ChatGPT

SwissSign und der S/MIME-Silver-Vorfall 2026

Executive Summary

Der derzeit öffentlich belegte Kern des Vorfalls ist ein am 17. April 2026 in Mozilla [1] Bugzilla veröffentlichtes Preliminary Incident Report von SwissSign, Bug 2033000, mit dem Titel „SwissSign: Certificate Profile error for S/MIME MV“. Darin erklärt SwissSign, die Auditoren hätten am selben Tag einen Fehler in Kapitel 3.3.1.7 der öffentlichen CPR für S/MIME gemeldet: Das Feld `subject:commonName` sei dort für Mailbox-Validated-Zertifikate als „GivenName Surname or pseudo: Pseudonym“ beschrieben, obwohl die S/MIME Baseline Requirements für Mailbox-Validated-Zertifikate dort, falls `commonName` überhaupt verwendet wird, nur eine Mailbox Address zulassen. SwissSign erklärt zugleich ausdrücklich, man habe betroffene Zertifikate stichprobenartig geprüft und diese seien „fully compliant with the S/MIME BR“. Die am 17. April 2026 datierte CPR-Version 15 ergänzt deshalb in genau diesem Profil den Hinweis, dass der tatsächliche `CN` im End-Entity-Zertifikat immer aus dem Feld „Email“ kopiert werde und damit stets die E-Mail-Adresse enthalte. Ergänzende Partnerhinweise von NoSpamProxy [2] und SEPPmail [3] nennen als betroffen den Zertifikatstyp „SwissSign Personal S/MIME E-Mail ID Silver“ und den Ausstellungszeitraum 15. Juli 2025 bis 17. April 2026; die automatische Widerrufung wurde dort für den 22. April 2026 um 15:00 Uhr angekündigt. [4]

Nach der heutigen Beleglage spricht mehr dafür, dass keine materielle Leaf-Zertifikatsabweichung, sondern primar ein Dokumentations- und Governance-Problem vorlag. Allerdings ist die Formel „blosser Dokumentationsfehler“ zu eng, weil die bindenden offentlichen Policy-Dokumente in der Public PKI nicht bloss Begleittext, sondern Auditobjekt, Zusicherung und Teil des Vertrauensvertrags sind. Zudem zeigt die aktuell gultige CP fur Mailbox-Validated/LCP-S-MIME neben dem CPR-Fehler weitere Formulierungen, die mit dem Mailbox-Validated-Profil der S/MIME BR nur schwer vereinbar sind; das Dokument spricht etwa von „additional attributes in the CN besides e-mail address“ und davon, dass in MV/LCP-Zertifikaten Pseudonyme verwendet werden konnten. Damit ist zwar immer noch nicht bewiesen, dass die real ausgestellten End-Entity-Zertifikate materiell falsch waren; es ist aber offentlich sichtbar, dass das Dokumentationsproblem wohl breiter war als eine einzige unglückliche Zeile in der CPR. [5]

Regulatorisch ist SwissSigns konservative Reaktion nachvollziehbar: Die S/MIME Baseline Requirements verlangen den Widerruf binnen funf Tagen, wenn ein Zertifikat nicht in Ubereinstimmung mit den Requirements oder mit der eigenen CP/CPS ausgestellt wurde, und die CCADB-Incident-Guidelines behandeln bereits Auditfeststellungen und Verstosse gegen eigene CA-Dokumente als meldepflichtige Incidents. Inhaltlich ist die Verhaltnismassigkeit jedoch ambivalent: Falls die Leaf-Zertifikate tatsachlich bereits BR-konform waren und bei einer Neuausstellung inhaltlich identisch geblieben waren, ist der kryptografische Sicherheitsgewinn des Massenwiderrufs sehr gering, wahrend Betriebsrisiko, Administrationsaufwand und Ausfallpotenzial real sind. Genau diese Spannung ist in Root-Store-Diskussionen bereits benannt worden; das 2025 Roundtable-Protokoll spricht offen von „pointless mass revocations“ bei trivialen CPS-Fehlern und warnt vor Fehlanreizen zu absichtlich vagen CP/CPS-Texten. Der Vorfall ist deshalb am besten als Schwache der Governance-, Audit- und Revokationsarchitektur der Public PKI zu verstehen, nicht als Versagen der asymmetrischen Kryptografie. Kurzere Laufzeiten andern an genau diesem Fehlertyp wenig; sie begrenzen nur, wie lange und in welcher Zahl problematische Zertifikate gleichzeitig im Umlauf bleiben. Da bisher nur ein Preliminary Incident Report offentlich vorliegt, bleiben endgultige Aussagen zu Volumen, Root Cause, finaler Rechtsauffassung und nachhaltigen Abhilfemassnahmen vorerst offen. [6]

Gesicherte Fakten

1. Am 17. April 2026 um 14:32:58 UTC wurde in Bugzilla der Incident Bug 2033000 „SwissSign: Certificate Profile error for S/MIME MV“ angelegt; es handelt sich offentlich erst um einen „Preliminary Incident Report“, nicht um einen abgeschlossenen Vollbericht. [7]

2. SwissSign gibt in diesem Bericht an, die Auditoren hatten „heute“ einen Fehler in Kapitel 3.3.1.7 der CPR S/MIME gemeldet; beanstandet wurde das Feld `commonName` des Mailbox-Validated-Profils gegen S/MIME BR 7.1.4.2.2. [8]

3. Die beanstandete CPR-Beschreibung lautete fur das Mailbox-Validated-Multipurpose-Profil in Version 14: `Common Name (CN): GivenName Surname or pseudo: Pseudonym (mandatory)`. [9]

4. Die gultige CPR-Version 15 vom 17. April 2026 enthalt fur genau dieses Profil einen neuen Hinweis: Die `CN`-Definition werde aus dem Template generiert, der tatsachliche `CN` in End-Entity-Zertifikaten werde aber stets aus dem Feld „Email“ kopiert und enthalte daher immer die E-Mail-Adresse des Subject. [10]

5. SwissSign schreibt im Preliminary Report ausdrucklich, man habe die betroffenen ausgestellten Zertifikate stichprobenartig gepruft; aufgrund dieser ersten Prufung seien die ausgestellten Zertifikate „fully compliant with the S/MIME BR“. [11]

6. SwissSign beruft sich zugleich auf S/MIME BR 4.9.1.1 Ziffer 11 und erklart, deshalb sei trotz BR-konformer Leaf-Zertifikate ein Widerruf binnen 120 Stunden erforderlich. [12]

7. Die S/MIME BR verlangen fur `subject:commonName` bei Mailbox-Validated-Zertifikaten, falls `commonName` vorhanden ist, eine Mailbox Address; zudem sind im Mailbox-Validated-Profil `givenName`, `surname` und `pseudonym` im Subject Distinguished Name jeweils `SHALL NOT`. [13]

8. Das betroffene CPR-Profil 3.3.1.7 listet zugleich `Subject Alternative Name` mit `RFC822: E-Mail address of the subject (mandatory)`, `Key Usage (critical): digitalSignature, keyEncipherment`, `Extended Key Usage: id-kp-emailProtection` und als BR-Policy-OID `2.23.140.1.5.1.2 (CAB SMIME BR Mailbox-Validated Multipurpose)`. Der offentliche Incident Report benennt fur diese Felder keinen Verstoss. [9]

9. Die offentliche SwissSign-Produktseite fur „E-Mail ID Silver (DV)“ beschreibt den Zertifikatstyp mit „CN = common name: e-mail address (mandatory)“, sagt, die SAN enthalte die E-Mail-Adresse, und dass weitere antragstellerspezifische Eintrage nicht erlaubt seien. [14]

10. Die SwissSign-FAQ erklart zusatzlich, dass die Platzierung der E-Mail-Adresse im `emailAddress`-Attribut des Subject Distinguished Name veraltet sei und von SwissSign nicht mehr verwendet werde. [15]

11. Die CPR-Revisionshistorie zeigt, dass Version 12 vom 19. Mai 2025 „Adding (MV, SV) and updating (OV) Multi-Purpose end-user profiles“ brachte und Version 15 vom 17. April 2026 den Hinweis zur tatsachlichen `CN`-Belegung in 3.3.1.7 nachtrug. [16]

12. Die CPR dokumentiert fur das Legacy-MV-Profil, dass dessen Ausstellung spatestens bis 15. Juli 2025 erfolgte; Partnerhinweise von NoSpamProxy und SEPPmail nennen fur den Vorfall als betroffen die „SwissSign Personal S/MIME E-Mail ID Silver“-Zertifikate, die zwischen dem 15. Juli 2025 und dem 17. April 2026 ausgestellt wurden. [17]

13. Dieselben Partnerhinweise nennen als automatische Widerrufsfrist den 22. April 2026, 15:00 Uhr Ortszeit. SwissSign selbst hat diese Frist im bisher offentlichen Bug bislang noch nicht in einem Full Incident Report mit eigener Timeline publiziert. [18]

14. Die Mozilla Root Store Policy macht offentlich dargelegte CP/CPS-Dokumente zum zentralen Prufobjekt; sie verlangt hinreichend detaillierte, offentlich verfugbare Dokumentation, historische Versionen und dass CA-Operationen jederzeit der anwendbaren CP/CPS entsprechen. [19]

15. Die CCADB-Incident-Reporting-Guidelines definieren bereits Verstosse gegen eigene CA-Policies, CA/B-Forum-Regeln, Root-Store-Policies oder Auditfeststellungen als Incident; ein audit finding muss innerhalb von 72 Stunden in einem Incident Report offengelegt werden. [20]

Materielle technische Analyse

Der Kernkonflikt liegt im Subject-Naming des Mailbox-Validated-Multipurpose-Profils. Die S/MIME BR erlauben bei Mailbox-Validated-Zertifikaten als `subject:commonName`, falls dieser uberhaupt vorhanden ist, nur eine Mailbox Address; gleichzeitig sind `givenName`, `surname` und `pseudonym` in diesem Profil verboten. Die alte CPR-Version 14 beschrieb jedoch gerade dieses `commonName`-Feld fur das relevante Profil 3.3.1.7 mit einem personellen/pseudonymen Inhalt, also so, wie man es eher bei Sponsor- oder Individual-Validated-Profilen erwarten wurde. Das ist ein klarer Normkonflikt auf Dokumentationsebene. [21]

Technisch wichtig ist aber die zweite Ebene: Dieselbe CPR-Version 15 halt nun explizit fest, dass der im End-Entity-Zertifikat eingesetzte `CN` immer aus „Email“ kopiert werde und daher immer die E-Mail-Adresse enthalte. Genau das deckt sich sowohl mit SwissSigns eigener Produktdokumentation fur Silver-Zertifikate als auch mit der FAQ-Aussage, dass SwissSign das alte `subject:emailAddress`-Attribut im Subject nicht mehr nutze. Wenn diese Selbstauskunft zutrifft, spricht sie stark dafur, dass die realen Leaf-Zertifikate beim kritischen Feld `commonName` materiell BR-konform waren und die Divergenz im Template bzw. in der CPR-Beschreibung lag. [22]

Bei den weiteren vom Auftrag besonders genannten Feldern zeigt die offentliche Aktenlage derzeit kein positives Indiz fur materielle Leaf-Abweichungen. Das betroffene CPR-Profil 3.3.1.7 nennt fur `subjectAltName` ein verpflichtendes RFC822-Name-E-Mail-Feld, fur `certificatePolicies` den korrekten MV-Multipurpose-BR-OID `2.23.140.1.5.1.2`, fur `EKU` `id-kp-emailProtection`, und fur `KeyUsage` `digitalSignature` plus `keyEncipherment`. Der Preliminary Report benennt keinen Verstoss bei SAN, `certificatePolicies`, `EKU` oder `KeyUsage`, sondern allein beim `commonName`. Auch das spricht eher gegen eine materielle Leaf-Fehlprofilierung in diesen Feldern. [23]

Beim Zusammenspiel von `givenName`, `surname`, `pseudonym` und `emailAddress` ist die Lage feiner. Im konkret beanstandeten CPR-Profil 3.3.1.7 werden `givenName`, `surname` und `pseudonym` nicht als eigene DN-Attribute aufgelistet; die Fehlbeschreibung steckt im Wert des `commonName`. Das mildert die technische Schwere: Ein falsches Label in der Profilbeschreibung ist etwas anderes als ein tatsachlich erzeugtes DN mit verbotenen Attributen. Gleichwohl ist das Dokumentationsumfeld unsauberer, als SwissSigns Preliminary Report derzeit erkennen lasst. Die aktuell gultige CP fur Mailbox-

Validated/LCP-S-MIME sagt im Ubersichtsteil, sie gelte fur Zertifikate „with additional attributes in the CN besides e-mail address“, und erklart spater, MV/LCP-Zertifikate enthielten eine E-Mail im `CN`, Pseudonyme konnten aber ebenfalls verwendet werden. Das passt schlecht zum Mailbox-Validated-Profil der S/MIME BR. Ich werte das nicht als Beweis fur materiell falsche Leafs, wohl aber als klaren Hinweis darauf, dass das Problem wahrscheinlich nicht auf eine einzige CPR-Zeile reduziert werden sollte. [24]

Soll-Ist-Wurdigung der wesentlichen Felder

`subject:commonName`
Soll nach S/MIME BR fur Mailbox-Validated: falls vorhanden, Mailbox Address. Ist nach CPR v14: „GivenName Surname or pseudo: Pseudonym“; Ist nach CPR v15 laut Nachtrag tatsachlich im Leaf immer die E-Mail-Adresse. Befund: offentliche Profildokumentation war falsch; offentliche Evidenz fur materiell falsche Leafs liegt derzeit nicht vor. [25]

`givenName`, `surname`, `pseudonym`
Soll nach S/MIME BR im Mailbox-Validated-Profil: jeweils `SHALL NOT`. Im betroffenen CPR-Profil 3.3.1.7 werden diese Attribute nicht als eigene DN-Felder gelistet; die CP enthalt aber weiterhin Text, der ihre Verwendung in MV/LCP nahelegt. Befund: kein offentlich belegter Leaf-Verstoss, aber deutliche Dokumentations- und Governance-Unsauberkeit. [26]

`subject:emailAddress` **und** `subjectAltName`
Soll nach S/MIME BR: SAN ist verpflichtend; Subjekt-Mailboxen mussen in SAN gespiegelt sein. CPR 3.3.1.7 nennt RFC822-SAN als obligatorisch; SwissSign sagt zudem, das alte `subject:emailAddress`-Attribut werde fur Silver nicht mehr genutzt. Befund: keine belegte materielle Abweichung. [27]

`certificatePolicies`, `EKU`, `KeyUsage`
CPR 3.3.1.7 nennt die BR-Policy-OID fur Mailbox-Validated Multipurpose, `id-kp-emailProtection` als EKU und `digitalSignature` plus `keyEncipherment` als Key Usage. Der Incident Report beanstandet keines dieser Felder. Befund: nach heutiger offener Evidenz kein materieller Leaf-Fehler in diesen Feldern nachweisbar. [23]

Meine strengste, quellengetreue Zwischenbewertung lautet deshalb: **Gesichert** ist ein dokumentierter Profil- und Policyfehler in den offentlichen Dokumenten. **Plausibel, aber noch nicht unabhangig verifiziert** ist, dass die realen End-Entity-Zertifikate materiell BR-konform waren. **Nicht gesichert** ist dagegen die weitergehende, stark vereinfachende These, es habe sich nur um einen einzigen isolierten Dokumentationssatz gehandelt; die offentliche CP spricht gegen eine so enge Charakterisierung. [28]

Regulatorische Analyse

Rechtlich-regulatorisch sind vier Ebenen zu unterscheiden. Erstens gelten die S/MIME Baseline Requirements des CA/Browser Forum [29] unmittelbar fur offentlich vertrauenswurdige S/MIME-Zertifikate. Zweitens macht die Mozilla Root Store Policy klar, dass S/MIME-End-Entity-Zertifikate im Mozilla-Scope den S/MIME BR entsprechen mussen. Drittens verlangt Mozilla detaillierte, offentlich verfugbare und historisch nachvollziehbare CP/CPS-Dokumente und bestimmt ausdrucklich, dass CA-Operationen jederzeit der anwendbaren CP/CPS entsprechen mussen. Viertens machen die CCADB-Guidelines aus Auditfindings und aus Verstoessen gegen eigene CA-Dokumente meldepflichtige, offentlich zu behandelnde Incidents. [30]

Damit ist die Rolle der CA-Dokumentation normativ deutlich starker als blosse „Beschreibung“. Sie ist zugleich Zusicherung, Auditgegenstand und Prufgrundlage fur Root Stores und Dritte. Das wird in den S/MIME BR nochmals bestarkt: Die CA erklart mit der Ausstellung, sie habe nicht nur passende Verifikationsverfahren implementiert und angewendet, sondern diese auch in CP/CPS korrekt beschrieben. Gerade deshalb kann eine dokumentarische Fehlbeschreibung regulatorisch erheblich sein, selbst wenn die Leaf-Zertifikate technisch richtig gebaut wurden. In diesem Punkt ist der Vorfall kein blosser Formalismus ohne Regelungszweck, sondern ein Zusammenprall mit einem zentralen Governance-Prinzip der Public PKI. [31]

Die scharfste Vorschrift ist dann S/MIME BR 4.9.1.1 Ziffer 11: Der CA muss binnen funf Tagen widerrufen, wenn sie erkennt, dass das Zertifikat nicht in Ubereinstimmung mit den Requirements oder mit der eigenen CP/CPS ausgestellt wurde. SwissSign beruft sich auf genau diese Norm. Aus streng positivistischer Sicht ist das eine gut vertretbare Lesart: Wenn die offentliche CPR den Zertifikatstyp anders beschreibt als die reale Ausstellung, entsteht ein Konflikt zwischen Zertifikat und CA-Dokumentation; damit greift die Widerrufsnorm. [12]

Vollig eindeutig ist die Sache dogmatisch aber nicht. Denn sowohl die SwissSign-CP als auch die SwissSign-CPS enthalten Klauseln, wonach im Kollisionsfall die Baseline Requirements den eigenen Dokumenten vorgehen. Gerade in einem ahnlichen TLS-Fall hat Entrust [32] 2024 spater argumentiert, bei einer typographischen CPS-Fehlstelle liege eigentlich gar keine Misissuance vor, weil das Dokument als Ganzes die BR priorisiere und die Leaf-Zertifikate technisch korrekt seien. Das zeigt: Die Frage, ob schon jede rein dokumentarische Profildifferenz zwingend zur Misissuance im materiellen Sinn fuhrt, ist im Root-Store-Umfeld umstritten. SwissSign hat sich im aktuellen S/MIME-Fall bislang fur die konservative Seite dieser Auslegung entschieden; ein offentliches Root-Store-Votum dazu liegt per 22. April 2026 noch nicht vor. [33]

Meine juristisch-technische Ableitung lautet daher: **Nach geltendem Regelwerk ist ein Incident Report klar geboten; ein Widerruf ist vertretbar und wohl regeltextnah. Nicht ebenso klar ist, dass ein solcher Fall in jedem denkbaren Interpretationsmodell zwingend als materielle Misissuance mit sofortigem Massenwiderruf behandelt werden muss.** Genau diese Differenz zwischen Regeltext, Governance-Zweck und Schadensrealitat ist der eigentliche Streitpunkt. [34]

Verhaltnismassigkeitsprufung

Pro harte Massenwiderrufe.
Das starkste Argument fur eine harte Reaktion ist die Integritat des Public-Trust-Regimes. Root Stores konnen eine globale Vertrauenskette nur dann seriell beaufsichtigen, wenn offentliche Dokumente, Audits und reale Ausstellung deckungsgleich sind. Sobald man beginnt, „harmlos“ und „nicht harmlos“ nach Fallgefuhl zu unterscheiden, entsteht schnell Ex-post-Kasuistik: Jede CA wird dann ihren eigenen Dokumentationsfehler als substanzlos darstellen. Eine klare funf-Tage-Regel schafft dagegen Vorhersehbarkeit, Vergleichbarkeit zwischen CAs und einen starken Anreiz, Policy-Dokumente und produktive Konfiguration aus einer gemeinsamen Quelle zu generieren. Genau diese Art von Single-Source-of-Truth-Massnahme hatte SwissSign bereits nach dem S/MIME-Vorfall 2024 als Abhilfe eingefuhrt. [35]

Contra harte Massenwiderrufe.
Das starkste Gegenargument ist der nahezu fehlende materielle Sicherheitsgewinn, sofern SwissSigns eigene Aussage zutrifft und die Leaf-Zertifikate bereits BR-konform waren. Dann werden nicht unsichere oder tauschende Zertifikate aus dem Verkehr gezogen, sondern funktional korrekte Zertifikate, die bei Neuausstellung inhaltlich im Wesentlichen identisch blieben. Der Nutzen liegt dann

fast ausschliesslich in Governance-Disziplin, nicht in Kryptografie oder Missbrauchsverhinderung. Dem stehen reale Kosten gegenuber: Austauschdruck in Stunden statt Wochen, Admin-Aufwand, mogliche Betriebsstorungen, unterbrochene Signatur- und Verschlusselungsablaufe und erhoter Support-Bedarf. Genau diese Lage wurde im Root-Store-Diskurs 2025 als „pointless mass revocations“ beschrieben. [36]

Kryptografischer Sicherheitsgewinn.
Nach der heutigen Evidenz gering. Weder nennt SwissSign einen privaten Schlusselfehler noch einen kryptografischen Angriff noch eine materielle Leaf-Profilverletzung im ausgestellten Zertifikat. Das Problem betrifft die Ubereinstimmung zwischen Dokumentation und Issuance. [11]

Governance- und Auditierbarkeitsgewinn.
Hoch. Der Fall erzwingt, dass CP/CPS/CPR nicht als Marketing- oder Nebenartefakte behandelt werden, sondern als bindende, auditable Systembeschreibung. Gerade dieser Druck dient der Funktionsfahigkeit von Root-Store-Aufsicht. [37]

Betrieblicher Schaden fur Kunden.
Real und vorhersehbar. Die Partnerhinweise beschreiben unmittelbaren Handlungsbedarf, Ersatzbeschaffung, Installationsdruck und die Gefahr, dass Signatur- und Verschlusselungsfunktion nach dem Widerruf nicht mehr sauber arbeiten. [38]

Anreizwirkungen fur CAs.
Ambivalent. Positiv ist der Anreiz zur Dokumentations- und Prozessdisziplin. Negativ ist die Gefahr, dass CAs CP/CPS/CPR absichtlich abstrakter und weniger prufbar formulieren, um sich nicht auf konkrete, widerrufsrelevante Details festzulegen. Genau diesen perversen Anreiz hat die Root-Store-Diskussion 2025 ausdrucklich benannt. [39]

Denkbare Alternativen und ihre Bewertung.
Ein alternativ niedrigerer Eingriff ware ein offentliches Incident Reporting mit sofortiger Dokumentkorrektur und historischer Annotation, kombiniert mit erhohtem Auditdruck und Austausch spatestens beim nachsten Renewal, sofern keine materielle Leaf-Abweichung nachweisbar ist. Sicherheitlich ware das nur dann vertretbar, wenn die Leaf-Zertifikate tatsachlich BR-konform sind; auditierbar ware es bei klarer offentlich dokumentierter Korrektur und Zusatzprufung durchaus; fur die Marktstabilitat ware es deutlich besser; die Anreizwirkung auf CAs ware jedoch schwacher als beim harten Widerruf und musste durch strengere Audits oder Sanktionen kompensiert werden. Ein zweites Modell ware gezielter Widerruf nur jener Zertifikate, deren reale Inhalte materiell abweichen; das ware proportionaler, setzt aber belastbare Leaf-Evidenz und saubere Segmentierung voraus. Ein drittes Modell ware die heutige Bright-Line-Regel beizubehalten, aber einen eng umrissenen, offentlich begrundeten Ausnahmeprozess fur rein dokumentarische, sicherheitsneutrale Abweichungen zu schaffen. Gerade eine solche Losung wurde im Roundtable 2025 sinngemass angedacht. [40]

Eigene abgewogene Bewertung.
Unter dem heutigen Regime war SwissSigns Entscheidung zum Massenwiderruf **rechtlich und governance-seitig defensibel**, vielleicht sogar die risikoarmste Wahl gegenuber Root Stores. **In materieller Sicherheitssubstanz erscheint sie hingegen eher schwach verhaltnismassig**, sofern sich SwissSigns Aussage uber BR-konforme Leaf-Zertifikate bestatigt. Anders gesagt: Die Massnahme passt zur gegenwartigen Public-PKI-Disziplinierungslogik, aber nur begrenzt zur tatsachlichen technischen Schadenslage. [41]

Grundsatzanalyse zur PKI-Frage

An der Nutzerkritik ist erstens richtig, dass dieser Vorfall **kein** Beispiel fur gebrochene Kryptografie ist. Es ging nicht um RSA, ECC, Signaturalgorithmen oder kompromittierte Schlusselfuhrung, sondern um Dokumentation, Profilgovernance und Revokationsfolgen. Zweitens ist richtig, dass immer kurzere Laufzeiten einen solchen Vorfall **nicht verhindern**: Ein falscher CPR/CP/CPS-Eintrag kann bei 825 Tagen, 398 Tagen oder 47 Tagen gleichermassen entstehen. Drittens ist richtig, dass der betriebliche Friktionsanteil in der Public PKI real ist und dass starre Revokationspflichten bei formalistischen Vorfallen den Eindruck eines „kaputten“ Systems verstarken konnen. [41]

Uberzeichnet ist die Kritik dort, wo sie Laufzeitverkurzungen als generell nutzlos darstellt. Kurze Laufzeiten reduzieren nachweislich andere Risikoklassen: Sie begrenzen die Zeit, wahrend der veraltete oder falsch wiederverwendete Validierungsdaten wirken, sie verkurzen das Fenster fur falsch gebliebene Subjektinformationen, und sie erleichtern die Durchsetzung neuer Profile und neuer Kryptografie. Genau dies ist sowohl in den geltenden S/MIME-BR-Grenzen fur Validity und Data Reuse als auch in der TLS-Debatte um SC-081 als Begrundung angelegt. Die Laufzeitverkurzung lost also das hiesige Governance-Problem nicht, sie reduziert aber die Halbwertszeit anderer, zeitgebundener Fehlerklassen. [42]

Die Aussage „Wenn PKI in Ordnung ware, konnte man Zertifikate auch fur tausend Jahre ausstellen“ ist fur die **offentliche Public-Trust-PKI** unzutreffend. Nicht die Mathematik allein bestimmt dort die sinnvolle Lebensdauer, sondern die Dynamik der attestierten Welt: Mailbox-Inhaberschaft andert sich, Organisationen verschwinden oder fusionieren, Algorithmen und Profile werden abgelost, Root-Store-Policies entwickeln sich weiter, und Application Software Suppliers konnen fruhere Praktiken nachtraglich fur unzureichend erklaren. In diesem Umfeld ist ein Zertifikat nicht bloss ein kryptografischer Schlusselcontainer, sondern ein zeitgebundener, regulatorisch uberwachter Tatsachenbefund. Darum begrenzen Root-Store- und BR-Regime Lebensdauern. [43]

Anders liegt der Fall in einer **internen Enterprise- oder Closed-PKI**. Dort sind Trust Anchors, Relying Parties, Identitatsquellen und Durchsetzungshoheit zentral gesteuert; Attribute und Prozesse konnen lokal festgelegt werden, und die Organisation kann ihre eigene Balance zwischen Laufzeit, Widerruf, Automatisierung und Betriebsstabilitat definieren. Das macht lange Laufzeiten eher denkbar als in der offenen Web- bzw. Mail-PKI. Aber auch dort werden tausend Jahre praktisch nicht vernunftig: Lange Laufzeiten erhohen die Blast Radius kompromittierter oder veralteter Schlusssel, erschweren Algorithmuswechsel und machen organisatorische Altlasten langlebig. Kontrolledichte ersetzt also nicht die Notwendigkeit zu Lebenszyklusmanagement; sie verandert nur die Trade-offs. [44]

Wenn man die strukturellen Schwachen sauber trennt, liegt das Hauptproblem dieses Vorfalls **nicht primar in der Kryptografie**, sondern in vier anderen Schichten: in der Revokationsarchitektur, die auch bei sicherheitsneutralen Vorfallen massive operative Folgen produziert; in der Root-Store-Governance, die globale harte Regeln fur heterogene Einzelfalle setzt; in der Audit- und Dokumentationslogik, die einerseits zurecht Genauigkeit fordert, andererseits aber nur begrenzte abgestufte Reaktionen kennt; und in der globalen Trust-Topologie, in der wenige Root-Programme weltweit faktisch normsetzend wirken. Der Satz „das PKI-System ist strukturell kaputt“ ist mir deshalb zu total, aber als Diagnose fur die **Governance- und Betriebsarchitektur** der Public PKI steckt darin ein erheblicher wahrer Kern. [45]

Vergleichsfalle und offene Punkte

Der naheliegendste Vergleichsfall ist ein fruherer SwissSign-S/MIME-Incident aus 2024, Bug 1929189. Dort meldete SwissSign selbst, dass 30’967 Sponsor-Validated-S/MIME-Zertifikate von der CPR

abwichen, weil ein Kommentar zu `Key Usage` die Kombination aller vier Key-Usage-Bits nicht korrekt abbildete; SwissSign behandelte dies als Misissuance, widerrief die betroffenen Zertifikate innert funf Tagen und fuhrte anschliessend die Automatisierung von CPR und CA-Konfiguration aus einer gemeinsamen Quelle als Abhilfemassnahme ein. Dieser Vergleich ist wichtig, weil er zeigt, dass SwissSign schon fruher eine eher strikte Lesart von Dokument-/Profilabweichungen vertreten hat. [46]

Der gegensatzliche Vergleichsfall ist der Entrust-TLS-Vorfall 2024 um einen typographischen CPS-Fehler. Dort betraf die Fehlstelle 6’008 OV-TLS-Zertifikate; Entrust hielt fest, die Zertifikate seien technisch entsprechend den TLS BR und dem intendierten Profil ausgestellt worden und wurden bei Neuausstellung identisch aussehen. Entrust entschied sich deshalb zunachst gegen den Widerruf und argumentierte spater zusatzlich, man habe die Lage wohl anfangs zu streng als Misissuance charakterisiert, weil die CPS insgesamt die BR priorisiere. Fur den hiesigen SwissSign-Fall bedeutet das nicht, dass Entrust recht hatte; es zeigt aber, dass das Verhaltnis zwischen BR-Konformitat, CP/CPS-Fehler und Widerrufspflicht im Oekosystem tatsachlich umstritten ist. [47]

Noch deutlicher wird der Streit in der Roundtable-Diskussion 2025 im Root-Store-Umfeld. Dort wurde offen benannt, dass ein gutglaubiger, trivialer CPS-Fehler dazu fuhren kann, dass hundert Prozent der betroffenen Zertifikate widerrufen und in identischer Form neu ausgestellt werden mussen. Gleichzeitig wurde darauf hingewiesen, dass dies Anreize schaffe, CP/CPS absichtlich vage zu halten. Diese Diskussion ist fur die Verhaltnismassigkeitsfrage fast exemplarisch: Sie bestatigt, dass das Problem nicht nur individuell empfunden wird, sondern auch innerhalb der Governance-Community selbst als echtes Strukturproblem erkannt ist. [48]

Offene Punkte und Beleglucken

Erstens liegt fur den aktuellen SwissSign-Silver-Fall bisher nur ein Preliminary Incident Report vor. Ein Full Incident Report mit ausgearbeiteter Timeline, expliziter Root Cause Analysis, Zertifikatszahlen, Action Items und Closure-Prozess ist bisher offentlich nicht verfugbar. [49]

Zweitens fehlt offentlich zugangliches Primarmaterial zu konkreten betroffenen End-Entity-Zertifikaten, mit dem sich SwissSigns Behauptung der materiellen BR-Konformitat unabhangig verifizieren liesse. Der derzeitige Stand ist daher: starke Plausibilitat, aber keine vollstandige Drittverifikation. [50]

Drittens ist offen, ob SwissSign nach der CPR-Korrektur auch die CP fur Mailbox-Validated/LCP inhaltlich bereinigen wird. Per 22. April 2026 ist sie weiterhin in einer Fassung offentlich, deren Wortlaut fur MV nur schwer mit den S/MIME BR zusammengeht. [51]

Viertens gibt es bislang keine offentliche, substantive Stellungnahme eines Root-Store-Akteurs zu genau diesem SwissSign-Fall, die uber die reine Entgegennahme des Preliminary Reports hinausgeht. Daher bleibt offen, ob SwissSigns konservative Widerrufslesart später bestatigt, relativiert oder kritisiert wird. [52]

Schlussurteil

Nach dem derzeit offentlich zuganglichen Material ist der SwissSign-/S/MIME-Silver-Vorfall 2026 in erster Linie ein Compliance- und Governance-Vorfall der Public PKI. Gesichert ist, dass die offentliche CPR das Mailbox-Validated-Multipurpose-Profil beim `commonName` falsch oder jedenfalls BR-widrig beschrieb. Ebenso gesichert ist, dass SwissSign selbst die real ausgestellten Zertifikate nach einer Stichprobe fur materiell BR-konform hielt und die CPR noch am 17. April 2026 mit einem klarstellenden

Hinweis versah. Daraus folgt, dass der offentliche Stand **eher** fur einen Dokumentations- als fur einen Leaf-Profilfehler spricht. [53]

Das Wort „bloss“ wurde ich dennoch vermeiden. In der Public PKI sind CP/CPS/CPR nicht Dekoration, sondern bindende, historisierte und auditierte Vertrauensdokumente. Wenn sie mit der Realitat der Issuance kollidieren, ist das kein folgenloser Schreibfehler, sondern ein echter Governance-Defekt. Zudem deuten die weiterhin offentlichen Formulierungen der MV/LCP-CP darauf hin, dass das Dokumentationsproblem wohl breiter war als nur ein einzelner CPR-Satz. Insofern ist die These „nur ein Dokumentationsfehler“ zwar im Materialkern plausibel, aber in ihrer Verengung irrefuhrend. [54]

Zur Verhaltnismassigkeit ist mein Urteil zweistufig. **Unter dem geltenden Regime** war der Massenwiderruf fur SwissSign eine nachvollziehbare, regeltextnahe und root-store-politisch vorsichtige Reaktion. **In materieller Sicherheitsbetrachtung** erscheint er dagegen nur begrenzt verhältnismassig, sofern die Leaf-Zertifikate tatsachlich bereits BR-konform waren und lediglich identisch neu ausgestellt werden mussten. Der Governance-Gewinn ist real; der kryptografische Sicherheitsgewinn dagegen gering. Die Hauptlast tragen Kunden und Betreiber. [55]

Die Grundsatzkritik am „strukturell kaputten PKI-System“ trifft also nicht den kryptografischen Kern, wohl aber einen empfindlichen Nerv der Public-PKI-Architektur. Das Problem liegt weniger in RSA oder X.509 als in der Kombination aus globaler Root-Store-Governance, starren Revokationsmechanismen, harschen Bright-Line-Regeln und unzureichend abgestuften Remediationsmodellen fur sicherheitsneutrale Dokumentationsfehler. Kurze Laufzeiten heilen dieses Problem nicht; sie mindern bloss die Dauer und Zahl gleichzeitig wirksamer Zertifikate. Wer daraus folgert, Laufzeitverkurzungen seien generell nutzlos, geht zu weit. Wer daraus folgert, die Public PKI leide an ernsthaften Governance- und Betriebsdefekten, liegt hingegen im Kern richtig. [56]

Mein zusammenfassendes Schlussurteil lautet daher: **Der Vorfall ist am ehesten als dokumentarisch-governancebezogene Misalignment-Misissuance ohne bisher nachgewiesene materielle Leaf-Fehlprofilierung einzuordnen. Der Massenwiderruf war aus Sicht des heutigen Regelwerks defensibel, aus Sicht des Sicherheitsnutzens jedoch nur eingeschrankt verhaltnismassig. Die eigentliche Lehre ist nicht, dass Public PKI kryptografisch versagt, sondern dass ihre Audit-, Dokumentations- und Sanktionslogik fur geringfugige, sicherheitsneutrale Abweichungen noch immer zu grob granuliert ist.** [57]

---

[1] [5] [24] [51] https://repository.swisssign.com/SwissSign_CP_LCP.pdf
https://repository.swisssign.com/SwissSign_CP_LCP.pdf

[2] [3] [19] [30] [37] [43] [44] [45] [54] https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

[4] [8] [11] [12] [28] [29] [36] [41] [49] [50] [52] [53] [57] https://bugzilla.mozilla.org/show_bug.cgi?id=2033000
https://bugzilla.mozilla.org/show_bug.cgi?id=2033000

[6] [13] [21] [25] [26] [27] [31] [35] [42] [55] https://cabforum.org/working-groups/smime/requirements/
https://cabforum.org/working-groups/smime/requirements/

[7] https://bugzilla.mozilla.org/rest/bug/2033000
https://bugzilla.mozilla.org/rest/bug/2033000

[9] [17] [23] [32] https://repository.swisssign.com/SwissSign_CPR_SMIME_R14.pdf
https://repository.swisssign.com/SwissSign_CPR_SMIME_R14.pdf

10 16 22 https://repository.swisssign.com/SwissSign_CPR_SMIME.pdf
https://repository.swisssign.com/SwissSign_CPR_SMIME.pdf

14 https://www.swisssign.com/en/certificate-webshop/email-id-silver.html
https://www.swisssign.com/en/certificate-webshop/email-id-silver.html

15 https://www.swisssign.com/support/faq/zertifikate
https://www.swisssign.com/support/faq/zertifikate

18 38 https://www.nospamproxy.de/de/swisssign-widerruft-smime-zertifikate-was-nospamproxy-kunden-jetzt-wissen-muessen/
https://www.nospamproxy.de/de/swisssign-widerruft-smime-zertifikate-was-nospamproxy-kunden-jetzt-wissen-muessen/

20 34 40 https://www.ccadb.org/cas/incident-report
https://www.ccadb.org/cas/incident-report

33 https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf
https://repository.swisssign.com/SwissSign_CPS_SMIME.pdf

39 https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/TqTpdOtOxfs
https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/TqTpdOtOxfs

46 https://bugzilla.mozilla.org/show_bug.cgi?id=1929189
https://bugzilla.mozilla.org/show_bug.cgi?id=1929189

47 https://bugzilla.mozilla.org/show_bug.cgi?id=1890896
https://bugzilla.mozilla.org/show_bug.cgi?id=1890896

48 https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/TqTpdOtOxfs/m/1RgDbNfKAQAJ
https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/TqTpdOtOxfs/m/1RgDbNfKAQAJ

56 https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/
https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/