Internet Engineering Task Force (IETF)
Request for Comments: 5924
Category: Experimental
ISSN: 2070-1721
June 2010

S. Lawrence
V. Gurbani
Bell Laboratories, Alcatel-Lucent

Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates

Abstract

This memo documents an extended key usage (EKU) X.509 certificate extension for restricting the applicability of a certificate to use with a Session Initiation Protocol (SIP) service. As such, in addition to providing rules for SIP implementations, this memo also provides guidance to issuers of certificates for use with SIP.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5924.

Copyright Notice

Table of Contents

1. Introduction

This memo documents an extended key usage (EKU) X.509 certificate extension for restricting the applicability of a certificate to use with a Session Initiation Protocol (SIP) service. As such, in addition to providing rules for SIP implementations, this memo also provides guidance to issuers of certificates for use with SIP.

2. Terminology

2.1. Key Words

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 [1].

Additionally, the following term is defined:

> SIP domain identity: A subject identity in the X.509 certificate that conveys to a recipient of the certificate that the certificate owner is authoritative for SIP services in the domain named by that subject identity.

2.2. Abstract Syntax Notation

All X.509 certificate X.509 [4] extensions are defined using ASN.1 X.680 [5], and X.690 [6].

3. Problem Statement

Consider the SIP RFC 3261 [2] actors shown in Figure 1.

```
  Proxy-A.example.com           Proxy-B.example.net
     +-------+                     +-------+
     | Proxy |--------------------| Proxy |
     +----+--+                     +---+---+
          |                            |
          |                            |
          |                            |
          |                          +---+
        0---0                        |   |
         /-\                         |___|
        +---+                       /    /
                                   +----+
   alice@example.com         bob@example.net
```

Figure 1: SIP Trapezoid

Assume that alice@example.com creates an INVITE for bob@example.net; her user agent routes the request to some proxy in her domain, example.com. Suppose also that example.com is a large organization that maintains several SIP proxies, and her INVITE arrived at an outbound proxy Proxy-A.example.com. In order to route the request onward, Proxy-A uses RFC 3263 [7] resolution and finds that Proxy-B.example.net is a valid proxy for example.net that uses Transport Layer Security (TLS). Proxy-A.example.com requests a TLS connection to Proxy-B.example.net, and in the TLS handshake each one presents a certificate to authenticate that connection. The validation of these certificates by each proxy to determine whether or not their peer is authoritative for the appropriate SIP domain is defined in "Domain Certificates in the Session Initiation Protocol (SIP)" [8].

A SIP domain name is frequently textually identical to the same DNS name used for other purposes. For example, the DNS name example.com can serve as a SIP domain name, an email domain name, and a web service name. Since these different services within a single organization might be administered independently and hosted separately, it is desirable that a certificate be able to bind the DNS name to its usage as a SIP domain name without creating the implication that the entity presenting the certificate is also authoritative for some other purpose. A mechanism is needed to allow the certificate issued to a proxy to be restricted such that the subject name(s) that the certificate contains are valid only for use in SIP. In our example, Proxy-B possesses a certificate making Proxy-B authoritative as a SIP server for the domain example.net; furthermore, Proxy-B has a policy that requires the client’s SIP domain be authenticated through a similar certificate. Proxy-A is authoritative as a SIP server for the domain example.com; when Proxy-A makes a TLS connection to Proxy-B, the latter accepts the connection based on its policy.

4. Restricting Usage to SIP

This memo defines a certificate profile for restricting the usage of a domain name binding to usage as a SIP domain name. RFC 5280 [3], Section 4.2.1.12, defines a mechanism for this purpose: an "Extended Key Usage" (EKU) attribute, where the purpose of the EKU extension is described as:

> If the extension is present, then the certificate MUST only be used for one of the purposes indicated. If multiple purposes are indicated the application need not recognize all purposes indicated, as long as the intended purpose is present. Certificate using applications MAY require that the extended key

usage extension be present and that a particular purpose be indicated in order for the certificate to be acceptable to that application.

A Certificate Authority issuing a certificate whose purpose is to bind a SIP domain identity without binding other non-SIP identities MUST include an id-kp-sipDomain attribute in the Extended Key Usage extension value (see Section 4.1).

4.1. Extended Key Usage Values for SIP Domains

RFC 5280 [3] specifies the EKU X.509 certificate extension for use in the Internet. The extension indicates one or more purposes for which the certified public key is valid. The EKU extension can be used in conjunction with the key usage extension, which indicates how the public key in the certificate is used, in a more basic cryptographic way.

The EKU extension syntax is repeated here for convenience:

```
ExtKeyUsageSyntax  ::=  SEQUENCE SIZE (1..MAX) OF KeyPurposeId

KeyPurposeId  ::=  OBJECT IDENTIFIER
```

This specification defines the KeyPurposeId id-kp-sipDomain. Inclusion of this KeyPurposeId in a certificate indicates that the use of any Subject names in the certificate is restricted to use by a SIP service (along with any usages allowed by other EKU values).

```
id-kp  OBJECT IDENTIFIER  ::=
   { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) 3 }

id-kp-sipDomain  OBJECT IDENTIFIER  ::=  { id-kp 20 }
```

5. Using the SIP EKU in a Certificate

Section 7.1 of Domain Certificates in the Session Initiation Protocol [8] contains the steps for finding an identity (or a set of identities) in an X.509 certificate for SIP. In order to determine whether the usage of a certificate is restricted to serve as a SIP certificate only, implementations MUST perform the steps given below as a part of the certificate validation:

The implementation MUST examine the Extended Key Usage value(s):

- If the certificate does not contain any EKU values (the Extended Key Usage extension does not exist), it is a matter of local policy whether or not to accept the certificate for use as a SIP certificate. Note that since certificates not following this specification will not have the id-kp-sipDomain EKU value, and many do not have any EKU values, the more interoperable local policy would be to accept the certificate.

- If the certificate contains the id-kp-sipDomain EKU extension, then implementations of this specification MUST consider the certificate acceptable for use as a SIP certificate.

- If the certificate does not contain the id-kp-sipDomain EKU value, but does contain the id-kp-anyExtendedKeyUsage EKU value, it is a matter of local policy whether or not to consider the certificate acceptable for use as a SIP certificate.

- If the EKU extension exists, but does not contain any of the id-kp-sipDomain or id-kp-anyExtendedKeyUsage EKU values, then the certificate MUST NOT be accepted as valid for use as a SIP certificate.

6. Implications for a Certification Authority

The procedures and practices employed by a certification authority MUST ensure that the correct values for the EKU extension and subjectAltName are inserted in each certificate that is issued. For certificates that indicate authority over a SIP domain, but not over services other than SIP, certificate authorities MUST include the id-kp-sipDomain EKU extension.

7. Security Considerations

This memo defines an EKU X.509 certificate extension that restricts the usage of a certificate to a SIP service belonging to an autonomous domain. Relying parties can execute applicable policies (such as those related to billing) on receiving a certificate with the id-kp-sipDomain EKU value. An id-kp-sipDomain EKU value does not introduce any new security or privacy concerns.

8. IANA Considerations

The id-kp-sipDomain purpose requires an object identifier (OID). The objects are defined in an arc delegated by IANA to the PKIX working group. No further action is necessary by IANA.

9. Acknowledgments

The following IETF contributors provided substantive input to this document: Jeroen van Bemmel, Michael Hammer, Cullen Jennings, Paul Kyzivat, Derek MacDonald, Dave Oran, Jon Peterson, Eric Rescorla, Jonathan Rosenberg, Russ Housley, Paul Hoffman, and Stephen Kent.

Sharon Boyen and Trevor Freeman reviewed the document and facilitated the discussion on id-kp-anyExtendedKeyUsage, id-kpServerAuth and id-kp-ClientAuth purposes in certificates.

10. Normative References

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

[2] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[3] 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, May 2008.

[4] International Telecommunications Union, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, ISO Standard 9594-8, March 2000.

[5] International International Telephone and Telegraph Consultative Committee, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", CCITT Recommendation X.680, July 2002.

[6] International International Telephone and Telegraph Consultative Committee, "ASN.1 encoding rules: Specification of basic encoding Rules (BER), Canonical encoding rules (CER) and Distinguished encoding rules (DER)", CCITT Recommendation X.690, July 2002.

[7] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[8] Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol (SIP)", RFC 5922, June 2010.

Appendix A. ASN.1 Module

```
   SIPDomainCertExtn
     { iso(1) identified-organization(3) dod(6) internet(1)
       security(5) mechanisms(5) pkix(7) id-mod(0)
       id-mod-sip-domain-extns2007(62) }

   DEFINITIONS IMPLICIT TAGS ::=
   BEGIN

   -- OID Arcs

   id-kp  OBJECT IDENTIFIER  ::=
      { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) 3 }

   -- Extended Key Usage Values

   id-kp-sipDomain  OBJECT IDENTIFIER  ::=  { id-kp 20 }

   END
```

Authors' Addresses

Scott Lawrence

EMail: scott-ietf@skrb.org

Vijay K. Gurbani
Bell Laboratories, Alcatel-Lucent
1960 Lucent Lane
Room 9C-533
Naperville, IL 60566
USA

Phone: +1 630 224-0216
EMail: vkg@bell-labs.com