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
Internet:	www.kpmg.com
Erstmals akkreditiert:	22.01.2002
Aktuelle Akkreditierung:	22.01.2022 bis 21.01.2027
Verzeichnis siehe:	www.sas.admin.ch (Akkreditierte Stellen)

Geltungsbereich der Akkreditierung ab 22.01.2022

Zertifizierungsstelle für Informations-Technologie und Sicherheit

Normen	Zugelassene technische Bereiche	Bemerkungen
ISO/IEC 27001:2013 inkl. Umsetzung auf Betriebssystemen und Netzwerkarchitekturen / Firewalls	**Information Security Management System ISMS**	Die Zertifizierungsstelle erfüllt die Vorgaben der Norm ISO/IEC 27006:2015/Amd. 1:2020
ISO 27799:2016	Health informatics – Information security management in health using ISO/IEC 27002	Kann nur in Verbindung mit einem Managementsystem nach ISO/IEC 27001 zertifiziert werden.
ISO/IEC 20000-1:2018	**IT Service Management (ITSM)**	Die Zertifizierungsstelle erfüllt die Vorgaben der Norm ISO/IEC 20000-6:2017
		EA-Code
	Transport, Speicherung, Kommunikation	31
	Informationstechnologie	33
	Andere Dienstleistungen	35

SCESm-Verzeichnis

Akkreditierungsnummer: SCESm 0071

Normen	Zugelassene technische Bereiche	Bemerkungen
SR 943.03 (ZertES) **SR 943.032** (VZertES) **SR 943.032.1** (TAV)	**Public Key Infrastructure PKI** Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate	EA-Code 33
ETSI EN 319 401:2021 inkl. Umsetzung auf Betriebssysteme-men und Netzwerkarchitekturen / Firewalls	Elektronische Signaturen und Infrastrukturen (ESI) - Allgemeine Anforderungen an die Policy für Vertrauensdienstanbieter	Managementsystem mit Kontrollzielen und Referenzen auf ISO/IEC 27002 sowie ISO/IEC 27005
ETSI EN 319 411-2:2021 beruhend auf den wesentlichen mitgeltenden Standards wie: **ETSI EN 319 411-1:2021** **ETSI EN 319 401:2021** **ETSI EN 319 412-5:2020** **ISO/IEC 9594-8:2020 /** Part 8: Public-key and attribute certificate frameworks **IETF RFC 3739**	Anforderungen an Vertrauensdiensteanbieter, die EU-qualifizierte Zertifikate ausgeben beinhaltend: Profil für EU-qualifizierte Zertifikate	
ETSI EN 319 411-1:2021 beruhend auf den wesentlichen mitgeltenden Standards wie mit: **ETSI EN 319 401:2021** **ETSI EN 319 412-2:2020** **ETSI EN 319 412-3:2020** **ETSI EN 319 412-4:2016** **IETF RFC 5280 (X.509)** **IETF RFC 6960 (OCSP)** **IETF RFC 3647 (CP/CPS)** **ISO/IEC 9594-8:2020 /** Part 8: Public-key and attribute certificate frameworks	Policy- und Sicherheitsanforderungen an Vertrauensdienstanbieter, die Zertifikate ausgeben beinhaltend: - Profile für Zertifikate, die an natürliche Personen ausgegeben werden - Profile für Zertifikate, die an juristische Personen ausgegeben werden - Zertifikatsprofile für Webseitenzertifikate - EV Extended-Validation-Zertifikate gemäss folgenden möglichen Richtlinien: - QCP: Qualified Certificate Policy - NCP: Normalized Certificate Policy - NCP+: Normalized Certificate Policy requiring a secure user device - LCP: Lightweight Certificate Policy - EVCP: Extended Validation Certificate Policy - EVCP+: Extended Validation Certificate Policy requiring a secure user device	

SCESm-Verzeichnis

Akkreditierungsnummer: SCESm 0071

Normen	Zugelassene technische Bereiche	Bemerkungen
ETSI EN 319 421:2021 sowie den wesentlichen mitgeltenden Standards wie **ETSI EN 319 401:2021** **ETSI EN 319 422:2016** **IETF RFC 3161** (TSA Protokoll) **IETF RFC 5816** (Update to RFC 3161)	Policy- und Sicherheitsanforderungen an Vertrauensdienstanbieter, die Zeitstempel ausgeben. Zeitstempel-Protokoll und Profile	
ISO 21188:2018	Public key infrastructure for financial services - Practices and policy framework	
CA/Browser Forum Network and certificate system security requirement Version 1.6	Network and Certificate System Security Requirements (Requirements) applied to all publicly trusted Certification Authorities (CAs)	
CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Version 1.7.3	Public Trusted Certificates	
CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.7.8	Public Trusted EV-Certificates	
CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates Version 2.3	Public Trusted Code Signing Certificates	
WEBTRUST CPA (Canada) Principles and Criteria for Certification Authorities Version 2.1	Framework for auditors to assess the adequacy and effectiveness of the controls used by Certification Authorities (CAs).	
WEBTRUST CPA (Canada) Principles and Criteria for Certification Authorities - SSL Baseline with network Security Version 2.3	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates and Network and Certificate System Security Requirements	
WEBTRUST CPA (Canada) Principles and Criteria for Certification Authorities - Extended Validation SSL	Public Trusted EV-Certificates	

SCESm-Verzeichnis

Akkreditierungsnummer: SCESm 0071

Normen	Zugelassene technische Bereiche	Bemerkungen
SN EN 419 241-1:2018 beruhend auf den wesentlichen mitgeltenden Standards welche Schutzprofile für Module: CEN EN 419 241-2:2019 (PP) CEN EN 419 221-5:2018 (PP) Die bereits zertifizierten Module gemäss den zwei obengenannten Schutzprofilen werden durch KPMG auf Basis der Sicherheitsintegration zertifiziert.	Sicherheitsanforderungen für vertrauenswürdige Systeme, die Serversignaturen unterstützen	Kann für folgende in SN EN 419 241-1 enthaltene Kontrollziele nur als Zusatz zu einer der angegebenen, bestehenden Zertifizierungen zertifiziert werden: **Sicherheitsniveau 1** (SCAL1) (bei ETSI EN 319 411-1) für fortgeschrittene Zertifikate **Sicherheitsniveau 2** (SCAL2) (bei ETSI EN 319 411-2) für qualifizierte Zertifikate
Sicherheitstechnische Überprüfung der Konfiguration und Integration von bereits zertifizierten Produkten/Modulen mit entsprechenden Schutzprofilen gemäss: - FIPS PUB 140-2 - ISO/IEC 15408:2009 (parts 1-3) - ISO/IEC 19790:2012 - SN EN 419 211-2:2013 (PP) - SN EN 419 211-3:2013 (PP) - SN EN 419 211-4:2013 (PP) - SN EN 419 211-5:2013 (PP) - SN EN 419 211-6:2014 (PP) - SN EN 419 221-5:2018 (PP) - SN EN 419 241-2:2019 (PP)	**Schutzprofile (PP)**	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)
SR 235.13 (VDSZ) inkl. Richtlinien des EDOEB über die Mindestanforderungen an ein Datenschutz-Managementsystem und dessen Anhang (Leitfaden für das Datenschutz-Management)	**Datenschutzmanagementsysteme (DSMS) nach Artikel 4 VDSZ: Zertifizierung von Organisation und Verfahren**	Basierend auf **SR 235.1** (DSG) inkl. spezialgesetzliche Datenschutzbestimmungen **SR 235.11** (VDSG) Inkl. **KVV Art. 59a** elektronische und physische Datenannahmestellen Zertifizierungen (Verordnung für die Krankenversicherungen)

SCESm-Verzeichnis

Akkreditierungsnummer: SCESm 0071

Normen	Zugelassene technische Bereiche	Bemerkungen
BS 10008:2014	**Evidential weight and legal admissibility of electronic information (Elektronisches Records Management System, ERMS)**	BIP 0008-1:2014 (Evidential weight and legal admissibility of information stored electronically) BIP 0008-2:2014 (Evidential weight and legal admissibility of information transferred electronically) BIP 0008-3:2014 (Evidential weight and legal admissibility of linking electronic identity to documents)
SR 816.11 (EPDV) Verordnung über das elektronische Patientendossier **SR 816.111 (EPDV-EDI),** Anhang 2 Ausgabe 4 Anhang 3 Ausgabe 3 Anhang 5 Ausgabe 4	Auditierung und Zertifizierung von Gemeinschaften und Stammgemeinschaften A2) Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften A3) Metadaten für den Austausch medizinischer Daten A5) Integrationsprofile inkl. Ergänzungen	Basierend auf SR 816.1 (EPDG) Bundesgesetz über das elektronische Patientendossier Inklusiv der technischen Überprüfung der IT-Infrastruktur und Software-Architektur des EPD Plattform Providers (PP) bezüglich den technischen Sicherheitseinstellungen mit Überprüfungen durch technische Sicherheitstestverfahren sowie Sample-Audits bei den Gesundheitseinrichtungen gemäss der Anforderung IAF MD-1: in der jeweils gültigen Fassung für das Patienten- und Gesundheitsfachpersonen- sowie Hilfspersonen-OnBoarding

* / * / * / * / *