

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

**SK ID Solutions AS**  
**Pärnu avenue 141**  
**11314 Tallinn, Estland**

für den Vertrauensdienst

**Klass3-SK certificates for website  
authentication**

die Erfüllung aller Anforderungen der Norm (EN)

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

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht  
aus 3 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



**Certificate ID: 67117.18**

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

**20**  
Zertifikat gültig bis  
30.11.2020

Essen, 30.11.2018

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

- Englisch Dokument: „Evaluation Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67117, Klass3-SK certificates for website authentication“, Version 2.1 vom 30.11.2018, 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

Die anwendbare ETSI Zertifizierungspolitik ist:

- OVCP: Zertifizierungspolitik mit Organisationsvalidierung

## Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienst:

### **Klass3-SK certificates for website authentication:**

<b>Aussteller des CA-Zertifikats (Root CA oder Intermediate CA):</b> <b>CN = EE Certification Centre Root CA</b> <b>Zertifikatsseriennummer: 54 80 f9 a0 73 ed 3f 00 4c ca 89 d8 e3 71 e6 4a</b>	
<b>Name der CA (wie im Zertifikat)</b>	<b>Seriennummer des Zertifikates</b>
CN = KLASS3-SK 2010	0a 19 b7 e3 1f 1a 87 70 55 70 57 9d 96 cd 9c da
CN = KLASS3-SK 2016	5e 53 3b 13 25 60 34 2b 58 49 57 30 8b 30 78 dc

zusammen mit der Certificate Policy (CP) des Betreibers:

- „SK ID Solutions AS – Certificate Policy for TLS Server Certificates“, Version 5.0 vom 03.11.2017, SK ID Solutions AS

und mit dem Certification Practice Statement (CPS) des Betreibers:

- „SK ID Solutions AS – Certification Practice Statement for KLASS3-SK“, Version 5.0 vom 30.11.2017 sowie Version 6.0 gültig ab 04.01.2019, SK ID Solutions AS

und mit dem Trust Service Statement (TSPS) des Betreibers:

- „SK ID Solutions AS – Trust Service Practice Statement“, Version 6.0 vom 17.10.2018, SK ID Solutions AS

## **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**

## Gegenstand des Nachtrags

Dieser Nachtrag vom 17.05.2019 ergänzt das Zertifikat mit der Certificate ID: 67117.18 vom 30.11.2018 aufgrund des durchgeführten Überwachungsaudits.

## 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

- Englischs Dokument: „Evaluation Report – Surveillance Onsite Inspection – ETSI EN 319 411-1, TUVIT-CA67117A1, Klass3-SK certificates for website authentication“, Version 1.1 vom 14.05.2019, 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:

- „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“, Version 1.6.3 vom 01.02.2019, CA/Browser Forum

Die anwendbare ETSI Zertifizierungspolitik ist:

- OVCP: Zertifizierungspolitik mit Organisationsvalidierung

### Prüfgegenstand

Der Prüfgegenstand ist charakterisiert durch die Zertifikatsinformation zum untersuchten Vertrauensdienst:

#### **Klass3-SK certificates for website authentication:**

<b>Aussteller des CA-Zertifikats (Root CA oder Intermediate CA):</b> <b>CN = EE Certification Centre Root CA</b> <b>Zertifikatsseriennummer: 54 80 f9 a0 73 ed 3f 00 4c ca 89 d8 e3 71 e6 4a</b>	
<b>Name der CA (wie im Zertifikat)</b>	<b>Seriennummer des Zertifikates</b>
CN = KLASS3-SK 2010	0a 19 b7 e3 1f 1a 87 70 55 70 57 9d 96 cd 9c da
CN = KLASS3-SK 2016	5e 53 3b 13 25 60 34 2b 58 49 57 30 8b 30 78 dc

zusammen mit der Dokumentation des Betreibers:

- „SK ID Solutions AS – Trust Service Practice Statement“, Version 6.0 vom 17.10.2018, SK ID Solutions AS
- „SK ID Solutions AS – Certificate Policy for TLS Server Certificates“, Version 6.0 gültig ab 22.05.2019, SK ID Solutions AS

- „SK ID Solutions AS – Certification Practice Statement for KLASS3-SK“, Version 7.0 gültig ab 22.05.2019, SK ID Solutions AS
- „Terms and Conditions for Use of Organisation Certificates“, vom 04.01.2019, SK ID Solutions AS

## **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**