

howto, dmarc, dkim, spf, mailserver, email, dig, dns

# DMARC

- <https://dmarc.org/2015/08/receiving-dmarc-reports-outside-your-domain/>
- <https://mxtoolbox.com/DMARCRecordGenerator.aspx?>
- [https://mxtoolbox.com/problem/dmarc/dmarc-external-validation?page=prob\\_dmarc](https://mxtoolbox.com/problem/dmarc/dmarc-external-validation?page=prob_dmarc)
- <https://dmarcadvisor.com/de/was-ist-external-destination-verification/>

```
#MX
dig -t MX +noall +answer netzwerkforensik.com
dig +noall +answer netzwerkforensik.com
```

netzwerkforensik.com.	150	IN	MX	5 smtpin.rzone.de.
smtpin.rzone.de.	1800	IN	A	81.169.145.97

```
# SPF
dig -t txt +noall +answer _spf.strato.com
dig -t txt +noall +answer netzwerkforensik.com
```

_spf.strato.com.	3600	IN	TXT	"v=spf1 ip4:81.169.146.128/25 ip4:85.215.255.0/24 ip6:2a01:238:20a:202::0/64 ip6:2a01:238:400::0/48 ip4:81.169.144.153 ip6:2a01:238:20a:202:50ff::153 -all"
------------------	------	----	-----	-------------------------------------------------------------------------------------------------------------------------------------------------------------

netzwerkforensik.com.	150	IN	TXT	"v=spf1 include:_spf.strato.com mx -all"
-----------------------	-----	----	-----	------------------------------------------

```
#DKIM Selector 1
dig -t txt +noall +answer strato-dkim-0002._domainkey.netzwerkforensik.com
```

strato-dkim-0002._domainkey.netzwerkforensik.com.	150	IN	TXT	"v=DKIM1; k=rsa; p=MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt3a1nbhQdD0MtbPT1r8DGZeFoQlj3fSgtWdINsXsRl550m0Af2QNR8B0SwC59dWqA+isuH/bQnU0f00m05A7p+cyfT9EekbWslP575NANAYpsUJlBv/008qa6T/cLoDz6LSUYv000gFRqSSUe1BZnJ/sjg0f96UCko mT1aQRpSUSDwNYCqpQKQ/fWg9IS2fL+" "d2kR1rckqwoKdgbEtjr4i+ICn2SUodI1KkGusIivuBueMYfDh8RGYKvFv40UZlBSfuX71GkzEPvQPnQTfXLqM9F8q1kWq/mdWYy5R0K rWptAnuAmCZqujkgWmcqzLoTmln04o0xGFp/zkf8iA75lwIDAQAB"
---------------------------------------------------	-----	----	-----	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

```
#DKIM Selector 2
dig -t txt +noall +answer strato-dkim-0003._domainkey.netzwerkforensik.com
```

strato-dkim-0003._domainkey.netzwerkforensik.com.	150	IN	TXT	"v=DKIM1; k=ed25519; p=hB4fid01tsRNeRkj6ySb9N2xwfNzERRFYLQhGQyQ9dE="
---------------------------------------------------	-----	----	-----	----------------------------------------------------------------------

```
#DMARC
dig -t txt +noall +answer _dmarc.netzwerkforensik.com
dig -t txt +noall +answer netzwerkforensik.com._report._dmarc.wiretrip.de
```

_dmarc.netzwerkforensik.com.	150	IN	TXT	"v=DMARC1; p=quarantine; rua=mailto:dmarc-report@wiretrip.de; ruf=mailto:postmaster@wiretrip.de; sp=reject; fo=0:1:d:s; pct=100; aspf=s"
------------------------------	-----	----	-----	------------------------------------------------------------------------------------------------------------------------------------------

netzwerkforensik.com._report._dmarc.wiretrip.de.	43200	IN	TXT	"v=DMARC1;"
--------------------------------------------------	-------	----	-----	-------------

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
```

```
<report_metadata>
  <org_name>google.com</org_name>
  <email>noreply-dmarc-support@google.com</email>
  <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
  <report_id>6934733341335759686</report_id>
  <date_range>
    <begin>1697673600</begin>
    <end>1697759999</end>
  </date_range>
</report_metadata>
<policy_published>
  <domain>netzwerkforensik.com</domain>
  <adkim>r</adkim>
  <aspf>s</aspf>
  <p>quarantine</p>
  <sp>reject</sp>
  <pct>100</pct>
  <np>reject</np>
</policy_published>
<record>
  <row>
    <source_ip>81.169.146.220</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>pass</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>netzwerkforensik.com</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>netzwerkforensik.com</domain>
      <result>pass</result>
      <selector>strato-dkim-0002</selector>
    </dkim>
    <dkim>
      <domain>netzwerkforensik.com</domain>
      <result>fail</result>
      <selector></selector>
    </dkim>
    <spf>
      <domain>netzwerkforensik.com</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
</feedback>
```

Der Fail in Zeile 43 kommt vermutlich vom zweiten Selector 0003 weil das kein RSA sondern ED25519 Zertifikat ist und google das noch nicht unterstützt. Sollte aber neutral bewertet werden - also Selector 1: pass und Selector 2: neutral.

~~DISCUSSION~~

From: <https://wiki.nanoscopic.de/> - nanoscopic wiki

Permanent link: <https://wiki.nanoscopic.de/doku.php/pages/howtos/mailserver/dmarc?rev=1697982021>

Last update: 2023/10/22 13:40

