

E-Mail-Sicherheit bei der Nachrichten- zustellung

EXUSG 2023 Q3
02.11.2023



About me

Andres Bohren



Cloud Engineer / Architect bei isolutions seit 2020

Seit 25 Jahren in der IT - Schwerpunkt in Messaging / Communication / Security

(Windows Server / Active Directory / MS SQL / Exchange / Lync / Skype4B / M365 / Azure / PowerShell)

Hobbies: Reisen / Tauchen / Bike / Tanzen



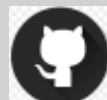
<https://blog.icewolf.ch>



<https://twitter.com/andresbohren> / @andresbohren



<https://www.linkedin.com/in/andres-bohren-4ba45293/>



<https://github.com/BohrenAn>



<https://isolutions.ch>



Agenda



Wiederholung bekannter Methoden

- Sender Policy Framework (SPF)
- Domain Key Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)

Neue Methoden

- DNS-based Authentication of Named Entities (DANE)
- Mail Transfer Agent Strict Transport Security (MTA-STS)
- Authenticated Received Chain (ARC)
- Brand Indicators for Message Identification (BIMI)
- Certification Authority Authorization (CAA)
- Null MX

Reports in Office 365

Swiss Domain Security Report



Wiederholung bekannter Methoden



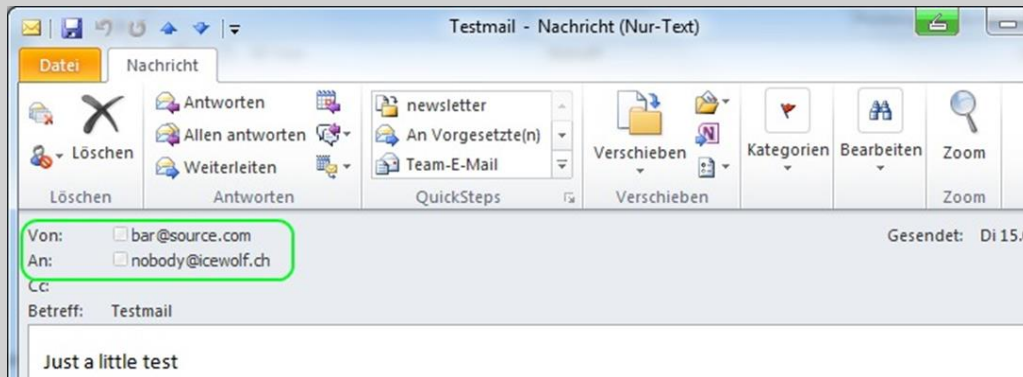
Email Basics

Envelope (Mailserver / MTA)

- Mail from (P1)
- Rcpt to

Header (Recipient / MUA / Outlook)

- From (P2)
- To



```
C:\>Administrator: Command Prompt
220 relay.icewolf.ch Microsoft ESMTMP MAIL Service ready at Tue, 15 May 2012 22:5
9:02 +0200
helo host.source.com
250 relay.icewolf.ch Hello [172.21.175.11]
mail from: foo@source.com
250 2.1.0 Sender OK
rcpt to: a.bohren@icewolf.ch
250 2.1.5 Recipient OK
data
354 Start mail input; end with <CRLF>.<CRLF>
Subject: Testmail
From: bar@source.com
To: nobody@icewolf.ch

Just a little test
.
250 2.6.0 <7660c575-6375-413b-bbfd-95f1c8458d70@ICESRU01.corp.icewolf.ch> [Inter
nalId=1288291] Queued mail for delivery
quit
221 2.0.0 Service closing transmission channel

Connection to host lost.
C:\>
```



Basics

Authenticate Outbound Email to Improve Deliverability

- <https://techcommunity.microsoft.com/t5/exchange-team-blog/authenticate-outbound-email-to-improve-deliverability/ba-p/3947623>
- SPF / DKIM / DMARC wird wärmstens empfohlen

We strongly recommend all our customers use these mechanisms to increase the chance of email being accepted by external recipients.

- [Learn more about SPF and how to set it up to authenticate email you send from Microsoft 365](#) (Microsoft Learn)
- [Learn more about DKIM and how to set it up to sign email you send from Microsoft 365](#) (Microsoft Learn)
- [Learn more about DMARC and how to set it up to validate email you send from Microsoft 365](#) (Microsoft Learn)



Sender Policy Framework (SPF)



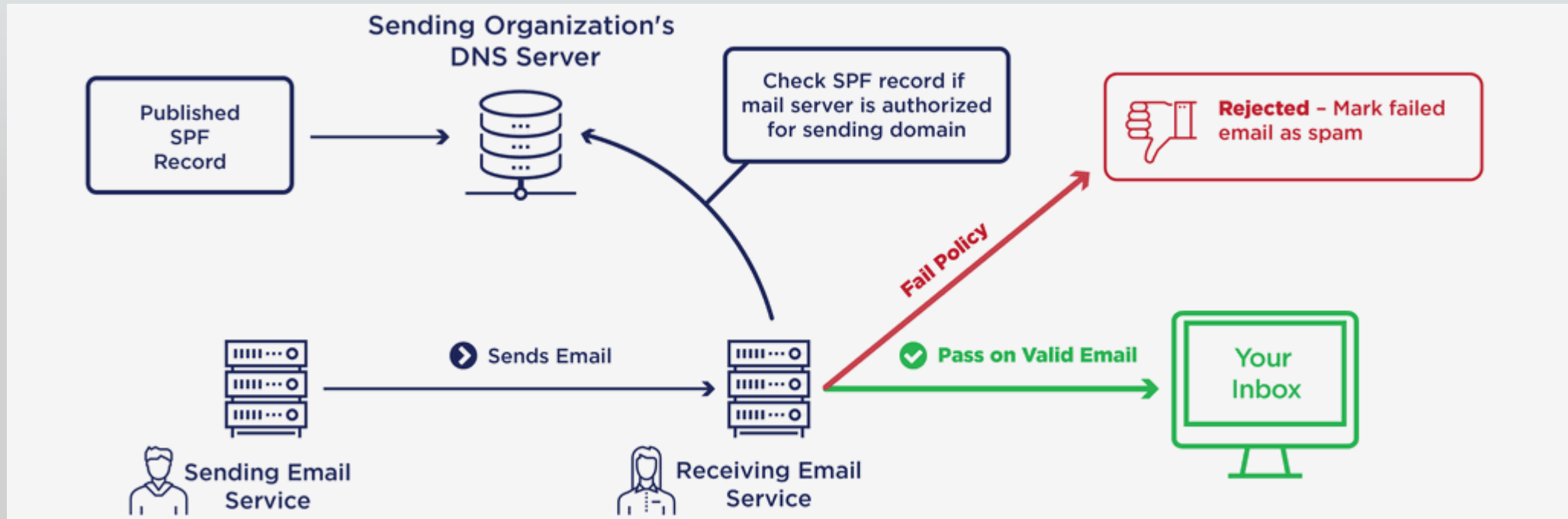
- SPF existiert seit 2003 mit Updates 2006 und 2014 [rfc7208](#)
- Definiert in einem DNS-TXT-Eintrag, welche Mailserver E-Mails für diese Domain versenden können
- Basierend auf E-Mails von (Umschlag / Mail From / P1)
- Hilft beim Schutz der Domain
- Es gibt Probleme, je nachdem, wie E-Mails weitergeleitet werden (Rewrite Envelope)
- Maximal 10 Lookups dürfen verwendet werden.

nslookup -type=txt icewolf.ch

"v=spf1 mx ip4:95.143.60.16/29 include:spf.protection.outlook.com -all"



SPF



Best Practices für SPF-Einträge

- Jede Domain hat einen SPF-Eintrag
- Includes und A-Einträge im SPF-Eintrag überschreiten nicht 10 DNS-Lookups
- SPF-Einträge haben "-all" (Hardfail) am Ende
- Verwenden von "v=spf1 -all" für Domains, die nicht für E-Mails verwendet werden



Domain Key Identified Mail (DKIM)

- Definiert in [rfc6376](#) von 2011 mit updates in [rfc8301](#) und [rfc8463](#).
- Basiert auf Zertifikaten > die headers in h= werden signiert
- Pass → Die signierten Header wurden nicht verändert
- Löst das Problem mit Weiterleitungen bei SPF
- Selector kann irgendetwas sein > selector1 / selector2 in Office 365

<https://blog.icewolf.ch/archive/2015/02/28/spf-dkim-dmarc.aspx>

```
Windows PowerShell
PS C:\> nslookup -type=txt selector1._domainkey.icewolf.ch
Server: ICESRV01.corp.icewolf.ch
Address: 172.21.175.10

Non-authoritative answer:
selector1._domainkey.icewolf.ch canonical name = selector1-icewolf-ch._domainkey.icewolfch.onmicrosoft.com
selector1-icewolf-ch._domainkey.icewolfch.onmicrosoft.com text =

        "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu/9+1UZY2vCHE+mA6PH3PM8tV2RG57yIlq9ZziziT4oz6Rs5DRZT+TTyCkfSgdnt9rLb+NIKkDAFCr7
043c0bS8xxMxL35rFh0zD4CjUAVhgQC9XOCpIPcEaJoJXSyIOCd1Rt3HP5FMv1pEScFCAPavTDxgeDs2b9M/+LXjRhDY1JQ00/zAw+RJsiiJxU/uD4"
        "SQeyInQ9wKKDCh4hRx0YSM1oi+ehU5DI4TsnYNjAcFidheHYCEqpljKxldxf6cjgl5G3s9kicWQJS/bgstph3pg0MHj9sFha/L16gNiCSCz8605fV9iIoRfPLBM5qbYC7Un1vjC5NDFc7
D8MJyIWQIDAQAB;"
PS C:\>
```



DKIM Header



Properties

Settings

ImportanceNormalSensitivityNormal

☐ Do not AutoArchive this item

Tracking options

☐ Request a delivery receipt for this message☐ Request a read receipt for this message

Delivery options

Have replies sent to☐ Expires afterNone00:00

Contacts...CategoriesNone

Internet headers

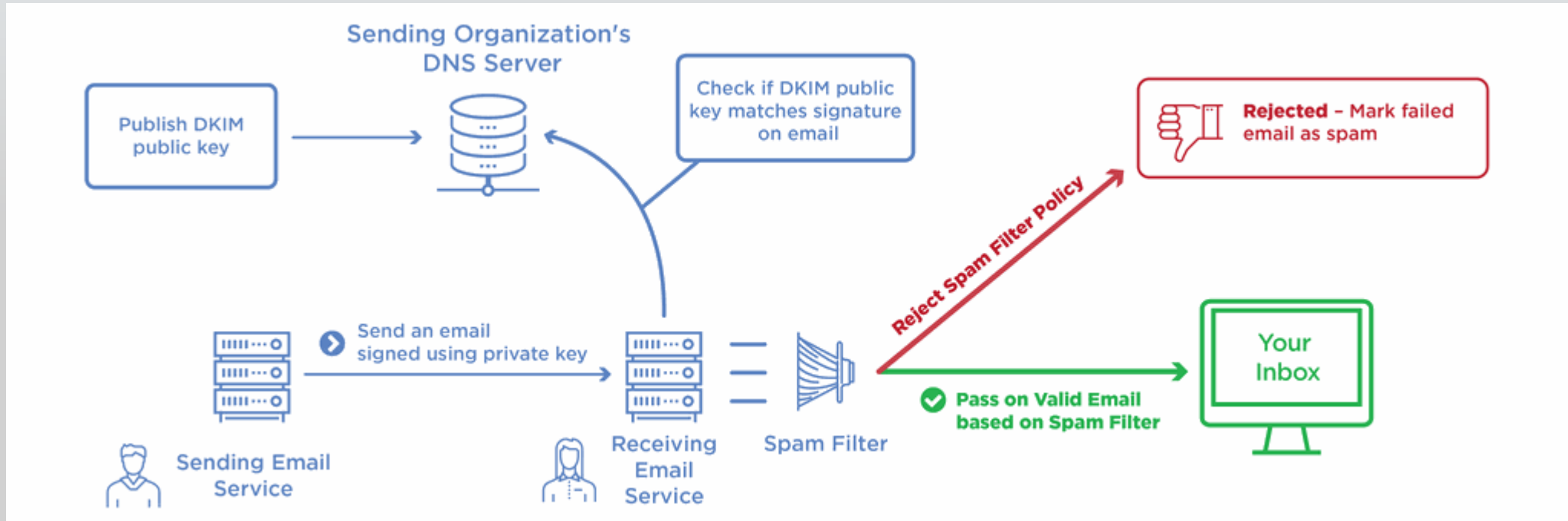
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=icewolf.ch; s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=SJI6uyuO0rFz4beqbOYbi5QB0BJo2QkWNBsVji2nmSU=; b=Rx1K0bzt/39T3LJj2KjQ3iN37TocsGVYInlwzHq/GTrkMcmDaa/FR7ntG;

Tag	Explanation
v=1	DKIM Version
a=ras-sha256	algorithm used to generate the signature
c=relaxed/relaxed	Header/Body Message canonicalization
d=icewolf.ch	Sending Domain
s=selector1	Selector used for this Mail
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck	Signed header fields
bh=hash	The hash of the canonicalized body part
b=signature	The signature data (Base64)



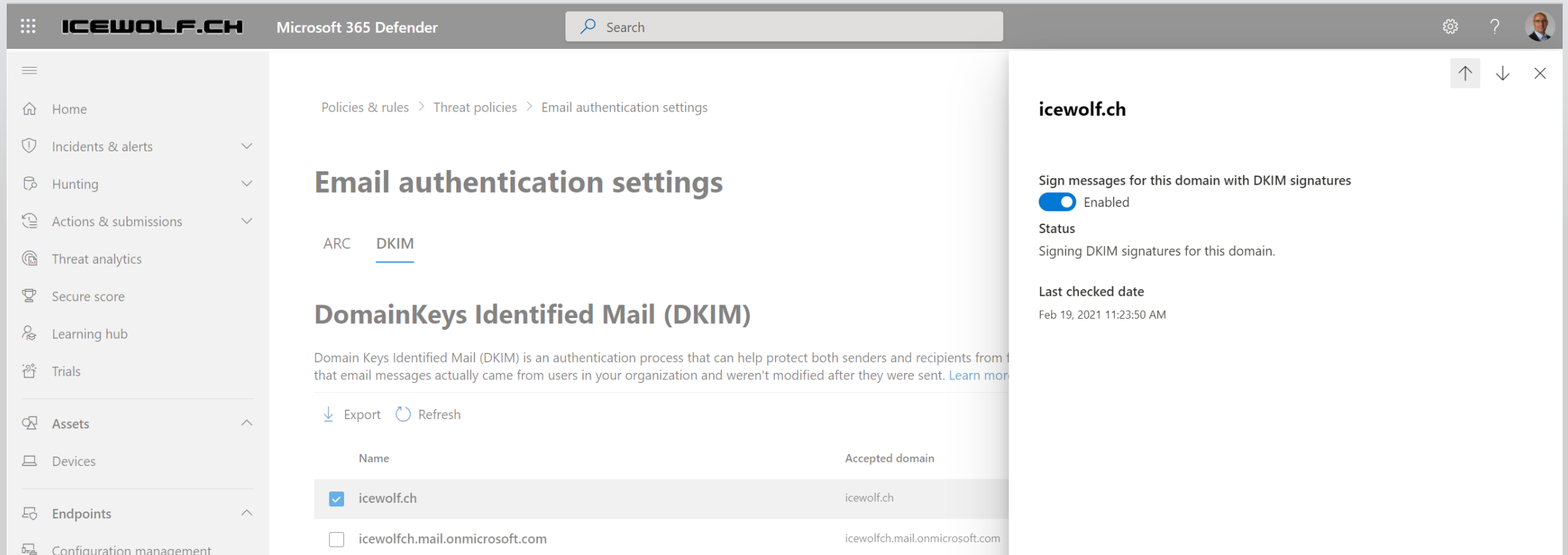
DKIM

Signatur über E-Mail-Header, die mit Zertifikaten und öffentlichen Schlüsseln geschützt sind



DKIM in Exchange Online I

<https://security.microsoft.com/authentication?viewid=DKIM>



The screenshot displays the Microsoft 365 Defender interface. The top navigation bar includes the 'ICEWOLF.CH' logo, 'Microsoft 365 Defender' text, a search bar, and user profile controls. The left sidebar lists various security features like Home, Incidents & alerts, Hunting, Actions & submissions, Threat analytics, Secure score, Learning hub, Trials, Assets, Devices, Endpoints, and Configuration management. The main content area is titled 'Email authentication settings' and shows the 'DKIM' tab selected. It includes a breadcrumb trail: 'Policies & rules > Threat policies > Email authentication settings'. Below the title, there's a section for 'DomainKeys Identified Mail (DKIM)' with a description and a 'Learn more' link. A table lists the domains configured for DKIM, with 'icewolf.ch' checked and 'icewolfch.mail.onmicrosoft.com' unchecked. On the right, a summary panel for 'icewolf.ch' shows that DKIM signing is 'Enabled', the status is 'Signing DKIM signatures for this domain.', and the last checked date is 'Feb 19, 2021 11:23:50 AM'.

ICEWOLF.CH Microsoft 365 Defender Search

Home Incidents & alerts Hunting Actions & submissions Threat analytics Secure score Learning hub Trials Assets Devices Endpoints Configuration management

Policies & rules > Threat policies > Email authentication settings

Email authentication settings

ARC DKIM

DomainKeys Identified Mail (DKIM)

Domain Keys Identified Mail (DKIM) is an authentication process that can help protect both senders and recipients from threats that email messages actually came from users in your organization and weren't modified after they were sent. [Learn more](#)

Export Refresh

Name	Accepted domain
<input checked="" type="checkbox"/> icewolf.ch	icewolf.ch
<input type="checkbox"/> icewolfch.mail.onmicrosoft.com	icewolfch.mail.onmicrosoft.com

icewolf.ch

Sign messages for this domain with DKIM signatures ☒ Enabled

Status
Signing DKIM signatures for this domain.

Last checked date
Feb 19, 2021 11:23:50 AM



DKIM in Exchange Online II

Get-DkimSigningConfig -Identity icewolf.ch | fl Domain, Enabled, Selector*

```
Windows PowerShell
PS C:\> Get-DkimSigningConfig -Identity icewolf.ch | fl Domain, Enabled, Selector*

Domain                : icewolf.ch
Enabled               : True
Selector1KeySize      : 2048
Selector1CNAME        : selector1-icewolf-ch._domainkey.icewolfch.onmicrosoft.com
Selector1PublicKey    : v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu/9+1UZY2vCHE+mA6PH3PM8tV2RG57yI1q9ZziziT4oz6Rs5DRZT+TTyCk
                        fSgdnt9rLb+NIkkDAFCr7O43c0bS8xxMxL35rFh0zD4CjUAVhgQC9XOCpIPcEaJoJXSyIOCd1Rt3HP5FMv1pEScFCAPavTDxgeDs2b9M/+LXjRhDY1JQ00/z
                        Aw+RJsiiIJxU/uD4SQeyInQ9wKKDCh4hRx0YSM1oi+ehU5DI4TsnYNjAcFidheHYCEqp1jkxldxf6cjgl5G3s9kicWQJS/bgstph3pg0MHj9sFha/L16gNiCS
                        Cz8605fV9iIoRFPLBM5qbYC7Un1vjc5NDFc7D8MJyIWQIDAQAB;
Selector2KeySize      : 1024
Selector2CNAME        : selector2-icewolf-ch._domainkey.icewolfch.onmicrosoft.com
Selector2PublicKey    : v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcQn10K95AAOM71uthw6nEmPqWS1cjBM2L4ruuPhd5gksaco6rc1PeK1eKkUWZno
                        OgUwe4RUWStwVvQ1Fk9pxSu13WvWveO5vuIFKUq9juFiq67R4UjX1xET1Z/ATzxWAVu0H3wdF3XLBCeqFNhcgGQqdmvIA5goioBHNvqCzvOQIDAQAB;
SelectorBeforeRotateOnDate : selector2
SelectorAfterRotateOnDate  : selector1

PS C:\>
```

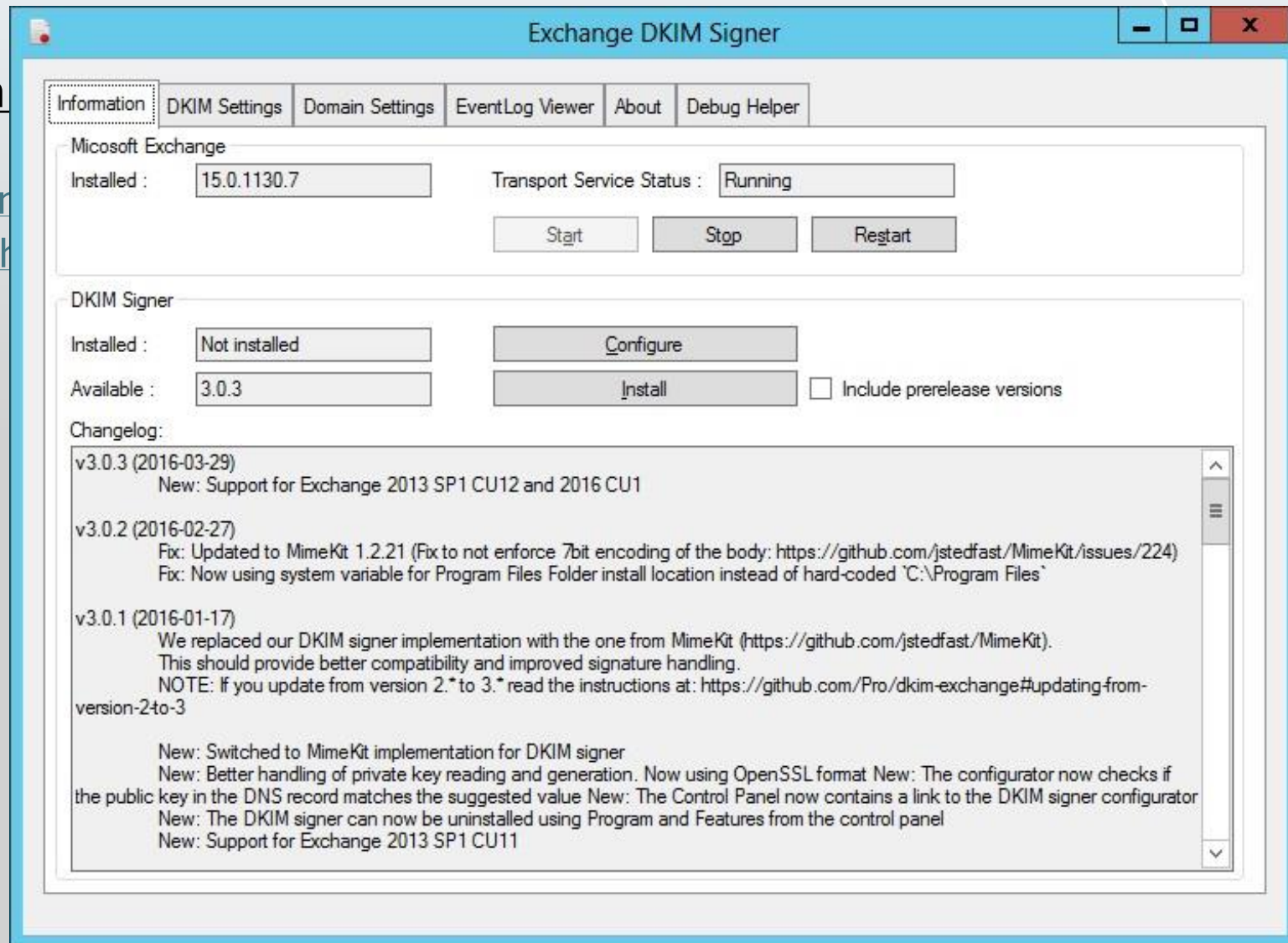


DKIM Signer – Exchange OnPrem

Das geht auch mit dem

<https://github.com/Pro/dkim-exchange>

<https://blog.icewolf.ch/archiv/2016/03/dkim-signer-exchange-onprem/>



DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC)

DMARC gibt es seit 2015 definiert in [rfc7489](#)

Die Mailserver von Empfängern, die DMARC unterstützen, geben den Domaininhabern Feedback über die Verwendung ihrer Domains. Dieses Feedback kann wertvolle Erkenntnisse über die Nutzung und den Missbrauch Ihrer Domains liefern.

```
nslookup -type=txt _dmarc.icewolf.ch
```

```
"v=DMARC1; p=reject; sp=reject;
```

```
rua=mailto:skmtvc6p@ag.eu.dmarcadvisor.com,mailto:44aa291caf@rua.easydmarc.eu;
```

```
ruf=mailto:postmaster@icewolf.ch"
```



DMARC Record

nslookup -type=txt _dmarc.icewolf.ch
"v=DMARC1; p=reject; sp=reject;
rua=mailto:skmtvc6p@ag.eu.dmarcadvisor.com,mailto:44aa291caf@rua.easydmarc.eu;
ruf=mailto:postmaster@icewolf.ch"

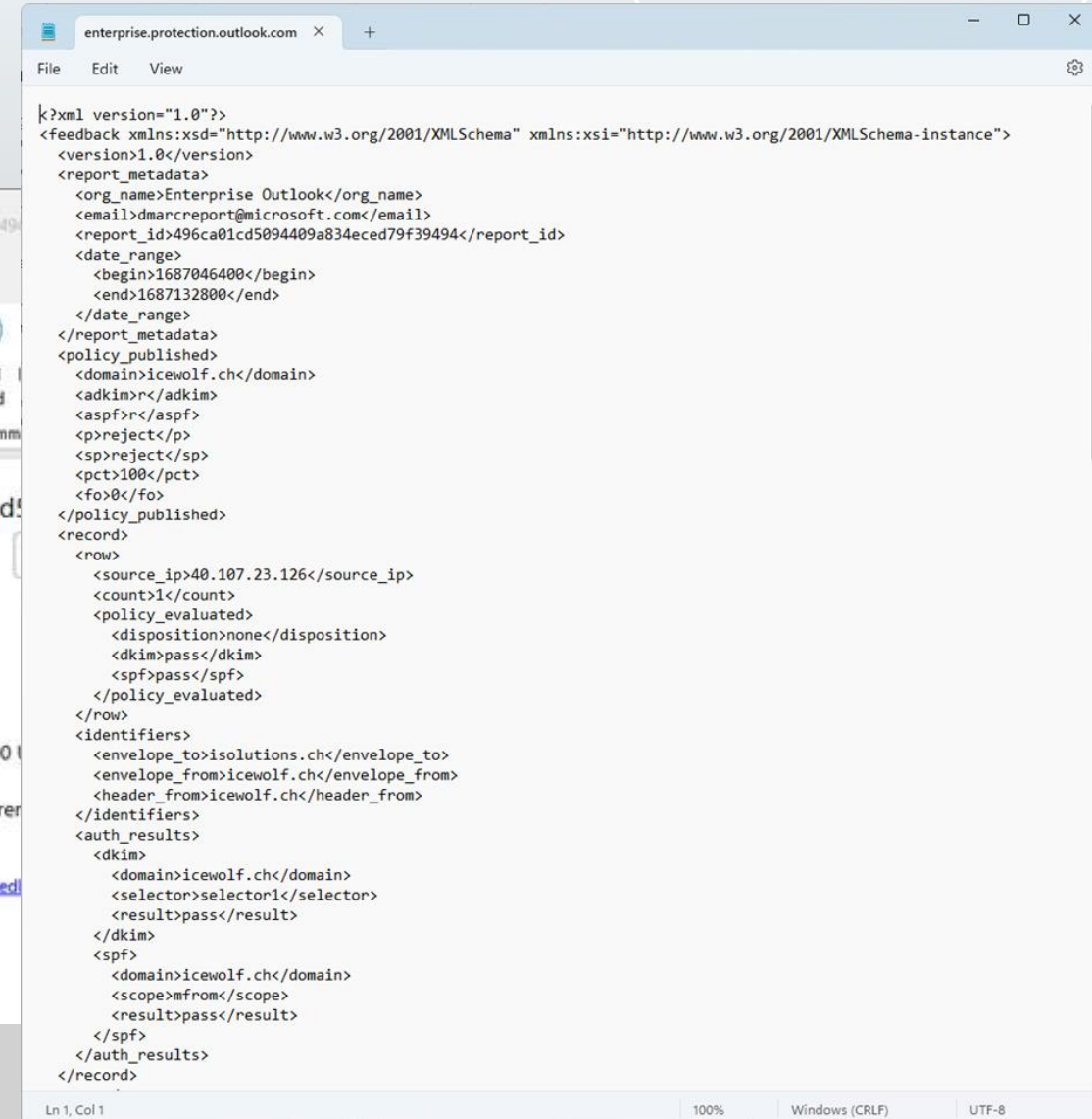
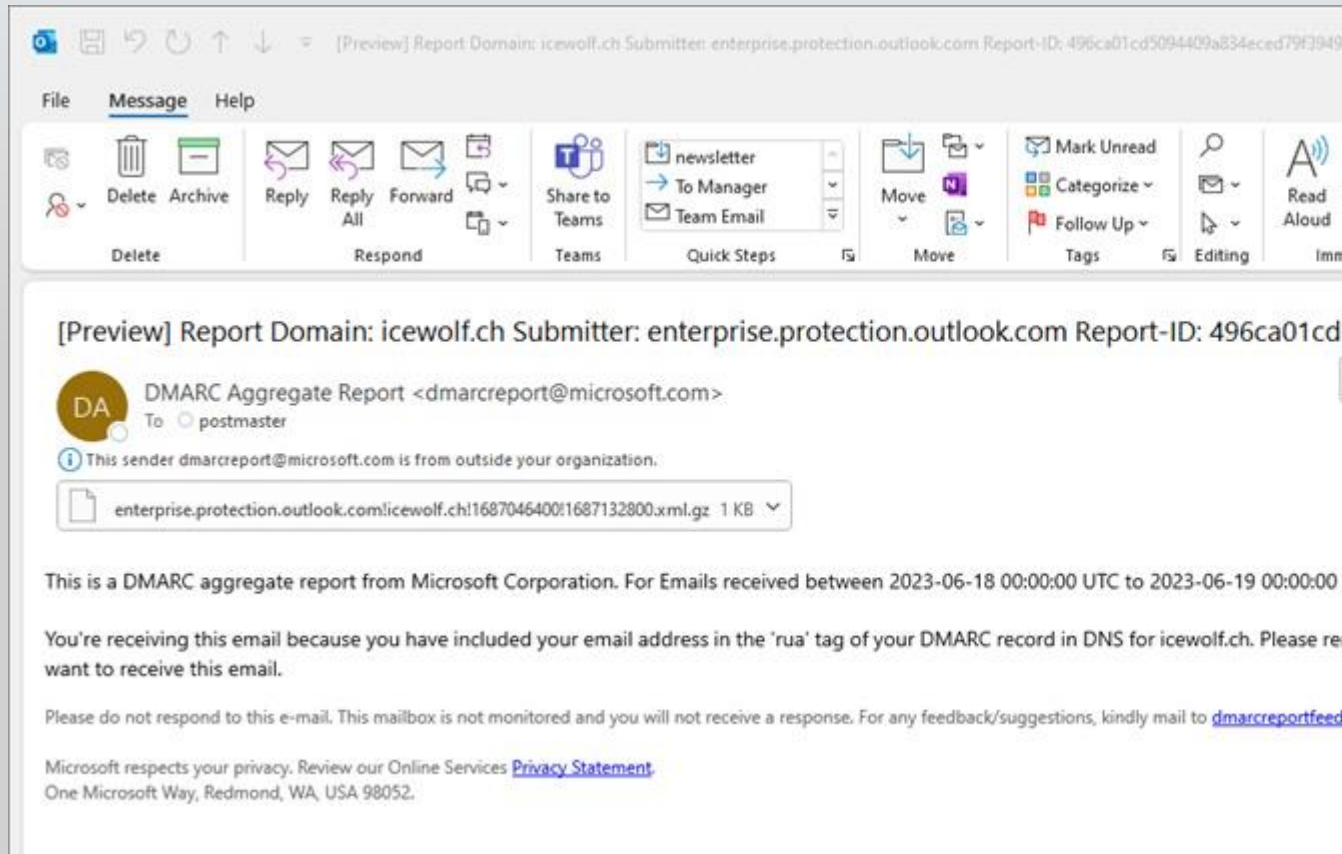


Tag Name	Zweck	Beispiel
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=none/quarantine/reject
sp	Policy for subdomains of the OD	sp=none/quarantine/reject
adkim	Alignment mode for DKIM	adkim=s (r=relaxed mode/s=strict mode)
aspf	Alignment mode for SPF	aspf=r (r=relaxed mode/s=strict mode)



DMARC RUA Reports

Reports sind Email mit ZIP Anhang welche XML enthalten



Dmarc Data Provider

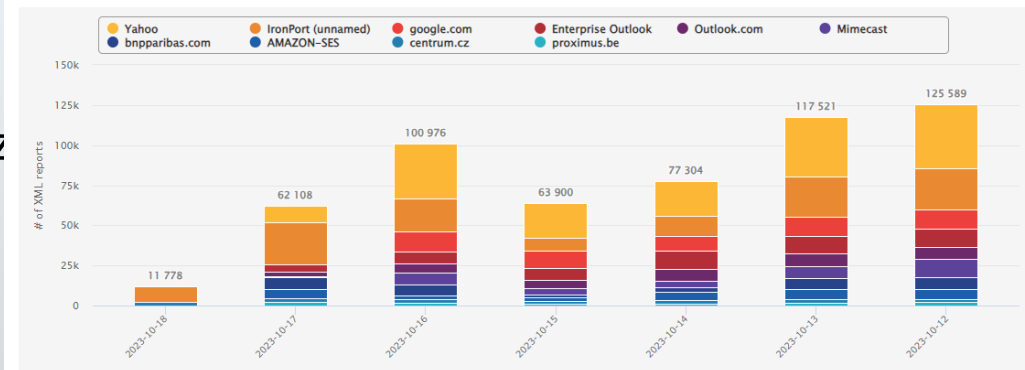
Bis April 2023 gab es nur wenige Mailserver, welche Reports z

- gmail.com
- yahoo.com
- outlook.com

<https://dmarcian.com/dmarc-data-providers/>

DMARC Data Reporters

This graph shows the top 10 DMARC XML data reporters to **dmarcian** for the past week dates in UTC



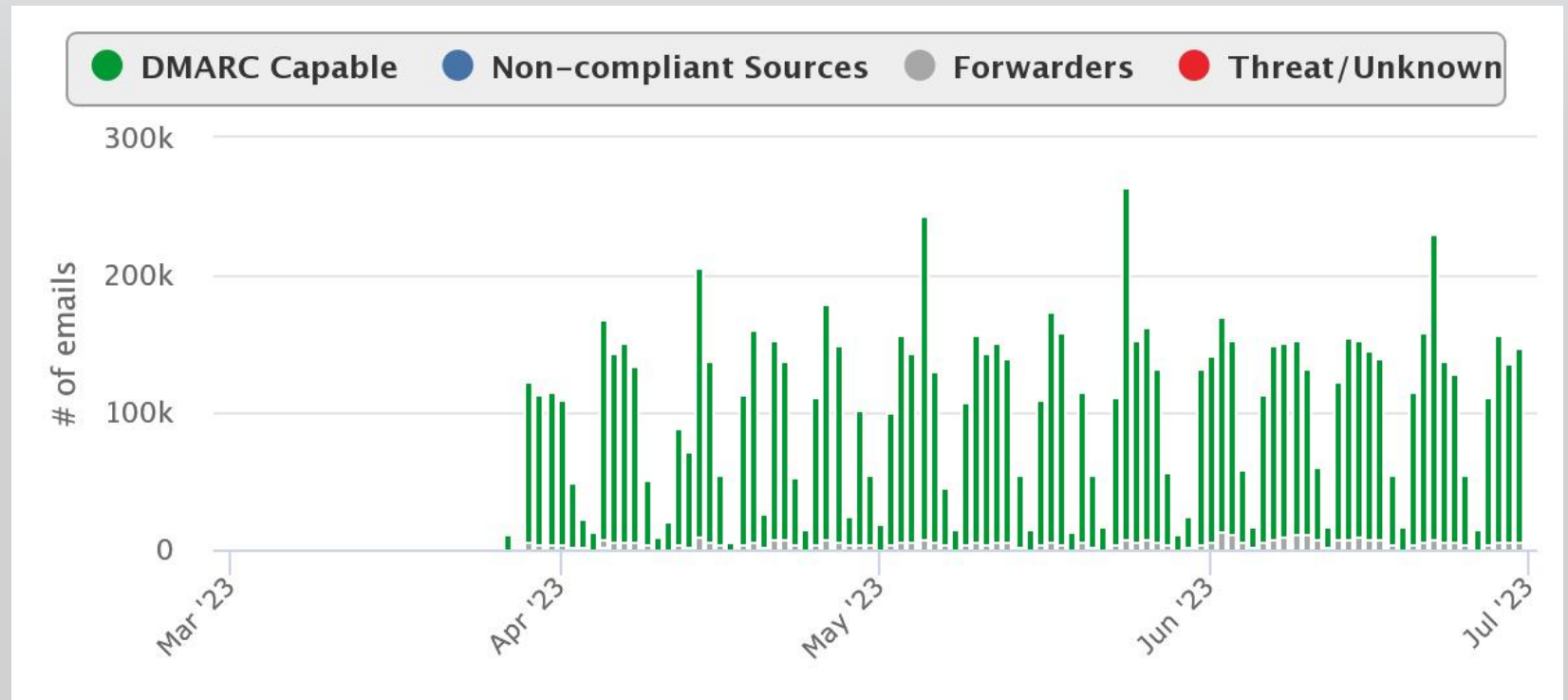
All providers that have provided **dmarcian** data over the past week (UTC). Counts indicate the number of XML reports received.

Enter search term									Filter
Provider	Total Reports	2023-10-18	2023-10-17	2023-10-16	2023-10-15	2023-10-14	2023-10-13	2023-10-12	
Yahoo	165,018	0	10,294	34,444	21,820	21,285	37,001	40,174	
IronPort (unnamed)	127,250	9,426	26,277	20,217	8,139	12,719	24,913	25,559	
google.com	56,209	0	0	12,514	10,278	9,257	12,127	12,033	
Enterprise Outlook	53,627	0	4,434	7,748	7,747	11,146	11,251	11,301	
Outlook.com	36,390	0	2,938	5,253	5,007	7,755	7,860	7,577	
Mimecast	34,710	0	339	7,787	3,954	3,908	7,406	11,316	
bnpparibas.com	33,110	0	7,387	6,852	1,833	2,510	6,897	7,631	
AMAZON-SES	27,752	0	5,757	2,411	2,525	5,478	5,815	5,766	
centrum.cz	14,839	2,352	2,497	1,864	1,614	2,063	2,328	2,121	
proximus.be	10,271	0	2,185	1,886	983	1,183	1,923	2,111	

1 to 10 of 4194 Per page 10 1 of 420 pages 1 2 3 4 5

Exchange Online DMARC RUA Report

Laut DMARCAdvisor wurden die aggregierten Berichte über Nacht verdoppelt, als Microsoft begann, DMARC-aggregierte Berichte zu versenden. In der zweiten Aprilwoche wurden fast 33 Millionen Berichte aus Enterprise Outlook verarbeitet. Zum Beispiel können Sie die DMARC Aggregate-Berichte eines Unternehmens in den Niederlanden sehen - im April 2023 gibt es eine massive Änderung.



DMARC Report Provider

Gibt verschiedene Anbieter um die RUA Reports auszuwerten.

- www.dmarcadvisor.com
- www.easydmARC.com
- www.dmarcian.com
- www.agari.com
- www.valimail.com (Kostenlos aber Reports haben zu wenig Details)



Neue Methoden



DANE



DNS-based Authentication of Named Entities (DANE)

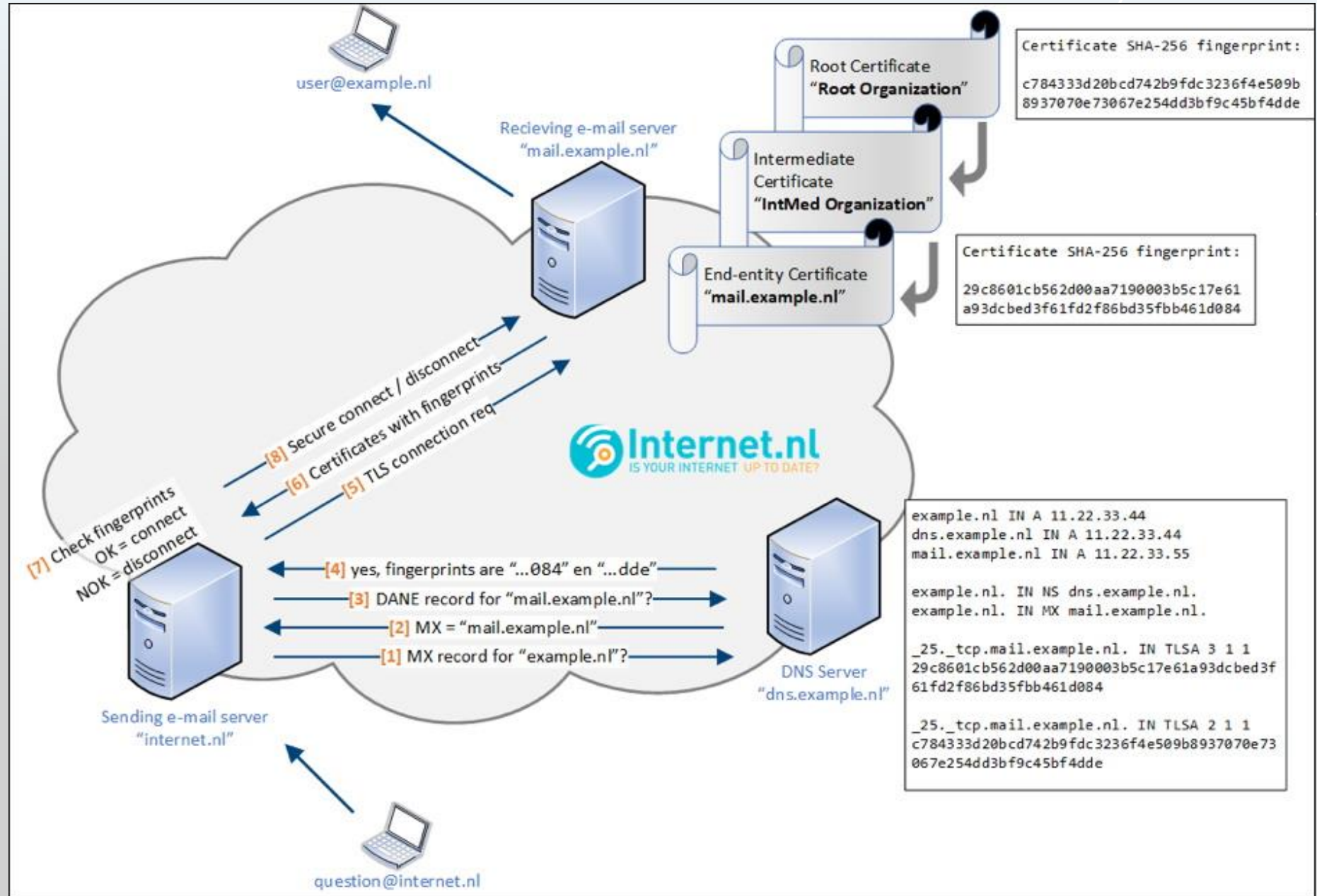
- Existiert seit 2015 [rfc8461](#)
- Benötigt DNSSEC (signierte DNS-Zone)
- Veröffentlichen Sie den Fingerabdruck des vom Mailserver verwendeten Zertifikats im DNS
- Komplex in der Implementierung
- Zertifikats-Rollover / Umgang mit Zertifikaten muss beherrscht werden

- Eingehender Support in Exchange Online ist allgemein verfügbar (GA)
- Ausgehender Support in Exchange Online Jahresende / H1 2024

- Fun Fact: Azure DNS unterstützt DNSSEC nicht



DANE



Signierte Zone?

Kann nicht

Kann nicht

\$Domain

\$json = Invoke-WebRequest

\$json

AD: Authentifizierung

```
Windows PowerShell
PS C:\> $Domain = "hostpoint.ch"
PS C:\> $json = Invoke-WebRequest -URI "https://dns.google/resolve?name=$Domain&type=MX"
PS C:\> $json

Status      : 0
TC           : False
RD           : True
RA           : True
AD           : True
CD           : False
Question    : {@{name=hostpoint.ch.; type=15}}
Answer      : {@{name=hostpoint.ch.; type=15; TTL=1673; data=1 mx.hostpoint.ch.}, @{{name=hostpoint.ch.; type=15; TTL=1673; data=20
              backupmx.hostpoint.ch.}}}

PS C:\> $Domain = "icewolf.ch"
PS C:\> $json = Invoke-WebRequest -URI "https://dns.google/resolve?name=$Domain&type=MX"
PS C:\> $json

Status      : 0
TC           : False
RD           : True
RA           : True
AD           : False
CD           : False
Question    : {@{name=icewolf.ch.; type=15}}
Answer      : {@{name=icewolf.ch.; type=15; TTL=3600; data=10 icewolf-ch.mail.protection.outlook.com.}}
Comment     : Response from 2620:1ec:8ec::3.

PS C:\>
```



TLSA Record

Kann nicht mit nslookup abgefragt werden

Kann nicht mit Resolve-DnsName

```
$TLSAQuery = "_25._tcp.mx.hostpoint.ch"
```

```
$json = Invoke-RestMethod -URI "https://dns.google/resolve?name=$TLSAQuery&type=TLSA"
```

```
$TLSA = $json.Answer.data
```

```
$TLSA
```



```
Windows PowerShell
PS C:\> $TLSAQuery = "_25._tcp.mx.hostpoint.ch"
PS C:\> $json = Invoke-RestMethod -URI "https://dns.google/resolve?name=$TLSAQuery&type=TLSA"
PS C:\> $TLSA = $json.Answer.data
PS C:\> $TLSA
3 1 1 acfel1f854ef8584750090f156e3c91a4c4cee0e31d5b9cac9946791367d2f7bd
PS C:\>
```



TLSA Record



Certificate Usage (0 - 3)

0=The Hash belongs to the Certificate Authority who is allowed to issue Certificates for this Host. The Client must trust this CA (Trusted Root CA or Trusted Subordinate CA)

1=The Hash belongs to the Servercertificate. It has to be from a CA that the Client trusts.

2=The Hash belongs to the Certificate Authority who is allowed to issue Certificates for this Host. The Client must trust this CA even if it's not in the List of the Trusted Root CA or Trusted Subordinate CA of the Client

3=The Hash belongs to the Servercertificate and the Client shall trust it without having a look at the Certificate Chain

Selector (0 or 1)

0=Hash will be from the complete Certificate

1=Hash will only be from the Public Key and the algorithm

Matching Type (0-2)

0=Hash contains the full certificate

1=Hash contains a SHA-256 hash

2=Hash contains a SHA-512 hash



Exchange Online DANE Inbound

Implementing Inbound SMTP DANE with DNSSEC for Exchange Online Mail Flow

<https://techcommunity.microsoft.com/t5/exchange-team-blog/implementing-inbound-smtp-dane-with-dnssec-for-exchange-online/ba-p/3939694>

The initial support for inbound SMTP DANE with DNSSEC will come in 2 waves:

- March 2024: opt-in Public Preview. For Accepted Domains provisioned in mail.protection.outlook.com, customers will be able to use the M365 Admin Center for enabling SMTP DANE on an Accepted Domain and will be able to migrate existing domains into the new DNSSEC-enabled zones.
- July 2024: post General Availability (GA), layering DNSSEC into Exchange Online for inbound mail flow. Between July and December 2024, we will gradually switch provisioning of all A records for new Accepted Domains into the new subdomains under mx.microsoft.

Microsoft Exchange

	Type	Status	Name	Value	TTL
<input type="checkbox"/>	MX	 OK	@	0 fabrikam-com.1j2b-v1.mx.microsoft	1 Hour



Herausforderungen

DANE hat hohe Anforderungen

- DNSSEC
- TLSA Records können bei den meisten DNS Providern nicht erstellt werden
 - Zumindest nicht im Admin Panel
 - Geht auch bei Azure DNS nicht (Unterstützt ja auch kein DNSSec)



Add record set

icewolf.ch

Name

.icewolf.ch

Type

A – Address record

A – Address record

AAAA – Address record

CAA – Certificate Authorities to authorize certificates

CNAME – Link your subdomain to another record

MX – Mail eXchange records

NS – Name Server records

SRV – Service records

TXT – Text record type

PTR – Pointer record type



MTA-STS / TLS Reporting



Mail Transfer Agent Strict Transport Security (MTA-STS)

- Existiert seit 2018 [rfc8461](#)
- E-Mails werden über eine sichere Verbindung (TLS) übertragen.
- Sie verwenden die TLS-Version 1.2 oder höher.
- Für die TLS-Zertifikate der Server gilt:
 - Der enthaltene Domainname entspricht dem des Servers für eingehende E-Mails. Das ist der Server in Ihren MX-Einträgen.
 - Sie sind signiert und werden von einer Stammzertifizierungsstelle als vertrauenswürdig eingestuft.
 - Sie dürfen nicht abgelaufen sein.

MTA-STS bietet Schutz gegen :

- Downgrade-Angriffe
- Man-In-The-Middle (MITM) -Angriffe
- Es löst mehrere SMTP-Sicherheitsprobleme, darunter abgelaufene TLS-Zertifikate und fehlende Unterstützung für sichere Protokolle.



MTA-STS DNS TXT Record

MTA-STS besteht aus:

- TXT Record (_mta-sts.domain.tld)
- MTA-STS Richtlinie ([https://mta-sts.\\$Domain/.well-known/mta-sts.txt](https://mta-sts.$Domain/.well-known/mta-sts.txt))

```
nslookup -type=txt _mta-sts.google.com
```

```
Resolve-DnsName -Name _mta-sts.google.com -Type TXT
```

```
v=STSV1; id=20210803T010101;
```

```
Windows PowerShell
PS C:\> Resolve-DnsName -Name _mta-sts.google.com -Type TXT
```

Name	Type	TTL	Section	Strings
----	----	----	-----	-----
_mta-sts.google.com	TXT	214	Answer	{v=STSV1; id=20210803T010101;}

```
PS C:\>
```

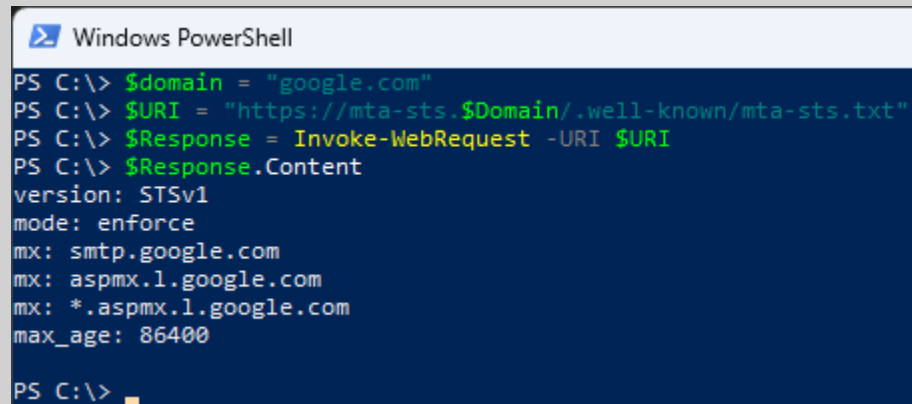


MTA-STS Richtlinie

<https://mta-sts.domain.tld/.well-known/mta-sts.txt>

```
$domain = "google.com"  
$URI = "https://mta-sts.$Domain/.well-known/mta-sts.txt"  
$Response = Invoke-WebRequest -URI $URI  
$Response.Content
```

```
version: STSv1  
mode: enforce  
mx: smtp.google.com  
mx: aspmx.l.google.com  
mx: *.aspmx.l.google.com  
max_age: 86400
```



```
Windows PowerShell  
PS C:\> $domain = "google.com"  
PS C:\> $URI = "https://mta-sts.$Domain/.well-known/mta-sts.txt"  
PS C:\> $Response = Invoke-WebRequest -URI $URI  
PS C:\> $Response.Content  
version: STSv1  
mode: enforce  
mx: smtp.google.com  
mx: aspmx.l.google.com  
mx: *.aspmx.l.google.com  
max_age: 86400  
PS C:\> █
```



MTA-STS für Exchange Online

MTA-STS Richtlinie für Office 365

<https://techcommunity.microsoft.com/t5/exchange-team-blog/introducing-mta-sts-for-exchange-online/ba-p/3106386>

version: STSv1

mode: enforce

mx: *.mail.protection.outlook.com

max_age: 604800



MTA-STS in Azure

Ich habe in Azure DevOps Starter (free) ein Repository angelegt

<https://blog.icewolf.ch/archive/2023/05/28/http-security-headers/>

#staticwebapp.config.json

```
{
```

```
"gl
```

```
},
```

```
"re
```

```
"2
```

```
}
```

```
}
```

Azure DevOps abohren / MTA-STS / Repos / Files / MTA-STS

Search

MTA-STS

Overview

Boards

Repos

Files

Commits

Pushes

Branches

MTA-STS

deployment

root

.well-known

mta-sts.txt

404.html

index.html

staticwebapp.conf...

azure-static-web-ap...

main

mta-sts.txt

Edit

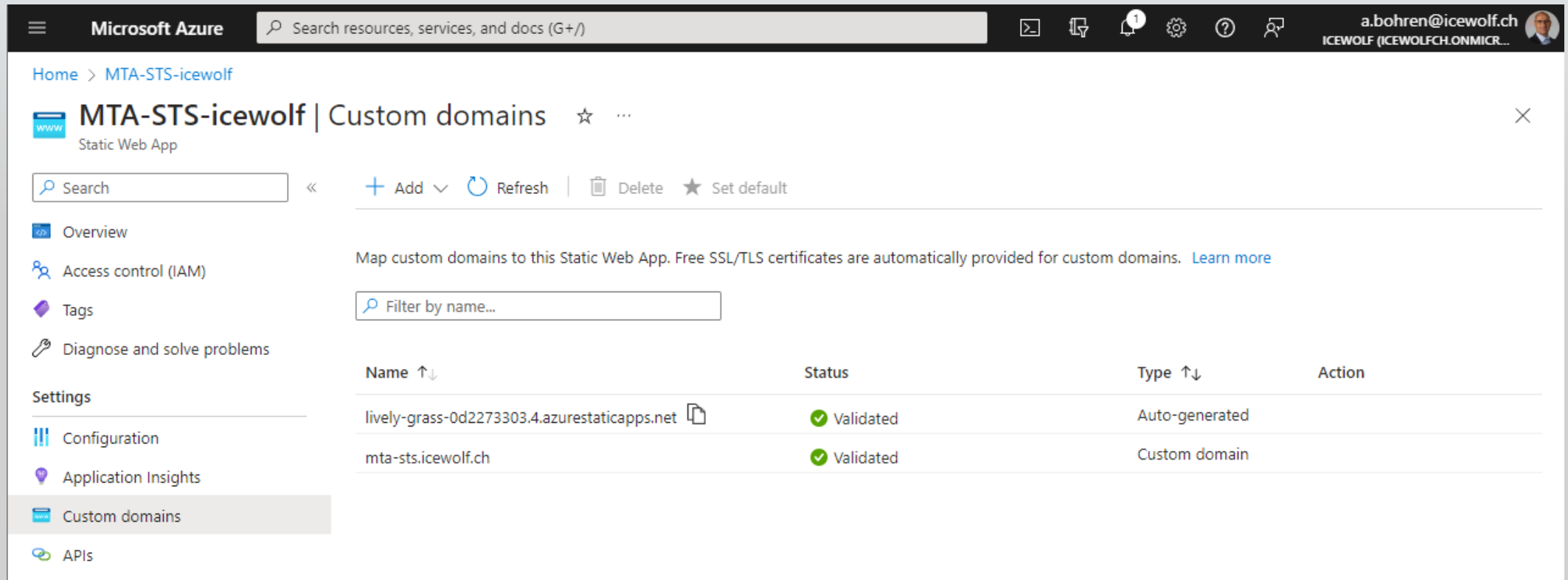
Contents History Compare Blame

```
1 version: STSv1
2 mode: enforce
3 mx: *.mail.protection.outlook.com
4 mx: mail.icewolf.ch
5 max_age: 604800
```



MTA-STS

Ein Push ins Repository triggert eine Pipeline und löst ein Deployment auf die Azure Static Web App aus.
Beim hinzufügen der Domain wird automatisch ein Zertifikat dafür ausgestellt (kein Management nötig)



The screenshot shows the Microsoft Azure portal interface. At the top, the 'Microsoft Azure' header is visible with a search bar and user profile 'a.bohren@icewolf.ch'. The main content area is titled 'MTA-STS-icewolf | Custom domains' and shows a list of domains mapped to the Static Web App. The left sidebar contains navigation links for Overview, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Application Insights, Custom domains (selected), and APIs.

Name ↑↓	Status	Type ↑↓	Action
lively-grass-0d2273303.4.azurestaticapps.net	Validated	Auto-generated	
mta-sts.icewolf.ch	Validated	Custom domain	



TLS-RPT (TLS-Reporting)

Existiert seit 2018 [rfc8461](#)

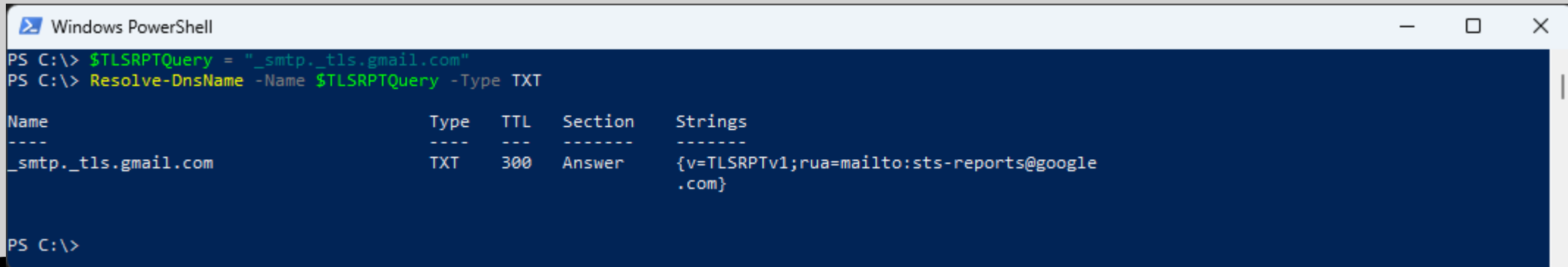
Reporting über Mails an folgende Emailadresse

_smtp._tls.domain.tld TXT

\$TLSRPTQuery = "_smtp._tls.gmail.com"

Resolve-DnsName -Name \$TLSRPTQuery -Type TXT

v=TLSRPTv1;rua=mailto:sts-reports@google.com



```
Windows PowerShell
PS C:\> $TLSRPTQuery = "_smtp._tls.gmail.com"
PS C:\> Resolve-DnsName -Name $TLSRPTQuery -Type TXT

Name                                Type  TTL  Section  Strings
----                                -
_smtp._tls.gmail.com                TXT   300   Answer   {v=TLSRPTv1;rua=mailto:sts-reports@google.com}
```



TLS-RPT

```
1 {
2   "organization-name": "Microsoft Corporation",
3   "date-range": {
4     "start-datetime": "2023-10-20T00:00:00Z",
5     "end-datetime": "2023-10-20T23:59:59Z"
6   },
7   "contact-info": "tlsrpt-noreply@microsoft.com",
8   "report-id": "133423898739584399+icewolf.ch",
9   "policies": [
10    {
11      "policy": {
12        "policy-type": "sts",
13        "policy-string": [
14          "version: STSv1",
15          "mode: enforce",
16          "mx: *.mail.protection.outlook.com",
17          "mx: mail.icewolf.ch",
18          "max_age: 604800"
19        ],
20        "policy-domain": "icewolf.ch"
21      },
22      "summary": {
23        "total-successful-session-count": 23,
24        "total-failure-session-count": 0
25      }
26    }
27  ]
28 }
```

Report-ID:

Select

All

Se

om Rep

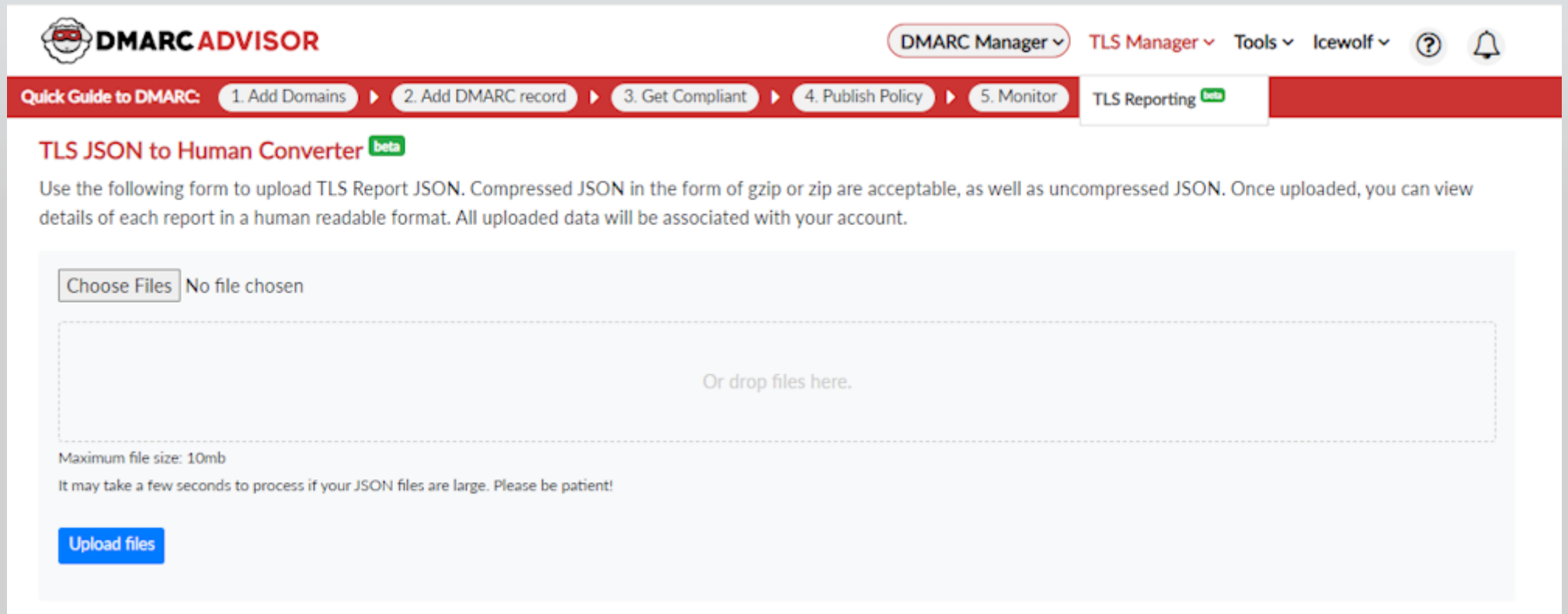
son.gz 88

```
1 {
2   "organization-name": "Google Inc.",
3   "date-range": {
4     "start-datetime": "2023-10-20T00:00:00Z",
5     "end-datetime": "2023-10-20T23:59:59Z"
6   },
7   "contact-info": "smtp-tls-reporting@google.com",
8   "report-id": "2023-10-20T00:00:00Z_icewolf.ch",
9   "policies": [
10    {
11      "policy": {
12        "policy-type": "sts",
13        "policy-string": [
14          "version: STSv1",
15          "mode: enforce",
16          "mx: *.mail.protection.outlook.com",
17          "mx: mail.icewolf.ch",
18          "max_age: 604800"
19        ],
20        "policy-domain": "icewolf.ch",
21        "mx-host": [
22          "*.mail.protection.outlook.com",
23          "mail.icewolf.ch"
24        ]
25      },
26      "summary": {
27        "total-successful-session-count": 2,
28        "total-failure-session-count": 0
29      }
30    }
31  ]
32 }
```



TLS RPT

Bei DMARC Advisor kann man die JSON Files hochladen (letzte 7 Tage) und dann im TLS Manager grafisch anschauen.



The screenshot shows the DMARC Advisor website interface. At the top, there is a navigation bar with the DMARC Advisor logo and several menu items: DMARC Manager, TLS Manager, Tools, Icewolf, a help icon, and a notification bell. Below the navigation bar is a red banner with a "Quick Guide to DMARC" section containing five steps: 1. Add Domains, 2. Add DMARC record, 3. Get Compliant, 4. Publish Policy, and 5. Monitor. The "TLS Reporting" section is highlighted with a green "beta" badge.

The main content area is titled "TLS JSON to Human Converter" with a green "beta" badge. It contains a paragraph explaining the functionality: "Use the following form to upload TLS Report JSON. Compressed JSON in the form of gzip or zip are acceptable, as well as uncompressed JSON. Once uploaded, you can view details of each report in a human readable format. All uploaded data will be associated with your account."

Below the text is a file upload form. It features a "Choose Files" button and the text "No file chosen". A large dashed box is provided for dropping files, with the text "Or drop files here." in the center. Below the dashed box, it states "Maximum file size: 10mb" and "It may take a few seconds to process if your JSON files are large. Please be patient!". At the bottom of the form is a blue "Upload files" button.



TLS-RPT

EasyDMARC unterstützt TLS Reports
Erst mit dem Premium Abo \$71 pro Monat
Und auch nur mit Managed MTA-STS
(CNAME's auf EasyDmarc)



EasyDMARC

Dashboard

All Domains

REPORTS

Aggregate Reports

Failure Reports

TLS Reports

FEATURES

Managed Solutions

EasySPF

Reputation Monitoring

Email Investigation

OTHER

Tools

New Alerts

Alerts

Settings

EasyDMARC premium 100k

Upgrade

0% Permitted volume usage

TLS Reports

serveralive.ch

Filter

Upload file

Export

Hide graph

Oct 03, 2023 - Nov 01, 2023

Success Count

Failure Count

Daily

Weekly

Monthly

Domain	Policy type	Success count	Failure count	Received
serveralive.ch	sts	0	3	Oct 28, 2023 12:00

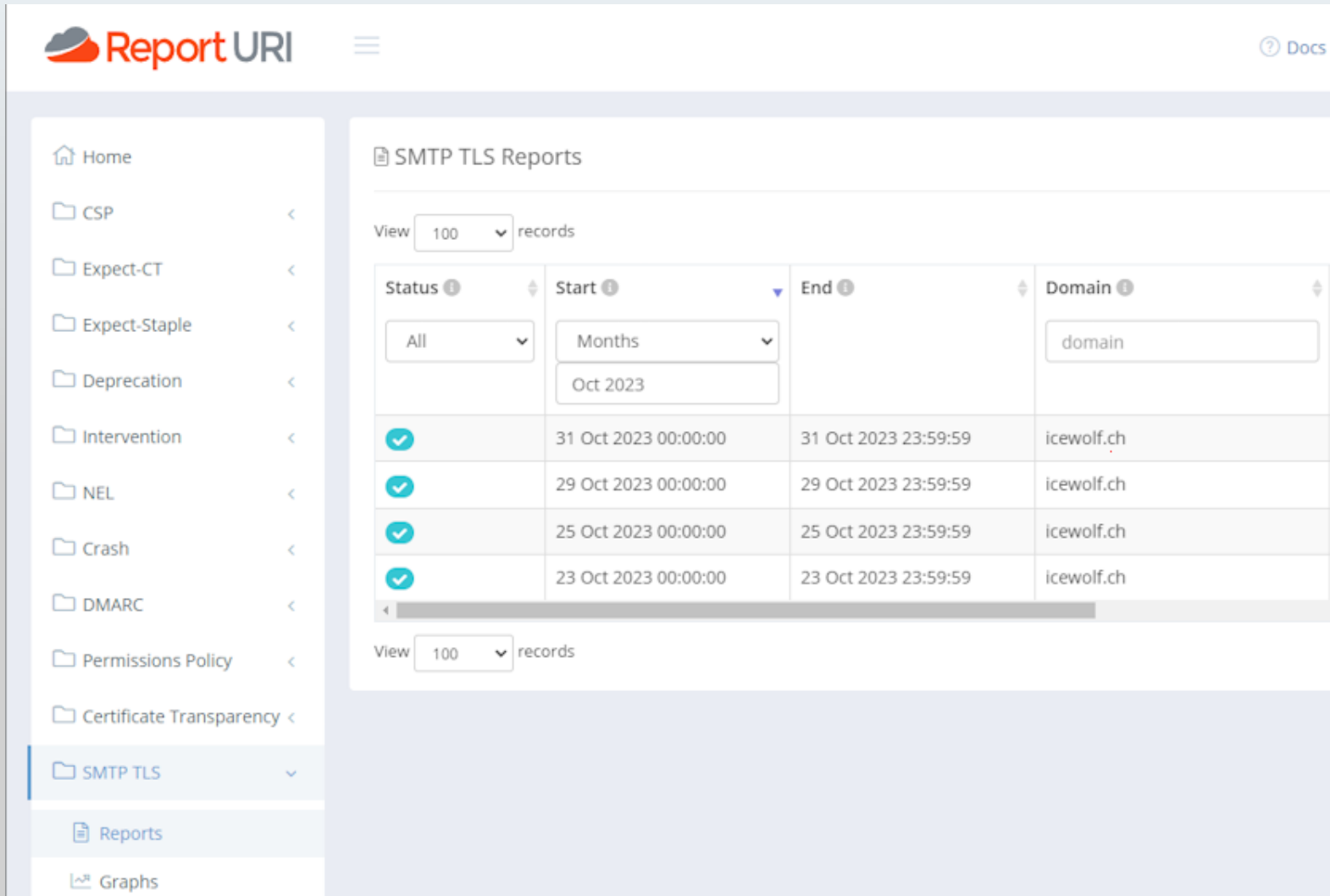
Reporter	Policy mode	Result type	Session count	Receiving MX	Receiving IP	Sending M
No data available in table						

Rows per page: 10

Showing 0 to 0 of 0 entries

Feedback

TLS-RPT



The screenshot shows the 'Report URI' web application. The left sidebar contains a navigation menu with items: Home, CSP, Expect-CT, Expect-Staple, Deprecation, Intervention, NEL, Crash, DMARC, Permissions Policy, Certificate Transparency, SMTP TLS (selected), Reports, and Graphs. The main content area is titled 'SMTP TLS Reports'. It features a 'View 100 records' dropdown and a table with columns: Status, Start, End, and Domain. The table displays four rows of data for the domain 'icewolf.ch' from October 2023. Below the table is another 'View 100 records' dropdown.

Report URI

SMTP TLS Reports

View 100 records

Status	Start	End	Domain
All	Months Oct 2023		domain
✓	31 Oct 2023 00:00:00	31 Oct 2023 23:59:59	icewolf.ch
✓	29 Oct 2023 00:00:00	29 Oct 2023 23:59:59	icewolf.ch
✓	25 Oct 2023 00:00:00	25 Oct 2023 23:59:59	icewolf.ch
✓	23 Oct 2023 00:00:00	23 Oct 2023 23:59:59	icewolf.ch

View 100 records

Pricing

We keep our pricing **simple**, there are no complex licenses here.

SET YOUR USAGE LEVEL

Popular

\$49.99/mo*

- ✓ 500,000 reports
- ✓ Unlimited Domains Monitored[†]
- ✓ 90 Day Retention
- ✓ Threat Intelligence
- ✓ Script Watch
- ✓ Data Watch
- ✓ Team Access
- ✗ Email Support

30-Day Free Trial

* prices may be subject to tax, paid annually

[†] excludes certificate transparency

No-commitment free trial, cancel any time



Authenticated Received Chain (ARC)

ARC is defined in RFC 8

<https://blog.icewolf.ch/>

Erlaubt es zwischenges
signieren

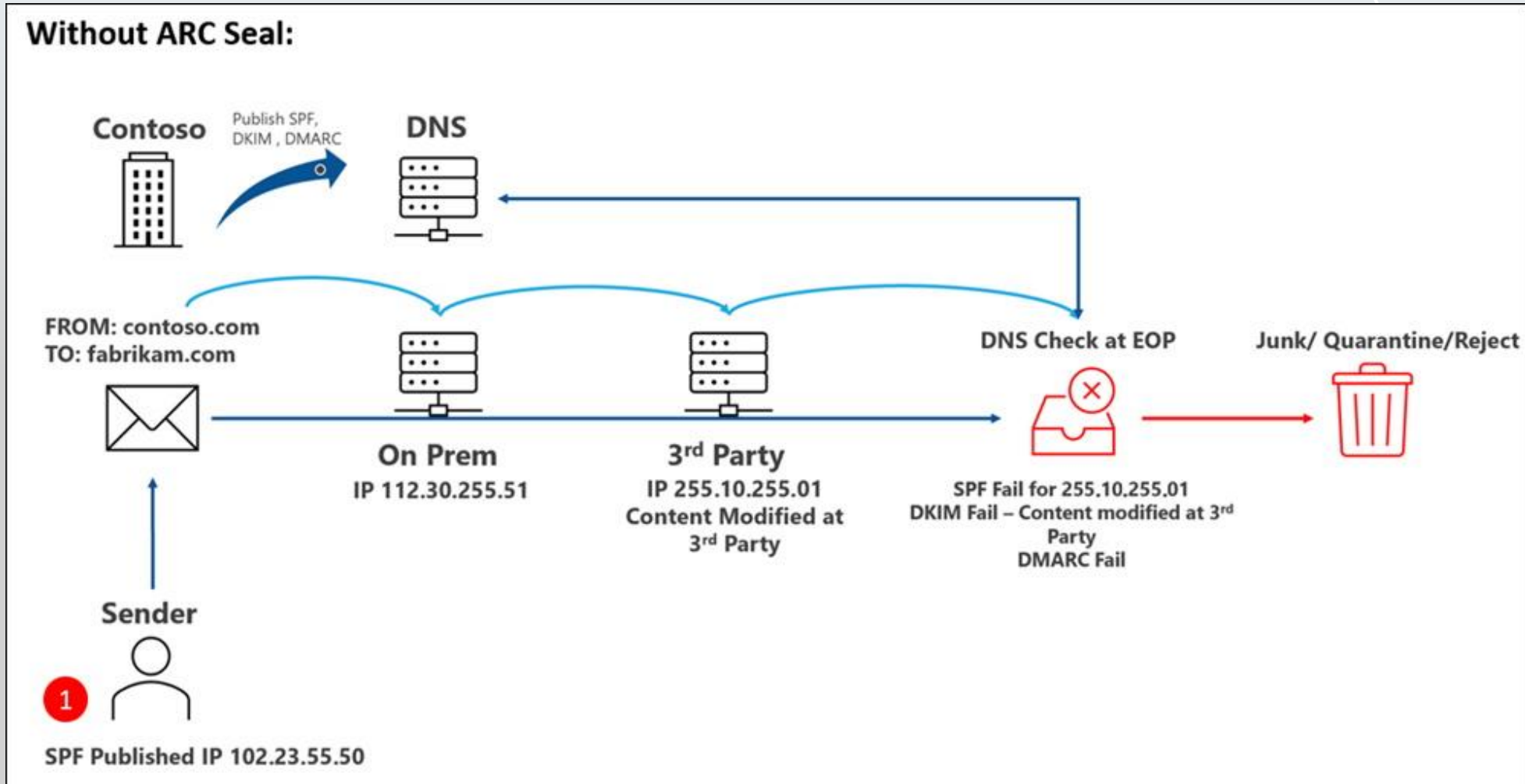
ARC defines three new m

- **ARC-Authentication-**
the SPF, DKIM, and DM
- **ARC-Seal** (abbreviate
ARC-Seal headers, an
- **ARC-Message-Signa**
signature of the entire

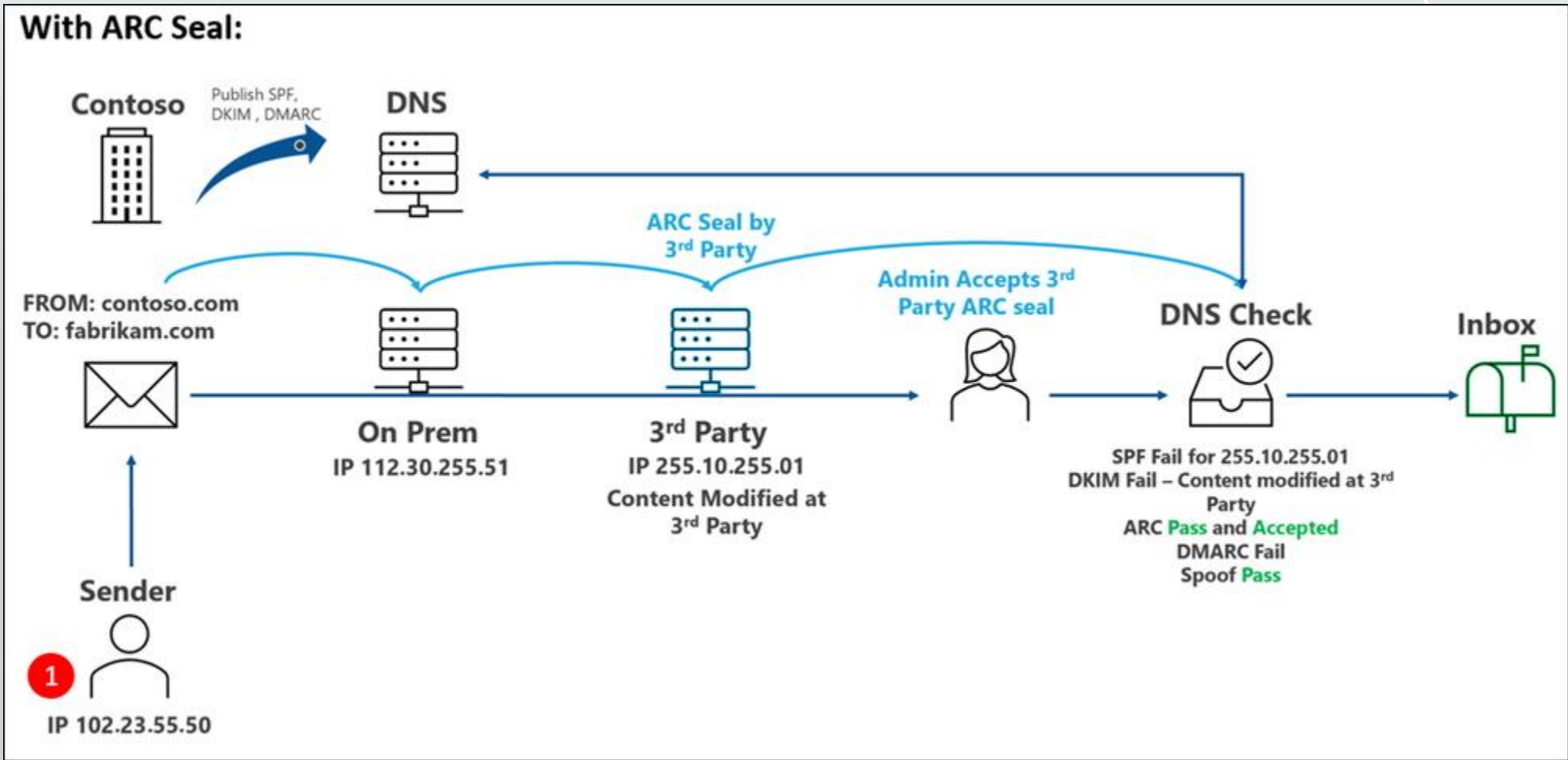
Other headers		
#1	Header	Value
1	Delivered-To	andres.bohren@gmail.com
2	X-Google-Smtp-Source	AMrXdXukHjnfGbeOF7Eb7ik25M5wlW2X4ULdmss9wtTaUCHNfUHTTLdHAAsKb7QRhbiasocIF
3	X-Received	by 2002:a17:906:6d47:b0:7c0:c312:acaa with SMTP id a7-20020a1709066d4700b007c0c312acaa/r25875119ejt.49.1672390484405; Fri, 30 Dec 2022 00:54:44 -0800 (PST)
4	ARC-Seal	i=2; a=rsa-sha256; t=1672390484; cv=pass; d=google.com; s=arc-20160816; b=qW165H4dhVBWddayWUxmJOT/Y8GGXPfAfcqTuqeWxncoa8mspwruke+VfAhyAK3s GF434Lmt+77HNILSA Fvra6KcUQ+szCDwzIOOrZgoimwlyCg3vWQisGejew14Ygqggpx WjUKP2vWb6PQdzTWNV1BYRaPHSD26OUJCKy/hPlrFick4mp4Vl0quTWsQhWYmnyzM09m 0Ozljp0AcAEsbSIGY8c6QlsgMjlf7Al gzlodmu8dkDustyETGMQDRn/i/4cCVWbhNbkI 3p3DHR2YRru1soUHelOzTHY/JsMoDTs/tq7/pYqF2FEKjZQUAg80yhQCIfcC3g4yQLZi 35+A==
5	ARC-Message-Signature	i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=mime-version:content-language:accept-language:message-id:date:thread-index:thread-topic:subject:to:from:dkim-signature; bh=NqzZ6VGKOkd04/AdVXHpkjKIQMi+mBopavISJHC/Jgk=: b=OkOvL9LU2NumyyMRqf8HrWMxVwYBEdUfNFUS0uy1TePWM2K7EmKgTCIfxOwf5qwZ 19T92vefV9L8psHK7KaqS 1c+IU1gOS+nfWXgYI92wuuc/fHZ4DWL8u/KX5Y9DTzTn7T g0OTKj64wh457oDqnFksx4r9FFKXc3zbkQ5zVU6YA3aNsPTRyR027ou70triQ9TYXKG wNFcW2cJ78ka81JnLcXQggiPr5vg2RkLdM4sph ERSOTOiNUyHsdNf/byq9PNkiBMVNio ZBFPzSYWmBimEU1s1r4RSBrjof7PO2Z9Zyusf60z5Gv5q8/hYssAZwa5qZEuhyLQIfc a2xg==
6	ARC-Authentication-Results	i=2; mx.google.com; dkim=pass header.i=@icewolf.ch header.s=selector1 header.b=Y3vR3OCL; arc=pass (i=1 spf=pass spfdomain=icewolf.ch dkim=pass dkdomain=icewolf.ch dmarc=pass fromdomain=icewolf.ch); spf=pass (google.com: domain of a.bohren@icewolf.ch designates 40.107.23.96 as permitted sender) smtp.mailfrom=A.Bohren@icewolf.ch; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=icewolf.ch
7	Return-Path	<A.Bohren@icewolf.ch>
8	Received-SPF	pass (google.com: domain of a.bohren@icewolf.ch designates 40.107.23.96 as permitted sender) client-ip=40.107.23.96;
9	Authentication-Results	mx.google.com; dkim=pass header.i=@icewolf.ch header.s=selector1 header.b=Y3vR3OCL; arc=pass (i=1 spf=pass spfdomain=icewolf.ch dkim=pass dkdomain=icewolf.ch dmarc=pass fromdomain=icewolf.ch); spf=pass (google.com: domain of a.bohren@icewolf.ch designates 40.107.23.96 as permitted sender) smtp.mailfrom=A.Bohren@icewolf.ch; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=icewolf.ch
10	ARC-Seal	i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none; b=JOX+YI2r7QzPVRHpQft2gGSgmEb4W15nXvny5MgEbdOZ6hE3vVjnG6Kysak/IligCaYagxk917XbUgD/ymEbHYW1zSMIIV8 5F6nUBkk5MAv6KDUI8XjWjAtasM006DRxiTq2NtkOUCv4RFzQDf5+ +2hCkU9vFNidO4mEvKdH+JyK5tZQX13vg3eZXB7qahdidkOrKinLtbhTs7+ZtxglLW9lgtWnoWV/2vGvJ9jk08q/Zgglye/Rf4B3 FYwbCbncAbtcPv9m6dkQol1CXHobAHI4b85p8/MKFhV7UYO+DCYHJDcn13ySMkOkhPE6pSyct9fL8i0dAp5XZHQ==
11	ARC-Message-Signature	i=1; 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=NqzZ6VGKOkd04/AdVXHpkjKIQMi+mBopavISJHC/Jgk=: b=kl4AmpBuvYPREUEVffQQ+IWnu V7X5e61rN39xv0NKb0pgXjVDwvKCDsv+3QtwP/YdGoDqZT1mEaXwXgI9eUlcHn/xAyVLIEFV3KecOJroQkkU+6HwwzhVESfQZBvLd3/dqGwiaTVwMHFL2+V91rqB0tWe41mMee7B9udpkCwl+D9 JN+FdAHdUaV5I2UzqNTkGqkY/S+AyvzErSLwxbg20IOfxH8GkF1ZgUcH7L/6CTXqYCiayC7WfReZ6w1761e2LIX10lofpaXco3c12x7m7nLuE1sD1nxWVrK3kjMYDwh7iRfc6ZtmrSONvYaPmh0U1o/ XEx+ZvkuaNKiHug==
12	ARC-Authentication-Results	i=1; mx.microsoft.com 1; spf=pass smtp.mailfrom=icewolf.ch; dmarc=pass action=none header.from=icewolf.ch; dkim=pass header.d=icewolf.ch; arc=none
13	DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=icewolf.ch; s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version:X-MS-Exchange-SenderADCheck; bh=NqzZ6VGKOkd04/AdV XHpkjKIQMi+mBopavISJHC/Jgk=: b=Y3vR3OCLNv256J3d0C6JlPifcRfulqGx1aI3J19Ckzh3sv5Obkwy5JXF7FVUKoAsDzZBKBOaAawZGegMxlvZfCpHwX42iL3ehk/IM/E6zISJHcVl4AVh5DE4w/b YLAdoRvKhZh3cWle28HEOXU6Yu2aVcnaBMjwklhz+8NsXSRkCmiz6y056dy4WmIWzqlinMcy7RXNDaEqV4OC/mOuzsYTU7roiOClzekFRkRP/o/Etjv11fNwaRwsYmZlXkmrTgzA6Nq84yGSZk zWvY94E+3/qC42gmqoMy1KI9uMolBX1+HjKx2M5Fidx8YofO0uHwCz3us3/NnRg==
14	Thread-Topic	Test ARC Seal



Authenticated Received Chain (ARC)

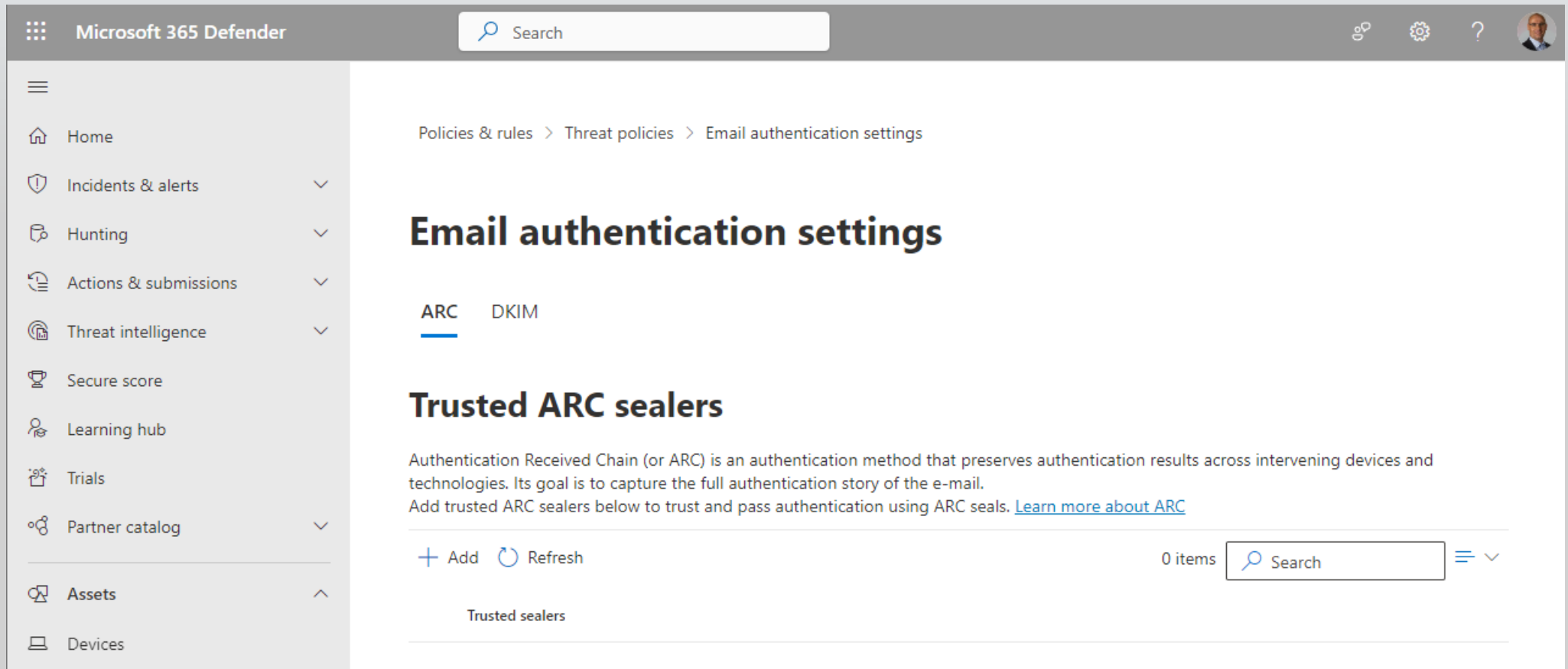


Authenticated Received Chain (ARC)



Authentication Received Chain (or ARC)

Exchange Online fügt eine ARC Signatur bei eingehenden Nachrichten hinzu
Und man kann weitere “Trusted ARC sealers” erlauben



The screenshot displays the Microsoft 365 Defender web interface. The left sidebar contains navigation links: Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, and Devices. The main content area is titled 'Email authentication settings' and includes tabs for 'ARC' (selected) and 'DKIM'. Below the tabs, the 'Trusted ARC sealers' section provides a description of ARC and a link to 'Learn more about ARC'. At the bottom, there are buttons for '+ Add' and 'Refresh', a search bar with '0 items', and a list of 'Trusted sealers'.

Microsoft 365 Defender

Search

Policies & rules > Threat policies > Email authentication settings

Email authentication settings

ARC DKIM

Trusted ARC sealers

Authentication Received Chain (or ARC) is an authentication method that preserves authentication results across intervening devices and technologies. Its goal is to capture the full authentication story of the e-mail.
Add trusted ARC sealers below to trust and pass authentication using ARC seals. [Learn more about ARC](#)

+ Add Refresh

0 items Search

Trusted sealers



BIMI



Brand Indicators for Message Identification (BIMI)

Anforderungen

- Die Domain ist mit SPF/DKIM/DMARC geschützt.
- DMARC muss erzwungen werden: Quarantäne oder Ablehnung für Domäne (p=) und Subdomäne (sp0)
- Die SVG-Datei sollte ein Quadrat sein, aber auch gut in einen Kreis passen (siehe Screenshot oben)
- SVG-Datei muss Tiny 1.2-Spezifikation entsprechen
- SVG-Datei muss kleiner als 32 KB sein
- SVG-Datei muss im Internet veröffentlicht werden
- BIMI-DNS-Eintrag (TXT-Eintrag) muss veröffentlicht werden
- Wenn Ihr Logo markenrechtlich geschützt ist, können Sie Verified Mark Certificates (VMC) kaufen
- VMC ist ein Zertifikat, das im BIMI-DNS-Eintrag veröffentlicht wird

<https://blog.icewolf.ch/archive/2022/01/20/how-does-brand-indicators-for-message-identification-bimi-work/>



BIMI DNS Record

default._bimi.domain.tld TXT

Resolve-DnsName -name default._bimi.meetup.com -Type TXT

v=BIMI1; l=https://amplify.valimail.com/bimi/meetup/gmwfvvsHEXej-entrust_3824239.svg;
a=https://amplify.valimail.com/bimi/meetup/gmwfvvsHEXej-entrust_3824239.pem


```
Windows PowerShell
PS C:\> Resolve-DnsName -name default._bimi.meetup.com -Type TXT

Name                                Type  TTL  Section  Strings
----                                -
default._bimi.meetup.com            TXT   1799  Answer   {v=BIMI1; l=https://amplify.valimail.com/bimi/meetup/gmwfvvsHEXej-entrust_3824239.svg; a=https://amplify.valimail.com/bimi/meetup/gmwfvvsHEXej-entrust_3824239.pem}
```



BIMI Zertifikat

Entrust
DigiCert

**ENTRUST**
SECURING A WORLD IN MOTION

digicert

1.877.438.8776

Already a DigiCert customer?

Sign in

Step 1

Configure your certificate

Step 2

Add account and organization details

Step 3

Check out

Order summary

Verified Mark Certificate

1-year plan

Price details

Base price

\$1,499.00 USD

Primary URL x 1 year

Subtotal

\$1,499.00 USD

Total

\$1,499.00 USD

Applicable tax not included

Your DigiCert certificate

Verified Mark Certificate

Certificate validity

1 year

- Get better visibility and control over the messages sent and received by your domain.
- Increase user trust, expand your brand visibility, and improve customer experience.
- Manage your certificate and account in the DigiCert CertCentral management console.



Certification Authority Authorization (CAA)

Existiert seit 2019 rfc8659

Definiert mit einem CAA DNS Record, welche Zertifizierungsstellen Zertifikate für diese Domain ausstellen darf.

Im März 2017 entschied das [CA/Browser Forum](#), dass CAs diesen Record prüfen müssen

https://de.wikipedia.org/wiki/DNS_Certification_Authority_Authorization

example.com. IN CAA 0 issue "ca.example.net"

example.com. IN CAA 0 issue ";"

example.com. IN CAA 0 issuewild ";"

example.com. IN CAA 0 iodef "mailto:security@example.com"

example.com. IN CAA 0 iodef "https://security.example.com/"

```
Windows PowerShell
PS C:\> $domain = "iis.se"
PS C:\> $json = Invoke-RestMethod -URI "https://dns.google/resolve?name=$Domain&type=CAA"
PS C:\> $json.Answer.data
0 issue "digicert.com"
0 issue "letsencrypt.org"
0 issue "sectigo.com"
0 issue "amazon.com"
PS C:\>
```



Null MX / No Service MX

<https://blog.icewolf.ch/archive/2017/12/30/use-rfc-7505-null-mx-to-disable-mail-for-domain/>

Existiert seit 2015 [rfc7505](#)

Ein Mechanismus um anzuzeigen, dass die Domain kein Email akzeptiert

Wird leider weder von Exchange noch Exchange Online unterstützt.

Am Besten in Kombination mit einem leeren SPF

IN MX 0 .

IN TXT "v=spf1 -all"

```
root@ns1:/var/named
[root@ns1 named]# cat irgendwoiminternet.ch
$ORIGIN irgendwoiminternet.ch.
$TTL 3H
@      IN SOA  ns1.icewolf.ch.  hostmaster.icewolf.ch. (
                                2017123001      ; serial
                                12H               ; refresh
                                1H               ; retry
                                1W               ; expire
                                3H )             ; minimum
                                IN      NS      ns1.icewolf.ch.
                                IN      NS      ns2.icewolf.ch.
                                IN      MX      0 .
                                IN      TXT      "v=spf1 -all"

@      IN      A      80.238.215.86
www    IN      A      80.238.215.86
[root@ns1 named]#
```



Get-Mailprotection

PSGallery

<https://www.powershellgallery.com/packages/Get-Mailprotection>

Dokumentation

https://github.com/BohrenAn/GitHub_PowerShellScripts/blob/main/Get-Mailprotection.ps1

Install-Script Get-Mailprotection

Get-Mailprotection -Domain domain.tld

Get-Mailprotection -Domain domain.tld -SMTPConnect

\$ReturnObject = Get-Mailprotection -Domain domain.tld

```
Windows PowerShell
PS C:\> C:\GIT_WorkingDir\GitHub_PowerShellScripts\Mailprotection\Get-Mailprotection.ps1 -Domain icewolf.ch
Check: DNS Zone Signed
Check: MX Record
Check: SMTPConnect
Check: StartTLS
Connect icewolf-ch.mail.protection.outlook.com 25
220 ZR0CHE01FT016.mail.protection.outlook.com Microsoft ESMTPL MAIL Service ready at Wed, 18 Oct 2023 08:58:21 +0000
EHLO ICE11.corp.icewolf.ch
250-ZR0CHE01FT016.mail.protection.outlook.com Hello [95.143.60.18]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250-SMTPUTF8
STARTTLS
220 2.0.0 SMTP server ready
Certificate Details:
Issuer: CN=DigiCert Cloud Services CA-1, O=DigiCert Inc, C=US
Subject: CN=mail.protection.outlook.com, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
ValidFrom: 8/1/2023 2:00:00 AM
ValidTo: 8/1/2024 1:59:59 AM
SerialNumber: 0FB8F2E93000790619DE073442599798
Thumbprint: 407BA218BA6F35D658873C36F0283E46775CB95
Check: DANE
Check: StartTLS Support
Check: SPF
Check: DKIM
Check: DMARC
Check: BIMI
Check: MTA-STX
Check: TLS-RPT
Check: Autodiscover
Check: Lyncdiscover
Check: Skype48 / Teams Federation
Check: M365 Tenant (OpenIDConnect)
Check: security.txt
An exception was caught: The remote server returned an error: (404) Not Found.
SUMMARY: icewolf.ch
Nameserver: ns1-03.azure-dns.com ns2-03.azure-dns.net ns3-03.azure-dns.org ns4-03.azure-dns.info
Zone DNS Signed: False
Certification Authority Authorization (CAA):
MXCount: 1
MXRecord: icewolf-ch.mail.protection.outlook.com
MXIP: 104.47.22.10 104.47.22.74
MXReverseLookup: mail-gv0che010010.inbound.protection.outlook.com mail-zr0che010074.inbound.protection.outlook.com
STARTTLS: 0
STARTTLS Support: None
SMTPBanner: 220 ZR0CHE01FT016.mail.protection.outlook.com Microsoft ESMTPL MAIL Service ready at Wed, 18 Oct 2023 08:58:21 +0000
SMTPCertIssuer: CN=DigiCert Cloud Services CA-1, O=DigiCert Inc, C=US
SPF: True
SPFRecord: v=spf1 ip4:95.143.60.16/29 include:spf.protection.outlook.com -all
DKIM: True
DKIM Support: True
DKIM Record: selector1-icewolf-ch._domainkey.icewolfch.onmicrosoft.com selector2-icewolf-ch._domainkey.icewolfch.onmicrosoft.com
DMARC: True
DMARCRecord: v=DMARC1; p=reject; sp=reject; rua=mailto:skmtvc6p@ag.eu.dmarcadvisor.com,mailto:44aa291caf@rua.easymarc.eu; ruf=mailto:postmaster@icewolf.ch
DANECount: 0
DANESupport: None
DANERecord:
BIMI: True
BIMI Record: v=BIMI1; l=https://www.icewolf.ch/images/icewolf_tiny.svg; a=;
MTA-STX: False
MTA-STX-Web:
TLS-RPT:
Autodiscover: autodiscover.outlook.com
Lyncdiscover: webdir.online.lync.com
SkypeFederation: sipfed.online.lync.com
M365: True
TenantID: 46bbad84-29f0-4e03-8d34-f6841a5071ad
SecurityTXT: False
PS C:\>
```



Office 365 Inbound Report

<https://admin.exchange.microsoft.com/#/reports/inboundconnectordetails>

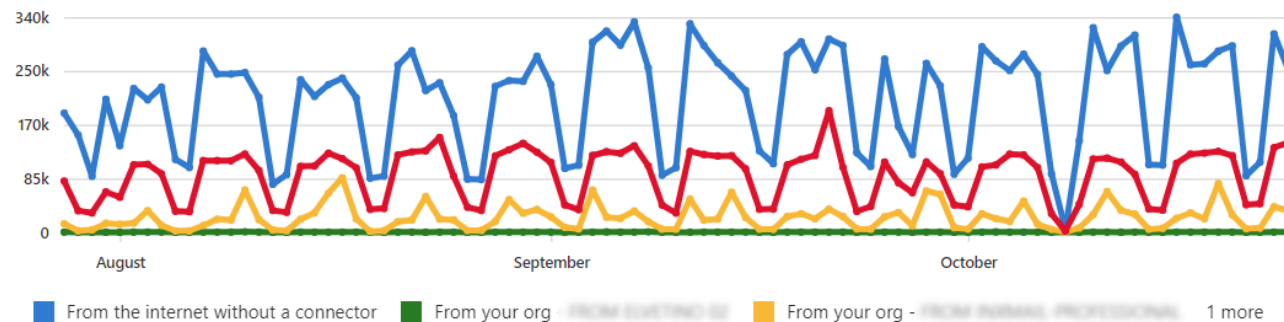
Bei einem grossen Kunden noch ca ~1% NoTLS

Berichte > E-Mail-Fluss > Bericht für eingehende Nachrichten

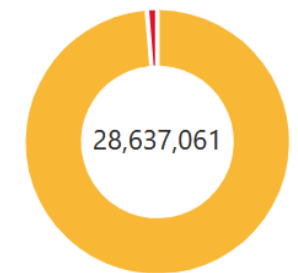
Bericht für eingehende Nachrichten

Verwenden Sie diesen Bericht zum Überwachen des Nachrichtenvolumens und der TLS-Verschlüsselung für jeden Connector. Der E-Mail-Verkehr zwischen Ihrer Microsoft Cloud-Organisation, Ihren lokalen E-Mail-Servern und Partnerservern ist häufig viel wichtiger, und Sie möchten möglicherweise zusätzliche Sicherheitsmaßnahmen für diese Verbindungen anwenden. Inbound umfasst Nachrichten aus dem Internet und von lokalen Organisationen an Office 365. [Weitere Informationen](#)

Nachrichtenvolumen



Von TLS verwendete Nachrichten



2 more



Office 365 Outbound Security Report

<https://admin.exchange.microsoft.com/#/reports/outboundsecurity>

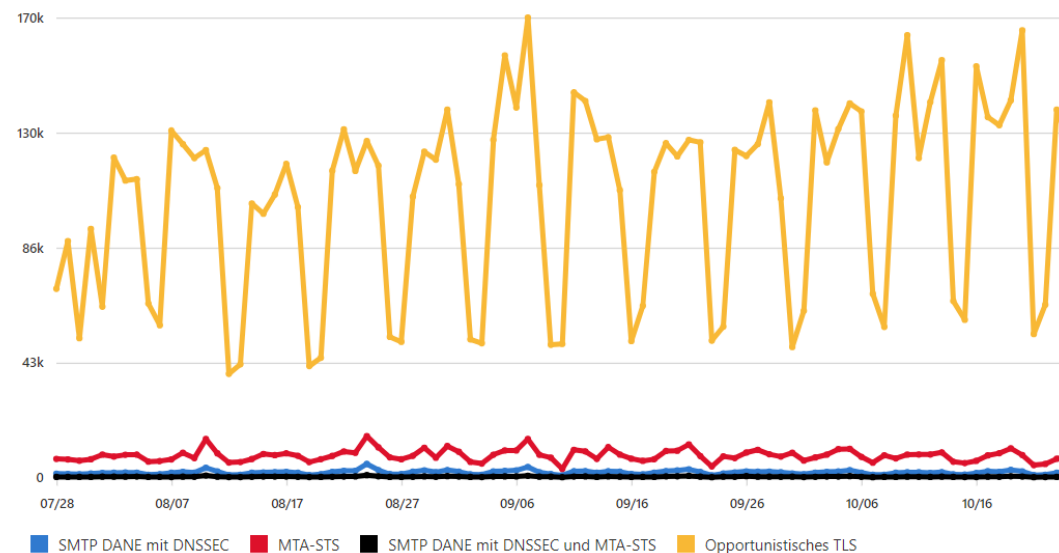
DANE 181'864 ~1.7%
MTA-STS 752'162 ~7.2%
DANE+MTA-STS 36'739 ~0.35%
TLS 9'461'262 ~90%

Berichte > E-Mail-Fluss > Bericht „Die Sicherheit einer ausgehenden Nachricht bei der Übertragung“

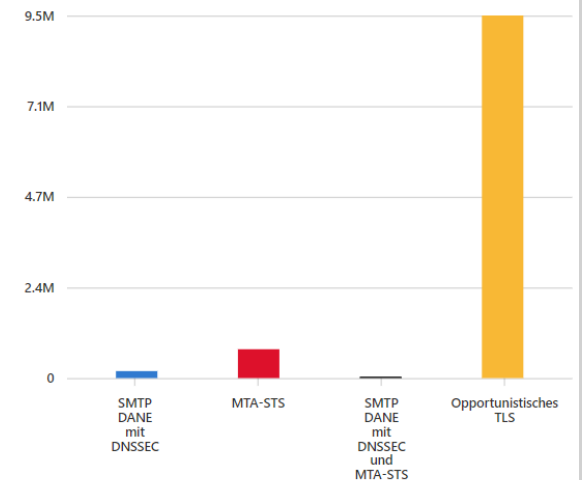
Blockierte Nachrichten Gesicherte Nachrichten

Bericht „Die Sicherheit einer ausgehenden Nachricht bei der Übertragung“

Das folgende Diagramm zeigt die Anzahl der von Ihren Benutzern gesendeten E-Mails, die durch einen bestimmten Sicherheitsmechanismus gesichert wurden: SMTP DANE mit DNSSEC, MTA-STS oder (Standardeinstellung von Exchange Online) opportunistisches TLS. [Weitere Informationen](#)



Zusammenfassung von „2023/07/28-2023/10/25“



Swiss Domain Security Report Q3 2022

Letztes Jahr habe ich alle .ch Domains abgefragt und damit eine Auswertung über eine ganze TLD gemacht

<https://blog.icewolf.ch/archive/2023/06/07/swiss-domain-security-report-q3-2022/>

40% der Domains haben DNSSEC

90% der Domains haben MX

87% der MX unterstützen STARTTLS

52% der Mail Domains haben SPF

- nur die Hälfte davon -all

5.7% der Mail Domains haben DKIM

- schwierig auszuwerten! Ungenau!

7.8% der Mail Domains haben DMARC

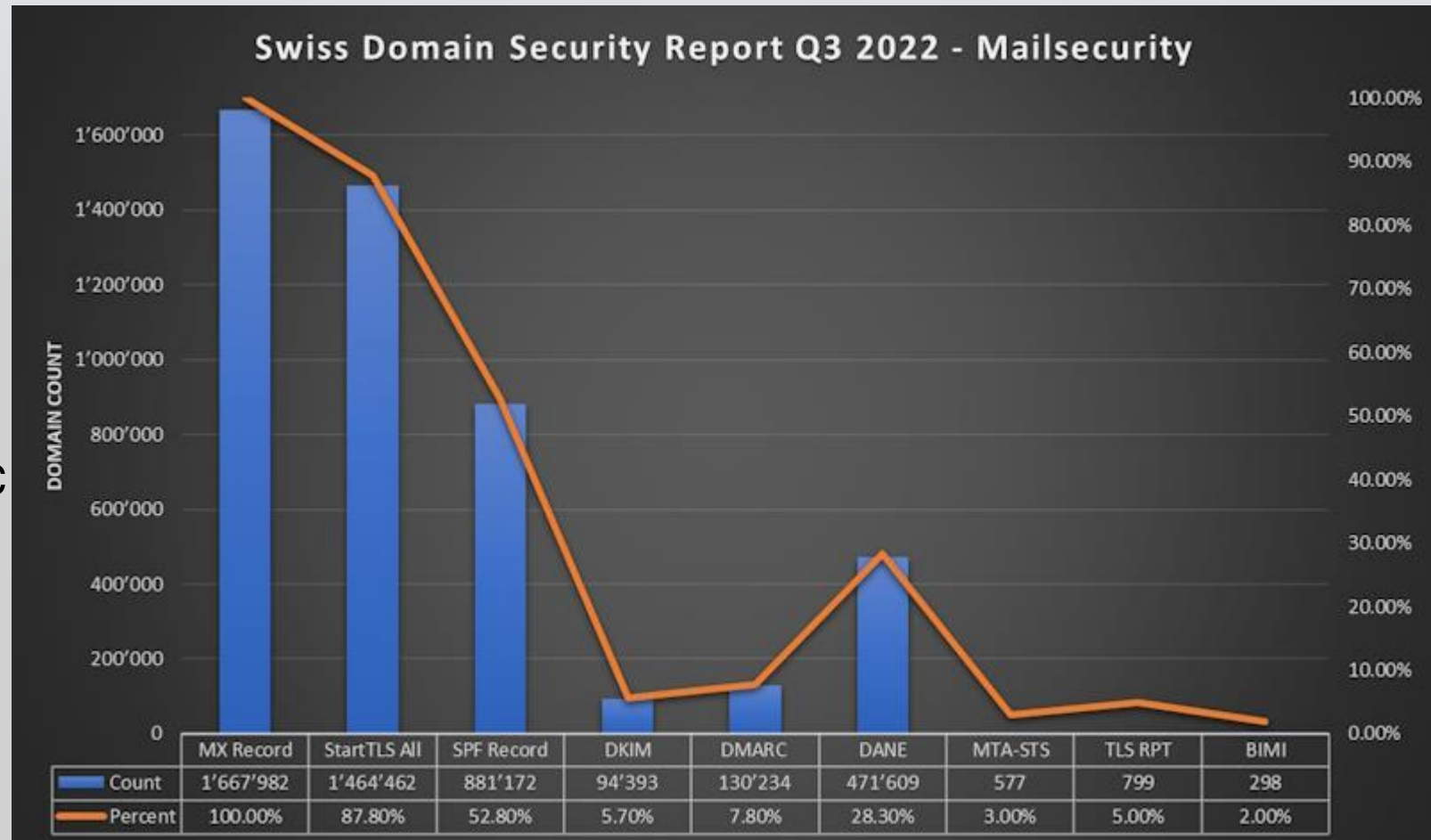
- 5.3% p=none / 1.8% p=reject

28% der Mail Domains haben DANE

3% der Mail Domains haben MTA-STS

2% der Mail Domains haben BIMI

1% der Domains haben CAA



Brain exploded?

