Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 27, 2015

E. Osterweil
Verisign Labs
S. Rose
D. Montgomery
NIST

August 26, 2014

Enterprise Requirements for Secure Email Key Management
draft-osterweil-dane-ent-email-reqs-00

Abstract

Individuals and organizations have expressed a wish to have the ability to send encrypted and/or digitally signed email end-to-end. One key obstacle to end-to-end email security is the difficulty in discovering, obtaining, and validating email credentials across administrative domains. This document addresses foreseeable adoption obstacles for DANE's cryptographic key management for email in enterprises, and outlines requirements.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 27, 2015.

Copyright Notice

Table of Contents

1. Introduction

The management of security protections for email constituencies can vary by organization and by type of organization. Some organizations can have large sets of users with prescribed controls and policies, some may have a lot of churn in their users, and there are many other ways in which deployments may differ.

As a result of the variability of deployments, aligning key management semantics with the behaviors of email users (and their organizations) can be an important differentiator when administrators choose a solution in which to invest. Designs and cryptographic protocols that do not fit the requirements of users run the risk that deployments may falter and/or may not gain traction.

This document addresses foreseeable requirements for DANE's cryptographic key management for email in enterprises, and outlines requirements. This document generally categorizes requirements as being relevant to the domain authorities, the Relying Parties (RPs), or both. In the following text, "domain authorities" refers to the owners of a given domain, which may not necessarily be the operators of the authoritative DNS servers for the zone(s) that make up the domain.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Requirements for Both

REQ-1 Credentials stored can be either entire credential (i.e. the key/certificate) or one-way hash of the credential.

Intuition: This can reduce the size of DNS responses.

REQ-2 The Protocol MUST be able to handle the use of DNS redirection via CNAME/DNAME and wildcards.

Intuition: Managing user domain names may be a different cardinality than number of S/MIME certificates. For example, if the domain's users employ the same certificate for both digital signature and encryption, a DNAME record enables a single Resource Record (RR) for each user.

3. Requirements for Authorities

REQ-3 The protocol MUST support incremental rollout of DANE-centric cryptographic protections, whereby not all users in an enterprise may be cut over to a DANE solution at the same time and MUST be backwards compatible

Intuition: Enterprise operations may wish be able to enroll subsets of all of their users in a DANE architecture without disrupting existing email cryptographic services for all users.

REQ-4 The protocol MUST have the ability to either scope a Certification Authority (CA) or local Trust Anchor (TA) in use for a given domain.

Intuition: Enterprises may issue certificates from a TA and prefer to authorize that certificate in DNS (instead of End Entity certificates for every user).

REQ-5 The protocol SHOULD have the ability to signal that a particular key/certificate is no longer to be trusted or is revoked.

Intuition: Allows default TA authorizations to be overridden by revocation.

REQ-6 The protocol SHOULD have the ability to signal that a particular email address is not (or no longer) a valid sender

for the given domain.

Intuition: Allows for authenticated denial of existence of a network identity.

REQ-7 The protocol MUST allow for separate management, publication, and learning of keys that are used for signing versus encryption.

Intuition: Separating, scaling, delegating, and general management for different keys in different ways and in different branches of the DNS allows administrators to manage different material in different systems if needed.

REQ-8 The protocol MUST have the ability to delegate authority for user names.

Intuition: Some enterprises may wish to use a service provider.

REQ-9 The protocol MUST have the ability to manage keys in different ways for different user names.

Intuition: Not all members of a medium/large enterprise may be migrated onto a DANE system overnight, and must operate alongside current email key management. This could include users that use a different email security protocol.

REQ-10 The protocol MUST have the ability to signal that a given network identity (or entire zone) only sends digitally signed messages.

Intuition: A domain owner may wish to signal that their email security policy is to sign all outgoing message so a receiver can infer an unsigned message is likely a phishing attempt.

4. Requirements for Relying Parties

REQ-11 Key material for DANE-enabled email users MUST be verifiably

discoverable and learnable using just an email address.

Intuition: Email addresses are all the RP has, but may point to external management systems.

REQ-12 The protocol SHOULD have the ability to provide opportunistic encryption at the user's discretion.

Intuition: Compliance controls (for example) may mandate the encryption of all messages under certain circumstances.

REQ-13 The protocol MUST support default verification configurations (such as enterprise TA or stapling) with user-specific overrides. Overrides MUST include specifying specific cryptographic information for specific users and disallowing users (either specific cryptographic or entirely).

REQ-14 The protocol MUST be resistant to downgrade attacks targeting the DNS response.

Intuition: If DNSSEC is stripped, the protocol MUST alert the user or refuse to send an unencrypted email message.

REQ-15 The protocol MUST provide separate semantics to discover certificates that are used for specific purposes.

Intuition: keep DNS response size minimal.

REQ-16 Encryption keys MUST be discoverable separately from signature keys. Possible means includes (but not limited to) naming conventions, sub-typing or unique RR types for each use

Intuition: Not all certificates for a user may be needed for all circumstances. Fetching them separately can be a management, a scaling, or even a security concern.

5. Acknowledgements

TBD

6. IANA Considerations

This document only discusses requirements for publishing and querying for security credentials used in email. No new IANA actions are required in this document, but specifications addressing these requirements may have IANA required actions.

This section should be removed in final publication.

7. Security Considerations

The motivation for this document is to outline requirements needed to facilitate the secure publication and learning of cryptographic keys for email, using DANE semantics. There are numerous documents that more generally address security considerations for email. By contrast, this document is not proposing a protocol or any facilities that need to be secured. Instead, these requirements are intended to inform security considerations in follow-on works.

8. Normative References

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

Authors' Addresses

Eric Osterweil
Verisign Labs
Reston, VA
US

Email:

Scott Rose
NIST
100 Bureau Dr.
Gaithersburg, MD 20899
US

Email: scottr@nist.gov

Doug Montgomery
NIST
100 Bureau Dr.
Gaithersburg, MD 20899
US

Email: dougm@nist.gov