

# Swiss Domain Security Report Q4 2023

6th cloud8 virtual  
summit 12.01.2024



# Sponsors



# About me

## Andres Bohren



Cloud Engineer / Architect at isolutions since 2020

Over 25 Years in IT - Messaging / Communication / Security  
(Windows Server / Active Directory / MS SQL / Exchange / Lync /  
Skype4B / M365 / Azure / PowerShell / MSGraph)

Hobbys: Traveling / Diving / Bike / Dance



<https://blog.icewolf.ch>



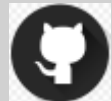
<https://twitter.com/andresbohren> / @andresbohren



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



<https://bsky.app/profile/andresbohren.bsky.social>



<https://github.com/BohrenAn>



<https://isolutions.ch>



# Agenda

- My Journey
- Domain Results
  - Overview
  - DNSSEC / NS / IDN
  - Certification Authority Authorization (CAA)
  - SecurityTXT
  - M365 Tenant
- Mailsecurity
  - MX / Null MX
  - STARTTLS / Banner
  - SPF / DKIM / DMARC
  - DANE
  - MTA-STS / TLSRPT
  - Brand Indicators for Message Identification (BIMI)
- Recap and Improvements



# Journey





# Journey

## 2015

Dec 2014 ~2 Mio .ch Domains

chilkat.spider Webcrawler collected 100'000 Domains in 1 Month

Checked MX / STARTTLS / SPF / DKIM / DMARC

Results

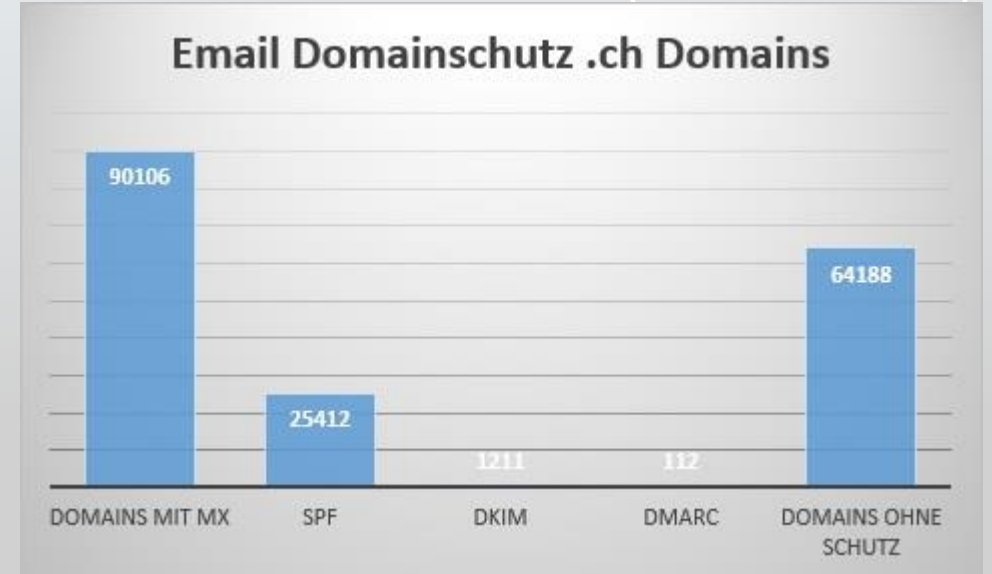
- 90% used MX
- 25% used SPF
- 1% used DKIM
- DMARC was barely used (new in 2015)

## 2022

- .ch TLD Open Data – Normalize Data / Import to SQL Database
- Get-Mailprotection published to PowerShell Gallery
- Swiss Domain Security Report Q3 2022

## 2023

- Swiss Domain Security Report Q4 2023



# Get-Mailprotection

The Script will extract Information for a Domain like:

- DNS Zone Signed (DNSSEC)
- CAA (Certification Authority Authorization)
- MX (MailExchanger)
- STARTTLS
- TLS Certificate Issuer
- SMTP Banner
- SPF (Sender Policy Framework)
- DKIM (DomainKeys Identified Mail)
- DMARC (Domain-based Message Authentication, Reporting and Conformance)
- DANE (DNS-based Authentication of Named Entities)
- BIMi (Brand Indicators for Message Identification)
- MTA-STS (SMTP MTA Strict Transport Security)
- MTA-STS Web (<https://mta-sts.domain.tld/.well-known/mta-sts.txt>)
- TLS-RPT (TLS Reporting)
- Autodiscover
- Lyncdiscover
- Skype4B / Teams Federation
- M365 Tenant
- SecurityTXT

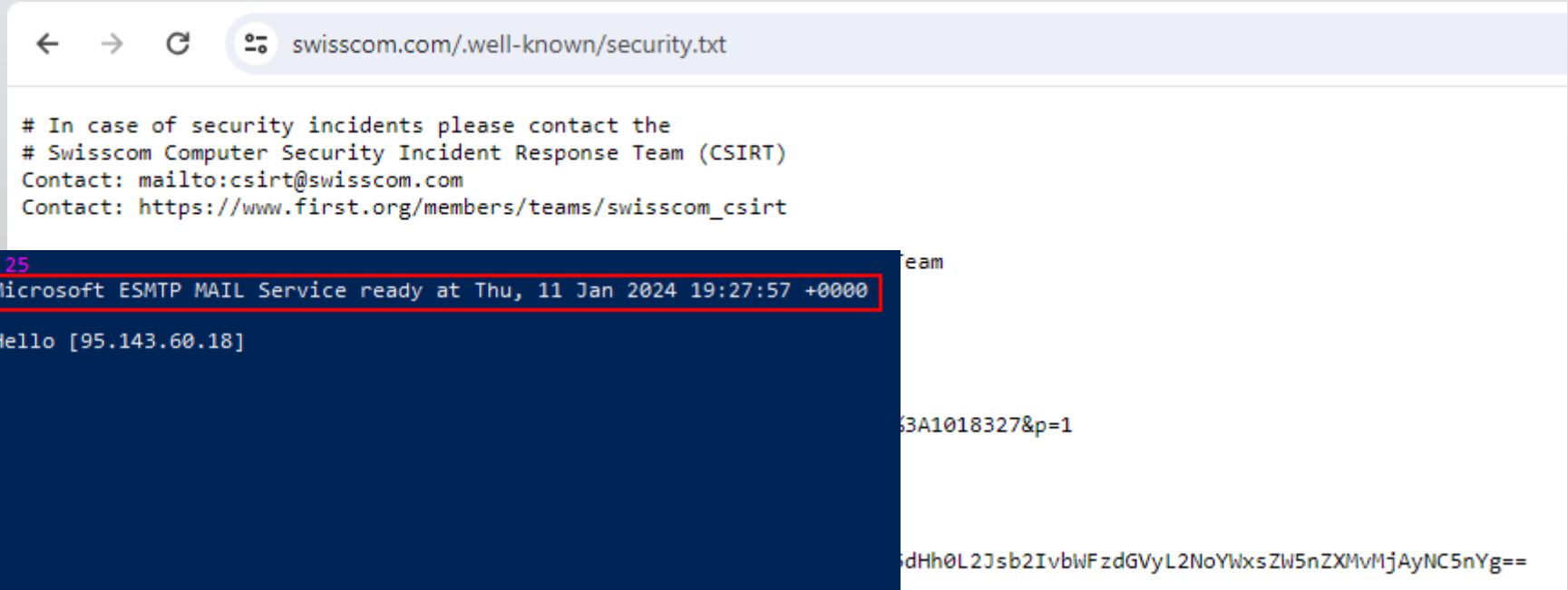


```
PS C:\> Get-Mailprotection -Domain icewolf.ch
Check: DNS Zone Signed
Check: CAA
Check: MX
Check: SMTPConnect
Check: StartTLS
Connect icewolf.ch.mail.protection.outlook.com 25
220 ZR0CHE01FT008.mail.protection.outlook.com Microsoft ESMTp MAIL Service ready at Thu, 11 Jan 2024 19:27:57 +0000
EHLO ICE11.corp.icewolf.ch
250-ZR0CHE01FT008.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: 12/14/2023 1:00:00 AM
ValidTo: 12/14/2024 12:59:59 AM
SerialNumber: 04BAD4FA78A66027A4BA6B70AC9B3A75
Thumbprint: 04C3E84F5B20825BF6FD5F0BE2EECA1D0A8C50BD
Check: DANE
Check: StartTLS Support
Check: SPF
Check: DKIM
Check: DMARC
Check: BIMi
Check: MTA-STS
Check: TLS-RPT
Check: Autodiscover
Check: Lyncdiscover
Check: Skype4B / 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): 0 issue "letsencrypt.org" 0 issue "digicert.com"
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: 1
STARTTLS Support: All
SMTPBanner: 220 ZR0CHE01FT008.mail.protection.outlook.com Microsoft ESMTp MAIL Service ready at Thu, 11 Jan 2024 19:27:57 +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.easydmarc.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-STS: True
MTA-STS-Web: version: STSV1
mode: enforce
mx: *.mail.protection.outlook.com
mx: mail.icewolf.ch
max_age: 604800
TLS-RPT: v=TLSRPTv1;rua=mailto:aef5fe2f58abfcd2a0a4be7d115e62-d@tlsrpt.report-uri.com
Autodiscover: autodiscover.outlook.com
Lyncdiscover: webdir.online.lync.com
SkypeFederation: sipfed.online.lync.com
M365: True
TenantID: 46bbad84-29f0-4e03-8d34-f6841a5071ad
SecurityTXT: True
PS C:\>
```

# Changes in 2023

I've added some new Properties to [Get-Mailprotection](#) and fixed several Bugs.

- SecurityTXT
- SMTPBanner
- SMTP Certificate Issuer
- Addet –Silent Parameter
- Better Return Object



```
Connect icewolf-ch.mail.protection.outlook.com 25
220 ZR0CHE01FT008.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Thu, 11 Jan 2024 19:27:57 +0000
EHLO ICE11.corp.icewolf.ch
250-ZR0CHE01FT008.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: 12/14/2023 1:00:00 AM
ValidTo: 12/14/2024 12:59:59 AM
SerialNumber: 04BAD4FA7BA66927A4BA6B70AC9B3A75
Thumbprint: 04C3E84F5B20825BF6FD5F0BE2EECA1D0A8C50BD
```





# Timeline



**September**  
Export Zone Data  
Import in SQL

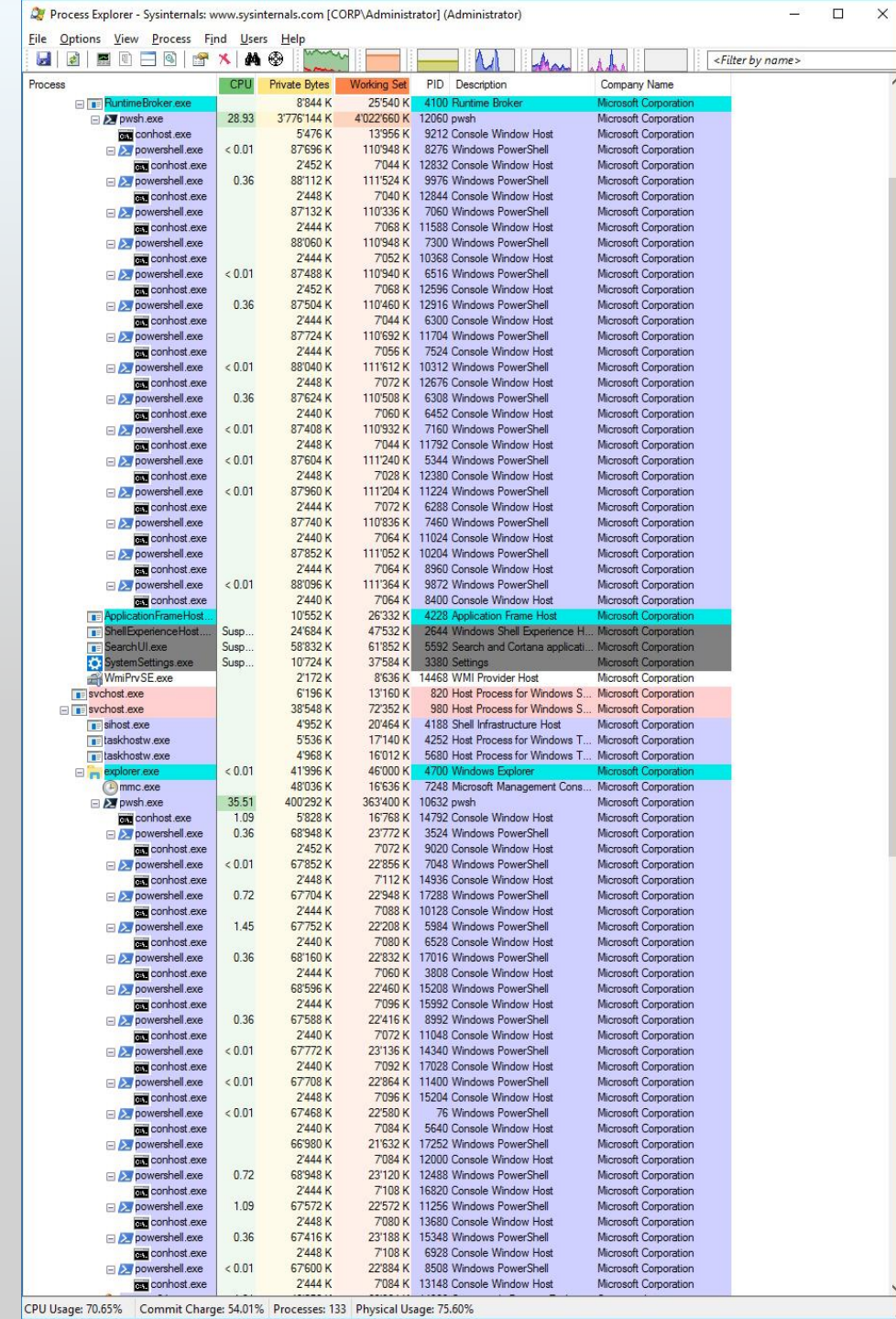
**October/November**  
Running Scripts  
to gather data



# Journey

- Used Get-Mailprotection Script to Analyze all the .ch Domains
- Turns out it was way more stable than last year
- But still took about 8 Weeks to gather data (4vCPU's / 16 GB RAM)
- PowerShell 7 with Scriptblock and -parallel Parameter
- Two PowerShell Scripts running each with 10-15 Childprocesses
  - from A --> Z
  - from Z --> A

Note: Did you notice that the Childprocesses are PowerShell 5.1?



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
RuntimeBroker.exe		8'844 K	25'540 K	4100	Runtime Broker	Microsoft Corporation
pwsh.exe	28.93	3'776'144 K	4'022'660 K	12060	pwsh	Microsoft Corporation
conhost.exe		5'476 K	13'956 K	9212	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	8'7696 K	110'948 K	8276	Windows PowerShell	Microsoft Corporation
conhost.exe		2'452 K	7'044 K	12832	Console Window Host	Microsoft Corporation
powershell.exe	0.36	88'112 K	111'524 K	9976	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'040 K	12844	Console Window Host	Microsoft Corporation
powershell.exe		87'132 K	110'336 K	7060	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'068 K	11588	Console Window Host	Microsoft Corporation
powershell.exe		88'060 K	110'948 K	7300	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'052 K	10368	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	87'488 K	110'940 K	6516	Windows PowerShell	Microsoft Corporation
conhost.exe		2'452 K	7'068 K	12596	Console Window Host	Microsoft Corporation
powershell.exe	0.36	87'504 K	110'460 K	12916	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'044 K	6300	Console Window Host	Microsoft Corporation
powershell.exe		87'724 K	110'692 K	11704	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'056 K	7524	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	88'040 K	111'612 K	10312	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'072 K	12676	Console Window Host	Microsoft Corporation
powershell.exe	0.36	87'624 K	110'508 K	6308	Windows PowerShell	Microsoft Corporation
conhost.exe		2'440 K	7'060 K	6452	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	87'408 K	110'932 K	7160	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'044 K	11792	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	87'604 K	111'240 K	5344	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'028 K	12380	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	87'960 K	111'204 K	11224	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'072 K	6288	Console Window Host	Microsoft Corporation
powershell.exe		87'740 K	110'836 K	7460	Windows PowerShell	Microsoft Corporation
conhost.exe		2'440 K	7'064 K	11024	Console Window Host	Microsoft Corporation
powershell.exe		87'852 K	111'052 K	10204	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'064 K	8960	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	88'096 K	111'364 K	9872	Windows PowerShell	Microsoft Corporation
conhost.exe		2'440 K	7'064 K	8400	Console Window Host	Microsoft Corporation
ApplicationFrameHost.exe		10'552 K	26'332 K	4228	Application Frame Host	Microsoft Corporation
ShellExperienceHost.exe	Susp...	24'684 K	47'532 K	2644	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	58'832 K	61'852 K	5552	Search and Cortana applica...	Microsoft Corporation
SystemSettings.exe	Susp...	10'724 K	37'584 K	3380	Settings	Microsoft Corporation
WmiPrvSE.exe		2'172 K	8'636 K	14468	WMI Provider Host	Microsoft Corporation
svchost.exe		6'196 K	13'160 K	820	Host Process for Windows S...	Microsoft Corporation
svchost.exe		38'548 K	72'352 K	980	Host Process for Windows S...	Microsoft Corporation
sihost.exe		4'952 K	20'464 K	4188	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		5'536 K	17'140 K	4252	Host Process for Windows T...	Microsoft Corporation
taskhostw.exe		4'968 K	16'012 K	5680	Host Process for Windows T...	Microsoft Corporation
explorer.exe	< 0.01	41'996 K	46'000 K	4700	Windows Explorer	Microsoft Corporation
mmc.exe		48'036 K	16'636 K	7248	Microsoft Management Cons...	Microsoft Corporation
pwsh.exe	35.51	400'292 K	363'400 K	10632	pwsh	Microsoft Corporation
conhost.exe	1.09	5'828 K	16'768 K	14792	Console Window Host	Microsoft Corporation
powershell.exe	0.36	68'948 K	23'772 K	3524	Windows PowerShell	Microsoft Corporation
conhost.exe		2'452 K	7'072 K	9020	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	67'852 K	22'856 K	7048	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'112 K	14936	Console Window Host	Microsoft Corporation
powershell.exe	0.72	67'704 K	22'948 K	17288	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'088 K	10128	Console Window Host	Microsoft Corporation
powershell.exe	1.45	67'752 K	22'208 K	5984	Windows PowerShell	Microsoft Corporation
conhost.exe		2'440 K	7'080 K	6528	Console Window Host	Microsoft Corporation
powershell.exe	0.36	68'160 K	22'832 K	17016	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'060 K	3808	Console Window Host	Microsoft Corporation
powershell.exe		68'596 K	22'460 K	15208	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'096 K	15992	Console Window Host	Microsoft Corporation
powershell.exe	0.36	67'588 K	22'416 K	8992	Windows PowerShell	Microsoft Corporation
conhost.exe		2'440 K	7'072 K	11048	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	67'772 K	23'136 K	14340	Windows PowerShell	Microsoft Corporation
conhost.exe		2'440 K	7'092 K	17028	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	67'708 K	22'864 K	11400	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'096 K	15204	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	67'468 K	22'580 K	76	Windows PowerShell	Microsoft Corporation
conhost.exe		2'440 K	7'084 K	5640	Console Window Host	Microsoft Corporation
powershell.exe		66'980 K	21'632 K	17252	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'084 K	12000	Console Window Host	Microsoft Corporation
powershell.exe	0.72	68'948 K	23'120 K	12488	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'108 K	16820	Console Window Host	Microsoft Corporation
powershell.exe	1.09	67'572 K	22'572 K	11256	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'080 K	13680	Console Window Host	Microsoft Corporation
powershell.exe	0.36	67'416 K	23'188 K	15348	Windows PowerShell	Microsoft Corporation
conhost.exe		2'448 K	7'108 K	6928	Console Window Host	Microsoft Corporation
powershell.exe	< 0.01	67'600 K	22'884 K	8508	Windows PowerShell	Microsoft Corporation
conhost.exe		2'444 K	7'084 K	13148	Console Window Host	Microsoft Corporation

CPU Usage: 70.65% Commit Charge: 54.01% Processes: 133 Physical Usage: 75.60%



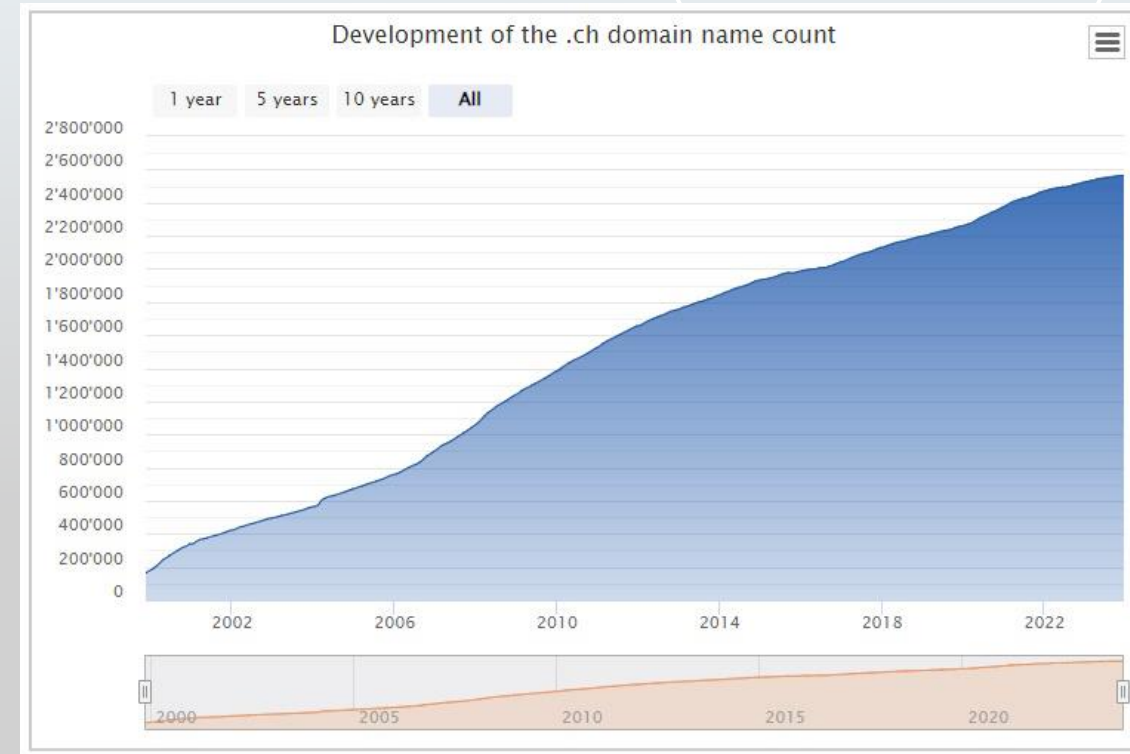
# Why does it take two Months?

Let's do a quick Math

There are about 2'5 Mio .ch Domains

Let's assume a query would take 1 Second

$2'500'000 \text{ Domains} / 60 \text{ Seconds} / 60 \text{ Minutes} / 24 \text{ Hours} =$   
It would take **29 Days**



Note: It takes longer than one Second because the Script connects to each MX Record to test STARTTLS



# Why did you do it?

Other Projects like [Hardenize .CH Resilience Report](#) (SWITCH) only shows Top 1'000 Domains

- Big Companies
- Professional IT
- Security awareness

Why did you do it?

- Messaging Engineer/Architect
- Whole TLD shows a better picture
- Spot trends and changes
- Fun hobby Project with PowerShell



## .CH Resilience Report

This dashboard monitors the web and email security configuration of the top 1,000 .ch domain names. [Maintained by SWITCH](#).

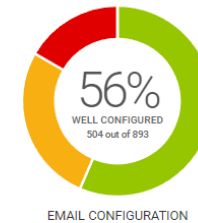
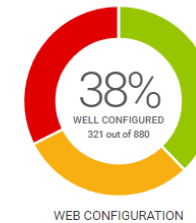
2,000  
HOSTS

2,825  
CERTIFICATES

4,104  
IP ADDRESSES

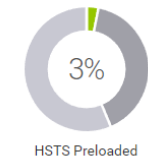
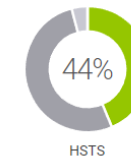
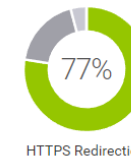
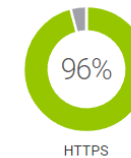
### Infrastructure Configuration Overview

Key aspects of web application and email infrastructure configuration and security.



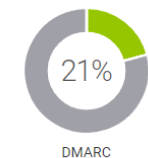
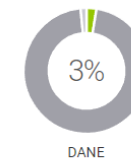
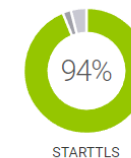
### Web Application Configuration

Key aspects of web application security of the hosts monitored by this dashboard.



### Email Infrastructure Configuration

Key aspects of email security of the hosts monitored by this dashboard.



# What the Report does NOT do



My main Focus on this Project was related to Mailsecurity and not about Websites

NOT checked

- HTTP/HTTPS of Website
- HTTPS [TLS Version](#) used
- HTTP Strict Transport Security ([HSTS](#))
- HTTP [Security Header](#)





# Overview



# Overview

## Domains

- 2'516'443 .ch Domains (September 2023) [NIC Statistics](#)
- 122'446 Domains more than about a year ago

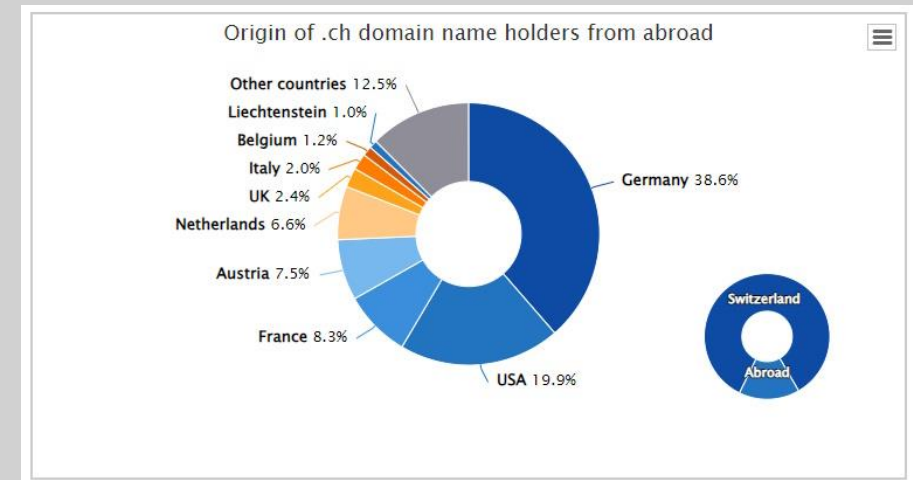
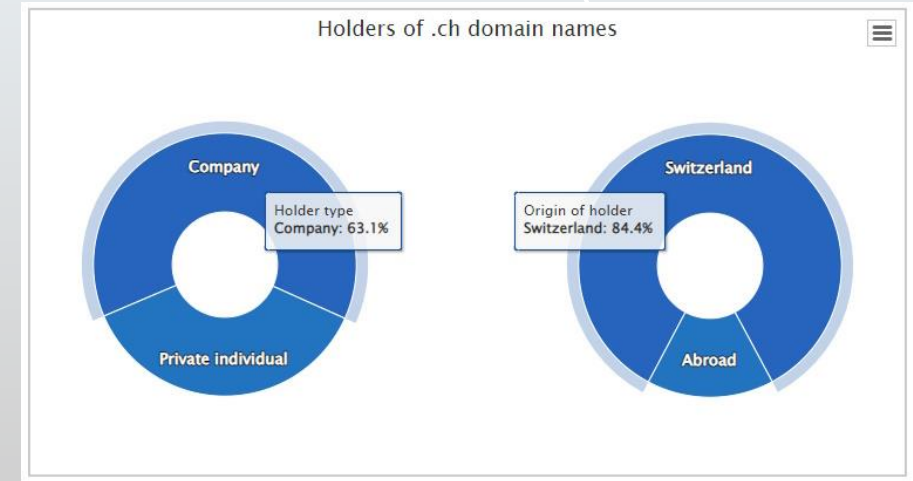
## Domain Holders

Domain Holders (Company / private Individual) [NIC Statistics](#)

- 63.1% (about 1'587'875) are owned by a Company
- 36.9% (about 928'567) are owned by a private Individual

## Top .ch Domain Holders outside Switzerland

- 38.6% Germany
- 19.9% USA
- 8.3% France
- 7.5 % Austria

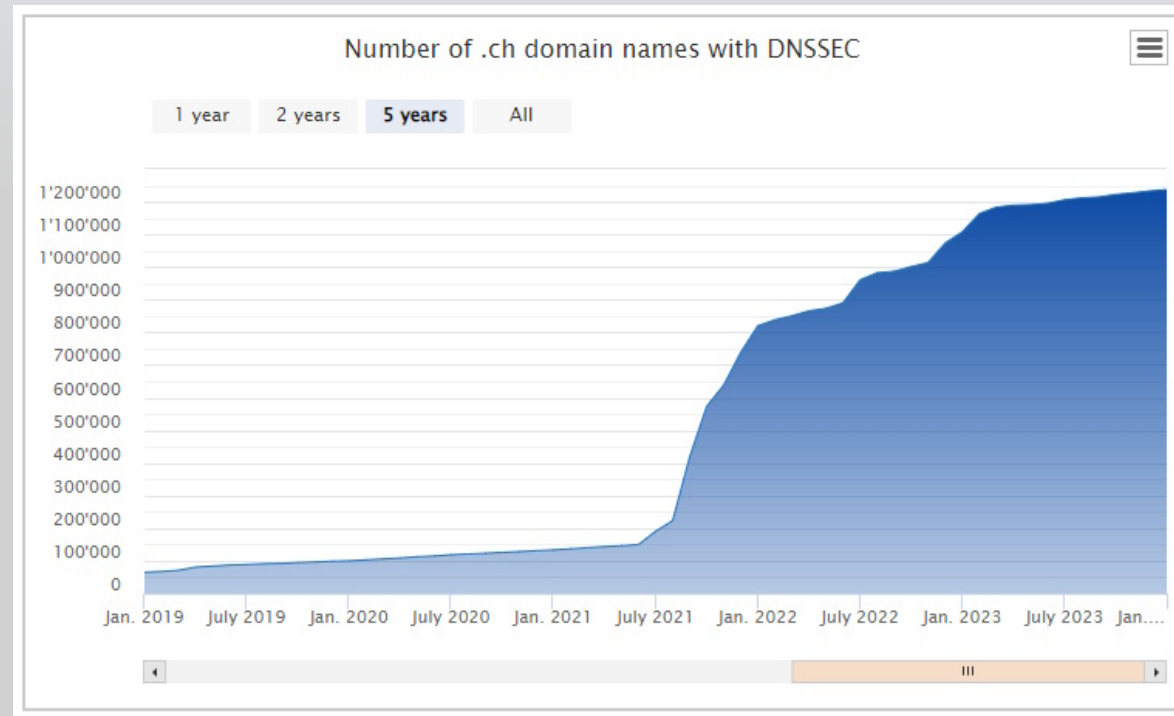


# DNSSEC and NS



# DNSSEC and NS

- 48.34% (1'216'341) of the DNS Zone Signed [NIC Statistics](#)
- with a huge bump since summer 2021
- 236'376 DNSSEC Domains more than about a year ago



# DNSSEC and NS

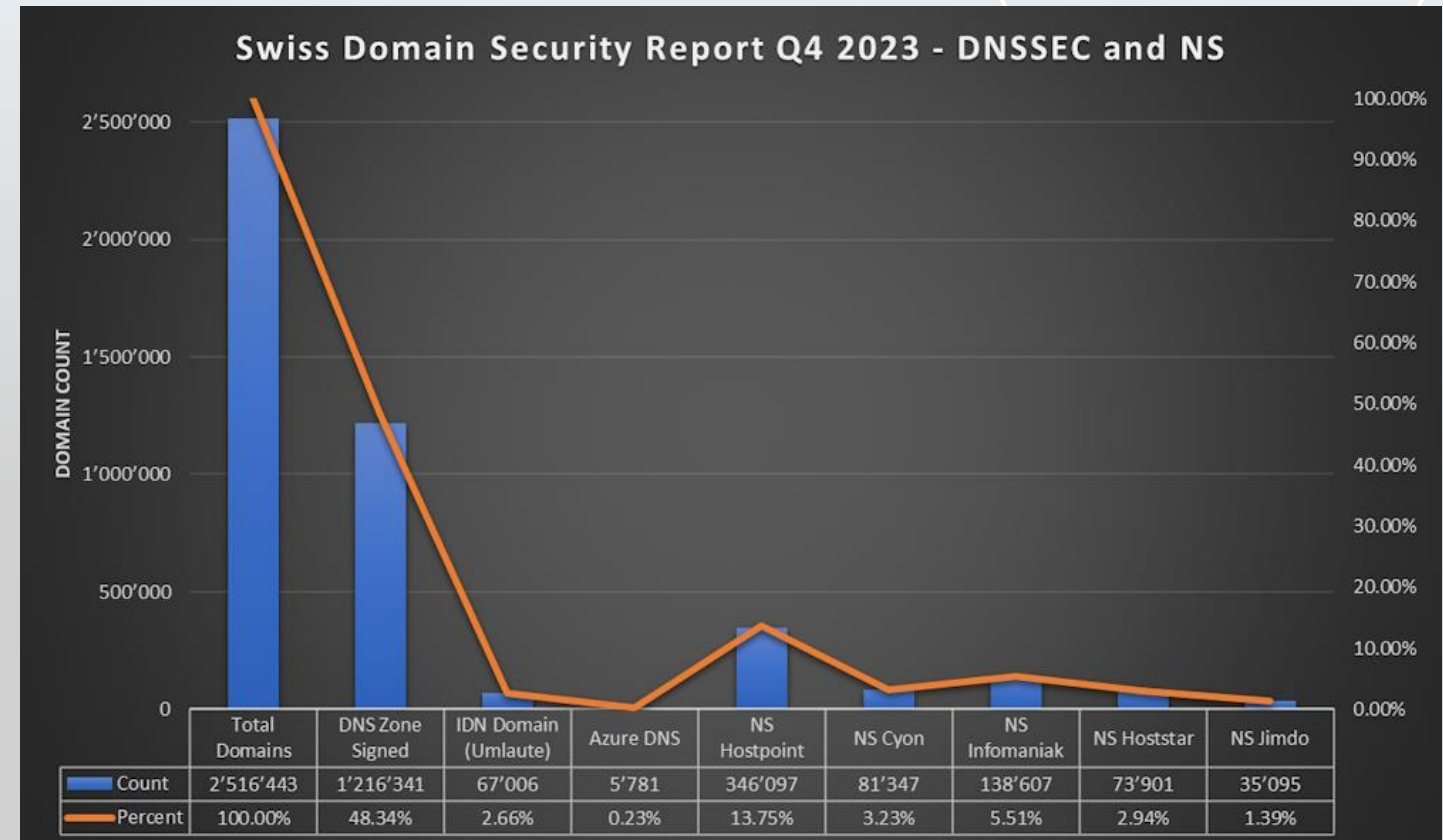
## NS Records

- 13.7% (346'097) point to Hostpoint
- 5.51% (138'607) point to Infomaniak
- 3.23% (81'347) point to Cyon
- 2.94% (73'901) point to Hoststar
- 1.39% (35'095) point to Jimdo
- 0.23% (5'781) point to Azure DNS

## IDN (internationalized domain name)

- 2.66% (67'006) are [IDN](#) using Punycode

Note: Azure DNS does not Support DNSSEC





# Other insights

## MX Records

- 70.76% of Domains have a MX Record

## CAA (Certification Authority Authorization)

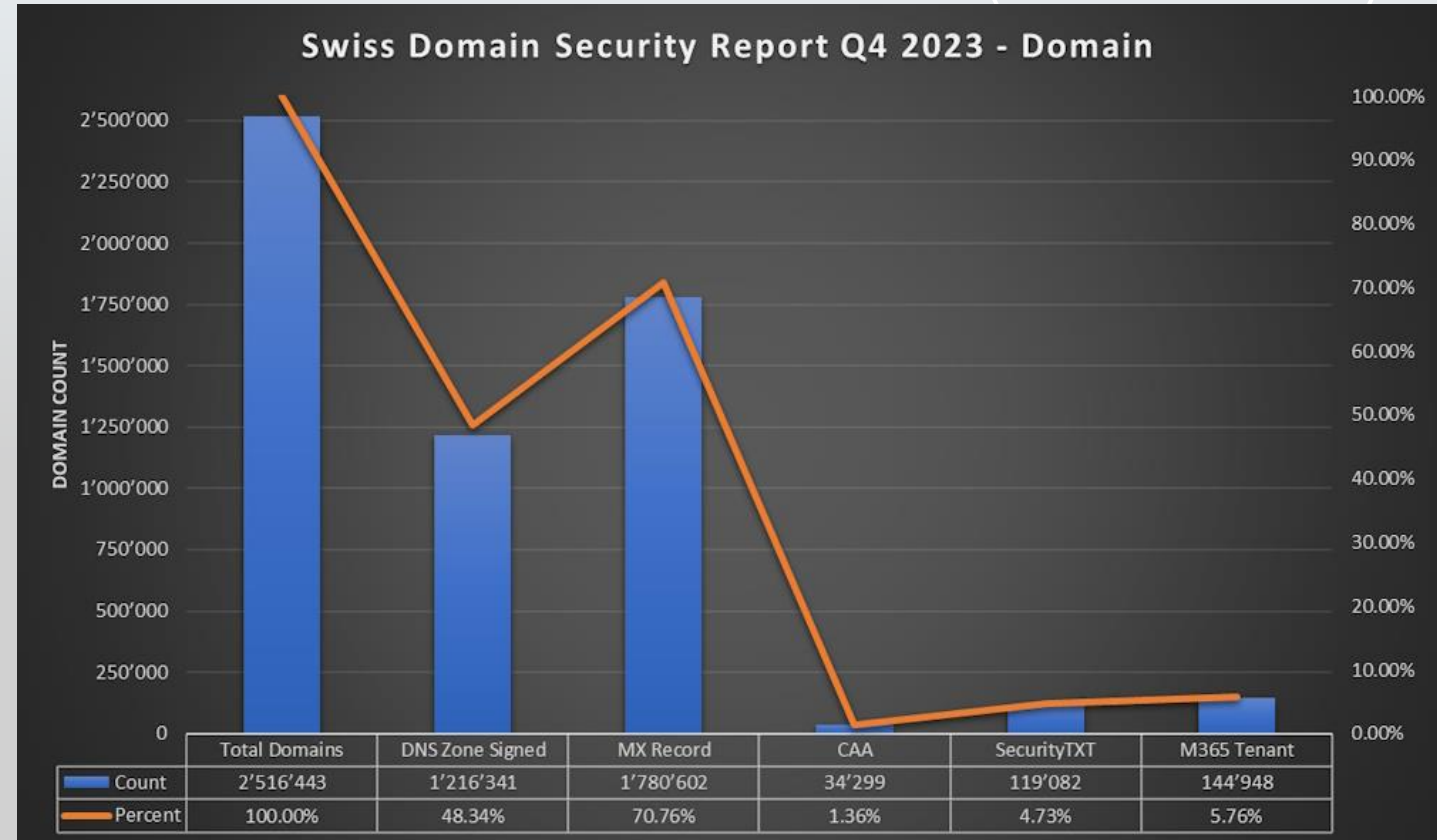
- CAA exists since 2019 [rfc8659](https://tools.ietf.org/html/rfc8659)
- 1.36% (34'299) of all .ch Domains support
- 6'278 Domains more last year
- [Wikipedia CAA](https://en.wikipedia.org/wiki/Certificate_authority#CAA)

## Security TXT <https://securitytxt.org>

- <https://domain.tld/security.txt> (old)
- <https://domain.tld/.well-known/security.txt>
- Exists since April 2022 [rfc9116](https://tools.ietf.org/html/rfc9116)
- 4.73% (119'082) Domains have SecurityTXT

## M365 Tenant

- 5.76% (144'948) of all .ch Domains have a M365 Tenant
- 110'657 unique Tenants with .ch Domains



# Mailsecurity



MX



# MX (Mail Exchange)

## MX Record

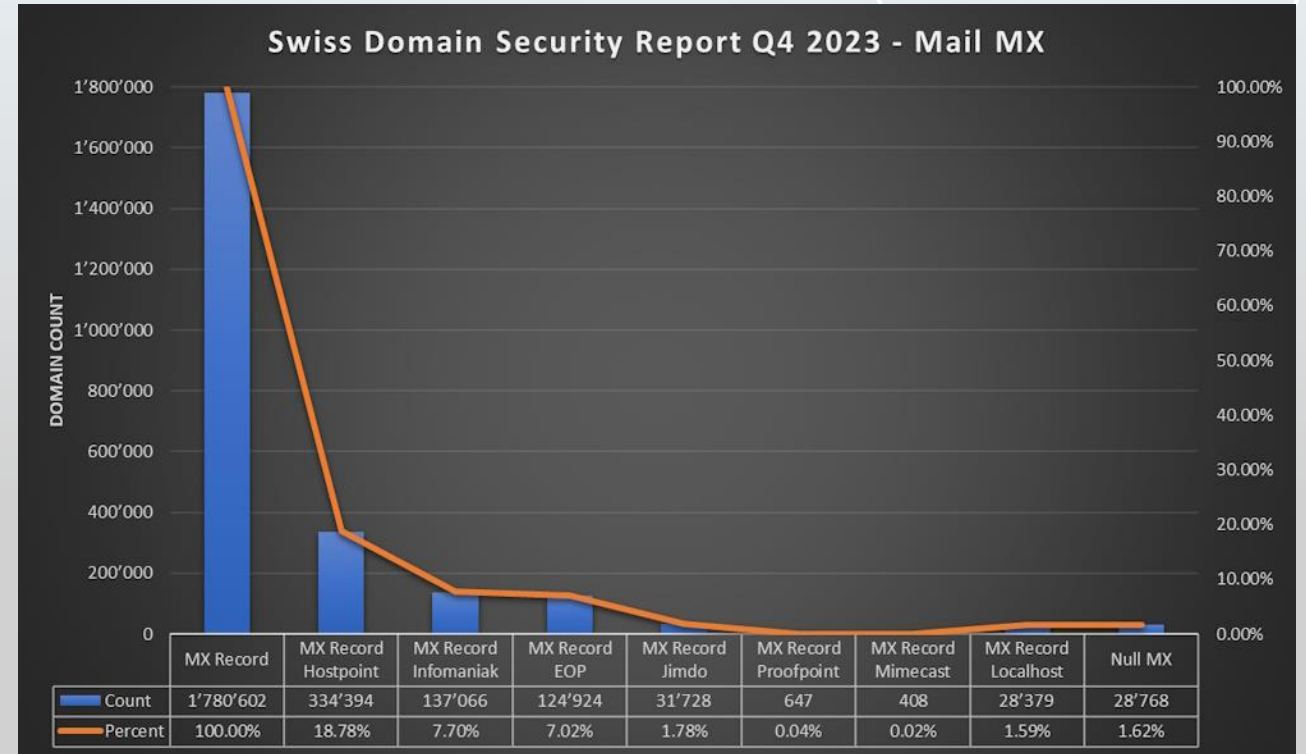
- MX Record exists since 1987 defined [rfc1035](#)
- 70.76% (1'780'602) of all Domains have MX

## Domains with MX Record

- 18.78% (334'394) point to Hostpoint
- 7.7% (137'066) point to Infomaniak
- 7.02% (124'924) point to Exchange Online
- 1.78% (31'728) point to Jimdo
- 0.04% (647) point to Proofpoint
- 0.02% (408) point to Mimecast

## Other insights

- 1.62% (28'768) of Domains use "Null MX" [rfc7505](#)  
(not supported by Microsoft Exchange / Exchange Online)
- 1.59% (28'379) of Domains with MX point localhost 😄  
(Mostly parked Domains)





# STARTTLS / Banner



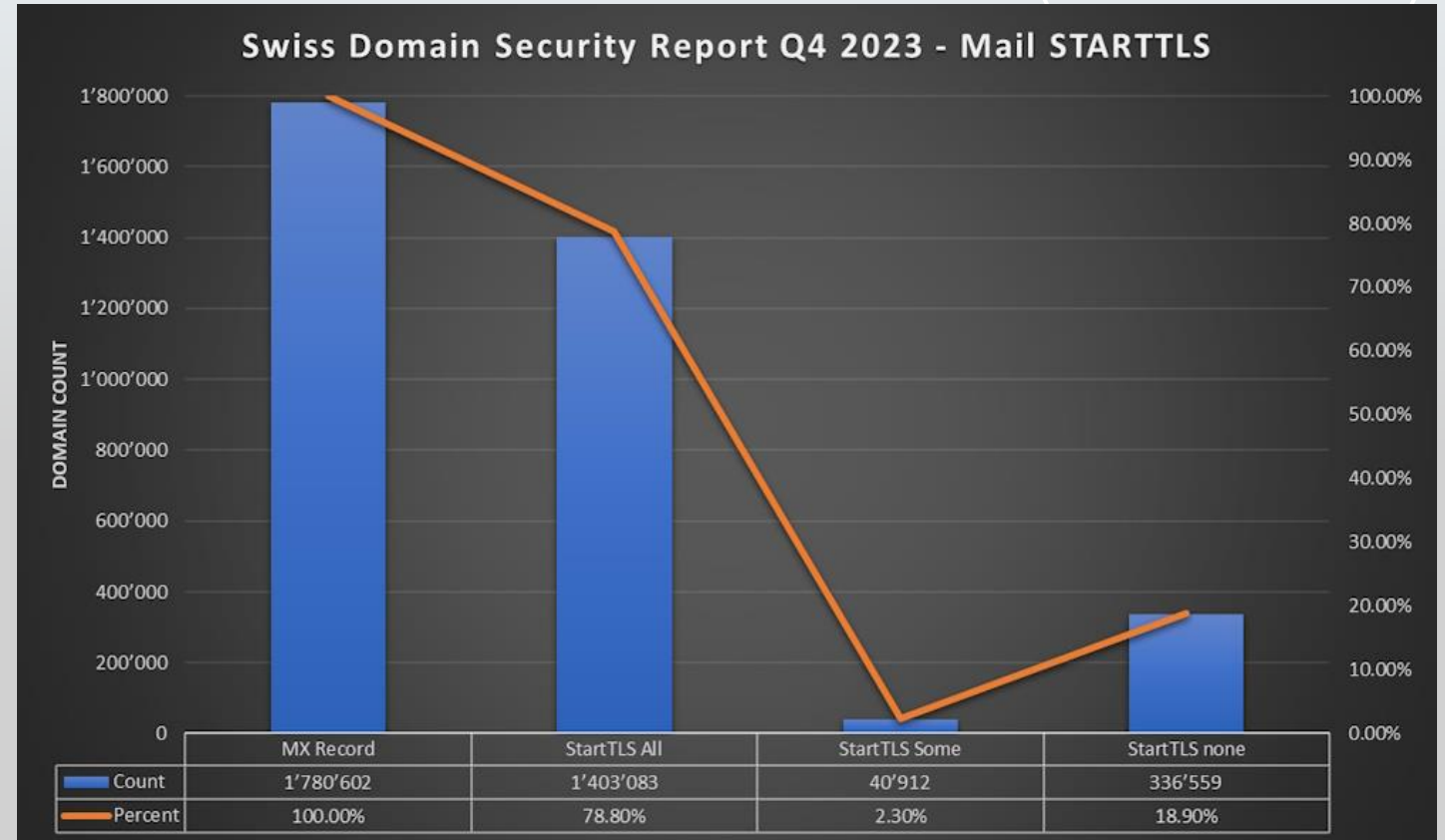


# STARTTLS

## STARTTLS

Domains with MX

- 78.80% (1'403'083) STARTTLS (on all MX records)
- 2.30% (40'912) STARTTLS (on some MX records)
- 18.90% (366'559) do not support STARTTLS



# SMTP Certificate Issuer (CA)

## Report based on Organization (O)

- O=Sectigo Limited
- O=Lets Encrypt
- O=DigiCert Inc
- O=Google Trust Services LLC
- O=Deutsche Telekom Security GmbH
- O="GoDaddy.com, Inc."
- O=SwissSign AG
- O="Entrust, Inc."
- O=GlobalSign nv-sa

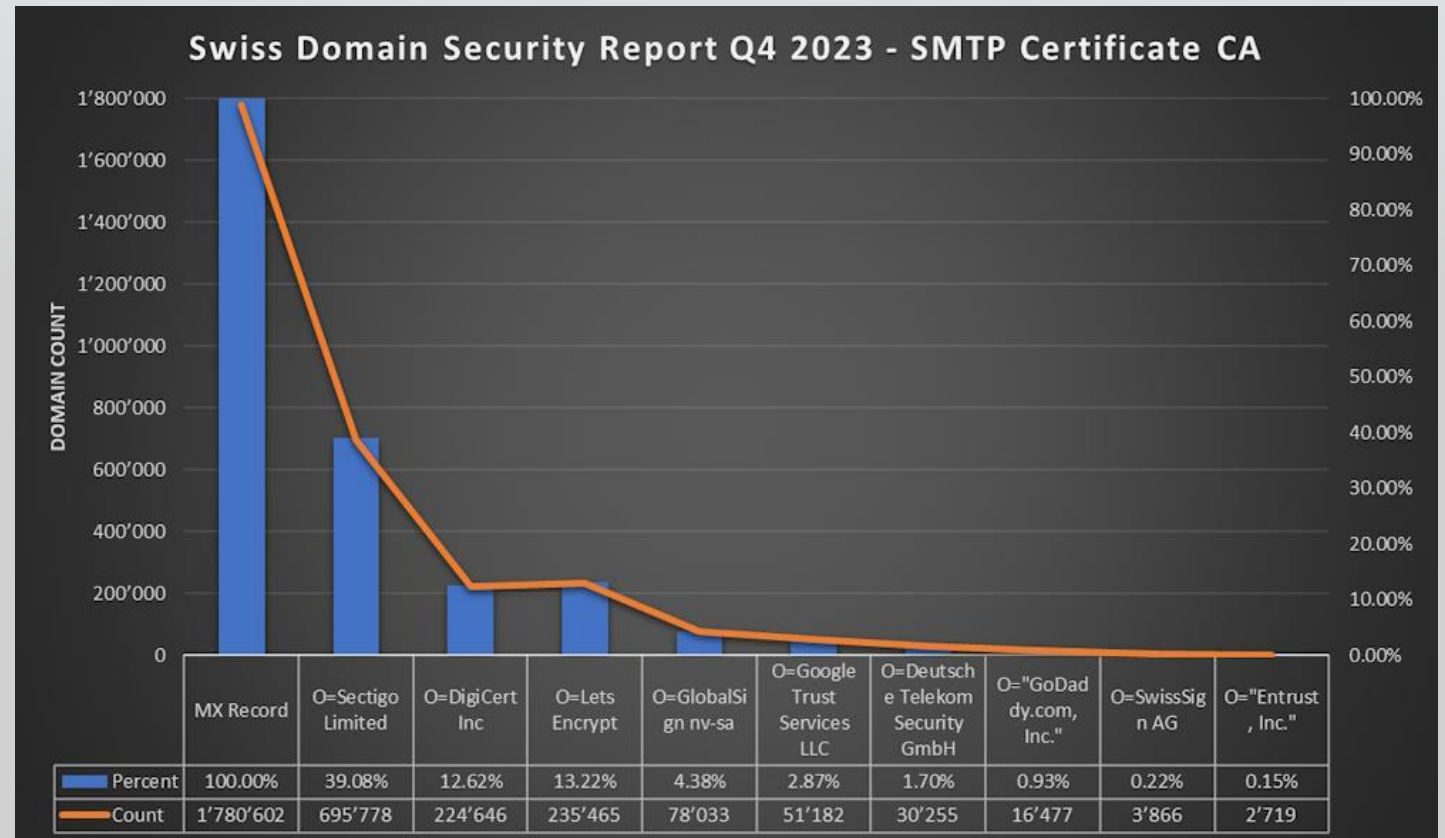
Digicert: Digicert, Geotrust, RapidSSL, Thawte

GlobalSign: AlphaSSL

**Over 13% for Let's Encrypt!**

### 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: 12/14/2023 1:00:00 AM
ValidTo: 12/14/2024 12:59:59 AM
SerialNumber: 04BAD4FA7BA66927A4BA6B70AC9B3A75
Thumbprint: 04C3E84F5B20825BF6FD5F0BE2EECA1D0A8C50BD
```



# SMTP Banner

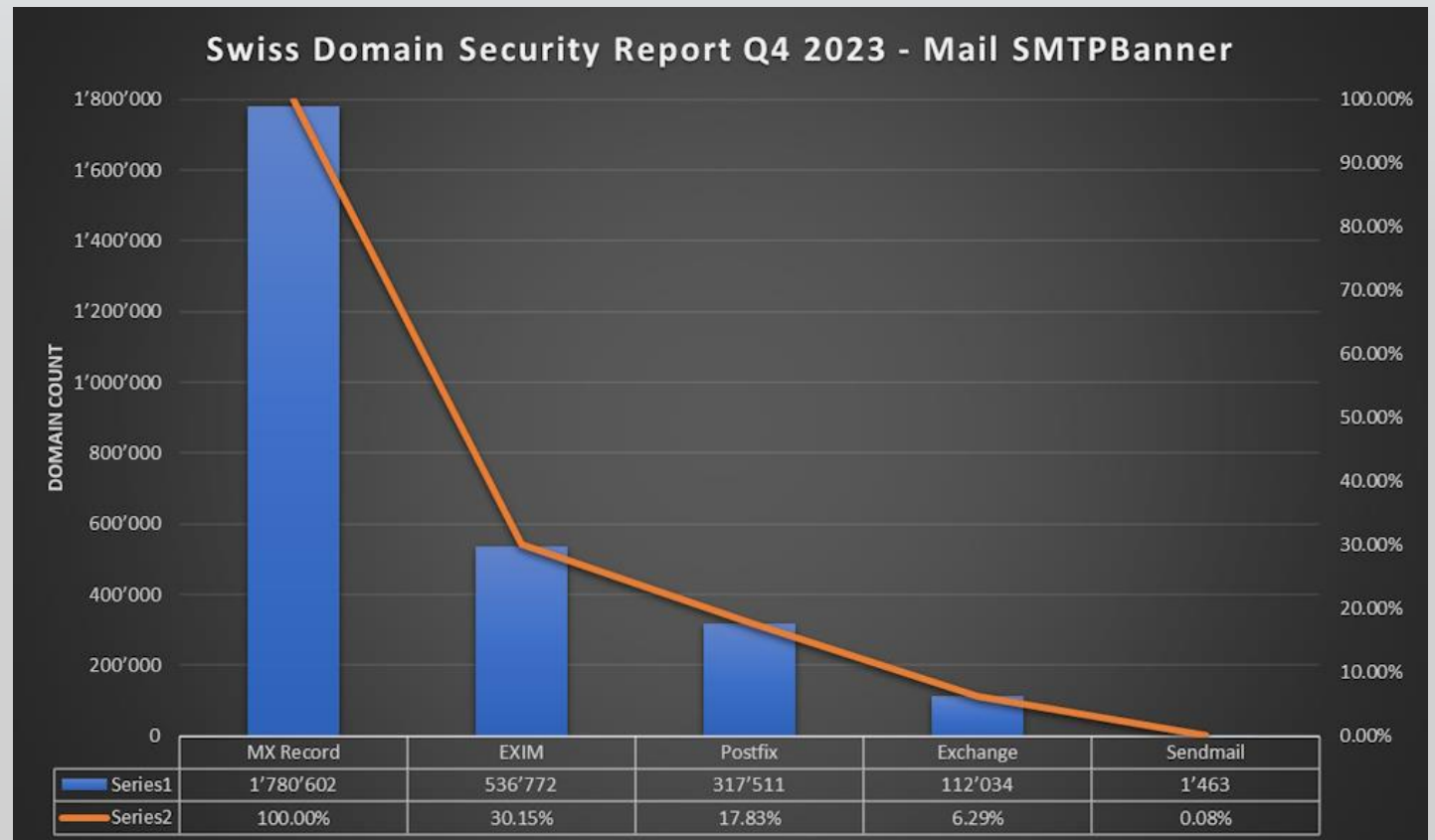
## Caution

Not all Mailservers will show the Software or even Version in the SMTP Banner.

## Results

- 30.15% (536'772) EXIM
- 17.83% (317'511) Postfix
- 6.29% (112'034) Exchange/EXO
- 0.08% (1'463) Sendmail

```
Connect icewolf-ch.mail.protection.outlook.com 25
220 ZR0CHE01FT008.mail.protection.outlook.com Microsoft ESMTPL MAIL Service ready at Thu, 11 Jan 2024 19:27:57 +0000
EHLO ICE11.corp.icewolf.ch
250-ZR0CHE01FT008.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
```



# SPF / DKIM / DMARC



# SPF / DKIM / DMARC

## SPF / DKIM / DMARC


- The holy trinity
- Becomes more and more important
- See announcements from Google, Yahoo and [Microsoft](#)
- You want to see “pass” for all the Tests

## Authenticate Outbound Email to Improve Deliverability

By  The Exchange Team

Published Oct 06 2023 09:45 AM

22.6K Views

 Subscribe

...



Email authentication is crucial for sending email. It helps protect recipients from malicious messages, such as spoofing and phishing. By setting up email authentication for your domain, you can ensure that your messages are less likely to be rejected or marked as spam by email providers like *Gmail*, *Yahoo*, *AOL*, *Outlook.com*. This is especially important when sending [bulk email](#) (large volume email), as it helps maintain the deliverability and reputation of your email campaigns. Please note that using Microsoft 365 to send bulk (mass) email is not a supported use of the service (more details below).

## What changed?

Microsoft 365 email senders may meet new difficulties in delivering emails to popular email service providers. For example, [Google has implemented stricter security requirements](#) to authenticate incoming email messages, particularly those sent in large

### Other headers

#1	Header	Value
1	<a href="#">Authentication-Results</a>	spf=pass (sender IP is 108.174.0.205) smtp.mailfrom=bounce.linkedin.com; dkim=pass (signature was verified) header.d=maile.linkedin.com; dmarc=pass action=none header.from=linkedin.com; compauth=pass reason=100
2	<a href="#">Received-SPF</a>	Pass (protection.outlook.com: domain of bounce.linkedin.com designates 108.174.0.205 as permitted sender) receiver=protection.outlook.com; client-ip=108.174.0.205; helo=maile-he.linkedin.com; pr=C
3	<a href="#">DKIM-Signature</a>	v=1; a=rsa-sha256; c=relaxed/relaxed; d=maile.linkedin.com; s=d2048-202308-0e; t=1704997899; bh=p9WyUQ2snjdHLLI6zP17VsV/GeVR3U+ou4cLbGMisv4=; h=From:Subject:MIME-Version:Content-Type:To:Date:X-LinkedIn-Class:X-LinkedIn-Template:X-LinkedIn-fbl; b=T8D7ckjfUJCIRBFxI5uDMck/qC3zud1XcFypWWWmpnMOVTBXuQhc0zEbeame4gGepx zI7ewMwZ+shO3vB7nyVpnaFY7G0FhdNI9dtuWLC3X8BMX4HI9iRQ8XaguGaDXCUkNGA cD172udmyoWZL3dHgneV3jyAjBa8lrjxScqC2wz1Ft8sWj+YrBJAYKUtlpLh/m7IT GNSEtUGizF6fnXnMPPxwkTFVBd4cKi8izqWbLwwlyfcvWXcU+hFSeTN5KVHHW2pJ6l /AgCUK4/gGXTIDkdz+8HX0JezLJcQagVO6zkG4LYYPi7fBqd5SctXlflvtSU82gb 7KF2a02wgPnVg==
4	<a href="#">DKIM-Signature</a>	v=1; a=rsa-sha256; c=relaxed/relaxed; d=linkedin.com; s=d2048-202308-00; t=1704997899; bh=p9WyUQ2snjdHLLI6zP17VsV/GeVR3U+ou4cLbGMisv4=; h=From:Subject:MIME-Version:Content-Type:To:Date:X-LinkedIn-Class:X-LinkedIn-Template:X-LinkedIn-fbl; b=Ufi853k6G8Jf8FhcQB0eglv13HbOaZ/wvpbmQTmXDENGUW79ZqSo4VjWPDg0NMkYy X8Nj5+rfMc2Yu9g4luVvnkrU/JbeOnHNmdCikK9kFfPON2rFY/a67I4527bqvhV8rH 6A+v3q+CuqN1NJNdrYSRWCPwumPJXEK7HJmp6IG9D7ImlovPNJuhfOhK27wZMPle8q szk7MQGhZqA/BD2mP8RhTxcrlvquSh17ugEMOR1f+h5sEGEUKICKq96AfQAFan1y4T tWnUw/faiOhn+0Kn15Gw5vbePmwhN3wAVwZsZl2+59rt9MbYnCsUMgLaL2ND/FFRI mgxYvq50kPPfw==



# Sender Policy Framework (SPF)

SPF exists since 2003 with Updates 2006 and 2014 [rfc7208](#)

## Domains with MX

- 78.13% (1'391'162) have a SPF Record
- 24.52% (436'578) have "SPF -all"
- 30.82% (548'760) have "SPF ~all"
- 17.15% (305'415) have a SPF Redirect
- 2.99% (53'180) have (v=spf1 -all)
- 0.36% (6'441) Multiple SPF Records

```
Command Prompt
C:\>nslookup -type=txt m-red.ch
Server: ICESRV01.corp.icewolf.ch
Address: 172.21.175.10

Non-authoritative answer:
m-red.ch      text =

"v=spf1 mx ip4:212.147.36.107 include:spf.protection.outlook.com ?all"
m-red.ch      text =

"sendinblue-code:035389e8895efca51f7a3dc4585f8eb9"
m-red.ch      text =

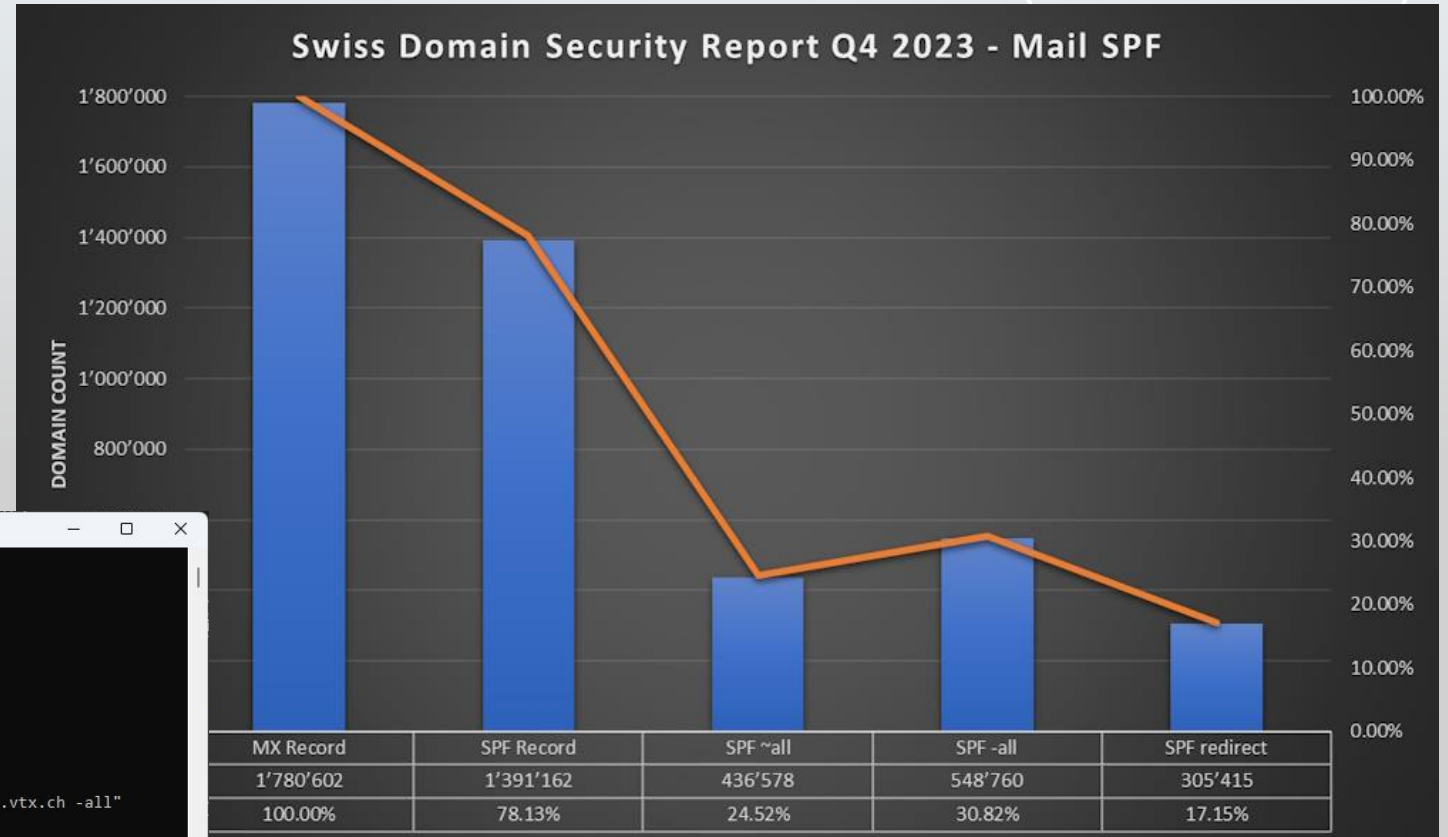
"v=spf1 mx ip4:217.193.165.27 include:spf.protection.outlook.com a:212-147-36-105.fix.access.vtx.ch -all"
m-red.ch      text =

"v=spf1 mx ip4:212.147.36.108 include:spf.protection.outlook.com ?all"
m-red.ch      text =

"v=spf1 mx ip4:217.193.165.27 include:spf.protection.outlook.com ?all"
m-red.ch      text =

"v=spf1 mx ip4:217.193.165.27 include:mail.m-groupe.ch include:spf.protection.outlook.com ?all"
m-red.ch      text =

"v=spf1 mx ip4:217.193.165.27 include:spf.ess.de.barracudanetworks.com include:spf.protection.outlook.com -all"
C:\>
```



# DomainKeys Identified Mail (DKIM)

## DKIM (DomainKeys Identified Mail)

- It is defined in [rfc6376](#) from 2011 with updates in [rfc8301](#) and [rfc8463](#) in 2018

```
Internet headers
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=bluewin.ch;
s=fxzs-2048-20230414; t=1704900697;
bh=zAExxW3ZPB5no8KjbnMvje1K6MmAX0pm7+Gwu8t5NM=;
h=From:To:Subject:Date:Message-ID:MIME-Version;
b=Ti604Fk9AadwH/0MzcmlA9F4uEDMeKy+
2/xC4ENdJqGqLf65LBS3IHLzvDabNCPEb
VnzjCWnZNdc8ZXFbGaKtclD51qldFe+sB5RtWYszz2PtFLX9ytX+KIW
Close
```

### Note:

Due the fact that the Selector can be anything it's hard to determine DKIM Records.

```
Windows PowerShell
PS C:\> Resolve-DnsName -Type "NS" -Name "_domainkey.bluewin.ch"

Name      Type TTL Section PrimaryServer NameAdministrator SerialNumber
----      -
bluewin.ch SOA  112 Authority ns31.scs-ns.ch admin.dns.swisscom.com 2023052728

PS C:\> Resolve-DnsName -Type "TXT" -Name "fxzs-2048-20230414._domainkey.bluewin.ch"

Name                                          Type TTL Section Strings
----
fxzs-2048-20230414._domainkey.bluewin.ch TXT  43148 Answer {v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBGKCAQEAAnVve5BU8eRBMSVCDREg7yHfum8VreQz0XDberDxE0142rQQL9rmjFRHOL1RYtf3JfTkVqXbCn97mL/FVLgm4kQP79TfiXSCPCxEge3rF8hcleia00HQ/SynZ
O+wONjHZqd9zn40F37NIyw4roeib, sBg7ggQ5CLHaMrEVFDrJeUX7PUgbQJQe0u3bsGstehMnlzE0wUSF
xCHZtlvp2LKfoP16N9xe8HoUR5ebAKE6zFNyGLrZqvFx+sqk1GkwIXsyDy/MZwomeaTTdaEnufir43SKB3
5R31UMxmEfUje6RCBnkRyD100CHJH9tjSKv741FjZb12KSw5 qm71FoipK8AwIDAQAB}
```

I've tried to figure out if the \_domainkey.domain.tld Zone exists.

- 7.08% (126'130) of Domains with MX have a high chance of having a DKIM Record
- 64.54% (1'149'289) of Domains with MX might have a DKIM Record or not

Summary: You can't tell from DNS unless you receive a Mail. Best guess is to use the Numbers from DMARC because that is built on top of SPF and DKIM



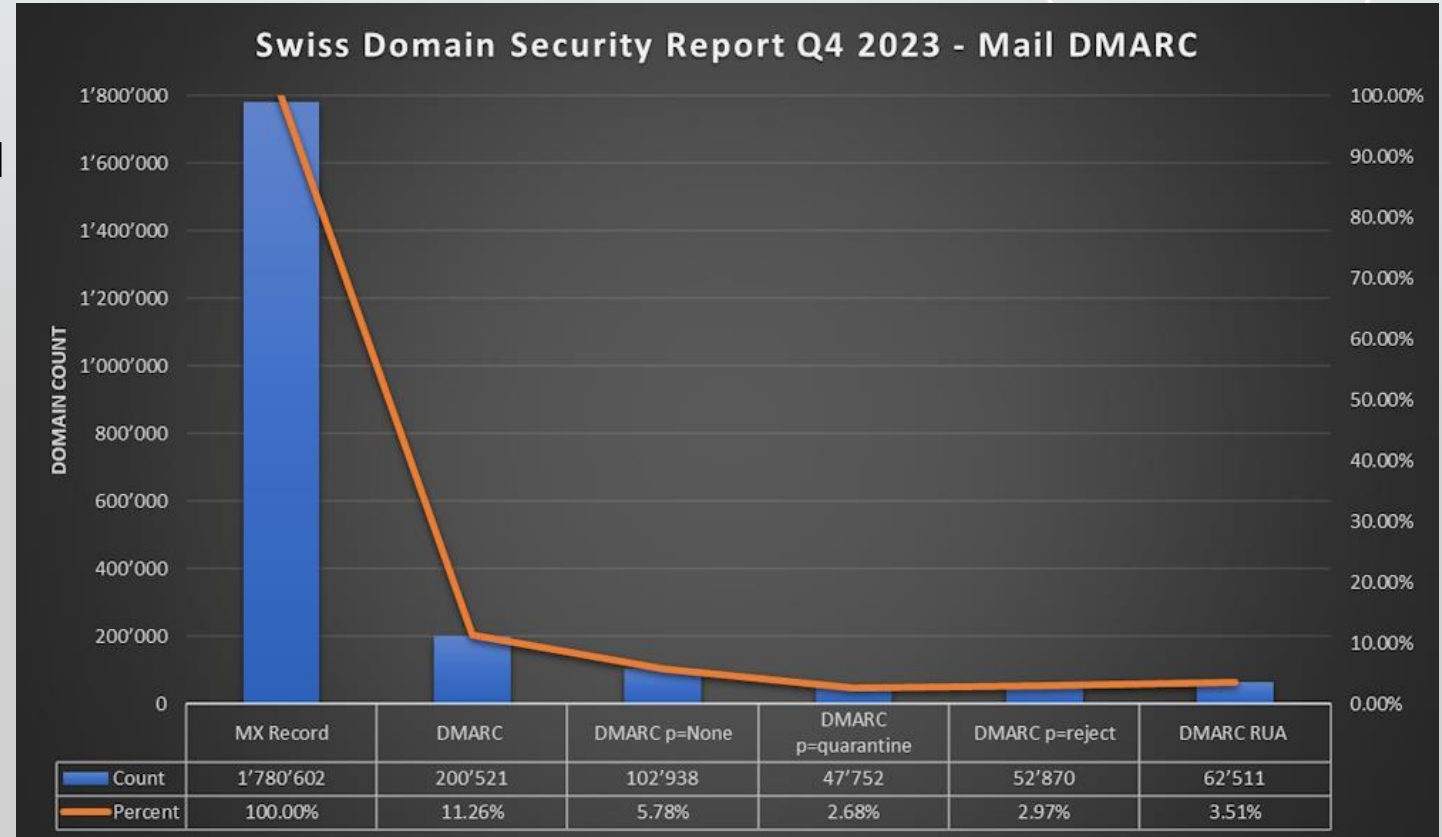
# DMARC

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

- DMARC Exists since 2015 defined in [rfc7489](https://tools.ietf.org/html/rfc7489)

### Domains with MX

- 11.26% (200'521) have a DMARC Record
- 5.78% (102'938) p=none
- 2.68.9% (47'752) p=quarantine
- 2.97% (52'870) p=reject
- 3.51% (62'511) have a rua defined



# DANE



# DANE

## DNS-based Authentication of Named Entities (DANE)

- Exists since 2015 [rfc7671](#)
- Requires DNSSEC
- Fingerprint of the Certificate used for SMTP published in DNS
- TLSA DNS Record not supported in all DNS Frontends
- Complex implementation
- Operational Challenges with Certificate-Rollover

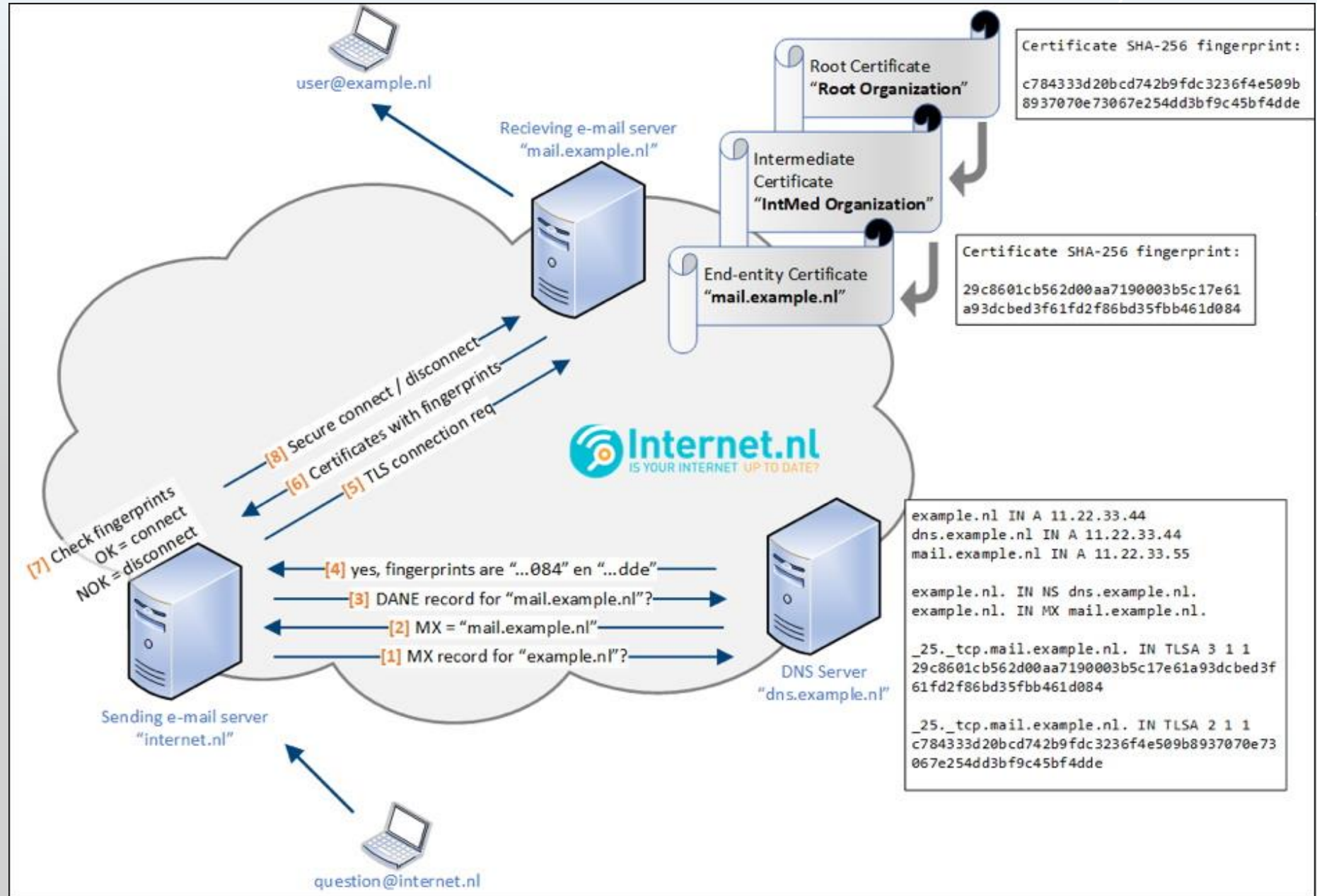
## Exchange / Exchange Online

- No Support in Exchange Server
- Outbound Support in Exchange Online is GA 2023
- [Inbound Support in Exchange Online H1 2024](#)





# DANE





# MTA-STS / TLSRPT



# MTA-STS

## Mail Transfer Agent Strict Transport Security (MTA-STS )

- Exists since 2018 [rfc8461](#)
- Emails are transmitted over a secure connection (TLS)
- You are using TLS version 1.2 or later
- The following applies to the TLS certificates of the servers:
  - CN must match the server in your MX records
  - Certificate is signed by a trusted public Root CA
  - Certificate is not expired

MTA-STS provides protection against :

- Downgrade Attacks
- Man-In-The-Middle (MITM) Attacks
- It solves several SMTP security issues, including expired TLS certificates and lack of support for secure protocols.



# TLSRPT

## TLS Reporting (TLSRPT)

- Exists since 2018 [rfc8461](#)
- Reporting of TLS Issues in SMTP to Emailaddress or Webservice

\_smtp.\_tls.domain.tld TXT

```
$TLRPTQuery = "_smtp._tls.gmail.com"
```

```
Resolve-DnsName -Name $TLRPTQuery -Type TXT
```

```
v=TLRPTv1;rua=mailto:sts-reports@google.com
```

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

Name                        Type  TTL  Section  Strings
----                        -
smtp._tls.gmail.com        TXT   300   Answer   {v=TLRPTv1;rua=mailto:sts-reports@google.com}

PS C:\>
```



# 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

Select

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 }
```



BIMI





# BIMI

## Brand Indicators for Message Identification (BIMI)

### Requirements

- The Domain is protected with SPF/DKIM/DMARC
- DMARC Policy must be «quarantine» or «reject» for Domain (p=) and subdomain (sp=)
- SVG File should be a square, but also fit nicely in a circle
- SVG File must meet Tiny 1.2 Specification
- SVG File must be less than 32kb
- SVG File must be published on the Internet
- BIMI DNS Record (TXT Record) must be published
- If your logo is protected by trademark, you can buy Verified Mark Certificates (VMC)
- VMC is a Certificate that will be published in the BIMI DNS Record

How does Brand Indicators for Message Identification (BIMI) work?

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



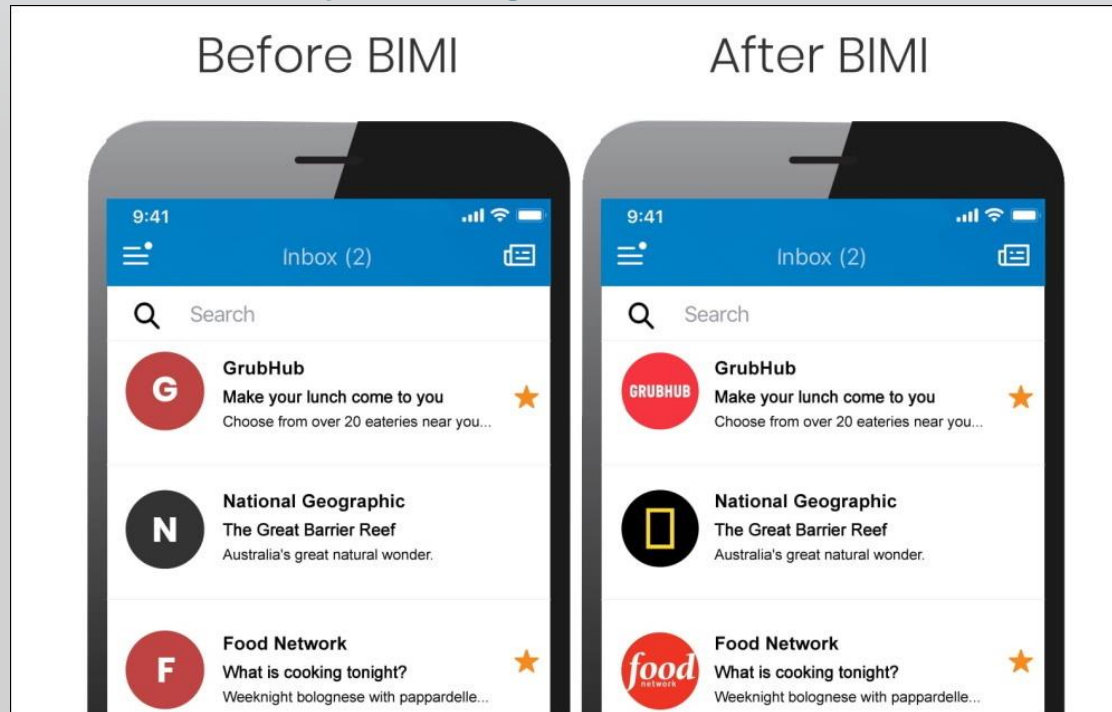
# BIMI

## Brand Indicators for Message Identification (BIMI)

That's how it should look like  
Who [does support BIMI](#)?

Vote for BIMI in Microsoft Feedback Portal

- [BIMI support in Outlook](#)
- [Allow BIMI Functionality in Exchange Server](#)



Supports BIMI	Considering BIMI	Does not support BIMI



# Summary

## SPF (2003)

- 78.13% (1'391'162) have SPF Record
- 30.82% (548'760) have "SPF ~all"

## DKIM (2011)

- can't really tell

## DMARC (2015)

- 11.26% (200'521) has DMARC Record
- 5.78% (102'938) p=none

## DANE (2015)

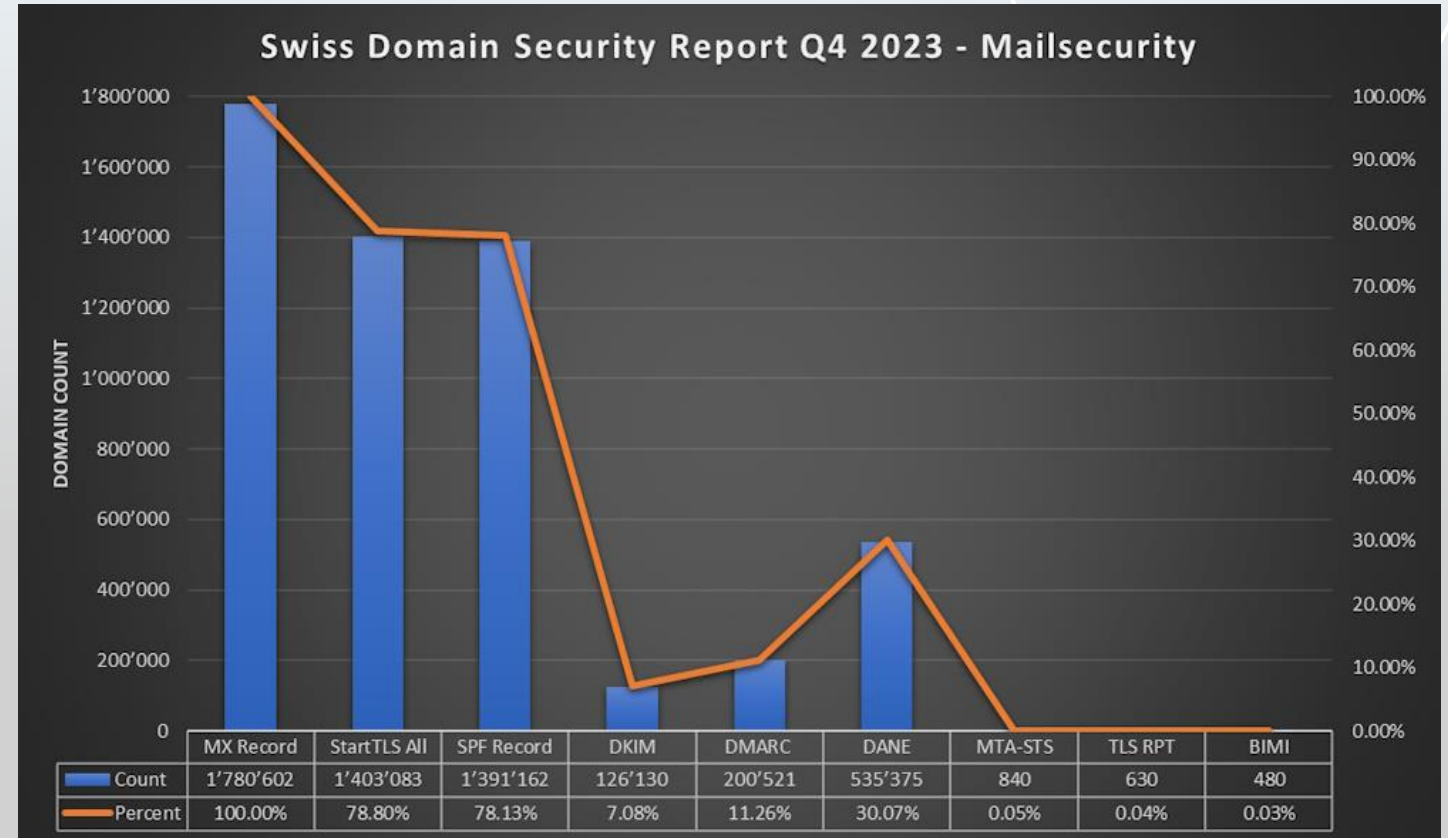
- 30.06% (535'208) has DANE Record

## MTA-STS / TLS-RPT (2018)

- 0.05% (840) support MTA-STS
- 0.04% (630) support TLS-RPT

## BIMI

- 0.03% (480) Support BIMI
- only 14 with a Certificate



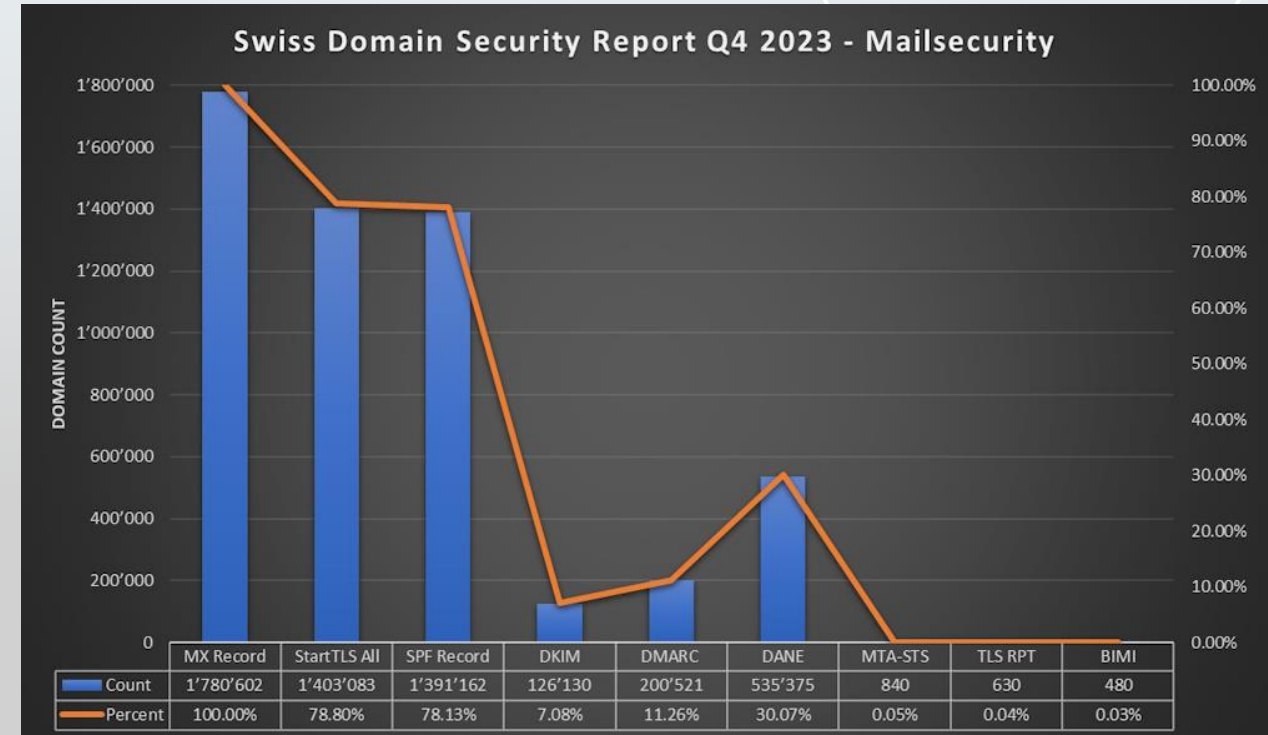
# Recap and Improvements



# Recap

Let's wrap it up

- Over 40% of the DNS Zones support DNSSEC
- STARTTLS is about 80%. That's impressive - the goal should be 100%
- SPF has improved to 78%.
  - Sadly only 30% have "-all" what should be standard (in my opinion)
- DMARC has improved from 7.8% to 11.26%
  - Half of it with "p=none"
  - "p=reject" should be standard.
  - Should be standard for all M365 Tenants
- DANE has improved from 28.3% to 30.06%
  - surprising high due to the fact it's quite complex to set up and it has a DNSSEC Requirement
- MTA-STS/TLS-RPT is surprising low at 0.05% as it's less complex than DANE. I bet this will still increase over time.





# M365 and Exchange Online



# Office 365 Inbound Report

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

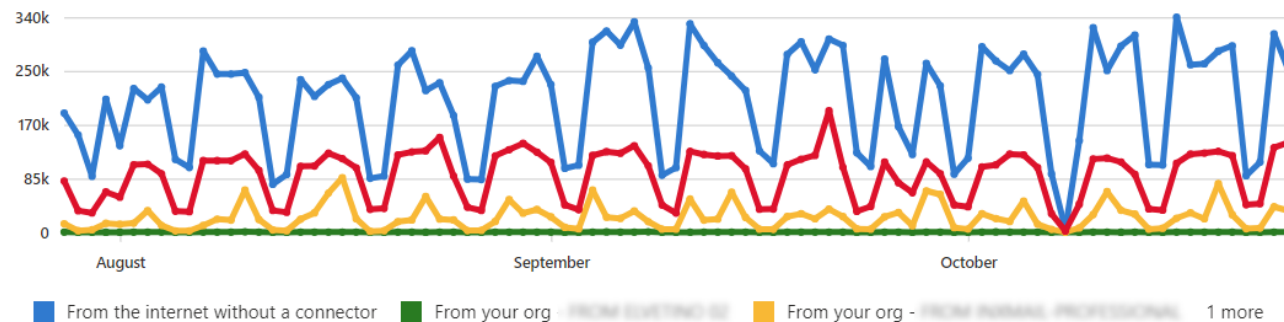
At a big customer (over 40'000 Mailboxes) ca ~1% NoTLS

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

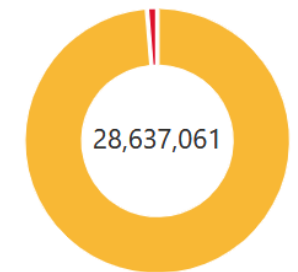
## Bericht für eingehende Nachrichten

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%

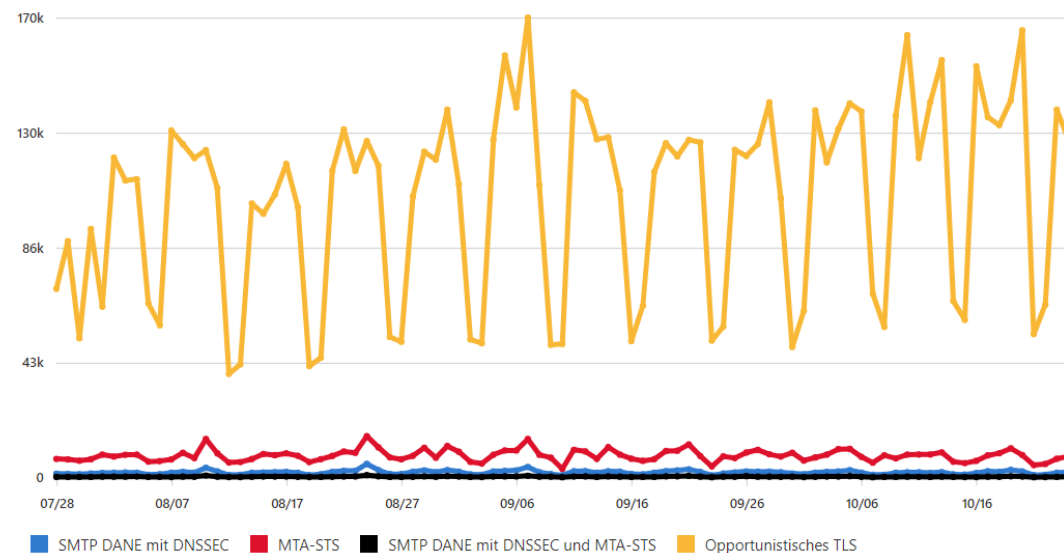
- TLS ist still mostly used
- MTA-STS is rising

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

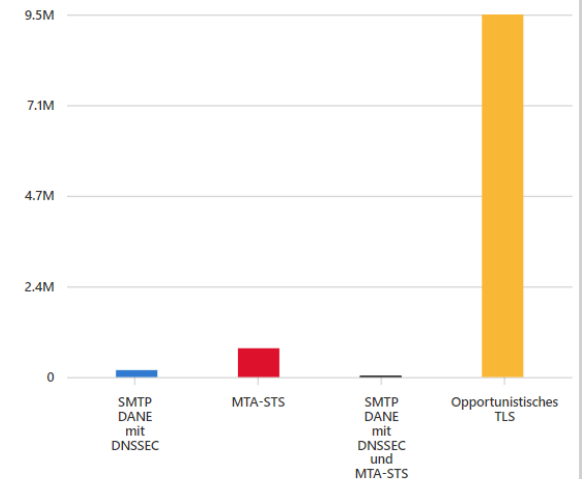
Blockierte Nachrichten   Gesicherte Nachrichten

### 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“



# Best Practices for SPF

- Every Domain has a SPF Record
- Includes and A Records in SPF does not exceed 10 DNS Lookups
- SPF Records end with "-all" (Hardfail)
- Use "v=spf1 -all" for Domains not intended to use for Email



# DKIM in Exchange Online

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=MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu/9+1UZY2vCHE+mA6PH3PM8tV2RG57yI
                        lq9ZziziT4oz6Rs5DRZT+TTyCkFsgdnt9rLb+NIKkDAFCr7043c0bS8xxMxL35rFh0zD4CjUAVhgQC9XOCpIPcEaJoJXSy
                        IOCd1Rt3HP5FMvlpEScFCAPavTDxgeDs2b9M/+LXjRhDYlJQ00/zAw+RJs1IJxU/uD4SQeyInQ9wKKDCh4hRx0YSM1oi+e
                        hU5DI4TsnYNjAcFidheHYCEqpljKxldxf6cjgl5G3s9kicWQJS/bgstph3pg0MHj9sFha/L16gNiCSCz8605fV9iIoRFPL
                        BM5qbYC7Un1vjc5NDFc7D8MJyIWQIDAQAB;
Selector2KeySize      : 1024
Selector2CNAME        : selector2-icewolf-ch._domainkey.icewolfch.onmicrosoft.com
Selector2PublicKey    : v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcQn10K95AAOM7luthw6nEmPqWS1cjBM2L4ruu
                        Phd5gksaco6rc1PeKleKkUWZnoOgUwe4RUWStwVvQ1Fk9pxSu13WvWveO5vuIFKUq9juFiq67R4UjX1xET1Z/ATzxWAVu0
                        H3wdF3XLBCEqFNhcvGQqdmvIA5goioBHNvqCzvOQIDAQAB;
SelectorBeforeRotateOnDate : selector2
SelectorAfterRotateOnDate  : selector1

PS C:\>
```

Create CNAME's in DNS

selector1.\_domainkey.domain.tld CNAME <Selector1CNAME>

selector2.\_domainkey.domain.tld CNAME <Selector2CNAME>

Set-DkimSigningConfig -Identity icewolf.ch -Enabled \$true





# DKIM in Exchange Online

View DKIM Public Key in DNS

Resolve-DnsName -Type "TXT" -Name "selector1-icewolf-ch.\_domainkey.icewolfch.onmicrosoft.com"

```
Windows PowerShell
PS C:\> Resolve-DnsName -Type "TXT" -Name "selector1-icewolf-ch._domainkey.icewolfch.onmicrosoft.com"

Name                                     Type  TTL  Section  Strings
----
selector1-icewolf-ch._domainkey.icewolfc TXT   3584  Answer  {v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQ
h.onmicrosoft.com                      EFAAOCAQ8AMIIBCgKCAQEAu/9+1UZY2vCHE+mA6PH
3PM8tV2RG57yIlq9ZziziT4oz6Rs5DRZT+TTyCkfS
gdnt9rLb+NIKKDAFCr7O43c0bS8xxMxL35rFh0zD4
CjUAVhgQC9XOCpIPcEaJoJXSyIOCd1Rt3HP5FMv1p
EScFCAPavTDxgeDs2b9M/+LXjRhDY1JQ00/zAw+RJ
siIJxU/uD4, SQeyInQ9wKKDCh4hRx0YSM1oi+ehU
5DI4TsnYNjAcFidheHYCEqpljkxldxf6cjg15G3s9
kicWQJS/bgstph3pg0MHj9sFha/L16gNiCSCz8605
fV9iIoRFPLBM5qbYC7Un1vjc5NDFc7D8MJyIWQIDA
QAB;}
```



# DKIM in Exchange Online

Or use the Microsoft Defender Admin Portal

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



The screenshot displays the Microsoft Defender Admin Portal interface. The top navigation bar includes the 'ICEWOLF.CH' logo, 'Microsoft Defender', a search bar, and user profile icons. The left sidebar lists various security management sections. The main content area is titled 'Email authentication settings' and shows the 'DKIM' tab selected. It includes a toggle switch for 'Sign messages for this domain with DKIM signatures', which is currently 'Enabled'. Below this, the 'Status' section indicates 'Signing DKIM signatures for this domain.' and the 'Last checked date' is 'Jun 24, 2023 10:44:42 AM'. A table lists identified domains for DKIM signing, with 'icewolf.ch' selected.

Name
<input checked="" type="checkbox"/> icewolf.ch
<input type="checkbox"/> icewolfch.mail.onmicrosoft.com
<input type="checkbox"/> icewolfch.onmicrosoft.com (default signing domain)
<input type="checkbox"/> irgendwoiminternet.ch
<input type="checkbox"/> sbv13920.cloudsbv.sunrise.ch
<input type="checkbox"/> subdomain.icewolf.ch

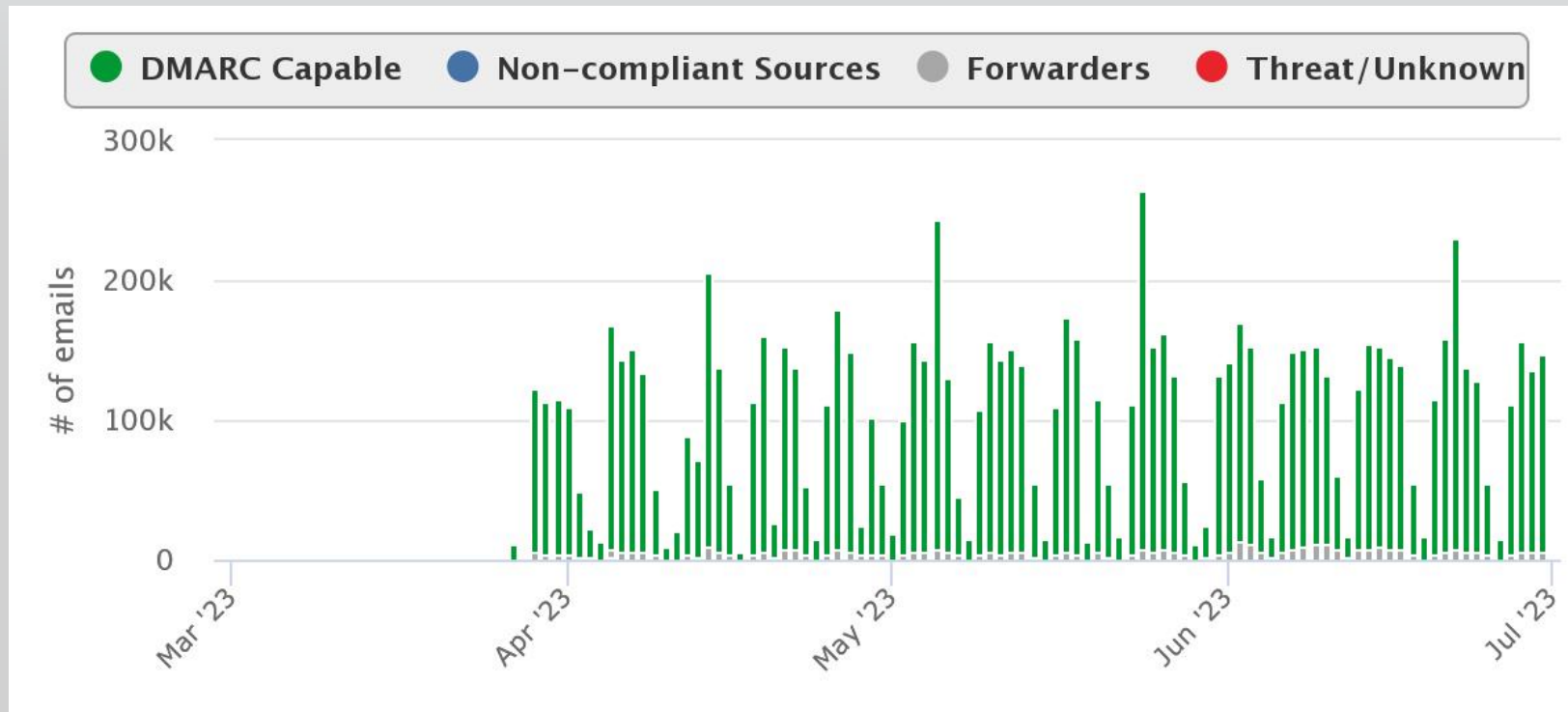


# Exchange Online DMARC RUA Report

Since April 2023 Exchange Online sends also DMARC RUA Reports.

According to DMARCAdivisor

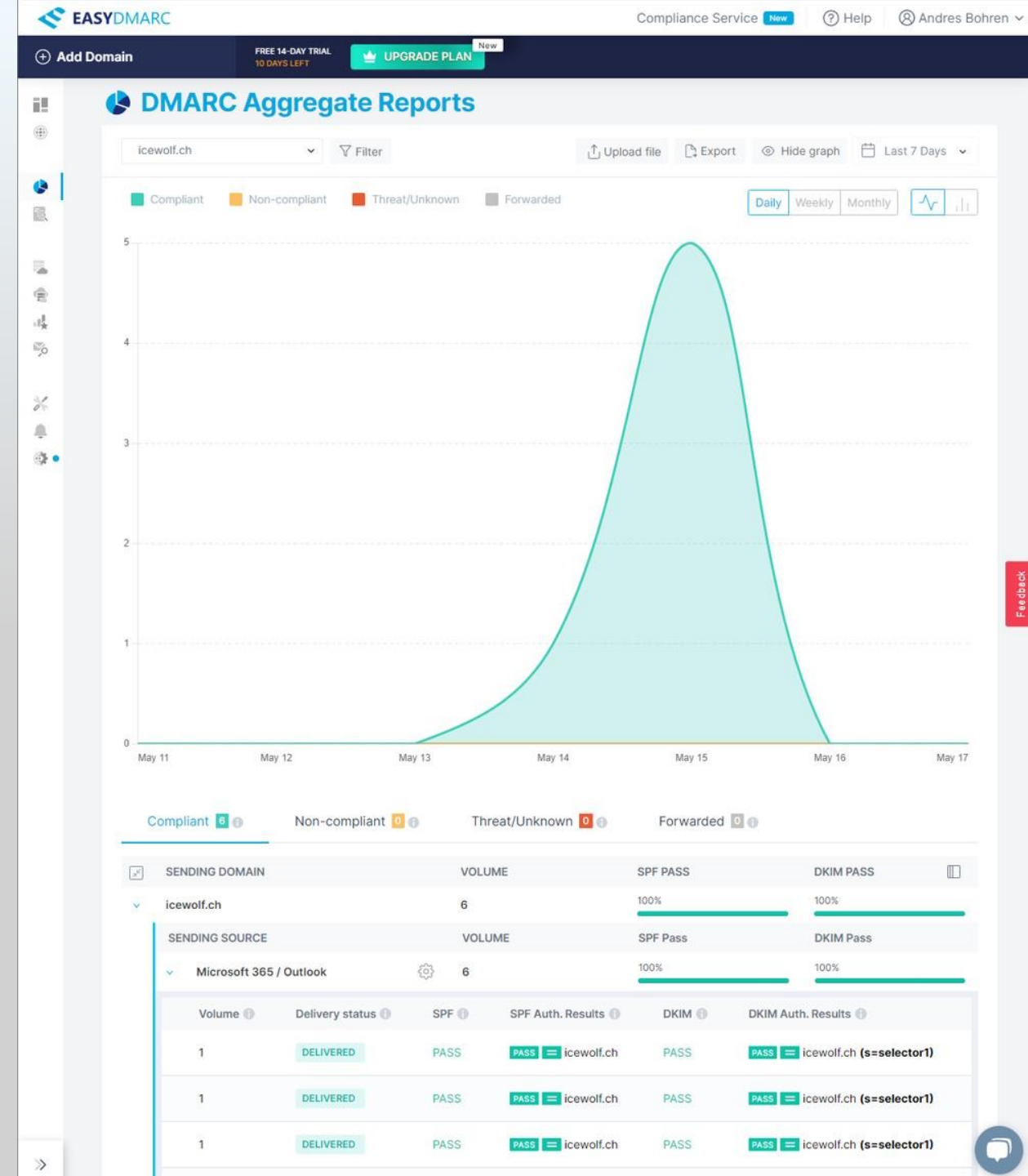
- RUA Reports have doubled over Night, when Microsoft started to send RUA Reports in EXO
- Second Week of April 33 Million Reports from «Enterprise Outlook» where processed



# DMARC Provider

Use one of the DMARC Report Providers

- [www.dmarcadvisor.com](http://www.dmarcadvisor.com)
- [www.easydmarc.com](http://www.easydmarc.com)
- [www.dmarcian.com](http://www.dmarcian.com)
- [www.agari.com](http://www.agari.com)
- [www.valimail.com](http://www.valimail.com) (Free but not enough Details)



# MTA-STS DNS TXT Record

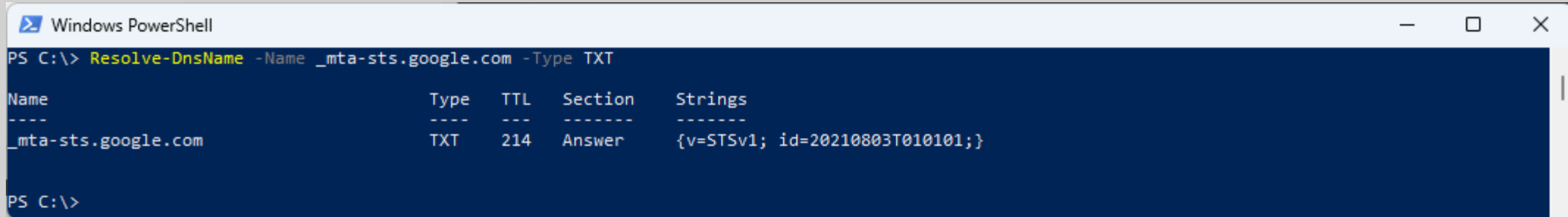
MTA-STS needs two things:

- 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;}
```





# MTA-STS Richtlinie

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

\$Domain = "microsoft.com"

\$URI = "https://mta-sts.\$Domain/.well-known/mta-sts.txt"

\$Response = Invoke-WebRequest -URI \$URI

\$Response.Content

## [MTA-STS Policy for Office 365](#)

version: STSv1

mode: enforce

mx: \*.mail.protection.outlook.com

max\_age: 604800

```
Windows PowerShell
PS C:\> $Domain = "microsoft.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: *.mail.protection.outlook.com
max_age: 604800
PS C:\>
```



# MTA-STS in Azure

Ich used Azure DevOps Starter (free) to host the GIT Repository

<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

root / .well-known / mta-sts.txt

mta-sts.txt

Edit

Contents History Compare Blame

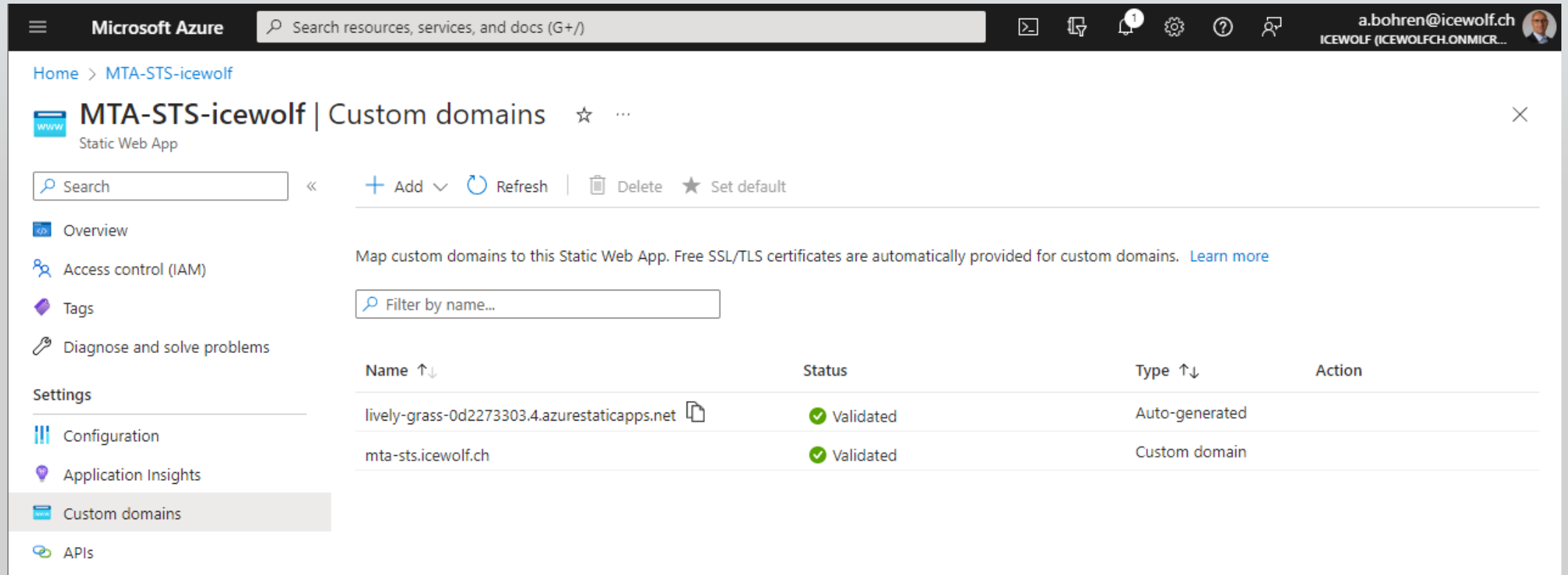
```
1 version: STSV1
2 mode: enforce
3 mx: *.mail.protection.outlook.com
4 mx: mail.icewolf.ch
5 max_age: 604800
```



# MTA-STS

A git push to the Repository triggers the Pipeline will start the deployment to the Azure Static Web App.  
Adding a custom domain will add a certificate in Azure Static Web App

- No Cost
- No Certificate Management



The screenshot shows the Microsoft Azure portal interface. At the top, the 'Microsoft Azure' logo and a search bar are visible. The user's profile 'a.bohren@icewolf.ch' is in the top right corner. The main content area displays the 'MTA-STS-icewolf | Custom domains' page for a Static Web App. The page includes a search bar, navigation links (Overview, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Application Insights, Custom domains, APIs), and a table of custom domains. The table has columns for Name, Status, Type, and Action. Two domains are listed: 'lively-grass-0d2273303.4.azurestaticapps.net' (Auto-generated) and 'mta-sts.icewolf.ch' (Custom domain), both with a 'Validated' status.

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



# Let's improve!

## Call to Action:

Let's make Email better and implement those well known Techniques to improve the Mailsecurity in Switzerland.



# Next Sessions



17:00

[Azure Automation and Microsoft Graph your dream team to find inactive and ownerless Microsoft Teams](#)

Thorsten Pickhan



17:00

[Building Intelligent Bots for Microsoft Teams with Azure OpenAI](#)

Nanddeep Nachan & Smita Nachan





# Brain exploded?

