

MTA Strict Transport Security

SMTP TLS Reporting

IETF 96

Dan Margolis <dmargolis@google.com>

Current Drafts

- SMTP MTA Strict Transport Security
 - [draft-ietf-uta-mta-sts-01](#)
- SMTP TLS Reporting
 - [draft-ietf-uta-smtp-tlsrpt-01](#)

STS in 60 Seconds...

1. TXT record

```
$ dig -t txt +short _mta_sts.example.com.
```

```
"v=STSV1\; id=20160707T010757\";
```

2. HTTPS endpoint with policy

```
$ curl https://policy.mta-sts.example.com/.well-known/mta-sts/current
```

```
{  
  "version": "STSV1",  
  "mode": "report",  
  "policy_id": "20160707T010757",  
  "mx": ["*.mail.example.com"],  
  "max_age": 123456  
}
```

Semantics:

- HTTPS cert validation
- HSTS-style policy cache
- "Report" or "enforce"

Draft Version 00 - Closed Issues

[Draft Version 00 - Closed Issues](https://github.com/mrisher/smtp-sts/milestone/1?closed=1)

<https://github.com/mrisher/smtp-sts/milestone/1?closed=1>

Major changes:

1. Standalone spec for reporting ("TLSRPT")

<https://tools.ietf.org/html/draft-ietf-uta-smtp-tlsrpt-01>

```
$ dig -t txt +short _smtp_tlsrpt.example.com.
```

```
"v=TLSRPT1\;rua=mailto:sts-reports@example.com |
```

2. Simplified STS TXT record (no policy, only version)

```
DNS: "v=STSV1\; id=20160707T010757\;"
```










```
HTTPS: { /*...*/ "policy_id": "20160707T010757" /*...*/ }
```

3. Eliminated DNSSEC policy validation, TLSA cert validation

See <https://github.com/mrisher/smtp-sts/wiki/Why-not-support-DNSSEC>











Draft Version 01 - Closed Issues

- [Draft Version 01 - Closed Issues](https://github.com/mrisher/smtp-sts/milestone/2?closed=1) <https://github.com/mrisher/smtp-sts/milestone/2?closed=1>

🔔 0 Open ✓ 12 Closed	
 Does DNS record dtext really need to support uppercase? #56 opened 4 days ago by eyeofthenico	💬 2
 max_age specified value should not have double quotes #53 opened 4 days ago by eyeofthenico	
 max_age should be marked as required #52 opened 4 days ago by eyeofthenico	💬 1
 policy_id should be marked as required #51 opened 4 days ago by eyeofthenico	
 Define the 'rua' parameter in section 3.1.1 #49 opened 5 days ago by lbaudoin	💬 1
 _mta_sts ID field is limited to 20 chars, should be 25 #48 opened 6 days ago by mrisher	

Draft Version 01 - Closed Issues (cont)

- [Draft Version 01 - Closed Issues](#)

 mailto uses wrong syntax in example #47 opened 6 days ago by mrisher	
 inconsistency around .well-known in the spec #46 opened 6 days ago by mrisher	
 max_age should not be in quotes #45 opened 6 days ago by mrisher	
 The DNS TXT record is underspecified and unparsable. #44 opened 13 days ago by lbaudoin	
 Incorrect ABNF character range for 'dtext' #42 opened 22 days ago by lbaudoin	 1
 Editorial fixes for policy syntax #36 opened on May 10 by danmarg	 1

Open Issues

<https://github.com/mrisher/smtp-sts/issues>

Questions:

1. HTTPS location (policy.mta-sts.example.org vs mta-sts.example.org)?
2. Smarthost policy (that of the smarthost owner domain, presumably)?
3. Follow HTTPS redirects on policy location?
4. Move .well-known/.../current -> .well-known/.../\$id.json?

Other feedback? (Clarity, operational, deployment?)

Known Current Efforts

- Google
 - Policy is live (<https://policy.mta-sts.gmail.com/.well-known/mta-sts/current>)
 - Send-time policy fetching & validation in progress (target Q3)
- Microsoft
 - Policy publication in progress
- Comcast
 - Policy DNS live; HTTPS in progress
 - Report processing planned
- Yahoo
 - DNS record and policy publication target Q3
 - Report-only mode in progress
- 1&1
 - Report-only mode target this summer
- Others?

TLSRPT in 5 seconds...

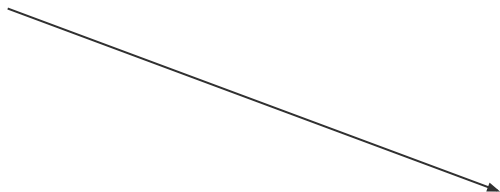
1. TXT record



```
$ dig -t txt +short _smtp_tlsrpt.example.com.
```

```
"v=TLSRPT1\;rua=mailto:sts-  
reports@example.com"
```

2. Reports



```
[{  
  "result-type":  
    "StarttlsNotSupported",  
  "sending-mta-ip": "98.22.33.99",  
  "receiving-mx-hostname": "mx2.mail.  
company-y.com",  
}]
```

References

FAQ: <https://github.com/mrisher/smtp-sts/wiki/FAQ> (<https://git.io/vVW6t>)

Why not DNSSEC for policy validation? <https://github.com/mrisher/smtp-sts/wiki/Why-not-support-DNSSEC>