

SSL-Zertifikat auf ADFS und Web Application Proxy tauschen

ADFS • WAP • Load Balancer

SSL-Zertifikat tauschen

auf allen Knoten, an allen Ports, bis zum letzten Load Balancer –
damit der Montag nicht mit einer Browserwarnung beginnt

boddenberg.de



WISSEN

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

› [Active Directory Federation Services](#)

BERATUNG

Zertifikatstausch in Farm, Perimeter und Load Balancer – geplant, begleitet und dokumentiert.

› [Consulting zu ADFS](#)

SCHULUNG

Zertifikatswechsel an einer Laborfarm üben, inklusive absichtlich fehlender Zwischenzertifizierungsstelle.

› [ADFS-Schulungen](#)

Es gibt diese eine Kalendererinnerung, die jedes Jahr pünktlich aufpoppt und jedes Jahr pünktlich weggeklickt wird: „SSL-Zertifikat sts.contoso.de läuft ab“. Irgendwann klickt sie niemand mehr weg, weil sie niemand mehr sieht – der Kollege, der sie angelegt hat, ist inzwischen woanders. Und dann beginnt ein Montag mit einer roten Browserwarnung auf der Anmeldeseite, einem Outlook, das nach Kennwörtern bittet, und einem Service Desk, der plötzlich sehr viel Zeit mit dir verbringen möchte.

Dabei ist das ADFS SSL-Zertifikat zu tauschen eigentlich keine Raketenwissenschaft. Es ist nur eine Aufgabe mit erstaunlich vielen Stellen, an denen man etwas vergessen kann: jeder ADFS-Knoten, das Service-Communications-Zertifikat, jeder Web Application Proxy, jede dort veröffentlichte Anwendung, der Port 49443 für Smartcards – und der Load Balancer, an den bis zum ersten Ausfall niemand denkt. Genau diese Stellen gehen wir in diesem Beitrag der Reihe nach durch: einmal per Mausklick, einmal per PowerShell, danach die typischen Fehler und am Ende eine Checkliste zum Abhaken.

Die Grundlagen zu Farm, Proxy und Vertrauensstellungen setze ich voraus. Wenn du die auffrischen willst, findest du alles auf der Übersichtsseite [Active Directory Federation Services](#). Hier geht es um den konkreten Handgriff.

FAKTEN – Das SSL-Zertifikat von ADFS in drei Sätzen

Es sichert die HTTPS-Verbindung zum Federation Service, also alles, was Browser, Outlook, Teams und Smartphones unter sts.contoso.de aufrufen – intern direkt auf der Farm, extern über den Web Application Proxy.

Es stammt in der Praxis fast immer von einer öffentlichen Zertifizierungsstelle, weil auch Geräte ohne Domänenmitgliedschaft und Partner ihm vertrauen müssen.

Mit dem Token-Signing-Zertifikat hat es nichts zu tun. Tauschst du das SSL-Zertifikat, müssen weder Microsoft 365 noch deine Relying Parties etwas davon erfahren.

Falls du gerade das Signaturzertifikat erneuern musst, bist du hier falsch abgebogen – das behandelt [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#). Die gute Nachricht: Der SSL-Tausch ist die harmlosere der beiden Operationen. Die schlechte: harmlos heißt nicht folgenlos.

Vorbereitung: Welches Zertifikat, wo überall und in welchem Zustand

Der häufigste Fehler beim Zertifikatstausch passiert nicht im Wartungsfenster, sondern eine Woche vorher: beim Beantragen. Wer hier schlampt, stellt am Abend des Tausches fest, dass ein Name fehlt oder sich das Zertifikat nicht auf den zweiten Knoten bringen lässt. Also erst einmal Bestandsaufnahme.

Vier Zertifikate, die gern verwechselt werden

ADFS kennt mehrere Zertifikate, und in der Verwaltungskonsolle stehen sie friedlich untereinander. Das verleitet dazu, das falsche zu tauschen. Die Tabelle trennt sie sauber:

Zertifikat	Zweck	Woher	Tausch betrifft Partner?
SSL-Zertifikat	HTTPS-Bindungen auf ADFS und WAP	öffentliche CA	nein
Service-Communications	Zertifikat in der Farmkonfiguration, u. a. für WCF-Nachrichtensicherheit; standardmäßig identisch mit dem SSL-Zertifikat	meist dasselbe wie SSL	nein
Token-Signing	signiert ausgestellte Token	meist selbstsigniert von ADFS	ja, alle Relying Parties
Token-Decrypting	entschlüsselt Token von Claims Providern	meist selbstsigniert von ADFS	ja, Claims Provider

Tabelle 1: Die ADFS-Zertifikate im Überblick – dieser Beitrag behandelt die ersten beiden Zeilen.

WICHTIG – Konsole und Wirklichkeit sind nicht dasselbe

Das Zertifikat, das in der AD FS-Verwaltung unter „Dienstkommunikation“ steht, ist nicht das Zertifikat an der HTTPS-Bindung. Microsoft weist ausdrücklich darauf hin: Das SSL-Zertifikat tauschst du nur per PowerShell. Wer nur in der Konsole klickt, hat danach ein neues Zertifikat in der Farmkonfiguration und ein altes an Port 443 – und wundert sich über die Browserwarnung am Stichtag.

Die Namen im Zertifikat

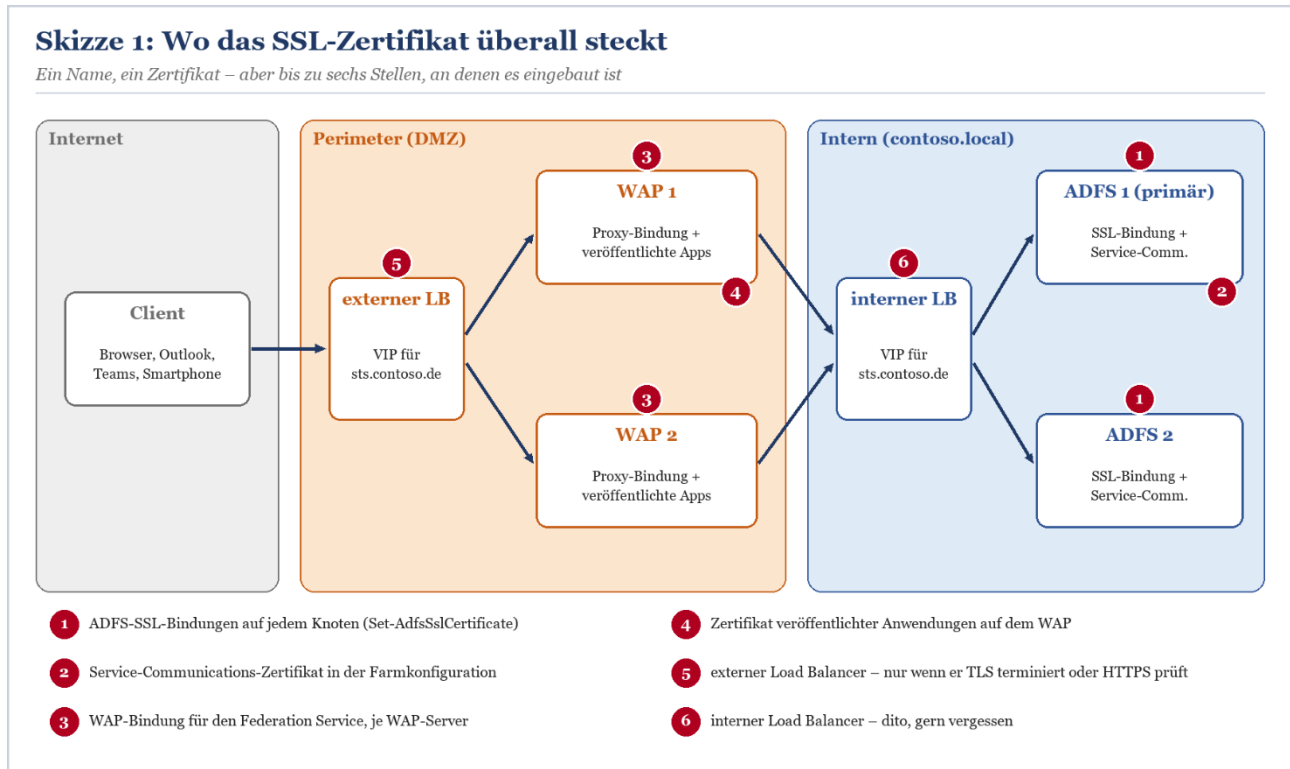
Das neue Zertifikat braucht mindestens den Namen des Federation Service, also sts.contoso.de, im Antragstellernamen oder im alternativen Antragstellernamen (SAN), dazu die erweiterte Schlüsselverwendung Serverauthentifizierung. Je nach Umgebung kommen weitere SAN-Einträge hinzu:

- certauth.sts.contoso.de, wenn du die Benutzerzertifikat-Anmeldung im alternativen Bindungsmodus über Port 443 betreibst.
- enterpriseregistration.contoso.de für jedes verwendete UPN-Suffix, wenn du Geräteregistrierung über ADFS nutzt.
- Namen veröffentlichter Anwendungen, falls der WAP dasselbe Zertifikat auch für Anwendungen verwendet – etwa ein SAN für owa.contoso.de.

Mein Tipp: Nimm das alte Zertifikat als Vorlage. Öffne es, notiere alle SAN-Einträge und frage bei jedem nach, ob er noch gebraucht wird. Ein Eintrag, den niemand mehr kennt, ist meistens einer, den ein Gerät im Keller noch benutzt.

Wo das Zertifikat überall eingebaut ist

Ein Name, ein Zertifikat – aber bis zu sechs Stellen, an denen es eingebaut ist. Skizze 1 zeigt eine typische Farm mit zwei ADFS-Knoten, zwei WAP-Servern und je einem Load Balancer davor. Mehr zur Topologie steht in [ADFS: Architektur, Einsatzszenarien und Hochverfügbarkeit](#).



Skizze 1: Die sechs Stellen, an denen das SSL-Zertifikat in einer typischen ADFS-Umgebung steckt.

Microsoft empfiehlt, auf allen ADFS- und WAP-Servern dasselbe Zertifikat zu verwenden. Das ist nicht nur bequem, sondern in den meisten Umgebungen Pflicht: Ist die ADFS-Eigenschaft ExtendedProtectionTokenCheck aktiv – und das ist der Standard – oder leitet der Proxy Anfragen mit integrierter Windows-Authentifizierung weiter, muss der WAP dasselbe Zertifikat mit demselben Schlüssel verwenden wie die Farm. Zwei verschiedene Zertifikate für innen und außen sind also keine kreative Lösung, sondern eine Einladung zu schwer erklärbaren Anmeldefehlern.

Den privaten Schlüssel exportierbar machen

Du brauchst das Zertifikat auf mindestens vier Servern. Das funktioniert nur, wenn du es als PFX mit privatem Schlüssel exportieren kannst. Erzeugst du den Zertifikatsantrag auf einem ADFS-Knoten, achte darauf, dass der Schlüssel als exportierbar markiert ist – in der Zertifikatskonsole unter den Eigenschaften der benutzerdefinierten Anforderung, Registerkarte „Privater Schlüssel“. Wer das vergisst, hat ein Zertifikat, das genau auf einem Server funktioniert. In einer Farm ist das ungefähr so nützlich wie ein Schlüssel, der nur für eine von vier Türen passt.

FAKTEN – Kürzere Laufzeiten für öffentliche Zertifikate

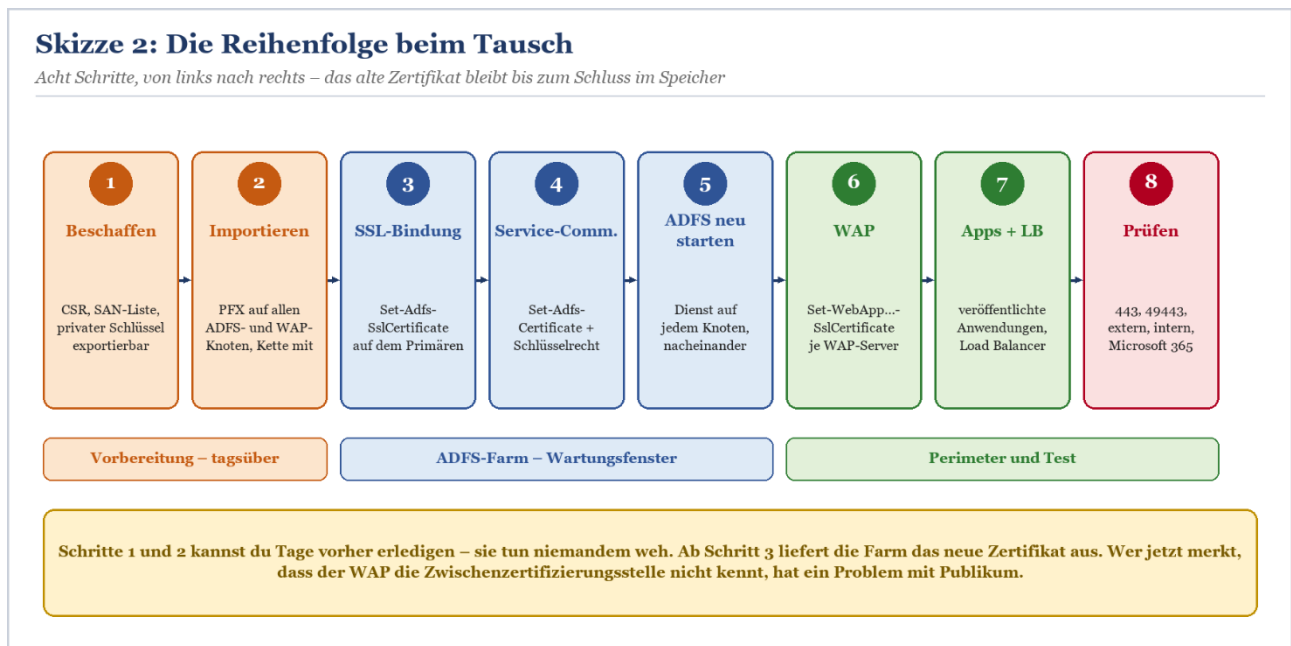
Das CA/Browser Forum hat die maximale Laufzeit öffentlicher TLS-Zertifikate schrittweise verkürzt: Seit März 2026 sind höchstens 200 Tage erlaubt, ab März 2027 werden es 100 Tage, ab März 2029

nur noch 47 Tage.

Für ADFS heißt das: Der Tausch ist kein jährliches Ritual mehr, sondern wird zur Routine. Spätestens jetzt lohnt sich ein sauber dokumentiertes Verfahren – oder ein Skript, das du nicht jedes Mal neu erfinden musst.

ADFS-Farm: Zertifikat importieren und die Bindungen tauschen

Die Reihenfolge ist entscheidend. Skizze 2 zeigt den Ablauf von der Beschaffung bis zum Test. Die ersten beiden Schritte erledigst du tagsüber, ohne dass es jemand merkt; ab Schritt 3 liefert die Farm das neue Zertifikat aus.



Skizze 2: Die Reihenfolge beim Tausch – Vorbereitung, Farm, Perimeter und Test.

Schritt 1: Import auf allen Knoten – per Mausklick

Importiere die PFX-Datei auf jedem ADFS-Knoten und jedem WAP-Server in den Computerspeicher. So geht es in der Oberfläche:

- certlm.msc starten (Zertifikate – Lokaler Computer).
- Eigene Zertifikate > Zertifikate > Rechtsklick > Alle Aufgaben > Importieren.
- PFX-Datei auswählen, Kennwort eingeben. „Alle erweiterten Eigenschaften mit einbeziehen“ aktiviert lassen.
- „Schlüssel als exportierbar markieren“ nur aktivieren, wenn du das Zertifikat von diesem Server aus später weiterverteilen willst – sonst lieber nicht.
- Zertifikatspeicher „Eigene Zertifikate“ wählen und abschließen.
- Das Zertifikat doppelklicken: Auf der Registerkarte „Allgemein“ muss „Sie besitzen einen privaten Schlüssel für dieses Zertifikat“ stehen, auf der Registerkarte „Zertifizierungspfad“ die vollständige Kette ohne Warnsymbol.

Schritt 1: Import auf allen Knoten – per PowerShell

Bei mehr als zwei Servern ist PowerShell schneller und vor allem gleichförmiger. Das folgende Beispiel kopiert die PFX auf die ADFS-Knoten und importiert sie dort. Die Servernamen sind Beispiele aus contoso.local:

```
$pfx = 'C:\Install\sts.contoso.de-2026.pfx'
$pw = Read-Host -AsSecureString -Prompt 'PFX-Kennwort'
$nodes = 'adfs01.contoso.local', 'adfs02.contoso.local'

foreach ($n in $nodes) {
    $s = New-PSSession -ComputerName $n
    Copy-Item -Path $pfx -Destination 'C:\Windows\Temp\ssl.pfx' -ToSession $s
    Invoke-Command -Session $s -ScriptBlock {
        Import-PfxCertificate -FilePath 'C:\Windows\Temp\ssl.pfx' `
            -CertStoreLocation Cert:\LocalMachine\My -Password $using:pw
        Remove-Item 'C:\Windows\Temp\ssl.pfx'
    }
    Remove-PSSession $s
}
```

Import der PFX auf allen ADFS-Knoten. Die WAP-Server im Perimeter sind meist nicht in der Domäne – dort importierst du lokal oder per Remoting mit expliziten Anmeldedaten.

Danach brauchst du den Fingerabdruck des neuen Zertifikats. Kopiere ihn nicht aus dem Eigenschaftendialog: Dort hängt sich gern ein unsichtbares Steuerzeichen an den Anfang, und das Cmdlet meldet dann, es finde kein Zertifikat. Hol ihn lieber per PowerShell:

```
Get-ChildItem Cert:\LocalMachine\My |
    Where-Object Subject -like '*sts.contoso.de*' |
    Select-Object Thumbprint, NotBefore, NotAfter, HasPrivateKey, Subject

$new = '<Fingerabdruck des neuen Zertifikats>'
```

Schritt 2: Set-AdfsSslCertificate auf dem primären Knoten

Jetzt der eigentliche Tausch. Seit Windows Server 2016 ist Set-AdfsSslCertificate ein Cmdlet für die ganze Farm: Du führst es einmal auf dem primären Knoten aus, und es aktualisiert die Bindungen auf allen Knoten per PowerShell Remoting. Unter Windows Server 2012 R2 musstest du es noch auf jedem Server einzeln starten. Voraussetzung für den Farmbetrieb ist ein Farm Behavior Level ab 2016 – falls deine Farm noch darunter liegt, hilft [ADFS-Farm upgraden – Farm Behavior Level anheben ohne Ausfall](#).

```
# Welcher Knoten ist primär? (bei WID-Farmen relevant)
Get-AdfsSyncProperties | Select-Object Role, PrimaryComputerName

# Vorher: Welche Bindungen gibt es, welches Zertifikat hängt daran?
Get-AdfsSslCertificate

# Tausch für alle Bindungen auf allen Knoten
Set-AdfsSslCertificate -Thumbprint $new

# Nachher: Jede Zeile muss den neuen Hash zeigen
Get-AdfsSslCertificate
```

Tausch der SSL-Bindungen im Standardbindungsmodus. Das Cmdlet braucht WinRM (TCP 5985) zu den anderen Knoten.

Zwei Details, die in vielen Anleitungen fehlen. Erstens: Das Cmdlet gibt dem ADFS-Dienst selbst – dem Prinzipal adfssrv – Leserecht auf den privaten Schlüssel. Das Dienstkonto musst du für die SSL-Bindung nicht extra berechtigen. Zweitens: Es braucht Remoting zu den anderen Knoten. Ist TCP 5985 zwischen den ADFS-Servern gesperrt, bricht es auf halber Strecke ab, und du hast eine Farm, in der jeder Knoten ein anderes Zertifikat ausliefert. Das fällt nicht sofort auf, sondern erst, wenn der Load Balancer dich zufällig auf den falschen Knoten schickt.

Standardmodus oder alternativer Bindungsmodus

Für die Anmeldung mit Benutzerzertifikaten, etwa per Smartcard, braucht ADFS eine eigene TLS-Bindung, die ein Clientzertifikat anfordert. Dafür gibt es zwei Modi, und für jeden ist ein anderes Cmdlet zuständig:

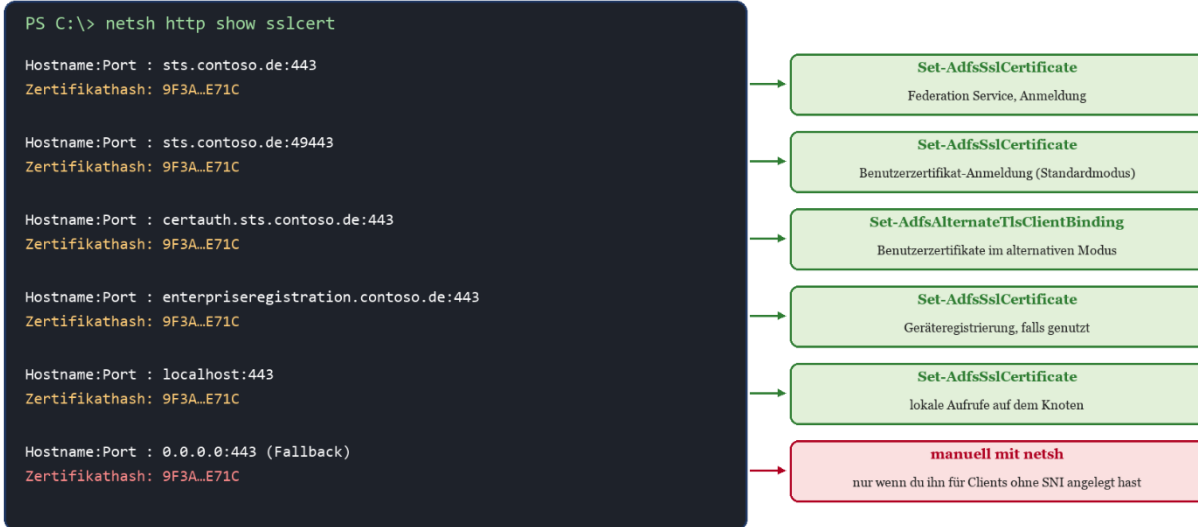
	Standardmodus	Alternativer Bindungsmodus
Benutzerzertifikate über	sts.contoso.de:49443	certauth.sts.contoso.de:443
Cmdlet für den Tausch	Set-AdfsSslCertificate	Set-AdfsAlternateTlsClientBinding
Zusätzlicher SAN-Eintrag	nicht nötig	certauth.sts.contoso.de
Firewall Client > WAP	TCP 443 und 49443	nur TCP 443
Typischer Fehler	49443 zeigt altes Zertifikat	certauth-Name fehlt im neuen Zertifikat

Tabelle 2: Die beiden Bindungsmodi für die Benutzerzertifikat-Anmeldung.

Läuft deine Farm im alternativen Modus, ersetzt Set-AdfsAlternateTlsClientBinding -Thumbprint \$new den Aufruf von oben. Laut Microsoft kümmert sich dieses Cmdlet dann nicht nur um die certauth-Bindung, sondern um alle Bindungen, an denen ADFS das SSL-Zertifikat verwendet. Welche Bindungen ein Knoten tatsächlich hat, zeigt netsh – Skizze 3 erklärt die Ausgabe.

Skizze 3: Welche Bindungen ein ADFS-Knoten wirklich hat

Ausgabe von netsh http show sslcert, auf das Wesentliche eingedampft – jede Zeile braucht denselben Hash



Die Liste ist ein Beispiel: Welche Zeilen bei dir existieren, hängt von Bindungsmodus, UPN-Suffixen und Historie ab.

Skizze 3: Die HTTP.SYS-Bindungen eines ADFS-Knotens. Alle Zeilen müssen nach dem Tausch denselben Zertifikatshash zeigen.

```
# Alle SSL-Bindungen des lokalen Knotens, auf Hostname und Hash reduziert
netsh http show sslcert | Select-String 'Hostname:Port|IP:Port|Zertifikathash|Certificate Hash'
```

Die Beschriftung der Felder hängt von der Sprache des Betriebssystems ab – deshalb sucht das Muster nach beiden Varianten.

WARNUNG — Bindungen nicht von Hand mit netsh umbiegen

Es ist verlockend, eine einzelne Bindung mit `netsh http delete sslcert` und `add sslcert` selbst zu tauschen. Lass es, solange es die Cmdlets tun. Die ADFS-Bindungen tragen eine feste Anwendungs-ID und Optionen wie die Aushandlung von Clientzertifikaten an Port 49443. Legst du sie von Hand neu an und vergisst eine Option, funktioniert die Smartcard-Anmeldung nicht mehr – und niemand weiß warum. Die einzige typische Ausnahme ist ein selbst angelegter o.o.o.o-Fallback für Clients

ohne SNI: Den kennt ADFS nicht, den musst du selbst nachziehen.

Schritt 3: Service-Communications mit Set-AdfsCertificate

Das Service-Communications-Zertifikat ist in den meisten Farmen dasselbe wie das SSL-Zertifikat – so richtet ADFS es bei der Installation ein, und Microsoft empfiehlt es auch so. Nach dem Tausch der Bindungen zeigt es aber noch auf das alte Zertifikat. Das rächt sich spätestens, wenn das alte abgelaufen ist und jemand es aufräumt.

Per Mausklick: AD FS-Verwaltung öffnen, Dienst > Zertifikate, im Aktionsbereich „Dienstkommunikationszertifikat festlegen ...“ (im englischen System „Set Service Communications Certificate ...“), das neue Zertifikat auswählen. Per PowerShell auf dem primären Knoten:

```
Set-AdfsCertificate -CertificateType Service-Communications -Thumbprint $new

Get-AdfsCertificate -CertificateType Service-Communications |
    Select-Object Thumbprint, @{n='NotAfter'; e={$_.Certificate.NotAfter}}
```

Anders als bei der SSL-Bindung vergibt hier niemand automatisch Rechte. Das ADFS-Dienstkonto braucht Leserecht auf den privaten Schlüssel – auf jedem Knoten. In certlm.msc: Rechtsklick auf das Zertifikat > Alle Aufgaben > Private Schlüssel verwalten > Dienstkonto hinzufügen, Recht „Lesen“. Bei einem Group Managed Service Account gibst du den Namen mit abschließendem Dollarzeichen ein und musst im Suchdialog den Objekttyp „Dienstkonten“ aktivieren. Mehr dazu steht in [gMSA als ADFS-Dienstkonto einrichten und umstellen](#).

```
# Dienstkonto der Farm ermitteln
(Get-CimInstance Win32_Service -Filter "Name='adfssrv']").StartName

# Danach auf jedem Knoten nacheinander – nie alle gleichzeitig
Restart-Service adfssrv
```

Den Dienst startest du Knoten für Knoten neu, während der Load Balancer die übrigen bedient.

TIPP — Der Weg über Entra Connect

Wenn du Entra Connect ohnehin mit ADFS-Verwaltung betreibst, bietet der Assistent eine Aufgabe zum Aktualisieren des ADFS-SSL-Zertifikats, die Farm und WAP in einem Durchgang bedient. Microsoft nennt das sogar den empfohlenen Weg. In der Praxis ist er bequem, wenn alle Server erreichbar und die Anmeldedaten für den Perimeter griffbereit sind. Die PowerShell-Variante bleibt trotzdem Pflichtwissen: Sie funktioniert auch dann, wenn der Assistent irgendwo hängen bleibt.

Web Application Proxy: Bindung, veröffentlichte Anwendungen und der Load Balancer

Die Farm ist fertig, intern läuft alles. Jetzt kommt der Teil, den Anwender aus dem Homeoffice sehen. Der WAP hat zwei Arten von Zertifikaten: das für den Federation Service, über das er die ADFS-Anmeldung nach außen reicht, und je ein Zertifikat pro veröffentlichter Anwendung. Beide müssen getauscht werden, wenn sie dasselbe Zertifikat verwenden. Architektur und Zukunft des Proxys behandelt [Web Application Proxy: Architektur und Ablöse](#).

Set-WebApplicationProxySslCertificate auf jedem WAP-Server

Anders als bei der Farm gibt es hier kein Cmdlet, das alle Server auf einmal bedient: Du führst den Befehl auf jedem WAP-Server aus. Vorher muss das Zertifikat samt Kette dort importiert sein.

```
# Auf jedem WAP-Server
Get-WebApplicationProxySslCertificate

Set-WebApplicationProxySslCertificate -Thumbprint $new

Get-WebApplicationProxySslCertificate
Restart-Service appproxysvc
```

Das Cmdlet tauscht die Bindungen des Federation Service auf dem Proxy – im Standard- wie im alternativen Bindungsmodus.

WARNUNG – Wenn das alte Zertifikat schon abgelaufen ist

Dann scheitert Set-WebApplicationProxySslCertificate häufig, weil der Proxy mit der Farm gar nicht mehr sprechen kann. Microsoft beschreibt für diesen Fall die Neukonfiguration mit Install-WebApplicationProxy: mit den Anmeldedaten eines Domänenbenutzers, der lokaler Administrator auf den ADFS-Servern ist, dem Fingerabdruck des neuen Zertifikats und dem Namen sts.contoso.de. Das stellt auch das Proxy-Vertrauen wieder her. Wie du das Vertrauen generell im Griff behältst, steht in [WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will](#).

Veröffentlichte Anwendungen prüfen

Jede über den WAP veröffentlichte Anwendung mit HTTPS-Adresse hat einen eigenen Eintrag für den Fingerabdruck des externen Zertifikats. Diese Einträge liegen in der ADFS-Konfiguration, gelten also für alle WAP-Server gemeinsam – das Zertifikat selbst muss aber auf jedem WAP-Server vorhanden sein. In der Remotezugriffsverwaltung findest du sie unter Web Application Proxy > Veröffentlichte Webanwendungen > Bearbeiten. Schneller geht es so:

```
$old = '<Fingerabdruck des alten Zertifikats>'

# Welche Anwendungen hängen noch am alten Zertifikat?
Get-WebApplicationProxyApplication |
    Where-Object ExternalCertificateThumbprint -eq $old |
    Select-Object Name, ExternalUrl, ExternalCertificateThumbprint

# Umstellen
Get-WebApplicationProxyApplication |
    Where-Object ExternalCertificateThumbprint -eq $old |
    ForEach-Object {
        Set-WebApplicationProxyApplication -ID $_.ID -ExternalCertificateThumbprint $new
    }
```

Anwendungen mit eigenem Zertifikat, etwa owa.contoso.de mit separatem Zertifikat, bleiben unberührt – der Filter auf den alten Fingerabdruck sorgt dafür. Und bitte: Schau dir die Liste an, bevor du den zweiten Block ausführst. Dort tauchen gelegentlich Anwendungen auf, von denen niemand mehr wusste, dass sie noch veröffentlicht sind. Das ist ein guter Moment für eine Aufräumnotiz.

Den Load Balancer nicht vergessen

Microsofts Vorgabe ist eindeutig: Ein Load Balancer vor ADFS soll TLS nicht terminieren, sondern die Verbindung durchreichen, weil sonst die Anmeldung mit Zertifikaten bricht. Wenn dein Load Balancer genau so arbeitet, hat er kein Zertifikat und du bist hier fertig. Die Praxis sieht aber oft anders aus:

Konfiguration am Load Balancer	Was beim Tausch zu tun ist
Layer 4, TLS wird durchgereicht	nichts – das Zertifikat liegt nur auf ADFS und WAP
TLS-Terminierung oder Re-Encryption (SSL Bridging)	neues Zertifikat samt Kette auf dem Load Balancer hinterlegen und dem virtuellen Dienst zuweisen; von Microsoft für ADFS nicht unterstützt

HTTPS-Health-Check mit Zertifikatsprüfung	Prüfung anpassen oder besser auf den HTTP-Endpunkt /adfs/probe umstellen
Zertifikat per Fingerabdruck fest in einem Profil	Profil aktualisieren, sonst liefert der Load Balancer weiter das alte aus
Interner und externer Load Balancer	beide prüfen – der interne wird gern vergessen

Tabelle 3: Was der Load Balancer beim Zertifikatstausch braucht.

Wer einen Kemp LoadMaster einsetzt, findet die Einstellungen am virtuellen Dienst unter der SSL-Beschleunigung; Details zu Health Probe, SNI und Persistenz stehen in [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#) und auf der Übersichtsseite [Kemp LoadMaster](#).

Prüfen, ob wirklich überall das neue Zertifikat ausgeliefert wird

„Im Browser sieht’s gut aus“ ist kein Testprotokoll. Dein Browser landet über den Load Balancer auf irgendeinem Knoten, und genau den prüfst du. Die anderen drei liefern vielleicht noch das alte Zertifikat aus – bis der Load Balancer jemand anderen dorthin schickt. Deshalb fragst du jeden Server einzeln ab, direkt über seine IP-Adresse, aber mit dem richtigen SNI-Namen.

```
function Get-RemoteSslCertificate {
    param([string]$Target, [string]$SniName = 'sts.contoso.de', [int]$Port = 443)
    $tcp = [System.Net.Sockets.TcpClient]::new($Target, $Port)
    $ssl = [System.Net.Security.SslStream]::new($tcp.GetStream(), $false, { $true })
    try {
        $ssl.AuthenticateAsClient($SniName)
        $c =
[System.Security.Cryptography.X509Certificates.X509Certificate2]::new($ssl.RemoteCertificate)
        [pscustomobject]@{ Ziel = "${Target}:$Port"; Thumbprint = $c.Thumbprint; NotAfter =
$c.NotAfter }
    } finally { $ssl.Dispose(); $tcp.Dispose() }
}

# ADFS-Knoten und WAP-Server einzeln, jeweils 443 und 49443 (Beispieladressen)
'10.0.20.11', '10.0.20.12', '192.168.50.21', '192.168.50.22' | ForEach-Object {
    Get-RemoteSslCertificate -Target $_
    Get-RemoteSslCertificate -Target $_ -Port 49443
}
```

Die Validierung ist im Skript bewusst abgeschaltet – es soll zeigen, welches Zertifikat kommt, nicht ob der Testrechner ihm vertraut.

Danach der Funktionstest aus Sicht der Anwender: extern ohne VPN auf die Anmeldeseite, die Metadaten unter /FederationMetadata/2007-06/FederationMetadata.xml abrufen, eine Anmeldung bei Microsoft 365, eine an einer über den WAP veröffentlichten Anwendung und – falls genutzt – eine Smartcard-Anmeldung. Wenn du ein Monitoring mit Ablaufwarnung betreibst, trägst du dort das neue Ablaufdatum ein; wie so ein Monitoring aussieht, zeigt [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#).

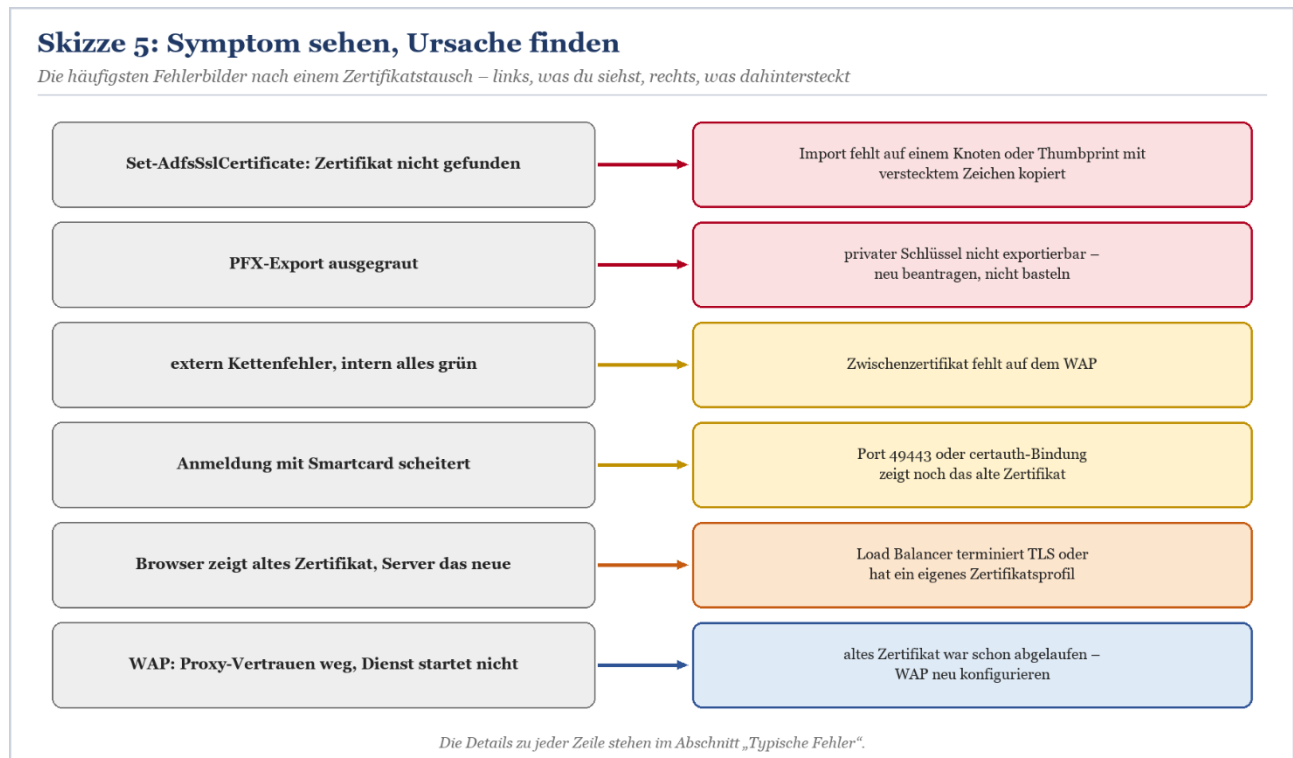
FAKTEN — Muss Microsoft 365 etwas davon erfahren?

Nein. Der Federation Trust in Entra ID enthält das Token-Signing-Zertifikat, nicht das SSL-Zertifikat. Ein Update der Domänenkonfiguration ist nach einem SSL-Tausch nicht nötig. Früher stand in fast jeder Anleitung trotzdem Update-MsolFederatedDomain – das Modul MSOnline ist ausgemustert und war für diesen Fall ohnehin überflüssig.

Wann ein Abgleich wirklich nötig ist, beschreibt [Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren](#).

Typische Fehler beim Tausch und wie du sie löst

Die meisten Probleme beim Zertifikatstausch sind alte Bekannte. Skizze 5 ordnet die häufigsten Symptome ihren Ursachen zu; die Abschnitte darunter liefern die Lösung.



Skizze 5: Die häufigsten Fehlerbilder nach einem Zertifikatstausch und ihre Ursachen.

Privater Schlüssel nicht exportierbar

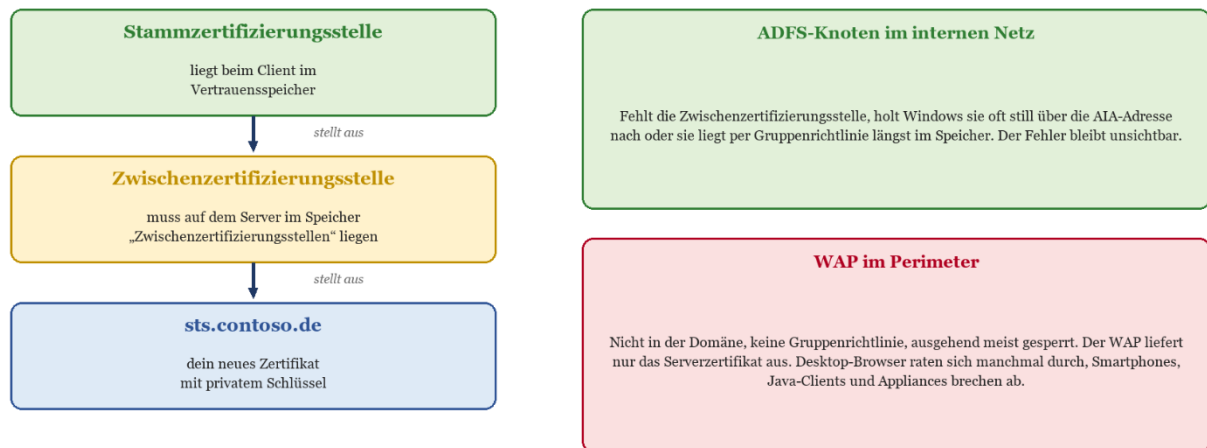
Der Klassiker. Das Zertifikat liegt auf dem Server, auf dem der Antrag erzeugt wurde, und beim Export ist die Option „Ja, privaten Schlüssel exportieren“ ausgegraut. Es gibt Werkzeuge, die den Schlüssel trotzdem aus dem Speicher holen – das ist in einer Produktionsumgebung aber genau die Art Basteln, die ein Sicherheitsaudit später mit hochgezogenen Augenbrauen quittiert. Der saubere Weg: einen neuen Antrag mit exportierbarem Schlüssel erzeugen und bei der Zertifizierungsstelle eine Neuausstellung (Rekey) anfordern. Die meisten öffentlichen Anbieter erlauben das innerhalb der Laufzeit ohne Zusatzkosten.

Kette unvollständig

Intern ist alles grün, extern meldet ein Teil der Geräte einen Zertifikatsfehler. Fast immer fehlt auf den WAP-Servern die Zwischenzertifizierungsstelle. Skizze 4 zeigt, warum das intern nicht auffällt.

Skizze 4: Die Zertifikatskette – und warum der WAP sie zuerst verliert

Der Server muss das Zwischenzertifikat mitliefern; das Stammzertifikat kennt der Client selbst



Merksatz: Die Kette wird mit der PFX exportiert – aber nur, wenn du beim Export „alle Zertifikate im Pfad“ ankreuzt.

Skizze 4: Die Zertifikatskette. Der Server muss das Zwischenzertifikat mitliefern, sonst scheitern strenge Clients.

Die Lösung: Das Zwischenzertifikat deiner Zertifizierungsstelle auf jedem WAP-Server in den Speicher „Zwischenzertifizierungsstellen“ des Computers importieren und den Dienst neu starten. Beim Export der PFX gleich „Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen“ ankreuzen, dann kommt die Kette beim Import mit. Achtung bei Anbietern, die die Zwischenzertifizierungsstelle gewechselt haben: Das alte Zwischenzertifikat im Speicher hilft beim neuen Serverzertifikat nicht.

Falsches Zertifikat an Port 49443

Die Anmeldung per Benutzername und Kennwort funktioniert, die Smartcard-Anmeldung meldet einen Zertifikatsfehler oder scheitert still. Ursache ist fast immer, dass jemand die Bindung an 443 von Hand oder mit einem veralteten Skript getauscht hat und die Bindung an 49443 noch das alte Zertifikat trägt. Prüfen kannst du das mit `Get-AdfsSslCertificate` auf der Farm, mit `Get-WebApplicationProxySslCertificate` auf dem Proxy und mit dem Testskript von oben. Die Lösung ist, `Set-AdfsSslCertificate` beziehungsweise `Set-WebApplicationProxySslCertificate` erneut auszuführen – die Cmdlets setzen alle Bindungen konsistent. Im alternativen Modus gilt dasselbe für die `certauth`-Bindung; dort fehlt außerdem gern der `certauth`-Name im neuen Zertifikat.

Weitere Stolpersteine auf einen Blick

Symptom	Ursache	Lösung
Set-AdfsSslCertificate findet das Zertifikat nicht	Import fehlt auf einem Knoten oder Fingerabdruck mit unsichtbarem Zeichen kopiert	Fingerabdruck per PowerShell auslesen, Import auf allen Knoten prüfen
Cmdlet bricht mit Remoting-Fehler ab	WinRM zwischen den Knoten gesperrt	TCP 5985 zwischen den ADFS-Servern freigeben, Aufruf wiederholen
ADFS-Dienst startet nach dem Tausch nicht	Dienstkonto darf den privaten Schlüssel des Service-Communications-Zertifikats nicht lesen	Leserecht auf jedem Knoten setzen
Knoten liefern unterschiedliche Zertifikate	Cmdlet lief nur teilweise durch oder alte Farm unter 2012 R2	Get-AdfsSslCertificate auf jedem Knoten prüfen, Aufruf wiederholen
Extern altes Zertifikat,	Load Balancer terminiert TLS oder	Zertifikat auf dem Load Balancer

Server zeigen das neue	hat eigenes Profil	tauschen
Clients ohne SNI erhalten kein Zertifikat	selbst angelegter o.o.o.o-Fallback zeigt noch auf das alte	Fallback-Bindung mit netsh nachziehen

Tabelle 4: Weitere typische Fehler beim SSL-Tausch auf ADFS und WAP.

Wenn nach dem Tausch die Anmeldung trotzdem scheitert und das Zertifikat offensichtlich nicht schuld ist, hilft der Blick in [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#) und in das Admin-Log, wie in [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#) beschrieben.

FAKTEN – Checkliste: ADFS SSL-Zertifikat tauschen

- › Altes Zertifikat analysiert: Antragstellernamen, alle SAN-Einträge, Zwischenzertifizierungsstelle, Ablaufdatum.
- › Neues Zertifikat mit exportierbarem privatem Schlüssel beantragt, alle benötigten Namen enthalten, ECU Serverauthentifizierung.
- › PFX mit vollständiger Kette exportiert und sicher abgelegt – nicht im Freigabeordner „Temp“.
- › Import auf allen ADFS-Knoten und allen WAP-Servern, privater Schlüssel und Kette jeweils geprüft.
- › Bindungsmodus geklärt: Standard (49443) oder alternativ (certauth).
- › Set-AdfsSslCertificate bzw. Set-AdfsAlternateTlsClientBinding auf dem primären Knoten ausgeführt.
- › Set-AdfsCertificate -CertificateType Service-Communications ausgeführt, Leserecht für das Dienstkonto auf jedem Knoten.
- › ADFS-Dienst Knoten für Knoten neu gestartet.
- › Set-WebApplicationProxySslCertificate auf jedem WAP-Server ausgeführt.
- › Veröffentlichte Anwendungen auf den neuen Fingerabdruck umgestellt.
- › Load Balancer geprüft: intern und extern, Profile, Health Checks.
- › Jeden Server einzeln auf 443 und 49443 getestet, danach extern und intern angemeldet.
- › Monitoring und Dokumentation mit neuem Ablaufdatum aktualisiert, Erinnerung für den nächsten Tausch gesetzt.
- › Altes Zertifikat erst nach einer Beobachtungsphase entfernt.

Fazit: Kein Hexenwerk, aber eine Frage der Vollständigkeit

Das ADFS SSL-Zertifikat zu tauschen ist technisch überschaubar: Import, zwei Cmdlets auf der Farm, eines pro Proxy, ein Blick auf die veröffentlichten Anwendungen und den Load Balancer. Schiefgehen tut es fast nie an der Technik, sondern an der Vollständigkeit – ein vergessener Knoten, eine fehlende Zwischenzertifizierungsstelle im Perimeter, ein Port 49443, an den niemand gedacht hat. Wer die Stellen aus Skizze 1 kennt und die Checkliste abarbeitet, erledigt den Tausch in einem entspannten Wartungsfenster.

Und weil öffentliche Zertifikate immer kürzer laufen, wird aus dem jährlichen Ereignis eine regelmäßige Übung. Das ist kein Grund zur Panik und auch kein Argument, ADFS morgen abzuschalten. Es ist ein guter Anlass, das Verfahren einmal sauber aufzuschreiben, zu skripten und im Monitoring zu verankern. Die Farm läuft in vielen Häusern seit über zehn Jahren – sie verdient einen Betrieb, der nicht von einer Kalendererinnerung abhängt, die niemand mehr liest.

Wenn du den Tausch lieber mit Begleitung durchziehst oder gleich das ganze Zertifikatsmanagement der Farm auf den Prüfstand stellen möchtest, unterstützen wir dich im

[Consulting zu ADFS \(Active Directory Federation Services\)](#). Wer den Ablauf einmal gefahrlos im Labor üben will, ist in unseren [ADFS-Schulungen](#) richtig. Und die Hintergründe zu Zertifikaten, Bindungen und Proxy-Vertrauen vertieft das Buch – mehr dazu unter [ADFS in der Praxis – das Buch im Detail](#).

WEITER – Passend zum Thema

- › [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#) – das andere Zertifikat, bei dem die Partner mitspielen müssen
- › [WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will](#) – wenn der WAP nach dem Tausch nicht mehr will
- › [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#) – SNI, Health Probe und warum TLS durchgereicht wird
- › [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#) – vor dem Eingriff eine Sicherung ziehen

FAQ: ADFS SSL-Zertifikat tauschen

Wie tausche ich das SSL-Zertifikat auf einer ADFS-Farm?

Importiere das neue Zertifikat mit privatem Schlüssel auf allen ADFS-Knoten und führe dann auf dem primären Knoten Set-AdfsSslCertificate -Thumbprint mit dem neuen Fingerabdruck aus. Ab Windows Server 2016 aktualisiert das Cmdlet alle Knoten der Farm per PowerShell Remoting. Anschließend setzt du das Service-Communications-Zertifikat mit Set-AdfsCertificate.

Muss ich Set-AdfsSslCertificate auf jedem ADFS-Server ausführen?

Ab Windows Server 2016 mit entsprechendem Farm Behavior Level nicht: Einmal auf dem primären Knoten genügt, sofern WinRM zu den anderen Knoten erreichbar ist. Unter Windows Server 2012 R2 musste das Cmdlet noch auf jedem Server laufen.

Reicht es, das Zertifikat in der AD FS-Verwaltung zu ändern?

Nein. In der Konsole änderst du nur das Service-Communications-Zertifikat. Die HTTPS-Bindungen tauschst du ausschließlich per PowerShell mit Set-AdfsSslCertificate oder im alternativen Bindungsmodus mit Set-AdfsAlternateTlsClientBinding.

Wie tausche ich das Zertifikat auf dem Web Application Proxy?

Zertifikat samt Kette auf jedem WAP-Server importieren und dort Set-WebApplicationProxySslCertificate -Thumbprint ausführen. Danach die veröffentlichten Anwendungen mit Set-WebApplicationProxyApplication auf den neuen Fingerabdruck umstellen, sofern sie dasselbe Zertifikat nutzen.

Was mache ich, wenn das alte Zertifikat auf dem WAP schon abgelaufen ist?

Dann funktioniert Set-WebApplicationProxySslCertificate oft nicht mehr. Konfiguriere den Proxy mit Install-WebApplicationProxy neu, mit dem neuen Fingerabdruck, dem Namen des Federation Service und den Anmeldedaten eines Kontos, das lokaler Administrator auf den ADFS-Servern ist.

Muss ich nach dem SSL-Tausch den Federation Trust in Microsoft 365 aktualisieren?

Nein. Entra ID speichert für die föderierte Domäne das Token-Signing-Zertifikat, nicht das SSL-Zertifikat. Ein SSL-Tausch erfordert keine Änderung an der Domänenkonfiguration.

Warum zeigt Port 49443 noch das alte Zertifikat?

Meist wurde die Bindung an Port 443 von Hand oder mit einem unvollständigen Skript getauscht. Führe Set-AdfsSslCertificate auf der Farm und Set-WebApplicationProxySslCertificate auf den Proxys erneut aus – beide Cmdlets setzen alle Bindungen, auch die für die Benutzerzertifikat-Anmeldung.

Kann ich für ADFS und WAP unterschiedliche Zertifikate verwenden?

Nur eingeschränkt. Ist ExtendedProtectionTokenCheck aktiv, was dem Standard entspricht, oder reicht der Proxy integrierte Windows-Authentifizierung durch, muss der WAP dasselbe Zertifikat mit demselben Schlüssel verwenden wie die Farm. Microsoft empfiehlt grundsätzlich ein gemeinsames Zertifikat.

Braucht das ADFS-Dienstkonto Rechte auf den privaten Schlüssel?

Für die SSL-Bindung nicht, das erledigt Set-AdfsSslCertificate für den Dienstprinzipal adfssrv. Für das Service-Communications-Zertifikat braucht das Dienstkonto dagegen Leserecht auf den privaten Schlüssel, und zwar auf jedem Knoten.

Wann darf ich das alte Zertifikat löschen?

Wenn alle Tests erfolgreich waren und eine Beobachtungsphase ohne Auffälligkeiten hinter dir liegt. Prüfe vorher mit Get-AdfsSslCertificate, Get-WebApplicationProxySslCertificate und der Liste der veröffentlichten Anwendungen, dass nichts mehr auf den alten Fingerabdruck verweist.