

Claims Provider Trust – Partnerorganisationen anbinden



WISSEN

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

› [Active Directory Federation Services](#)

BERATUNG

Partnerföderation planen, Regeln prüfen, zwei Farmen nach einer Übernahme sauber verheiraten.

› [Consulting zu ADFS](#)

SCHULUNG

Zwei Farmen im Labor föderieren – und absichtlich einen Partner-Claim zu viel durchlassen.

› [ADFS-Schulungen](#)

Es beginnt fast immer mit einer Pressemitteilung. Der Konzern hat eine Firma gekauft, der Vorstand spricht von Synergien, und drei Wochen später steht in deinem Postfach: „Die Kolleginnen und Kollegen der Tochter sollen ab Montag die Reisekosten-App und das Intranet nutzen. Mit ihren eigenen Konten, bitte. Und ohne neue Passwörter.“ Die Tochter hat ein eigenes Active Directory, eine eigene ADFS-Farm und eine eigene Meinung darüber, wer hier wen übernommen hat. Ein Forest Trust ist politisch tot, bevor jemand das Wort ausgesprochen hat. Willkommen in der anderen Richtung der Föderation.

Bisher hat deine Farm Tokens an Anwendungen ausgestellt – über Relying Party Trusts. Jetzt soll sie Tokens annehmen, die eine fremde Farm ausgestellt hat. Dafür gibt es den ADFS Claims Provider Trust: Die Partnerorganisation wird zum Anspruchsanbieter, deine Farm zum Übersetzer, und die Anwendung merkt von all dem nichts. Dieser Beitrag zeigt dir, wie du den Partner-IdP einbindest, wie du mit Acceptance Transform Rules kontrollierst, was hereinkommt, wie Home Realm Discovery die Benutzer zum richtigen Anmeldeserver schickt und wie du den Partner auf genau die Anwendungen beschränkst, für die er gedacht ist. Am Ende steht ein vollständiger Praxisfall: ein Konzernverbund mit zwei Farmen. Die Grundlagen zu Farm, Protokollen und Tokens setzen wir voraus – die findest du auf der Übersichtsseite [Active Directory Federation Services](#).

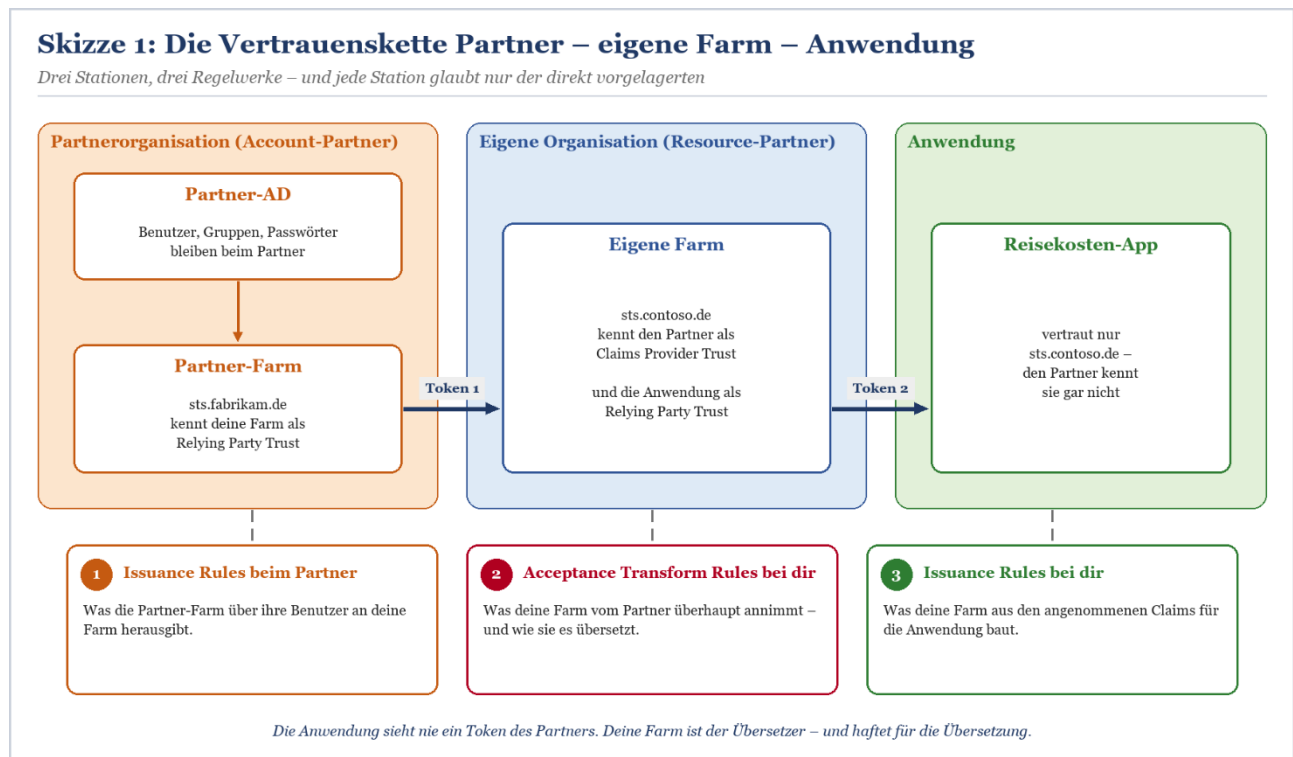
WICHTIG – Zwei Trust-Typen, zwei Richtungen

Ein Relying Party Trust beschreibt, wem deine Farm Tokens ausstellt. Ein Claims Provider Trust beschreibt, von wem sie Tokens annimmt. Für eine Partnerföderation brauchst du immer beides: den Claims Provider Trust auf deiner Seite und einen Relying Party Trust für deine Farm auf der Seite des Partners. Wie ein Relying Party Trust im Detail angelegt wird, steht in [Relying Party Trust anlegen – per Metadaten und von Hand](#).

Die andere Richtung: Was ein Claims Provider Trust leistet

Ein Claims Provider Trust – in der deutschen ADFS-Verwaltung „Anspruchsanbieter-Vertrauensstellung“ – ist der Datensatz, mit dem deine Farm einem fremden Identity Provider glaubt. Er enthält den Bezeichner des Partners, seine Endpunkte, sein Token-Signing-Zertifikat und die Regeln, nach denen deine Farm die eingehenden Claims annimmt. Jede ADFS-Farm hat von Haus aus genau einen davon: „Active Directory“. Das ist der Trust zu deinem eigenen Verzeichnis, und er lässt sich nicht löschen – er ist das Fundament, auf dem alles andere steht.

Fügst du einen zweiten Anspruchsanbieter hinzu, ändert sich die Rolle deiner Farm. Sie ist dann nicht mehr nur Identity Provider für die eigenen Benutzer, sondern zusätzlich Federation Provider: eine Drehscheibe, die Tokens von außen annimmt, prüft, übersetzt und als eigene Tokens an die Anwendungen weitergibt. In der klassischen ADFS-Sprache heißt der Partner mit den Benutzern Account-Partner, die Organisation mit den Anwendungen Resource-Partner. Die Begriffe sind alt, die Logik ist es nicht.



Skizze 1: Die Anwendung vertraut nur deiner Farm, deine Farm vertraut dem Partner – drei Regelwerke entscheiden, was am Ende im Token steht.

Warum die Anwendung den Partner nie kennenlernt

Der eigentliche Charme dieser Konstruktion: Die Anwendung bleibt unverändert. Sie hat einen Relying Party Trust zu deiner Farm, sie prüft die Signatur deiner Farm, und sie bekommt Claims in dem Format, das du ihr beigebracht hast. Ob der Benutzer aus deinem Active Directory stammt oder aus dem der Tochter, sieht sie nur, wenn du es ihr sagst. Das ist bequem – und gefährlich zugleich. Denn wenn deine Farm alles durchreicht, was der Partner schickt, unterschreibt sie mit ihrem eigenen Zertifikat für Behauptungen, die sie nie geprüft hat. Dazu gleich mehr im Kapitel über die Acceptance Transform Rules.

Merkmal	Relying Party Trust	Claims Provider Trust
Richtung	Deine Farm stellt Tokens aus	Deine Farm nimmt Tokens an

Gegenüber	Anwendung oder fremde Farm, die deine Benutzer anmeldet	Fremder IdP, der seine Benutzer anmeldet
Regelwerk	Issuance Transform Rules	Acceptance Transform Rules
Zertifikat des Gegenübers	Optional: Verschlüsselung, Anfrage-Signatur	Pflicht: Token-Signing-Zertifikat des Partners
Cmdlet	Add-AdfsRelyingPartyTrust	Add-AdfsClaimsProviderTrust
Sichtbar für Benutzer	Nein	Ja, als Eintrag auf der Auswahlseite (Home Realm Discovery)
Standardobjekt	Keins – Relying Party Trusts legst du selbst an	„Active Directory“ – nicht löschar

Tabelle 1: Relying Party Trust und Claims Provider Trust im Vergleich.

Was du vom Partner brauchst – und er von dir

Föderation ist ein Tauschgeschäft. Bevor irgendjemand eine Konsole öffnet, sollten beide Seiten wissen, was sie austauschen. Am einfachsten geht das über die Federation-Metadaten, die jede ADFS-Farm unter einem festen Pfad veröffentlicht. Ist der Partner kein ADFS, sondern ein anderes SAML-Produkt, brauchst du dieselben Angaben – nur eben aus dessen Dokumentation oder als XML-Datei per Mail.

Angabe	Du brauchst vom Partner	Der Partner braucht von dir
Metadaten	https://sts.fabrikam.de/FederationMetadata/2007-06/FederationMetadata.xml	https://sts.contoso.de/FederationMetadata/2007-06/FederationMetadata.xml
Bezeichner	Bei ADFS üblich: http://sts.fabrikam.de/adfs/services/trust	http://sts.contoso.de/adfs/services/trust
Protokoll	SAML 2.0 oder WS-Federation – beide Seiten müssen sich einigen	dasselbe
Zertifikat	Token-Signing-Zertifikat des Partners	Optional: dein Verschlüsselungszertifikat
Claims	Liste der Claims, die er senden wird – mit Typ und Beispielwert	Liste der Claims, die du erwartest
Kontakt	Wer kündigt Zertifikatswechsel an, wer ist bei Störung erreichbar?	dasselbe – in beide Richtungen

Tabelle 2: Die Austauschliste. Die Adressen sind Beispiele; sie gelten für ADFS-Standardpfade.

FAKTEN – Der Bezeichner einer ADFS-Farm

Der Federation Service Identifier einer ADFS-Farm lautet standardmäßig <http://<Dienstname>/adfs/services/trust> – mit http, nicht https. Das ist kein Tippfehler, sondern ein Bezeichner, keine Adresse. Wer ihn in einem manuell angelegten Trust „korrigiert“, sucht danach sehr lange nach einem Fehler, den er selbst eingebaut hat. Den tatsächlichen Wert deiner Farm zeigt (Get-AdfsProperties).Identifier.

Den Claims Provider Trust anlegen – Konsole und PowerShell

In der ADFS-Verwaltung findest du den Assistenten unter „Anspruchsanbieter-Vertrauensstellungen“ und dort „Anspruchsanbieter-Vertrauensstellung hinzufügen“. Er bietet dieselben drei Wege wie beim Relying Party Trust: Metadaten-URL, Metadaten-Datei oder manuelle Eingabe. Wenn der Partner eine erreichbare Metadaten-URL hat, nimm sie. Der Grund steht im Warnkasten weiter unten und hat mit Zertifikaten zu tun, die immer genau dann ablaufen, wenn niemand hinsieht.

Per Metadaten-URL – der Normalfall

```
# Auf einem primären ADFS-Server der eigenen Farm (sts.contoso.de)
Add-AdfsClaimsProviderTrust `
  -Name "Fabrikam (Tochter)" `
  -MetadataUrl "https://sts.fabrikam.de/FederationMetadata/2007-06/FederationMetadata.xml" `
  -MonitoringEnabled $true `
  -AutoUpdateEnabled $true `
  -Notes "Tochter seit 2026, Ansprechpartner IAM-Team Fabrikam, Ticket CHG-0815"

# Kontrolle: Was hat ADFS aus den Metadaten übernommen?
Get-AdfsClaimsProviderTrust -Name "Fabrikam (Tochter)" |
  Format-List Name, Identifier, ProtocolProfile, Enabled, MonitoringEnabled,
  AutoUpdateEnabled,
  LastMonitoredTime, LastPublishedPolicyCheckSuccessful, TokenSigningCertificates
```

Listing 1: Claims Provider Trust über die Metadaten der Partner-Farm anlegen und prüfen.

Der Name, den du hier vergibst, ist nicht nur Verwaltungsetikett. Er erscheint später als Auswahl auf der Anmeldeseite, und er ist der Wert, mit dem du den Partner in Relying Party Trusts referenzierst. „Fabrikam (Tochter)“ ist also eine bessere Wahl als „CPT_Test_neu_final2“ – auch wenn Letzteres ehrlicher wäre.

Per Datei oder von Hand – wenn der Partner nichts veröffentlicht

Manche Partner veröffentlichen ihre Metadaten nicht ins Internet, oder deine Farm darf sie wegen der Ausgangsfirewall nicht abrufen. Dann bekommst du die XML-Datei per Mail und importierst sie mit -MetadataFile. Fehlen auch die Metadaten, legst du den Trust manuell an. Pflicht sind dann Name, Bezeichner und das Token-Signing-Zertifikat des Partners; dazu kommt der Endpunkt, an den deine Farm die Benutzer zur Anmeldung schickt.

```
# Variante 1: Metadaten-Datei des Partners importieren
Add-AdfsClaimsProviderTrust -Name "Fabrikam (Tochter)" -MetadataFile "C:\Temp\fabrikam-
metadata.xml"

# Variante 2: vollständig von Hand (SAML 2.0)
$cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("C:\Temp\fabrikam-signing.cer")
$ssso = New-AdfsSamlEndpoint -Binding "POST" -Protocol "SAMLSingleSignOn" `
  -Uri "https://sts.fabrikam.de/adfs/ls/"

Add-AdfsClaimsProviderTrust `
  -Name "Fabrikam (Tochter)" `
  -Identifier "http://sts.fabrikam.de/adfs/services/trust" `
  -TokenSigningCertificate $cert `
  -ProtocolProfile "SAML" `
  -SamlEndpoint $ssso
```

Listing 2: Import aus Datei und manuelle Anlage. New-AdfsSamlEndpoint erzeugt das Endpunktojekt.

WARNUNG – Das Zertifikat des Partners ist dein Problem

Tauscht der Partner sein Token-Signing-Zertifikat, lehnt deine Farm ab diesem Moment jedes seiner Tokens ab. Mit Metadaten-URL, Überwachung und automatischer Aktualisierung zieht deine Farm das neue Zertifikat selbst nach – sofern sie die URL erreicht. Bei einer importierten Datei oder einem manuellen Trust erfährst du vom Wechsel meist am Montagmorgen durch die Hotline. Vereinbare deshalb, dass der Partner Wechsel ankündigt, und lies, wie der Rollover auf ADFS-Seite funktioniert: [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#).

Die Gegenseite: Deine Farm als Relying Party beim Partner

Damit die Partner-Farm überhaupt Tokens für deine Farm ausstellt, muss sie dich als Relying Party Trust kennen. Das ist Aufgabe des Partners, aber du solltest wissen, was er tun muss – schon weil er dich anrufen wird, wenn es nicht klappt. Auf einer ADFS-Farm sieht das so aus:

```
# Auf der Partner-Farm (sts.fabrikam.de) – erledigt das Team des Partners
Add-AdfsRelyingPartyTrust `
  -Name "Konzern-Farm contoso" `
  -MetadataUrl "https://sts.contoso.de/FederationMetadata/2007-06/FederationMetadata.xml" `
  -MonitoringEnabled $true -AutoUpdateEnabled $true `
  -AccessControlPolicyName "Permit everyone"

# Was der Partner herausgibt, bestimmt er selbst – hier: UPN, Name und Gruppen
$rules = @'
@RuleName = "UPN, Anzeigenname und Gruppen an den Konzern"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
  Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory",
  types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name",
    "http://schemas.xmlsoap.org/claims/Group"),
  query = ";userPrincipalName,displayName,tokenGroups;{0}", param = c.Value);
'@
Set-AdfsRelyingPartyTrust -TargetName "Konzern-Farm contoso" -IssuanceTransformRules $rules
```

Listing 3: So sieht die Gegenseite aus, wenn der Partner ebenfalls ADFS betreibt.

Beachte die Arbeitsteilung: Der Partner entscheidet, welche Daten seine Organisation verlassen. Du entscheidest, welche davon deine Farm glaubt. Beides ist legitim, und beides gehört in eine schriftliche Absprache – nicht nur wegen des Datenschutzes, sondern weil sich in zwei Jahren niemand mehr erinnert, warum die Gruppen eigentlich mitgeschickt werden.

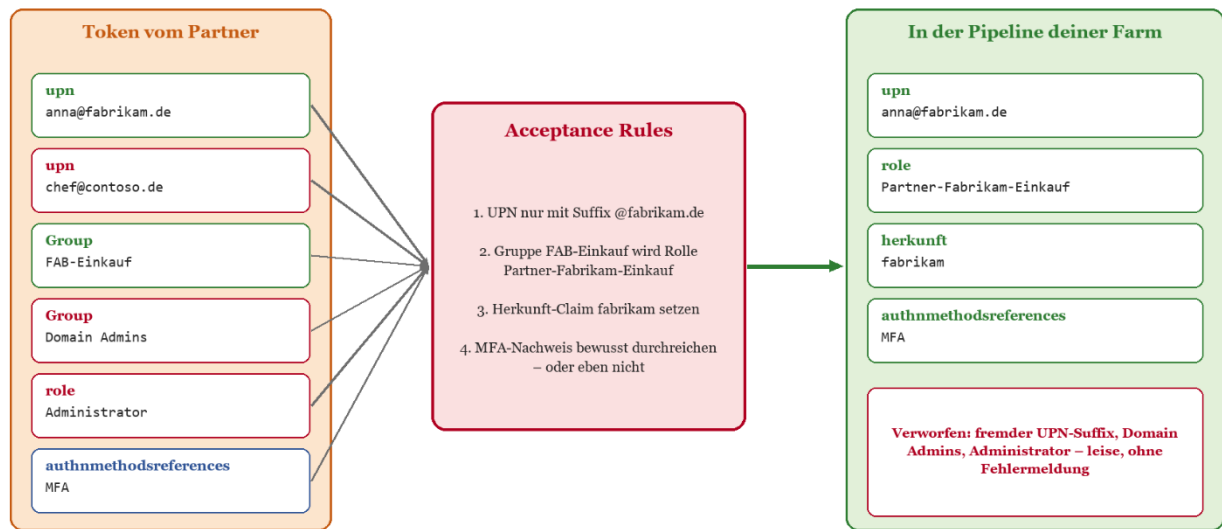
Acceptance Transform Rules – der Türsteher deiner Farm

Die Acceptance Transform Rules, in der Konsole über „Anspruchsregeln bearbeiten“ am Claims Provider Trust erreichbar, sind die erste Station, die ein Partner-Token in deiner Farm durchläuft. Sie entscheiden, welche der eingehenden Claims in die Claims-Pipeline gelangen und in welcher Form. Alles, was keine Regel ausdrücklich ausstellt, ist danach verschwunden – die Issuance Rules deiner Anwendungen sehen es nie.

Daraus ergeben sich die zwei klassischen Fehler. Erstens: Ein frisch angelegter Partner-Trust hat in der Regel keine Annahmeregeln. Der Benutzer meldet sich beim Partner erfolgreich an, kommt mit einem prall gefüllten Token zurück – und deine Farm wirft alles weg. Die Anwendung bekommt einen Benutzer ohne Eigenschaften und lehnt ihn ab. Zweitens, und das ist der gefährlichere: Jemand behebt den ersten Fehler mit einer Regel „Alle Claims durchreichen“. Ab jetzt glaubt deine Farm dem Partner alles.

Skizze 2: Acceptance Transform Rules als Türsteher

Was nicht ausdrücklich angenommen wird, existiert für deine Farm nicht



Ohne Regeln kommt gar nichts durch. Mit „alles durchreichen“ kommt alles durch. Beides ist falsch.

Skizze 2: Die Annahmeregeln lassen nur durch, was ausdrücklich erlaubt ist – und übersetzen Partner-Gruppen in eigene Rollen.

Warum „alles durchreichen“ ein Sicherheitsproblem ist

Stell dir vor, ein Administrator der Tochter – oder jemand, der dessen Konto übernommen hat – ändert eine Issuance Rule auf der Partner-Farm. Ab sofort schickt sie für einen beliebigen Benutzer den UPN „chef@contoso.de“ und die Rolle „Administrator“. Reicht deine Farm das ungeprüft durch, signiert sie ein Token, in dem ein fremder Benutzer als dein Geschäftsführer auftritt. Die Anwendung hat keine Chance, das zu bemerken: Die Signatur stammt ja von deiner Farm. Der Partner kann sich über eine Partnerföderation also genau so viele Rechte verschaffen, wie deine Annahmeregeln ihm erlauben. Nicht mehr – aber auch nicht weniger.

WARNUNG – Die drei Regeln, die jeder Partner-Trust braucht

1. Identität nur mit dem Suffix des Partners annehmen. Ein UPN mit deinem eigenen Suffix hat in einem Partner-Token nichts verloren.
2. Keine Rollen- oder Gruppen-Claims im Original durchreichen, sondern gezielt in eigene, eindeutig benannte Werte übersetzen – nie in Namen, die auch eigene Gruppen tragen.
3. Einen Herkunfts-Claim setzen, damit deine Issuance Rules und Zugriffsrichtlinien Partnerbenutzer zuverlässig erkennen.

Ein belastbares Regelwerk für den Partner

```
$acceptance = @'
@RuleName = "UPN nur mit Partner-Suffix annehmen"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn",
  Value =~ "(?i)^[^@]+\@fabrikam\.de$"]
=> issue(claim = c);

@RuleName = "Anzeigenamen annehmen"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"]
=> issue(claim = c);

@RuleName = "Partnergruppe Einkauf in eigene Rolle übersetzen"
```

```

c:[Type == "http://schemas.xmlsoap.org/claims/Group", Value == "FAB-Einkauf"]
=> issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/role",
        Value = "Partner-Fabrikam-Einkauf");

@RuleName = "Herkunft markieren"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn",
    Value =~ "(?i)^[^@]+@fabrikam\.de$"]
=> issue(Type = "https://contoso.de/claims/herkunft", Value = "fabrikam");
'@

Set-AdfsClaimsProviderTrust -TargetName "Fabrikam (Tochter)" -AcceptanceTransformRules
$acceptance

# Kontrolle
(Get-AdfsClaimsProviderTrust -Name "Fabrikam (Tochter)").AcceptanceTransformRules
  
```

Listing 4: Annahmeregeln mit Suffix-Prüfung, Rollenübersetzung und Herkunfts-Claim. Der Claim-Typ für die Herkunft ist frei gewählt.

Der Herkunfts-Claim ist der unscheinbarste Teil, aber der nützlichste. Mit ihm kannst du in den Issuance Rules jeder Anwendung sauber unterscheiden, ob ein Benutzer aus dem eigenen Verzeichnis oder vom Partner kommt – ohne dich auf Suffixe zu verlassen, die sich nach der nächsten Umfirmierung ändern. Die Syntax der Regelsprache, die Unterschiede zwischen issue und add und die Regex-Fallen erklärt der [ADFS Claim Rules Leitfaden](#) ausführlich.

Aspekt	Acceptance Transform Rules	Issuance Transform Rules
Wo	Am Claims Provider Trust	Am Relying Party Trust
Wann	Direkt nach Eingang des Partner-Tokens	Bevor deine Farm das Token für die Anwendung baut
Wirkung	Gilt für alle Anwendungen, die dieser Partner nutzt	Gilt nur für diese eine Anwendung
Typischer Inhalt	Filtern, normalisieren, Herkunft markieren	Anwendungsspezifisches Format, NameID, Rollen
Fehler wirkt sich aus auf	Den ganzen Partner	Eine Anwendung
Für den AD-Trust	Vorgegebene Standardregeln – ändere sie nur mit gutem Grund	Wie bei Partnern

Tabelle 3: Annahme- und Ausstellungsregeln im Vergleich.

TIPP – MFA des Partners bewusst behandeln

Hat der Benutzer sich beim Partner mit MFA angemeldet, steht das im Claim `http://schemas.microsoft.com/claims/authnmethodsreferences`. Reichst du ihn in den Annahmeregeln durch, können deine Zugriffsrichtlinien ihn auswerten – du vertraust damit aber der MFA-Umsetzung des Partners. Reichst du ihn nicht durch, verlangt eine MFA-pflichtige Richtlinie bei dir eine eigene zweite Anmeldung. Beides ist vertretbar, nur unbewusst sollte es nicht passieren. Wie MFA auf deiner Farm angebunden ist, steht in [ADFS mit Entra-MFA koppeln – Adapter, Zertifikat und Fallstricke](#).

Home Realm Discovery und die Beschränkung auf bestimmte Anwendungen

Sobald deine Farm mehr als einen Anspruchsanbieter kennt, hat sie ein Problem: Ein Benutzer ruft die Reisekosten-App auf, die App schickt ihn zu `sts.contoso.de` – und die Farm weiß nicht, ob er sich am eigenen Active Directory oder bei der Tochter anmelden muss. Diese Frage zu beantworten heißt Home Realm Discovery. Ohne weitere Konfiguration beantwortet ADFS sie, indem es den Benutzer fragt: Es zeigt eine Auswahlseite mit den Anzeigenamen aller Anspruchsanbieter. Für die

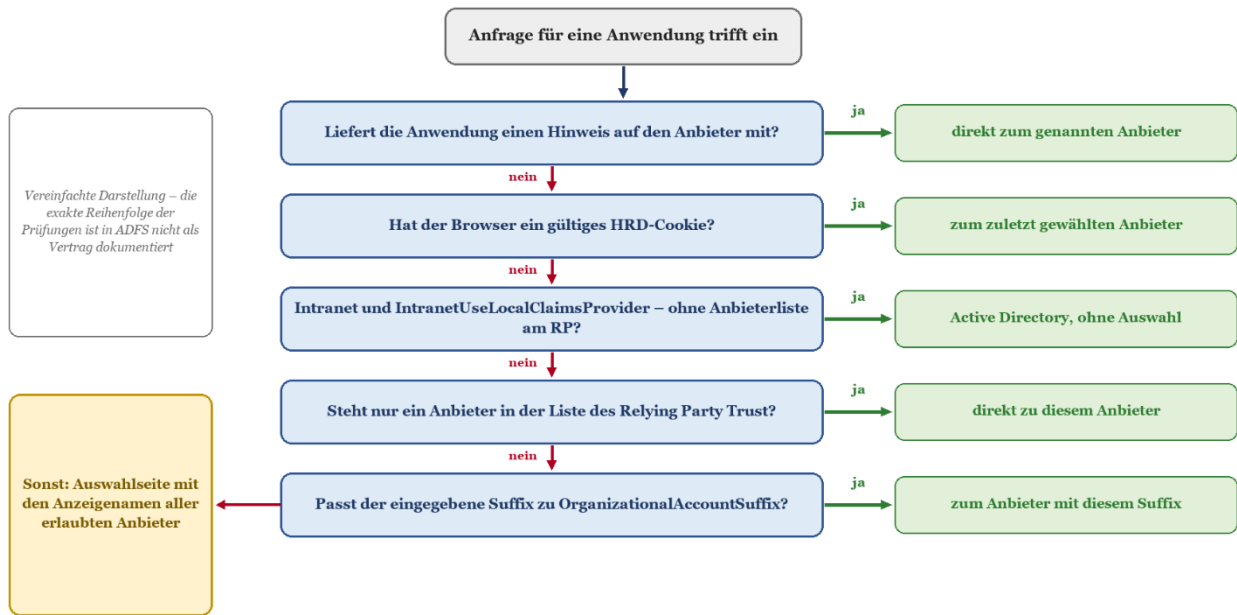
Tochter-Benutzer ist das in Ordnung. Für die zwanzigtausend Konzern-Benutzer, die ab Montag bei jeder Anmeldung eine Frage beantworten müssen, die sie nicht verstehen, eher nicht.

FAKTEN – Der Anzeigename von „Active Directory“

Auf der Auswahlseite erscheint für das eigene Active Directory nicht „Active Directory“, sondern der Anzeigename des Federation Service. Wer dort beim Einrichten der Farm „ADFS-Test“ eingetragen hat, sieht diesen Namen jetzt vor zwanzigtausend Benutzern wieder. Ändern lässt er sich mit Set-AdfsProperties -DisplayName.

Skizze 3: Wie ADFS entscheidet, wohin der Benutzer zur Anmeldung muss

Home Realm Discovery – von oben nach unten, die erste zutreffende Regel gewinnt



Skizze 3: Die Werkzeuge der Home Realm Discovery – jedes davon erspart einer Gruppe von Benutzern die Auswahlseite.

Die Werkzeuge im Überblick

Werkzeug	Wirkung	Konfiguration
Anbieterliste am Relying Party Trust	Die Anwendung zeigt nur die genannten Anbieter; steht nur einer drin, entfällt die Auswahl	Set-AdfsRelyingPartyTrust - ClaimsProviderName
Organisations-Suffix	Benutzer tippt seine Adresse ein, ADFS wählt den Anbieter anhand des Suffixes	Set-AdfsClaimsProviderTrust - OrganizationalAccountSuffix
Intranet direkt an AD	Interne Zugriffe gehen ohne Auswahl ans eigene AD	Set-AdfsProperties - IntranetUseLocalClaimsProvider \$true
HRD-Cookie	Der Browser merkt sich die letzte Auswahl; Lebensdauer in Tagen	Set-AdfsWebConfig - HRDCookieEnabled / - HRDCookieLifetime
Hinweis der Anwendung	Die Anwendung nennt den Anbieter bereits in der Anfrage, etwa per whr-Parameter bei WS-Federation	In der Anwendung, nicht in ADFS
Weitergabe von Hinweisen	ADFS leitet prompt- und login_hint-Parameter an eine Partner-Farm weiter	Set-AdfsClaimsProviderTrust - PromptLoginFederation

Tabelle 4: Werkzeuge der Home Realm Discovery und wo du sie einstellst.

```
# Benutzer der Tochter anhand ihres Suffixes erkennen
Set-AdfsClaimsProviderTrust -TargetName "Fabrikam (Tochter)" `
```

```
-OrganizationalAccountSuffix @"fabrikam.de")

# Interne Zugriffe ohne Auswahlseite direkt an das eigene AD
Set-AdfsProperties -IntranetUseLocalClaimsProvider $true

# Bei ADFS-zu-ADFS-Föderation Hinweise an die Partner-Farm weiterreichen
Set-AdfsClaimsProviderTrust -TargetName "Fabrikam (Tochter)" `
    -PromptLoginFederation ForwardPromptAndHintsOverWsFederation

# Aktuelle HRD-Cookie-Einstellung prüfen
Get-AdfsWebConfig | Format-List HRDCookieEnabled, HRDCookieLifetime
```

Listing 5: Home Realm Discovery für den Partner einstellen.

WICHTIG – IntranetUseLocalClaimsProvider und Anbieterlisten vertragen sich nur mit AD in der Liste

Microsoft weist ausdrücklich darauf hin: Hat ein Relying Party Trust eine eigene Anbieterliste, zeigt ADFS die Auswahlseite auch im Intranet – trotz IntranetUseLocalClaimsProvider. Damit interne Benutzer sie überspringen, muss „Active Directory“ in der Liste dieses Relying Party Trust stehen. Wer das übersieht, bekommt Tickets von Kolleginnen und Kollegen, die im Büro plötzlich gefragt werden, aus welcher Firma sie kommen.

Den Partner auf bestimmte Anwendungen beschränken

Ein Claims Provider Trust gilt zunächst farmweit. Jeder Relying Party Trust ohne eigene Anbieterliste bietet ihn an – also auch die Personalverwaltung, das Controlling-Portal und die Testanwendung, die seit 2019 niemand mehr anfasst. Das willst du nicht. Die erste Verteidigungslinie ist deshalb die Anbieterliste am Relying Party Trust: Nur Anwendungen, in deren Liste der Partner steht, bieten ihn an. Für alle anderen setzt du die Liste ausdrücklich auf „Active Directory“.

```
# Anwendungen, die der Partner nutzen darf
Set-AdfsRelyingPartyTrust -TargetName "Reisekosten" -ClaimsProviderName @"(Active
Directory", "Fabrikam (Tochter)")
Set-AdfsRelyingPartyTrust -TargetName "Intranet (SharePoint)" -ClaimsProviderName @"(Active
Directory", "Fabrikam (Tochter)")

# Alle übrigen Anwendungen ausdrücklich auf das eigene AD festnageln
$erlaubt = "Reisekosten", "Intranet (SharePoint)"
Get-AdfsRelyingPartyTrust | Where-Object { $_.Name -notin $erlaubt } | ForEach-Object {
    Set-AdfsRelyingPartyTrust -TargetName $_.Name -ClaimsProviderName @"(Active Directory")
}

# Bestandsaufnahme: leere Liste bedeutet "alle Anbieter"
Get-AdfsRelyingPartyTrust | Select-Object Name, @{n="Anbieter"; e={ $_.ClaimsProviderName -join
    ", " }}
```

Listing 6: Anbieterlisten setzen und kontrollieren. Teste die Schleife zuerst mit -WhatIf.

Die Anbieterliste ist allerdings eine Frage der Benutzerführung, nicht der Autorisierung. Sie entscheidet, was auf der Auswahlseite steht. Die zweite Verteidigungslinie gehört deshalb in die Zugriffssteuerung der Anwendung selbst: Eine Access Control Policy oder eine Issuance Authorization Rule, die Partnerbenutzer – erkennbar am Herkunfts-Claim – nur dort zulässt, wo sie hingehören. Wie du das ohne Regelakrobatik baust, steht in [Access Control Policies in ADFS – Zugriffsregeln ohne Claim-Rule-Akrobatik](#). Beide Linien zusammen ergeben eine Konfiguration, die auch dann hält, wenn jemand in einem Jahr eine Anbieterliste versehentlich leert.

TIPP – Neue Relying Party Trusts nicht vergessen

Jeder neu angelegte Relying Party Trust beginnt mit leerer Anbieterliste und bietet damit alle Partner an. Nimm „-ClaimsProviderName @"(Active Directory)"“ in deine Vorlage für neue Trusts auf und

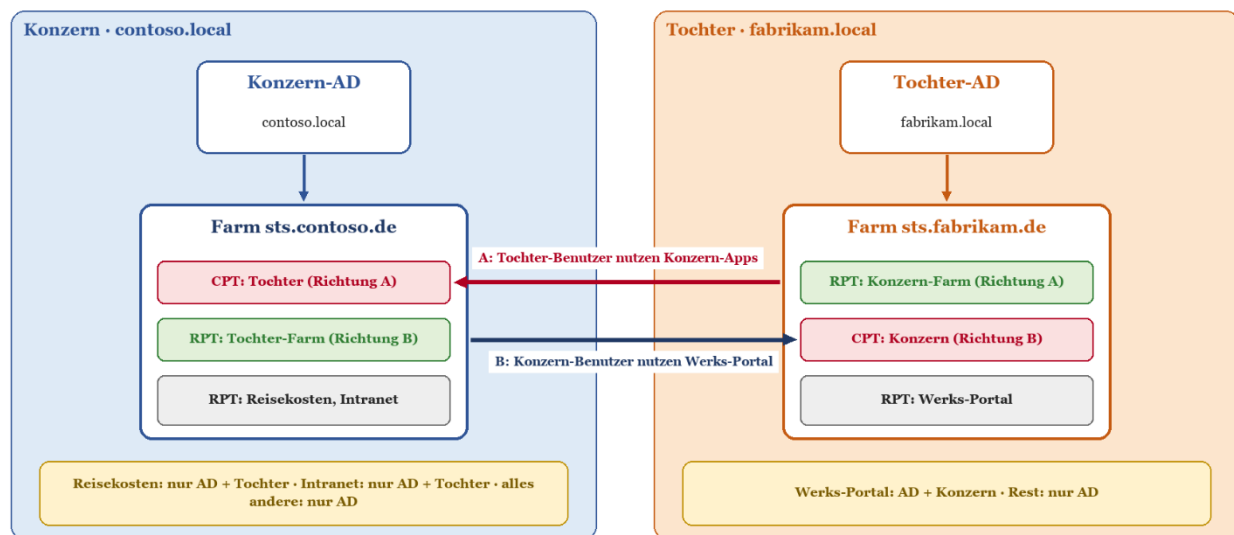
prüfe die Listen bei der regelmäßigen Bestandsaufnahme mit – wie sie aussieht, zeigt [Relying Parties inventarisieren](#) – die Bestandsaufnahme vor der Entra-Migration.

Praxisfall: Konzernverbund mit zwei Farmen

Zurück zur Pressemitteilung. Der Konzern betreibt seine Farm sts.contoso.de für das Verzeichnis contoso.local, die übernommene Tochter ihre eigene Farm sts.fabrikam.de für fabrikam.local. Beide Farmen laufen seit Jahren stabil, beide Teams möchten ihre Farm behalten, und die Anforderung kommt – wie das bei Übernahmen so ist – in zwei Wellen: zuerst sollen die Tochter-Benutzer zwei Konzernanwendungen nutzen, ein halbes Jahr später die Konzern-Einkäufer das Werks-Portal der Tochter. Die Konten bleiben, wo sie sind. Kein Forest Trust, keine Synchronisation, keine Schattenkonten.

Skizze 4: Praxisfall Konzernverbund – zwei Farmen, zwei Richtungen

Jede Richtung braucht ein eigenes Paar: Claims Provider Trust auf der einen, Relying Party Trust auf der anderen Seite



Kein Gesamtvertrauen, kein Forest Trust, keine Kontensynchronisation – nur Tokens, die an genau definierten Stellen angenommen werden.

Skizze 4: Zwei Farmen, zwei Richtungen – jede Richtung ist ein eigenes Paar aus Claims Provider Trust und Relying Party Trust.

Der Ablauf in sechs Schritten

Schritt	Wo	Was	Prüfung
1	Beide Farmen	Metadaten gegenseitig erreichbar machen: DNS, Firewall, Proxy, TLS	Metadaten-URL des Partners vom ADFS-Server aus im Browser öffnen
2	Tochter-Farm	Relying Party Trust „Konzern-Farm contoso“ mit Issuance Rules für UPN, Name, Gruppen	Get-AdfsRelyingPartyTrust auf der Tochter-Farm
3	Konzern-Farm	Claims Provider Trust „Fabrikam (Tochter)“ mit Überwachung anlegen	LastPublishedPolicyCheckSuccessful
4	Konzern-Farm	Annahmeregeln: Suffix-Prüfung, Rollenübersetzung, Herkunfts-Claim	Testanmeldung, Token mit Claims-Viewer-Anwendung prüfen
5	Konzern-Farm	Anbieterlisten: Partner nur an Reisekosten und Intranet, alle anderen nur AD	Listing 6, Bestandsaufnahme
6	Konzern-Farm	HRD: Suffix fabrikam.de, IntranetUseLocalClaimsProvider,	Anmeldung aus Intranet, Extranet und mit Tochter-Konto

Anzeigename prüfen

Tabelle 5: Richtung A – Tochter-Benutzer an Konzernanwendungen. Richtung B läuft spiegelbildlich.

Richtung B ist exakt dasselbe in Grün: Die Tochter-Farm bekommt einen Claims Provider Trust „Konzern contoso“, die Konzern-Farm einen Relying Party Trust für die Tochter-Farm, und die Tochter beschränkt den Konzern auf ihr Werks-Portal. Wichtig ist nur, die beiden Richtungen nicht zu vermischen. Der Relying Party Trust, den die Konzern-Farm in Richtung B für die Tochter anlegt, ist ein völlig anderes Objekt als der Claims Provider Trust aus Richtung A – auch wenn beide auf dieselbe Metadaten-URL zeigen. Benenne sie so, dass man es sieht.

Die Stolpersteine, die wir in solchen Projekten immer wieder sehen

- Das Intranet läuft auf SharePoint Server. Dort reicht es nicht, den Partner in ADFS freizuschalten – der Trusted Identity Token Issuer in SharePoint muss mit den Claims umgehen können, die deine Farm für Partnerbenutzer ausstellt, und die Berechtigungen müssen auf Rollen statt auf AD-Gruppen basieren.
- Überlappende Suffixe. Bekommt die Tochter im Zuge der Umfirmierung zusätzlich Adressen mit contoso.de, kollidiert die Suffix-Prüfung mit dem eigenen Verzeichnis. Kläre die Namensplanung, bevor sie dir den Herkunfts-Claim unbrauchbar macht.
- Gleichnamige Gruppen. Beide Firmen haben eine Gruppe „Einkauf“. Wer Partnergruppen ungeprüft als Rolle durchreicht, gibt den Tochter-Einkäufern die Rechte der Konzern-Einkäufer. Genau dafür übersetzt Listing 4 in eindeutig benannte Rollen.
- Abmeldung. Eine Abmeldung in der Konzernanwendung beendet nicht automatisch die Sitzung bei der Tochter-Farm. Wer Single Logout über zwei Farmen erwartet, sollte das früh testen – und die Erwartung im Zweifel herunterschrauben.
- Zertifikatswechsel ohne Absprache. Die Tochter erneuert ihr Token-Signing-Zertifikat, die Konzern-Farm erreicht die Metadaten-URL wegen einer neuen Proxy-Regel nicht mehr, und die automatische Aktualisierung läuft ins Leere. Die Überwachung meldet das – wenn jemand das Admin-Log liest.

Symptom	Wahrscheinliche Ursache	Erste Prüfung
Partnerbenutzer wird nach erfolgreicher Anmeldung abgewiesen	Keine oder zu strenge Annahmeregeln	AcceptanceTransformRules am Claims Provider Trust
Fehlermeldung direkt nach Rückkehr vom Partner	Signatur ungültig, Partner hat Zertifikat gewechselt	TokenSigningCertificates mit den aktuellen Metadaten des Partners vergleichen
Partner bekommt Fehlermeldung, keine Anmeldeseite	Deine Farm ist beim Partner nicht als Relying Party Trust bekannt	Bezeichner deiner Farm im Trust des Partners
Konzern-Benutzer sehen plötzlich eine Auswahlseite	Anbieterliste am Relying Party Trust ohne Active Directory oder leer	ClaimsProviderName des betroffenen Relying Party Trust
Partner taucht bei einer Anwendung auf, bei der er nichts zu suchen hat	Leere Anbieterliste – neuer Trust ohne Vorlage	Bestandsaufnahme mit Listing 6

Tabelle 6: Fehlerbilder in der Partnerföderation und wo du zuerst nachsiehst.

Für die genauere Diagnose helfen das Admin-Log und das Debug-Tracing der ADFS-Server; wie du die Einträge liest, ohne in ihnen zu ertrinken, zeigt [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#). Die allgemeinen Ursachen fehlgeschlagener Anmeldungen hat [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#) zusammengetragen.

FAKTEN — Und wenn einer der Partner ADFS ablöst?

Eine Partnerföderation ist kein Hindernis für den späteren Umzug nach Entra ID – sie muss nur mitgedacht werden. Zieht die Tochter nach Entra ID um, kann ihr Tenant weiterhin als SAML-Identity-Provider auftreten; der Claims Provider Trust auf deiner Seite zeigt dann auf neue Metadaten, die Annahmeregeln bleiben. Ziehen dagegen deine Anwendungen um, übernehmen andere Mechanismen die Rolle des Federation Providers, etwa die Zusammenarbeit über mandantenübergreifende Zugriffseinstellungen. Den größeren Rahmen beschreibt der Themenbereich [Microsoft Entra ID](#).

Fazit: Fremde Benutzer, eigene Regeln

Ein Claims Provider Trust ist technisch in fünf Minuten angelegt. Die eigentliche Arbeit steckt in den Entscheidungen drumherum: welche Claims deine Farm annimmt, wie sie Partnerbenutzer kennzeichnet, welche Anwendungen den Partner überhaupt anbieten und wie die eigenen Benutzer von all dem nichts merken. Wer die Annahmeregeln als Türsteher versteht und nicht als Durchreiche, wer die Anbieterlisten pflegt und die Herkunft markiert, hat eine Partnerföderation, die ruhig läuft – auch dann noch, wenn die Pressemitteilung längst vergessen ist und das nächste Unternehmen gekauft wird.

ADFS kann das seit vielen Jahren zuverlässig, und in vielen Konzernverbünden ist genau diese Konstruktion der Kitt zwischen Gesellschaften, die technisch nie zusammengewachsen sind. Wenn du eine solche Föderation planst, einen gewachsenen Bestand an Partnern aufräumen oder die Föderation in einen Ausstiegsplan einbinden willst, unterstützen wir dich im [Consulting zu ADFS \(Active Directory Federation Services\)](#). Wer zwei Farmen lieber erst im Labor miteinander verheiratet, ist in den [ADFS-Schulungen](#) richtig. Und die Föderation mit Partnern, die Regelsprache und die Rolle der Farm als Federation Provider vertieft das Buch – mehr dazu unter [ADFS in der Praxis – das Buch im Detail](#).

WEITER – Passend zum Thema

- › [ADFS Claim Rules Leitfaden](#) – die Regelsprache hinter Annahme und Ausstellung
- › [Relying Party Trust anlegen – per Metadaten und von Hand](#) – die Gegenseite jeder Partnerföderation
- › [Access Control Policies in ADFS – Zugriffsregeln ohne Claim-Rule-Akrobatik](#) – Partnerbenutzer gezielt zulassen
- › [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#) – warum Vertrauen in fremde Tokens ein Sicherheitsthema ist
- › [ADFS-Anmeldeseite anpassen – Logo, Texte, Hilfelinks](#) – die Auswahlseite für Partner verständlich gestalten
- › [SharePoint Server mit ADFS – SAML-Authentifizierung einrichten](#) – wenn das Intranet auch Partnerbenutzer bedienen soll

FAQ: ADFS Claims Provider Trust und Partnerföderation

Was ist ein Claims Provider Trust in ADFS?

Die Vertrauensstellung, mit der deine Farm Tokens eines fremden Identity Providers annimmt. Der Partner meldet seine Benutzer an, deine Farm prüft und übersetzt die Claims und stellt den Anwendungen ein eigenes Token aus.

Was ist der Unterschied zwischen Claims Provider Trust und Relying Party Trust?

Ein Relying Party Trust beschreibt, wem deine Farm Tokens ausstellt, ein Claims Provider Trust, von wem sie Tokens annimmt. Für eine Partnerföderation brauchst du beides – den einen bei dir, den anderen beim Partner.

Wie lege ich einen Claims Provider Trust per PowerShell an?

Mit `Add-AdfsClaimsProviderTrust`. Für den Import genügen `-Name` und `-MetadataUrl` oder `-MetadataFile`; manuell brauchst du `-Name`, `-Identifier` und `-TokenSigningCertificate` sowie einen Endpunkt.

Warum kommen nach der Anmeldung beim Partner keine Claims an?

Weil der Claims Provider Trust keine passenden Acceptance Transform Rules hat. Alles, was keine Annahmeregeln ausdrücklich ausstellt, verwirft deine Farm.

Darf ich in den Annahmeregeln einfach alle Claims durchreichen?

Technisch ja, sinnvoll nein. Deine Farm signiert dann alles, was der Partner behauptet – auch einen UPN mit deinem eigenen Suffix oder eine Administratorrolle. Nimm nur an, was du brauchst, und prüfe Suffixe.

Wie verhindere ich, dass meine Benutzer die Auswahlseite sehen?

Mit `IntranetUseLocalClaimsProvider` für interne Zugriffe, mit Anbieterlisten an den Relying Party Trusts, mit Organisations-Suffixen am Partner-Trust und mit dem HRD-Cookie, das die letzte Auswahl speichert.

Wie beschränke ich einen Partner auf bestimmte Anwendungen?

Mit `Set-AdfsRelyingPartyTrust -ClaimsProviderName`: Nur Anwendungen, in deren Liste der Partner steht, bieten ihn an. Zusätzlich sollte die Zugriffssteuerung der Anwendung Partnerbenutzer anhand eines Herkunfts-Claims prüfen.

Was bedeutet eine leere Anbieterliste am Relying Party Trust?

Die Anwendung bietet alle aktivierten Anspruchsanbieter an. Das ist der Standard bei jedem neu angelegten Relying Party Trust – und der häufigste Grund, warum ein Partner plötzlich bei Anwendungen auftaucht.

Was passiert, wenn der Partner sein Token-Signing-Zertifikat erneuert?

Mit Metadaten-URL, Überwachung und automatischer Aktualisierung übernimmt deine Farm das neue Zertifikat selbst. Ohne diese Einstellungen musst du es manuell nachtragen, sonst scheitern alle Anmeldungen des Partners.

Muss der Partner selbst ADFS betreiben?

Nein. Jeder Identity Provider, der SAML 2.0 oder WS-Federation spricht, lässt sich als Claims Provider Trust einbinden. Bei ADFS-zu-ADFS-Föderation gibt es zusätzlich Komfortfunktionen wie die Weitergabe von Anmeldehinweisen über `PromptLoginFederation`.