

ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover

ADFS

Token-Signing-Zertifikat erneuern

mit und ohne AutoCertificateRollover – bevor der Stichtag deine Farm erledigt

boddenberg.de

Token-Signing
CN=ADFS Signing – sts.contoso.de

Not After

T - 20 T - 15 T - 0

WISSEN

Grundlagen, Architektur und alle Praxisbeiträge rund um ADFS an einem Ort.

> [Active Directory Federation Services](#)

BERATUNG

Rollover-Fahrplan, Inventur der Relying Parties und PKI-Zertifikate – gemeinsam geplant statt am Stichtag improvisiert.

> [Consulting zu ADFS](#)

SCHULUNG

Zertifikatswechsel an einer Laborfarm durchspielen, inklusive absichtlich vergessener Relying Party.

> [ADFS-Schulungen](#)

Es gibt Zertifikate, deren Ablauf niemand bemerkt, weil ein Dienst einfach weiterläuft. Und es gibt das Token-Signing-Zertifikat deiner ADFS-Farm. Das läuft einmal im Jahr ab, erneuert sich im Normalfall sogar selbst – und legt trotzdem regelmäßig ganze Anmeldelandschaften lahm. Nicht weil ADFS etwas falsch macht, sondern weil irgendwo eine SaaS-Anwendung, ein SharePoint oder eine Eigenentwicklung aus dem Jahr 2016 das alte Zertifikat fest eingetragen hat und von der Erneuerung schlicht nichts mitbekommt.

Das Tückische daran: Der Ausfall passiert meistens nicht am Ablaufdatum, das irgendwer irgendwann in einen Kalender eingetragen hat, sondern ein paar Tage früher. Dann nämlich, wenn ADFS das neue Zertifikat zum primären macht. Wer an diesem Morgen im Service Desk sitzt, erlebt einen jener Tage, an denen Kaffee nicht mehr als Getränk, sondern als Überlebensstrategie gilt.

In diesem Beitrag geht es genau um diesen einen Handgriff: das ADFS Token-Signing-Zertifikat erneuern. Einmal mit AutoCertificateRollover, der Automatik, die in jeder neuen Farm eingeschaltet ist – mit ihren Zeitpunkten, dem sekundären Zertifikat und der Promotion. Und einmal ohne Automatik, mit einem Zertifikat aus deiner eigenen PKI. Dazu kommt die Frage, die in den meisten Anleitungen fehlt: Wer muss eigentlich Bescheid wissen, bevor du auf „Als primär festlegen“ klickst? Die Grundlagen zu Farm, Rollen und Vertrauensstellungen setze ich voraus; die findest du auf der Übersichtsseite [Active Directory Federation Services](#).

FAKTEN – Token-Signing-Zertifikat in drei Sätzen

Mit dem privaten Schlüssel dieses Zertifikats signiert ADFS jedes Token, das es ausstellt – SAML-Assertions, WS-Federation-Token, ID-Token und Access-Token.

Jede Relying Party prüft diese Signatur mit dem öffentlichen Schlüssel, den sie von dir kennt. Kennt sie den falschen, ist die Anmeldung ungültig, egal wie korrekt Benutzer, Kennwort und MFA waren.

Das Zertifikat hat mit dem SSL-Zertifikat für sts.contoso.de nichts zu tun. Wer die beiden

verwechselt, tauscht am Stichtag mit viel Aufwand das falsche aus.

Falls du gerade eher das Webserver-Zertifikat erneuern musst, bist du hier falsch abgebogen: Das behandelt [SSL-Zertifikat auf ADFS und Web Application Proxy tauschen](#). Hier geht es um die Signatur – und die ist ungleich gnadenloser.

Warum dieses eine Zertifikat Farmen am Stichtag umbringt

Ein abgelaufenes SSL-Zertifikat erzeugt eine hässliche Browserwarnung, und jeder sieht sofort, was los ist. Ein neues Token-Signing-Zertifikat erzeugt dagegen gar nichts – auf deiner Seite. ADFS zeigt die Anmeldeseite, der Benutzer meldet sich an, MFA klappt, ADFS stellt ein Token aus. Erst die Anwendung sagt dann: „Signatur ungültig“, „Invalid SAML response“ oder zeigt einfach eine generische Fehlerseite. Im ADFS-Protokoll steht häufig nicht einmal ein Fehler, denn aus Sicht von ADFS ist alles perfekt gelaufen.

Deshalb landen solche Tickets zuerst bei den Anwendungsverantwortlichen, dann beim Netzwerk, dann bei der Firewall und erst am Nachmittag bei dir. Bis dahin hat das halbe Haus eine Theorie, und keine davon lautet „ADFS hat planmäßig sein Signaturzertifikat gewechselt“.

Wer mit dem Zertifikat etwas anfangen muss

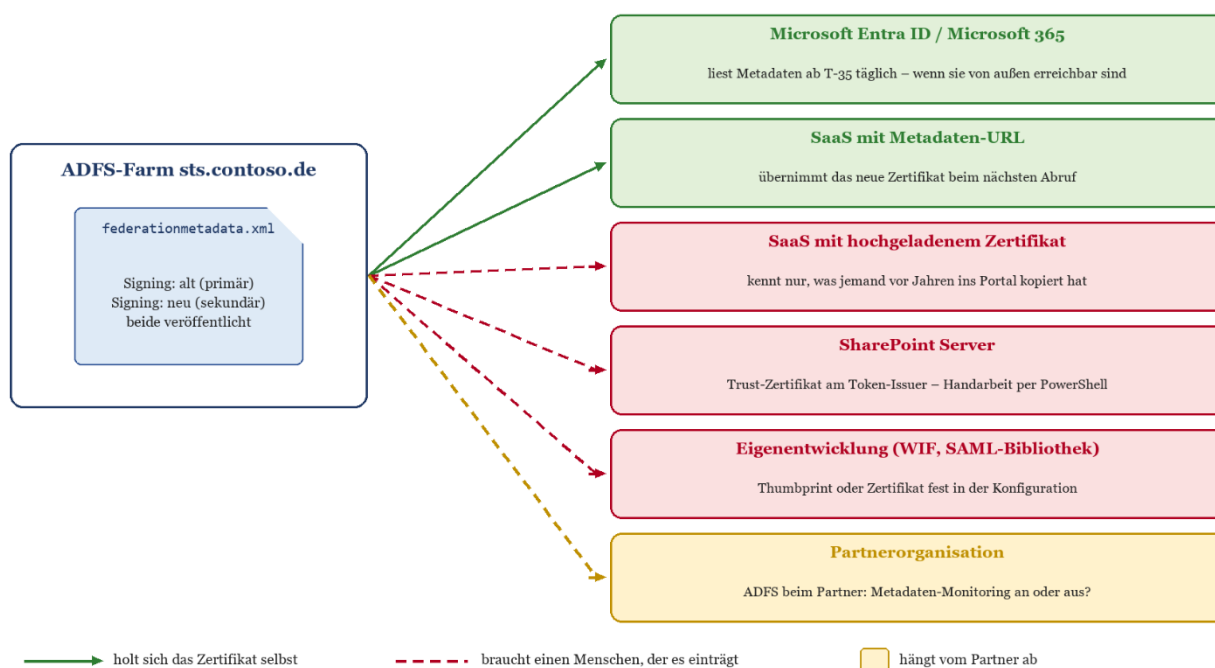
Jede Vertrauensstellung, in der ADFS Token ausstellt, hängt am Token-Signing-Zertifikat. Für die Frage, ob ein Rollover schiefgeht, zählt nur ein Merkmal: Holt sich die Gegenseite dein neues Zertifikat selbst aus den Federation-Metadaten, oder hat jemand es einmal von Hand eingetragen?

Relying Party	Wie sie dein Zertifikat kennt	Was beim Rollover passiert
Microsoft Entra ID / Microsoft 365	Federation-Einstellungen der Domäne, automatisch per Metadaten-Abruf gepflegt	läuft, wenn die Metadaten von außen erreichbar sind; sonst Handarbeit
SaaS mit Metadaten-URL	fragt federationmetadata.xml regelmäßig ab	übernimmt das neue Zertifikat, sobald es in den Metadaten steht
SaaS mit hochgeladenem Zertifikat	jemand hat eine .cer-Datei ins Admin-Portal geladen	scheitert ab der Promotion
SharePoint Server	Zertifikat am SPTrustedIdentityTokenIssuer	scheitert ab der Promotion, bis das SharePoint-Team nachzieht
Eigenentwicklung	Thumbprint oder Zertifikat in web.config oder Konfigurationsdatei	scheitert ab der Promotion
Partnerorganisation mit eigenem ADFS	Claims Provider Trust beim Partner, Monitoring an oder aus	hängt davon ab, ob der Partner deine Metadaten überwacht

Tabelle 1: Relying Parties nach der Frage sortiert, die am Stichtag zählt

Skizze 2: Wer das neue Zertifikat von allein bemerkt – und wer nicht

Ein Rollover, sechs Arten von Relying Parties, drei Ausgänge



Skizze 2: Grün holt sich das neue Zertifikat selbst, Rot braucht einen Menschen, Gelb hängt vom Partner ab.

Die roten Kästen sind das Problem. Sie sind in fast jeder Farm vorhanden, die länger als fünf Jahre läuft, und sie sind nirgends zentral dokumentiert. Die Anwendung wurde damals über ein Projekt angebunden, die Projektleitung ist längst in einem anderen Unternehmen, und im Admin-Portal der SaaS-Anwendung steht ein Zertifikat, das seit Jahren jemand still verlängert hat – oder eben nicht. Wie du Relying Parties sauber anlegst, sodass sie dir beim Rollover nicht auf die Füße fallen, zeigen [Relying Party Trust anlegen – per Metadaten und von Hand](#) und [SAML-Anwendung an ADFS anbinden – Praxisbeispiel SaaS](#).

WICHTIG – Auch das Token-Decrypting-Zertifikat rollt mit

AutoCertificateRollover erneuert Token-Signing und Token-Decrypting gemeinsam. Das Entschlüsselungszertifikat brauchen Partner, die dir verschlüsselte Token schicken – typischerweise Claims-Provider-Partner. Für sie gilt dieselbe Logik: Metadaten-Monitoring an, alles gut; statisch hinterlegt, Ärger. Wie du solche Partner anbindest, steht in [Claims Provider Trust – Partnerorganisationen anbinden](#).

AutoCertificateRollover: die Automatik und ihr Fahrplan

In jeder neu installierten ADFS-Farm ist AutoCertificateRollover eingeschaltet. ADFS erzeugt dann bei der Einrichtung selbstsignierte Zertifikate für Token-Signing und Token-Decrypting, legt sie verschlüsselt in der Konfigurationsdatenbank ab und kümmert sich vor dem Ablauf selbst um Nachfolger. Du musst nichts auf den einzelnen Knoten importieren, und kein Dienstkonto braucht Rechte auf einen privaten Schlüssel im Zertifikatsspeicher. Das ist tatsächlich bequem.

Ob die Automatik bei dir aktiv ist und mit welchen Werten sie arbeitet, zeigt ein einziger Befehl:

```
Get-AdfsProperties |
Format-List AutoCertificateRollover, Certificate*
```

```
Get-AdfsCertificate -CertificateType Token-Signing |
  Select-Object Thumbprint, IsPrimary,
    @{ n = 'NotBefore'; e = { $_.Certificate.NotBefore } },
    @{ n = 'NotAfter'; e = { $_.Certificate.NotAfter } }
```

Listing 1: Rollover-Einstellungen und aktuelle Signaturzertifikate auf einem ADFS-Knoten anzeigen

Die Schwellwerte – und was sie wirklich bedeuten

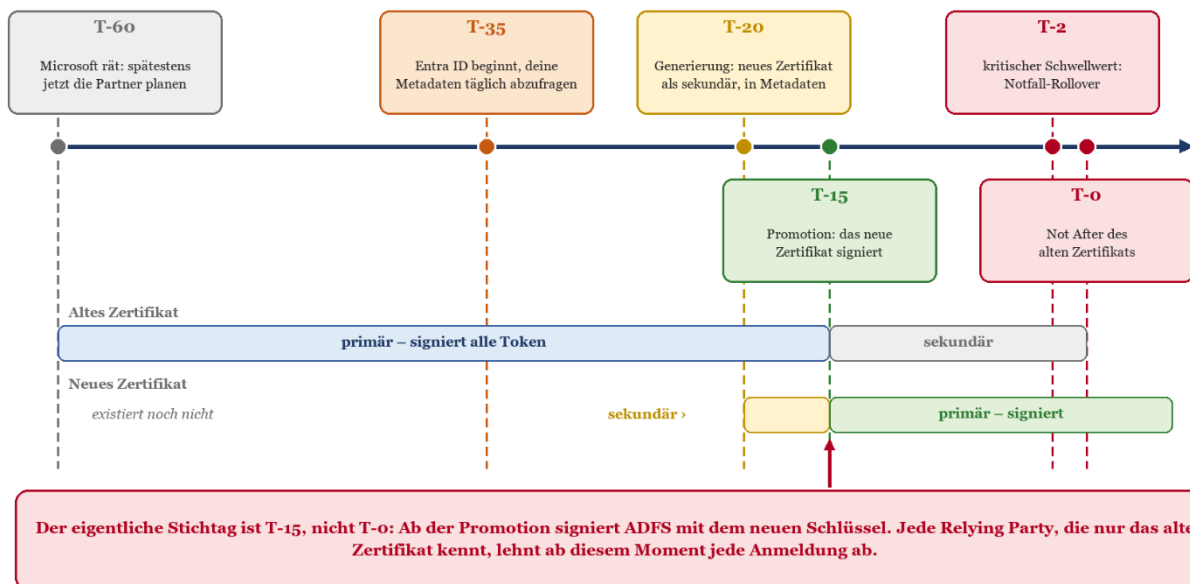
Eigenschaft	Typischer Wert	Bedeutung
AutoCertificateRollover	True	ADFS erzeugt und wechselt Signatur- und Entschlüsselungszertifikate selbst
CertificateGenerationThreshold	20 Tage	so viele Tage vor dem Not After des primären Zertifikats erzeugt ADFS den Nachfolger – als sekundäres Zertifikat
CertificatePromotionThreshold	5 Tage	so lange bleibt der Nachfolger sekundär, danach wird er primär und signiert
CertificateDuration	365 Tage	Laufzeit der selbst erzeugten Zertifikate
CertificateCriticalThreshold	2 Tage	Notbremse: Hat ADFS bis dahin keinen Nachfolger, erzeugt und aktiviert es sofort einen – ohne Vorlauf für Partner
CertificateRolloverInterval	720 Minuten	wie oft ADFS prüft, ob ein Schwellwert erreicht ist

Tabelle 2: Die Rollover-Eigenschaften aus Get-AdfsProperties mit den Werten, die man in frisch installierten Farmen typischerweise sieht

Rechne die Standardwerte einmal durch: 20 Tage vor Ablauf erscheint das neue Zertifikat, fünf Tage später wird es primär. Der tatsächliche Wechsel passiert also rund 15 Tage vor dem Ablaufdatum des alten Zertifikats. Wer sich nur das Ablaufdatum notiert hat, plant seinen Einsatz zwei Wochen zu spät.

Skizze 1: Der Fahrplan von AutoCertificateRollover

Standardwerte einer frisch installierten Farm – was deine Farm eingestellt hat, zeigt Get-AdfsProperties



Zwischen Generierung und Promotion liegen standardmäßig fünf Tage. Das ist die gesamte Vorwarnzeit für alle, die das neue Zertifikat von Hand eintragen müssen – falls ihnen überhaupt jemand Bescheid sagt.

Skizze 1: Der Rollover-Fahrplan mit Standardwerten. Der Ausfall für statische Relying Parties beginnt an der Promotion.

Das sekundäre Zertifikat: der Vorlauf, den keiner nutzt

Sobald ADFS den Nachfolger erzeugt, veröffentlicht es beide Zertifikate in den Federation-Metadaten unter `/federationmetadata/2007-06/federationmetadata.xml`. Signiert wird weiterhin mit dem alten. Diese Phase ist genau dafür gedacht, dass Partner das neue Zertifikat kennenlernen, bevor es gebraucht wird. Wer die Metadaten überwacht, trägt das neue Zertifikat zusätzlich ein und merkt von der Promotion anschließend nichts.

Mit Standardwerten dauert dieser Vorlauf fünf Tage. Fünf Tage, in denen jemand merken muss, dass ein neues Zertifikat existiert, die Anwendungsverantwortlichen informieren, deren Change-Verfahren anstoßen und das Zertifikat in jedem statischen Portal hinterlegen lassen muss. Wer schon einmal einen Change durch einen Änderungsausschuss gebracht hat, lacht an dieser Stelle – leise und ein bisschen verzweifelt.

Skizze 3: Primär, sekundär, Promotion – vier Phasen eines Rollovers

Was ADFS signiert, was in den Metadaten steht und was eine statische Relying Party davon hält



Metadaten-Konsumenten lernen das neue Zertifikat in Phase B kennen und merken von der Promotion nichts. Statische Relying Parties merken sie sofort – meistens über das Telefon des Service Desk.

Skizze 3: Die vier Phasen eines Rollovers aus Sicht von ADFS, Metadaten und einer statischen Relying Party.

Die Promotion – und wie du sie in die Hand nimmst

Wenn du weißt, dass es statische Relying Parties gibt, hast du zwei saubere Möglichkeiten, dir mehr Luft zu verschaffen. Die erste: Du verlängerst den Vorlauf dauerhaft, indem du die Schwellwerte anpasst. Mit einer Generierung 60 Tage vor Ablauf und einer Promotion 30 Tage danach steht das neue Zertifikat einen Monat lang in den Metadaten, bevor es signiert. Achte darauf, dass die Promotion deutlich vor dem kritischen Schwellwert liegt, sonst hebelst du den eigenen Plan aus.

```
# Vorlauf dauerhaft verlängern: 60 Tage vor Ablauf erzeugen, 30 Tage später promoten
Set-AdfsProperties -CertificateGenerationThreshold 60 -CertificatePromotionThreshold 30

# Nachfolger sofort erzeugen (landet als sekundäres Zertifikat)
Update-AdfsCertificate -CertificateType Token-Signing
```

Listing 2: Schwellwerte anpassen und bei Bedarf den Nachfolger gezielt vorziehen

Die zweite Möglichkeit ist situativ: Sobald der Nachfolger existiert, schaltest du `AutoCertificateRollover` vorübergehend aus. Damit hält ADFS die Promotion an, und du setzt das

neue Zertifikat selbst zum Wunschtermin primär – etwa im Wartungsfenster, wenn das SharePoint-Team und die Verantwortlichen der statischen SaaS-Anwendungen bereitstehen. Danach schaltest du die Automatik wieder ein. Das Wieder-Einschalten ist der Teil, den man gern vergisst, und dann läuft die Farm im nächsten Jahr ohne Automatik auf den Stichtag zu.

```
# 1. Automatik anhalten, nachdem der Nachfolger erzeugt wurde
Set-AdfsProperties -AutoCertificateRollover $false

# 2. Im Wartungsfenster: Nachfolger zum primären Zertifikat machen
$neu = Get-AdfsCertificate -CertificateType Token-Signing |
    Where-Object { -not $_.IsPrimary }
Set-AdfsCertificate -CertificateType Token-Signing -Thumbprint $neu.Thumbprint -IsPrimary

# 3. Automatik wieder einschalten – und das Ticket erst danach schließen
Set-AdfsProperties -AutoCertificateRollover $true
```

Listing 3: Promotion anhalten und zum eigenen Termin durchführen (auf dem primären Knoten bei WID-Farmen)

TIPP – Neuen öffentlichen Schlüssel für Partner exportieren

Für alle, die deine Metadaten nicht lesen, brauchst du das neue Zertifikat als Datei. Das geht direkt aus ADFS, ohne Umweg über den Zertifikatsspeicher:

```
$c = (Get-AdfsCertificate -CertificateType Token-Signing | Where-Object { -not $_.IsPrimary
}).Certificate
```

```
[IO.File]::WriteAllBytes('C:\Temp\adfs-signing-neu.cer', $c.Export('Cert'))
```

Die Datei enthält nur den öffentlichen Schlüssel und darf per Mail raus. Der private Schlüssel verlässt ADFS dabei nicht.

Microsoft Entra ID: automatisch, aber nicht bedingungslos

Microsoft 365 ist die Relying Party, um die sich die meisten Sorgen drehen – und bei der die Automatik am besten funktioniert. Microsoft Entra ID beginnt 35 Tage vor dem Ablauf des aktuellen Signaturzertifikats, deine Federation-Metadaten abzufragen, und wiederholt das täglich, bis ein neues Zertifikat auftaucht. Dann übernimmt Entra ID es als nächstes Signaturzertifikat, und die Promotion geht ohne Unterbrechung durch.

Das klappt unter zwei Bedingungen: AutoCertificateRollover ist aktiv, und die Metadaten sind aus dem Internet erreichbar – in der Regel über den Web Application Proxy. Blockiert deine Sicherheitsabteilung den Metadaten-Endpunkt nach außen, sieht Entra ID nichts, verschickt eine Benachrichtigung an die hinterlegten Kontakte und wartet. Mit Standardwerten entsteht das neue Zertifikat übrigens erst bei T-20; eine Mail um T-35 herum kann deshalb auch dann kommen, wenn eigentlich alles in Ordnung ist. Microsoft weist selbst darauf hin, dass solche Hinweise gelegentlich ohne Handlungsbedarf verschickt werden.

Den Abgleich prüfst du mit Microsoft Graph PowerShell. So sieht er im Kern aus:

```
Connect-MgGraph -Scopes 'Domain.Read.All'

# Was Entra ID für die Domäne gespeichert hat
Get-MgDomainFederationConfiguration -DomainId 'contoso.de' |
    Format-List IssuerUri, SigningCertificate, NextSigningCertificate

# Was ADFS gerade verwendet
Get-AdfsCertificate -CertificateType Token-Signing |
    ForEach-Object { [Convert]::ToBase64String($_.Certificate.RawData) }
```

Listing 4: Signaturzertifikate in Entra ID und ADFS vergleichen – stimmen die Base64-Werte überein, ist alles synchron

Wenn du von Hand nachziehen musst, erledigt das Update-MgDomainFederationConfiguration mit den Parametern -SigningCertificate und -NextSigningCertificate – pro föderierter Domäne. In

älteren Anleitungen steht an dieser Stelle Update-MsolFederatedDomain aus dem MSOnline-Modul; so stand es früher in jeder Anleitung, heute ist das kein Weg mehr, auf den du dich verlassen solltest. Die vollständige Schrittfolge mit allen Stolperstellen rund um mehrere Domänen und die Federation-ID beschreibt der Beitrag [Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren](#).

FAKTEN — Die Entscheidungsmatrix von Microsoft für Entra ID

AutoCertificateRollover aktiv, Zertifikate synchron, Metadaten öffentlich erreichbar: nichts zu tun.

AutoCertificateRollover aktiv, aber Zertifikate nicht synchron und weniger als 15 Tage Restlaufzeit: sofort von Hand aktualisieren.

AutoCertificateRollover aus und weniger als 35 Tage Restlaufzeit: sofort erneuern und Entra ID von Hand aktualisieren.

Ohne Automatik: Token-Signing mit eigenem PKI-Zertifikat

Viele Unternehmen schalten AutoCertificateRollover bewusst ab. Die Gründe sind nachvollziehbar: Die Sicherheitsrichtlinie verlangt Zertifikate aus der eigenen PKI, der Schlüssel soll in einem Hardware Security Module liegen, oder man möchte den Wechsel nicht einem Algorithmus überlassen, der keine Change-Termine kennt. Das ist legitim – nur musst du dann wissen, dass du ab sofort selbst der Rollover bist.

Kriterium	AutoCertificateRollover	Eigenes PKI-Zertifikat
Wer erzeugt das Zertifikat?	ADFS, selbstsigniert	keine Zertifizierungsstelle
Ablage des privaten Schlüssels	verschlüsselt in der ADFS-Konfiguration	Zertifikatsspeicher jedes Knotens oder HSM
Laufzeit	über CertificateDuration steuerbar	nach Vorlage und Richtlinie der PKI
Wechselzeitpunkt	Schwellwerte, ohne Rücksicht auf Change-Termine	du bestimmst ihn – und musst ihn auch bestimmen
Aufwand pro Jahr	gering, solange alle Metadaten lesen	Antrag, Import, Rechte, Promotion, Aufräumen
Größtes Risiko	statische Relying Parties an der Promotion	vergessener Termin, fehlende Rechte auf den Schlüssel
Sperrprüfung durch Partner	entfällt bei selbstsignierten Zertifikaten	Sperrliste muss für Partner mit Sperrprüfung erreichbar sein

Tabelle 3: Automatik und eigenes PKI-Zertifikat im Vergleich

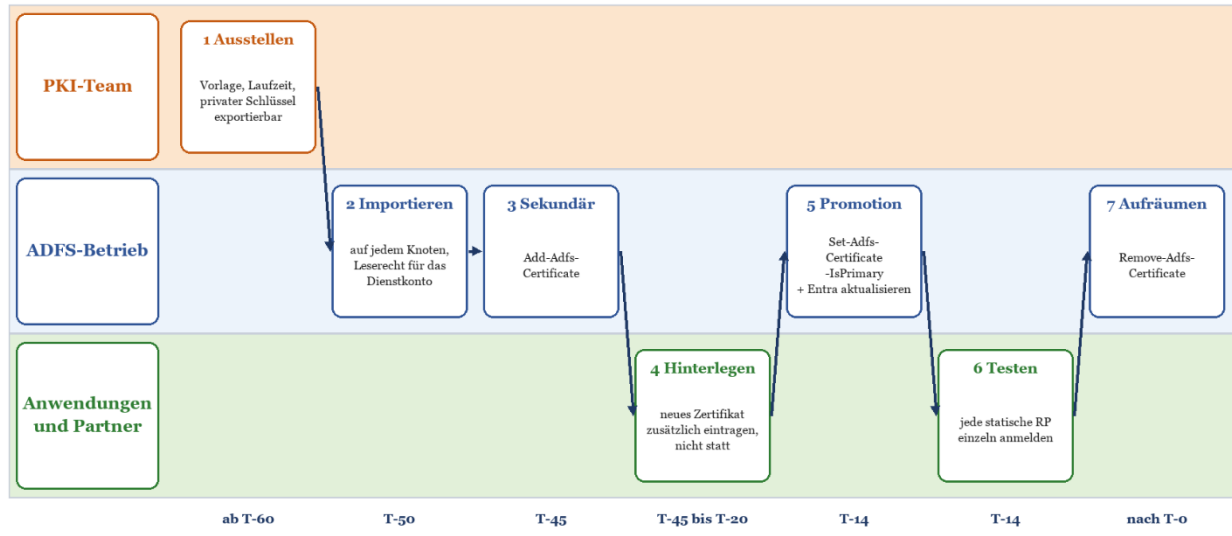
WICHTIG — Ein Zertifikat aus der PKI ist nicht automatisch sicherer

Relying Parties prüfen in aller Regel nur, ob die Signatur zum hinterlegten öffentlichen Schlüssel passt. Die Vertrauenskette zu deiner Stamm-CA spielt dabei selten eine Rolle. Der Sicherheitsgewinn eines PKI-Zertifikats liegt deshalb weniger im Zertifikat selbst als darin, wo und wie gut der private Schlüssel geschützt ist. Wer ihn exportierbar auf vier Servern liegen hat, hat gegenüber der Automatik nichts gewonnen.

Schritt für Schritt: vom Antrag bis zur Promotion

Skizze 4: Manuelle Erneuerung mit eigenem PKI-Zertifikat

Drei Beteiligte, sieben Schritte – der kritische Pfad sind nicht die Cmdlets, sondern die Menschen



Die Zeitangaben sind ein bewährter Rahmen, keine Vorschrift. Entscheidend ist der Abstand zwischen Schritt 3 und 5: Er muss lang genug sein, dass auch die langsamste Partnerorganisation ihr Change-Verfahren durchlaufen hat.

Skizze 4: Der manuelle Ablauf verteilt sich auf drei Beteiligte. Der Abstand zwischen Schritt 3 und 5 entscheidet über Erfolg oder Ausfall.

Das Zertifikat selbst ist unspektakulär: ein Schlüssel für die digitale Signatur, eine sinnvolle Laufzeit und ein sprechender Antragstellernamen wie CN=ADFS Signing sts.contoso.de, damit in drei Jahren noch jemand weiß, wofür es da ist. Weil du es auf allen Knoten einer WID- oder SQL-Farm brauchst, muss der private Schlüssel beim Ausstellen exportierbar sein – oder er liegt gleich im HSM, dann gelten dessen Regeln.

Danach importierst du das Zertifikat mit privatem Schlüssel in den Speicher Lokaler Computer › Eigene Zertifikate auf jedem ADFS-Knoten. Und dann kommt der Schritt, an dem gefühlt jede zweite manuelle Erneuerung hängt: Das ADFS-Dienstkonto braucht Leserecht auf den privaten Schlüssel. In der Zertifikatskonsole geht das über Alle Aufgaben › Private Schlüssel verwalten. Läuft ADFS unter einem gMSA, heißt der Eintrag dort zum Beispiel CONTOSO\gmsaADFS\$. Fehlt das Recht, startet der Dienst nach der Promotion nicht sauber oder kann nicht signieren – mehr dazu im Beitrag [gMSA als ADFS-Dienstkonto einrichten und umstellen](#).

```
# Automatik abschalten – sonst verweigert ADFS manuelle Zertifikatsänderungen
Set-AdfsProperties -AutoCertificateRollover $false

# Neues Zertifikat (auf allen Knoten importiert) als sekundär hinzufügen
Add-AdfsCertificate -CertificateType Token-Signing -Thumbprint '3F2A...E91C'

# Kontrolle: zwei Zertifikate, das neue mit IsPrimary = False
Get-AdfsCertificate -CertificateType Token-Signing

# --- Wochen später, im Wartungsfenster ---
Set-AdfsCertificate -CertificateType Token-Signing -Thumbprint '3F2A...E91C' -IsPrimary

# --- Nach Ablauf des alten Zertifikats ---
Remove-AdfsCertificate -CertificateType Token-Signing -Thumbprint 'A7C4...0B2D'
```

Listing 5: Manueller Wechsel mit PKI-Zertifikat. In WID-Farmen auf dem primären Knoten ausführen, in SQL-Farmen auf einem beliebigen.

WARNUNG – Nicht einfach wieder einschalten

Die Microsoft-Dokumentation schaltet AutoCertificateRollover nach dem Hinzufügen eines Zertifikats im Beispiel wieder ein. Für selbstsignierte Zertifikate ist das in Ordnung. Wer bewusst PKI-Zertifikate einsetzt, lässt die Automatik aus – sonst ersetzt ADFS dein sorgfältig beantragtes Zertifikat beim nächsten Schwellwert durch ein selbstsigniertes, und niemand hat es angekündigt.

Die Relying Parties, die du selbst versorgen musst

Zwischen dem Hinzufügen als sekundäres Zertifikat und der Promotion liegt die eigentliche Arbeit – und die findet nicht auf dem ADFS-Server statt. Jede Relying Party ohne Metadaten-Monitoring bekommt das neue Zertifikat zusätzlich zum alten, sofern sie zwei Zertifikate verträgt. Viele SaaS-Portale und die meisten SAML-Bibliotheken können das. Wo nur ein Zertifikat möglich ist, muss der Tausch exakt zum Promotionszeitpunkt passieren – dann sitzt die verantwortliche Person im Wartungsfenster mit am Tisch.

SharePoint Server ist so ein Fall. Das Signaturzertifikat hängt am SPTrustedIdentityTokenIssuer, und in vielen Farmen ist dort genau eines hinterlegt. Der Tausch gehört daher ins selbe Fenster wie die Promotion:

```
# Auf einem SharePoint-Server in der SharePoint Management Shell
$cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2('C:\Temp\adfs-signing-neu.cer')
New-SPTrustedRootAuthority -Name 'ADFS Token-Signing 2026' -Certificate $cert
Set-SPTrustedIdentityTokenIssuer -Identity 'ADFS contoso' -ImportTrustCertificate $cert
```

Listing 6: Neues Signaturzertifikat in SharePoint Server hinterlegen

Die Einrichtung der SAML-Anmeldung in SharePoint und was du dort sonst noch beachten solltest, steht in [SharePoint Server mit ADFS – SAML-Authentifizierung einrichten](#); den großen Rahmen rund um die Plattform liefert die Themenseite [SharePoint](#). Eigenentwicklungen auf Basis von Windows Identity Foundation führen die erlaubten Aussteller oft als Liste von Thumbprints in der Konfiguration. Dort trägst du vorab beide Thumbprints ein und entfernst den alten nach der Promotion.

TIPP – Ein Hinweis, kein Beweis

Relying Party Trusts, die bei dir ohne Metadaten-URL angelegt wurden, sind ein guter Startpunkt für die Suche nach statischen Partnern – wer auf deiner Seite von Hand gearbeitet hat, hat es auf der Gegenseite oft auch:

Get-AdfsRelyingPartyTrust | Where-Object { -not \$_.MetadataUrl } | Select-Object Name, Identifier, Enabled

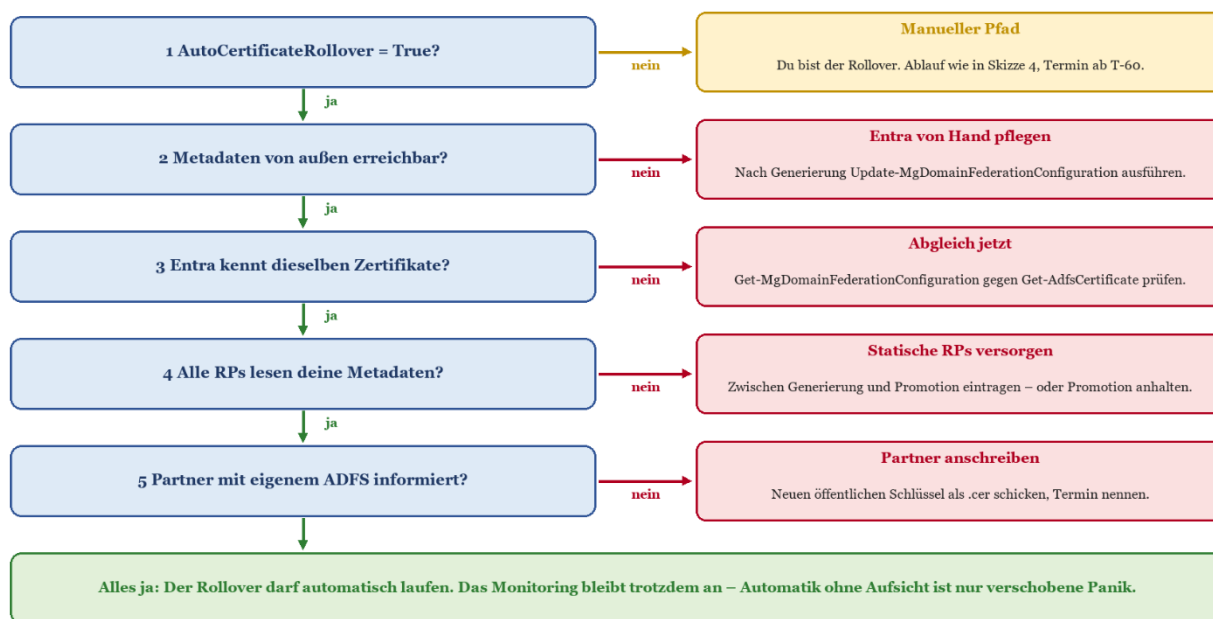
Verlässlich wird die Liste erst, wenn du jede Anwendung einzeln geprüft hast. Wie so eine Inventur aussieht, beschreibt [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#).

Wer vor dem Wechsel Bescheid wissen muss

Der technische Teil eines Token-Signing-Wechsels dauert keine zehn Minuten. Der organisatorische Teil entscheidet darüber, ob du danach Feierabend machst oder die Nacht mit Rollback-Überlegungen verbringst. Denn ein Rollback gibt es praktisch nur in eine Richtung: Du kannst das alte Zertifikat wieder primär setzen, solange es nicht abgelaufen ist – aber jede Relying Party, die inzwischen auf das neue umgestellt wurde, fällt dann ihrerseits um.

Skizze 5: Muss ich vor dem nächsten Rollover etwas tun?

Fünf Fragen, von oben nach unten – jede mit einem Cmdlet oder einem Telefonat beantwortbar



Frage 4 ist die ehrliche: Die meisten Farmen wissen nicht aus dem Stand, welche Relying Party statisch konfiguriert ist.

Skizze 5: Fünf Fragen, die vor jedem Rollover beantwortet sein sollten – nicht erst am Morgen danach.

Wer	Warum	Wann informieren	Was sie brauchen
Microsoft-365-/Entra-Verantwortliche	Federation-Einstellungen der Domänen müssen passen	vor der Generierung	Termin, Prüfbefehl aus Listing 4
Verantwortliche statischer SaaS-Anwendungen	Zertifikat im Admin-Portal eintragen	sobald das neue Zertifikat existiert	.cer-Datei, Promotionstermin, Ansprechpartner
SharePoint-Team	Token-Issuer muss umgestellt werden	bei Terminplanung für das Wartungsfenster	.cer-Datei, Listing 6, Anwesenheit im Fenster
Entwicklungsteams von Eigenanwendungen	Thumbprint in der Konfiguration	mit Vorlauf für ein Deployment	neuen Thumbprint, Termin
Externe Partnerorganisationen	Claims Provider Trust auf ihrer Seite	so früh wie möglich, mindestens vier Wochen	Metadaten-URL oder .cer-Datei, Termin
PKI-Team (bei PKI-Zertifikat)	Zertifikat ausstellen, Sperrliste erreichbar halten	ab T-60	Vorlage, Antragstellernamen, Laufzeit
Service Desk	erste Anlaufstelle, wenn doch etwas hakt	eine Woche vorher und am Tag selbst	Fehlerbild, Liste betroffener Anwendungen, Eskalationsweg
Change-Management	Promotion ist eine produktive Änderung	nach deinem regulären Vorlauf	Change-Antrag mit Rückfallplan
Informationssicherheit	Schlüsselschutz, HSM, Protokollierung	bei Konzeptänderungen	Ablage des privaten Schlüssels, Zugriffskreis

Tabelle 4: Wer muss informiert werden – die Liste, die in keinem Wiki fehlen sollte

WARNUNG – Ein Kalendereintrag reicht nicht

Der klassische Kalendereintrag „ADFS-Zertifikat läuft ab“ hat drei eingebaute Fehler. Erstens steht dort das Ablaufdatum, der Ausfall kommt aber mit der Promotion, also rund zwei Wochen früher.

Zweitens hängt er im Postfach einer Person, die im entscheidenden Jahr im Urlaub, krank oder nicht mehr im Unternehmen ist. Drittens sagt er nichts darüber, wen du anrufen musst.

Was stattdessen funktioniert: ein geplanter Task, der die Signaturzertifikate täglich prüft und an ein Teampostfach meldet, sobald ein sekundäres Zertifikat auftaucht oder die Restlaufzeit unter deinen Schwellwert fällt – plus eine gepflegte Liste der statischen Relying Parties mit Ansprechpartnern. Der Kalendereintrag darf bleiben, als Erinnerung daran, dass es die anderen beiden gibt.

```
# Tägliche Prüfung, z. B. als geplante Aufgabe auf einem ADFS-Knoten
$schwelle = 45
$zert = Get-AdfsCertificate -CertificateType Token-Signing | ForEach-Object {
    [pscustomobject]@{
        Thumbprint = $_.Thumbprint
        Primaer    = $_.IsPrimary
        NotAfter   = $_.Certificate.NotAfter
        Resttage   = [int]($_.Certificate.NotAfter - (Get-Date)).TotalDays
    }
}
$kritisch = $zert | Where-Object { $_.Primaer -and $_.Resttage -lt $schwelle }
$sekundaer = $zert | Where-Object { -not $_.Primaer }
if ($kritisch -or $sekundaer) {
    # Meldung an Teampostfach oder Monitoring-System übergeben
    $zert | Format-Table -AutoSize | Out-String
}
```

Listing 7: Signaturzertifikate täglich prüfen – die Übergabe an Mail oder Monitoring hängt von deiner Umgebung ab

Wer ohnehin ein ordentliches ADFS-Monitoring betreibt, hängt diese Prüfung dort an, statt noch ein Skript auf einen Server zu legen, das in drei Jahren niemand mehr kennt. Welche Werkzeuge sich dafür anbieten, zeigt [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#). Und wenn der Rollover doch zugeschlagen hat: ADFS selbst protokolliert in solchen Fällen meist keinen Fehler, die Spur findest du auf der Seite der Anwendung. Wie du die ADFS-Seite trotzdem sauber ausschließt, steht in [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#).

TIPP – Aus der Praxis – anonymisiert, aber leider nicht erfunden

In einer Farm mit über 40 Relying Parties lief AutoCertificateRollover jahrelang problemlos. Dann wurde eine Reisekostenanwendung angebunden, deren Anbieter nur einen Zertifikatsupload kannte. Elf Monate später, an einem Dienstag um 7:12 Uhr, promotete ADFS planmäßig den Nachfolger. Microsoft 365 lief weiter, die Reisekostenanwendung nicht. Die Fehlersuche begann beim Anbieter, der seinerseits ein Ticket eröffnete. Die Lösung dauerte zwei Minuten: .cer-Datei exportieren, ins Portal laden. Die Suche dauerte einen Tag. Seitdem steht die Anwendung auf einer Liste, und die Liste hat ein Teampostfach.

Schlüsselschutz, HSM und der Notfallwechsel

Ein Token-Signing-Zertifikat regelmäßig zu erneuern ist Betrieb. Der private Schlüssel dahinter ist aber auch das begehrteste Stück deiner Identitätsinfrastruktur: Wer ihn besitzt, kann Token für beliebige Benutzer ausstellen, ohne dass ADFS davon etwas mitbekommt. Diese Angriffstechnik ist unter dem Namen Golden SAML bekannt geworden. Microsoft empfiehlt deshalb ausdrücklich, die Schlüssel in einem Hardware Security Module zu schützen. Wie das im Gesamtbild aus Härtung, Protokollierung und MFA aussieht, beschreibt [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#).

Für die Erneuerung heißt das: Ein HSM ändert am Fahrplan nichts, wohl aber an den Handgriffen. Das Zertifikat wird im HSM erzeugt, die Knoten greifen über den Anbieter-Treiber darauf zu, und das Recht auf den Schlüssel regelst du über die Werkzeuge des HSM statt über die

Zertifikatskonsole. Plane den ersten Wechsel mit HSM unbedingt vorher in einer Testfarm durch – die Dokumentation des HSM-Herstellers ist an dieser Stelle wichtiger als jede ADFS-Anleitung.

Wenn der Schlüssel kompromittiert sein könnte

Besteht der Verdacht, dass jemand den privaten Schlüssel abgegriffen hat, ist die reguläre Erneuerung zu langsam. Microsoft beschreibt dafür einen Notfallwechsel, und der hat eine Eigenheit, die man kennen muss: Du erzeugst nicht ein, sondern zwei neue Zertifikate. Das erste ersetzt das kompromittierte mit Update-AdfsCertificate -Urgent sofort als primäres, das zweite wird sekundär. Der Grund: Entra ID merkt sich neben dem aktuellen auch das vorherige Zertifikat. Erst mit dem zweiten neuen Zertifikat verdrängst du das alte vollständig aus den Federation-Einstellungen.

```
# Notfallwechsel bei aktivem AutoCertificateRollover
Update-AdfsCertificate -CertificateType Token-Signing -Urgent # sofort neues primäres
Zertifikat
Update-AdfsCertificate -CertificateType Token-Signing # zweites Zertifikat als
sekundär
Remove-AdfsCertificate -CertificateType Token-Signing -Thumbprint 'A7C4...0B2D' #
kompromittiertes entfernen
```

Listing 8: Notfallwechsel. Anschließend Entra ID aktualisieren, alle Partner informieren und Aktualisierungstoken widerrufen.

WARNUNG – Notfall heißt Ausfall

Ein Notfallwechsel überspringt jeden Vorlauf. Jede Relying Party ohne Metadaten-Monitoring fällt sofort aus, bis sie das neue Zertifikat hat, und auch Metadaten-Konsumenten brauchen bis zum nächsten Abruf. Das ist der Preis dafür, dass ein Angreifer mit dem alten Schlüssel nichts mehr anfangen kann. Bei einem echten Verdacht zahlst du ihn gern – für einen bloß vergessenen Termin ist er zu hoch.

Ein letzter Punkt, der gern untergeht: Wer die ADFS-Konfiguration sichert, sichert bei selbstsignierten Zertifikaten auch das Schlüsselmateriale mit – entsprechend sorgfältig gehören solche Sicherungen verwahrt. Wie Sicherung und Wiederherstellung praktisch funktionieren, steht in [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#). Wenn du Rollover-Plan, Schlüsselschutz und Inventur nicht allein stemmen willst, unterstützen wir dich gern über [Consulting zu ADFS \(Active Directory Federation Services\)](#).

Fazit: Die Automatik ist gut – solange alle mitlesen

AutoCertificateRollover ist eine der wenigen ADFS-Funktionen, die man guten Gewissens eingeschaltet lassen kann. Sie erzeugt den Nachfolger rechtzeitig, veröffentlicht ihn in den Metadaten und sorgt dafür, dass Microsoft 365 den Wechsel ohne Zutun mitmacht – vorausgesetzt, die Metadaten sind von außen erreichbar. Das Problem sind nicht die Zertifikate, sondern die Relying Parties, die nicht mitlesen. Für sie ist der Stichtag die Promotion, nicht das Ablaufdatum.

Wer auf eigene PKI-Zertifikate setzt, tauscht die Automatik gegen Kontrolle – und gegen die Pflicht, jedes Jahr selbst an den Wechsel zu denken, die Rechte auf den privaten Schlüssel zu setzen und alle Beteiligten rechtzeitig ins Boot zu holen. Beides ist ein sauberer Weg. Kaputt geht es nur dort, wo niemand weiß, welcher Weg eigentlich gewählt wurde.

Und mit Blick nach vorn: Jede Relying Party, die du für den Rollover inventarisierst, ist eine, die du bei einem späteren Umzug nach Microsoft Entra ID schon kennst. ADFS läuft in vielen Unternehmen seit über zehn Jahren stabil, und es spricht nichts dagegen, es bis zum geplanten Ausstieg ordentlich zu betreiben. Wie der Weg für Microsoft 365 später aussehen kann, zeigt [Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout](#). Die Zusammenhänge

zwischen Zertifikaten, Vertrauensstellungen und Claims findest du ausführlich im Buch [ADFS in der Praxis – das Buch im Detail](#), und wer einen Rollover lieber einmal gefahrlos im Labor erlebt, bevor die Produktion dran ist, ist in unseren [ADFS-Schulungen](#) richtig.

WEITER — Passend zum Thema

- › [Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren](#) – Entra ID nach dem Wechsel von Hand abgleichen
- › [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#) – HSM, Golden SAML und Schlüsselschutz
- › [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#) – die Liste der statischen Relying Parties aufbauen
- › [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#) – wenn die Anmeldung trotzdem scheitert
- › [SSL-Zertifikat auf ADFS und Web Application Proxy tauschen](#) – das andere Zertifikat, das gern verwechselt wird

FAQ: ADFS Token-Signing-Zertifikat erneuern

Wie erneuere ich das ADFS Token-Signing-Zertifikat, wenn AutoCertificateRollover aktiv ist?

Im Normalfall gar nicht, das erledigt ADFS selbst. Du kannst den Nachfolger aber mit Update-AdfsCertificate -CertificateType Token-Signing vorziehen. Er erscheint dann als sekundäres Zertifikat in den Metadaten und wird nach dem CertificatePromotionThreshold primär.

Wann wird das neue Zertifikat bei AutoCertificateRollover aktiv?

Mit typischen Standardwerten erzeugt ADFS den Nachfolger 20 Tage vor Ablauf und macht ihn fünf Tage später zum primären Zertifikat – also etwa 15 Tage vor dem Ablaufdatum. Welche Werte deine Farm nutzt, zeigt Get-AdfsProperties.

Was ist der Unterschied zwischen primärem und sekundärem Token-Signing-Zertifikat?

Mit dem primären Zertifikat signiert ADFS alle Token. Das sekundäre steht zusätzlich in den Metadaten, damit Partner es vorab kennenlernen, wird aber noch nicht zum Signieren verwendet. Die Promotion macht das sekundäre zum primären.

Muss ich Microsoft 365 nach dem Zertifikatswechsel aktualisieren?

Nicht, wenn AutoCertificateRollover aktiv ist und deine Federation-Metadaten aus dem Internet erreichbar sind. Dann holt sich Entra ID das neue Zertifikat ab 35 Tagen vor Ablauf selbst. Andernfalls aktualisierst du die Domäne mit Update-MgDomainFederationConfiguration.

Warum fällt eine Anwendung aus, obwohl das alte Zertifikat noch gültig ist?

Weil ADFS ab der Promotion mit dem neuen Schlüssel signiert. Eine Relying Party, die nur das alte Zertifikat kennt, hält jede Signatur für ungültig – unabhängig davon, dass das alte Zertifikat noch Tage oder Wochen gültig wäre.

Kann ich die Promotion bei AutoCertificateRollover verschieben?

Ja. Entweder dauerhaft über größere Werte für CertificateGenerationThreshold und CertificatePromotionThreshold, oder situativ: Automatik nach der Generierung abschalten, das neue Zertifikat zum Wunschtermin mit Set-AdfsCertificate -IsPrimary aktivieren und die Automatik danach wieder einschalten.

Welche Rechte braucht das ADFS-Dienstkonto bei einem eigenen Zertifikat?

Leserecht auf den privaten Schlüssel des Zertifikats, und zwar auf jedem ADFS-Knoten. Das setzt du in der Zertifikatskonsole über Private Schlüssel verwalten. Bei einem gMSA trägst du das Konto mit abschließendem Dollarzeichen ein.

Kann ich das alte Token-Signing-Zertifikat nach dem Wechsel löschen?

Ja, sobald es abgelaufen ist oder du sicher bist, dass es niemand mehr braucht, mit Remove-AdfsCertificate. Bei einem Verdacht auf Kompromittierung entfernst du es sofort – ein noch hinterlegtes altes Zertifikat kann sonst weiter genutzt werden.

Ist das Token-Signing-Zertifikat dasselbe wie das SSL-Zertifikat von ADFS?

Nein. Das SSL-Zertifikat sichert die HTTPS-Verbindung zu sts.contoso.de und stammt meist von einer öffentlichen Zertifizierungsstelle. Das Token-Signing-Zertifikat signiert die ausgestellten Token und ist standardmäßig selbstsigniert. Beide werden unabhängig voneinander erneuert.