Zertifikat

KPMG AG bescheinigt hiermit

Bundesamt für Informatik und Telekommunikation

Eichenweg 3, CH-3003 Bern

für den Geltungsbereich als **Qualifizierter Trust Service Provider (TSP)** für die folgenden qualifizierten Trust-Services:

- Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten
- Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten

gemäss SR 943.03 Bundesgesetz über die elektronische Signatur (ZertES), SR 943.032 Verordnung über die elektronische Signatur (VZertES) und SR 943.032.1 Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate.

Diese ZertES-Zertifizierung enthält die Bewertung in Verbindung mit den ZertES Produktanforderungen und den folgenden international anerkannten ETSI und CEN-Normen:

ETSI EN 319 401 (2026-01)
ETSI TS 119 431-1 (2025-02)
CEN EN 419 241-1 (2018-09)

Die Einzelheiten für jedes Kontrollziel werden im Konformitätsbewertungsbericht validiert.

Dieses Zertifikat ist gültig bis 3. August 2028.
Der qualifizierte Trust Service Provider (QTSP) unterliegt jährlichen Audits.

Zertifikat-Nummer 288 / 2026
Zürich, 4. August 2026

Reto P. Grubenmann
Head of Certification Body
KPMG AG
Switzerland

Jonathan Peters
Lead Trust Services
KPMG AG
Switzerland

Anlage 1 zum Zertifikat 288 / 2026

Zertifizierungsprogramm

Die Zertifizierungsstelle der KPMG AG ist bei der Schweizerischen Akkreditierungsstelle SAS für die Zertifizierung von Produkten in den nach ISO/IEC 17065 und ETSI EN 319 403-1 akkreditiert. Die Zertifizierungsstelle führt ihre Zertifizierungen auf Basis des folgenden akkreditierten Zertifizierungsprogramms durch:

– Certification Scheme F: Remote Signing
  Version 1.1 vom 31.06.2026, KPMG AG

Konformitätsbewertungsbericht

– Server Signing Re-Zertifizierung 2026 gemäss ZertES, Version 1.0 vom 31.07.2026, KPMG AG

Konformitätsbewertungsanforderungen

Die Konformitätsbewertungsanforderungen sind in der ZertES Gesetzgebung definiert: SR 943.03 Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (ZertES) der Bundesversammlung der Schweizerischen Eidgenossenschaft vom 18. März 2016 (Stand am 1. Januar 2020), sowie SR 943.032 Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (VZertES) des Schweizerischen Bundesrat vom 23. November 2016 (Stand am 1. November 2025) und den Technischen und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (TAV) des Bundesamt für Kommunikation BAKOM in der Ausgabe 3 vom 20. August 2025.

Anlage 2 zum Zertifikat 288 / 2026

Konformitätsbewertungsgegenstand

Der Konformitätsbewertungsgegenstand wird charakterisiert durch Zertifikatsinformation des untersuchten Vertrauensdienstes:

Type	Subject Distinguished Name	Fingerprint (SHA256)
Root CA	CN = Swiss Government Root CA IV OU = Swiss Government PKI O = Bundesamt fuer Informatik und Telekommunikation (BIT) C = CH	5A:0B:AF:55:88:E7:3F:CC:33:6C:90:39:B8:59:81:18:92:96:67:0E:FA:99:45:20:FF:00:8B:9A:CF:4D:26:02
Issuing CA	CN = Swiss Government Regulated CA 03 OU = Swiss Government PKI O = Bundesamt fuer Informatik und Telekommunikation (BIT) 2.5.4.97 = NTRCH-CHE-221.032.573 C = CH	E1:A4:A6:58:25:45:1E:14:E1:2D:1A:3B:64:0D:76:DE:28:02:F7:54:91:00:8F:AB:82:E6:D6:78:AF:5E:84:DA

Zusammen mit der Dokumentation des Service Providers:

– Swiss Government PKI - Root CA IV - CP_CPS EN: Certificate Policy and Certification Practice Statement of the Swiss Government Root CA IV, Version 1.42, Datum 13.10.2025

Konformitätsbewertungsergebnis

– Der Konformitätsbewertungsgegenstand erfüllt alle anwendbaren Anforderungen zur Konformitätsbewertung.
– Die im Zertifizierungsprogramm definierten Zertifizierungsanforderungen sind erfüllt.