

[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://dmarcadvisor.com/de/was-ist-external-destination-verification/>

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

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

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

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

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

```
<?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>
</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=1697981468>

Last update: 2023/10/22 13:31

