Network Working Group
Internet-Draft
Intended status: Informational
Expires: 18 October 2025

G. Nitzsche
Private Contributor
19 April 2025

Enforcing DNSSEC via HTTPS: Combining DANE and MTA-STS
draft-frickl-mta-sts-dnssec-policy-02

Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Title: Enforcing DNSSEC via HTTPS: Combining DANE and MTA-STS

Abstract

This document proposes a minimal, backward-compatible extension to the SMTP MTA-STS policy format by adding an optional field "dnssec:" to indicate whether the recipient domain operator expects DNSSEC validation to be active. This allows sending MTAs to detect silent DNSSEC stripping attacks and apply more secure delivery behavior accordingly. The mechanism leverages the existing HTTPS-secured delivery channel of MTA-STS and does not require changes to the DNS infrastructure or SMTP protocol.

Table of Contents

1. Introduction

SMTP MTA Strict Transport Security (MTA-STS) [RFC8461] provides a secure channel for recipient domains to signal their TLS policy over HTTPS. However, it was explicitly designed without relying on DNSSEC [RFC4033], and does not provide a way to declare DNSSEC expectations. On the other hand, DANE [RFC7672] clients rely on DNSSEC to activate validation. If DNSSEC data is suppressed via MITM attacks on the resolver path, DANE is not used at all. The result is not a failed DANE validation, but rather its absence--leaving the sender to fall back to opportunistic delivery.

This document proposes a simple extension to the MTA-STS policy file format to include a "dnssec: yes" directive, enabling recipient domains to declare their DNSSEC deployment status explicitly. Sending MTAs can use this signal to enforce DNSSEC validation and abort or defer delivery in the absence of signatures.

2. Policy Semantics

The semantics of the ‘dnssec:‘ field are as follows:

- "yes": The domain operator expects DNSSEC signatures to be available.
- Other values are undefined and MUST be ignored.

Note that when ‘dnssec: yes‘ is present, clients MAY still evaluate the TLS-related fields in the policy (e.g., ‘mode‘, ‘mx‘, etc.), depending on local policy or implementation logic. This allows for mixed-mode policies that signal DNSSEC expectations while retaining compatibility with traditional MTA-STS behavior.

Clients SHOULD also respect ‘max_age‘ and associated caching behavior as defined in the MTA-STS specification.

3. Sender MTA Behavior

Sending MTAs that support this HTTPS-based DNSSEC policy signaling (e.g., "dnssec: yes") MUST perform DNSSEC validation when retrieving delivery-related DNS records. In that case, if DNSSEC data is missing, they MUST treat the DNS data as potentially tampered and MUST:

- defer delivery (e.g., treating as a 450 temporary failure),
- or report a permanent failure.

They MUST NOT attempt fallback delivery using opportunistic TLS or plaintext. This is to prevent downgrade attacks and preserve the intent of the recipient domain.

This mechanism is intentionally isolated from traditional MTA-STS semantics and acts as an extension to DANE-style validation by providing an authenticated hint via HTTPS that DNSSEC enforcement is expected. Implementations MAY refer to this mechanism as "DANE-STS" or another suitable designation when referencing this policy layer.

4. Example Policy File

A typical MTA-STS policy file with the extended DNSSEC directive might look like this:

```
version: STSv1
mode: enforce
mx: mail.example.com
max_age: 86400
dnssec: yes
```

This example shows the introduction of the new ‘dnssec‘ field in the context of a valid and complete MTA-STS policy. The field is interpreted only by clients that support this specification. All others will ignore it.

5. Deployment Considerations

While it is theoretically possible to publish DNSSEC enforcement expectations directly within the DNS zone (e.g., via custom TXT records or DNSSEC-based flags), this method cannot provide equivalent security to the HTTPS-based signaling described in this document. Due to the nature of DNS over UDP and its susceptibility to spoofing, race conditions, and cache poisoning, any DNS-only flag remains vulnerable to manipulation--especially in scenarios where the attacker has visibility into or control over authoritative DNS traffic--which is precisely the kind of MITM threat that DANE aims to eliminate. HTTPS over TCP provides a significantly more robust and authenticated channel for delivering such policy hints, making it the preferred mechanism in this context.

Encrypted DNS protocols such as DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) can protect the client-to-resolver path, but offer no protection between the resolver and the authoritative name servers. Therefore, an attacker with access to authoritative DNS traffic--or any point on the resolution chain beyond the client--can still suppress or strip DNSSEC records. This underscores the value of HTTPS-based signaling to ensure policy integrity.

This attack scenario also applies to setups described in [DNSCurve], where a passive observer of upstream DNS traffic can forge unsigned responses that arrive before the legitimate DNSSEC-signed ones. Without a signal like the one proposed here, such attacks remain undetected.

While it would be technically possible to introduce a separate well-known HTTPS endpoint (e.g., ‘https://dane-sts.example.com/.well-known/dane-sts.txt‘) for DNSSEC-related policy signaling, this specification deliberately reuses the existing MTA-STS infrastructure. The MTA-STS mechanism is already widely deployed, benefits from mature tooling and operational experience, and provides an authenticated HTTPS channel suited for policy distribution. Leveraging this existing framework reduces complexity, avoids redundant infrastructure, and allows operators to manage transport-related policies in a unified location--even if traditional MTA-STS and DANE are generally intended as mutually exclusive strategies.

6. Security Considerations

The HTTPS-based delivery of the MTA-STS policy protects this metadata from DNS manipulation. This makes the "dnssec:" field resistant to MITM attacks that affect DNS-only channels. However, this mechanism does not protect against forged or misconfigured HTTPS certificates on the policy endpoint.

This proposal mitigates the risk of DNSSEC downgrading by forged DNS reply packets, which could otherwise remain undetected by SMTP senders.

7. IANA Considerations

This document does not require any IANA actions.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

[RFC8461] Margolis, D., et al., "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018.

[RFC7672] Dukhovni, V., "SMTP Security via Opportunistic DANE TLS", RFC 7672, DOI 10.17487/RFC7672, October 2015.

8.2. Informative References

[RFC4033] Arends, R., et al., "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005.
[DNSCurve] Bernstein, D. J., "Forged DNS Responses", https://dnscurve.org/forgery.html

Author’s Address:
Gunther Nitzsche
Private Contributor
Email: gn@frickl.de

NOTE: This draft is intended for discussion and feedback within the DANE and DNSOP communities. Feedback is highly welcome before potential submission as -02 or for adoption.