MTA Strict Transport Security
SMTP TLS Reporting
IETF 100
Nicolas Lidzborski <nlidz+ietf@google.com>
Current Drafts

- **SMTP MTA Strict Transport Security**
  - [Draft-ietf-uta-mta-sts-11](#)

- **SMTP TLS Reporting**
  - [Draft-ietf-uta-smtp-tlsrpt-11](#)
Known Current Efforts

- Google (gmail.com, googlemail.com, google.com)
  - Send-time policy fetching & validation in progress
- Comcast (comcast.net)
  - Live policy ([https://mta-sts.comcast.net/.well-known/mta-sts.txt](https://mta-sts.comcast.net/.well-known/mta-sts.txt))
- Yahoo (yahoo.com)
- 1&1 (web.de, gmx.net, gmx.com and mail.com)
- Microsoft (live.com)
  - DNS record and policy publication work in progress
STS in 60 Seconds...

1. TXT record

$ dig -t txt +short _mta-sts.gmail.com

"v=STSv1; id=20171114T070707;" 

2. HTTPS endpoint with policy

$ curl https://mta-sts.gmail.com/.well-known/mta-sts.txt

version: STSv1
mode: report
mx: gmail-smtp-in.l.google.com
mx: .gmail-smtp-in.l.google.com
max_age: 86400

Semantics:

● HTTPS cert validation
● HSTS-style policy cache
● Mode: "none", "report" or "enforce"
Quick summary of MTA-STS work

- HTTPS policy in https://mta-sts.example.com/.well-known/mta-sts.txt
- Policy format with key-value pairs (originally JSON)
- DNS policy ID MUST uniquely identify a given policy
- MTAs MUST support TLS 1.2 or later
- SMTP client and HTTPS server MUST support TLS SNI
- SNI extension of HTTPS MUST have name of the policy host
- SNI extension of SMTP server MUST contain MX hostname
- Operational considerations:
  - Policy updates (update the HTTPS policy body before TXT RR)
  - Policy delegation using CNAME
  - Policy removal
- DoS attack mitigations
TLSRPT in 30 seconds...

1. TXT record

```
$ dig -t txt +short _smtp-tlsrpt.gmail.com.
"v=TLSRPTv1;rua=mailto:sts-reports@google.com"
```

2. Reports
   (HTTPS POST or SMTP)

```
"result-type": "validation-failure",
"sending-mta-ip": "47.97.15.2",
"Receiving-mx-hostname": "mx-backup.mail.company-y.com",
"failed-session-count": 3,
"failure-error-code": "X509_V_ERR_PROXY_PATH_LENGTH_EXCEEDED"
```
Quick summary of TLSRPT draft work

- DNS TLSRPT entry in TXT RR for _smtp-tlsrpt.example.com
- Supports both MTA-STS and DANE
- SMTP reports MUST have DKIM signature
- DKIM signature MUST NOT use the "l=" attribute (length)
- Report plain text file encoded in the I-JSON format
- Generic errors as "validation-failure" with "failure-reason-code"
- Report media type, Subject and filename recommendation
- Report GZIP compression
- Delivery retry for 24h
Closed Issues

- Clarified 302 redirects and cache-control.
- policy-to-SAN matching vs policy-to-hostname matching: policy-to-SAN (needed by DANE [RFC7672])
- TLS 1.2: MTAs MUST have support for TLS version 1.2 or better
Open Issues

Other feedback? (Clarity, operational, deployment?)

Time for last call?