SMTP Strict Transport Security
IETF 95
Mark Risher <risher@google.com>
Downgrades and interception a problem
Reporting valuable, sometimes sufficient
DNSSEC not (yet) universal
SMTP STS: Failure reporting & enforcement for large and small domains
Desired Properties

1. Deployable without DNSSEC
2. Suitable for multi-domain hosting
3. “Report-only” possible without MTA changes
4. Minimal “wheel-reinvention”
Some of the Issues:

1. DNSSEC and DANE interop
2. Distribution
3. Reporting
DNSSEC and STS in draft-00

Authenticate policies via \texttt{a=dnssec} or \texttt{a=webpki}

Validate policies via \texttt{c=tlsa} or \texttt{c=webpki}
Proposed Edits for DNSSEC and hosting

- Remove DANE-based MX validation ("c=tlsv")?
- Remove DNSSEC-based policy authentication ("a=dnssec")?
- Remove policy from DNS
- Move cache control to HTTPS Cache-Control?

Current

```
dig TXT _smtp_sts.example.com

"v=STS1; to=false; c=tlsv; a=dnssec; mx=*.host.com; rua=mailto:sts-feedback@example.com"
```

Possible

```
https://policy._smtp_sts.example.com
Cache-Control:public, max-age=# medium

v=STS1
to=false
mx=*.host.com
e=# long policy validity
```
Chris Newman on In-Band Distribution

“DEEP uses deployed cert validation for in-protocol SMTP submission policy.

Can SMTP STS use in-protocol model?”
Options on Reporting Formats

Standalone specification?

XML vs. JSON?

Reuse some generalized format?

Split into its own spec

Reporting granularity and specificity
Working Group?
Potential Future Work

Working group

Forensic reports

Certificate Pinning (RFC7469)

Recipient-to-sender reporting & enforcement

Certificate Transparency as distribution/reporting (RFC6962)
References


