Certificate Authentication in SIP
draft-dotson-sip-certificate-auth-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 17, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

This document defines requirements for adding certificate authentication to the Session Initiation Protocol (SIP). It is intended that potential solutions specifying certificate authentication within SIP will use these requirements as guidelines. Supporting certificate authentication in SIP would provide strong authentication and increase the types of possible deployment scenarios.

Table of Contents

1. Introduction .................................................. 3
   1.1. Use Cases ................................................. 3
   1.2. SIP Digest ............................................... 4
   1.3. Terminology ............................................... 4
2. Requirements and Recommendations ............................. 5
3. Related Work .................................................... 6
4. IANA Considerations ............................................ 8
5. Security Considerations ....................................... 9
6. Normative References ......................................... 10
Author’s Address .................................................. 11
Intellectual Property and Copyright Statements ................. 12
1. Introduction

SIP enables many next generation multimedia architectures. While it offers many advantages, it is restrictive regarding the types of credentials supported. As of this writing, it only provides for username and pre-shared key based credentials. The lack of additional credential types, specifically certificate based credentials, is restricting certain deployment scenarios and the advantages that can be realized by them.

Certificate based credentials offer relatively stronger authentication, for example, when compared to username and passwords (as used commonly). They are currently in successful use within various deployment scenarios (such as cable) where each client is pre-configured with certificates that are used for identification, authentication and establishing secure communications. While this offers many advantages, the most prominent is the ability to authenticate certificates without pre-configuration of each certificate in the Service Provider’s network (for example, by using Public Key Infrastructure).

Support for certificate based credentials within SIP networks is not only desired, but a necessity in certain deployments. However, support for certificates within SIP networks requires careful consideration. This document aims to present assumptions and requirements regarding the use of certificates in SIP networks. There is no intent to specify solution-specific details in this document.

1.1. Use Cases

In regards to the entity being authenticated, there are several use cases that can be readily identified.

- The entity may be a device, in which case the certificate would contain information related to the device identity (e.g., MAC address, FQDN, etc). The users "behind" the device may or may not be authenticated by the device.

- The entity may be a user, in which case the certificate would contain information related to the user identity (e.g., SIP URI, etc).

- Users may be mapped to the device certificate. The device certificate could be used to bootstrap user identity certificates. The device certificate could be associated with users through some backend system.
It is for discussion whether this level of detail in the use of the certificates is within scope of the procedures and scope of the problem. For example, the validity checks for a user certificate could include validation of the CN or subjectAltName attributes in relation to the identity represented in SIP messages. However, the actual mapping of certificate to device or user or both may not need to be defined by the methodology and could be left to local policy.

1.2. SIP Digest

RFC 3261 [RFC3261] defines procedures for performing SIP Digest authentication using usernames and passwords. SIP Digest is a challenge based mechanism for authentication. Any time a UA or proxy server receives a request it may challenge the initiator of the request to provide assurance of its identity.

SIP Digest utilizes a challenge-response authentication mechanism that may be used by a server to challenge a client request and by a client to provide authentication information. The Digest scheme challenges using a nonce value. A valid response contains a checksum of the password, username, the provided nonce value, and other parameters. As a result, the password is never sent in the clear. SIP Digest provides authentication and replay detection. Because it is based on passwords, it suffers from the security weaknesses of password based systems.

1.3. Terminology

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].

This document borrows SIP related terminology as specified in RFC 3261 [RFC3261].

end entity - user of PKI certificates and/or end user system that is the subject of a certificate
2. Requirements and Recommendations

The following are the general requirements and recommendations for the support of certificate based authentication in SIP networks. A proposed solution MUST meet all the requirements stated in this section.

1. The solution MUST utilize an end entity certificate for authentication.

2. A certificate MUST represent an end entity that will be authenticated. The certificate MUST contain enough information that allows the end entity to be identified. Examples of an end entity include client, user, service provider, etc.

3. All certificates necessary for validation of the client’s identity MUST be available, or made available, to the server. For solutions providing mutual authentication of the client and the SIP network, all necessary certificates for validation of the server’s identity MUST be available, or made available, to the client.

4. Relying parties MUST check the validity of certificates as defined in RFC 3280 [RFC3280].

5. Unless mutual authentication is achieved by other means (for example, additional protocols), mutual authentication MUST be supported. Client-only authentication MUST always be supported.

6. The solution MUST allow for intermediate proxies within the SIP network, including when confidentiality is required.

The following are the recommendations that are expected to be considered by solutions complying with this document.

1. A mechanism MAY be necessary for the entities to agree on the authentication to be used.

2. The methodology SHOULD consider message size impacts and SHOULD attempt to limit them.
3. Related Work

The following sections provide an analysis of existing work in the IETF related to the requirements presented in this document.

RFC 4474 [RFC4474] SIP Identity provides a mechanism to cryptographically assure the identity of originators of SIP messages. As described in Section 5, Identity uses a private key and a certificate associated with the domain indicated in the From header. An authentication service authenticates the UAC and then inserts an Identity header and an Identity-Info header in the forwarded request. The Authentication Service is typically located at the outbound proxy and may authenticate the UAC using digest authentication and/or a TLS session. SIP Identity does not meet all the requirements listed in this document.

- Identity does not have a mechanism to pass certificates in the SIP messages.
- Unless the UA is directly connected to the Authentication Service, TLS is not available to the UA to perform mutual TLS to the Authentication Service.
- The protocol requires the use of certificates for authentication, and the UA may not contain other credentials besides certificates.
- There is potentially some reuse of the identity header and cryptographic assertion. In this case, the UA could act as the authentication service and provide an identity header to the entity requesting authentication. However, Identity requires the Authentication Service to be authoritative for a domain, and this is typically not supported on a UA as the UA would need to be its own domain.

RFC 3261 [RFC3261] discusses the use of S/MIME and certificates to provide confidentiality, integrity and authentication of UAs. The procedures are based on the use of the CMS content types signedData, for signing messages, and enveloped data, for encrypting data. RFC 3261 does not have a means to negotiate authentication methods, as there is only one allowed method of authentication. RFC 3261 does not describe a mechanism to provide a list of trusted roots.

RFC 3893 [RFC3893] Authenticated Identity Body (AIB) Format defines a more specific mechanism than the S/MIME solution in RFC 3261 [RFC3261]. It changes the MIME type and reduces the number of headers included in the cryptographic operation from those
recommended in RFC 3261. As the solution is similar to RFC 3261 S/MIME in relation to the requirements in this document, the solution does not meet all the requirements in this document as described in the previous paragraph.
4. IANA Considerations

None.
5. Security Considerations

This document defines the requirements for certificate-based authentication within SIP. As such, it does not define a specific solution or set of technologies. However, the eventual technical architecture meeting these requirements must consider the security of the solution.

Depending on the solution, confidentiality and integrity of messages may be necessary. Replay protection must be provided.
6. Normative References


Author’s Address

Steve Dotson
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
US

Email: s.dotson@cablelabs.com