SMEXOP
Smart Exchange Online Protection

Christian Schindler

ETC

Agenda

- Überblick/Architektur
- E-Mail Authentication
- Anti Malware
- Anti Spam
- Perimeter Protection
- Anti Phishing
- Safe Attachements/Links
- Tools
- Reporting
- Automated Response

ETC

Modul 01: Überblick/Architektur

ETC

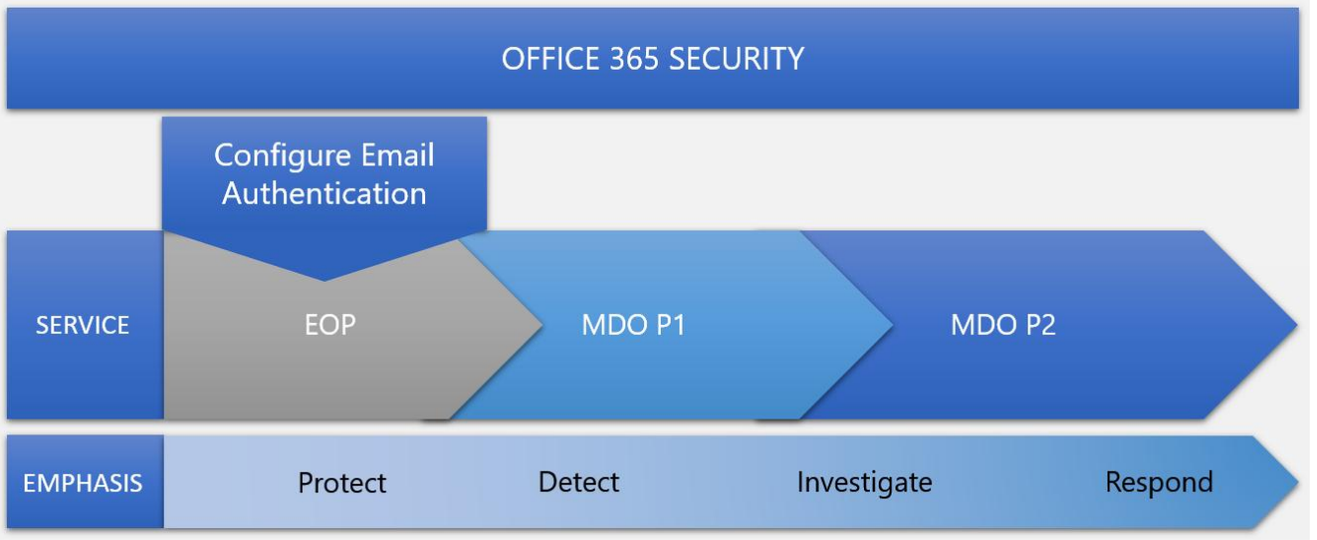
Exchange Online Protection (EOP) Portfolio

- E-Mail-Hygiene in der Microsoft 365 Cloud
- Lösung für mehrere Szenarien
  - Nur Exchange Online Postfächer
  - Hybrid Umgebungen
  - Nur Exchange On Premises Postfächer
- Funktionen abhängig von der Lizenz
- Unterscheidung zwischen „EOP“ und „Microsoft Defender for Office 365“

ETC

EOP vs. Microsoft Defender for Office 365 (MDO)

- EOP = Basisschutz
  - Connection Filtering, Allow/Block Lists, etc.
  - Anti Malware
  - Anti Phishing
  - Anti Spam
- MDO 365 = Erweiterter Schutz
  - Anti Phishing extended (Plan 1)
  - Safe Links (Plan 1)
  - Safe Attachments (Plan 1)
  - Threat Explorer (Plan 2)
  - Automated simulation training (Plan 2)
  - Automated investigation & response (Plan 2)
  - Etc.



https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

ETC

Lizenzierung

Exchange Online Protection

Als Bestandteil von O365/M365 Lizenzen

Standalone Lizenzierung (für On Premises Schutz)

Microsoft Defender for Office 365

Zusätzlich zu Exchange Online Protection

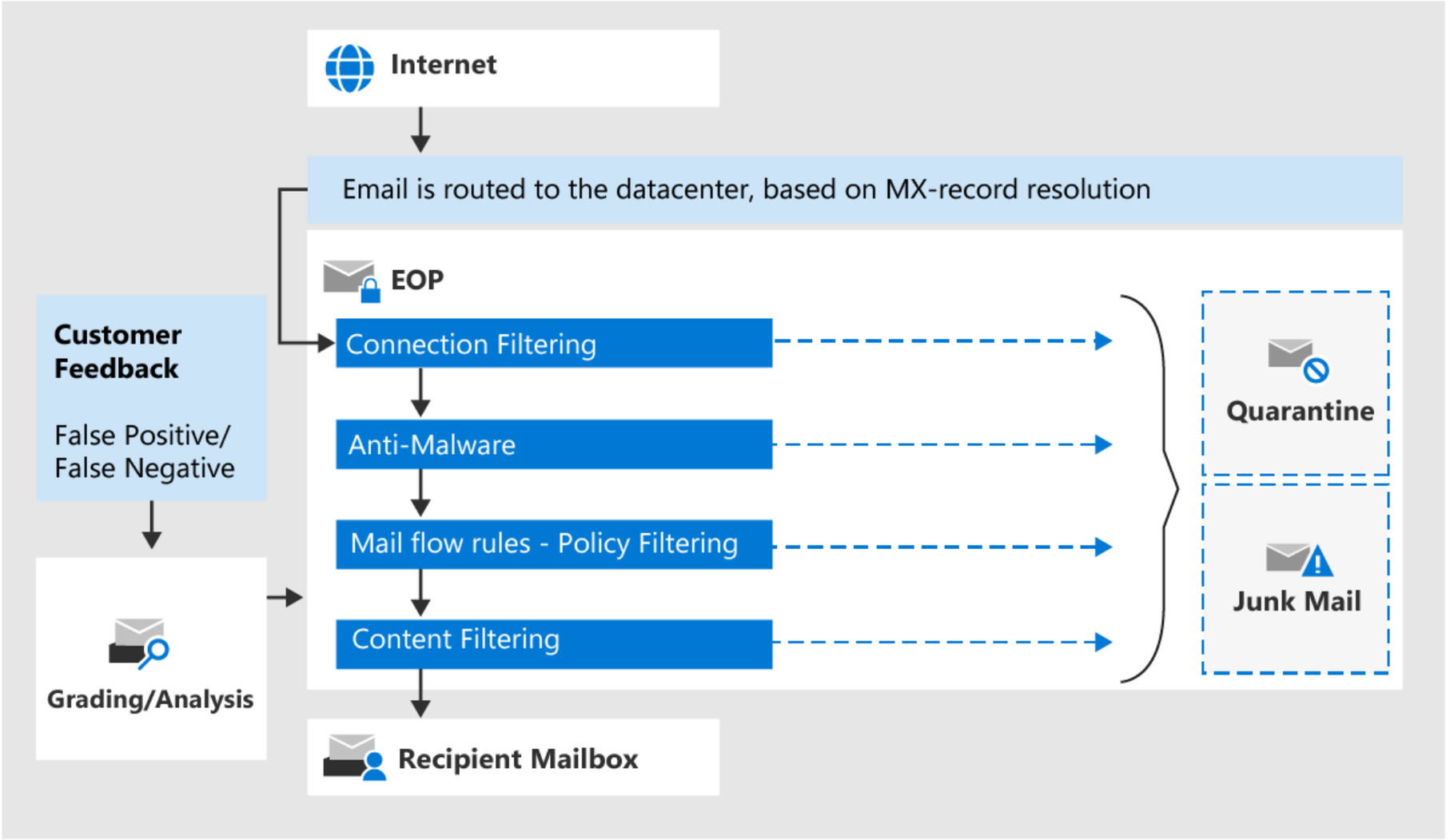
Lizenziert pro Benutzer/Monat

Plan 1 oder Plan 2

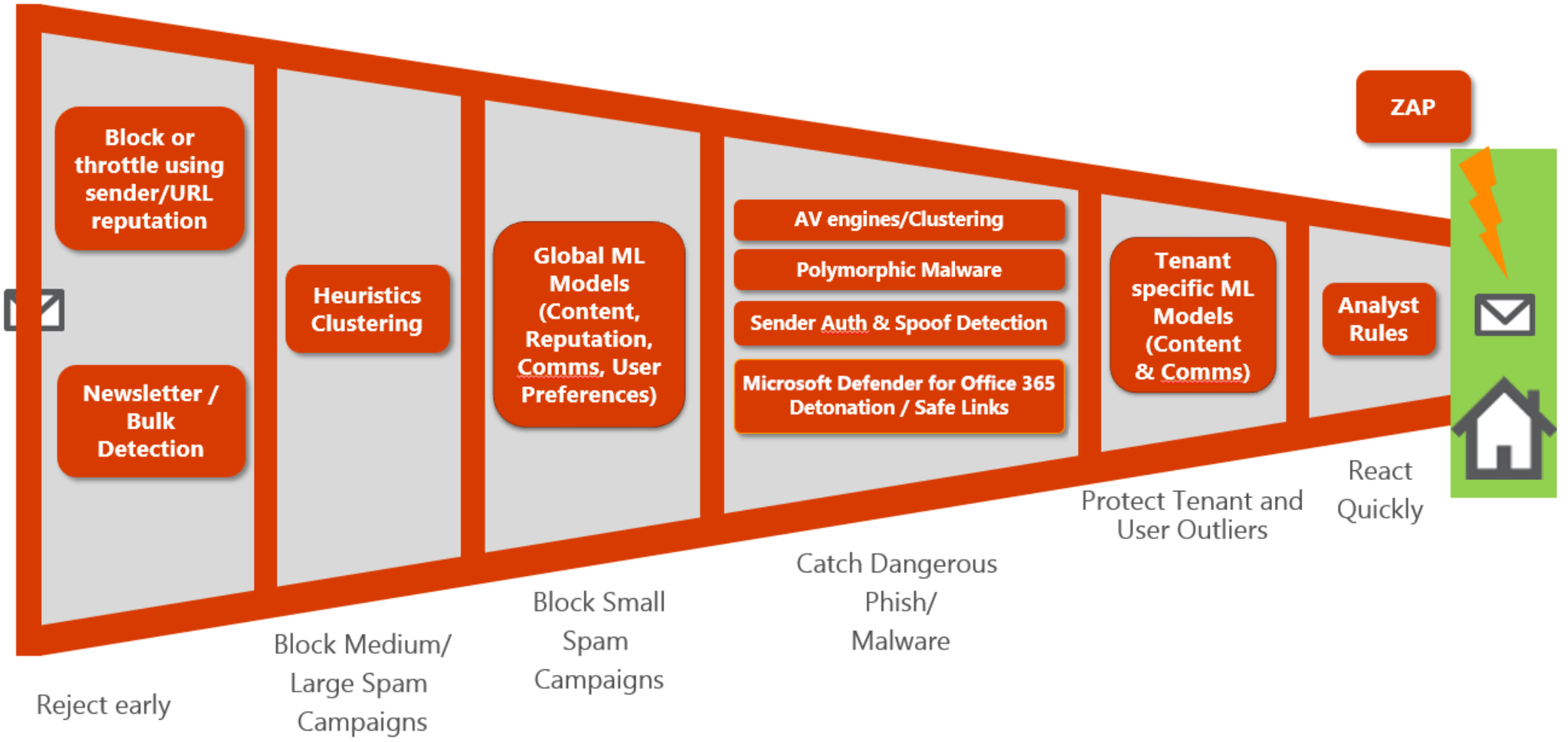
Office 365/Microsoft 365 E5 enthält Plan 2

ETC

Email Processing Pipeline



Protection Pipeline



Connectoren

- Erlauben das Empfangs- und Sendeverhalten von EOP zu beeinflussen
- Standardmäßig keine erforderlich
- Für Spezialszenarien
  - Hybrid Umgebungen
  - Anbinden von Partnerfirmen
  - Geräte die über EOP senden
  - Etc.
- Ähnlich Receive- und Send Connectoren in Exchange On Premises

ETC

Modul 2:
Perimeter Protection

ETC

Was bedeutet „Perimeter Protection“?

- Maßnahmen die beim Verbindungsaufbau getätigt werden
- Sondert bereits einen Großteil der unerwünschten Nachrichten aus
- Technologien die hier zum Einsatz kommen:
  - Directory Based Edge Blocking
  - Connection Filter Allow/Block List
  - Microsoft Safe IP List
  - Reputation Block

ETC

Eine Nachricht wird empfangen…

- …und EOP analysiert, woher die Nachricht kommt:
  - Von OnPremises Absendern (Hybrid Umgebung) via TLS
  - Von einer Partnerfirma via TLS
  - Von einem „sicheren“ Absender (wird vom Empfänger in Outlook als solcher definiert und an EOP gesynced…)
  - Von einem (anonymen) Absender aus dem Internet

- EOP fügt der Nachricht Header hinzu, die Auskunft über die Herkunft der Nachricht geben

ETC

Directory Based Edge Blocking (DBEB)

- EOP ermittelt ob der Empfänger der im „RCPT TO:“ übergeben wird, existiert
  - Empfänger bekannt: Nachricht wird weiter verarbeitet
  - Empfänger unbekannt: Nachricht wird mit „*550 5.4.1 Recipient address rejected: Access denied*“ zurückgewiesen
- Nur für Empfänger in autoritativen Domains!

Error Details

Reported error:	*550 5.4.1 Recipient address rejected: Access denied. AS(201806281) [DB5EUR01FT043.eop-EUR01.prod.protection.outlook.com]*
DSN generated by:	DU0PR02MB8037.eurprd02.prod.outlook.com

https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/use-directory-based-edge-blocking

ETC

Connection Filter/Microsoft IP Safe List

Connection Filter

- **Allow** oder **Block** von IP-Adressen
- Manuell gepflegte Liste

Microsoft IP Safe List

- Microsoft abonniert Dritthersteller Listen von „vertrauenswürdigen“ IP-Adresse
- Soll helfen, dass vertrauenswürdige Absender nicht versehentlich als SPAM markiert werden…

ETC

Reputation Block

- Microsoft führt eine Reputationsliste über „böse“ Sender-IPs
- Geblockte Nachrichten werden automatisch gelöscht bzw. nicht angenommen!
- Ist die IP-Adresse des Absenders nicht gelistet, wird der Nachricht ein Header mit dieser Information hinzugefügt
- Entfernung aus der Reputation List: https://sender.office.com

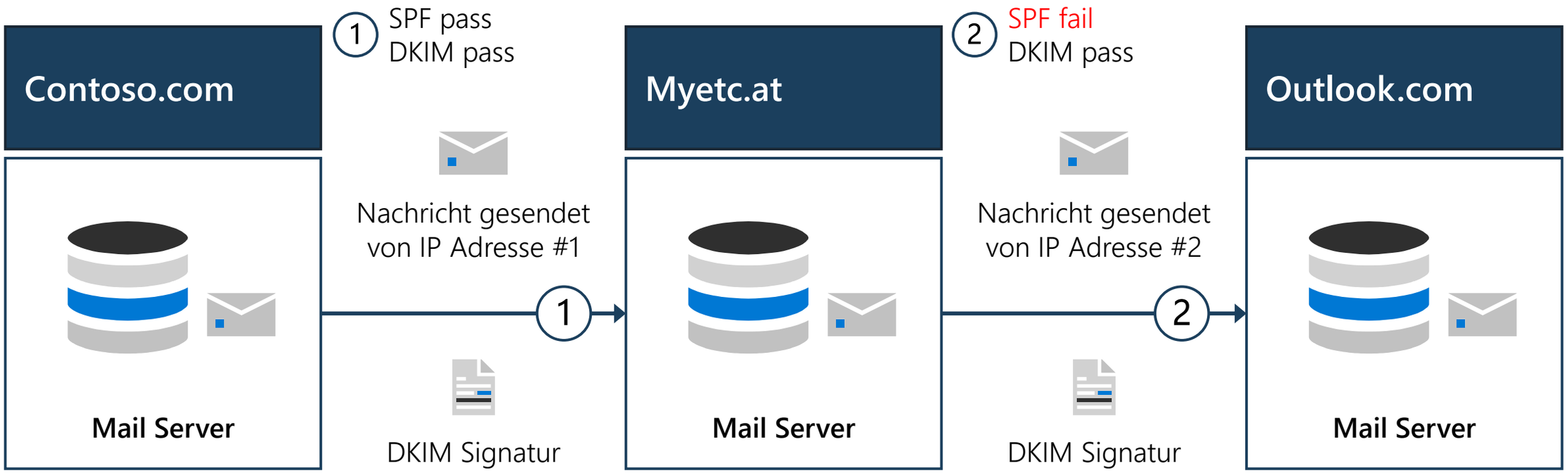
***550** 5.7.606 Access denied, banned sending IP [194.166.246.26]. To request removal from this list please visit https://sender.office.com/ and follow the directions. For more information please go to http://go.microsoft.com/fwlink/?LinkID=526655 AS(1430) [DB5EUR01FT107.eop-EUR01.prod.protection.outlook.com]*

ETC

E-Mail Authentication

- Maßnahmen, um Spoofing zu verhindern bzw. vermindern
- Verifizierung des Absenders, um die Legitimität einer Nachricht zu bestimmen
  - Kommt die Nachricht dieser Absenderdomäne von einem zu erwartenden System?
- Benutzt SPF, DKIM und DMARC zur Überprüfung
- Ergebnisse der Überprüfung werden in E-Mail-Header vermerkt
  - Nachgelagerte Mechanismen verwenden diese Information bei der weiteren Verarbeitung

Schutz vor Spoofing



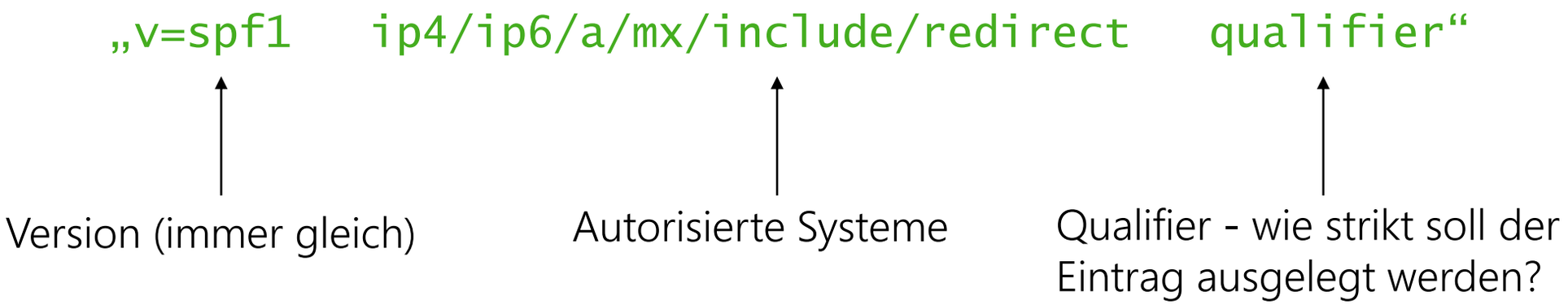
Spoofing ist das Senden von Nachrichten im Namen eines anderen Absenders. Angreifer nutzen dies, um die Identität eines Anderen vorzutäuschen.

SPF, DKIM, DMARC, MTA-STS und DANE sollen helfen, diese Attacken abzuschwächen

ETC

Sender Policy Framework (SPF) – RFC 7208

- Zur Validierung ausgehender E-Mails
- Empfängersystem prüft anhand eines DNS Records, ob die Nachricht von einem autorisierten Absendersystem kommt
- DNS TXT Record wird in der Zone des Domänenbesitzers erzeugt
  - Enthält die Systeme, die im Namen der Domäne Emails versenden dürfen
- SPF (TXT) Record Aufbau:



Verschachtelung der SPF Records

- SPF Records können verschachtelt werden
  - Um die Länge des Records zu verringern
- Auslagerung der SPF Records in eine eigene Zone (z.B.: spf.protection.outlook.com)
- Erlaubt es, Sender aus anderen Domänen zu autorisieren (Newsletter Versand, etc.)
- Verschachtelung bedingt zusätzliche DNS-Abfragen
  - Deshalb maximal 10 Verschachtelungen erlaubt (PermError bei Überschreitung)
- Folgende Keywords bedingen zusätzliche DNS-Abfragen:
  - A
  - MX
  - PTR
  - EXISTS
  - INCLUDE
  - REDIRECT

SPF Record Qualifier

- Gibt an, wie strikt das Empfängersystem den Record auslegen soll

Qualifier	Name	Bedeutung
+	Pass	Die Direktive definiert keine autorisierten Sender; dies ist der Standard, d. h. ist kein Qualifier angegeben, so wird + angenommen
-	Fail	Die Direktive definiert ausschließlich autorisierte Sender
~	Softfail	Die Direktive definiert autorisierte Sender, der Empfänger soll einen Fehler aber großzügig behandeln
?	Neutral	Die Direktive definiert Sender, über deren Legitimität nichts ausgesagt werden soll; der Sender muss so behandelt werden, als wenn kein Qualifier angegeben wäre

Qualifier den EOP erfordert

ETC

SPF Record – Validierungsergebnisse

Ergebnis	Bedeutung
None	SPF Record nicht vorhanden
Neutral	Der SPF Record gibt keine autorisierten Sender bekannt. Entspricht Qualifier „?“. Muss wie „None“ behandelt werden!
Pass	Die IP-Adresse wird im SPF Record als autorisierter Absender geführt
Fail	Die IP-Adresse ist nicht autorisiert Nachrichten im Namen der Domäne zu versenden.
Softfail	Die IP-Adresse wurde nicht autorisiert, der Qualifier „~“ gibt aber bekannt, dass Fehler großzügig behandelt werden sollen.
TempError	Bei der Abfrage des SPF Records ist es zu einem Fehler gekommen (DNS, Netzwerk, etc.)

ETC

SPF Makros

- Ermöglichen dynamische und skalierbarere SPF-Einträge
- Verweise auf bestimmte Mechanismen im SPF-Record
  - Empfangender MTA extrahiert Mechanismen aus den Verweisen
- Makros beginnen mit einem „%“ Zeichen und verwenden geschwungene Klammern:

Name	Bedeutung
%{s}	<sender>
%{l}	local-part of <sender>
%{o}	domain of <sender>
%{d}	<domain>
%{i}	<ip>
%{p}	the validated domain name of <ip> (do not use)
%{v}	the string "in-addr" if <ip> is ipv4, or "ip6" if <ip> is ipv6
%{h}	HELO/EHLO domain

ETC

SPF Record Beispiele

- Microsoft.com:

v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.msft.net include:spf-a.hotmail.com include:_spf1-meo.microsoft.com –all

- Gmail.com:

v=spf1 redirect=_spf.google.com

v=spf1 include:_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com ~all

- Post.at (verwendet Makros):

v=spf1 include:%{ir}.%{v}.%{d}.spf.has.pphosted.com -all

ETC

Domain Keys Identified Mail (DKIM)

- Fügt Nachrichten einen Signatur-Header hinzu
  - Nachricht ist *nicht vollständig* signiert!
- Public Key zur Prüfung der Signatur wird im Sender-DNS als TXT Record publiziert
- Empfänger überprüft Signatur mittels Public Key aus dem DNS TXT Record
- Stellt sicher, dass Nachrichten, die über Systeme weitergeleitet werden, die nicht im SPF vermerkt sind, nicht als SPAM gekennzeichnet werden.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=aETC.onmicrosoft.com;
 s=selector2-aETC-onmicrosoft-com;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck;
 bh=PKZI0SBgFFjzrzcvpt2hh/FvoEx8ymyMaPgWbOluork=;
 b=JVwgV0/Pwoef+qoUhEKQDeNdJI5wb+EOrpVjtvGCDScrPI3fkYHAADYTujrs6O4+Vsg3bd17B5HXgjKiSiFw
```

DKIM-Selektoren

- Ermöglichen multiple Sendersysteme mit unterschiedlichen Signaturen (z.B. Newsletter Versand mit 3rd Party, etc.)
- Werden im DKIM-Header angeführt
- CNAME Records im DNS
- Für regelmäßigen Schlüsseltausch werden meist zwei Selektoren verwendet
- Werden in der Subdomain „_domainkey“ erzeugt

- Beispiele:

Microsoft 365:

CNAME: Selector1._domainkey.myetc.at -> selector1-myetc-at._domainkey.ntxbocgat.x-yz.dkim.mail.microsoft

Dynamische Subdomain

Mailchimp:

CNAME: k2._domainkey.myetc.at -> dkim2.mcsv.net

DKIM Keys

- Public Key wird in DNS TXT Record abgelegt
- Wird meistens vom Provider gemacht
  - Ausnahme: OnPremises Appliances, die selbst DKIM anbieten

```
> set q=cname
>
> selector1._domainkey.smexop-2543t.myetc.at
Server:  UnKnown
Address:  10.10.2.30

Non-authoritative answer:
selector1._domainkey.smexop-2543t.myetc.at      canonical name = selector1-smexop2543t-myetc-at01e._domainkey.wwlx767512.y-v1.dkim.mail.microsoft
>
> set q=txt
>
> selector1-smexop2543t-myetc-at01e._domainkey.wwlx767512.y-v1.dkim.mail.microsoft
Server:  UnKnown
Address:  10.10.2.30

Non-authoritative answer:
selector1-smexop2543t-myetc-at01e._domainkey.wwlx767512.y-v1.dkim.mail.microsoft        text =

        "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA08zCQQG16Te72W8RyFMhLE3wSGUsQ6LOVzKF7hM3hlpZTHwtQOetJ666qpO8J60S7ChRvZ4OIi18U4nkvWws
IStYp419/+WRJn3YZu77ZJgrN4D8Q1LHkJUiQulVvrxS+okA4/KMjqA/FwBEb6z1zjkuPeSQAYx4efyShG+K7YQ7Y0Q67evvlAMjmDk1ZIRE1"
        "NJFv9k5yB7RvQtdgwCWpSpaUBYQ8EQDnho3Y1SUkqrr5l0XDEmLFgaqnnsfnmTYf8jJ+XFTjR4bdmzSYWbdo5+Z/BLwkNgZb+86Q23a/v1SdpOxoprAC5NNWqhTYI7URK7kqNQsIPQIHnFkgug
hgQIDAQAB;"
```

DKIM @ Microsoft 365

- Inbound DKIM automatisch aktiviert
- Outbound DKIM muss pro Domäne aktiviert werden (Defender for Office 365 Portal)
  - Schlüsselpaar generieren
  - Erzeugen der DNS-Einträge
  - Aktivieren von DKIM

- Exchange Online PowerShell:

```
Get/New/Set/Rotate-DkimSigningConfig
```

ETC

DMARC

- **Domain-based Message Authentication, Reporting, and Conformance**
- Baut auf SPF und DKIM auf
  - Statement wie Empfänger Spammails behandeln sollen
  - Konformität obliegt dem Empfänger…
- Prüft zusätzlich ob „mail from:“ (P1) und „From:“ (P2) gleich sind, oder die DKIM-Domain („d“ Feld) mit dem „From:“ (P2) übereinstimmt
- Eigener DNS TXT Record
  - Gilt auch für Sub-Domains!
- Server mit DMARC Agent können (…) Reports and den Domain-Owner versenden
  - E-Mail-Adresse wird im DNS Record publiziert
  - Möglichkeit von „aggregate“ und „forensic“ Reports

ETC

Anatomie eines DMARC DNS Records

- v=DMARC1; p=reject; pct=100; rua=mailto:itex-rua@microsoft.com; ruf=mailto:itex-ruf@microsoft.com; fo=1

Feld	Bedeutung
v=DMARC1	Version. Derzeit immer 1
p	Policy. Gültige Werte: none, quarantine, reject
pct	Prozensatz der Nachrichten die entsprechend „p“ gefiltert werden
rua	E-Mail-Addresse an die der „aggregate“ Report gesendet wird
ruf	E-Mail-Addresse an die der „forensic“ Report gesendet wird
adkim	Wie streng die Prüfung bezüglich DKIM sind: strict/relaxed
aspf	Wie streng die Prüfung bezüglich SPF sind: strict/relaxed
fo	fo=0 (Default) Fehlerbericht wenn SPF & DKIM auf "failed" fo=1 Fehlerbericht wenn SPF oder DKIM auf "failed" gehen fo=d Melde fehlerhafte Signatur unabhängig vom SPF/DKIM Ergebnis fo=s Melde SPF=Fail-Fehler, unabhängig von DKIM Mehrere Werte kombinierbar mit "colon„. Normalerweise aber nur „1“

ETC

DMARC Reports

- Empfänger „kann“ (…) DMARC Reports senden
- Reports im XML-Format
- Provider bieten entsprechende Dienstleistung zur effizienten Auswertung an (MX Toolbox, etc.)

- **Achtung!**
- Wenn die Report E-Mail-Adresse in einer anderen Domäne liegt muss in der Empfängerdomain ein eigener DNS-Record zur Bestätigung erzeugt werden:

```
myetc.at._report._dmarc.mxtoolbox.dmarc-report.com TXT "v=DMARC1"
```

Domäne des DMARC Records

Domäne des Providers der die Reports empfängt

ETC

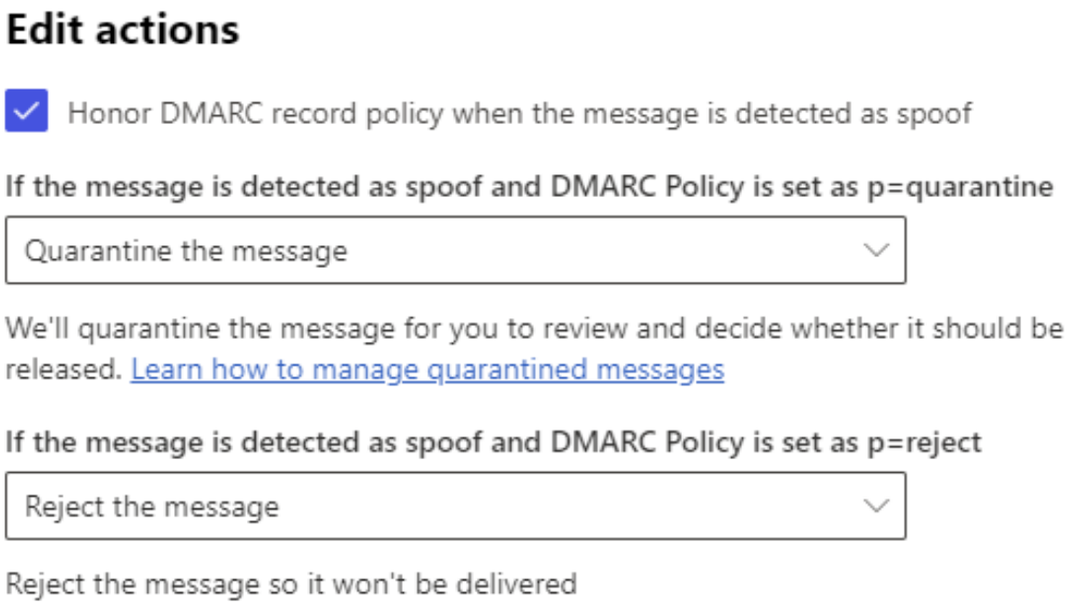
DMARC Report Beispiel


```
▼<feedback xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <version>1.0</version>
  ▼<report_metadata>
    <org_name>Enterprise Outlook</org_name>
    <email>dmarcreport@microsoft.com</email>
    <report_id>0594b73080134794b7bb8c546c56445f</report_id>
    ▼<date_range>
      <begin>1694822400</begin>
      <end>1694908800</end>
    </date_range>
  </report_metadata>
  ▼<policy_published>
    <domain>ntx.at</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>quarantine</p>
    <sp>quarantine</sp>
    <pct>100</pct>
    <fo>0</fo>
  </policy_published>
  ▼<record>
    ▼<row>
      <source_ip>40.107.7.81</source_ip>
      <count>1</count>
      ▼<policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    ▼<identifiers>
      <envelope_to>etc.at</envelope_to>
      <envelope_from>ntx.at</envelope_from>
      <header_from>ntx.at</header_from>
    </identifiers>
    ▼<auth_results>
      ▼<dkim>
        <domain>ntx.at</domain>
        <selector>selector2</selector>
        <result>pass</result>
      </dkim>
      ▼<spf>
        <domain>ntx.at</domain>
        <scope>mfrom</scope>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
```

DMARC @ Microsoft 365

- Ist standardmäßig aktiv
- DNS-Record muss manuell erzeugt werden
- Seit 10.8.23 befolgt EOP den DMARC DNS Record in den Anti-Phising policies!

https://admin.cloud.microsoft/#/MessageCenter/:/messages/MC640228



ETC

Composite Authentication

- Für Nachrichten bei denen SPF/DKIM/DMARC nicht oder nur unvollständig konfiguriert ist
- Benutzt den „From:“ Header zur Evaluierung und vermerkt Ergebnis im „compauth“ Header

```
Authentication-Results:
   compauth=<fail | pass | softpass | none> reason=<yyy>
```

- From Header und SPF Record match

```
Authentication-Results: spf=pass (sender IP is 10.2.3.4)
  smtp.mailfrom=fabrikam.com; contoso.com; dkim=none
  (message not signed) header.d=none; contoso.com; dmarc=bestguesspass
  action=none header.from=fabrikam.com; compauth=pass reason=109
From: chris@fabrikam.com
To: michelle@contoso.com
```

- From Header aber kein SPF/DKIM/DMARC

```
Authentication-Results: spf=none (sender IP is 192.168.1.8)
  smtp.mailfrom=maliciousdomain.com; contoso.com; dkim=pass
  (signature was verified) header.d=maliciousdomain.com;
  contoso.com; dmarc=none action=none header.from=contoso.com;
  compauth=fail reason=001
From: chris@contoso.com
To: michelle@fabrikam.com
```

Falsche DKIM-Domain!

ETC

ARC - Authenticated Received Chain

- Für durch Anbieter weitergeleitete Nachrichten (Mailing Lists, etc.)
- Jeder Anbieter (kann) Nachrichten einen ARC-Signatur-Header hinzufügen
- Definiert 3 neue Header:

  `ARC-Authentication-Results (AAR)`

  `ARC-Message-Signature (AMS)`

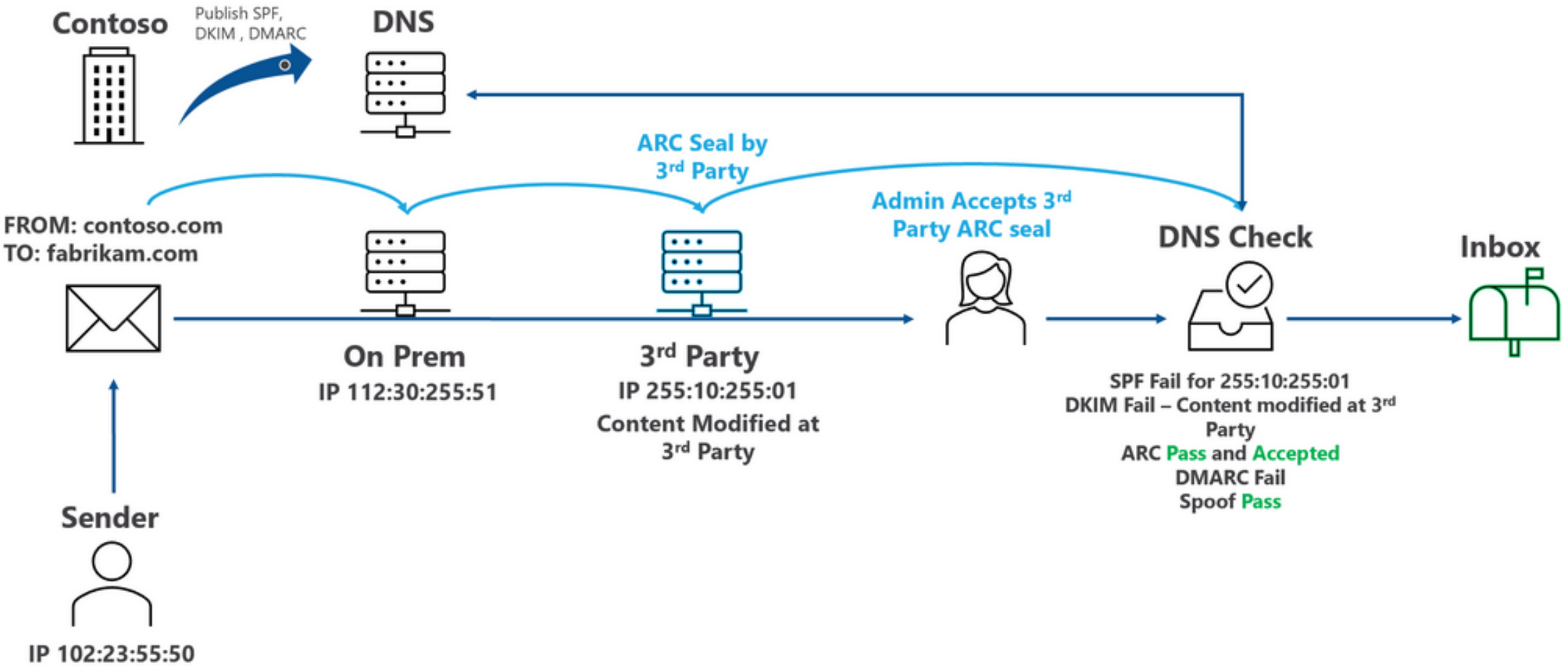
  `ARC-Seal (AS)`

- Header sind miteinander verkettet

```
ARC-Seal: i=2; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass;
 b=Ys4mi/TdEMW7HJo+4dTE62hwzBxBsJ8sMJIgNcVAXUAnjlggjkyyLavBdEcWIPVDV2klhUJAuawfY9s+3fVXy8MC4mNaWCZniLeUSr5kD8OBhyV/qWC+zo0vUqjWU5HuU3IB97JdgrS8ME/dd6BJRkqwfbK6OswoBIJFSfxeGk18DK7g0u/c
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=microsoft.com;
 s=arcselector9901;
 h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-AntiSpam-MessageData-ChunkCount:X-MS-Exchange-AntiSpam-MessageData-0:X-MS-Exchange-AntiSpam-MessageData-1;
 bh=PKZI0SBgFFjzrzcvpt2hh/FvoEx8ymyMaPgWbOluork=;
 b=L24gbtV5NXA55f4UsqrSUI1VFFm2xWDhK/ngeX1dBN2rcl5JfZjrybTVMqwHwI9N8goJKZUjgGH5CQEG1VYyPo0zjgjwCwQeBUEC6zj9rKYyqNg1klsNNBBdlwpgbmn6t0shhFQY4/N+q4+bqBy4tRTH6sfFZVaxtKT1MZz6wbr3n67VoA+M
ARC-Authentication-Results: i=2; mx.microsoft.com 1; spf=pass (sender ip is
 40.107.13.59) smtp.rcpttodomain=ntx.at smtp.mailfrom=etc.at; dmarc=pass
 (p=none sp=none pct=100) action=none header.from=etc.at; dkim=pass (signature
 was verified) header.d=aetc.onmicrosoft.com; arc=pass (0 oda=1 ltdi=1
 spf=[1,1,smtp.mailfrom=etc.at] dkim=[1,1,header.d=etc.at]
 dmarc=[1,1,header.from=etc.at])
```

ETC

ARC in action



MTA-STS (Strict transport security)

- Kombiniert DNS und HTTPS, um STARTTLS Zertifikate zu verifizieren
- DNS TXT-Record für Versionierung/Reporting
- Policy Datei enthält Info über MX und Zertifikat und maximale Cache-Dauer
- Datei muss folgendermaßen konfiguriert werden:
  - Name des Servers: mta-sts.domain.com
  - Virtuelles Verzeichnis: **/.well-known**
  - Dateiname: **mta-sts.txt**
  - Server muss über *offizielles SSL-Zertifikat* verfügen

https://mta-sts.myetc.at/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
mx: *.mail.protection.outlook.com
max_age: 604800
```

https://learn.microsoft.com/en-us/purview/enhancing-mail-flow-with-mta-sts

ETC

DNS Records für MTA-STS

- TXT-Record für Versionierung:

_mta-sts.myetc.at "v=STSv1; id=20211201000000Z;„

Datum/Uhrzeit der letzten Änderung

- TXT-Record für Reporting

_smtp._tls.myetc.at "v=TLSRPTv1;rua=mailto:smtp.reporting@myetc.at"

E-Mail-Adresse für Aggregate Report
(ähnlich DMARC)

MTA-STS Fehler bei der Validierung

Reason: [{LED=450 4.4.317 Cannot connect to remote server [Message=451 4.4.8 MX hosts of 'smexop2543.myetc.at' failed MTA-STS validation.]
[LastAttemptedServerName=smexop2543.myetc.at]
[AM1PEPF0002EAE7.eurprd04.prod.outlook.com 2025-01-28T12:32:26.828Z
08DD3E481401440C]};{MSG=451 4.4.8 MX hosts of 'smexop2543.myetc.at' failed .
OutboundProxyTargetHostName: smexop2543.myetc.at

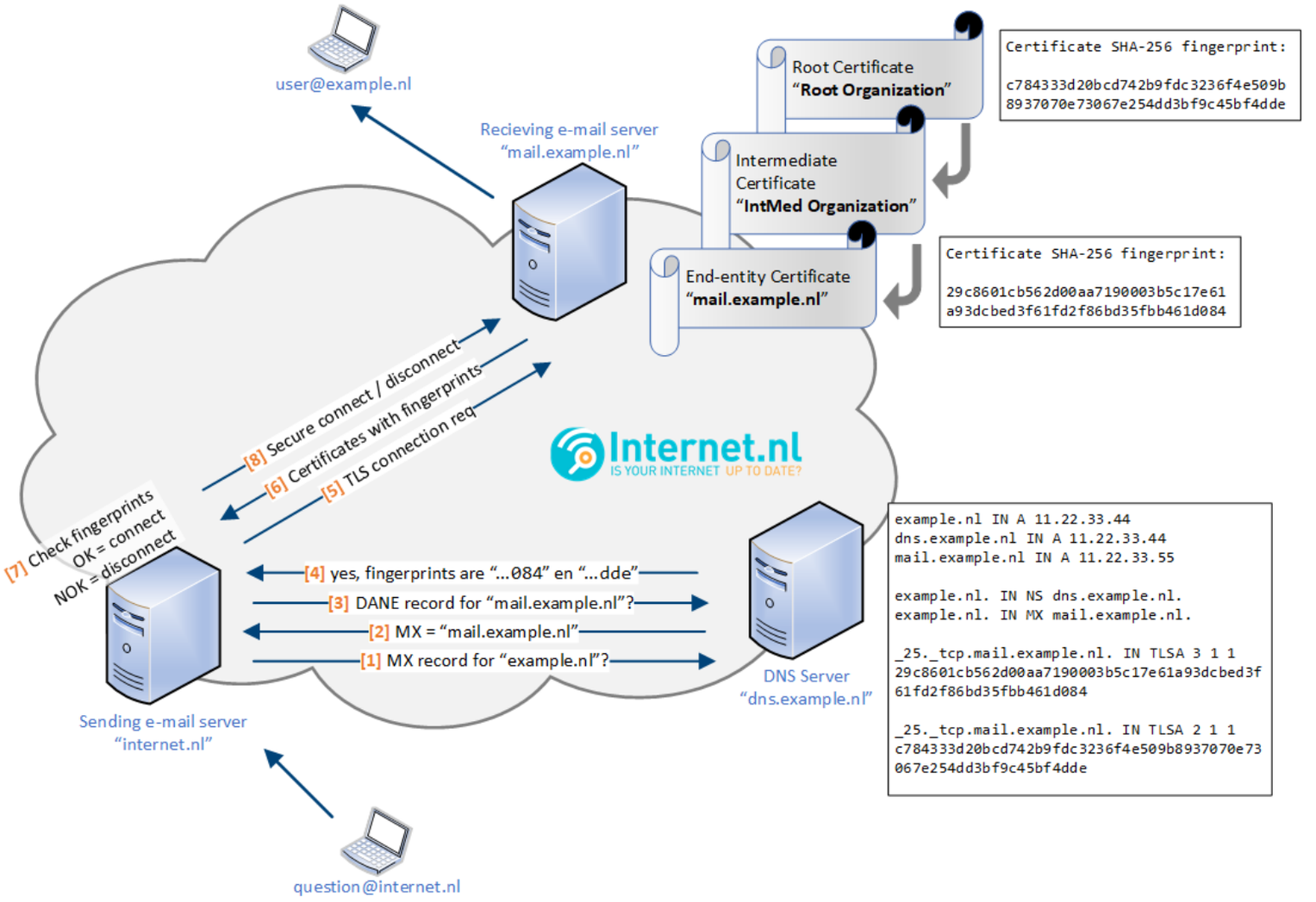
DANE - DNS-Based Authentication of Named Entities

- Erlaubt die Publizierung von TLS Public Keys im DNS
  - Geeignet für sämtliche TLS-basierenden Protokolle
  - Derzeit nur SMTP-Implementierungen
- Schutz vor Spoofing, DNS Cache Poisoning, DNS-Hijacking
- Eigener DNS-Record: TLSA
  - Angabe des Protocols (TCP-Port) und Zertifikates
- Erfordert DNSSEC zur Absicherung
- Status in Exchange Online: General Availability

https://learn.microsoft.com/en-us/purview/how-smtp-dane-works

ETC

DANE in action



TLSA Ressource Records

- Wird benutzt, um das X.509 Zertifikat oder den Public Key im DNS zu veröffentlichen
- Angabe des Dienstes und Protokolls (ähnlich SRV)

Type	Domain Name	TTL	Record
TLSA	_25._tcp.mx.contoso.com	3600	3 1 1 abc123…xyz789

- Record enthält 4 Datenfelder
  - Certificate Usage
  - Selector
  - Matching Type
  - Certificate Data
- Erfordert DNSSEC

ETC

TLSA @ Microsoft 365

Name	TTL	TLSA	CertUsage	Selector	MatchingType	CertificateData
smtpdane.mx.microsoft.	900	TLSA	3	1	1	7B8F7594E008F86E325ACE172709B7D2230820421DC1DD0AB5AFF54165A3EDEB
smtpdane.mx.microsoft.	900	TLSA	2	0	1	5F88694615E4C61686E106B84C3338C6720C535F60D36F61282ED15E1977DD44
smtpdane.mx.microsoft.	900	TLSA	3	1	1	3FBBF85495707A04F565B79D6CFDEA056C873C9D637CCA3DBEDEF859D8DACC88
smtpdane.mx.microsoft.	900	TLSA	3	1	1	7324C400A1578206F382CECA68F9BE9398A05952A039160C47B4985985D6A050
smtpdane.mx.microsoft.	900	TLSA	3	1	1	EA9D0BF13F63DA402ADC8E4B88B6EDF9968EBACBA927AE7ECECEC746B6BB1FEC

https://www.nslookup.io/tlsa-lookup/

ETC

TLSA Usages

Wert	Abkürzung	Beschreibung
0[1]	PKIX-TA	*CA constraint* Das veröffentlichte Zertifikat ist das CA-Zertifikat. Das Server Zertifikat muss von dieser CA ausgestellt sein
1[1]	PKIX-EE	*Service certificate constraint* Das veröffentlichte Zertifikat muss mit dem Serverzertifikat übereinstimmten und von einer vertrauenswürdigen CA stammen
2	DANE-TA	*Trust anchor assertion* Das veröffentlichte Zertifikat entspricht einem der Zertifikate aus der CA-Kette. Das vom Server präsentierte Zertifikat muss bis zu diesem Zertifikat validierbar sein.
3	DANE-EE	*Domain issued certificate* Das veröffentlichte Zertifikat entspricht dem im TLS-Handshake verwendeten Zertifikat des Servers

[1]Nicht von EXO verwendet

ETC

TLSA Selector & Matching Type

Selector

Wert	Abkürzung	Beschreibung
0	Cert	Das gesamte Zertifikat soll zur Prüfung verwendet werden
1	SPKI (Subject Public Key Info)	Nur der öffentliche Schlüssel und dessen Algorithmus wird zur Prüfung verwendet

Matching Type

Wert	Abkürzung	Beschreibung
0	Full	Die Daten enthalten das gesamte Zertifikat oder den SPKI
1	SHA-256	Die Daten enthalten einen SHA-256 Hash des Zertifikats oder SPKI
2	SHA-512	Die Daten enthalten einen SHA-512 Hash des Zertifikats oder SPKI

ETC

Inbound-DANE bei EXO – neue MX Records

- Neue MX-Domain bei Microsoft (ersetzt *.mail.protection.outlook.com)

***.mx.microsoft**

- MX Records werden in zufälliger Subdomain erzeugt
- SMTP Protocol Records verweisen auf TLSA von Microsoft (CNAME)

```
> set q=cname
> _25._tcp.myetc-at.n-v1.mx.microsoft
Server:  dns.quad9.net
Address:  2620:fe::fe

Non-authoritative answer:
_25._tcp.myetc-at.n-v1.mx.microsoft     canonical name = smtpdane.mx.microsoft
```

ETC

Implementieren von Inbound DANE (1)

- 2 Schritte, um DANE zu aktivieren

    1. DNSSEC für Accepted Domain aktivieren
    2. DANE für Accepted Domain aktivieren

- Im Moment nur über Exchange Online Management PowerShell

Aktivieren von DNSSEC und neuem MX Record

- TTL des vorhandenen MX Records auf 300 Sekunden reduzieren
- Aktivieren für eine E-Mail-Domäne

Enable-DnssecForVerifiedDomain -DomainName <DomainName>

```
DnssecMxValue                Result
-------------                ------
myetc-at.n-v1.mx.microsoft Success
```

- MX Record (*.mx.microsoft) mit Priorität 100 erzeugen
- Test von DNSSEC und neuem MX
  - https://testconnectivity.microsoft.com/tests/O365DaneValidation/input (Nur DNSSEC testen)
  - https://testconnectivity.microsoft.com/tests/O365InboundSmtp/input
- Priorität der MX Records tauschen
  - *.mx.microsoft = 0
  - *.mail.protection.outlook.com = 100
- Test der Nachrichtenzustellung

ETC

Aktivieren von DANE

- Aktivieren für eine E-Mail-Domäne

```
Enable-SmtpDaneInbound -DomainName <DomainName>
```

- Test
  - https://testconnectivity.microsoft.com/tests/O365DaneValidation/input

- Abfrage des Protocol Records mittels *nslookup*

```
Set q=cname
_25._tcp.myetc-at.n-v1.mx.microsoft.com
```

ETC

DNSSEC/DANE PowerShell Befehle

DNSSEC

- Enable-DnssecForVerifiedDomain
- Get-DnssecForVerifiedDomain
- Disable-DnssecForVerifiedDomain

DANE

- Enable-SmtpDaneInbound
- Get-SmtpDaneInbound
- Disable-SmtpDaneInbound

ETC

SMTP DANE-Flussdiagramm