalt der Aufzeichnungen, die zum Nachweis der Zertifizierung in Gerichtsverfahren benötigt werden, gegeben ist (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

Die CA stellt sicher, dass die gesetzlichen Anforderungen eingehalten werden (siehe die Richtlinie 1999/93/EG, Artikel 8).

Die CA stellt sicher, dass alle relevanten Informationen über ein qualifiziertes Zertifikat für einen angemessenen Zeitraum aufgezeichnet werden, insbesondere zum Zweck des Nachweises der Zertifizierung in Gerichtsverfahren (siehe die Richtlinie 1999/93/EG, Anhang II (i)).

## **5 Organisation**

Die CA stellt sicher, dass ihre Organisation zuverlässig ist (siehe die Richtlinie 1999/93/EG, Anhang II (a)).