

Informationen aus der SwissGovernment PKI

Cornelia Enke PO Zertifikate / Beat Roth PM TRUST 24.02.2026



Inhalt

- Ist-Situation
- Warum „Abwarten“ keine Option ist
- Verkürzung der Gültigkeitsdauer der Zertifikate
- Erforderliche Massnahmen
- Herausforderungen
- Roadmap der Swiss Government PKI



Ist-Situation

- **Public Key Infrastructur ist das Fundament digitalen Vertrauens**
Sie schützt Benutzeridentitäten, Geräte, Anwendungen und Kommunikation.
- **Quantencomputer bedrohen das bisherige Sicherheitsmodell**
Alle Verfahren, die auf RSA basieren, werden zukünftig angreifbar. Die langfristige Sicherheit klassischer Algorithmen ist durch Quantencomputing nicht mehr gewährleistet.
- **Risiko für das gesamte Unternehmen**
Eine Kompromittierung der PKI untergräbt die Vertrauensbasis aller sicherheitskritischen Prozesse.



Warum „Abwarten“ keine Option ist

- Angriffe, bei denen die Daten erst gesammelt und dann erst später entschlüsselt werden, finden bereits statt.
- Kryptografische Übergänge dauern Jahre, nicht Monate
- Eingesetzte Technologien haben einen bekannten Quantenbruchpunkt
- Die Nachrüstung von PQC in bestehende PKI-Systeme ist betrieblich komplex
- Compliance und regulatorischer Druck



Verkürzung Gültigkeitsdauer der Zertifikate am Beispiel Klasse C Public



- Ab **15 März 2026**, die maximale Laufzeit für TLS Zertifikate beträgt **200** Tage.
- Ab **15 März 2027**, die maximale Laufzeit für TLS Zertifikate beträgt **100** Tage.
- Ab **15 März 2029**, die maximale Laufzeit für TLS Zertifikate beträgt **47** Tage.



Verkürzung der Gültigkeit der Domain und IP Address-Informationen Validierung



- Ab **15 März 2026**, beträgt die maximale Laufzeit für TLS Zertifikate beträgt **200** Tage.
- Ab **15 März 2027**, beträgt die maximale Laufzeit für TLS Zertifikate beträgt **100** Tage.
- Ab **15 März 2029**, beträgt die maximale Laufzeit für TLS Zertifikate beträgt **10** Tage.



Erforderliche Massnahmen

- Automatisierter Lebenszyklus und richtlinienbasierte Steuerung
- Erhöhung der Schlüssellängen für die Klasse A, B, C & E
- Unterstützung hybrider Kryptografie
- Kryptografische Transparenz und Bestandsbewusstsein
- Algorithmen-Flexibilität



Herausforderungen

- Manuelles und fragmentiertes Zertifikatsmanagement
- Interoperabilitäts- und Abwärtskompatibilitätsbeschränkungen
- Komplexität der hybriden und phasenweisen Migration
- Kompatibilität von Endgeräten, Peripherien, Betriebssystemen, Anwendungen, Kommunikationskomponenten
- Beweiswerterhaltung
- Testen, Testen, Testen.....

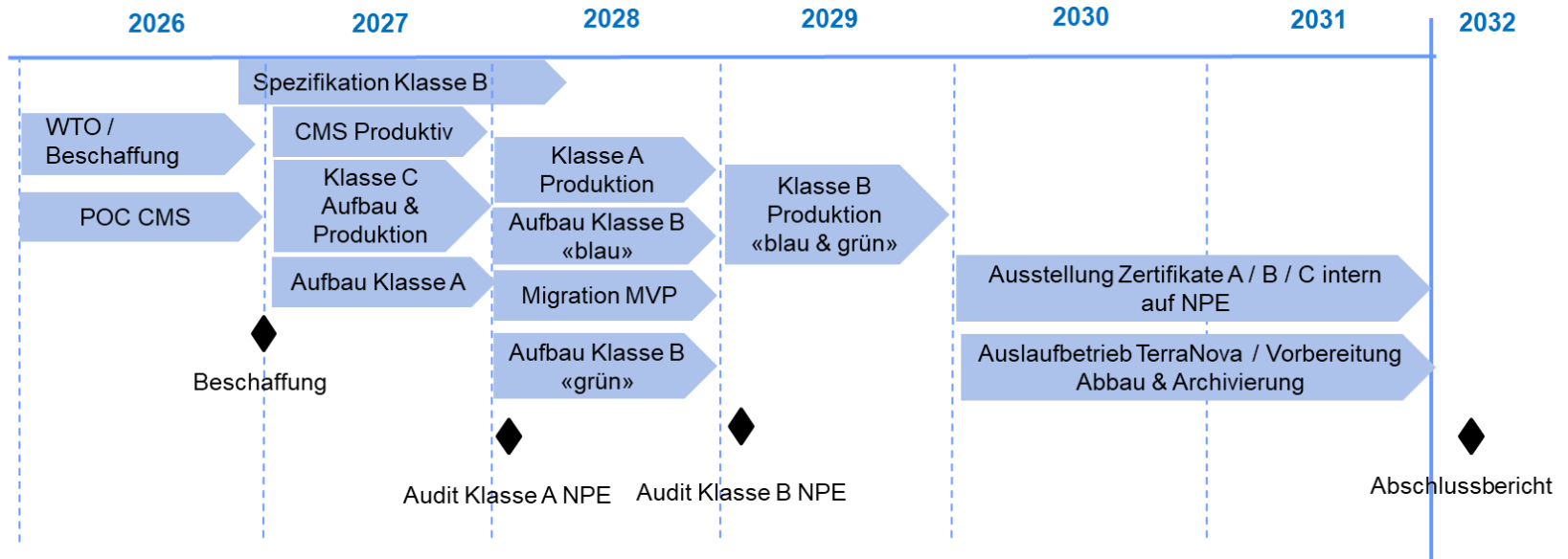


Roadmap der Swiss Government PKI

- Automatisierung bei Zertifikatsbezug und Validierung für Zertifikate der Klasse C PublicTrusted 2026
- Erhöhung der Schlüssellängen für alle Klassen bis 2027
- Einführung einer neuen PKI-Lösung ab 2027 NewPKIEngine
- Ablösung IDPrime 830 durch IDPrime 930
- Bereitstellung hybrider Test Zertifikate – aktuell möglich



Roadmap der Swiss Government PKI



| Meilenstein | Kurzbeschreibung Ergebnis | Zieltermin |
|------------------|--|------------|
| Beschaffung | Komponenten für CA / RA / CMS und Dienstleistungen evaluiert und beschafft | 31.12.2026 |
| Audit Klasse A | Interne Audits und externe Audits KPMG erfolgreich abgeschlossen und Freigabe für Produktion | 31.03.2028 |
| Audit Klasse B | Interne Audits und externe Audits KPMG erfolgreich abgeschlossen und Freigabe für Produktion | 31.03.2029 |
| Abschlussbericht | Abschluss des Projektes NPE | 31.03.2032 |



Handlungsempfehlungen

- Können die Applikationen und Devices mit 3k und 4k Schlüsseln umgehen?
- Können die Applikationen und Devices hybride Zertifikate nutzen?

→ Nehmen Sie Kontakt zu den entsprechenden Leistungserbringern der durch Sie genutzten Applikationen auf, um die Kompatibilitätsprüfungen und Anpassungen durchzuführen!

→ Planen Sie Zeit, Ressourcen und Budget!



Klasse A

- Umstellung der Klasse A mit Signaturdienst ist abgeschlossen
- Klasse A auf Smartcard mit 31.12.2025 abgekündigt. Die ausgegebenen Zertifikate behalten ihre Gültigkeit.

Änderungen VZertES und TVA (Info am 21.08.2025)

Die neuen Fassungen der VZertES und der TVA wurden genehmigt und unterzeichnet.

Sie treten am **1. November 2025** in Kraft. Übergangsbestimmungen sind vorgesehen.

Die neue Ausgabe 3 der TVA wurde auf unserer Seite [Elektronische Signatur](#) veröffentlicht (neben Ausgabe 2).

Die VZertES-Änderung ist über die Medienmitteilung zugänglich news.admin.ch/de/news/bZvmp2f1y7Mwekx_Bk8Vu (Link auf der Webseite [Elektronische Signatur](#)).



Klasse B (Smartcard)

- Anpassung A006 im Q1 2026
 - Keine IDPrime 830 mehr zugelassen ab 2027
 - ID Prime 930 - Ablösung erforderlich beim Einsatz PQC resilienter Algorithmen
- Anpassung der SG PKI Client Tools Q1 2026 für 3k Schlüssel
- Möglichkeit zum **Testen** der neuen Klasse B Karten mit 3k Schlüsseln ab **Juni 2026**
- Umstellung der Schlüssellänge der Klasse B Karten zum Januar 2027
- CY Chrypt ist die massgebende Stelle für Anforderungen der Armee



Klasse C

- Umstellungstermin 3k Schlüssel Abnahme März 2026
- Umstellungstermin 3k Schlüssel Produktion Juli 2026
- Betroffene Marktleistungen:
 - Zertifikate Klasse C Person Auth / Person Sign / Person Encrypt
 - Zertifikate Klasse C Organisation Auth / Organisation Sign / Organisation Encrypt / Organisation Auth/Sign/Encrypt
 - Zertifikate Klasse C System Auth / System Sign / System Encrypt / System Auth/Sign/Encrypt / Sign/Encrypt



Klasse E

- Umstellungstermin Systemgruppe «Non PROD» (z. B. INTEG, ADRI, VOS, ADRV, ADBD) **28. Januar 2026**
- Ab Februar können Sie in Ihren Testumgebungen die Änderungen prüfen.
- Umstellungstermin Systemgruppe PROD (INTRA, ADR, ADA) **25. März 2026**
- Nach diesem Datum werden keine 2k Schlüssel mehr ausgestellt

Kundeninformation vom 10. Dezember 2025

FRAGEN?





Weiterführende Links

- [Allgemeine Informationen zum Post Quanten Computing](#)
- [Empfohlene Algorithmen](#)
- Link zum Umschlüsselungstool [Link zur RETAppl-Anleitung](#)