Exchange Server und TLS-Zertifikate

Tech Talk – 20

MVP
Microsoft®
Most Valuable Professional

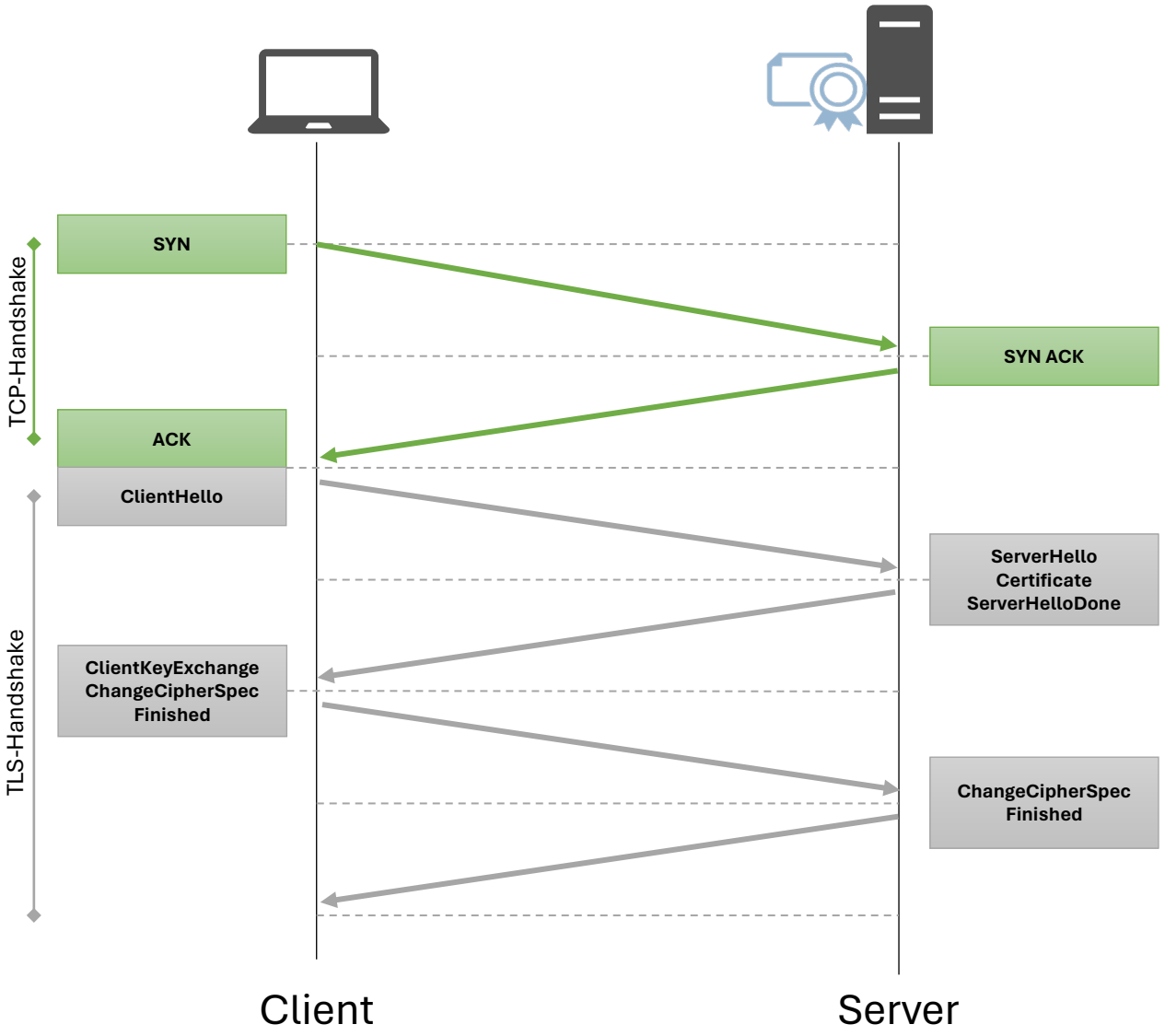
TLS – Transport Layer Security

Eine kurze Einführung

Transport Layer Security

- Verschlüsselte TCP-Verbindung zwischen zwei Systemen, die sich auf eine Form der Transportverschlüsselung geeinigt haben, bestehend aus
  - **TLS-Version**
  - **Verschlüsselungsmechanismus**
- Ziele von TLS
  - **Vertraulichkeit** – Die Datenübertragung erfolgt nicht als Klartext
  - **Authentifizierung**
    - Überprüfung der Serveridentität durch den Client (Hauptanwendungsfall für HTTPS-Verbindungen)
    - Überprüfung der Clientidentität durch den Server
  - **Integrität** – Schutz gegen Manipulation der Datenübertragung
- Ports für TLS-verschlüsselte Verbindungen (Auswahl)
  - TCP 443 – HTTPS
  - TCP 995 – POP3
  - TCP 993 – IMAP4
  - TCP 25, 587 – SMTP

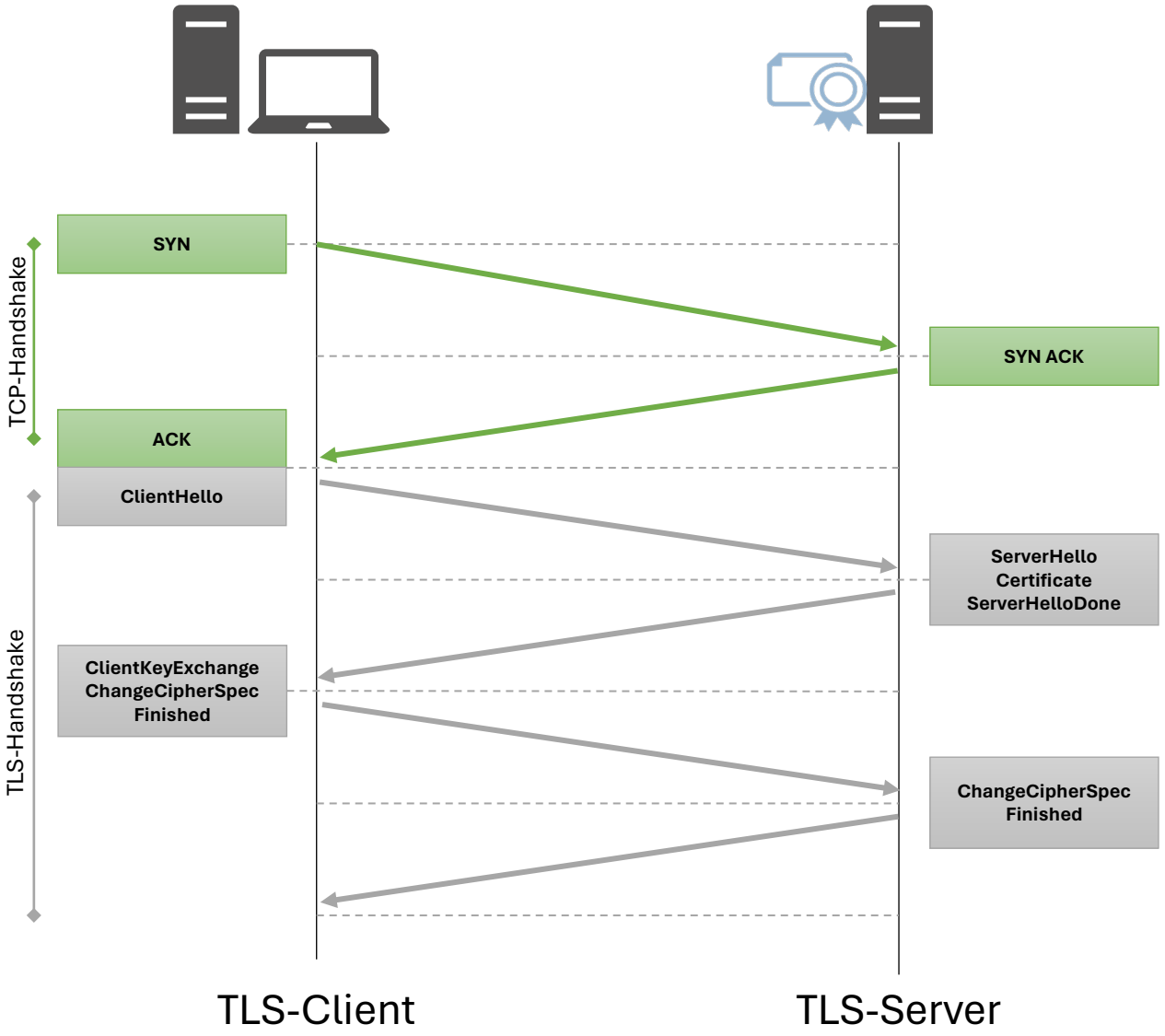
TLS-Verbindungsaufbau



TLS-Handshake

- Wahl der TLS-Version (1.3, 1.2, 1.1 usw.)
- Entscheidung über die zu verwendenden Cipher-Suiten
  - Verschlüsselungsschlüssel
  - Sitzungsschlüssel
- Authentifizierung der Server-Identität mit Hilfe des **Server**-Zertifikates
- Generierung der **Sitzungsschlüssel** für die weitere Kommunikation
- TLS 1.3 benötigt nur noch einen Round-Trip zur TLS-Aushandlung

TLS-Verbindungsaufbau



TLS-Handshake

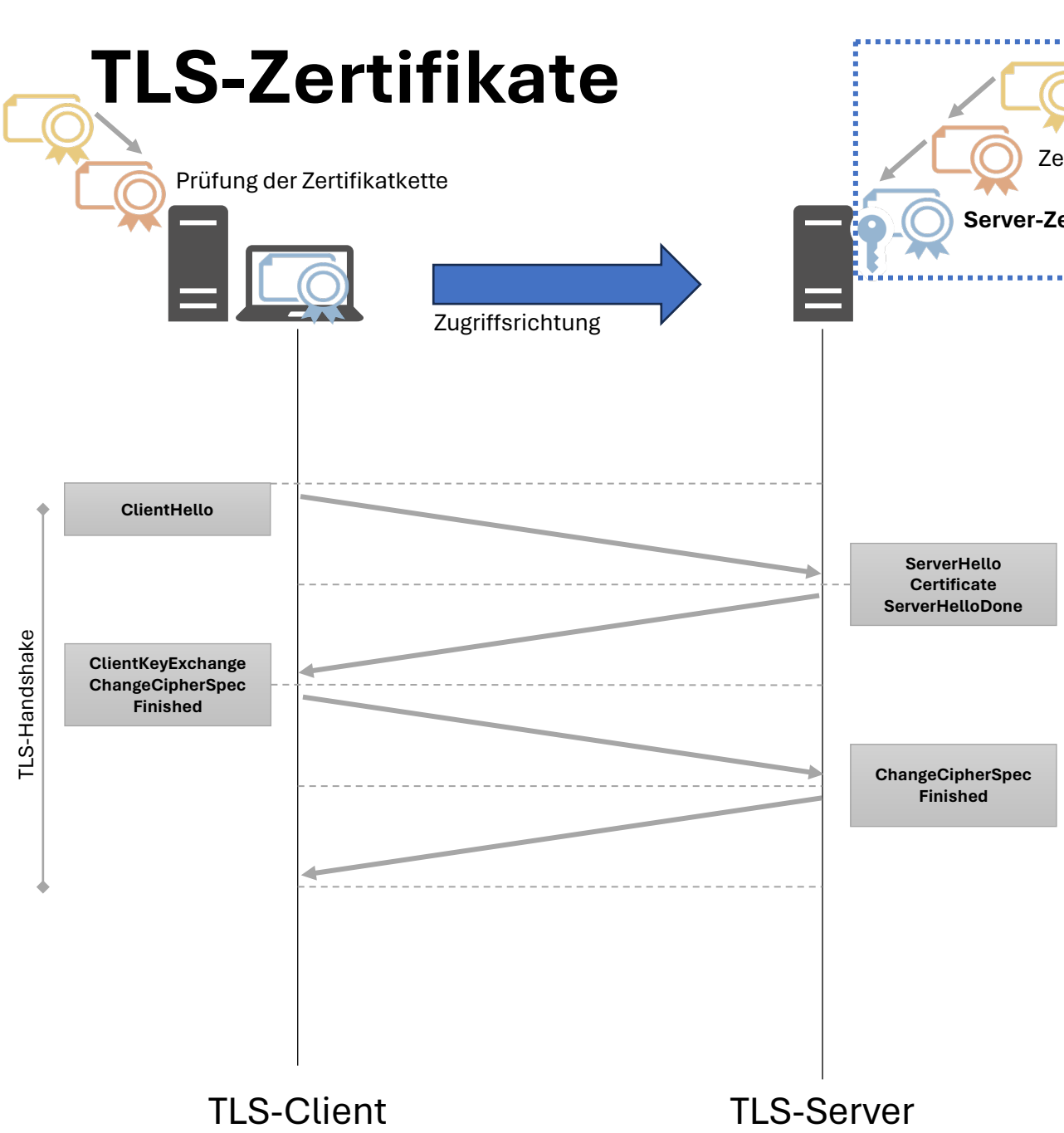
- Die Begriffe **Client** und **Server** bezeichnen den **Start-** und **Endpunkt** einer TLS-Verbindung
- **Client → *TLS-Client***
  - Das System, das die TLS-Verbindung initiiert
- **Server → *TLS-Server***
  - Das System, das die TLS-Verbindung bedient und steuert

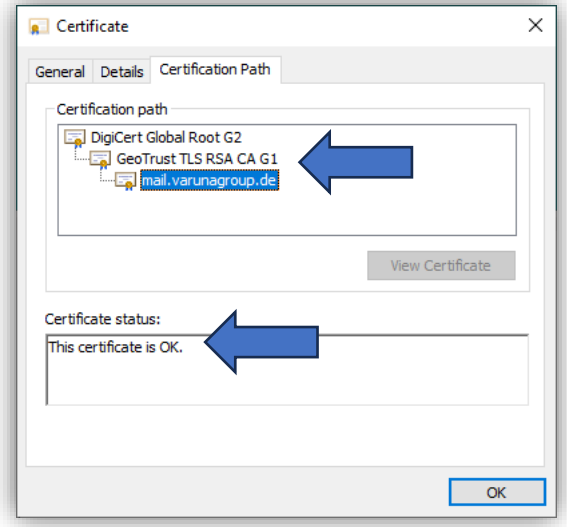
- Die Begriffe beziehen sich **nicht** auf Client- oder Server-Betriebssysteme
- Ein Betriebssystem kann somit TLS-Client **und** TLS-Server zugleich sein

Exchange Server, TLS, Cipher Suiten und CRLs

Abhängigkeiten und Fallstricke

TLS-Zertifikate



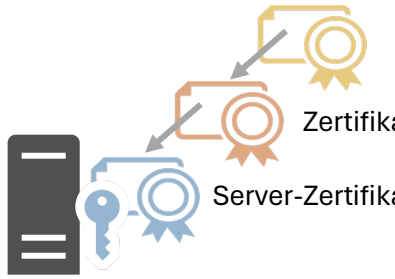


TLS-Handshake

- TLS-Server
  - Server-Zertifikat kann nur verwendet werden, wenn die **TLS-Zertifikatkette** intakt ist
- TLS-Client
  - TLS-Verbindung wird nur aufgebaut, wenn das Server-Zertifikat überprüft werden kann
  - Alle Zertifikate des Zertifikatkette müssen auf dem TLS-Client vorhanden sein
  - Optionale manuelle Bereitstellung der Zertifikate von Root- und Zwischen-zertifizierungsstellen

TLS-Protokolle

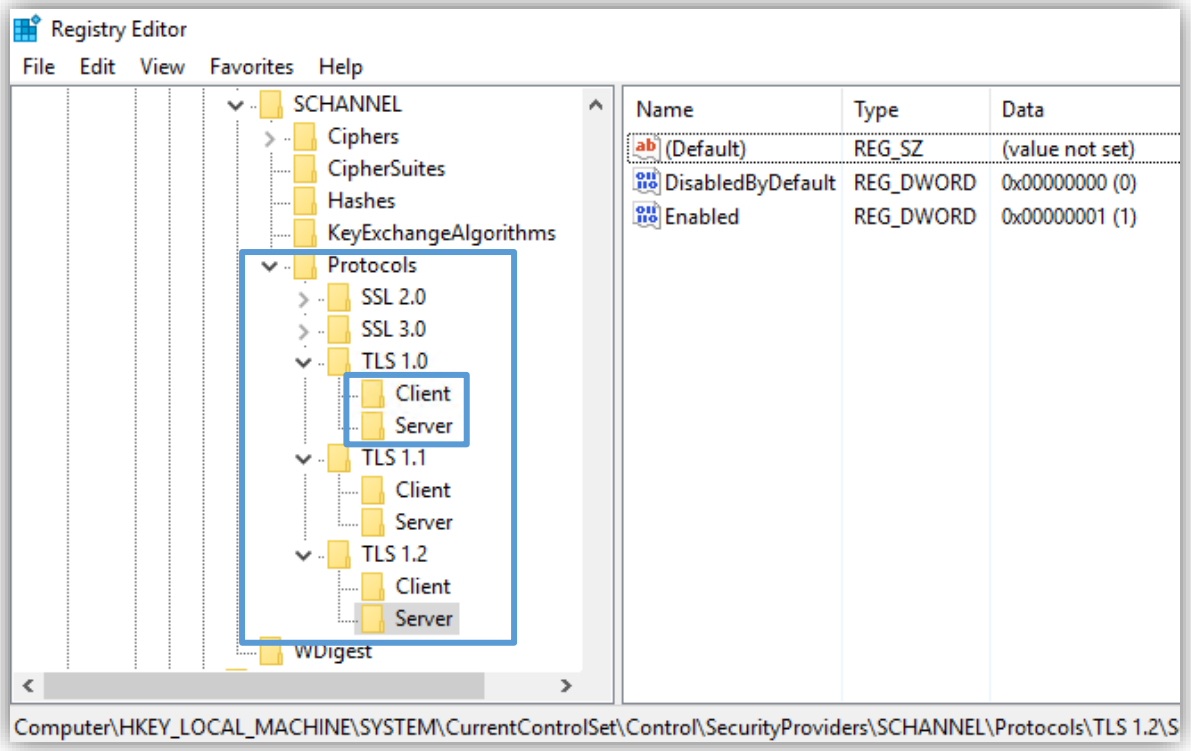
Zugriffsrichtung



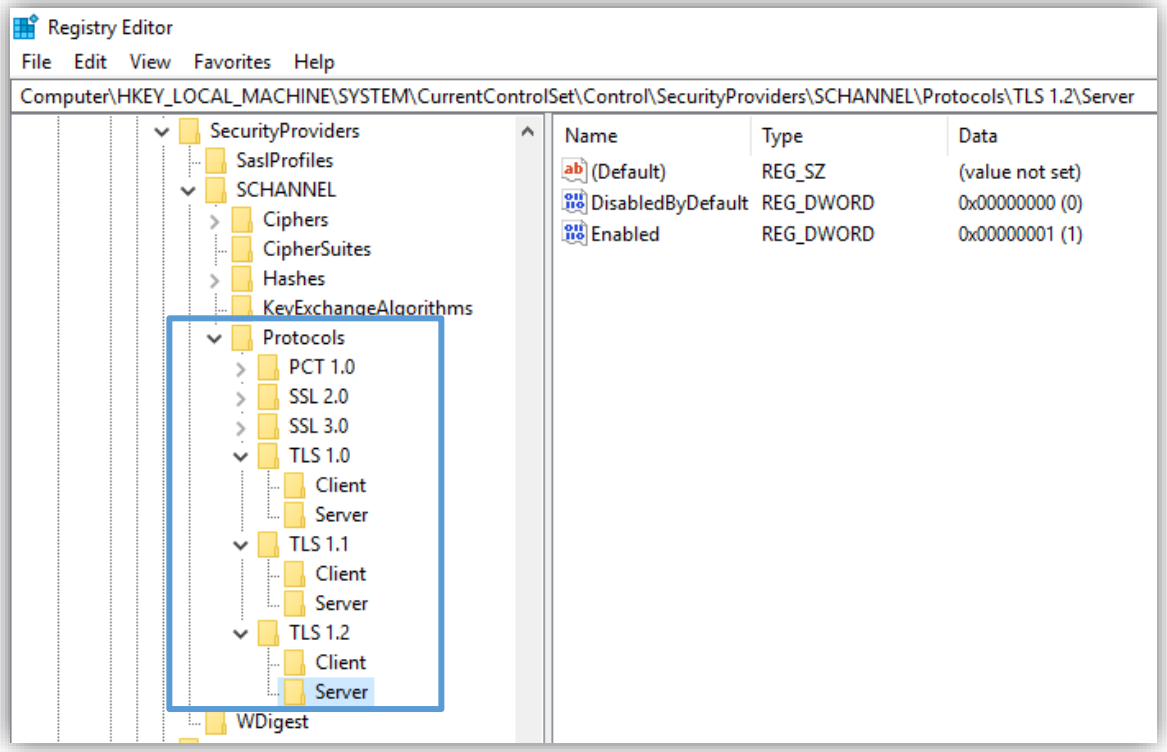
Zertifikat der Root-Zertifizierungsstelle

Zertifikat der Zwischenzertifizierungsstelle

Server-Zertifikat



Exchange Server 2016
auf Windows Server 2016

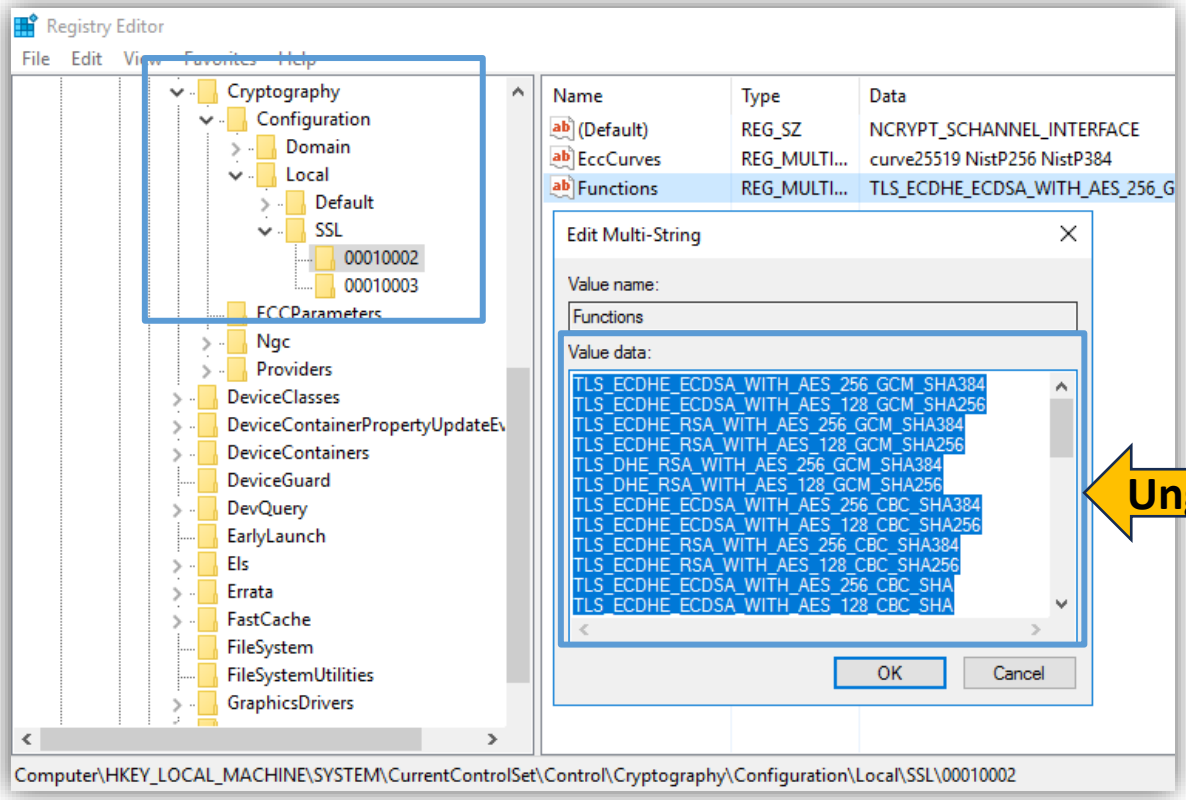


Exchange Server 2019
auf Windows Server 2019

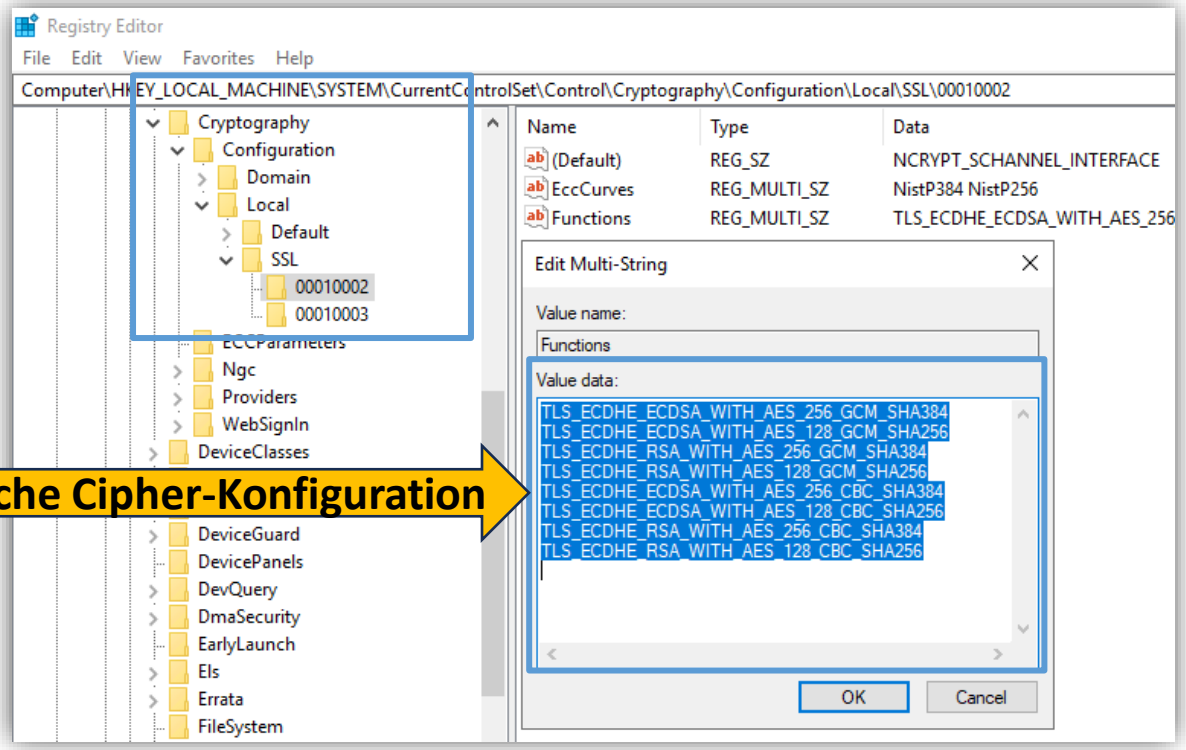
HKLM\SYSTEM\CurrentControlSet\Control**SecurityProviders**\SCHANNEL

TLS-CipherSuiten

Exchange Server 2019 konfiguriert CipherSuiten des Betriebssystems



Ungleiche Cipher-Konfiguration

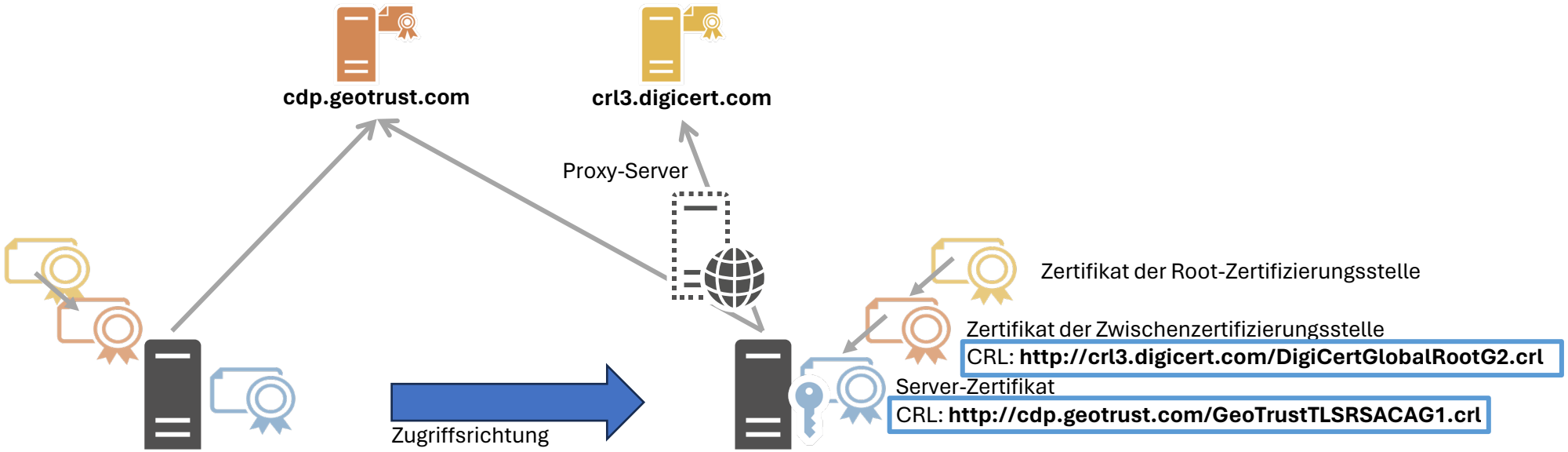


Exchange Server 2016
auf Windows Server 2016

Exchange Server 2019
auf Windows Server 2019

HKLM\SYSTEM\CurrentControlSet\Control**Cryptography**\Configuration\Local\SSL\00010002

CRL – Certificate Revocation List

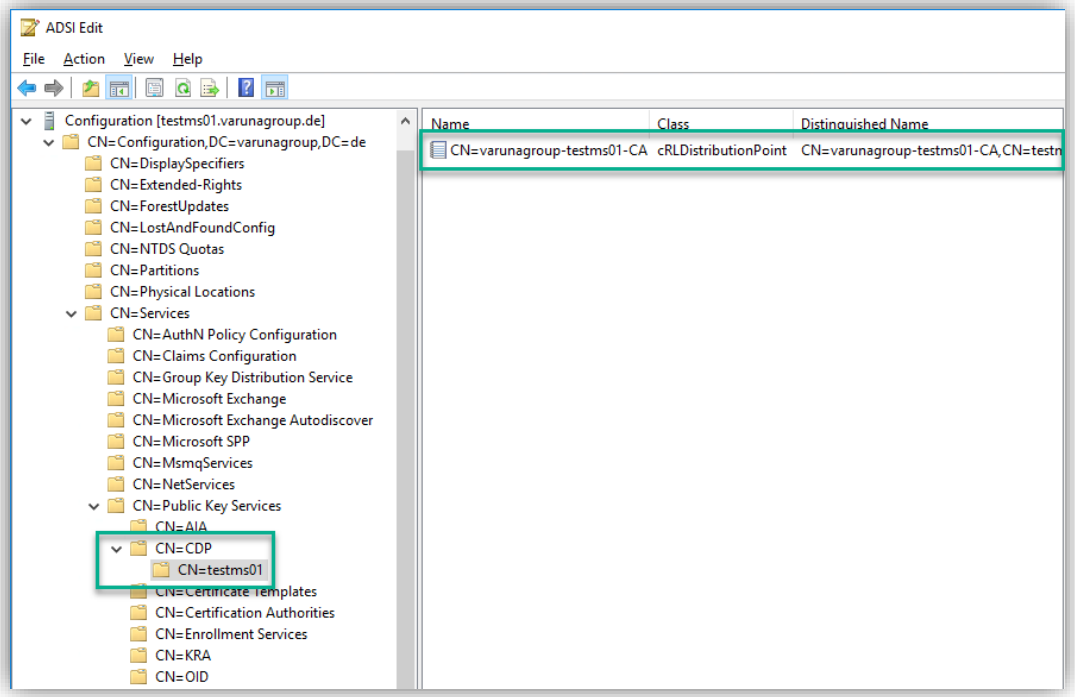


- Eine Zertifizierungsstelle stellt eine Liste der zurückgezogenen Zertifikate zur Verfügung
  → Zertifikatsrückzugliste – Certificate Revocation List, CRL
- Ein Zertifikat enthält Informationen über den zugehörigen CRL-Endpunkt
- Bereitstellung u.a. über LDAP, HTTP
  - Systeme müssen in der Lage sein, (externe) CRL-Endpunkte zu erreichen
- Der CRL-Endpunkt **kann**, muss aber nicht abgefragt werden

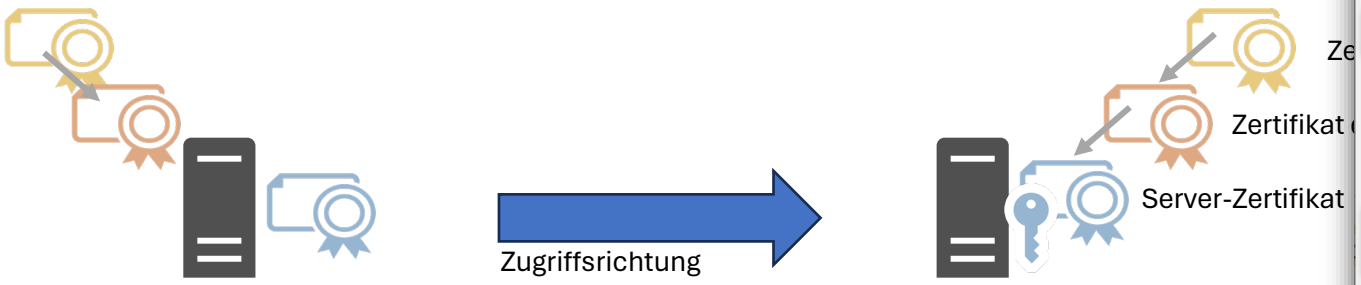
→ Der Verzicht auf die Prüfung eines zurückgezogenen Zertifikates **beeinträchtigt** die **TLS-Sicherheit**

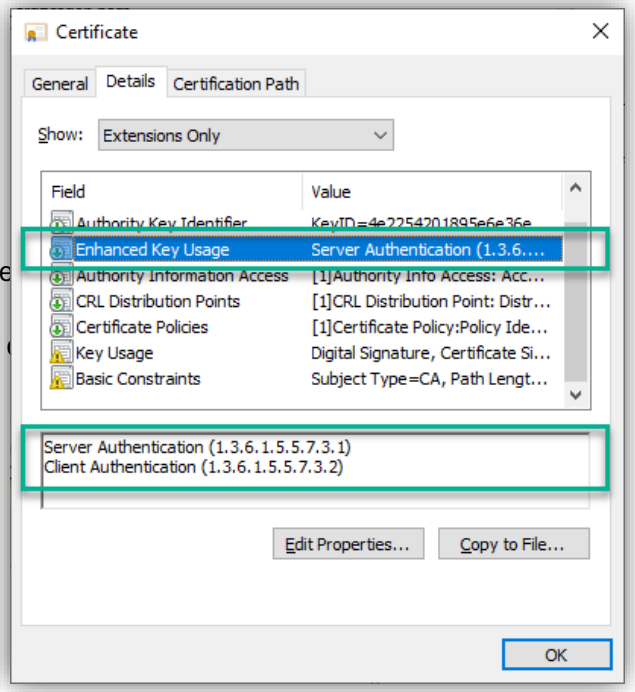
CRL – Certificate Revocation List

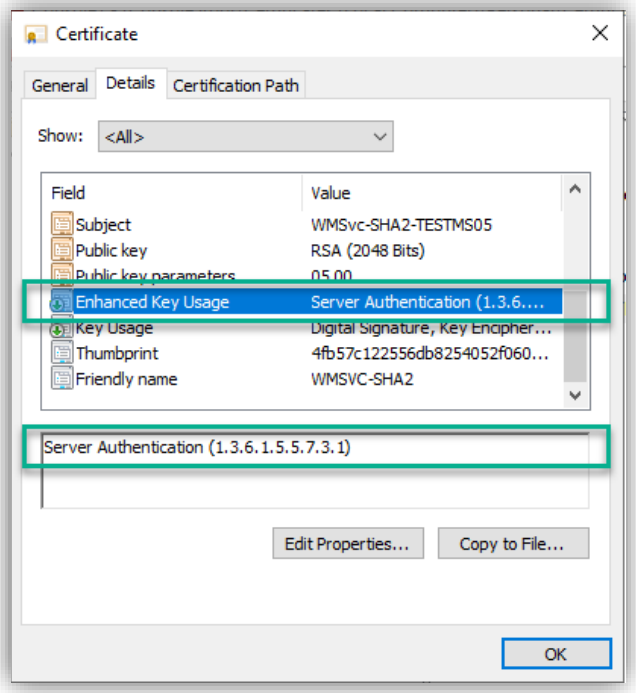
- Eine Microsoft **Enterprise-Zertifizierungsstelle** nutzt im Standard einen **LDAP-Endpunkt**
  Beispiel:
  - ldap:///CN=varunagroup-testms01-CA,CN=testms01,CN=CDP,CN=Public Key Services,CN=Services,**CN=Configuration,DC=varunagroup,DC=de**?certificateRevocationList?base?objectClass=cRLDistributionPoint
- Die CRL-Speicherung erfolgt in der **Active Directory Configuration Partition**
- Weitere Endpunkte müssen in Konfiguration der Zertifizierungsstelle vor der Ausstellung von produktiven Zertifikaten zusätzlich **manuell** konfiguriert werden



Verwendungszweck eines Zertifikates







- **Key Usage** und **Enhanced Key Usage** Parameter definieren den Verwendungszweck eines Zertifikates für das lokale System
- Key Usage
  - **Digital Signature**, **Key Encipherment**
- Enhanced Key Usage
  - **Server Authentication** (1.3.6.1.5.5.7.3.1)
    Das Zertifikat kann für die Bereitstellung einer TLS-Verbindung als TLS-Server verwendet werden
  - **Client Authentication** (1.3.6.1.5.5.7.3.2)
    Das Zertifikat kann zur Authentifizierung als TLS-Client zum TLS-Server verwendet werden

Weitere Anwendungsfälle für Zertifikate

- TLS-Client Authentifizierung
  - Ein TLS-Server erwartet, dass der TLS-Client ein **bestimmtes** TLS-Zertifikat präsentiert, um sich als legitim **auszuweisen**
  - Das Zertifikat muss nicht unbedingt identisch mit dem Zertifikat für die TLS-Verbindung selbst sein
- S/MIME-E-Mail-Verschlüsselung
  - Zertifikatsbasierte **Verschlüsselung** von E-Mail-Nachrichten
    - Erweiterte Schlüsselverwendung: **Digitale Signatur**, **Schlüsselverschlüsselung**, **Datenverschlüsselung**
    - Schlüsselverwendung: **Sichere E-Mail** (1.3.6.1.5.5.7.3.4)
  - **Common Name** enthält die **primäre E-Mail-Adresse**
  - **Alternative Namen** können bei Bedarf weitere E-Mail-Adressen enthalten, z.B. bei Domainänderungen
  - Persönliche Zertifikate mit unterschiedlicher **Sicherheit für die Validierung** der E-Mail-Adresse im Zertifikat
    → Ausführliche Validierung (Enhanced Validation, EV) = Höherer Preis
- Signierung und Verschlüsselung von **Authentifizierungstoken**
  - Verbundauthentifizierung mit **AD FS** oder **Entra ID**

Was bedeutet all das für Exchange Server?

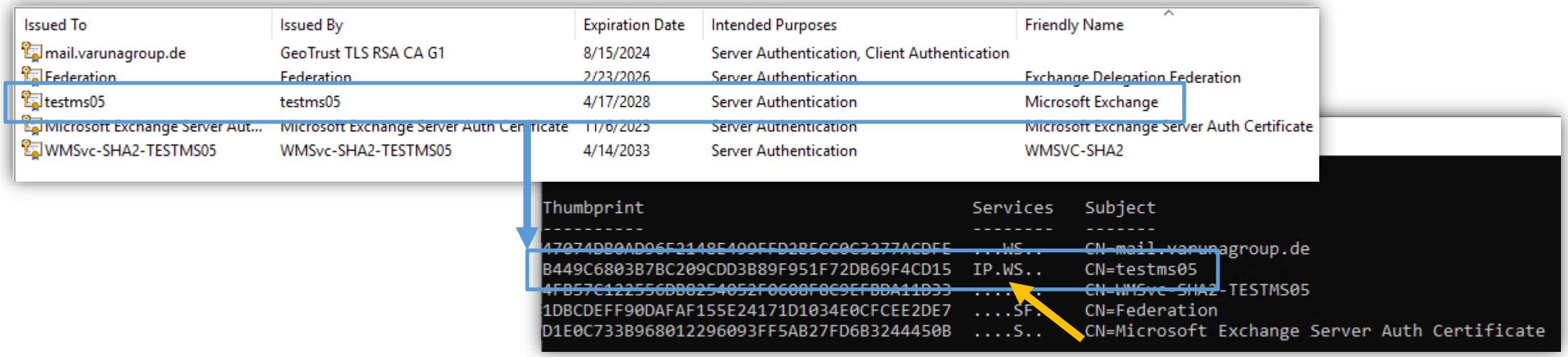
Exchange Server und Exchange Online

TLS-Abhängigkeiten

Exchange Server - Standardzertifikate

"**Microsoft Exchange**"-Zertifikat

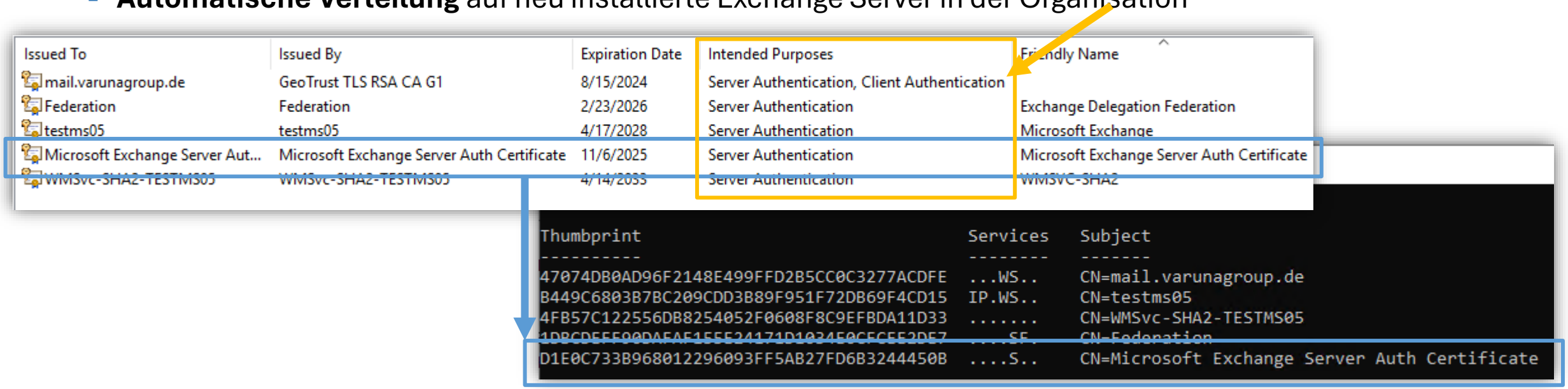
- **Selbstsigniertes** TLS-Zertifikat mit dem NETBIOS- und FQDN-Namen des lokalen Servers
- **Exchange Setup** erstellt dieses Zertifikat und bindet es automatisch für SMTP, POP3, IMAP4 und IIS
- **Automatisch vertrauensvoll** für **alle Exchange Server** der Organisation, **inkl.** Edge-Transport-Server
- Interne und externe Clients vertrauen dem Zertifikat nicht
- Nutzung für **Opportunistic TLS**
- SHA256 Signatur-Hash für neue Installationen ab [Exchange 2019 CU11 oder Exchange 2016 CU22]



Exchange Server - Standardzertifikate

"**Microsoft Exchange Server Auth Certificate**"-Zertifikat

- **Selbstsigniertes** TLS-Zertifikat mit **fünf Jahren** Laufzeit
- Absicherung der **Exchange Server-zu-Server-Kommunikation**
- Absicherung der **OAuth Server-zu-Server-Kommunikation** mit externen Systemen, z.B. Skype for Business, Exchange Online
- Erste **Erstellung** durch den **ersten Exchange Server** in der Organisation, seit Exchange Server 2013
- **Automatische Verteilung** auf neu installierte Exchange Server in der Organisation



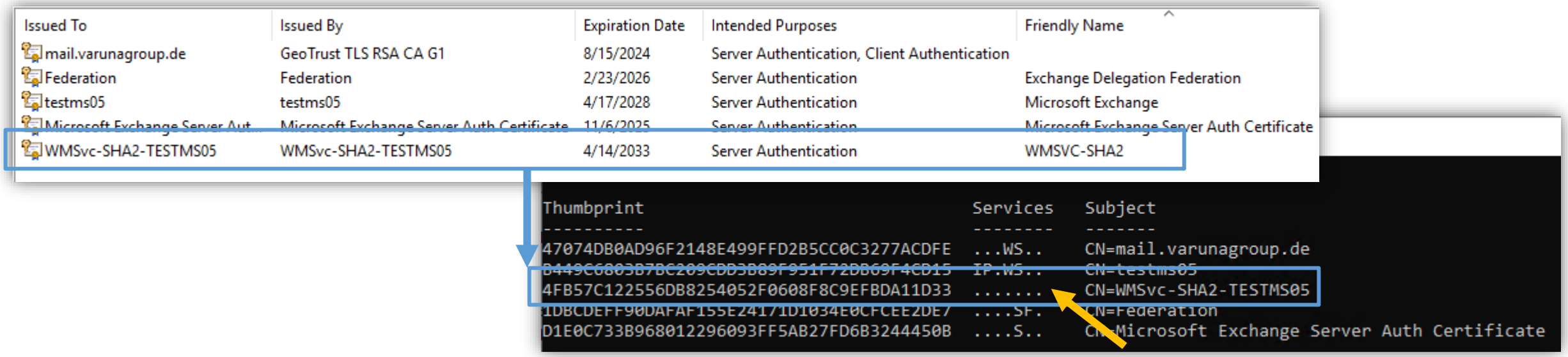
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
mail.varunagroup.de	GeoTrust TLS RSA CA G1	8/15/2024	Server Authentication, Client Authentication	
Federation	Federation	2/23/2026	Server Authentication	Exchange Delegation Federation
testms05	testms05	4/17/2028	Server Authentication	Microsoft Exchange
Microsoft Exchange Server Aut...	Microsoft Exchange Server Auth Certificate	11/6/2025	Server Authentication	Microsoft Exchange Server Auth Certificate
WMSvc-SHA2-TESTMS05	WMSvc-SHA2-TESTMS05	4/14/2033	Server Authentication	WMSVC-SHA2

```
Thumbprint                                Services   Subject
----------                                --------   -------
47074DB0AD96F2148E499FFD2B5CC0C3277ACDFE  ...WS..    CN=mail.varunagroup.de
B449C6803B7BC209CDD3B89F951F72DB69F4CD15  IP.WS..    CN=testms05
4FB57C122556DB8254052F0608F8C9EFBDA11D33  .......    CN=WMSvc-SHA2-TESTMS05
1DBCDEFF90DAFAF155F24171D1034F0CFCFE2DE7  ....SF.    CN=Federation
D1E0C733B968012296093FF5AB27FD6B3244450B  ....S..    CN=Microsoft Exchange Server Auth Certificate
```

Exchange Server - Standardzertifikate

"**WMSVC-SHA2**"-Zertifikat

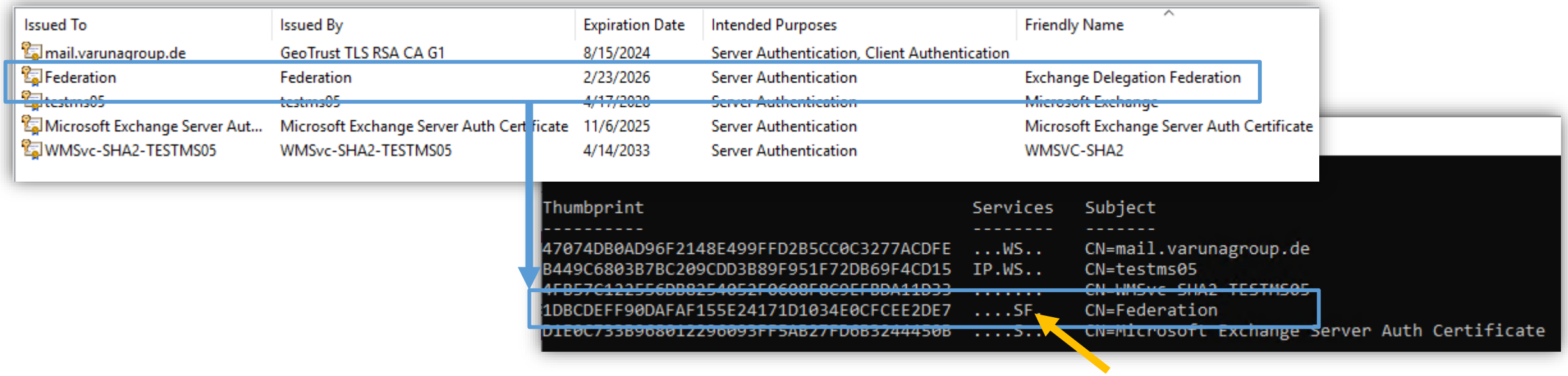
- **Selbstsigniertes** TLS-Zertifikat mit **zehn Jahren** Laufzeit
- Common Name ist **WMSVC-SHA2-*SERVERNAME***
- Absicherung des **Remote Management** für den **IIS Web Management Dienst** (WMSVC)
- WMSVC-Dienst kann **nicht ausgeführt** werden, wenn das Zertifikat **gelöscht** wurde
  → **Installation** von Exchange Updates oder Deinstallation von Exchange Server **nicht möglich**



Exchange Server - Standardzertifikate

"**Federation**"-Zertifikat

- **Selbstsigniertes** TLS-Zertifikat mit **fünf Jahren** Laufzeit
- Benötigt für die **Verbundvertrauensstellung** zwischen den Exchange Servern und dem Microsoft Federation Gateway
- Meist erfolgt die Einrichtung der Verbundvertrauensstellung mit der ersten Ausführung des **Hybrid Configuration Wizards** (HCW)
- Erfordert eine **manuelle Erneuerung** vor Ablauf des Zertifikates



Exchange Server Zertifikate - Übersicht

Zertifikat	Verwendungszweck	Hinweise
Microsoft Exchange	Exchange interne SMTP-Kommunikation	Jeder Exchange Server hat ein eigenes Zertifikat, Laufzeit startet mit dem Tag der Installation
Microsoft Exchange Server Auth Certificate	Authentifizierung innerhalb der Exchange Organisation und externe Systeme	Zertifikat wird von Exchange auf alle Exchange Server der Organisation verteilt
WMSVC-SHA2	IIS Web Management Dienst	Jeder Exchange Server hat ein eigenes Zertifikat, Laufzeit startet mit dem Tag der Installation
Federation	Verbundvertrauensstellung mit dem Microsoft Federation Gateway	Zertifikat wird von Exchange auf alle Exchange Server der Organisation verteilt

HTTPS

Exchange Server – Interne HTTPS-Kommunikation

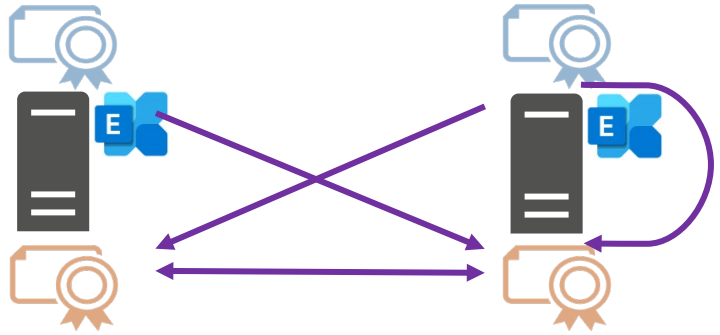
```
Machine: testms05.varunagroup.de
[PS] C:\>Get-ExchangeCertificate

Thumbprint                                Services   Subject
----------                                --------   -------
47074DB0AD96F2148E499FFD2B5CC0C3277ACDFE  ...WS..    CN=mail.varunagroup.de
B449C6803B7BC209CDD3B89F951F72DB69F4CD15  IP.WS..    CN=testms05
1DBCDEFF90DAFAF155E24171D1034E0CFCEE2DE7  ....SF.    CN=Federation
D1E0C733B968012296093FF5AB27FD6B3244450B  ....S..    C
```

https://go.granikos.eu/PSIISBindings

```
Machine: testms05.varunagroup.de
[PS] E:\SCRIPTS>.\Get-IisTlsBindings.ps1

Sites                  : Default Web Site
CertificateFriendlyName :
CertificateDnsNameList  : {mail.varunagroup.de, autodiscover.varunagroup.de, content.varunagroup.de}
CertificateNotAfter     : 8/15/2024 1:59:59 AM
CertificateIssuer       : CN=GeoTrust TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US

Sites                  : Exchange Back End
CertificateFriendlyName : Microsoft Exchange
CertificateDnsNameList  : {testms05, testms05.varunagroup.de}
CertificateNotAfter     : 4/17/2028 1:12:04 PM
CertificateIssuer       : CN=testms05
```

Default (Front End) – TCP 443
Drittanbieterzertifikat
oder aus Enterprise CA

Back End – TCP 444
Selbstsigniertes Zertifikat



`https://autodiscover.varunagroup.de`
`https://mail.varunagroup.de`
`https://content.varunagroup.de`

`https://testms05.varunagroup.de`

Internes Netzwerk

Exchange Server – Interne HTTPS-Kommunikation

- **Protokolltests** der Health-Postfächer
  - Erreichbarkeit HTTPS-Endpunkte
    - HTTP 200 OK Antwort
  - Auch zur Prüfung der Protokolle SMTP, POP4 und IMAP4

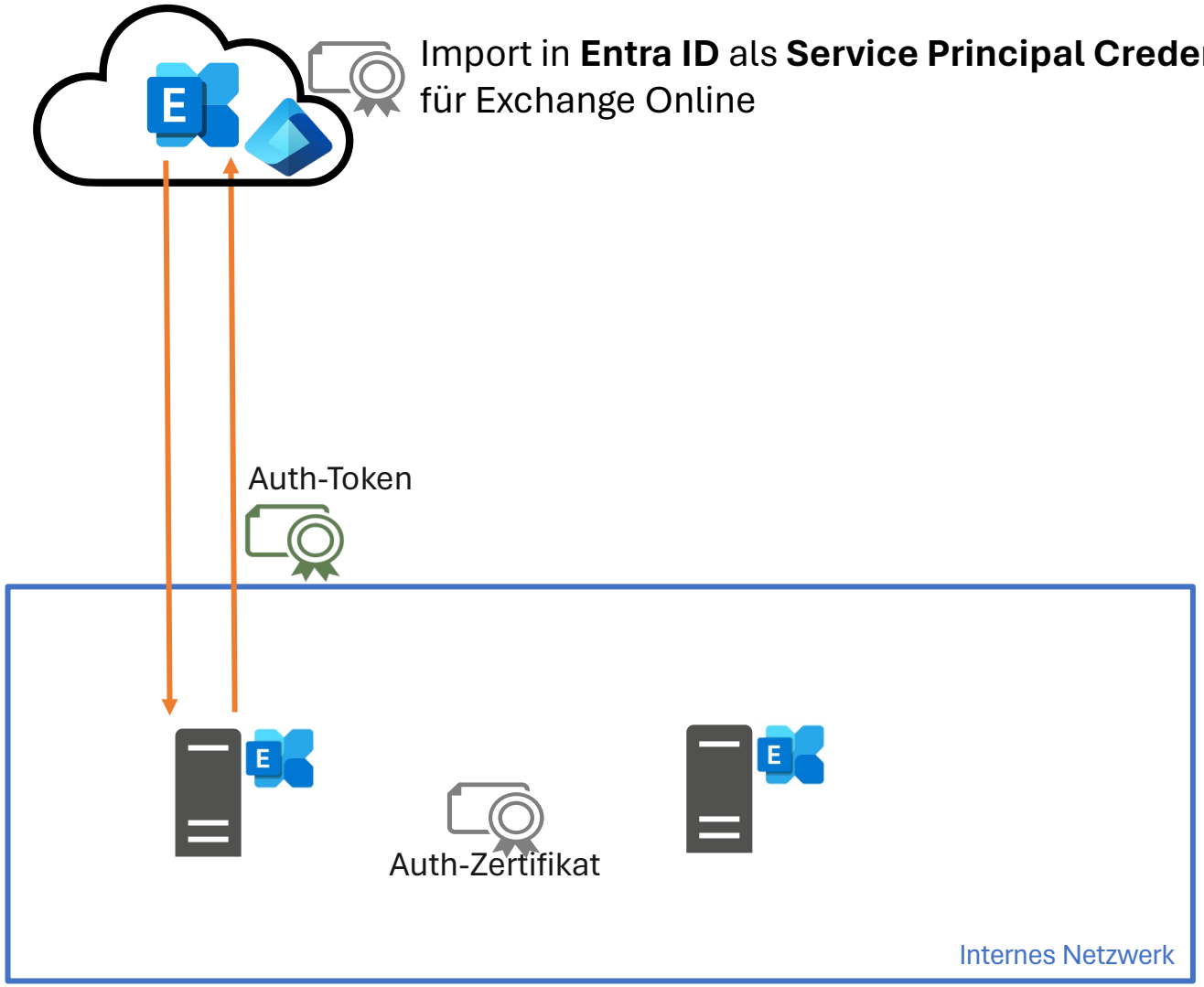
- Einziges Kriterium
  - Zertifikat ist im **aktiven Gültigkeitszeitraum**

→ Nicht Erreichbarkeit der getesteten Endpunkte oder HTTP-Fehler wirken sich direkt auf die **Managed Availability** aus

Exchange Server zu Exchange Online (Classic Hybrid)

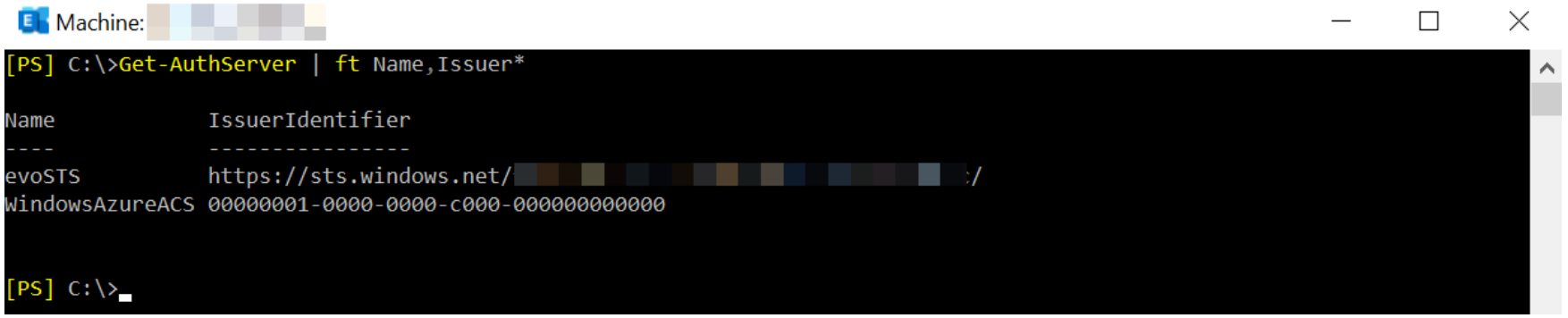
- Abfrage von Hybrid-Informationen von Empfängerobjekten in Exchange Online
  - Frei-/Gebucht-Zeiten
  - Mailtipps u.a.
- Authentifizierung über Exchange Auth-Zertifikat
  - Exchange Namensraum wird im Entra ID Dienstprinzipal hinterlegt
    - **https://mail.varunagroup.de**
    - **https://autodiscover.varunagroup.de**

```
Services   Subject
--------   -------
...WS..    CN=mail.varunagroup.de
IP.WS..    CN=testms05
.......    CN=WMSvc-SHA2-TESTMS05
....SF.    CN=Federation
....S..    CN=Microsoft Exchange Server Auth Certificate
```



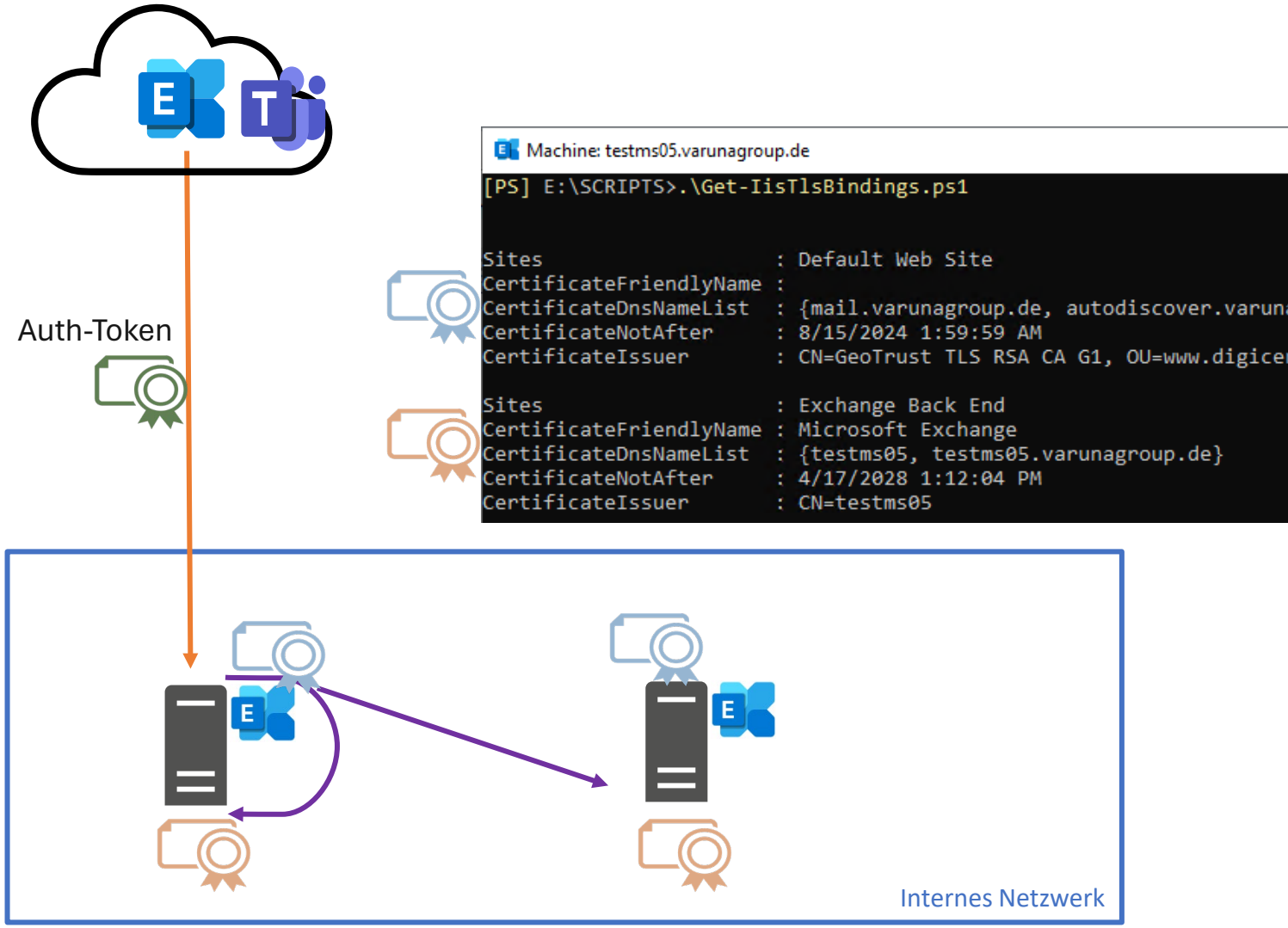
Exchange Server Auth-Server und Metadaten

- evoSTS
  - AuthMetadataUrl
    https://login.windows.net/HYBRIDDOMAIN/federationmetadata/2007-06/federationmetadata.xml
- WindowsAzureACS
  - AuthMetadataUrl
    https://accounts.accesscontrol.windows.net/HYBRIDDOMAIN/metadata/json/1
- URLs müssen für jeden Exchange Postfach-Server der Organisation erreichbar sein

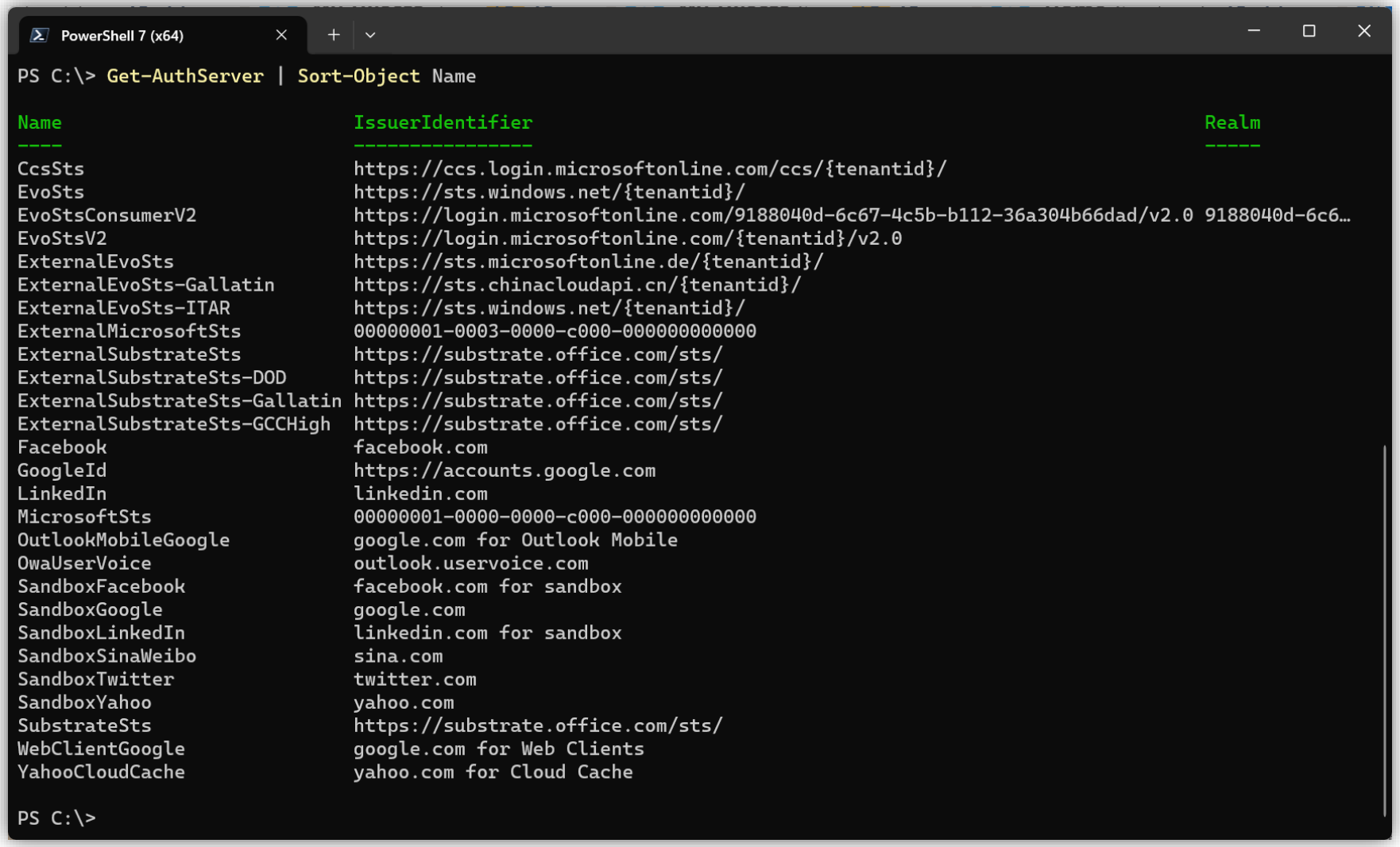


Exchange Online zu Exchange Server (Classic Hybrid)

- Abfrage von Hybrid-Informationen von Empfängerobjekten in lokaler Exchange Organisation
  - Frei-/Gebucht-Zeiten
  - Mailtipps u.a.
- Verschieben von Postfächern
  - Mailbox Replication Service (MRS) Proxy
- Exchange Server **vertraut Token**, die von **erlaubten Auth-Servern** ausgestellt sind
  - `Get-AuthServer`
- Microsoft Teams Backenddienste



Exchange Online Auth-Server

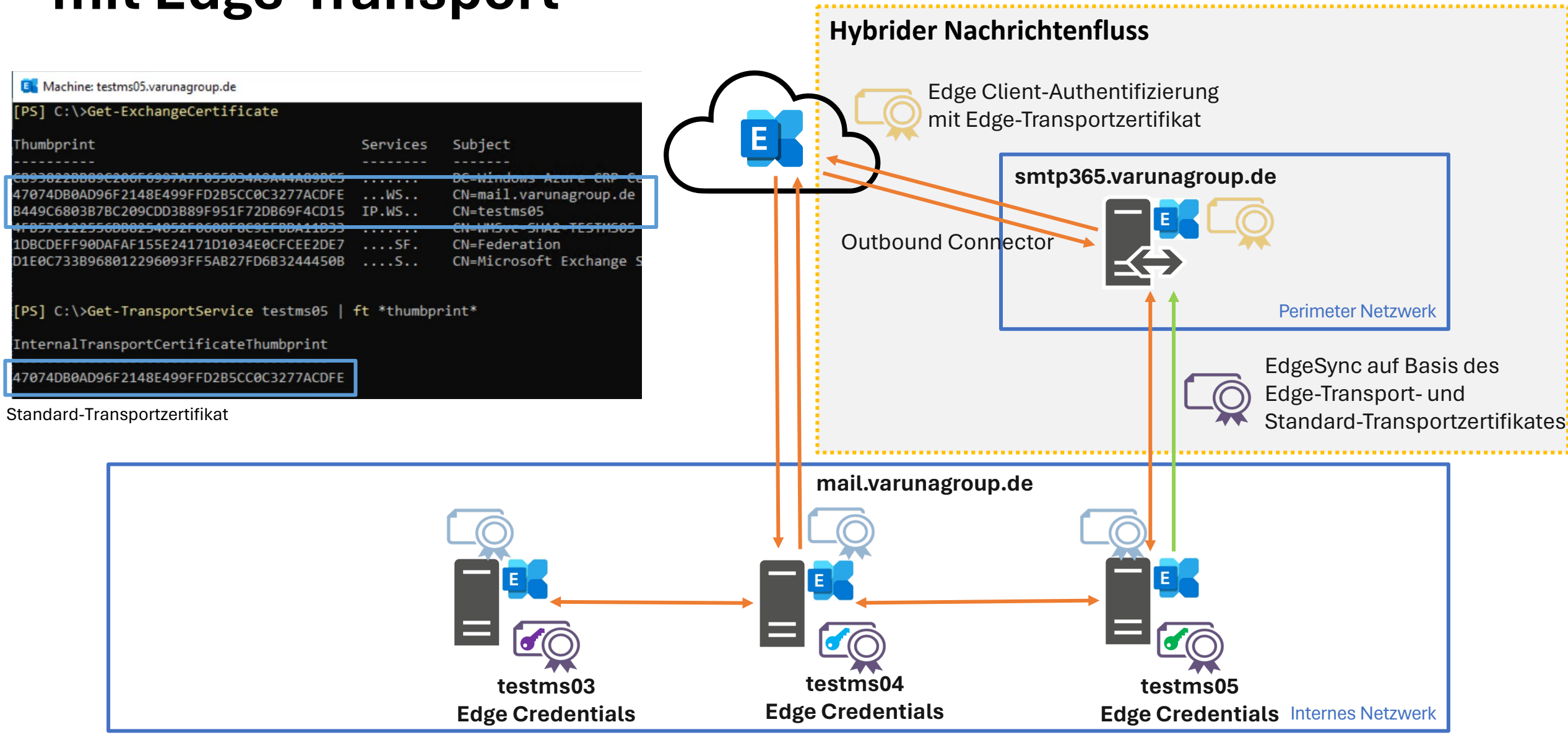


SMTP

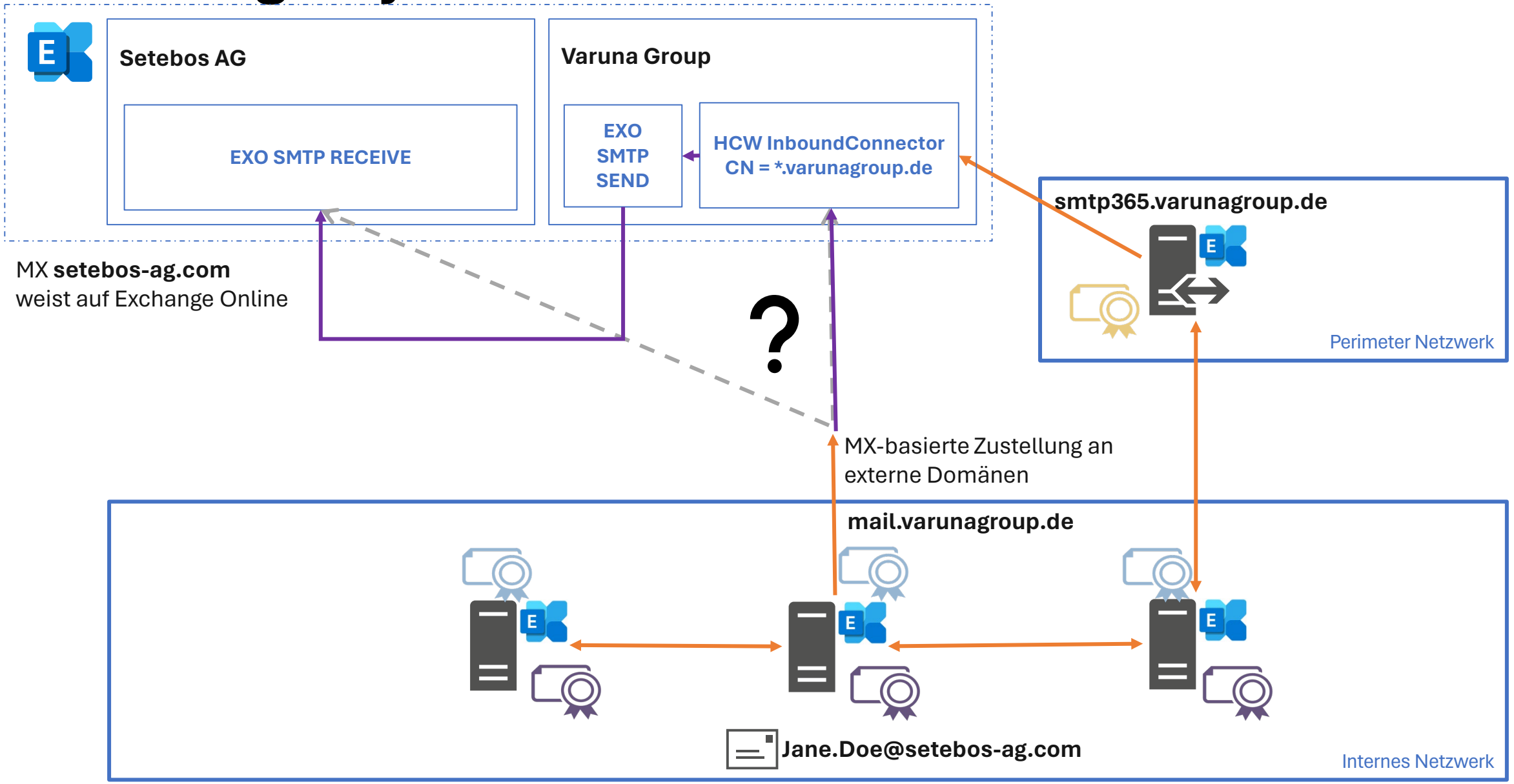
Exchange Hybrid – SMTP mit Edge-Transport

```
Machine: testms05.varunagroup.de
[PS] C:\>Get-ExchangeCertificate

Thumbprint                                Services   Subject
----------                                --------   -------
47074DB0AD96F2148E499FFD2B5CC0C3277ACDFE  ...WS..    CN=mail.varunagroup.de
B449C6803B7BC209CDD3B89F951F72DB69F4CD15  IP.WS..    CN=testms05
1DBCDEFF90DAFAF155E24171D1034E0CFCEE2DE7  ....SF.    CN=Federation
D1E0C733B968012296093FF5AB27FD6B3244450B  ....S..    CN=Microsoft Exchange S

[PS] C:\>Get-TransportService testms05 | ft *thumbprint*

InternalTransportCertificateThumbprint

47074DB0AD96F2148E499FFD2B5CC0C3277ACDFE
```

Standard-Transportzertifikat



Exchange Hybrid – SMTP



Exchange Hybrid – SMTP

Änderung des erwarteten TLS-Common Namens am **Inbound Connector**

Setebos AG

EXO SMTP RECEIVE

Varuna Group

EXO SMTP SEND

HCW InboundConnector
CN = ~~*.varunagroup.de~~
smtp365.varunagroup.de

MX **setebos-ag.com**
weist auf Exchange Online

smtp365.varunagroup.de

Perimeter Netzwerk

MX-basierte Zustellung an externe Domänen

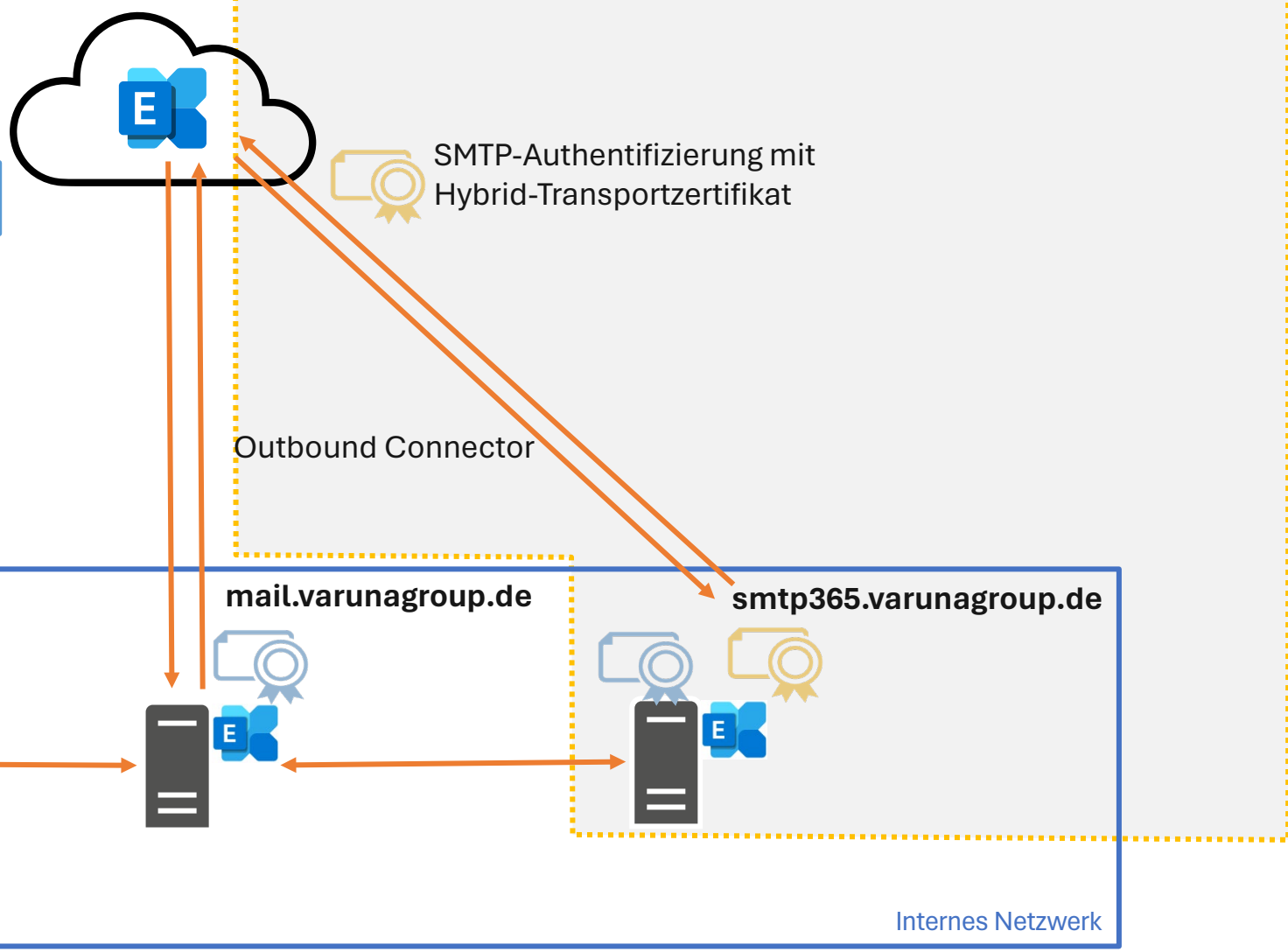
mail.varunagroup.de

Jane.Doe@setebos-ag.com

Internes Netzwerk

Exchange Hybrid – SMTP ohne Edge-Transport

```
Machine: testms05.varunagroup.de
[PS] C:\>Get-ExchangeCertificate

Thumbprint                                Services   Subject
----------                                --------   -------
47074DB0AD96F2148E499FFD2B5CC0C3277ACDFE  ...WS..    CN=mail.varunagroup.de
B449C6803B7BC209CDD3B89F951F72DB69F4CD15  IP.WS..    CN=testms05
1DBCDEFF90DAFAF155E24171D1034E0CFCEE2DE7  ....SF.    CN=Federation
D1E0C733B968012296093FF5AB27FD6B3244450B  ....S..    CN=Microsoft Exchange S

[PS] C:\>Get-TransportService testms05 | ft *thumbprint*

InternalTransportCertificateThumbprint
--------------------------------------
47074DB0AD96F2148E499FFD2B5CC0C3277ACDFE
```



Exchange Hybrid – SMTP

- **Dediziertes TLS-Zertifikat** für **hybriden Nachrichtenfluss** (auch ohne Edge-Transport-Server)
- Exchange Server **Standard-Transportzertifikat** ist Teil der **EdgeSync-Verschlüsselung**
  - **Alle** Exchange Server **einer AD-Site** sollten das gleiche Standard-Transportzertifikat nutzen
  - Prüfung des Standard-Transportzertifikates **vor** der Einrichtung des Edge-Abonnements
  - **Änderung** des Standard-Transportzertifikates **nach** der Einrichtung des Edge-Abonnements **bricht EdgeSync** für den betroffenen Exchange Server
- Prüfung und ggf. Anpassung des Zertifikatnamens im Exchange Online InboundConnector **nach jeder** Ausführung des Hybrid Configuration Wizards
  - *.varunagroup.de → smtp365.varunagroup.de
- Ein Exchange **Sendekonnektor** erfordern nur dann eine **TLS-Zertifikatbindung**, wenn eine **Client-Authentifizierung** am Zielserver erforderlich ist

TLS und Empfangskonnektoren – 1

- Fqdn
  - Bestandteil des Standard-SMTP-Banners, falls nicht angepasst
  - EHLO/HELO-Antwort des Konnektors
  - TLS-Authentifizierung
  - Teil des "Received"-Header einer E-Mail-Nachricht
  - Basis für die Zertifikatsuche im Zertifikatspeicher
  - Nie den "Default SERVERNAME"-Konnektor ändern
- TlsCertificateName
  - Fest referenziertes Zertifikat für die TLS-Verschlüsselung
  - Format: **<I>**X.500Issuer**<S>**X.500Subject
    Beispiel: ***<I>****CN=GeoTrust TLS RSA CA G1****<S>***cn=smtp.varunagroup.de*
- TlsDomainCapabilities
  - Aktivierung von Empfangskonnektorfunktionen für aus externe SMTP-Server nach TLS-Authentifizierung
  - Format: Domain:Funktion
    Beispiel: mail.protection.outlook.com:AcceptOorgProtocol

TLS und Empfangskonnektoren – 2

- DomainSecureEnabled
  - Das sendende System muss ein TLS-Zertifikat zur Authentifizierung präsentieren

Voraussetzungen

- **AuthMechanism** muss **Tls** und darf *ExternalAuthoritative* **nicht** enthalten
- Absenderdomäne für Mutual TLS-Authentifizierung
  - Muss Teil der **TLSReceiveDomainSecureList** der **TransportConfig** sein
  - Es muss ein korrespondierer **Sendekonnektor** exisitieren, in dem die Domain als **TlsDomain** konfiguriert ist
  - Muss Teil der **TLSSendDomainSecureList** der Set-TransportConfig sein

TLS und Sendekonnektoren – 1

- Fqdn
  - EHLO/HELO-Antwort des Konnektors
  - TLS-Authentifizierung
  - Teil des "Received"-Header einer E-Mail-Nachricht
  - Standardwert: `$null` → Verwendung des Server-FQDN
- TlsAuthLevel
  - *EncryptionOnly* → Verschlüsselung des Transportkanals
  - *CertificateValidation* → Verschlüsselung des Transportkanals, inkl. Prüfung des Zertifikates der Gegenseite (Zertifikatkette und Zertifikatrückzugsliste)
  - *DomainValidation* → Verschlüsselung des Transportkanals, inkl. Prüfung des Zertifikates der Gegenseite (Zertifikatkette und Zertifikatrückzugsliste), Zertifikat der Gegenseite muss den im Parameter *TlsDomain* konfigurierten FQDN enthalten
    - Ist TlsDomain nicht konfiguriert, vergleicht der Sendekonnektor die Zertifikatnamen gegen die Empfängerdomäne der E-Mail-Nachricht

TLS und Sendekonnektoren – 2

- TlsCertificateName
  - Fest referenziertes Zertifikat für die TLS-Verschlüsselung zur TLS-Clientauthentifizierung
  - Format: **<I>**X.500Issuer**<S>**X.500Subject
    Beispiel: ***<I>****CN=GeoTrust TLS RSA CA G1****<S>****CN=smtpo.varunagroup.de***
  - Der Hybrid Configuration Wizard konfiguriert das im HCW ausgewählte Zertifikat für den hybriden Outbound-Sendekonnektor
- TlsDomain
  - Domainname, um den FQDN des TLS-Zertifikates des Zielsystems zu überprüfen
  - Dieser Parameter muss für **TlsAuthLevel** *DomainValidation* konfiguriert sein

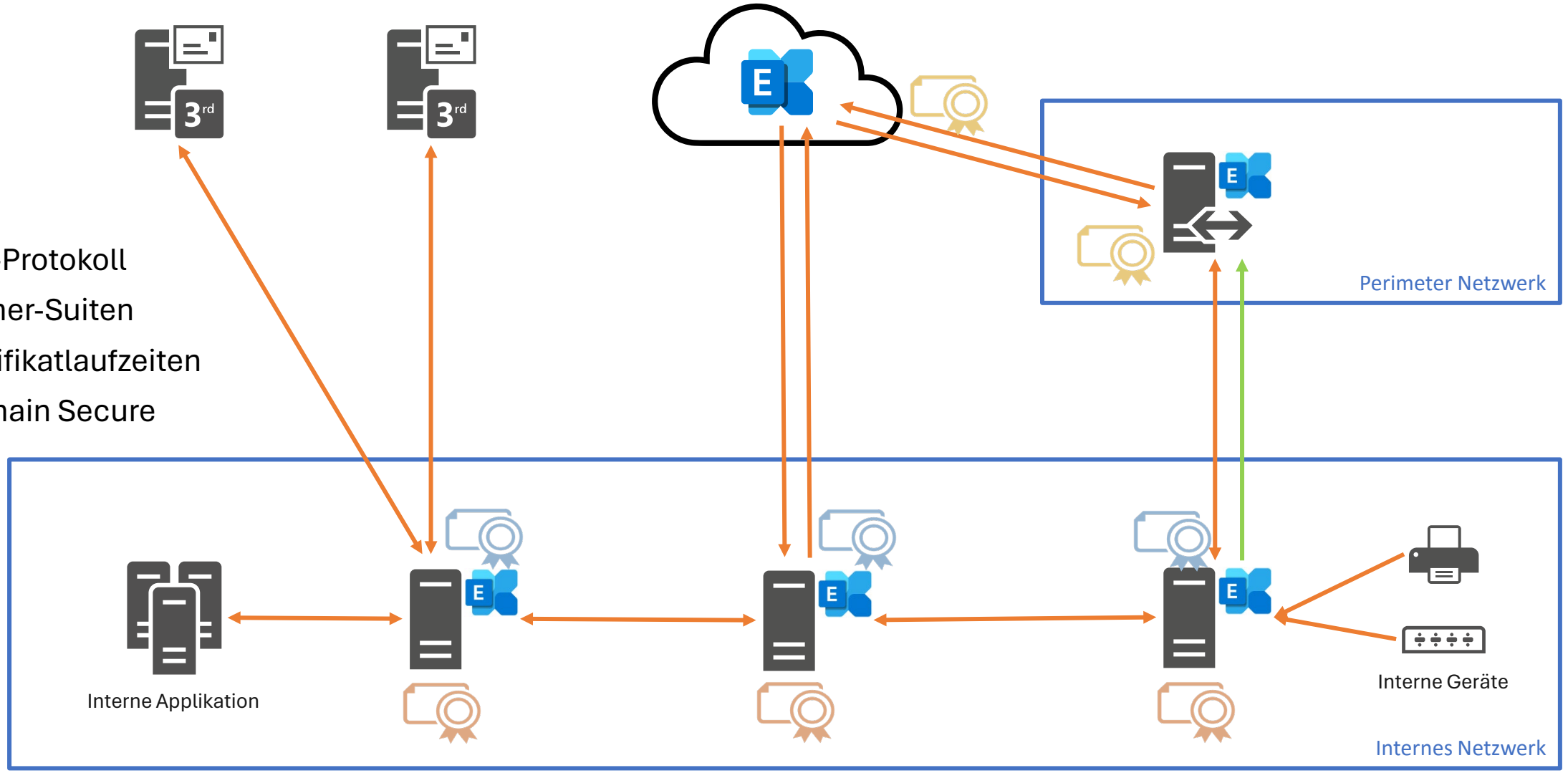
Und wie spielen die Clients mit?

Exchange Server, Clients und Applikationen

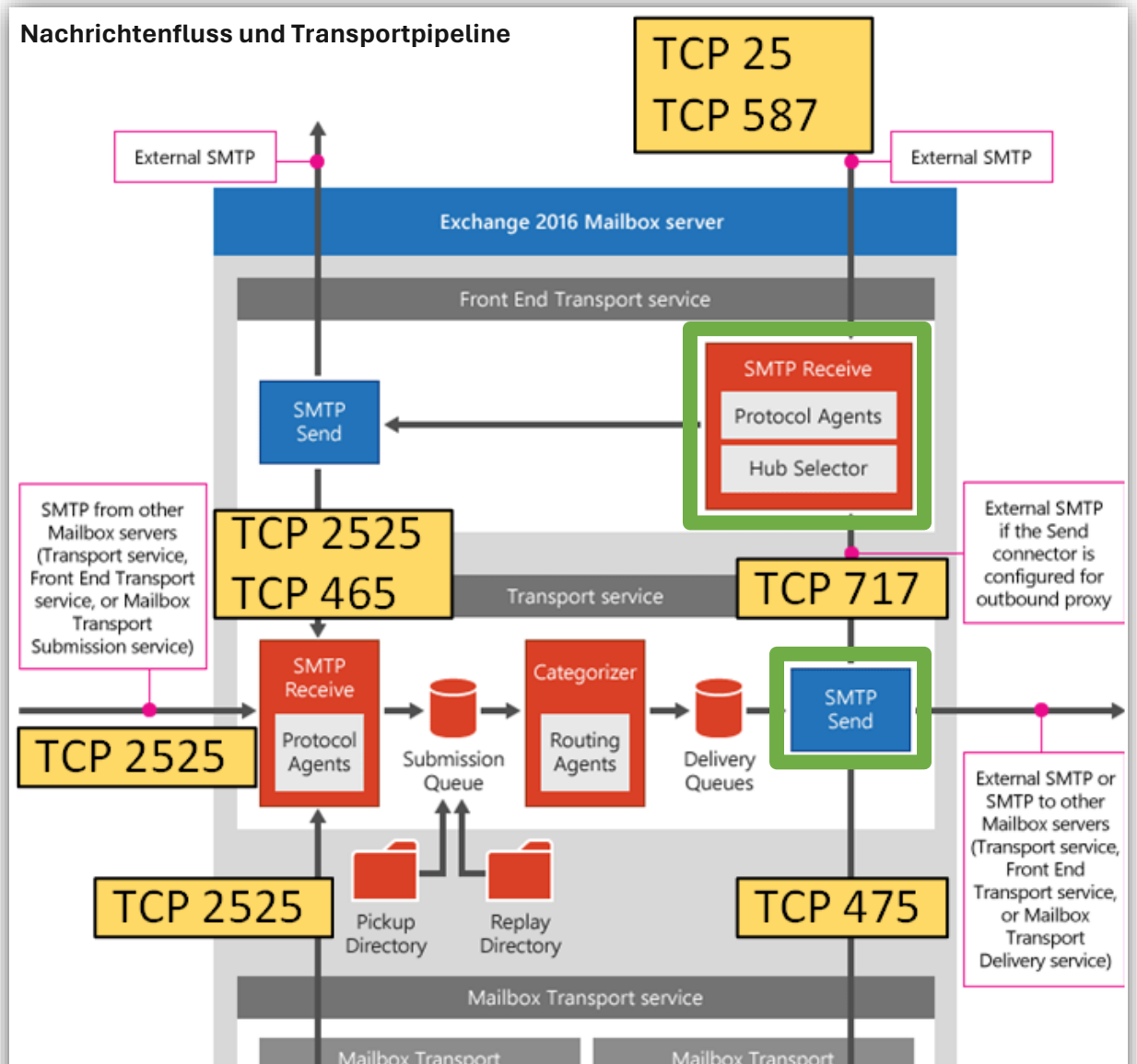
Abhängigkeiten und Fallstricke

Exchange Server und TLS-Zertifikate

- TLS-Protokoll
- Cipher-Suiten
- Zertifikatlaufzeiten
- Domain Secure

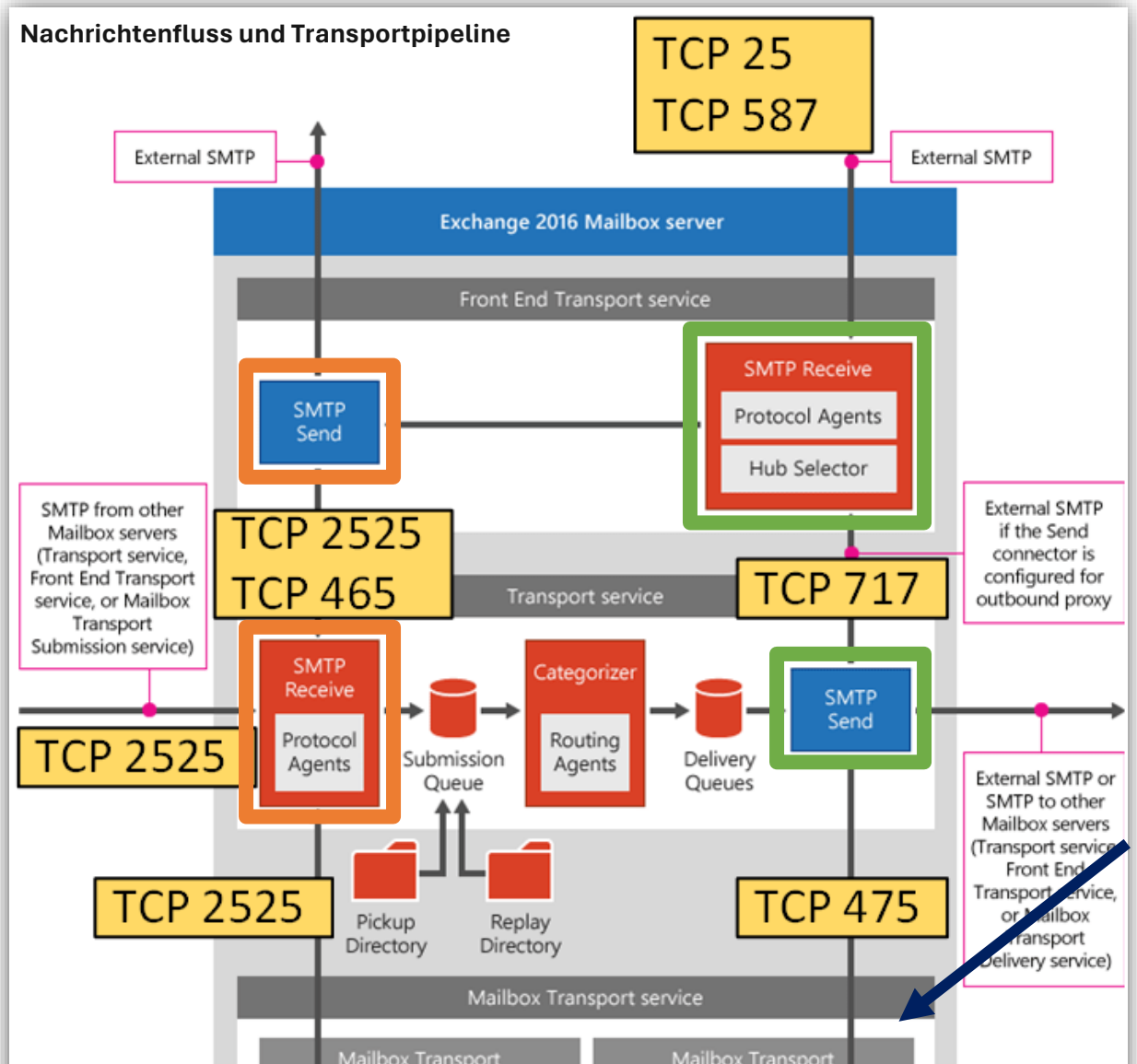


Exchange Transport und TLS-Zertifikate – 1



- Konnektoren mit konfiguriertem FQDN
  - Common Name (CN) oder SAN enthält den Konnektor FQDN
  - Zertifikat ist für SMTP aktiviert
  - Zertifikat ist gültig
- Konnektor mit explizit konfiguriertem Zertifikat, z.B. Hybrid-Konnektor
  - Zertifikat mit eindeutig passendem CN und Aussteller
  - Zertifikat ist für SMTP aktiviert
  - Zertifikat ist gültig
- Sind mehrere zeitlich gültige Zertifikate mit gleichem Namen im Zertifikatspeicher
  - Exchange Server nutzt das jüngste (längste Restlaufzeit) Zertifikat
  - Exchange Server präferiert ein PKI- vor einem selbstsignierten Zertifikat

Exchange Transport und TLS-Zertifikate – 2



- SMTP-Send via Front End Transport
  - Besondere SMTP-Routing-Anforderungen
- Hub-Transport-Empfangskonnektoren
  - Standard-Konnektor je Server dient der Exchange internen Kommunikation
    → zurückhaltende Anpassung
  - Individuelle Konnektoren gehören ins Front End
    → Header Firewall und Hub Selector
- SMTP-Receive im Mailbox Transport Delivery Service
  - Interner Konnektor für die lokale Zustellung in Postfachdatenbanken

Best Practices

- So wenig TLS-Zertifikate als möglich, so viele wie nötig
- Selbstsignierte Zertifikate von Exchange Server nicht löschen, Standardlaufzeit beachten und rechtzeitig erneuern
- Interne Exchange Kommunikation erfordert TLS-Zertifikate mit dem Computernamen
  - NETBIOS und FQDN
  - Nutzung des automatisch ausgestellten Computerzertifikats birgt Risiko des Verlustes der Zertifikatbindung bei automatischer Erneuerung durch das Betriebssystem
- Dediziertes TLS-Zertifikate für hybride SMTP-Kommunikation, insbesondere bei Nutzung von Edge-Transport-Servern
- Prüfung und ggf. Anpassung der InboundConnector-Einstellung nach Erstellung bzw. Aktualisierung durch den Hybrid Configuraton Wizard
- Rechtzeitige Erneuerung ablaufender Zertifikate, insbesondere bei Zertifikaten mit erweiterter (EV) Prüfung der Domaineigentümerschaft
- Sicherung individueller Zertifikate mit privatem Schlüssel für eine Notfallwiederherstellung (Dial-Tone-Recovery)

Exchange Server ist eine sehr tolerante Server-Applikation

Abweichungen von den Best Practices sind normal

Bücher anklicken – mehr erfahren

Microsoft® Most Valuable Professional

Thomas Stensitzki

Experte

Granikos GmbH & Co. KG
MVP | M365

https://linktr.ee/stensitzki

Thomas' Tech Talk wird produziert mit Camtasia

Ressourcen

- Demystifying the TLS Handshake: What it is and how it works
- Certreq – Parameterübersicht
- Best Practices für Exchange Server Zertifikate
- Microsoft Federation Gateway
- Wie konfigurieren Sie die OAuth-Authentifizierung zwischen Ihren lokalen Exchange- und den Exchange-Online-Organisationen?
- Receive Connector – DomainSecureEnabled
- Selection of Inbound STARTTLS certificate