

Informations provenant de la SwissGovernment PKI

Cornelia Enke PO Certificats / Beat Roth PM TRUST 24.02.2026



Contenu

- Situation actuelle
- Pourquoi « attendre » n'est pas une option
- Diminution de la durée de validité des certificats
- Mesures nécessaires
- Défis
- Feuille de route de la Swiss Government PKI



Situation actuelle

- **L'infrastructure à clé publique est le fondement de la confiance numérique**
Elle protège les identités des utilisateurs, les appareils, les applications et les communications.
- **Les ordinateurs quantiques menacent le modèle de sécurité actuel**
Toutes les procédures basées sur RSA seront vulnérables à l'avenir. La sécurité à long terme des algorithmes classiques n'est plus garantie par l'informatique quantique.
- **Risque pour l'ensemble de l'entreprise**
Une compromission de l'infrastructure PKI compromet la confidentialité de tous les processus critiques pour la sécurité.



Pourquoi « attendre » n'est pas une option

- Des attaques consistant à collecter d'abord les données puis à les décrypter ultérieurement ont déjà lieu.
- Les transitions cryptographiques prennent des années, pas des mois
- Les technologies utilisées ont un point de rupture quantique connu
- La mise à niveau des systèmes PKI existants vers la cryptographie post-quantique (PQC) est complexe sur le plan opérationnel
- Conformité et pression réglementaire

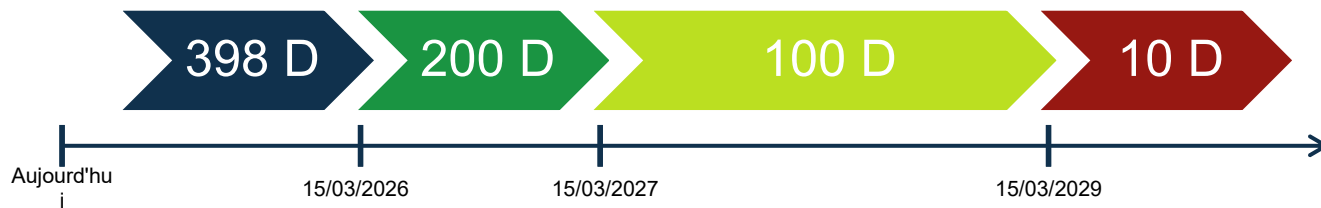
❖ Réduction de la durée de validité des certificats : Exemple de la Classe C publique



- À partir du **15 mars 2026**, la durée maximale des certificats TLS sera de **200** jours.
- À partir du **15 mars 2027**, la durée maximale des certificats TLS sera de **100** jours.
- À partir du **15 mars 2029**, la durée maximale des certificats TLS sera de **47** jours.



Réduction de la durée de validité de la validation des informations relatives au domaine et à l'adresse IP



- À partir du **15 mars 2026**, la durée maximale des certificats TLS sera de **200** jours.
- À partir du **15 mars 2027**, la durée maximale des certificats TLS sera de **100** jours.
- À partir du **15 mars 2029**, la durée maximale des certificats TLS sera de **10** jours.



Mesures nécessaires

- Cycle de vie automatisé et contrôle basé sur des directives
- Augmentation de la longueur des clés pour les classes A, B, C et E
- Prise en charge de la cryptographie hybride
- Transparence cryptographique et connaissance de l'inventaire
- Flexibilité des algorithmes



Défis

- Gestion manuelle et fragmentée des certificats
- Restrictions en matière d'interopérabilité et de compatibilité ascendante
- Complexité de la migration hybride et progressive
- Compatibilité des terminaux, périphériques, systèmes d'exploitation, applications, composants de communication
- Conservation des preuves
- Tester, tester, tester...

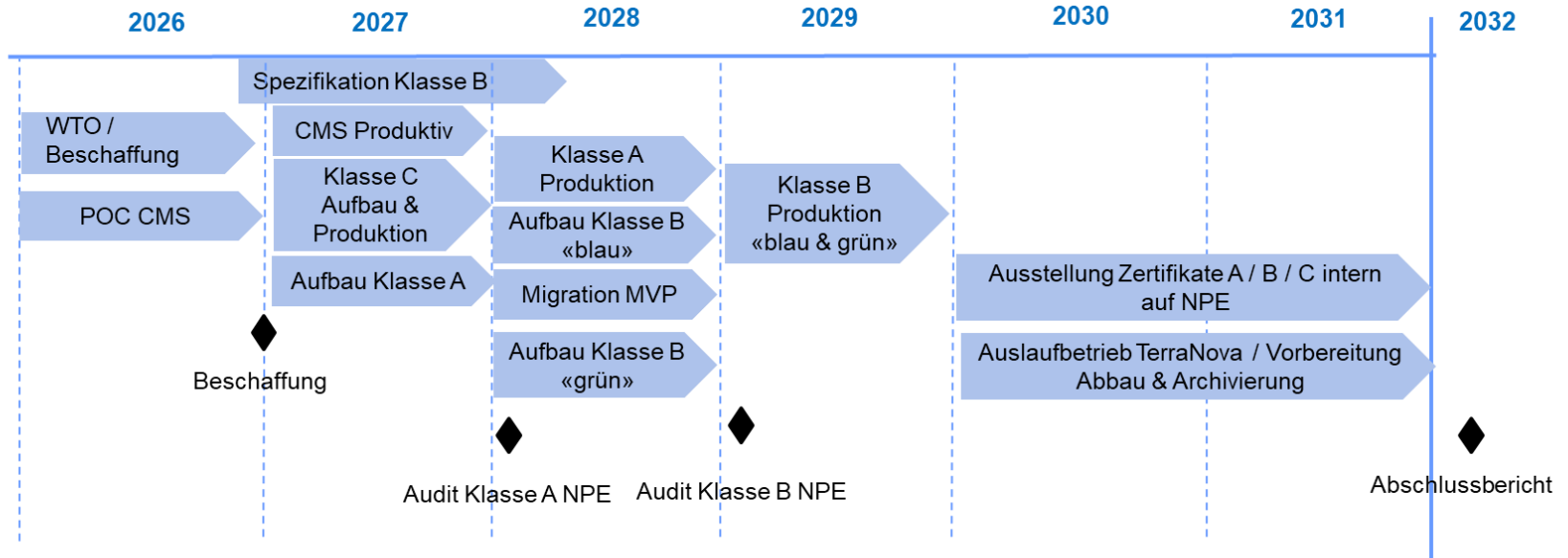


Roadmap de la Swiss Government PKI

- Automatisation de l'obtention et de la validation des certificats de classe C PublicTrusted 2026
- Augmentation de la longueur des clés pour toutes les classes d'ici 2027
- Introduction d'une nouvelle solution PKI à partir de 2027 New PKIEngine
- Remplacement d>IDPrime 830 par IDPrime 930
- Mise à disposition de certificats de test hybrides – actuellement possible



Roadmap de la 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



Recommandations

- Les applications et les appareils peuvent-ils gérer les clés 3k et 4k ?
- Les applications et les appareils peuvent-ils utiliser des certificats hybrides ?

→ *Contactez les responsables des applications que vous utilisez (à partir du niveau 3 pour les applications spécialisées - au niveau des départements et des offices) afin de procéder aux tests de compatibilité et aux adaptations nécessaires !*

→ *Prévoyez du temps, des ressources et un budget !*



Classe A

- La transition vers la classe A avec service de signature est terminée
- La classe A sur carte à puce sera supprimée au 31 décembre 2025. Les certificats délivrés restent valables.

Modifications de l'OCertES et de l'OTSA (info du 21 août 2025)

Les nouvelles versions de l'OCertES et de l'OTSA ont été approuvées et signées.

Elles entreront en vigueur le **1er novembre 2025**. Des dispositions transitoires sont prévues.

La nouvelle édition 3 de la TAV a été publiée sur notre page [Signature électronique](#) (à côté de l'édition 2).

La modification de l'OCertSE est accessible via le communiqué de presse news.admin.ch/fr/newnsb/bZvmp2f1y7Mwekx_Bk8Vu (lien sur le site web [Signature électronique](#)).



Classe B (carte à puce)

- Adaptation A006 au premier trimestre 2026
 - IDPrime 830 n'est plus autorisé à partir de 2027
 - ID Prime 930 - Remplacement nécessaire en cas d'utilisation d'algorithmes résilients PQC
- Adaptation des outils client SG PKI au premier trimestre 2026 pour les clés 3k
- Possibilité de **tester** les nouvelles cartes de classe B avec des clés 3k à partir de **juin 2026**
- Changement de la longueur de clé des cartes de classe B en janvier 2027
- KDO Cy KRYPT est l'autorité compétente pour les exigences de l'armée



Classe C

- Date de conversion 3k Clé Acceptation (Pre-Prod) mars 2026
- Date de conversion 3k Clé Production juillet 2026
- Prestations commerciales concernées :
 - Certificats de classe C Person Auth / Person Sign / Person Encrypt
 - Certificats de classe C Organisation Auth / Organisation Sign / Organisation Encrypt / Organisation Auth/Sign/Encrypt
 - Certificats de classe C Système Auth / Système Sign / Système Encrypt / Système Auth/Sign/Encrypt / Sign/Encrypt



Classe E

- Date de migration Groupe de systèmes « Non PROD » (par exemple INTEG, ADRI, VOS, ADRV, ADBD) **28 janvier 2026**
- À partir de février, vous pourrez vérifier les modifications dans vos environnements de test.
- Date de transition du groupe de systèmes PROD (INTRA, ADR, ADA) **25 mars 2026**
- Après cette date, aucune clé 2k ne sera plus délivrée.

Information client du 10 décembre 2025



**DES
QUESTIONS
?**



Liens complémentaires

- [Informations générales sur l'informatique post-quantique](#)
- [Le Q-Day arrive ! Optez dès maintenant pour un cryptage quantique sécurisé !](#)
- [Algorithmes recommandés](#)
- Lien vers l'outil de conversion [Lien vers le guide RETAppI](#)