Secure Telephone Identity for Message Layer Security

Abstract

This document specifies Message Layer Security (MLS) Credential Types for use with Secure Telephone Identity Revisited (STIR), one for STIR certificates and another for the Personal Assertion Token (PASSporT).

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 https://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 25 April 2024.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.
1. Introduction

The STIR problem statement [RFC7340] describes widespread problems enabled by impersonation in the telephone network, including illegal robocalling, voicemail hacking, and swatting. As telephone services have migrated onto the Internet using Voice over IP (VoIP) protocols such as SIP [RFC3261], it is necessary for these protocols to support stronger identity mechanisms to prevent impersonation. [RFC8224] defines a SIP Identity header capable of carrying PASSporT [RFC8225] objects in SIP as a means to cryptographically attest that the originator of a telephone call is authorized to use the calling party number (or, for native SIP cases, SIP URI) associated with the originator of the call. [RFC8226] in turn defines an extension to X.509 certificates (TNAuthList) suitable attesting ownership of telephone numbers and signing PASSporTs.

The problem of bulk, unsolicited commercial communications is not, however, limited to telephone calls. Spammers and fraudsters are increasingly turning to messaging applications to deliver undesired content to consumers. And as STIR sees further deployment in the telephone network, the governance structures put in place for securing telephone network resources with STIR could be repurposed to help secure the messaging ecosystem. This problem and its applicability to STIR is described in [I-D.ietf-stir-messaging], both for signing individual messages with STIR and securing message streams negotiated by SIP.

Message Layer Security (MLS) [RFC9420] defines a key exchange mechanism to enable secure messaging between groups of users. Members in MLS groups are identified by credentials, which can include X.509 certificates. Because many messaging systems use
telephone numbers as identifiers for users, having a secure means to identify MLS group members by telephone number is desirable.

This specification explores the applicability of [RFC8226] certificates to MLS, and how both service-provider level certificates and delegate certificates [RFC9060] might be used as credentials for MLS users for those cases where a telephone number is the primary identifier of a group member. It also specifies a way to use a [RFC8225] PASSporT as an MLS Credential. These MLS Credential Types could be used for carrier-adjacent deployments (e.g. RCS) or for over-the-top implementations.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. MLS Credential Type for STIR Certificates

MLS already specifies the use of X.509 certificates as an MLS Credential Type. The guidance in [RFC9420] Section 5.3 allows MLS applications significant leeway in determining how to derive identifiers that will be rendered to users. An application could, for example, extract identifiers from the subjectAltName extension of an X.509 certificate.

[RFC8226] certificates used by STIR contain a TNAuthList extension, which may contain one or more telephone numbers, telephone number ranges, or Service Provider Codes (SPCs). In North American carrier deployments, the Service Provider Code field is most commonly used to convey an Operating Company Number (sometimes also known as a Service Provider ID), which designates only the serving carrier. These certificates do not convey any individual telephone number associated with a potential member in an MLS group, so that identifier would need to be conveyed separately by the application. Moreover, the keying material would in this case be held by a carrier, rather than an end-user device, so any security association created with that keying material would not be end-to-end.

[RFC9060] specifies delegate certificates in STIR, which allow intermediate certification authorities to issue subordinate keys that attest to a subset of a given carrier's authority. Delegate certificates may be issued down to the individual telephone number level, and are recommended for applications where end-to-end security is required, per [RFC8862]. MLS applications could extract
the telephone number from the TNAuthList field to use as an identifier for the group member.

The subjectAltName field, or a similar X.509 extension, could be used to convey the user's name in delegate certificates. Another [RFC8226] extension is JWTClaimsConstraint, which can place restrictions on the content of PASSporT objects that can be signed with a certificate. These can include constraints on Rich Call Data (RCD), which includes elements like proper names and images or logos associated with the certificate. A claim constraint on the "nam" RCD element, for example, could also be used by MLS applications as an alternative way to find a proper name for a group member.

In deployments at this time, however, delegate certificates are rarely used, and few intermediate certification authorities exist who are capable of issuing delegate certificates.

3.1. MLS STIR Certificate Credential Structure Definitions

struct {
  // Certificate chain, where Certificate is defined in RFC 9420 (and the ordering requirements apply), and certificates are in the form defined by RFC 8226 / RFC 9060. The subjectPublicKey of the first certificate must match the signature_key of the enclosing LeafNode.
  Certificate certificates<V>;
} STIRCertificateCredential;

4. MLS Credential Type for STIR PASSporTs

Instead of using a STIR certificate, implementations may also use a STIR PASSporT [RFC8225] as an MLS Credential Type. The PASSporT's contents contain identity information that could be consumed by messaging applications. Effectively, in this case a PASSporT would be created on a per-group basis.

The "orig" field of a PASSporT would indicate the telephone number identity of the group member. Further RCD data, including the "nam" field, could give additional identifiers for the member, including a proper name. The "dest" field of the PASSporT would contain a suitable identifier for the MLS group [TBD].

While PASSporTs themselves do not convey keying material suitable for MLS, they can carry an "mky" field containing a fingerprint of keying material. This allows a PASSporT signed by an SPC-level certificate to contain an "mky" field with keying material generated by an end-user device. While this introduces certain security risks (see the Security Considerations), it provides a means to integrate STIR as commonly deployed today with MLS.
Note that PASSporTs as traditionally used by STIR have a short expiry, typically less than one minute, in order to prevent replay. Sessions negotiated by SIP that use PASSporTs only check their validity at session initiation, even if the session itself is long-lived. With the use of "mky", however, the risk of a success replay attack is significantly mitigated, and it is safer to use longer expiry timers. PASSporTs created for use with MLS MUST contain an "mky" element.

4.1. MLS PASSporT Credential Structure Definitions

```c
struct {
  // Certificate chain, where Certificate is defined in RFC 9420 (and th
  // ordering requirements apply), and certificates are in the form defi
  // RFC 8226 / RFC 9060. The subjectPublicKey of the first certificate
  // verify the signature on the object in the passport field.
  Certificate certificates[V];

  // A PASSporT encoded as a byte string, signed by the first certificat
  // `certificates` vector. The PASSporT MUST have an "mky" claim, whic
  // match the signature_key field in the enclosing LeafNode.
  opaque passport[V];
} STIRPASSporTCredential;
```

5. MLS Group Messaging with STIR

TBD.

6. Acknowledgments

7. IANA Considerations

TBD.

8. Privacy Considerations

TBD.

9. Security Considerations

This specification inherits the security considerations of [I-D.ietf-stir-messaging].

The use of PASSporTs as MLS Credentials signed with SPC-level STIR certificates creates a potential key substitution attack where a rogue service provider injects its own "mky" value before signing the PASSporT. MLS applications would need some out-of-band way to check the epoch authenticator in order to detect this substitution.
10. References

10.1. Normative References


10.2. Informative References


Authors' Addresses

Jon Peterson
TransUnion

Email: jon.peterson@transunion.com

Richard Barnes
Cisco

Email: rlb@ipv.sx