Independent Stream W. Chuang
Internet-Draft A. Robinson
Intended status: Experimental B. Nan
Expires: 19 August 2026 Google, Inc.
15 February 2026

Mutual TLS for Email Authentication
draft-chuang-mutual-tls-email-authentication-00

Abstract

Valid client and server TLS certificates authenticate the traffic coming from the SMTP sending and receiving servers. Domain owners can delegate email sending and receiving to servers using Mail eXchange (MX) DNS resource records. This enables transitive authentication of mail traffic from sending and receiving domains of envelope sender much like Sender Policy Framework and the envelope recipient. This document also proposes an Automatic Certificate Management Environment responder using these DNS records to automate TLS certificate issuance.

Table of Contents

1. Introduction

Simple Mail Transfer Protocol (SMTP) [RFC5321] supports delivery of Internet email messages. TLS encrypts and authenticates socket connections by building upon the X.509/PKIX [RFC5280] certificate trust system. SMTP leverages TLS to encrypt and authenticate email transport. The client and server TLS certificates identify the server name as a subject hostname and associate the traffic coming from SMTP sender and receiver servers via the private key used to establish the TLS connection. SMTP TLS end-entity certificates hold the subject name validated by a Certificate Authority (CA). Evidence of this validation is by certificate issuance, typically from an intermediate CA that is itself issued from a root CA. The SMTP TLS transaction counterparty, be it the receiver or sender, can validate the issuance to a root CA that it trusts thereby is able to trust the content of the entity certificate. The counterparty can then trust that the TLS traffic is coming from the identified hostname of the sender or receiver.

Once the TLS authenticated sender or receiver is established, this document describes a process by which we can associate and verify the SMTP envelope sender and recipient. This corresponds to the address given in the SMTP MAIL FROM and RCPT TO. The association is done through Client and Server DNS Mail eXchange (MX) resource records corresponding to the sending and receiving SMTP server. This document just further specifies the name of the SMTP [RFC5321] MX record to Server MX to distinguish from the Client MX specified in this document. These MX records are published by the domain owner to indicate the delegated mail servers that handle message delivery on its behalf. The Server MX is used to discover the receiving mail delivery server as described in [RFC5321], and also specifies the permitted hostnames that may be present in the Server TLS certificates. The Client MX specifies the permitted hostnames that may be present in the Client TLS certificates. Publication of Client MX indicates adherence and consent to validation using the methods in this specification. Verification of SMTP envelope MAIL FROM sender domain is analogous to the Sender Policy Framework (SPF) [RFC7208] sender but uses TLS instead of IP addresses. Verification of client and server TLS certificates permits the mutual verification of both the sender and receiver which is analogous to the mTLS in other applications such as HTTP specified in [RFC8120].

To encourage further adoption of SMTP TLS especially in light of recent server certificate policy changes, this also specifies extending an Automatic Certificate Management Environment (ACME) [RFC8555] validation responder using Server and Client MX. This enables supporting delegation through the MX lookup where the ACME HTTP responder is present at the hostname.

1.1. Terminology and Definitions

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].

1.2. Client and Server Validation

This document defines a procedure for validating the authenticity of traffic sent from and to the SMTP sender and recipient Mailbox domains using SMTP TLS.

1.2.1. Client and Server MX

This document refers to MX DNS records defined in [RFC1035] to be Server MX records that help differentiate against the Client MX record specified in this document. This document defines a Client MX record with a distinct resource record type as defined by IANA Resource Record TYPE registry. The Client MX record has the same format as Server MX records as defined in Section 3.3.9 of [RFC1035].

SMTP [RFC5321] defines mail delivery between a SMTP sender and recipient represented by their respective email addresses. The structure of an email address into local-part@domain where this domain is considered the Mailbox domain. Section 5 defines the process of resolving the Mailbox domain into server hostname domain using the MX record mapping. There may be multiple MX records found resulting in multiple hostnames when resolving the Mailbox domain.

Any domain accepting email delivery publishes one or more server MX records, however this does not indicate any sort of usage of SMTP TLS, or usage of TLS certificates issued by a public CA with valid hostname alignment. Because of this, using TLS certificates for email authentication is risky. Instead this document specifies an opt in process using publication of the Client MX record. When a domain publishes one or more Client MX records, this indicates that the domain agrees to use the specification in this document to validate its servers’ hostname identities. Compliant SMTP servers MUST support TLS, and the SMTP TLS certificates must be issued from a valid public CA. In addition the SMTP sending and receiving server hostnames MUST match the appropriate Server or Client MX hostnames as defined later.

1.2.2. TLS Certificate Validation

SMTP TLS socket sessions will exchange client and server TLS certificates corresponding to the sending and receiving servers. The counter party receiving and sending server MUST validate the end-entity certificates using the path validation procedures in [RFC5280] Section 6. The validator MAY check other certificate profile information such as public key algorithm and key size, signature algorithm and key size, Key Usage, Extended Key Usage, Policy, Certificate Transparency [RFC6962] and other information according to local-policy. When the sender’s server TLS certificate validation fails, it checks if the receiver has published Client MX records that indicate adherence to this protocol. If found, it closes the SMTP TLS socket to prevent Man-In-The-Middle. When the receiver’s client TLS certificate validation fails, it checks if the sender has published Client MX records. If so and according to local-policy, the receiver either MAY choose to report an authentication failure or MAY otherwise close the SMTP TLS socket with a SMTP error. A valid TLS certificate defines one or more server hostnames as either Subject Alternative Name extension dnsNames otherwise Subject Distinguished Name common names.

1.2.3. Hostname Validation

[RFC5321] defines the SMTP sender and recipient with the corresponding sender and recipient Mailbox domain. After TLS Certificate Validation, the validator resolves the SMTP Mailbox domain to a set of server hostnames and one of the server hostnames MUST exactly match one of the corresponding TLS certificate hostnames. One of the receiver MX defined hostnames MUST exactly match one of server TLS certificate hostnames. If it does not match, then the sender looks up the receiver Client MX certificate. If found, it closes the SMTP TLS socket to prevent Man-In-The-Middle. Similarly one sender MX defined hostnames MUST exactly match client TLS certificate hostnames. If it does not match, then the receiver looks up the sender Client MX. If so and according to local policy, the receiver MAY either choose to report an authentication failure or otherwise MAY close the SMTP TLS socket with a SMTP error.

TODO: discuss strict hostname alignment.

1.2.4. Validation Results

Receivers check the result of client TLS certificate passes path validation and hostname matching. If both pass, then the authentication result is a pass, otherwise it is a fail. Because this validates the authenticity of the SMTP sender Mailx domain which is the same as the MAIL FROM Mailbox domain, this MAY be used in the same way as SPF authentication. This document modifies Domain-based Message Authentication, Reporting, and Conformance (DMARC) [RFC7489] to permit this result to be substituted for SPF.

Upon completion of a successful SMTP transaction, the receiver MAY report the result of the sender validation in Authentication-Result [RFC8601]. The method name is "mtls". The status results:

* PASS: client TLS certificate passes path validation and hostname matching

* FAIL: fails either TLS certificate path validation or hostname matching

1.3. ACME for SMTP TLS

This document specifies extending ACME [RFC8555] validation responder using Server and Client MX. The ACME client MAY request to the CA that it use SMTP Client or Server MX DNS record lookup for discovering the ACME HTTP verification responder at the location of the SMTP servers. Publication of the MX record demonstrates the domain owners delegation to the SMTP servers. As there are multiple possible MX records, this supports multiple servers.

This modifies ACME to support two new challenges corresponding to Client and Server MX. They are identified by ACME challenge type "client-mx-http-01" and "server-mx-http-01". The CA is given a domain and respectively uses Client or Server MX lookup. The CA provides a path at which a set of validations identifiers will present. The CA resolves the domain using [RFC5321] section 5 to hostnames and then iterates over the MX hostnames. For hostname it looks up the identifier at the path specified using HTTP as specified in [RFC8555] section 8.3. The rest of the interface and interaction between the ACME client and CA is the same as the HTTP challenge method.

1.4. Security Considerations

This proposes a new email authentication protocol that reduces some of the risk of the SPF by simplifying the delegation process to the well understood DNS MX lookup. SPF uses a rich policy specification with features like the include mechanism, macros and policy qualifiers that have caused permitted spoofing vulnerabilities. The identification foundation of this protocol leverages the existing and very well understood TLS, and most senders and receivers have deployed SMTP TLS. It also encourages adoption of PKIX/X.509 best practices linking SMTP TLS to email authentication.

This protocol puts further weight on the security of TLS for email communication and the email community SHOULD understand the changes and challenges there. For example there is significant TLS/PKIX IETF work in Post Quantum Cryptography.

1.5. IANA Considerations

NOTE: These values are just INFORMATIVE placeholders for discussion of this draft. No such registrations have been done.

IANA maintains a registry of Resource Record (RR) TYPEs under the category of Domain Name System (DNS) Parameters. This document proposes a new Resource Record (RR) TYPEs called "client mail exchange" as value 265. This proposes naming "mail exchange" value 15 to "server mail exchange".

This also proposes modifying the ACME Identifier Types registry to include two new types:

* label: "server-mx-http-01"

* label: "client-mx-http-01"

This also proposes extending the Email Authentication Methods registration. This proposes a new method "mtls" along with a "pass" and "fail" result.

2. References

2.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/rfc/rfc5321>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/rfc/rfc6962>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/rfc/rfc7208>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/rfc/rfc8555>.

[RFC8601] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 8601, DOI 10.17487/RFC8601, May 2019, <https://www.rfc-editor.org/rfc/rfc8601>.

2.2. Informative References

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/rfc/rfc7489>.

[RFC8120] Oiwa, Y., Watanabe, H., Takagi, H., Maeda, K., Hayashi, T., and Y. Ioku, "Mutual Authentication Protocol for HTTP", RFC 8120, DOI 10.17487/RFC8120, April 2017, <https://www.rfc-editor.org/rfc/rfc8120>.

Appendix A. Acknowledgments

We thank Nicholas Lidzborkski for his advice.

Authors’ Addresses

Weihaw Chuang
Google, Inc.
Email: weihaw@google.com

Allen Robinson
Google, Inc.
Email: arobins@google.com

Bruce Nan
Google, Inc.
Email: brucenan@google.com