







Certification Services

KPMG's Conformity Assessment Bodies

Norms / Standards / Regulations	Accredited Certification Bodies	Conformity Assessment Symbols
<p>Information Security Management System (ISMS) ISO/IEC 27001 incl. assessment of operating systems and network architecture and firewalls</p> <p>Health Informatics, Security ISO 27799</p> <p>Information Security on Cloud Infrastructure ISO/IEC 27018 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	
<p>The Standard for Privacy Information Management (PIMS) ISO/IEC 27701 allows an organization to demonstrate effective privacy data management. ISO/IEC 27701 establishes the parameters for a PIMS in terms of privacy protection and processing personally identifiable information (PII).</p>	<p>Certification Body Zurich</p>	<p>ISO/IEC 27701 is an impressive way of demonstrating to consumers, external organizations and internal stakeholders, that mechanisms are in place to keep data safe and to comply with the Swiss data privacy & data protection as well as GDPR regulations and other privacy laws.</p>
<p>IT Service Management ISO/IEC 20000-1</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	
<p>Anti-bribery management system ISO/IEC 37001</p>	<p>Certification Body Zurich DAkks D-ZM-21060-01-00</p>	

Norms / Standards / Regulations	Accredited Certification Bodies	Conformity Assessment Symbols
<p>Evidential weight and legal admissibility of electronic information management system (Archiving System) BS 10008 BIP 0008-1: for information stored electronically BIP 0008-2: for information transferred electronically BIP 0008-3: for linking electronic identity to documents</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	
<p>Graphic technology – Management of security printing processes ISO 14298 and CWA 15374 Security management system for suppliers to the secure printing industry</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	
<p>Business Continuity Management (BCM) System ISO/IEC 22301</p>	<p>KPMG AG</p>	
<p>Data Protection / Data Privacy Management System DSG, SR 235.1 VDSG, SR 235.11 VDSZ, SR 235.013.1 incl. Swiss DRG, KVV Art. 59a invoicing, Medical Clinical Dataset (MCD) for electronic data access management at health care insurance</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	
<p>Swiss Qualified Electronic Signatures (QES) and Swiss Advanced Electronic Signatures (AES) ZertES, SR 943.03 VZertES, SR 943.032 TAV, 943.032.1 and ETSITS Norms: ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 412-5 IETF RFC 3739 ETSI EN 319 411-1 ETSI EN 319 412-2 ETSI EN 319 412-3 ETSI EN 319 412-4 IETF RFC 5280 (X.509) IETF RFC 6960 (OCSP) ISO/IEC 9594-8 / Part 8: ETSI EN 319 421 ETSI EN 319 401 ETSI EN 319 422 IETF RFC 3161 (TSA Protocol) IETF RFC 5816 (Update to RFC 3161)</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	

Norms / Standards / Regulations	Accredited Certification Bodies	Conformity Assessment Symbols
<p>(Continuation)</p> <p>FIPS PUB 140-2, Security Level 3 ISO/IEC 15408 (parts 1 to 3) ISO/IEC 19790:2012 SN EN 419 211-2 (PP) SN EN 419 211-3 (PP) SN EN 419 211-4 (PP) SN EN 419 221-5 (PP) SN EN 419 211-6 (PP) prEN 419 241-2:2017 (PP) EN 419 241-5 (PP)</p>		
<p>Server Signing Signature Platform Server Signing CEN/TS 419.241, Trustworthy Systems. Supporting Server Signing (TW4S), for Sole Control Assurance Level 1 (SCAL1) and Sole Control Assurance Level 2 (SCAL 2) for QES electronic signatures</p> <p>CEN EN 419 241-2 (PP) CEN EN 419 241-5 (PP)</p> <p>ETSITS 119 432 ETSITS 119 431-1 ETSITS 119 431-2</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071 Seco-SAS SCESp 0127 DAkKS D-ZE-20924-01-00</p>	
<p>Remote Identification Process ETSITS 119 461, Policy and security requirements for trust service components providing identity proofing of trust service subjects as a specialized Identity Proofing Service Provider (IPSP) with the technical support of norm ISO/IEC 30107-3, Information technology: Biometric presentation attack detection, Part 3: Testing and reporting</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	
<p>eIDAS (EU) Reg. 910: 2014 and ETSI EN 319.403 Qualified Electronic Signatures (QES) for European Union (EU) member states</p> <p>CIR 2005/1502: Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification</p> <p>P1: General Provisions P2: Qualified Trust services P3: Qualified Electronic signatures P4: Electronic Seals P5: Electronic Time Stamps</p>	<p>Certification Body Fürstentum Liechtenstein FLCES 006 DAkKS D-ZE-20924-01-00</p>	 

Norms / Standards / Regulations	Accredited Certification Bodies	Conformity Assessment Symbols
<p>(Continuation)</p> <p>P6: Electronic Registered Delivery P7: Website Authentication P8: Qualified Preservation Service/Archive</p>		
<p>Web-Trust CA/Browser Forum, Extended Validation (EV) EV SSL Baseline Certificate Guidelines, WebTrust Extended Validation SSL Code Signing Working Group</p> <p>ETSI EN 319 403 ETSITS 403-2 ETSITS 403-3 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</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	<p>Certification Authorities</p> 
<p>FINMA circle for video- and online-Identification FINMA RS 2016 / 7</p>	<p>KPMG AG</p>	
<p>Electronic Patient Records Management System EPDG, SR 816.1 EPDV, 816.11 EPDV (EDI) TOZ Appendix 2, SR 816.111 IHE (Integrating the Healthcare Enterprise) standards and techniques: IAF MD-1:2018 Inclusive the technical assessment for IT-infrastructure of the EPD platform providers (PP) fort he technical security settings with the security script testing and sample audits of health care organizations based on norm IAF MD-1:2018 for Patient- and healthcare-, and deputy administration-OnBoarding.</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071</p>	 

Norms / Standards / Regulations	Accredited Certification Bodies	Conformity Assessment Symbols
<p>Electronic Patient Identity Product System EPDG, SR 816.1 EPDV, SR 816.1 EPDV (EDI) IDP Appendix 8, SR 816.111 Electronic Patient Identity Management System Technical and organizational Certification Requirements for Electronic Authentication Means and Their Issuers (Protection Profile for Authentication Means)</p> <p>In accordance with (Level of Assurance 3) and Norm ISO/IEC 29115; Security Assurance Requirements (SAR) for the Protection Profile (PP) in accordance with EAL2; Dedicated requirements to norm ISO/IEC 24760-2; Dedicated requirements to norm ISO/IEC 27001; Dedicated requirements to the frameworks SAML-V2 (Assertions and Protocols); incl. technical Vulnerability- and Penetration Testings for the business logic and IDP platform architecture.</p>	<p>Certification Body Zurich Seco-SAS SCESm 0071 Seco-SAS SCESp 0127</p>	 
<p>International Standard on Assurance Engagements ISAE 3000 Typ1, Typ2 (SOC 2) ISAE 3402 Typ1, Typ2 (SOC 2)</p>	<p>KPMG AG</p>	
<p>Electronic Archiving System OR 958ff, GeBüV Based on Verordnung über die Führung und Aufbewahrung der Geschäftsbücher, incl. Obligationenrecht OR Art. 958f</p>	<p>KPMG AG</p>	
<p>Schweizer Prüfungsstandard Softwareprüfung PS 870</p>	<p>KPMG AG EXPERTsuisse</p>	
<p>Prüfungshandlungen bei einem Review-Auftrag PS 910</p>	<p>KPMG AG EXPERTsuisse</p>	

Contact

KPMG AG

Badenerstrasse 172
 PO Box
 CH-8026 Zurich

kpmg.ch

Reto Grubenmann

Director
 Certification Services

+41 58 249 42 46
retogrubenmann@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2023 KPMG AG, a Swiss corporation, is a subsidiary of KPMG Holding AG, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.