p-square
IT Consulting & Managed Services

SMTP for DNS Admins

DDI User Group June 2025

Jens Hoffrichter

2025-06-26

About

Jens Hoffrichter

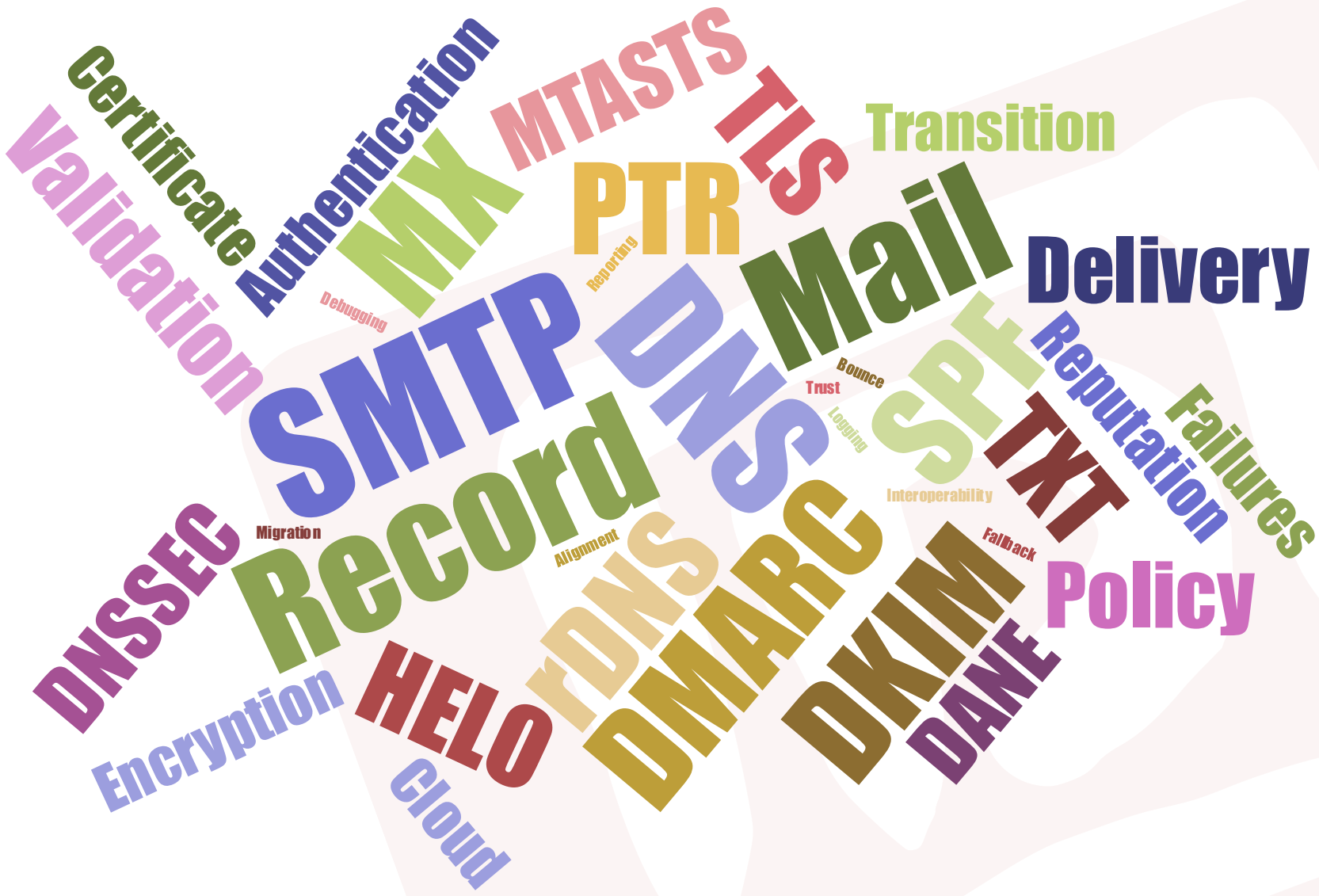
- Dipl.-Ing. (BA) in information technology, specialization in network and media technology
- One of two managing directors of p-square GmbH
- Having run SMTP and Internet DNS for a large automotive company for 10+ years as admin, later as operations manager

p-square

- Small specialized consulting and operations team for managed services and infrastructure, especially in DNS, DDI and SMTP

So many new records….

p-square
IT Consulting & Managed Services



Body vs Envelope

Testmail

From Jens <jens@hoffrichter.no> Monday
To jens.hoffrichter@p-square.de

Spoofing

From boss@ddiug.de on 2025-06-26 09:30
Details Headers

```
Hey Jens,

Just a quick test to see if this would pass through your filters. 😉
Best regards,
Boss
```

Spoofing (2)


```
Return-Path: <jens.hoffrichter@p-square.de>
X-Original-To: dmarc@p-square.dev
Delivered-To: dmarc@p-square.dev
Received: from localhost (localhost [127.0.0.1])
        by smtp (Postfix) with ESMTP id 68F65683685
        for <dmarc@p-square.dev>; Wed, 25 Jun 2025 15:09:35 +0200 (CEST)
From: boss@ddiug.de
To: jens.hoffrichter@p-square.de
Subject: Spoofing
Date: Wed, 26 Jun 2025 09:30:00 +0200
Message-ID: <spoof123@example.com>
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"

Hey Jens,

Just a quick test to see if this would pass through your filters. 😉
Best regards,
Boss
```

MX Records (Mail Exchangers)

dig mx hoffrichter.no

```
;; ANSWER SECTION:
hoffrichter.no.         600     IN      MX      20 mailsec.protonmail.ch.
hoffrichter.no.         600     IN      MX      10 mail.protonmail.ch.
```

- Looks up the domain from the RCPT TO (Envelope to)
- Shows the mail servers for this domains

PTR Records (Pointer)

dig mail.protonmail.ch

```
;; ANSWER SECTION:
mail.protonmail.ch.     1200    IN      A       185.205.70.128
mail.protonmail.ch.     1200    IN      A       176.119.200.128
mail.protonmail.ch.     1200    IN      A       185.70.42.128
```

dig PTR 128.70.205.185.in-addr.arpa

```
;; ANSWER SECTION:
128.70.205.185.in-addr.arpa. 1200 IN    PTR     mail.protonmail.ch.
```

- Mail servers have to have a PTR record
- The forward lookup on that domain should resolve to the same IP address
- IP shouldn’t be in a dynamic pool

SPF Records (Sender Policy Framework)

- SPF records are just specially styled TXT records
- SPF records designate which servers are allowed to send out mails for a specific domain

dig TXT hoffrichter.no

```
;; ANSWER SECTION:
hoffrichter.no.         300     IN      TXT     "protonmail-verification=b612d6036ec868aba690f662010fe9f6ed387413"
hoffrichter.no.         300     IN      TXT     "v=spf1 include:_spf.protonmail.ch mx -all"
```

dig TXT _spf.protonmail.ch

```
;; ANSWER SECTION:
_spf.protonmail.ch.     1200    IN      TXT     "v=spf1 ip4:185.70.40.0/24 ip4:185.70.41.0/24 ip4:185.70.43.0/24 ip4:79.13
5.106.0/24 ip4:79.135.107.0/24 ip4:109.224.244.0/24 include:_spf2.protonmail.ch ~all"
```

- -all is better than ~all (everything not in this list is not allowed)
- Limit of 10 DNS queries per SPF check (RFC 7208 / 4.6.4)
- Works on the ENVELOPE FROM or RETURN-PATH

DKIM (Domain Keys Identified Mail)

- Cryptographic signature of parts of the mail
- Public key is in DNS
- Domain which is used for signature is freely choosable (but alignment can be problematic -> more about this later)
- Message fields which are signed are in there

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=hoffrichter.no;
        s=protonmail; t=1750670143; x=1750929343;
        bh=JLYBBGbRjRBGEFnP/Br1oHs2o2aOKLDFcZ7ZSPJi76A=;
        h=Date:To:From:Subject:Message-ID:Feedback-ID:From:To:Cc:Date:
         Subject:Reply-To:Feedback-ID:Message-ID:BIMI-Selector;
        b=DmAvqnoQYTxk8g8taMKpMQVpi6n3fTM7mEJg9bFmNZMX2MO4br9BMY6VKFrMoJ460
         nRUvAA8ZfoFjvpDsbbd0INXO6rJuHwFlE8x5pGZNWMHuWWfApzV/pwfrALfGxtupOC
         DmnRx8BP28Yucex+nkQnqGkb0q55ialcFvkG+0knrisd4C6uDPeobxKCHwRi1P4q3Z
         uZqQCtfdAilgJ7qdmLg872aXcnH7L53435pK1xLHdnYRjAQ5GGqcIAW5wsQyZdmU1z
         BBI/YBzWN1wKFto0FdFMlZSojim3Xufz+Ot5fabzPhDWPZvbbjqyq6SVJHSStdi0pO
         Iif7F9qJh0OSQ==
```

DKIM (2)

- DKIM keys can always be found under <selector>._domainkey.<domain>
- Also just TXT records
- dig TXT protonmail._domainkey.hoffrichter.no

```
;; ANSWER SECTION:
protonmail._domainkey.hoffrichter.no. 300 IN CNAME protonmail.domainkey.dmrx5ylgmqa3um45kori5qd
wlml3kdmttps2jgbxbch5eltgqs47a.domains.proton.ch.
protonmail.domainkey.dmrx5ylgmqa3um45kori5qdwlml3kdmttps2jgbxbch5eltgqs47a.domains.proton.ch. 1
200 IN TXT "v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv+FVVDL8ZUM4eJjb+tv1tdD
LxefqMrVnauxAYS+scdCdjbpYl0Oc0APT59WJEW0wZOUqOZEb/58fCyvjivGGPpsbJuzxaYy8KjvGpOFZZF00Wcc7KOC/+6
1BEFBsnYv4MXenjW1e+Uxzq+4yVbPQqWB66vJIjTEdqnQ380o6tj5bIwQmx6N71ZOfNoxZ0tzyFSQ" "T/RWUqfWPJdlJkt
Xo/lXcZMQGMKMLDWzNgv1kMpAwR7GfDSkb3g6MRAMW4hVtVDbFkrsIGYorpL0hVw7I7GZFtRJXEjwcOl9rPOiwcatjII9zh
uEHydLdEhCjz2KCu0X8FPCx++FJ/yos8ZunpwIDAQAB;"
```

DMARC (Domain based message authentication…)

- TXT record which tells the receiving mail system what to do with emails which fail SPF check and DKIM check, or are not aligned
- Always under _dmarc.<domainname>
- Tell the receiving mail server where to send reports about failed mails to
- dig TXT _dmarc.p-square.de

```
;; ANSWER SECTION:
_dmarc.p-square.de.     120     IN      TXT     "v=DMARC1; p=none; rua=mailto:dmarc@p-square.dev"
```

- The domain receiving the reports (if not the same) needs to have another specific record
- dig TXT p-square.de._report._dmarc.p-square.dev

```
;; ANSWER SECTION:
p-square.de._report._dmarc.p-square.dev. 3600 IN TXT "v=DMARC1"
```

DMARC (2)

- p=reject is really what to strive for in any domain
- Difficult for domains with marketing domains, and grown usage

- Not everyone sends out DMARC reports (Microsoft e.g. still doesn't send out reports)
- RUF reports are very problematic on a data privacy level – if someone asks you to add those records, be sure that is allowed

SPF & DKIM alignment

- This is a new requirement when DMARC validation comes into play
- Traditionally, SPF was validated on the Envelope MAIL FROM or RETURN-PATH domain
- DKIM is validated on the d= attribute of the DKIM signature
- But for DMARC validation, at least one of those domains need to align to the Header From, otherwise DMARC will fail

	DMARC RESULT	FROM:DOMAIN (DMARC)	DKIM DOMAIN (DKIM)	ENVELOPE_FROM / RETURN-PATH (SPF)
Full Alignment	✓	@client.net	@client.net	@client.net
DKIM Only	✓	@client.net	@client.net	@sample.net
SPF Only	✓	@client.net	@sample.net	@client.net
Fail	✗	@client.net	@sample.net	@sample.net

(Table from dmarcadvisor.com)

Why does this matter?

- Business often argues that there is no value in setting up SPF and DMARC, as it does nothing for inbound and legitimate outbound mails

But:

- Increases reputation for a domain and mail server -> Better chance of hitting Inbox for mail users, instead of “Other” or even Spam
- Gmail, Yahoo, Hotmail and outlook.com requires it for mail domains which at any point in time have send more than 5000 mails to their servers in a day
- Will most likely be industry standard in the near future

Best practices for mail domains

- Tight SPF records – only have the mail servers in there you need, audit regularly
- Ending of an SPF record is important
  - An SPF record with ~all is nice, but doesn't do much
  - An SPF record with ?all could as well not exist
  - Look to implement –all
- DKIM should be standard these days.
  - Recommendations are that DKIM keys should be rotated every 6 months
- DMARC with p=reject should be the goal, but can be difficult to achieve
- DNSSEC should be activated for all DNS domains, so DANE can be activated (upcoming slides)

Best practices for non-mail domains

- E-Mail admins often don’t think about all the other domains, as they are out of scope for their work
- Domains not sending emails should have an empty SPF record, and a reject DMARC record
- Domains not receiving email should have a NullMX records

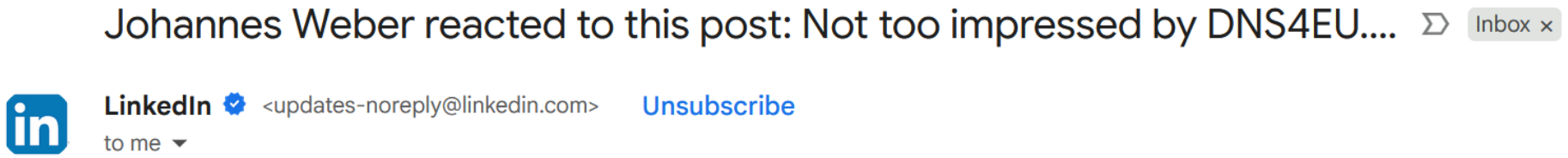
```
p2-server.de              IN      TXT     "v=spf1 -all"
p2-server.de              IN      MX      .
_dmarc.p2-server.de       IN      TXT     "v=DMARC1; p=reject"
```

- Further reading: BSI TR-03182 Email Authentication

(Note: MX in figure above should contain a priority before the ., and should read:
p-server.de IN MX 0 .)

BIMI / VMC (Brand Indicators for Message Identifi…)

- Makes it possible to show the brand logo next to messages for popular companies



- Used for showing visual legitimacy of emails to users
- Supported by most freemailing systems, but not Office 365
- Needs a registered picture trademark
- Needs DMARC with p=quarantine or p=reject
- Needs a signed verified mark certificate (~1000 USD)

DANE (DNS-Based Authentication of Named Entities)

- Adds a TLSA record with the fingerprint of the certificate of the service being called
- Does only work if DNSSEC is enabled for the recipient domain and MX server domain
- Provides strong indication of authenticity and integrity for a connection, even over opportunistic TLS
- Relatively low spread
- dig TLSA _25._tcp.mxext1.mailbox.org

```
;; ANSWER SECTION:
_25._tcp.mxext1.mailbox.org. 3600 IN    TLSA    3 1 1 4758AF6F02DFB5DC8795FA402E77A8A0486AF5E85D2CA
60C294476AA DC40B220
_25._tcp.mxext1.mailbox.org. 3600 IN    TLSA    3 1 1 996AD31D65E03F038B8EC950F6F26611529DA03E3A283
E4400CBA2ED D04B8A88
_25._tcp.mxext1.mailbox.org. 3600 IN    TLSA    3 1 1 E41CC7633029AFDBA53744D7E5FC31EF507E592DE9DFB
33557BF3B9A 79239446
```

MTA-STS (Mail Transfer Agent Strict Transport Se…)

- Competing protocol to DANE
- Enforces TLS for supporting MTAs
- Lower authenticity confidence than with DANE (Needs external CA trust)
- Public key is published via HTTPS
- No DNSSEC implementation necessary
- dig TXT _mta-sts.mailbox.org

```
;; ANSWER SECTION:
_mta-sts.mailbox.org.   300     IN      TXT     "v=STSv1;" "id=20181001090000"
```

MTS-STS (2)

- curl https://mta-sts.mailbox.org/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
max_age: 2419200
mx: *.mailbox.org
mx: mx1.mailbox.org
mx: mx2.mailbox.org
mx: mx3.mailbox.org
mx: mxtls1.mailbox.org
mx: mxtls2.mailbox.org
```

TLS Reporting

- Useful when using enforced TLS to get reports about failed TLS connections, DANE problems, MTA-STS problems etc.
- Get daily JSON reports from supported sending servers about TLS problems

- dig TXT _smtp._tls.mailbox.org

```
;; ANSWER SECTION:
_smtp._tls.mailbox.org. 3600    IN      TXT     "v=TLSRPTv1;rua=mailto:abuse@heinlein-support.de"
```

- Needs a parser able to read the reports