MVP Community Week Münster

IT-Admin Weckruf

Frank Carius

Net at Work
Building IT-Excellence.

Über mich

Frank Carius

- Microsoft MVP Microsoft 365 (Exchange, Teams)
- Microsoft Certified Master (Lync)
- Webseite: https://www.msxfaq.de
- frank.carius@netatwork.de
- https://de.linkedin.com/in/frankcarius

Net at Work - Systemhaus/Softwarehaus

- Solution Partner „Modern Work“ and „Security“
- Gründung 1995, Paderborn, 150+ Mitarbeiter
- NoSpamProxy: Spamfilter, SMIME-Gateway, DMARC-Reporting

Net at Work
Building IT-Excellence.

noSpam proxy®

Microsoft® Most Valuable Professional

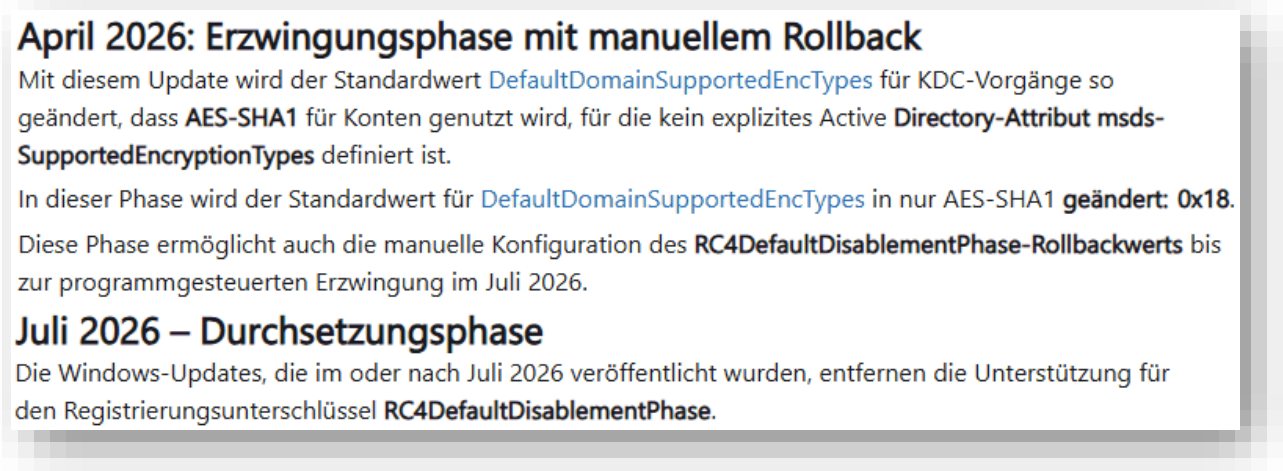
www.msXfaq.de

Microsoft CERTIFIED Master

Kerberos RC4->AES

Meldungen von Microsoft

- CVE-2026-20833 Windows Kerberos Information Disclosure Vulnerability
  - CVSS 5,5/4,8. Kein Public Disclosure, noch keine Expoits bekannt, “less likely
  - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20833
- How to manage Kerberos KDC usage of RC4 for service account ticket issuance changes related to CVE-2026-20833 https://support.microsoft.com/en-us/topic/how-to-manage-kerberos-kdc-usage-of-rc4-for-service-account-ticket-issuance-changes-related-to-cve-2026-20833-1ebcda33-720a-4da8-93c1-b0496e1910dc
- Zeitplan
  - 13. Jan 2026 Windows Update
    - Auditing mit System-Eventlog 201-209 addiert
    - Enforcement manuell möglich
    - vorher kein Schutz gegen CVE2026-20833
  - 14. April 2026 Windows Update
    - DefaultEncryptionType = AES-SHA1
    - kann manuell deaktiviert werden
    - Systeme mit manueller Konfiguration in msds-SupportedEncryptionTypes
  - Juli 2026 Windows Update
    - Enforcement nicht mehr deaktivierbar. Default = AES-SHA1
    - msds-SupportedEncryptionTypes kann weiter überstimmen



April 2026: Erzwingungsphase mit manuellem Rollback

Mit diesem Update wird der Standardwert DefaultDomainSupportedEncTypes für KDC-Vorgänge so geändert, dass **AES-SHA1** für Konten genutzt wird, für die kein explizites Active **Directory-Attribut msds-SupportedEncryptionTypes** definiert ist.

In dieser Phase wird der Standardwert für DefaultDomainSupportedEncTypes in nur AES-SHA1 **geändert: 0x18**.

Diese Phase ermöglicht auch die manuelle Konfiguration des **RC4DefaultDisablementPhase-Rollbackwerts** bis zur programmgesteuerten Erzwingung im Juli 2026.

Juli 2026 – Durchsetzungsphase

Die Windows-Updates, die im oder nach Juli 2026 veröffentlicht wurden, entfernen die Unterstützung für den Registrierungsunterschlüssel **RC4DefaultDisablementPhase**.

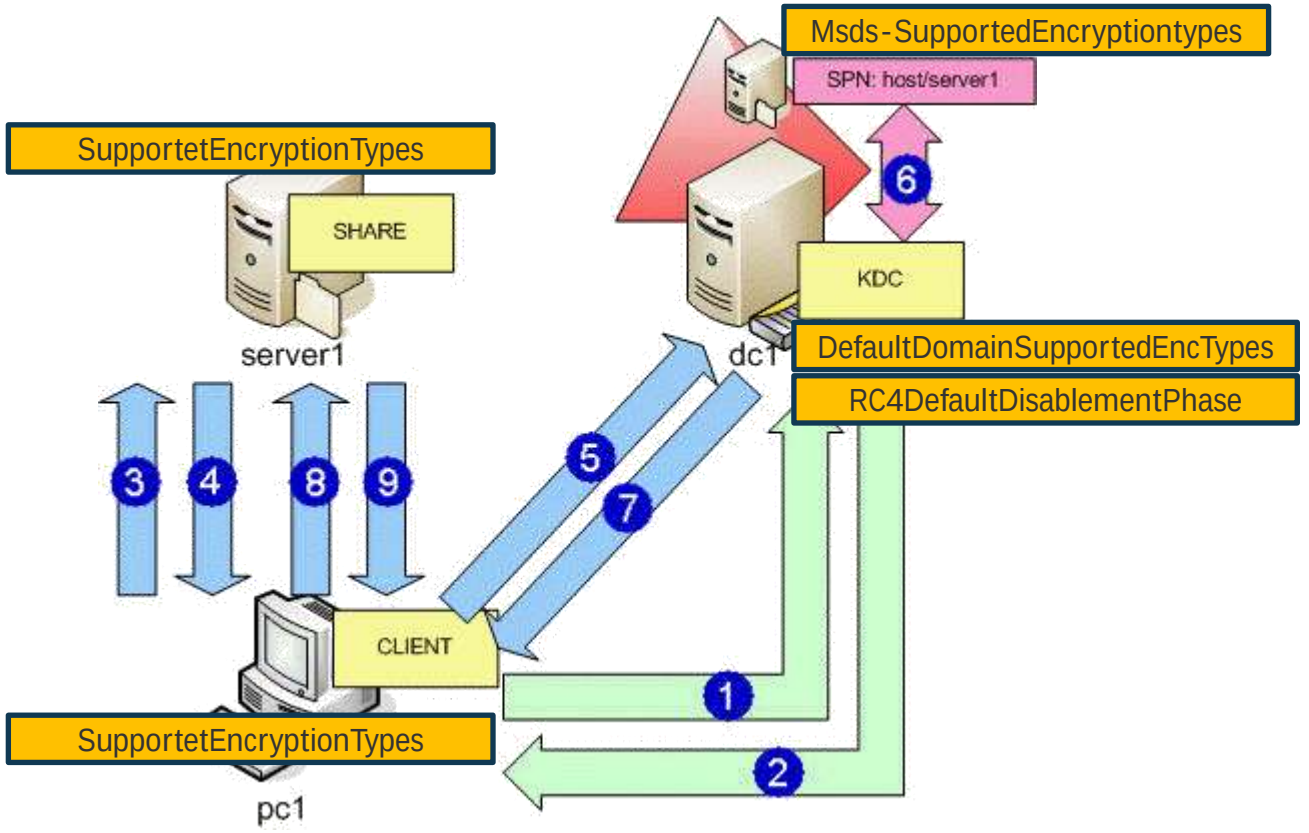
Keine RC4-Abschaltung! RC4 funktioniert weiter, aber AES wird Default

Default Einstellungen und Möglichkeiten

Betriebssystem	DES_CBC_CRC	DES_CBC_MD5	RC4_HMAC_MD5	AES128_HMAC_SHA1	AES256_HMAC_SHA1
Windows 2000	Supportet	Supportet	Supportet	Kein Support	Kein Support
Windows XP	Supportet	Supportet	Supportet	Kein Support	Kein Support
Windows 2003	Supportet	Supportet	Supportet	Kein Support	Kein Support
Windows Vista	Supportet	Supportet	Supportet	Supportet	Supportet
Windows 2008	Supportet	Supportet	Supportet	Supportet	Supportet
Windows 7	Deaktiviert	Deaktiviert	Supportet	Supportet	Supportet
Windows 2008R2	Deaktiviert	Deaktiviert	Supportet	Supportet	Supportet
Windows 10	Deaktiviert	Deaktiviert	Supportet	Supportet	Supportet
Windows 2012	Deaktiviert	Deaktiviert	Supportet	Supportet	Supportet
Windows 2012R2	Deaktiviert	Deaktiviert	Supportet	Supportet	Supportet
Windows 2016	Deaktiviert	Deaktiviert	Deaktiviert ab Apr 2026	Supportet	Supportet
Windows 2019	Deaktiviert	Deaktiviert	Deaktiviert ab Apr 2026	Supportet	Supportet
Windows 2022	Deaktiviert	Deaktiviert	Deaktiviert ab Apr 2026	Supportet	Supportet
Windows 2025	Deaktiviert	Deaktiviert	Deaktiviert ab Apr 2026	Supportet	Supportet
Windows 11	Deaktiviert	Deaktiviert	Supportet	Supportet	Supportet
Samba	Deaktiviert	Deaktiviert	Deaktiviert ab 4.17.4	Supportet	Supportet
NetApp	Aktiv	Aktiv	Aktiv	Ab 9.13.1 Default	Ab 9.13.1 Default
Apache	Konfiguration	Konfiguration	Konfiguration	Konfiguration	Konfiguration
Hitachi	Supportet	Supportet	Supportet	Supportet	Supportet

Kerberos 101

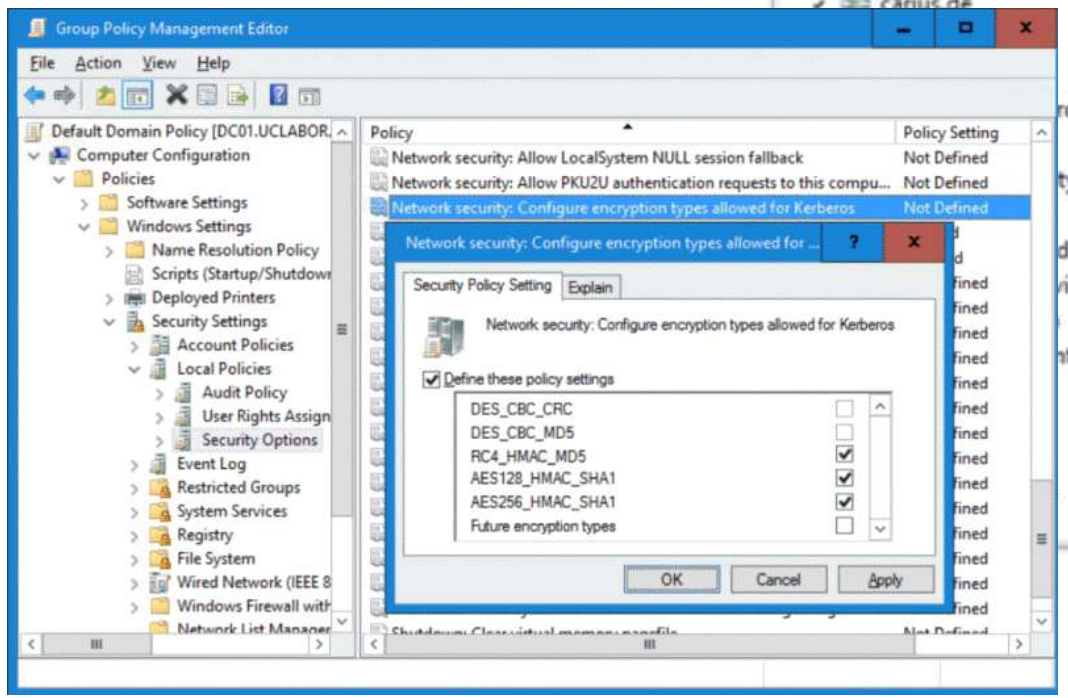
1. Anmeldung am DC
   - Sie identifizieren sich bei der Bank
2. Erhalte eines TGT (Ticket Granting Ticket)
   - Die Bank stellt eine Debit-Karte aus
3. Zugriff auf einen Service
   - Sie wollen in den Zug einsteigen
4. Der Server lehnt anonymen Zugriff ab
   - Der Schaffner schickt sie zum Automaten
5. Sie fordern ein TGS an (Ticket Service Ticket)
   - Sie stecken ihre Debit-Karte in den Automaten
6. Der KDC sucht nach dem Service-Konto
   - Der Automat fragt bei der Bank nach der Autorisierung
7. Der KDC erzeugt und liefert ein TGS für den Service
   - Der Fahrkartenautomat druckt das Ticket aus
8. Sie greifen auf dem Service mit dem Ticket zu
   - Sie zeigen den Fahrschein beim Schaffner
9. Die erhalten die gewünschten Informationen
   - Der Schaffner lässt sie einsteigen und fahren

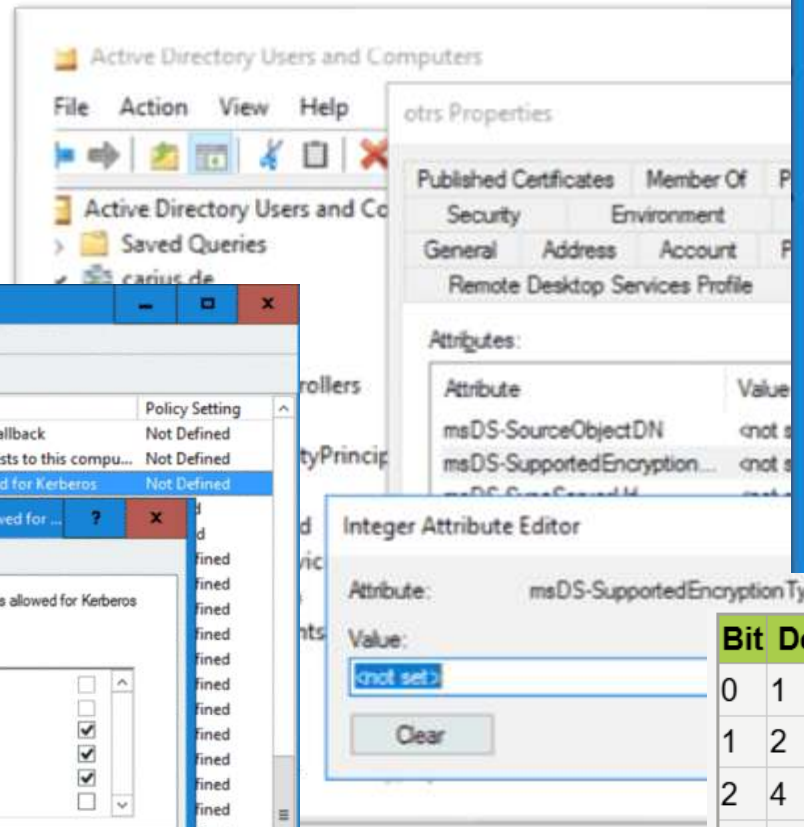


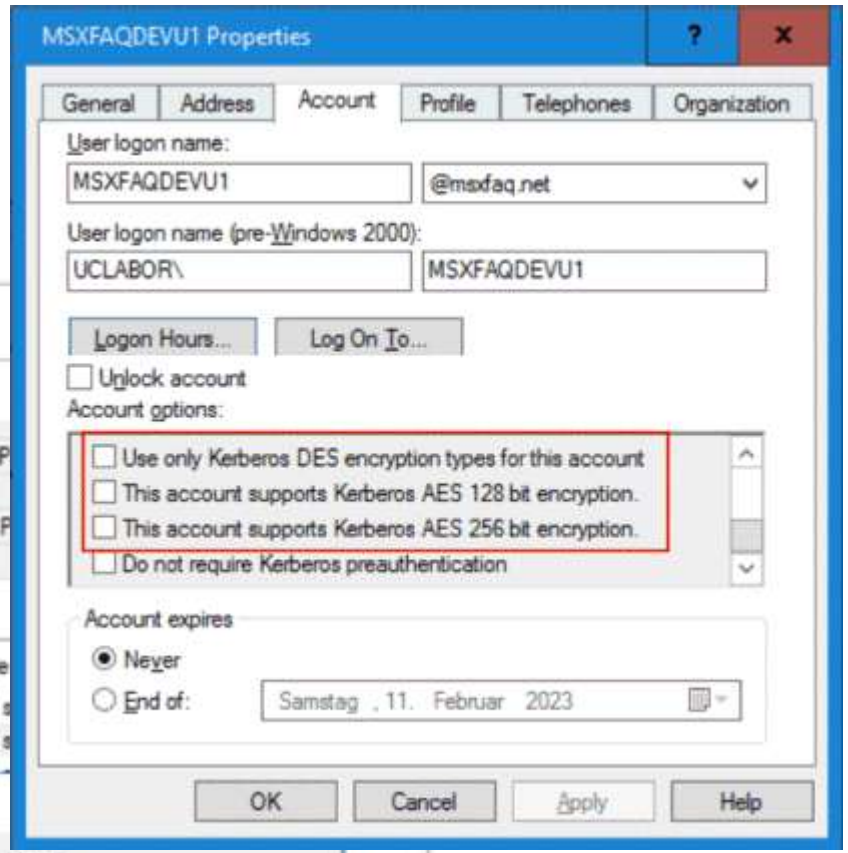
Die Tickets (TGT) sind kryptografisch gesichert
- Signiert durch den KDC (KRBTGT-Konto)
- Verschlüsselt mit dem Service-Account

Msds-SupportedEncryptionTypes

- LDAP-Feld am Computer oder Dienstkonto
- Windows Domain Computer aktualisieren das Feld!
- Statisch für Dienstkonten
- Statisch für Keytab-Konten



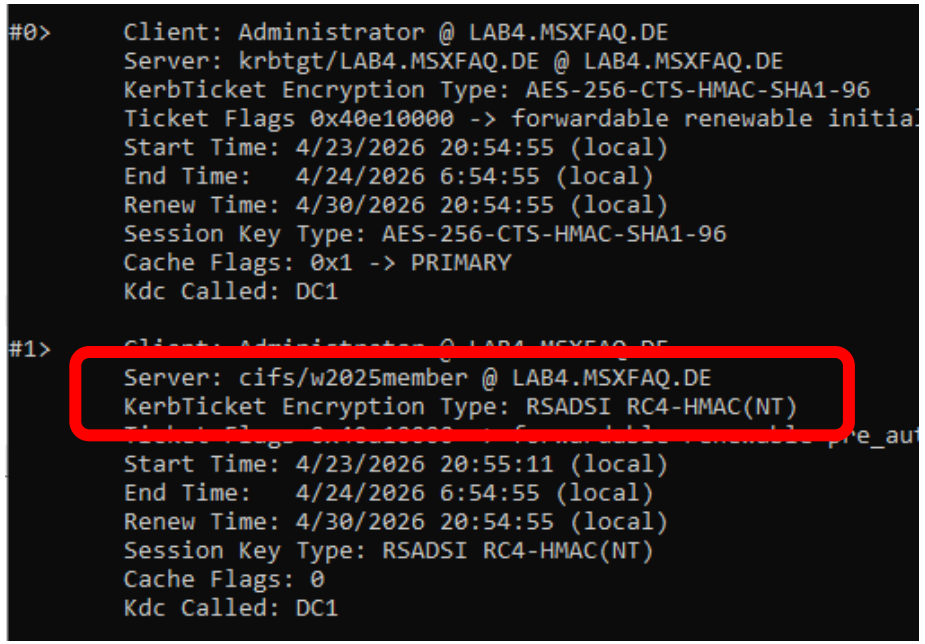




Bit	Dez-Wert	Hex-Wert	Verfahren
0	1	0x01	DES_CBC_CRC
1	2	0x02	DES_CBC_MD5
2	4	0x04	RC4-HMAC
3	8	0x08	AES128-CTS-HMAC-SHA1-96
4	16	0x10	AES256-CTS-HMAC-SHA1-96

Risiken

- Nur relevant für Kerberos
  - Nicht relevant für NTLM-Anmeldungen
  - Nicht relevant für TLS-Einstellungen
- msds-supportedEncryptionType
  - Manuelle Anweisung an den DC, kein AES auszustellen
  - Domain Computer überschreiben Feld!
  - Andere Systeme (Keytab mit RC4)
  - Überstimmt Domain-Defaults
- KRBTGT-Konto muss AES-Geheimnis haben
  - Key Rollover muss auf Windows 2008 erfolgt sein
  - https://www.msxfaq.de/windows/kerberos/krbtgt_keyrollover.htm
- Kontrolle
  - Eventlog
  - KList




```
Get-WinEvent `
   -LogName Security `
   -FilterXPath "*[System[Provider[@Name='Microsoft-Windows-Security-Auditing'] `
                         and (EventID=4768)]`
                  and ( `
                       EventData[Data[@Name='TicketEncryptionType']='0x17'] `
                     or EventData[Data[@Name='TicketEncryptionType']='0x18'] `
                        ) `
                  ]"
```

CA Browser Forum und Zertifikate

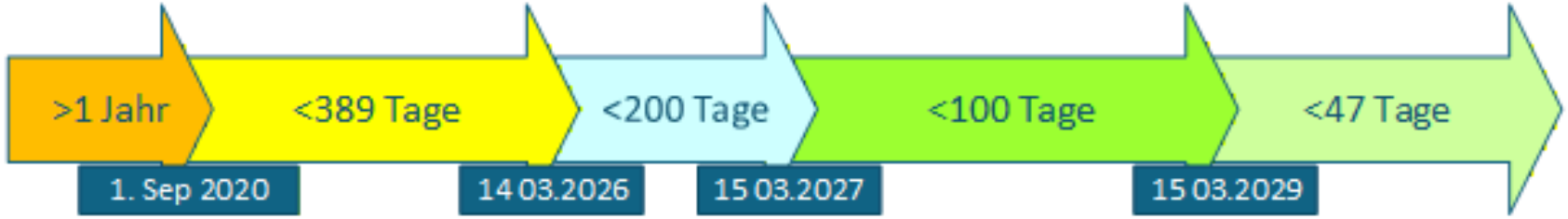
200/100/47 Tage

Worum geht es

- CA/Browser-Forum - Zusammenschluss der Browser-Hersteller und CAs
  - Entschluss 1: Gültigkeit schrittweise auf 47 Tage
  - Entschluss 2: EnhancedKeyUsage ohne „ClientAuthentication“
  - Sicherheit und Kosteneinsparung durch kleinere CRLs/weniger OCSP-Anfragen
  - CA/Browser Forum: Ballot SC081v3: Introduce Schedule of Reducing Validity and Data Reuse Periods https://cabforum.org/2025/04/11/ballot-sc081v3-introduce-schedule-of-reducing-validity-and-data-reuse-periods/
  - CA-Browser-Forum - Latest Baseline Requirements https://cabforum.org/working-groups/server/baseline-requirements/requirements/
  - Hinweis: Let‘s Encrypt stellt schon früher von 90 auf 45 Tage um https://letsencrypt.org/2025/12/02/from-90-to-45
- Details
  - Der Browser akzeptiert und warnt zukünftig
  - CAs stellen Webserver-Zertifikate gemäß „Baseline Requirements“ aus
  - Andere Zertifikate (SMIME, etc.) sind nicht betroffen

Gültigkeitsdauer

- Vor 15. März 206: 1x im Jahr Zertifikat als Admin aktualisieren
- Seit 15. März 2026: Maximaldauer 200 Tage
  - Könnte man noch manuell machen, wenn es wenige Server sind
- Ab 15. März 2027: Maximaldauer 100 Tage
  - Jetzt fängt es an zu nerven
- Ab 15. März 2028: Keine Änderung!
- An 15. März 2029: Maximaldauer 47 Tage
  - Spätestens jetzt sollte ist über Automatisierung nachdenken

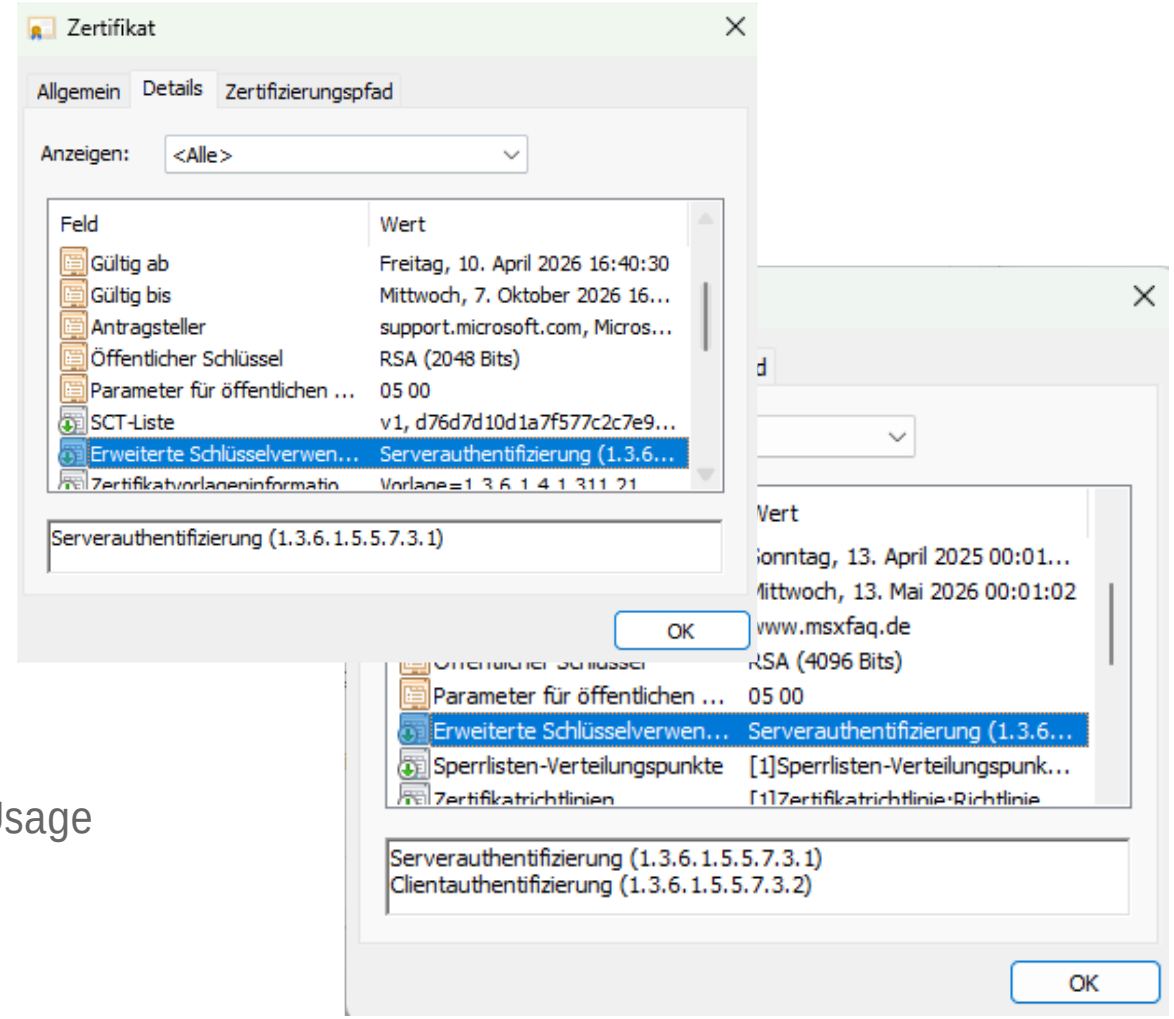


Wir werden ein Certificate Lifecycle Management (CLM) brauchen!

EnhancedKeyUsage

- Serverauthentifizierung (1.3.6.1.5.5.7.3.1)
  - Client verbindet sich zum Server
  - Client kann prüfen, ob er den richtigen Server erreicht hat
  - Protokolle: HTTPS, POP3S, IMAP4S, SMTPS
- Clientauthentifizierung (1.3.6.1.5.5.7.3.2)
  - Clients sendet sein Zertifikat mit
  - Anmeldung bei MTLS bei SMTP, SIP, 802.1x
  - Server prüft Legitimation des Clients
  - Exchange Hybrid Mail, Teams Direct Routing
- ABER
  - Exchange Online ignoriert EnhancedKeyUsage
  - Teams Direct Routing ignoriert EnhancedKeyUsage
  - Audiocodes Gegenrichtung abschaltbar

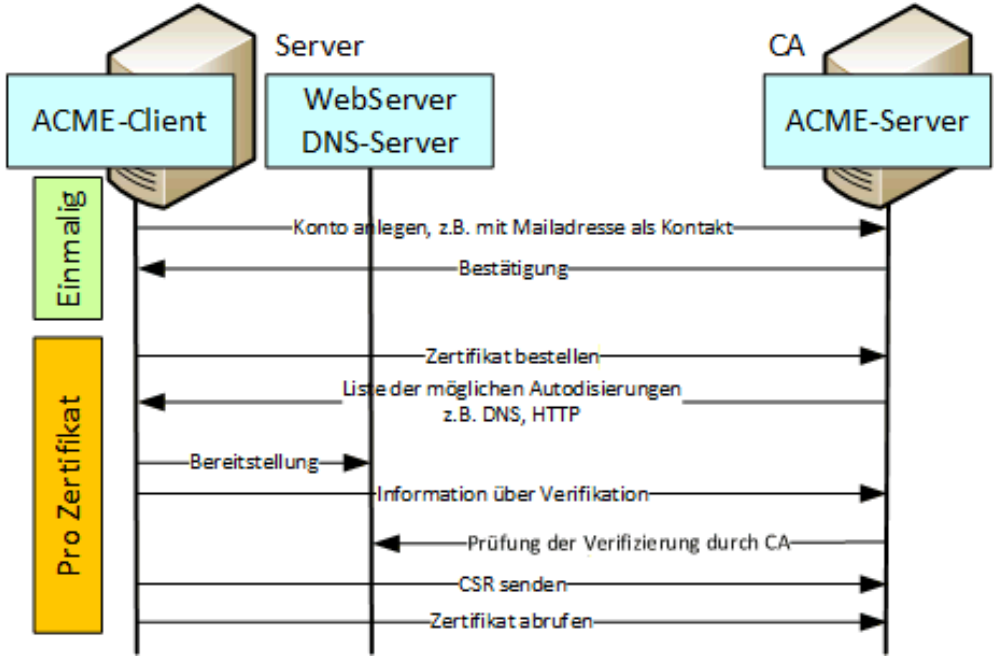
Bisher keine Probleme ...



https://www.msxfaq.de/signcrypt/zertifikate/clientauthentication_in_zertifikaten.htm

CLM, Autoenrollment, ACME

- Es gibt schon „AutoEnrollment“-Schnittstellen
  - Interne Windows CA mit RPC und Gruppenrichtlinien
  - SCEP/PKCS/ NDES – Für Netzwerkgeräte, MDM (Intune)
    https://www.msxfaq.de/signcrypt/scep.htm
  - ACME – Let‘s Encrypt – Seit 2016
- ACME wird es wohl werden
  - Alle größeren öffentlichen CAs bieten mittlerweile ACME an
  - Viele Endgeräte haben oder bekommen ACME-Support
  - ACME-Clients für viele Systeme verfügbar
    https://acmeclients.com/
  - RFC 8555-Standardisierung
- Managementsysteme – der Markt „sortiert“ sich gerade
  - Einige CAs haben gleich mehrere Lösungen
  - 3rd-Party Hersteller wittern auch viel Umsatz

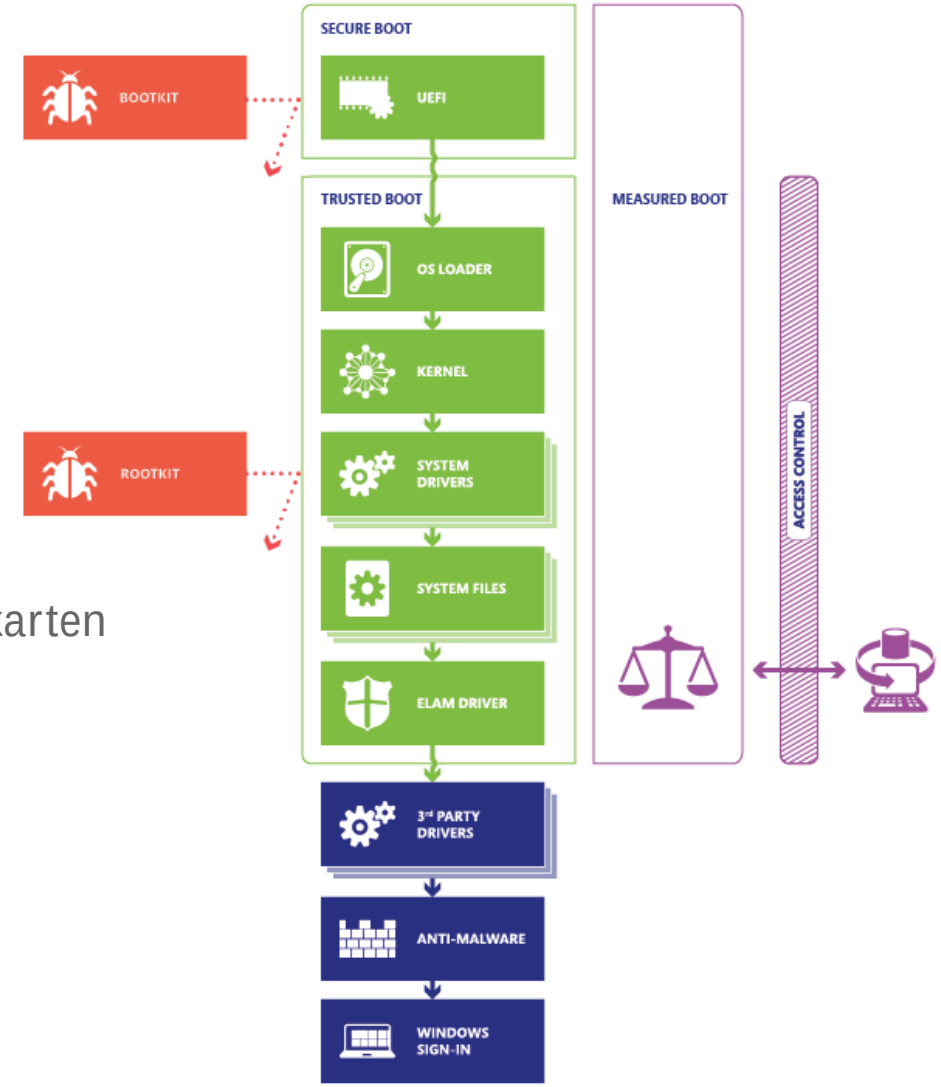


Je nach Größe: Planen Sie Investitionen und Aufwände

UEFI-Zertifikate

Worum geht es?

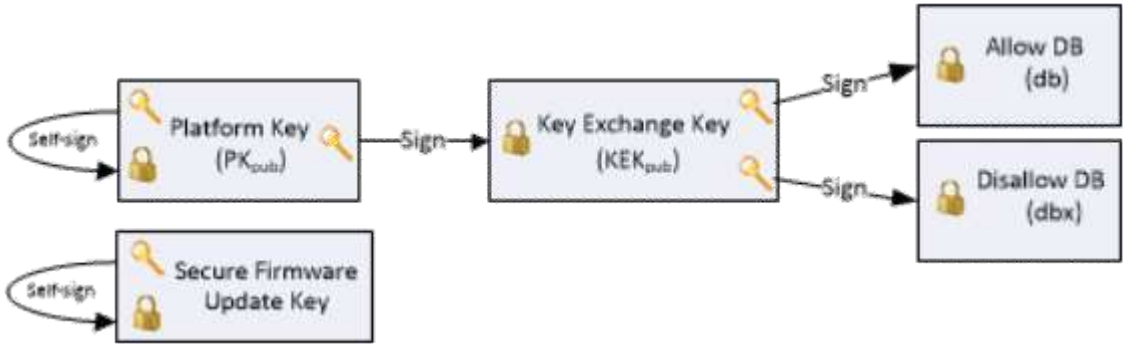
- Secure Boot
  - Schutz gegen Schadsoftware
  - Schutz gegen Veränderungen
  - „Sichere Umgebung“ für Bitlocker
- Digitale Signatur aller Komponenten
  - Hersteller Firmware/BIOS ist der Startpunkt
  - BIOS prüft Signatur anderer Komponenten
    - Raid-Controller, Netzwerkkarten (PXE-Boot), Grafikkarten
  - BIOS prüft Signatur des Windows Bootloader
  - BIOS prüft UEFI-Konfiguration
  - Freigabe von TPM (für Bitlocker, Windows Hello etc.)
- Und alles ohne „Internet“
  - keine CRL-Prüfung
  - kein automatisches RootCA-Update



https://learn.microsoft.com/de-de/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process

Firmware und UEFI-Speicher

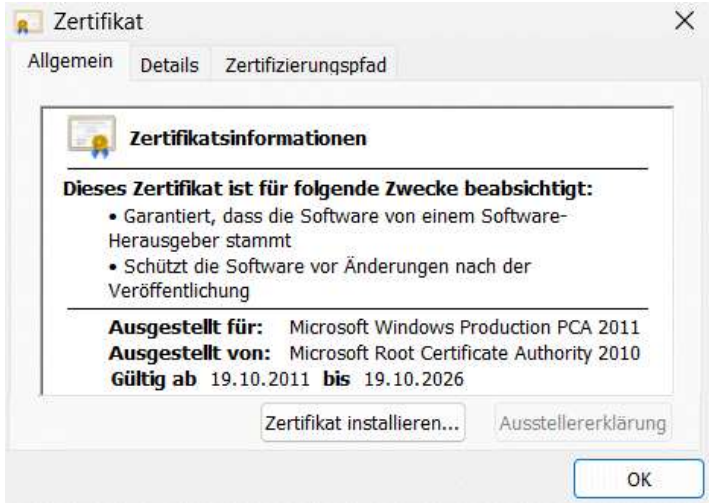
- PK (Plattform Key)
  - Kommt vom Bios/Hardware Hersteller z.B. Lenovo, HP, Dell, Fujitsu
  - Gibt es genau einmal auf dem Computer
  - Aktualisierung durch Firmware Update
    - Hersteller oder Windows Update



- KEK (Key Exchange Keys)
  - Von Microsoft o.a. und signiert von den PKs der Hersteller
  - Ohne gültigen KEK gibt es keine DB/DBX Updates
- DB-Keys
  - Liegen im UEFI-Speicher
  - Mehrere Keys möglich
  - Signieren den Windows Bootloader
  - Updates müssen mit KEK signiert sein
- DBX
  - Liste der gesperrten Zertifikate
  - Updates müssen mit KEK signiert sein

Warum müssen wir aktiv werden?

- KEK: „Microsoft Corporation KEK CA 2011“ läuft 2026 aus
  - Windows Update addiert „Microsoft Corporation KEK 2K CA 2023“
  - Nur möglich, wenn Update-Paket durch gültigen PK signiert
  - Risiko: Nach dem Ablauf im Juni 2026 können keine DB/DBX-Updates installiert werden
- DB: „Microsoft UEFI CA 2011“ läuft 2026 aus
  - Windows Update addiert „Windows UEFI CA 2023“
  - Nur möglich, wenn Paket durch KEK signiert ist.
  - Risiko: Nach dem Ablauf im Juni 2026 können keine neuer Bootloader mehr installiert werden
- Aber
  - Auch nach dem Juni 2026 wird Windows booten
  - Einige Updates könnten blockiert sein



Elefant 1: Black Lotus CVE-2022-21894, CVE-2023-24932

- Sicherheitslücke erlaubt **Signierung von Bootloader mit Schadcode**
- Alle schädlichen Bootloader waren von der „Microsoft UEFI CA 2011“ signiert
- **Sperrung** der Bootloader über DBX nicht sinnvoll, da **DBX-Speicher begrenzt**
- Lösung: „Microsoft UEFI CA 2011“ zurückziehen
  - Hat nur kaum jemand im Jahr 2023 schon gemacht
  - Sie wird am 19.10.2026 sowieso ablaufen

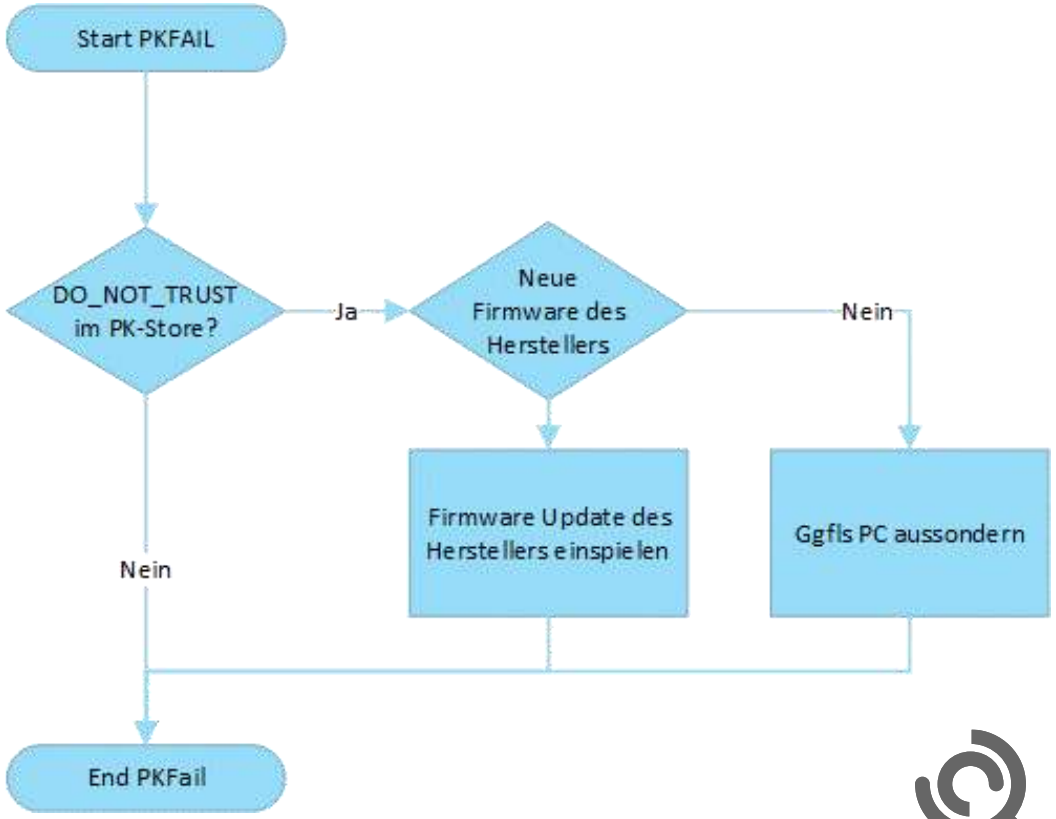
- Links
  - https://www.microsoft.com/en-us/security/blog/2023/04/11/guidance-for-investigating-attacks-using-cve-2022-21894-the-blacklotus-campaign/
  - https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win64/BlackLotus!MSR

Elefant 2: PKFail CVE-2024-8105

- AMI hat einen „Test-PK“
- Der Private Key wurde öffentlich
- Hersteller haben anscheinend Firmware mit dem Key verteilt

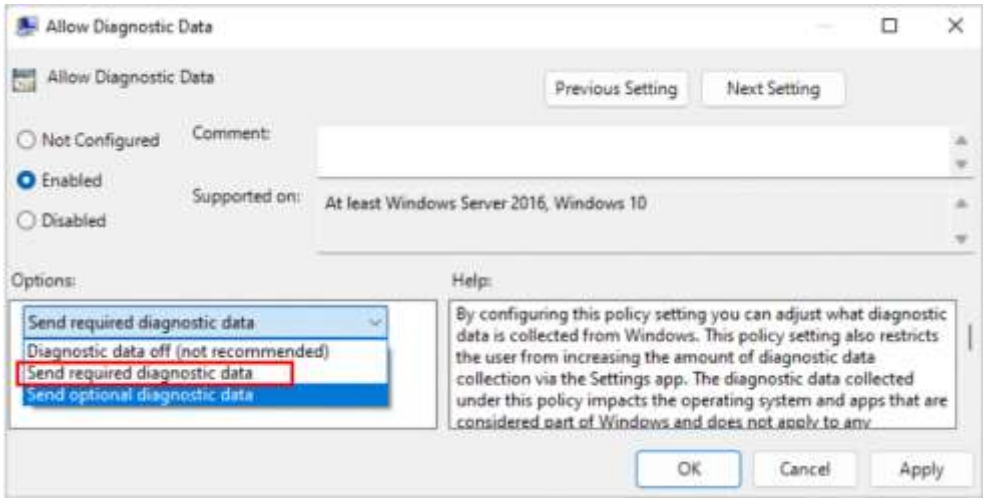
https://www.binarly.io/blog/pkfail-untrusted-platform-keys-undermine-secure-boot-on-uefi-ecosystem

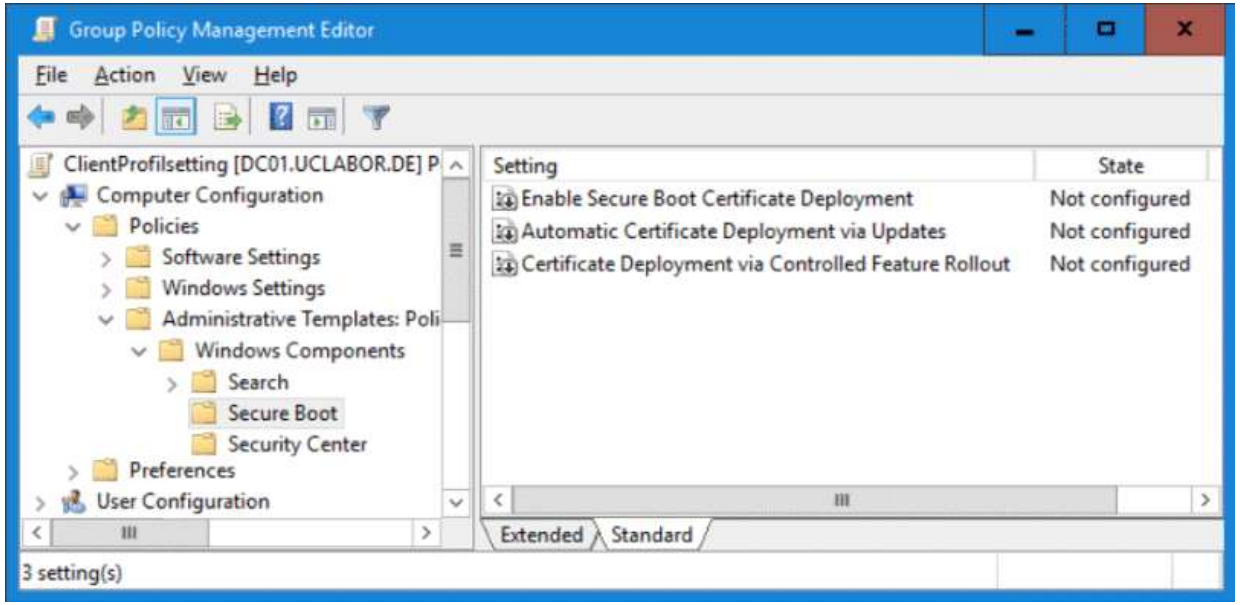
```
00000040  02 16 A0 03 02 01 02 02 10 55 FB EF 87 81 23 00  .........U....#.
00000050  84 47 17 0B B3 CD 87 3A F4 30 0D 06 09 2A 86 48  .G.....:.0...*.H
00000060  86 F7 0D 01 01 0B 05 00 30 25 31 23 30 21 06 03  ........0%1#0!..
00000070  55 04 03 13 1A 44 4F 20 4E 4F 54 20 54 52 55 53  U....DO NOT TRUS
00000080  54 20 2D 20 41 4D 49 20 54 65 73 74 20 50 4B 30  T - AMI Test PK0
00000090  1E 17 0D 31 37 31 31 30 38 32 33 33 32 35 33 5A  ...171108233253Z
000000A0  17 0D 32 31 31 31 30 38 32 33 33 32 35 32 5A 30  ..211108233252Z0
000000B0  25 31 23 30 21 06 03 55 04 03 13 1A 44 4F 20 4E  %1#0!..U....DO N
000000C0  4F 54 20 54 52 55 53 54 20 2D 20 41 4D 49 20 54  OT TRUST - AMI T
000000D0  65 73 74 20 50 4B 30 82 01 22 30 0D 06 09 2A 86  est PK0.."0...*.
000000E0  48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82  H.............0.
```



Die Rolle von Windows Update

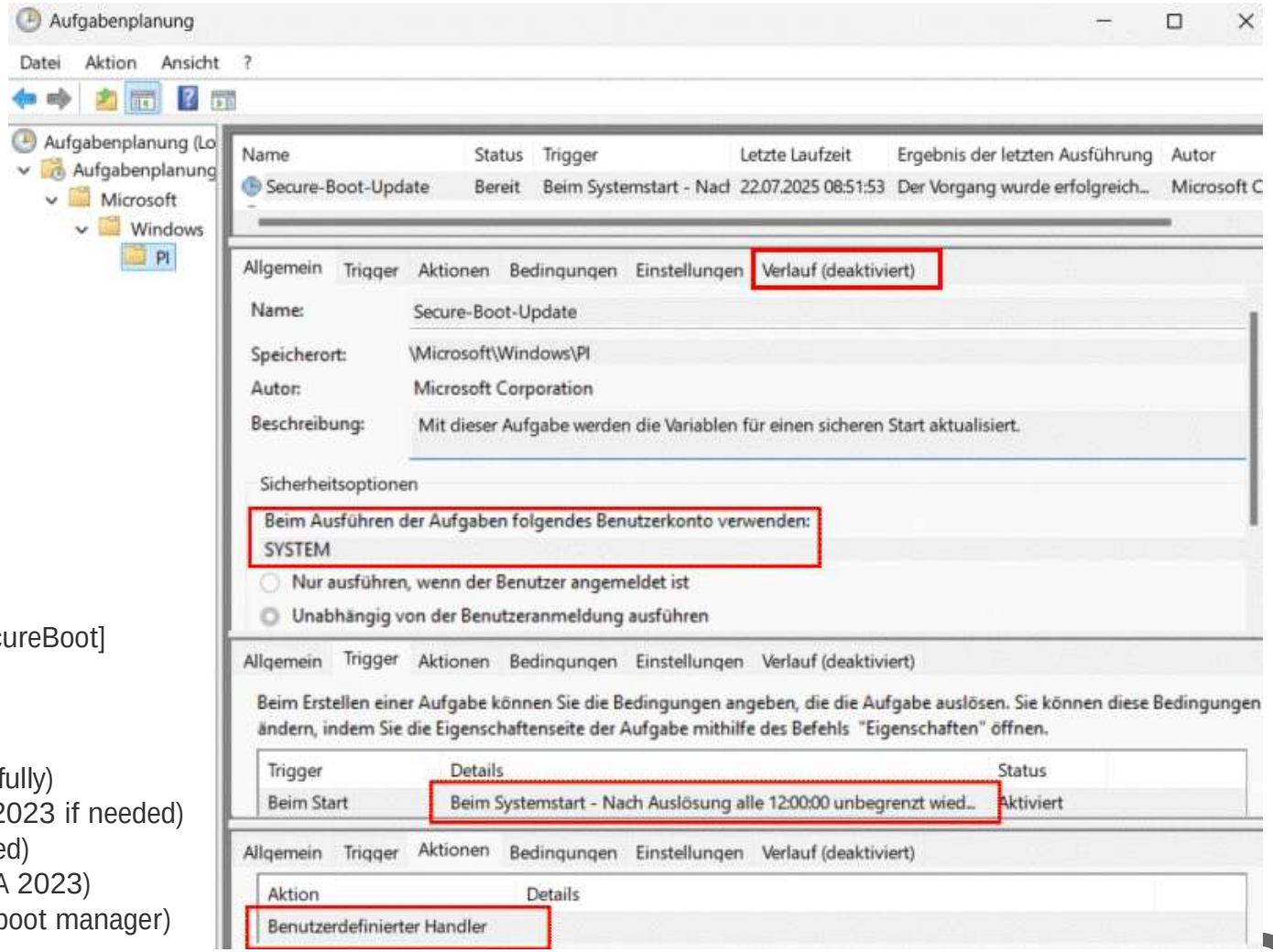
- Automatisch
  - Windows 11 Clients mit Telemetrie
  - Windows 10 Client mit ESU
  - Windows 365 (Cloud VM, Autopatch)
- Manuell
  - Windows Server
  - Windows 11 ohne Telemetrie
  - Hyper-V, VMWare, Proxmox etc.
  - Azure Virtual Desktop
  - Linux-Systeme
- Steuerbar durch GPO und Registry





Mehrstufiger Prozess

- Schritte
  - 1. Update des PK, wenn erforderlich
  - 2. Update des KEK
  - 3. Update der DB/DBX
  - 4. Tausch des Bootloaders
- Gesteuert durch geplanten Task
- Manuell antriggerbar



Registrierungsschlüssel setzen

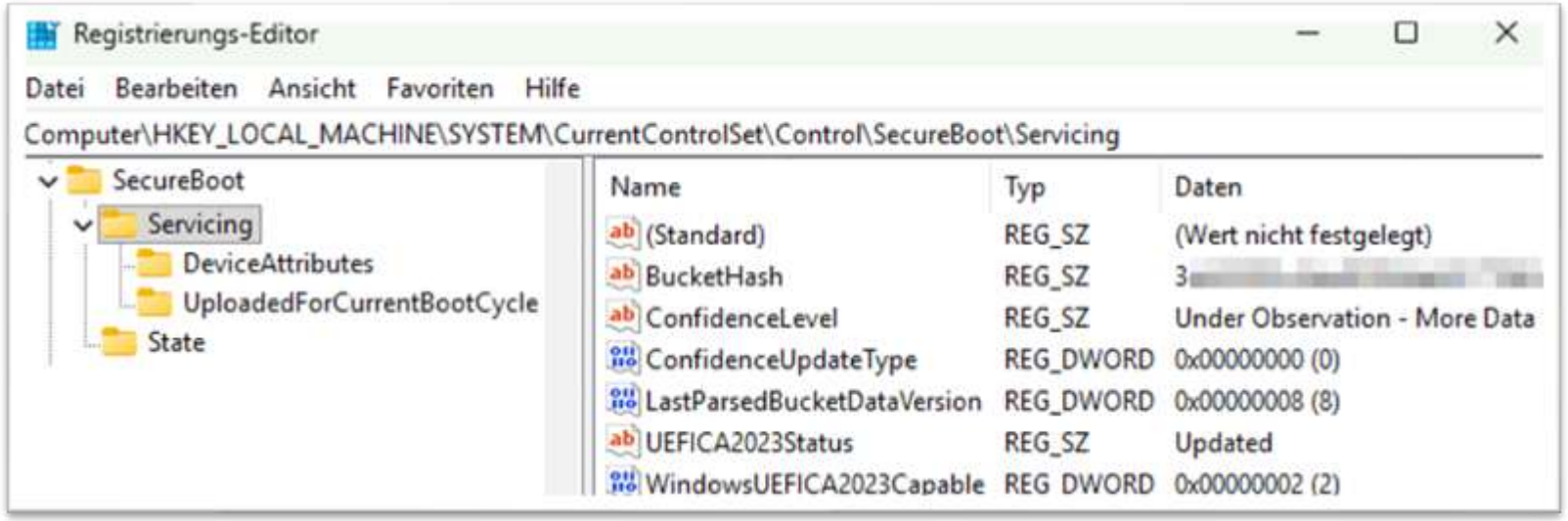
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot]
"AvailableUpdates"=dword:00005944
```

Ablauf überwachen

Start: 0x5944
0x0040 → 0x5904 (Applied the Windows UEFI CA 2023 successfully)
0x0800 → 0x5104 (Applied the Microsoft Option ROM UEFI CA 2023 if needed)
0x1000 → 0x4104 (Applied the Microsoft UEFI CA 2023 if needed)
0x0004 → 0x4100 (Applied the Microsoft Corporation KEK 2K CA 2023)
0x0100 → 0x4000 (Applied the Windows UEFI CA 2023 signed boot manager)

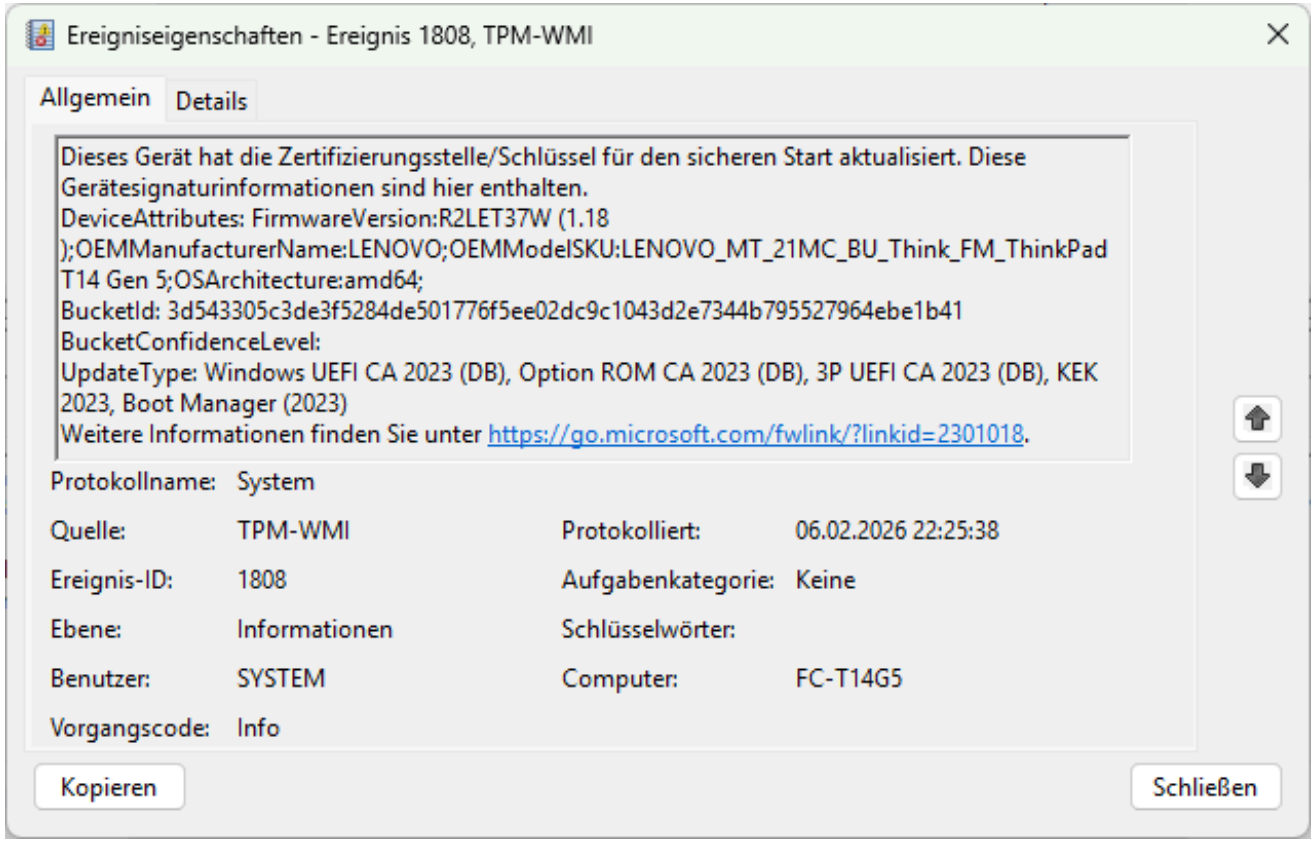
Kontrolle: Registrierung

- HKLM\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing\UEFICA2023Status
  - NotStarted: Das Update wurde noch nicht gestartet
  - InProgress: Das Update wird aktuell durchgeführt. Es kann einige Neustarts bedeuten
  - Updated : Die Aktualisierung ist erfolgreich gewesen
- HKLM\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing\ WindowsUEFICA2023Capable
  - 0/ fehlt : Das “Windows UEFI CA 2023” Zertifikat ist nicht in der DB
  - 1 : Das “Windows UEFI CA 2023” Zertifikat ist in der DB
  - 2 : Das “Windows UEFI CA 2023” Zertifikat ist in der DB und der Bootmanager ist damit signiert

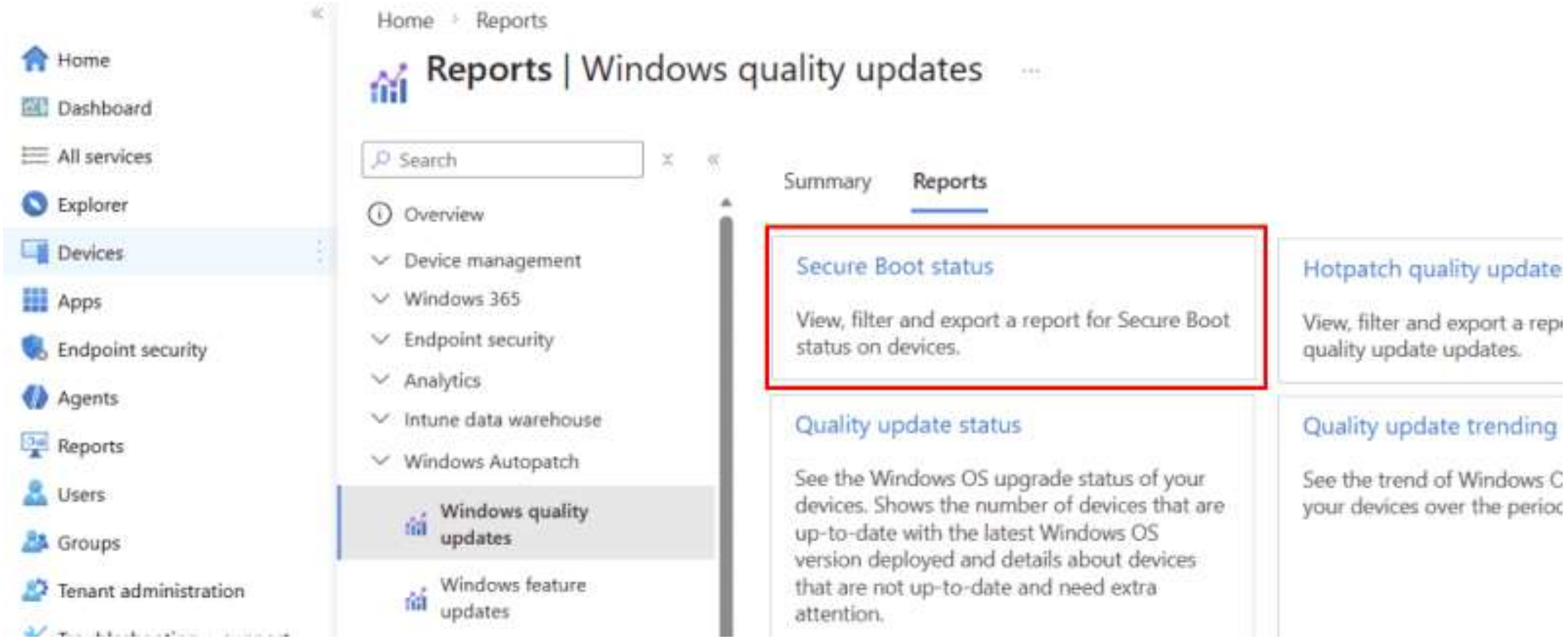


Kontrolle: Eventlog

```
Eventlog: System
Source  : TPM-WMI
EventID : 1799
Level   : Information
Text    : Boot Manager signed with Windows UEFI CA 2023 was installed successfully
```



Kontrolle: Intune-Report



Exchange Online onmicrosoft.com-Domain

Domain: <tenantname>.onmicrosoft.com

- Jeder Tenant hat eine (oder mehrere) Domains
  - Default Domain
  - UPN für Cloud-Only User und DirSync-User mit anderer Domain
  - Mail-Domain für Office Groups und Teams
  - Routing-Domain für Exchange Hybrid
  - Microsoft-Managed: Keine Pflege von SPF-Einträgen durch Kunde möglich
  - https://www.msxfaq.de/cloud/exchangeonline/betrieb/b2b_mail_default_domain.htm
- Risiko: Throttling
  - Maximal 100 externe Empfänger/24h
  - Limiting OnMicrosoft Domain Usage for Sending Emails | Microsoft Community Hub https://techcommunity.Microsoft.com/blog/exchange/limiting-onmicrosoft-domain-usage-for-sending-emails/4446167
- Risiko: B2BMails
  - Jan 2026:
- Lösung
  - Default Domain im Tenant kontrollieren und ggfls. umstellen
  - Betrifft nur neue Objekte, keine Bestandsobjekte

MOERA outgoing email throttling starts	Exchange seats in the tenant
October 15, 2025	Trial
December 1, 2025	< 3
January 7, 2026	3 – 10
February 2, 2026	11 – 50
March 2, 2026	51 – 200
April 1, 2026	201 – 2,000
May 4, 2026	2,001 – 10,000
June 1, 2026	> 10,001

I would like to inform you that starting January 2026, Microsoft Entra B2B invitation emails are no longer sent from invites@microsoft.com. They are now sent from the primary (default) domain of the inviting Entra tenant.

So, in your scenario this causes invitations to be sent from: *invites@ onmicrosoft.com*.

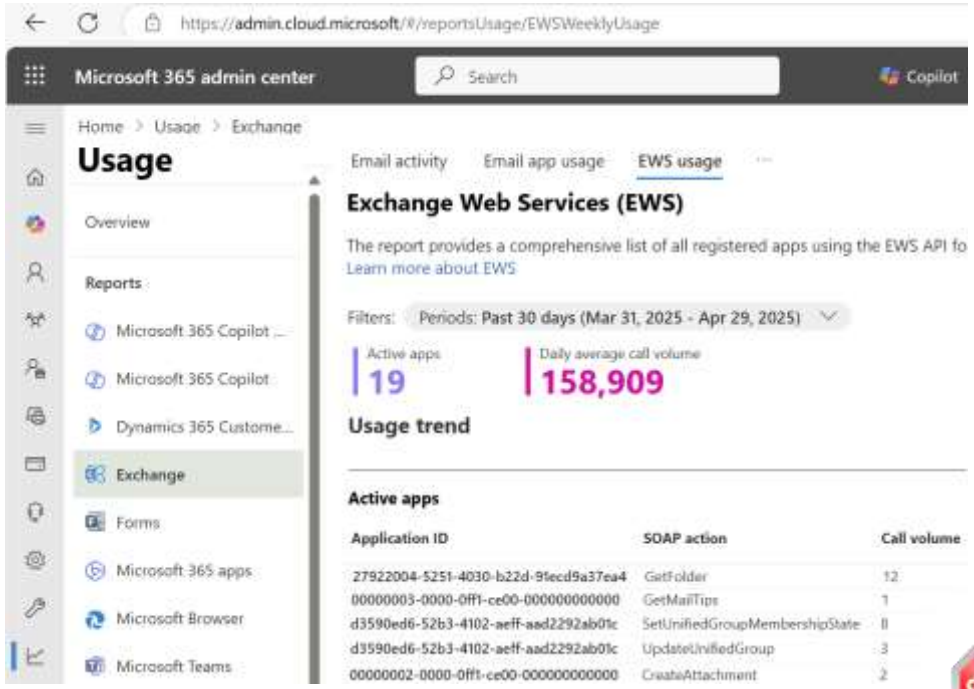
Exchange Online

EWS

EWS-Abschaltung in Exchange Online

- Timeline
  - Bisher: Immer wieder angekündigt, immer wieder verschoben
  - Microsofts interne Tools/Dienste mussten auch erst auf Graph umgestellt werden
  - 1. April 2026: EWS wird tageweise bei Tenants deaktiviert (Admins aufwecken)
  - 1. Okt 2026: EWS wird abgeschaltet. Kann für einzelne AppIDs bis April 2027 zugelassen werden
  - 1. April 2027: Endgültige Abschaltung von EWS (wenn sich nichts ändert)
- Aktionsplan:
  - Wer nutzt EWS?

    Siehe: Report im Microsoft 365 Admin Center
  - Ansprechen der 3rd-Party Hersteller
  - Prüfen der internen Nutzung
  - Umstellen auf Graph
  - ...oder Migration zurück nach Exchange OnPremises



https://www.msxfaq.de/cloud/exchangeonline/betrieb/ews_ende_2026.htm

Exchange Online SMTP BasicAuth

Microsoft 365 Message Center Post MC 786329

(Updated) Exchange Online to retire Basic Auth for Client Submission (SMTP AUTH)

Archive Share Copy link Mark as unread

Summary

Exchange Online will retire SMTP AUTH Basic Authentication by default starting December 2026, with OAuth as the supported method. Basic Auth removal is on hold until 2027, when a final date will be announced. Administrators can enable Basic Auth temporarily, but should prepare to switch to OAuth or alternatives.

Updated January 27, 2026: Based on customer feedback and visibility into adoption progress, we are refining the Exchange Online SMTP AUTH Basic Authentication Deprecation timeline to provide clearer milestones and additional runway.

- Now to December 2026: SMTP AUTH Basic Authentication behavior remains unchanged.
- End of December 2026: SMTP AUTH Basic Authentication will be disabled by default for existing tenants. Administrators will still be able to enable it if needed.
- New tenants created after December 2026: SMTP AUTH Basic Authentication will be unavailable by default. OAuth will be the supported authentication method.
- Second half of 2027: Microsoft will announce the final removal date for SMTP AUTH Basic Authentication.

Relevance
High

Service & monthly active users
Exchange Online

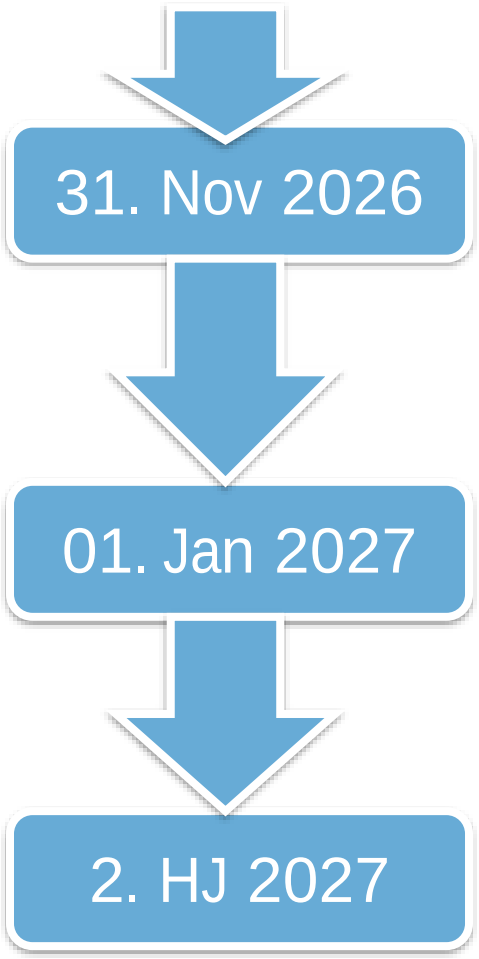
Message ID
MC786329

Published
Apr 26, 2024

Last updated
Jan 27, 2026

Tag
MAJOR UPDATE ADMIN IMPACT RETIREMENT USER IMPACT

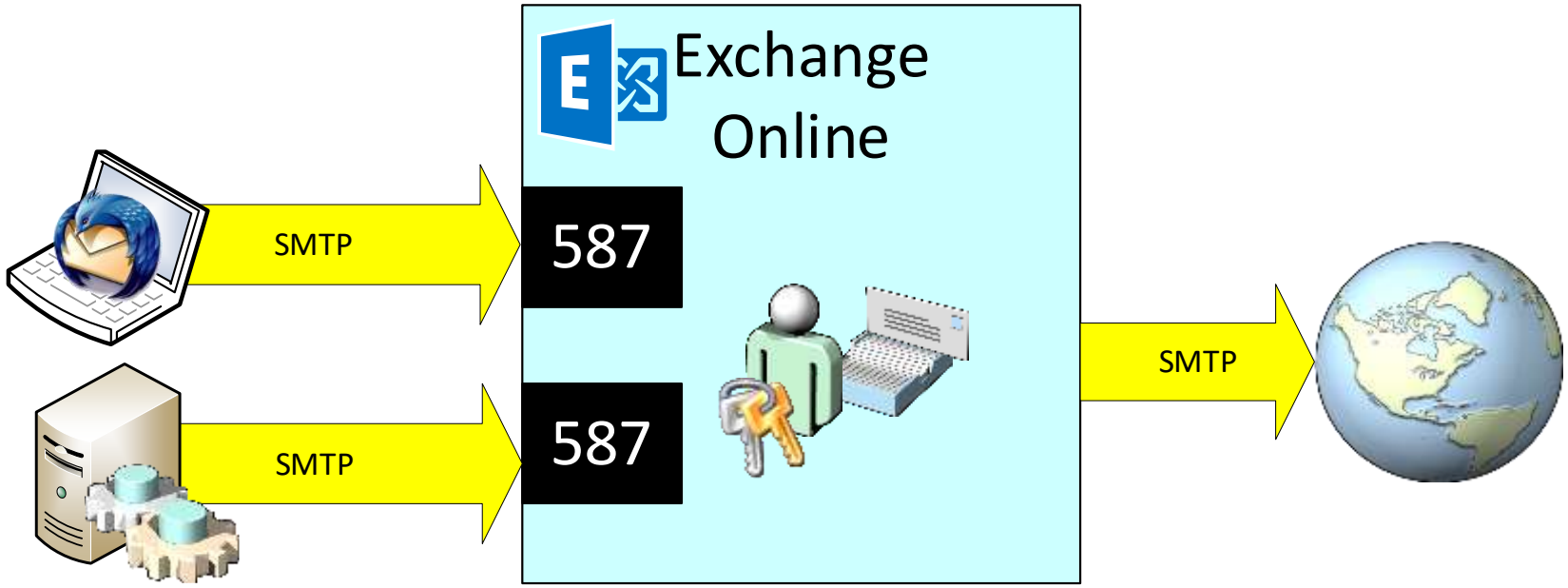
Zeitlicher Ablauf SMTP-BasicAuth Abschaltung



- Bis 31. Nov 2026 - Keine Änderung
  - Basic Authentication ist weiterhin aktiv
  - Administrator kann Report auswerten
  - Administrator kann Basic Authentication selbst deaktivieren
- 01. Jan 2027 – Rollout
  - Neue Tenants: Default = „OFF“
  - Bestehende Tenants: „Weckruf“ an Admins“
    - Rollout der Abschaltung
    - Reaktivierung möglich
- 2. HJ 2027 – Deaktivierung erzwungen

Worum geht es?

- authentifizierte SMTP-Einlieferung zum Versand ins Internet
- Anmeldung mit Username + Kennwort (BasicAuth) ist nicht sicher
- Nicht Outlook, nicht OWA, nicht ActiveSync!

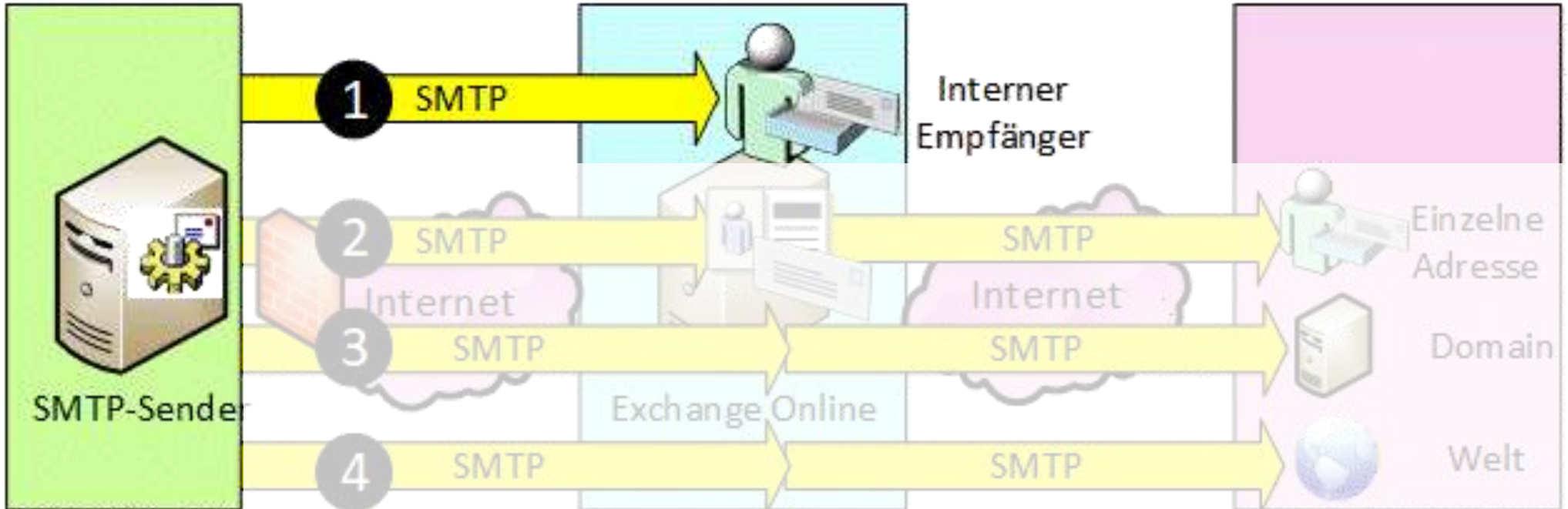


Wer nutzt diesen Weg?

- Report im Exchange Admin Center
  - https://admin.cloud.microsoft/exchange?#/reports/smtpauthmailflowdetails

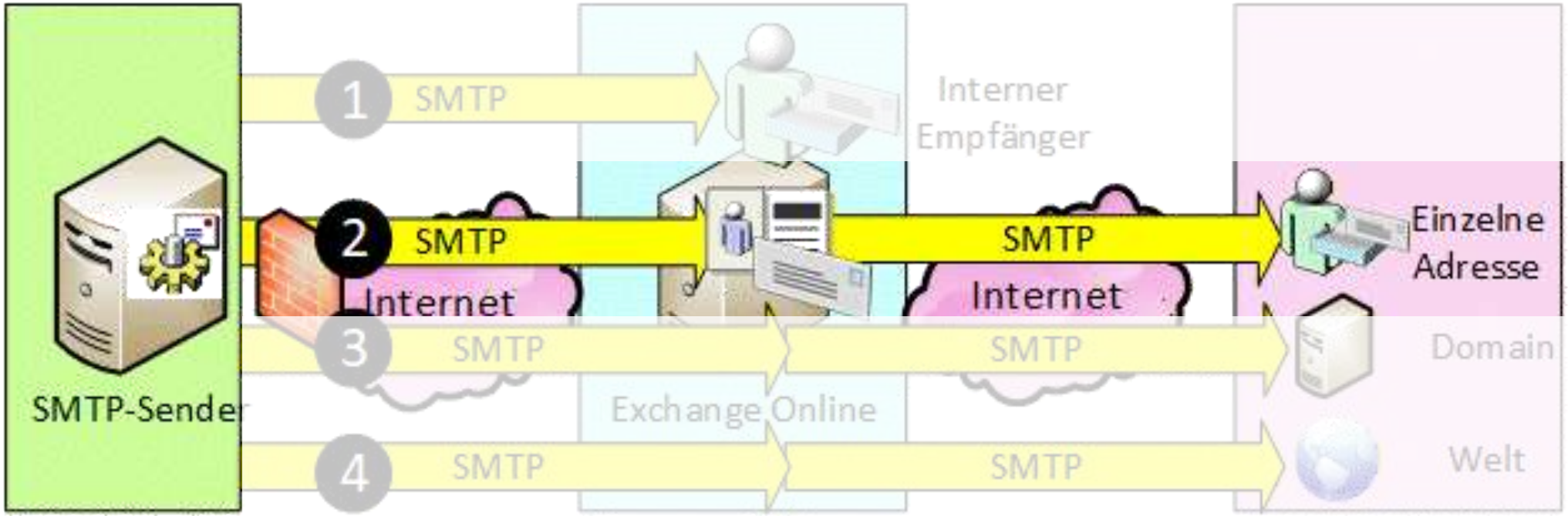
Szenario: Mail an interne Empfänger

- Anwendungsfälle
  - Scan2Mail
  - „Backup erfolgreich“
  - Monitoring-Meldungen
  - Formulare auf Webseiten
- Anonym zustellen
  - Risiko Spamfilter
  - Erkennen als Phishing
- DirectSend
  - Inbound Connector
  - SPF-Eintrag
  - Absender fälschbar



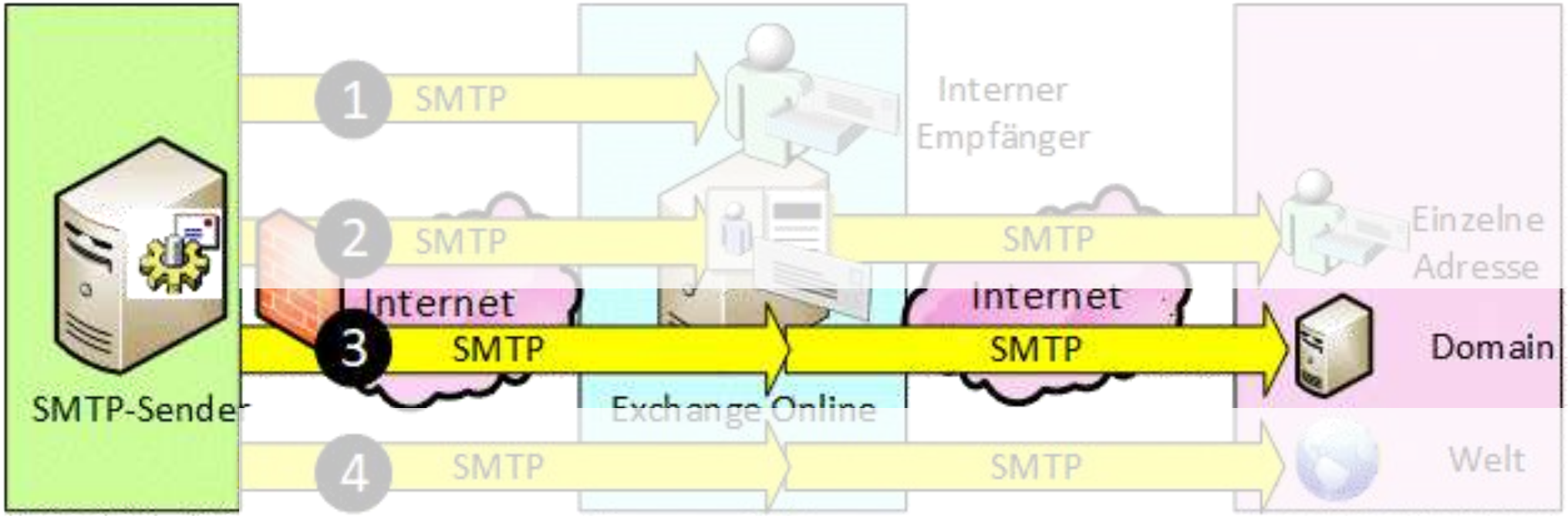
Szenario: Mail an 1x externen Empfänger

- Einsatzfall
  - Druckerwartung (Toner Low)
  - Alarmmails an externen Dienstleister
  - Externe Support-Postfächer
- Mailkontakt in Exchange Online
  - ProxyAdresse aus eigener Domain
  - Zieladresse ist extern
  - Oder Transportregel
- Anonym einliefern
  - Absicherung mit (DirectSend)



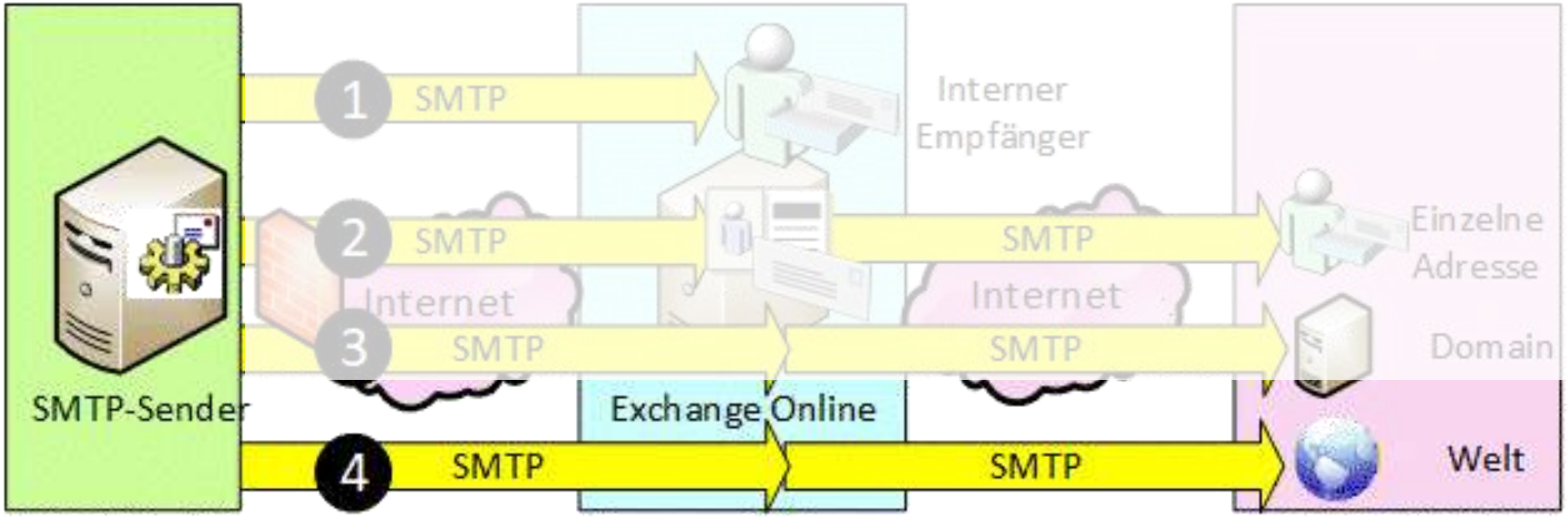
Szenario: Mail an eine einzelne externe Domain

- Einsatzzweck
  - Partnerunternehmen, Konzernmitglieder
- OnPremises: Accepted Domain: External Relay + Connector
- Online: OnPrem-Connector (Zertifikat oder IP-Adresse, Absenderdomain aus AcceptedDomain)
  - Achtung: nur noch mit Hybrid oder Microsoft Support Ticket möglich, da Missbrauchspotential



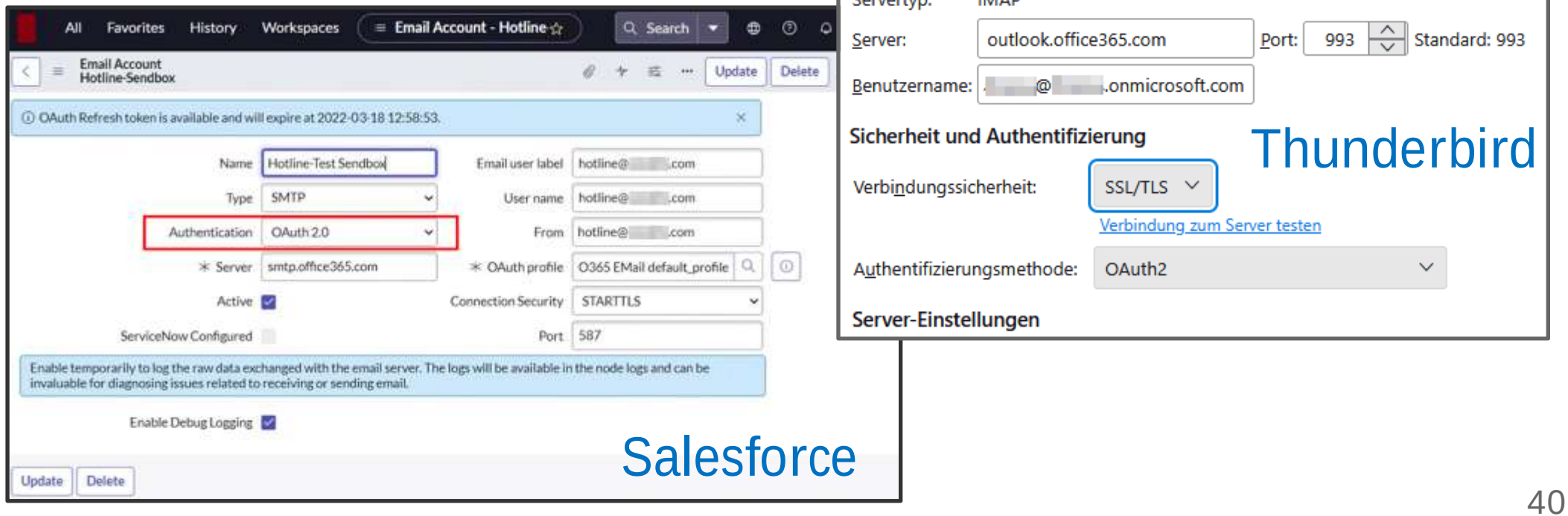
Szenario: Versand in die Welt

- Der einzige Weg, der durch die Abschaltung wirklich betroffen ist, wenn Sie keine OAUTH-Anmeldung an Exchange Online durchführen können.



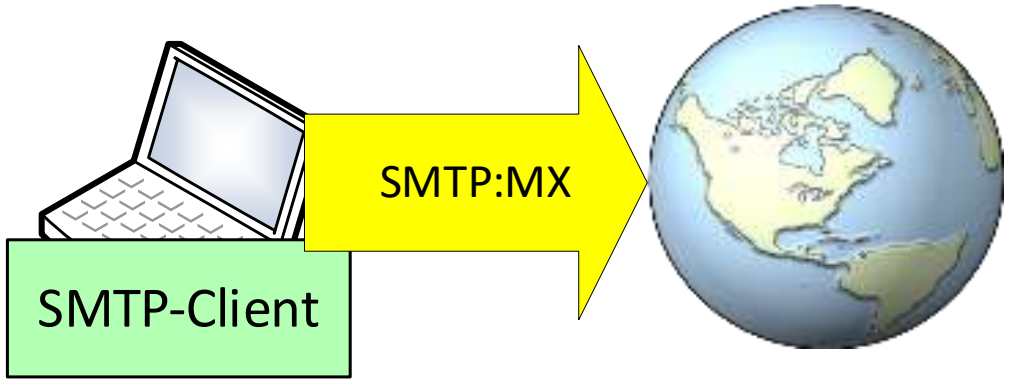
Option 1: Anmelden per OAUTH

- Client kann OAUTH
- Administrator muss ggfls. AppID zulassen (Consent)
- Client nutzt Username/Kennwort/AppID gegen Entra ID um ein SAML/OAUTH-Token zu holen
- SMTP-Client meldet sich per OAUTH-Token an
- Exchange Online Postfach mit Lizenz erforderlichb



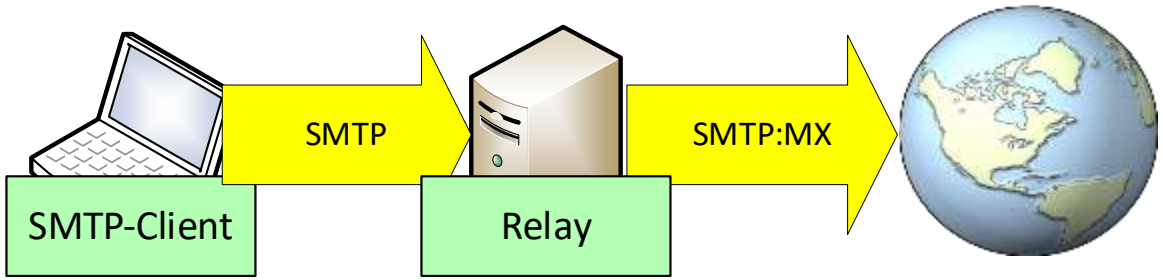
Option 2: Direkter Eigenversand

- Software/Skript sendet selbst
- Firewall-Freischaltung
- DNS-Auflösung: MX-Record
- SPF-Eintrag für die Domain!
- Queuing, Fehlerbehandlung



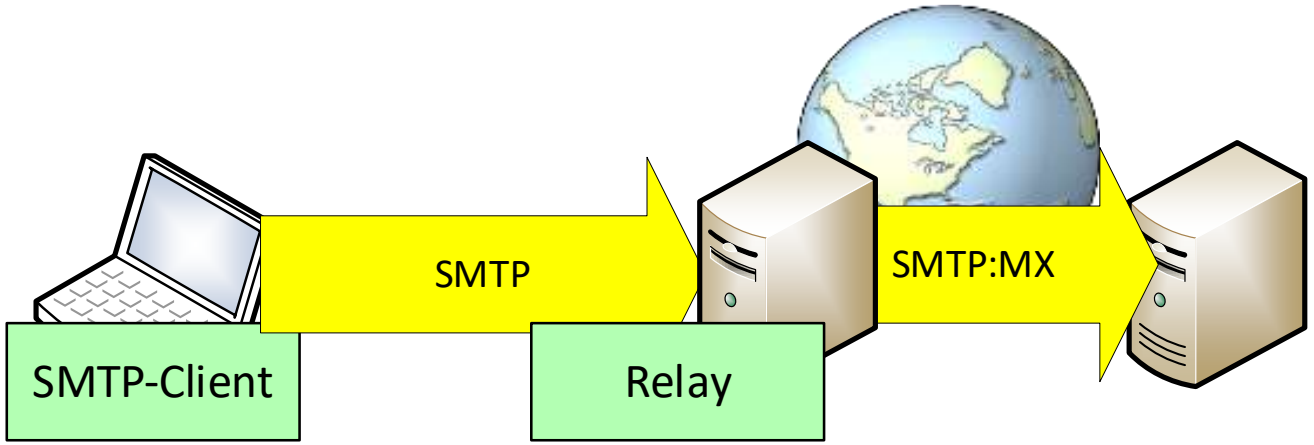
Option 2: Versand über eigenen Smarthost/Relay

- Eigener lokaler SMTP-Server
  - Postfix, SendMail, Exim,
  - Hinweis: Windows SMTP-Service ist EOL
  - HMailServer u.a. (Lifecycle beachten https://www.hmailserver.com/state)
  - SMTP als Modul ihrer Netzwerkfirewall
  - Betriebskostenb
- Exchange Hybrid Server
  - Könnte auch POP3/IMAP4 mit BasicAuth intern bereitstellen
  - Local Bridgehead für eingehendes SMTP
- SMTP-Proxy mit OAUTH
  - O2Popper
    https://www.nips.ac.jp/~murata/o2popper/
  - Email OAuth 2.0 Proxy
    https://github.com/simonrob/email-oauth2-proxy
- SPF/DKIM beachten



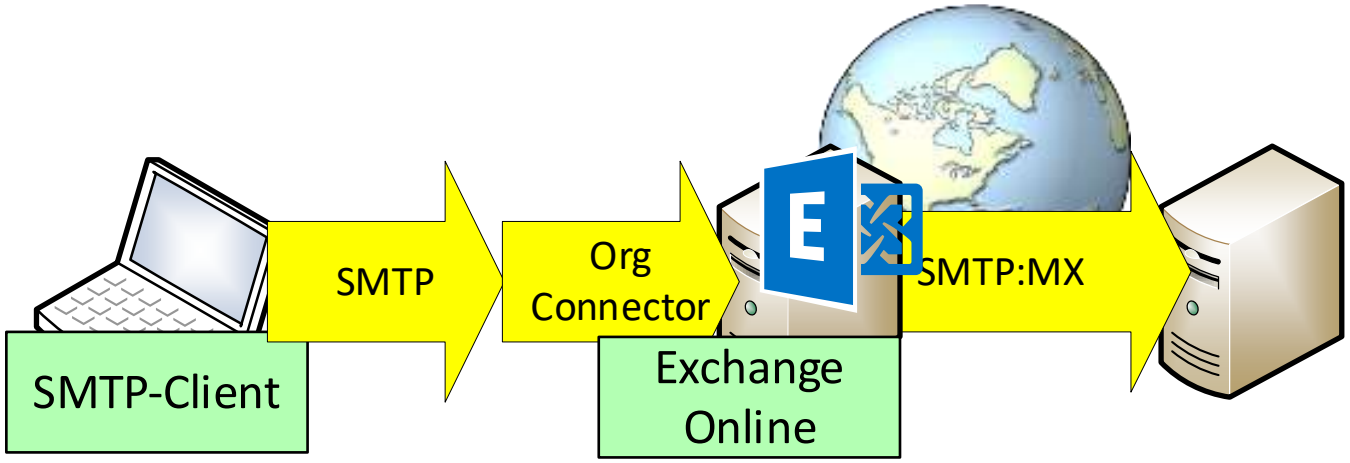
Option 3: Versanddienstleister

- Externe 3rd Party Relays
  - Azure Communication Services
  - Amazon AWS SMTP-Relay, SendGrid, MailGun, Mailchimp, etc.
- Webhoster
  - Meist bieten Sie auch SMTP mit BasicAuth an
  - Webseiten sendet sowieso per PHP-Mail
- Dran denken
  - SPF/DKIM
  - Geeignete Domain



Option 4: Exchange Online Organization Connector

- Achtung: Versender kann sich als „Exchange Server“ ausgeben
- MTLS mit Zertifikat (oder Source-IP)
- Inbound Organization Connector
- Absenderdomain muss in „AcceptedDomain“ sein
- TERRL/ERRL gelten weiter



SPF, DKIM,

DMARC, ARC

–

und p=reject

SPF und DKIM

- Wer hat noch nicht „SPF -All“ und „DMARC p=reject?
  - Es geht um Phishing-Schutz und Missbrauch, um zuverlässige Zustellung (Google)
  - Jede Domain ist individuell, alle User einer Domain habe die gleiche Einstellung
- SPF
  - Prüft, ob Absenderdomain (Envelope-From) oder Mailserver zur IP-Adresse der Domain passen
  - Einfache Variante gegen Missbrauch der eigenen Domain.
  - Keine Lösung für Weiterleitungen, Mailinglisten etc. oder Fälschung der „Header-From“-Adresse
- DKIM
  - Autorisierter Server signiert die Mail und öffentlicher Schlüssel ist im DNS
  - Empfangender Mailserver kann Authentizität prüfen, auch wenn Source-IP nicht passt.
  - Domain wird aus dem „Header-From“ genutzt.
  - Schutz gegen Veränderungen der Mail

DMARC, ARC – und p=reject

- DMARC steuert folgende Dinge
  - Alignment: Der Abgleich der Absenderdomain aus Header und Envelope
  - Reporting: Welche Reports gehen an welche Mailboxen
    - rua=<mailadresse> für Analysereport
    - ruf=<mailadresse> für forensische Reports (Datenschutz beachten)
    - Reporting macht meist Dienstleister (25Reports, Dmarcian, Agari, u.a.)
  - Policy: Steuert, wie der Empfänger bei nicht verifizierten Mails damit umgehen sollte
    - p=none | quarantine | reject

  Achtung: funktioniert alles nur, wenn der Empfänger auch DMARC auswertet

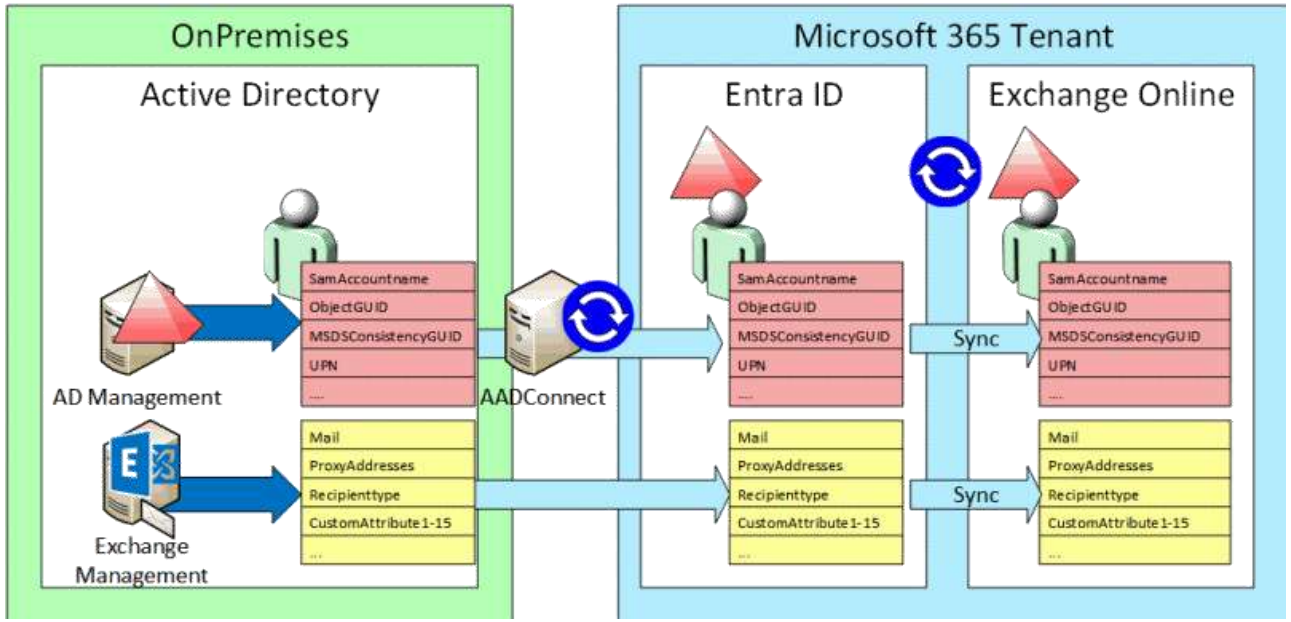
- Einführung
  - Vorarbeit: Absende-Server in SPF aufnehmen, DKIM signieren
  - Start: DMARC mit p=none + RUA + Auswerten
  - Dazwischen: SPF/DKIM und Mailserver richtig konfigurieren
  - Einige Wochen später; p=reject

Exchange Online ohne lokales Exchange

isExchangeCloudManaged

Exchange Online mit Entra ID Sync

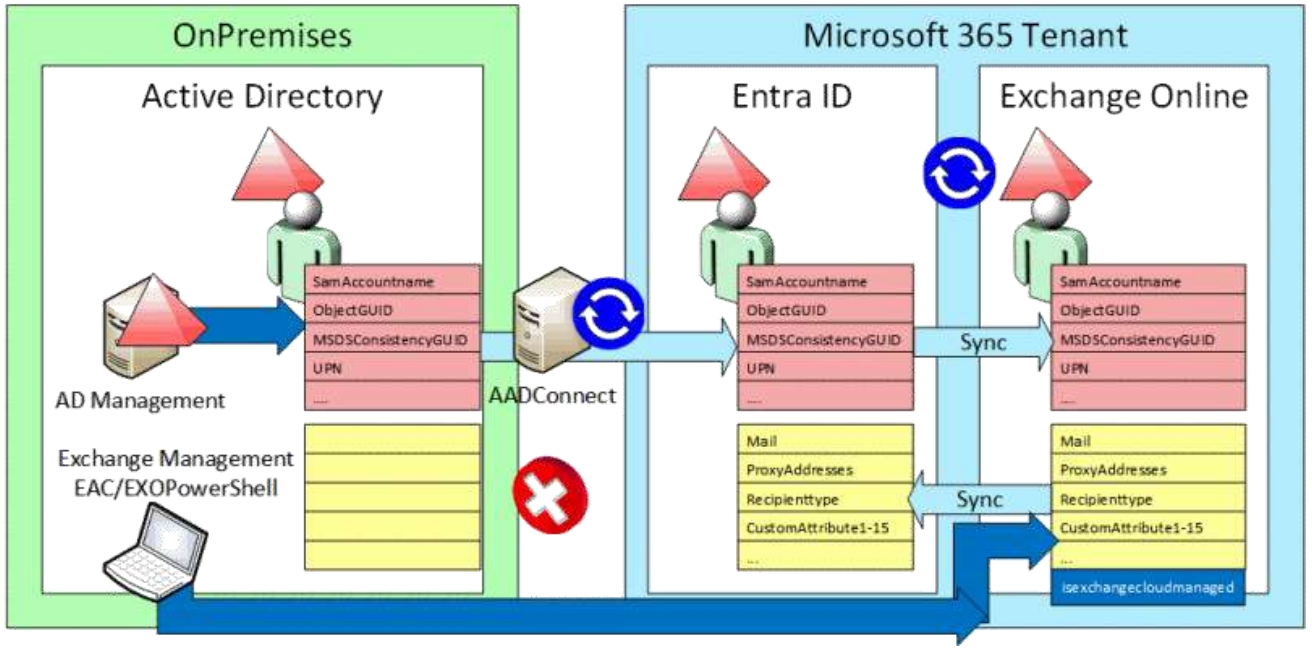
- Klassisches Modell
  - Lokales AD mit Exchange Schema
  - Verwaltung mit Exchange Server (PowerShell oder ECP, RBAC, Auditing
  - Verwaltung mit Exchange Management Shell (PowerShell, lokale Rechte
- Nicht erlaubt
  - Direkte Änderungen mit ADSIEDIT/LDAP



https://www.msxfaq.de/cloud/exchangeonline/betrieb/exchange_online_provisioning.htm

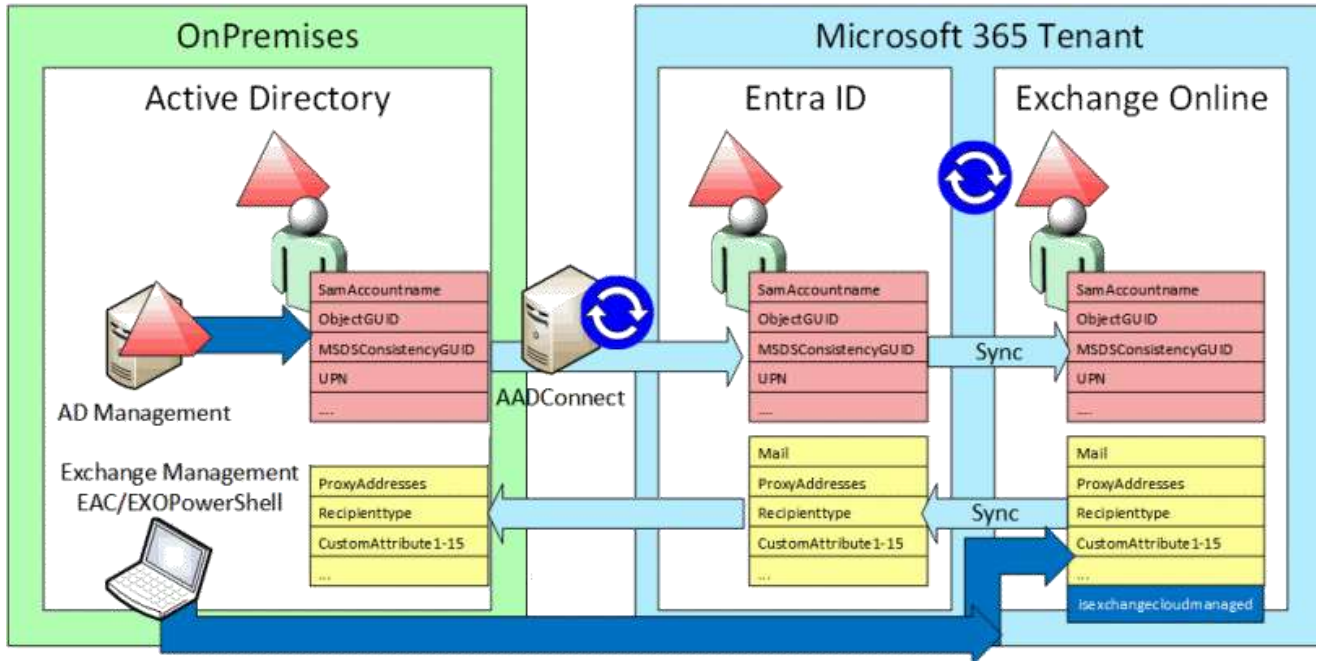
Exchange mit „isExchangeCloudManaged“

- Seit Oktober 2025 GA
  - Mindestens Entra ID Connect 2.5.76.0, Besser 2.5.190.0
- Pro Benutzer in Exchange Online aktivierbar
  - EXOPS: Set-Mailbox <identity> -IsExchangeCloudManaged:$true
- Auch als Default für neue Objekte
  - EXOPS: Set-OrganizationConfig -ExchangeAttributesCloudManagedByDefault
- Nicht für Gruppen
  - Cloud Only Verteiler
- Nicht für MailContacts
  - Gastuser
  - CloudOnly Kontakte



isExchangeCloudManaged und WriteBack (Phase 2)

- „Coming Soon“ (überfällig)
- Erfordert Entra Cloud Sync oder Connect Sync 2.5.190.0
- Writeback der Exchange Properties
  - Viele aber nicht alle
  - z.B. nicht „mail“
  - Z.B. nicht MailNickName
- Ausblick: Cloud SOA
  State of Authority
  - User
  - Kontakte
  - Gruppen



Links

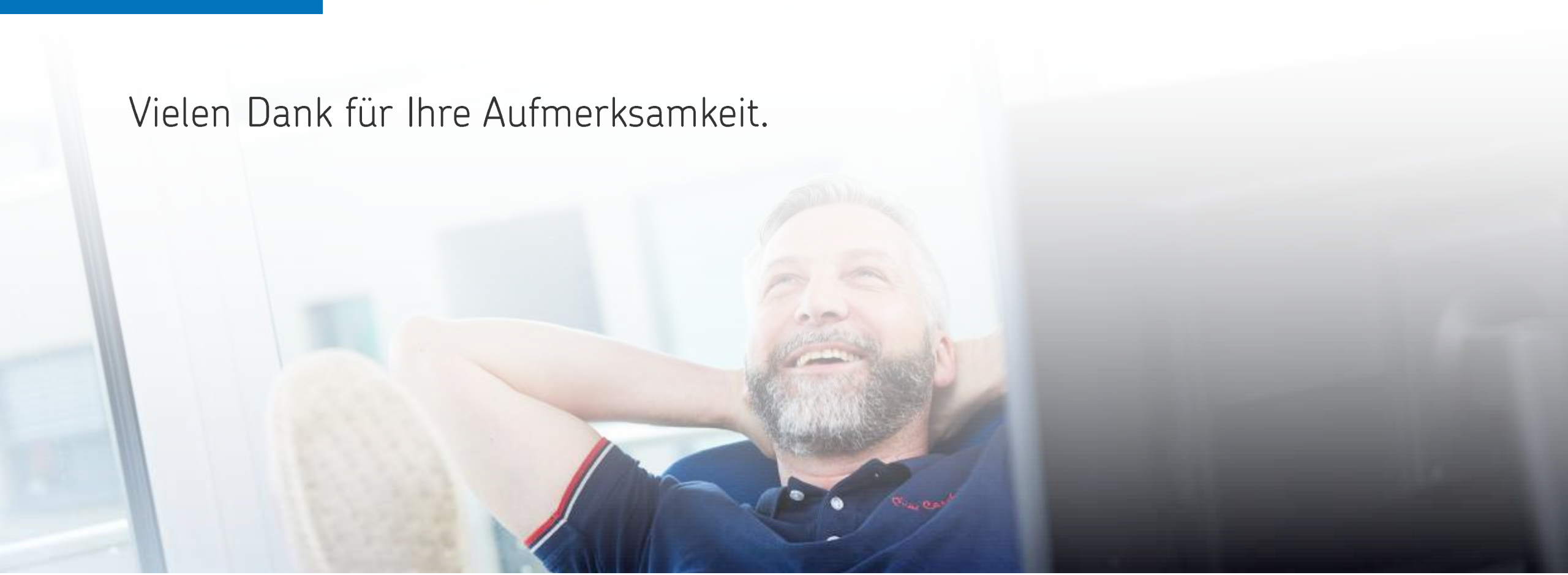
- Cloud-based management of Exchange attributes for Remote Mailboxes in hybrid environments
  https://learn.microsoft.com/en-us/exchange/hybrid-deployment/enable-exchange-attributes-cloud-management
- https://www.msxfaq.de/cloud/exchangeonline/betrieb/provisioning_mit_isexchangecloudmanaged.htm
- https://www.msxfaq.de/cloud/exchangeonline/betrieb/isexchangecloudmanaged.htm
- https://learn.microsoft.com/en-us/exchange/hybrid-deployment/enable-exchange-attributes-cloud-management
- Configure user Source of Authority
  https://learn.microsoft.com/en-us/entra/identity/hybrid/how-to-user-source-of-authority-configure
- Configure Group Source of Authority
  https://learn.microsoft.com/en-us/entra/identity/hybrid/how-to-group-source-of-authority-configure
- Configure Contact SOA
  https://learn.microsoft.com/en-us/entra/identity/hybrid/how-to-user-source-of-authority-configure#configure-contact-soa
- Group writeback with Microsoft Entra Cloud Sync
  https://learn.microsoft.com/en-us/entra/identity/hybrid/group-writeback-cloud-sync

Bonusthemen

Bonus Themen

- Exchange Online SMTP-Hintertür
  - MX-Record für „<tenantname>.onmicrosoft.com“, „<tenantname>.mail.onmicrosoft.com“
  - Jeder User hat eine MOERA-Adresse und die ist auch erreichbar!
  - Hintertür, wenn man 3rd Party Spamfilter nutzt -> Partner Connector mit „*“
- Exchange Online Transport Limits
  - TERRL – Tenant External Recipient Limit ($500 * (Lizenzen^{0,7}) + 9500$ pro 24h, pro Tenant
  - ERRL – External Recipient Limit (10.000 Recipients, davon max. 2000 externe pro 24h
- Exchange OnPremises MFA
  - Ist ihr OnPremises Server noch erreichbar (z.B. Autodiscover, EWS)
  - Welche Authentifizierung bietet ihr Server an? Risiko bei Basic/Negotiate
  - Hybrid Modern Auth oder PreAuthentication (Reverse Proxy)
- Exchange Hybrid Dedicated Hybrid App
  - Seit Oktober 2025 erforderlich
  - Free/Busy-Anfragen von OnPremises Postfach an EXO-Postfach geht sonst nicht mehr
- Microsoft 365 Message Center
  - Aktuell Quelle, auch für OnPremises Änderungen
  - Update per Mail in Support Ticket System, Planner oder Dienstleister

Vielen Dank für Ihre Aufmerksamkeit.



Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn

Kontakt
jane.doe@netatwork.de
john.doe@netatwork.de

Building IT-Excellence.

www.netatwork.de