

SECURITY & COMPLIANCE

Windows: Außerplanmäßige Updates nach Kompromittierung eMudhra-Zwischenzertifizierungsstellen

Executive Summary

Stell dir vor, der Hausmeister verliert den Generalschlüssel nicht etwa – er graviert ihn gleich in die Glastür, damit jeder Besucher ihn nachfeilen kann. Ungefähr so ist es bei eMudhra gelaufen. Der indische Zertifikatsanbieter hat am 30. April 2025 acht Zwischenzertifizierungsstellen erzeugt, deren private Schlüssel sich aus dem öffentlichen Zertifikat zurückrechnen lassen. Kein Hack, kein Insider, keine Nordkorea-Romantik: Die geheimen Werte waren schlicht kleiner als 256. Einer davon war die Zahl 4. Nicht vier Kilobyte. Vier.

Wer diese Schlüssel hat, kann Website-Zertifikate ausstellen oder Software signieren, denen Windows vertraut hätte. Sechs der acht Stellen waren für TLS gedacht, zwei für Code-Signing. Microsoft reagiert laut Microsoft-Ankündigung MC1526780 und dem zugehörigen MSRC-Blogbeitrag in drei Stufen: Seit dem 20. Oktober 2026 blockiert die Windows-Sperrliste die acht Zwischenstellen. Am 26. Oktober kamen außerplanmäßige Windows-Updates, die sieben Zertifikate aus der Windows-Vertrauensliste werfen – sechs eMudhra-G3-Wurzeln und ein Cross-Zertifikat unter Sectigos „AAA Certificate Services“. Ab heute, dem 27. Oktober, verschwinden dieselben sieben auch aus der Edge-Vertrauensliste.

Für dich heißt das: Auf verbundenen Geräten passiert das meiste automatisch. Gefährlich wird es dort, wo „automatisch“ seit Jahren ausgeschaltet ist – in Produktionsnetzen, Laboren, Kassensystemen, Behördennetzen und jeder VM, die seit dem letzten Golden Image niemand mehr angefasst hat.

Fakten: Das Wichtigste auf einen Blick

- **Was:** Acht eMudhra-Zwischenstellen mit trivial berechenbaren Schlüsseln, sechs TLS, zwei Code-Signing.
- **Microsoft-Reaktion:** Sperrliste seit 20.10., Out-of-Band-Updates seit 26.10., Edge-Bereinigung ab 27.10.2026.
- **Wer handeln muss:** Admins von getrennten Geräten oder Geräten mit abgeschalteten Zertifikats-Updates – sofort.
- **Kosten:** keine, kein Lizenzthema. Beahlt wird nur mit Arbeitszeit, und zwar mit deiner.

Worum geht es im Detail?

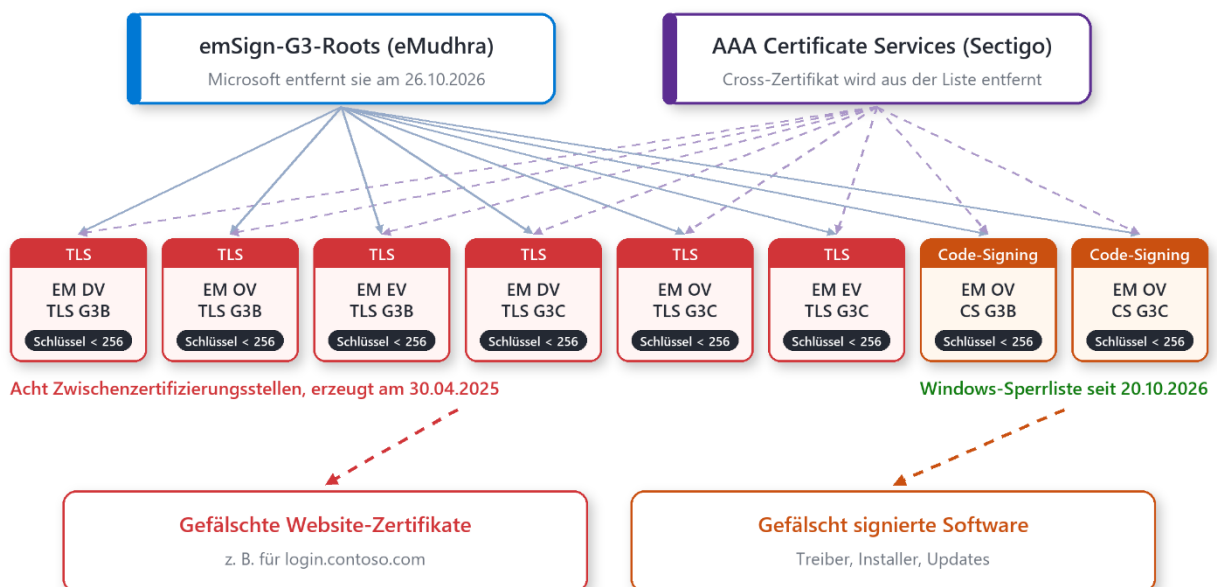
Damit du einordnen kannst, wie ernst das ist, ein kurzer Ausflug in die Vertrauenskette. Dein Browser vertraut einer Website nicht, weil sie nett aussieht, sondern weil ihr Zertifikat von einer Zwischenstelle unterschrieben ist, die wiederum von einer Wurzelzertifizierungsstelle unterschrieben ist. Diese Wurzeln liefert Microsoft über das Trusted Root Program aus. Windows

bringt nur einen Teil davon ab Werk mit und lädt den Rest bei Bedarf als Vertrauensliste (Certificate Trust List, CTL) von `ctldl.windowsupdate.com` nach. Daneben gibt es eine zweite, oft vergessene Liste: die Sperrliste mit ausdrücklich nicht vertrauenswürdigen Zertifikaten. Beide aktualisiert Windows standardmäßig selbständig – auf Geräten mit Internetzugang täglich.

Die eMudhra-Panne sitzt genau in der Mitte dieser Kette. Die acht Zwischenstellen nutzen elliptische Kurven vom Typ P-384. Ein geheimer Wert unter 256 bedeutet: Ein Angreifer probiert 255 Kandidaten durch und ist fertig, bevor der Kaffee durchgelaufen ist. Nach vorläufiger Erklärung von eMudhra hat ein Fehler im Skript der Key-Ceremony neben dem starken Schlüsselpaar ein zweites, schwaches erzeugt, und weil die Bezeichnungen ähnlich aussahen, landete das falsche in den Zertifikatsanträgen. Ein Buchstabe Unterschied im Label, und die Kryptografie eines ganzen Hierarchiezweigs ist Makulatur. Wer schon einmal „prod“ und „prd“ verwechselt hat, fühlt mit.

Pikant: Etwa einen Monat nach der Erzeugung hat Sectigo alle acht Zwischenstellen unter der eigenen Wurzel „AAA Certificate Services“ gegengezeichnet. Damit hing jeder schwache Schlüssel an zwei Vertrauensankern. Siebzehn Monate lang fiel es niemandem auf. Am 17. Oktober 2026 meldete ein Sicherheitsforscher den Fund an die Root-Programme der Browser – stilecht mit einer Nachricht, die er mit allen acht Schlüsseln signiert hatte. eMudhra und Sectigo widerriefen die Zertifikate am 18. und 19. Oktober. Am 22. Oktober beschloss der eMudhra-Vorstand, sich aus dem weltweiten TLS-Zertifikatsgeschäft zurückzuziehen. Konsequenz kann man das nennen. Oder Notbremse.

Wo die Kette gerissen ist: die eMudhra-G3-Hierarchie



Durchgezogen: Ausstellung durch eMudhra · Gestrichelt oben: Cross-Signatur durch Sectigo · Gestrichelt unten: theoretischer Missbrauch

Jeder, der das öffentliche Zertifikat kennt, kann den privaten Schlüssel in Sekundenbruchteilen ausprobieren.

Wurzeln selbst nicht kompromittiert, aber Träger des Vertrauens – deshalb fliegen sie trotzdem raus.

Abbildung 1: Acht schwache Zwischenstellen, zwei Vertrauensanker – und zwei Missbrauchswege.

Die gute Nachricht: Google hat in den Certificate-Transparency-Logs kein Zertifikat gefunden, das an diesen Zwischenstellen hängt, und eMudhra gibt an, darüber keine Kundenzertifikate ausgestellt zu haben. Die schlechte Nachricht: Code-Signing-Zertifikate landen nicht in CT-Logs. Ob irgendwo eine Software kursiert, die mit einem dieser Schlüssel signiert wurde, kann niemand

vollständig prüfen. Der MSRC-Blog stellt außerdem klar, dass Microsofts eigene Systeme nicht kompromittiert wurden und die Untersuchung noch läuft.

Vom Schlüsselfehler zum Notfall-Update: 18 Monate in sieben Schritten

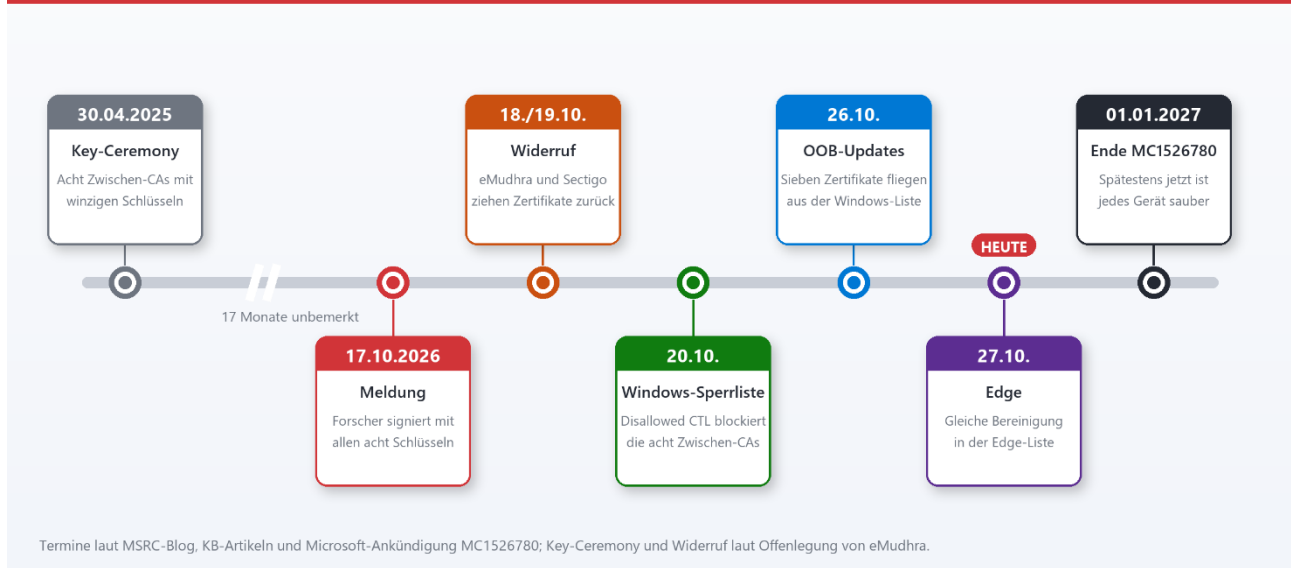


Abbildung 2: Der Weg von der fehlerhaften Key-Ceremony bis zum Ende des Meldezeitraums.

Microsoft unterscheidet dabei bewusst zwei Ebenen. Das Blockieren der acht Zwischenschlüssel über die Sperrliste ist die chirurgische Maßnahme. Das Entfernen der Wurzeln aus der Vertrauensliste ist eine breitere Vertrauensentscheidung: Alles, was an den G3-Wurzeln hängt, verliert in Windows und Edge sein Vertrauen – auch völlig harmlose Zertifikate. Über die übrigen eMudhra-Wurzeln entscheidet Microsoft separat und will weitere Schritte erst setzen, wenn betroffene Kunden umgezogen sind. Für Edge und WebView2 kommt zusätzlich ein CRLSet über den Komponenten-Updater, der die betroffenen TLS-Zertifikate blockiert, ohne dass eine neue Browserversion nötig ist.

Die Out-of-Band-Pakete stehen laut den KB-Artikeln ausschließlich im Microsoft Update-Katalog. Windows Update und WSUS bieten sie nicht von selbst an. Das ist kein Versehen: Die Pakete sind für Geräte gedacht, die keine aktuellen CTL-Updates bekommen. Sie sind kumulativ, als „nicht sicherheitsrelevant“ eingestuft und enthalten das Oktober-Update vom 13.10.2026.

Betriebssystem	Paket	Hinweis
Windows 11, Version 26H1	KB5134134	Nur Update-Katalog
Windows 11, Versionen 24H2, 25H2, 26H2	KB5134133	Builds 26100/26200/26300.9725; Prüfpunkt-Update KB5043080 vorher nötig
Windows 11, Version 23H2	KB5134130	Nur Update-Katalog
Windows Server 2025	KB5134137	Nur Update-Katalog
Windows Server 2022	KB5134140	Build 20348.5773; aktuelles SSU KB5126654 vorausgesetzt
Windows 10 22H2 und Enterprise LTSC 2021	KB5134125	Nur Update-Katalog
Windows 10 Enterprise LTSC 2019 und Server 2019	KB5134124	Nur Update-Katalog

Betriebssystem	Paket	Hinweis
Windows Server 2016	KB5134123	Nur Update-Katalog

Wichtig: Hotpatch-Geräte verlieren den Hotpatch-Takt

Laut KB-Artikel zu KB5134133 erhalten Windows-11-Geräte im Hotpatch-Verfahren nach der Installation dieses Pakets keine Hotpatches mehr, bis sie das Baseline-Update vom Januar 2027 installiert haben. Wer Hotpatch nutzt und online ist, braucht das Paket gar nicht – die automatische CTL-Aktualisierung reicht. Also: Finger weg, wenn du es nicht brauchst.

Und jetzt der Teil, der dich als Admin interessiert: Die Aktualisierung der Vertrauens- und Sperrliste ist standardmäßig aktiv. Ohne Registry-Eintrag gilt beides als eingeschaltet. Abschalten lässt sie sich über die Gruppenrichtlinie „Turn off Automatic Root Certificates Update“ unter Computerkonfiguration, Administrative Vorlagen, System, Internetkommunikationsverwaltung, Internetkommunikationseinstellungen – oder direkt über die Registry-Werte DisableRootAutoUpdate (1 = aus) und EnableDisallowedCertAutoUpdate (0 = aus) unter HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot. Mit RootDirURL unter HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate leitest du den Abruf auf eine interne Freigabe um. Bei Edge ist es die Richtlinie ComponentUpdatesEnabled: Steht sie auf 0, kommt auch kein CRLSet an. Die Details beschreibt Microsoft im Learn-Artikel [Konfigurieren vertrauenswürdiger Stammzertifikate und unzulässiger Zertifikate](#).

Wie die neue Vertrauensliste auf deine Geräte kommt

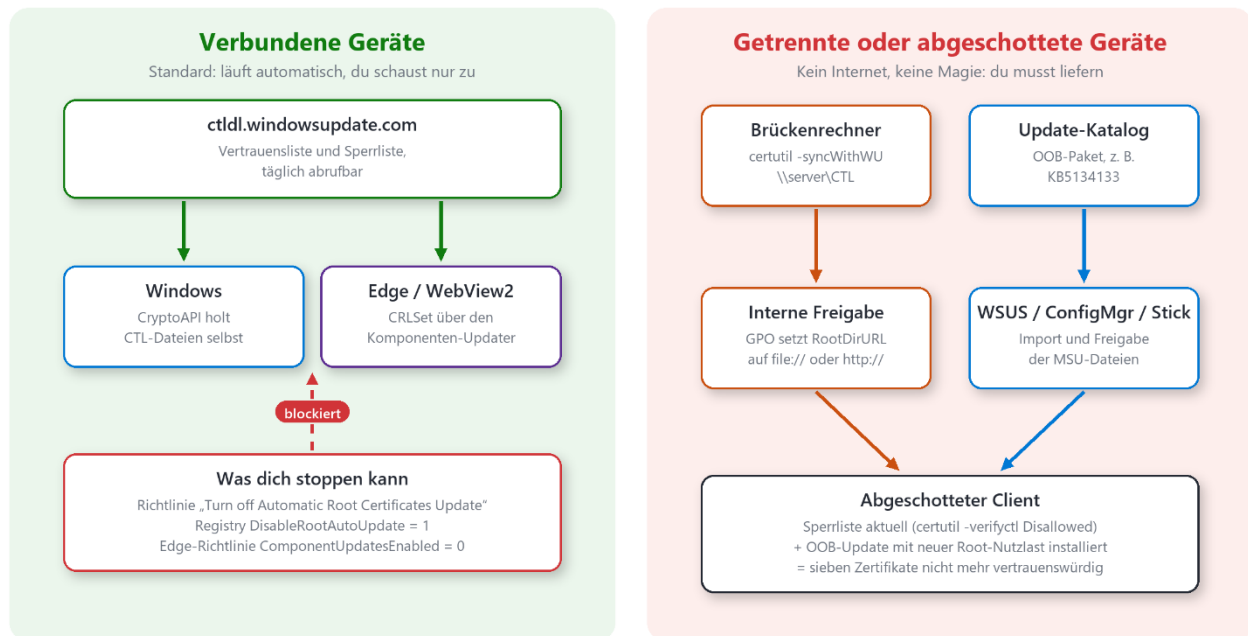


Abbildung 3: Verbundene Geräte erledigen das selbst – getrennte Geräte brauchen einen Brückenrechner oder das Katalogpaket.

Was sind Chancen? Was sind Risiken?

Klingt komisch, aber so ein Vorfall hat auch sein Gutes. Er ist ein kostenloser Penetrationstest deines Update-Prozesses, und die Rechnung bekommst du nur, wenn du durchfällst. Jede

Organisation, die heute nicht in einer Stunde sagen kann, auf welchen Geräten die Sperrliste vom 20. Oktober angekommen ist, hat gerade etwas Wichtiges über sich gelernt.

Chancen	Risiken
Kostenloser Realitätstest für Zertifikats- und Update-Prozesse in abgeschotteten Netzen	Gefälschte, aber gültig wirkende TLS-Zertifikate auf Geräten mit veralteter Sperrliste – ideal für Man-in-the-Middle
Anlass, ein Inventar aller internen und externen Zertifikatsketten aufzubauen	Mit eMudhra-Schlüsseln signierte Software lässt sich nicht über CT-Logs aufspüren
Bereinigung von Altlasten: verwaiste Golden Images, vergessene VMs, abgeschaltete Richtlinien	Legitime Dienste mit eMudhra-G3-Kette brechen ab 26.10. in Windows und Edge
Argument für Budget: Zertifikats-Monitoring ist plötzlich kein „nice to have“ mehr	Hotpatch-Unterbrechung, wenn das OOB-Paket unnötig auf verbundene Geräte verteilt wird

Das größte reale Risiko ist nicht der Hackerangriff von morgen früh, sondern die stille Lücke. Ein Kunde aus dem Maschinenbau hatte vor zwei Jahren die automatische Root-Aktualisierung in der Fertigung abgeschaltet, „weil die Firewall-Logs so voll waren“. Dokumentiert war das nirgends. Der Admin von damals arbeitet inzwischen bei einem Wettbewerber, die GPO hieß „Test_neu_final2“. Solche Geräte sehen gefälschte Zertifikate als gültig an, bis jemand sie manuell versorgt. Und weil diese Richtlinie die Registry tätowiert, bleibt sie auch dann wirksam, wenn die GPO längst gelöscht ist.

Für deutsche Organisationen kommt die Compliance-Seite hinzu. Ein erfolgreicher Man-in-the-Middle-Angriff mit einem gefälschten Zertifikat ist eine Verletzung der Vertraulichkeit im Sinne von Art. 32 DSGVO und schnell ein meldepflichtiger Vorfall nach Art. 33 – mit 72-Stunden-Uhr. Für öffentliche Auftraggeber zählen zusätzlich die BSI-Mindeststandards und, wo vorhanden, die Vorgaben für Netze mit Verschlusssachen. Gerade VS-NfD-Netze sind oft physisch getrennt und damit exakt die Zielgruppe dieser Meldung. Die Mitbestimmung bleibt dagegen entspannt: Zertifikatslisten erfassen kein Verhalten der Belegschaft, ein Fall für den Betriebs- oder Personalrat ist das nicht. Lizenzkosten fallen nicht an.

Warnung: Lokales Vertrauen ist der Notausgang mit Selbstschussanlage

Microsoft erlaubt ausdrücklich, ein Zertifikat lokal wieder als vertrauenswürdig einzutragen – aber nur nach eigener Sicherheitsbewertung. Übersetzt: Wer die eMudhra-G3-Wurzel per GPO zurück in den Stammzertifikatsspeicher importiert, weil „die Fachanwendung sonst nicht geht“, erklärt einen Schlüssel für vertrauenswürdig, den jeder Praktikant mit Taschenrechner nachbauen kann. Das ist kein Workaround, das ist eine Einladung mit Wegbeschreibung.

Was müssen wir jetzt schon vorbereiten?

Gute Nachricht für alle Freunde des geregelten Feierabends: Für die meisten verbundenen Clients reicht Prüfen statt Handeln. Schlechte Nachricht: Prüfen musst du trotzdem. Der Plan unten ist nach Dringlichkeit sortiert und orientiert sich am Meldezeitraum von MC1526780, der am 1. Januar 2027 endet.

Wann	Was	Wer
Heute, 27.10.2026	Prüfen, ob die automatische CTL-Aktualisierung irgendwo per GPO, Intune-Konfigurationsprofil oder Registry abgeschaltet ist; Edge-Richtlinie ComponentUpdatesEnabled kontrollieren	Client- und Server-Admins
Bis 31.10.2026	Stichproben mit <code>certutil -verifyctl Disallowed findstr /i lastsynctime</code> auf je einem Gerät pro Netzsegment; Datum muss nach dem 20.10. liegen	Admins
Bis 31.10.2026	Getrennte Netze versorgen: Brückenrechner mit <code>certutil -syncWithWU \\server\CTL</code> , Freigabe per <code>RootDirURL</code> verteilen, OOB-Paket aus dem Katalog einspielen	Admins, OT-Verantwortliche
Bis 15.11.2026	Inventar aller Zertifikate, die an den sieben entfernten Zertifikaten hängen; Ersatz oder alternative Kette besorgen	PKI-Team, Fachbereiche
Bis 30.11.2026	Golden Images, VM-Vorlagen und Azure-Images aktualisieren; für Scale Sets und Einzel-VMs die aktualisierten Marketplace-Images nutzen	Infrastruktur
Bis 01.01.2027	Abschlussbericht an IT-Leitung und Datenschutz; Abschaltungen der CTL-Aktualisierung dokumentieren oder rückbauen	IT-Leitung, Datenschutz

Für das Inventar genügt für den Anfang ein PowerShell-Einzeiler pro Gerät: `Get-ChildItem Cert:\LocalMachine -Recurse | Where-Object Issuer -match 'emSign|eMudhra'`. Spannender sind die Zertifikate, die nicht bei dir liegen, sondern bei Partnern: Schnittstellen zu Dienstleistern, Behördenportale, Zahlungsanbieter mit Indien-Bezug. Frag aktiv nach, statt am Montagmorgen von einem Verbindungsabbruch überrascht zu werden.

Tipp: Nur die Sperrliste automatisch, die Vertrauensliste unter Kontrolle

Microsoft beschreibt ein unabhängiges Opt-in: Du kannst die Sperrliste automatisch aktualisieren lassen und die Vertrauensliste selbst steuern. Wer aus Compliance-Gründen keine automatische Root-Erweiterung will, schaltet damit wenigstens die Sperrungen nicht mit ab. Das ist genau die Einstellung, die in diesem Vorfall den Unterschied macht.

Wichtig: GPO löschen heißt nicht Einstellung löschen

Die Richtlinien für `DisableRootAutoUpdate`, `EnableDisallowedCertAutoUpdate` und `RootDirURL` werden nicht zurückgesetzt, wenn du die GPO entfernst oder die Verknüpfung löst. Du musst sie aktiv umkehren – per GPO oder direkt in der Registry. Wer das vergisst, sucht in drei Jahren wieder.

Bleibt die Kommunikation an die Belegschaft. Eine kurze Mitteilung reicht: Zertifikatswarnungen im Browser werden nicht weggeklickt, sondern gemeldet. Ja, das wissen eigentlich alle. Und ja, gefühlt die Hälfte klickt trotzdem auf „Weiter zur Website (nicht empfohlen)“, weil das Wort „empfohlen“ in einer IT-Meldung offenbar als Mutprobe gelesen wird. Für den Helpdesk lohnt eine Sprachregelung: Wenn ab dieser Woche ein bisher funktionierender Dienst mit Zertifikatsfehler ausfällt, ist das kein Windows-Fehler, sondern die gewollte Wirkung – Ticket an das PKI-Team, nicht an Microsoft.

Häufig gestellte Fragen

Muss ich die Out-of-Band-Updates von Oktober 2026 auf allen Windows-Geräten installieren?

Nein. Geräte mit Internetzugang und aktiver automatischer Aktualisierung der Zertifikatslisten erhalten die Änderungen über Windows Update ohnehin. Die Pakete aus dem Microsoft Update-Katalog sind für getrennte Geräte und Geräte gedacht, auf denen diese Aktualisierung abgeschaltet ist.

Wie prüfe ich, ob ein Windows-Gerät die aktuelle Sperrliste für Zertifikate hat?

Führe in einer Eingabeaufforderung mit Administratorrechten den Befehl `certutil -verifctl Disallowed` aus und filtere nach „lastsynctime“. Liegt das angezeigte Datum nach dem 20. Oktober 2026, enthält die Liste die Sperrung der acht eMudhra-Zwischenstellen.

Was passiert mit Websites, die ein eMudhra-Zertifikat verwenden?

Zertifikate, die an den entfernten eMudhra-G3-Wurzeln hängen, gelten in Windows und Edge nicht mehr als vertrauenswürdig, und Besucher sehen eine Zertifikatswarnung. Betreiber müssen ein neues Zertifikat über eine andere Kette oder einen anderen Anbieter beschaffen.

Darf ich ein entferntes eMudhra-Stammzertifikat per Gruppenrichtlinie wieder als vertrauenswürdig eintragen?

Technisch ja, Microsoft rät aber nur nach eigener Sicherheitsbewertung dazu. Weil die betroffenen Schlüssel öffentlich berechenbar sind, öffnet eine solche Ausnahme die Tür für gefälschte Zertifikate und sollte allenfalls zeitlich eng befristet und dokumentiert erfolgen.

Ist ein Windows-Gerät ohne Internetzugang automatisch sicher vor gefälschten Zertifikaten?

Nein, im Gegenteil: Ohne Verbindung erhält es weder die neue Sperrliste noch die bereinigte Vertrauensliste. Solche Geräte müssen über eine interne Freigabe mit den Zertifikatslisten oder über das Out-of-Band-Paket aus dem Update-Katalog versorgt werden.