

## SCESm-Verzeichnis

## Akkreditierungsnummer: SCESm 0071

Internationale Norm: ISO/IEC 17021-1:2015  
 Schweizer Norm: SN EN ISO/IEC 17021-1:2015

KPMG AG  
 Risk Consulting  
 Zertifizierungsstelle SCESm 0071  
 Badenerstrasse 172  
 8036 Zürich

Leiter: Reto P. Grubenmann  
 MS-Verantwortlicher: Dr. Matthias Bossardt  
 Telefon: +41 58 249 42 46  
 E-Mail: [retogrubenmann@kpmg.com](mailto:retogrubenmann@kpmg.com)  
 Internet: [www.kpmg.com](http://www.kpmg.com)  
 Erstmals akkreditiert: 22.01.2002  
 Aktuelle Akkreditierung: 22.01.2017 bis 21.01.2022  
 Verzeichnis siehe: [www.sas.admin.ch](http://www.sas.admin.ch)  
 (Akkreditierte Stellen)

### Geltungsbereich der Akkreditierung ab 01.09.2021

#### Zertifizierungsstelle für Informations-Technologie und Sicherheit

Normen	Zugelassene technische Bereiche	Bemerkungen
<b>ISO/IEC 27001:2013</b> inkl. Umsetzung auf Betriebssystemen und Netzwerkarchitekturen / Firewalls	<b>Information Security Management System ISMS</b>	Die Zertifizierungsstelle erfüllt die Vorgaben der Norm ISO/IEC 27006:2015
<b>ISO 27799:2016</b>	Health informatics – Information security management in health using ISO/IEC 27002	Kann nur in Verbindung mit einem Managementsystem nach ISO/IEC 27001 zertifiziert werden.
<b>ISO/IEC 20000-1:2018</b> <b>ISO IEC 20000-1:2011</b>	<b>IT Service Management (ITSM)</b>	Die Zertifizierungsstelle erfüllt die Vorgaben der Norm ISO/IEC 20000-6:2017 Zertifikate nach ISO/IEC 20000-1:2011 bleiben längstens bis 29.09.2021 gültig.
	Transport, Speicherung, Kommunikation Informationstechnologie Andere Dienstleistungen	EA-Code 31 33 35



## SCESm-Verzeichnis

## Akkreditierungsnummer: SCESm 0071

Normen	Zugelassene technische Bereiche	Bemerkungen
<p><b>SR 943.03</b> (ZertES) <b>SR 943.032</b> (VZertES) <b>SR 943.032.1</b> (TAV)</p> <p><b>ETSI EN 319 401</b> inkl. Umsetzung auf Betriebssystemen und Netzwerkarchitekturen / Firewalls</p> <p><b>ETSI EN 319 411-2</b> beruhend auf den wesentlichen mitgeltenden Standards wie: <b>ETSI EN 319 411-1</b> <b>ETSI EN 319 401</b> <b>ETSI EN 319 412-5</b> <b>ISO/IEC 9594-8 / Part 8: Public-key and attribute certificate frameworks</b> <b>IETF RFC 3739</b></p> <p><b>ETSI EN 319 411-1</b> beruhend auf den wesentlichen mitgeltenden Standards wie mit: <b>ETSI EN 319 401</b> <b>ETSI EN 319 412-2</b> <b>ETSI EN 319 412-3</b> <b>ETSI EN 319 412-4</b> <b>IETF RFC 5280 (X.509)</b> <b>IETF RFC 6960 (OCSP)</b> <b>IETF RFC 3647 (CP/CPS)</b> <b>ISO/IEC 9594-8 / Part 8: Public-key and attribute certificate frameworks</b></p>	<p><b>Public Key Infrastructure PKI</b> Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate</p> <p>Elektronische Signaturen und Infrastrukturen (ESI) - Allgemeine Anforderungen an die Policy für Vertrauensdiensteanbieter</p> <p>Anforderungen an Vertrauensdiensteanbieter, die EU-qualifizierte Zertifikate ausgeben beinhaltend: Profil für EU-qualifizierte Zertifikate</p> <p>Policy- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zertifikate ausgeben beinhaltend:</p> <ul style="list-style-type: none"> <li>- Profile für Zertifikate, die an natürliche Personen ausgegeben werden</li> <li>- Profile für Zertifikate, die an juristische Personen ausgegeben werden</li> <li>- Zertifikatsprofile für Webseitenzertifikate</li> <li>- EV Extended-Validation-Zertifikate</li> </ul> <p>gemäss folgenden möglichen Richtlinien:</p> <ul style="list-style-type: none"> <li>- QCP: Qualified Certificate Policy</li> <li>- NCP: Normalized Certificate Policy</li> <li>- NCP+: Normalized Certificate Policy requiring a secure user device</li> <li>- LCP: Lightweight Certificate Policy</li> <li>- EVCP: Extended Validation Certificate Policy</li> <li>- EVCP+: Extended Validation Certificate Policy requiring a secure user device</li> </ul>	<p>EA-Code 33</p> <p>Managementsystem mit Kontrollzielen und Referenzen auf ISO/IEC 27002 sowie ISO/IEC 27005</p>



## SCESm-Verzeichnis

## Akkreditierungsnummer: SCESm 0071

Normen	Zugelassene technische Bereiche	Bemerkungen
<p><b>ETSI EN 319 421</b> sowie den wesentlichen mitgelieferten Standards wie <b>ETSI EN 319 401</b> <b>ETSI EN 319 422</b> <b>IETF RFC 3161</b> (TSA Protokoll) <b>IETF RFC 5816</b> (Update to RFC 3161)</p> <p><b>ISO 21188:2018</b></p> <p><b>CA/Browser Forum</b> Network and certificate system security requirement Version 1.6</p> <p><b>CA/Browser Forum</b> Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Version 1.7.3</p> <p><b>CA/Browser Forum</b> Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.7.8</p> <p><b>CA/Browser Forum</b> Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates Version 2.3</p> <p><b>WEBTRUST CPA (Canada)</b> Principles and Criteria for Certification Authorities Version 2.1</p> <p><b>WEBTRUST CPA (Canada)</b> Principles and Criteria for Certification Authorities - SSL Baseline with network Security Version 2.3</p> <p><b>WEBTRUST CPA (Canada)</b> Principles and Criteria for Certification Authorities - Extended Validation SSL</p>	<p>Policy- und Sicherheitsanforderungen an Vertrauensdiensteanbieter, die Zeitstempel ausgeben.</p> <p>Zeitstempel-Protokoll und Profile</p> <p>Public key infrastructure for financial services - Practices and policy framework</p> <p>Network and Certificate System Security Requirements (Requirements) applied to all publicly trusted Certification Authorities (CAs)</p> <p>Public Trusted Certificates</p> <p>Public Trusted EV-Certificates</p> <p>Public Trusted Code Signing Certificates</p> <p>Framework for auditors to assess the adequacy and effectiveness of the controls used by Certification Authorities (CAs).</p> <p>Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and Network and Certificate System Security Requirements</p> <p>Public Trusted EV-Certificates</p>	



## SCESm-Verzeichnis

## Akkreditierungsnummer: SCESm 0071

Normen	Zugelassene technische Bereiche	Bemerkungen
<p><b>SN EN 419 241-1</b> beruhend auf den wesentlichen mitgeltenden Standards welche Schutzprofile für Module: CEN EN 419 241-2 (PP) CEN EN 419 241-5 (PP) Die bereits zertifizierten Module gemäss den zwei obengenannten Schutzprofilen werden durch KPMG auf Basis der Sicherheitsintegration zertifiziert.</p> <p><b>Sicherheitstechnische Überprüfung der Konfiguration und Integration von bereits zertifizierten Produkten/Modulen mit entsprechenden Schutzprofilen gemäss:</b></p> <ul style="list-style-type: none"> <li>- FIPS PUB 140-2</li> <li>- ISO/IEC 15408 (parts 1 to 3)</li> <li>- ISO/IEC 19790:2012</li> <li>- SN EN 419 211-2 (PP)</li> <li>- SN EN 419 211-3 (PP)</li> <li>- SN EN 419 211-4 (PP)</li> <li>- SN EN 419 221-5 (PP)</li> <li>- SN EN 419 211-6 (PP)</li> <li>- prEN 419 241-2:2017 (PP)</li> <li>- EN 419 241-5 (PP)</li> </ul> <p><b>SR 235.13 (VDSZ)</b> inkl. Richtlinien des EDOEB über die Mindestanforderungen an ein Datenschutz-Managementsystem und dessen Anhang (Leitfaden für das Datenschutz-Management)</p>	<p>Sicherheitsanforderungen für vertrauenswürdige Systeme, die Serversignaturen unterstützen</p> <p><b>Schutzprofile (PP)</b></p> <p><b>Datenschutzmanagementsysteme (DSMS) nach Artikel 4 VDSZ: Zertifizierung von Organisation und Verfahren</b></p>	<p>Kann für folgende in SN EN 419 241-1 enthaltene Kontrollziele nur als Zusatz zu einer der angegebenen, bestehenden Zertifizierungen zertifiziert werden: <b>Sicherheitsniveau 1 (SCAL1)</b> (bei ETSI EN 319 411-1) für fortgeschrittene Zertifikate <b>Sicherheitsniveau 2 (SCAL2)</b> (bei ETSI EN 319 411-2) für qualifizierte Zertifikate</p> <p>Die Zertifizierungsstelle erfüllt die Vorgaben der Normen ETSI EN 319 403 ETSI EN 119 403-2 (SAS: SCESp 0127 DAkKS: D-ZE-20924-01-00)</p> <p>Basierend auf <b>SR 235.1 (DSG)</b> inkl. spezialgesetzliche Datenschutzbestimmungen</p> <p><b>SR 235.11 (VDSG)</b></p> <p>Inkl. <b>KVV Art. 59a</b> elektronische und physische Datenannahmestellen Zertifizierungen (Verordnung für die Krankenversicherungen)</p>

