SIP WG	S. Lawrence	
Internet-Draft	Bluesocket Inc.	
Updates: 3261 (if approved)	V. Gurbani	
Intended status: Standards Track	Bell Laboratories, Alcatel-Lucent	
Expires: August 21, 2008	February 18, 2008	

TOC

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

Status of this Memo

Abstract

This memo documents an extended key usage (EKU) X.509 certificate extension for identifying the holder of a certificate as authoritative for a Session Initiation Protocol (SIP) service in the domain named by the DNS name in the certificate.

Table of Contents

1. Terminology
    1.1. Key Words

1.2. Abstract syntax notation
2. Problem statement
3. Restricting usage to SIP
3.1. Extended Key Usage values for SIP domains
4. Using the SIP EKU in a certificate
5. Guidelines for a Certification Authority
6. Security Considerations
7. IANA Considerations
8. Acknowledgments
9. References
9.1. Normative References
9.2. Informative References
Appendix A. ASN.1 Module
§ Authors' Addresses
§ Intellectual Property and Copyright Statements

1. Terminology

TOC

1.1. Key Words

TOC

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 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [1].

1.2. Abstract syntax notation

TOC

All X.509 certificate X.509 (International International Telephone and Telegraph Consultative Committee, “Information Technology - Open Systems Interconnection - The Directory: Authentication Framework,” November 1988.) [4] extensions are defined using ASN.1 X.680 (International International Telephone and Telegraph Consultative Committee, “Specification of Abstract Syntax Notation One (ASN.1): Specification of Basic Notation,” July 1994.) [5],X.690 (International Telecommunications Union, “Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER),” 1994.) [6].

2. Problem statement

TOC

Consider the SIP [2] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) trapezoid shown in Figure 1 (SIP Trapezoid).

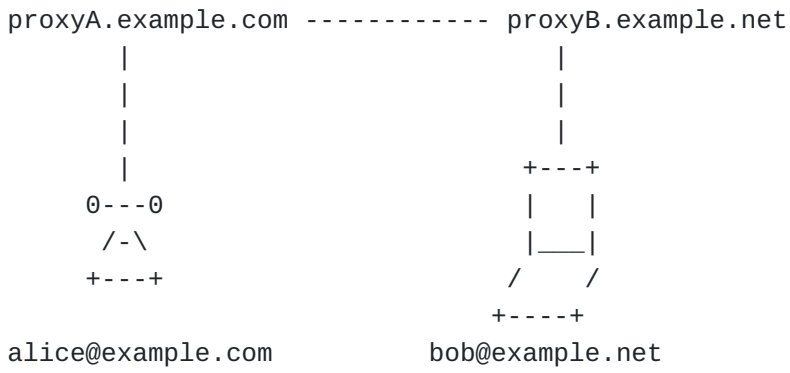

Figure 1: SIP Trapezoid

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 normal resolution rules cause her INVITE to be sent to an outbound proxy proxyA.example.com, which then uses RFC 3263 (Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Location SIP Servers," June 2002.) [7] resolution and finds that proxyB.example.net is a valid proxy for example.net that uses TLS. proxyA.example.com requests a TLS connection to proxyB.example.net, and each presents a certificate to authenticate that connection. This is the basic mutual authentication model explored in depth in [8] (Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol (SIP)," November 2007.).
However, there arise certain cases where one SIP proxy needs to know whether it has reached an authoritative proxy in target SIP domain. For instance, billing transactions may be triggered when an authoritative SIP proxy in one domain sends messages to its equivalent in another domain. In Figure 1 (SIP Trapezoid), proxyA.example.com performs certain DNS queries to arrive at proxyB.example.net. Because of the answers to the DNS queries, proxyA has a certain expectation that

proxyB is a valid proxy in the example.net domain and is authorized to receive inbound requests targeted to that domain.
However, the problem for proxyB is different; it is presented with a connection from a specific host, but what it needs to determine is whether or not that connection can be treated as coming from a particular SIP domain. If it receives a certificate that contains only the name proxyA.example.com, then it cannot determine that proxyA is authorized to act as a SIP outbound proxy for example.com, because example.com may use different systems for inbound messages so SIP DNS resolution of example.com may not lead to proxyA.example.com (if this is the case, proxyB should not reuse this connection if it needs to send a request to example.com). The certificate usage in SIP should not require that every outbound proxy for a domain must also be an inbound proxy for that domain, but should provide for certificate based binding of the SIP domain name to a particular connection.
Thus, there is a need for an extra attribute that allows a proxy to know that its peer is an authorized proxy for that domain. This memo discusses such an attribute as part of the X.509 certificate exchanged by the proxies when a TLS connection is first established.

---

3. Restricting usage to SIP

TOC

This memo defines a certificate profile for binding a SIP domain name to an entity. A SIP domain name is frequently textually identical to the same DNS name used for other purposes. For example, the DNS name example.com may serve as a SIP domain name, an email domain name, and web service name. Since these different services within a single organization might be administered independently and hosted separately, it should be possible to create a certificate that binds the DNS name to its usage as a SIP domain name without creating the implication that the usage is also valid for some other purpose. RFC 3280 (Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” April 2002.) [3] section 4.2.1.13 defines a mechanism for this purpose: an "Extended Key Usage" attribute. Certificates whose purpose is to bind a SIP domain identity without binding other non-SIP identities MUST include an id-kp-SIPdomain attribute.

3.1. Extended Key Usage values for SIP domains

TOC

RFC 3280 (Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” April 2002.) [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 may be used. The EKU extension can be used in conjunction with the key usage extension, which indicates how the public key in the certificate may be 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 any DNS Subject names in the certificate are intended to identify the holder as authoritative for a SIP service in the domain named by the subjectAltName values. Whether or not to include this restriction is up to the certificate issuer, but if it is included, it MUST be marked as critical so that implementations that do not understand it will not accept the certificate for any other purpose.

```
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 VALUE-TBD }
```

See Section 4 (Using the SIP EKU in a certificate) for how the presence of an id-kp-sipDomain value affects the interpretation of the certificate.

---

4. Using the SIP EKU in a certificate

TOC

Section 7.1 of [8] (Gurbani, V., Lawrence, S., and A. Jeffrey, “Domain Certificates in the Session Initiation Protocol (SIP),” November 2007.) contains two steps for finding an identity (or a set of identities) in an X.509 certificate. In order to determine whether a SIP proxy is authoritative for its domain, implementations MUST perform the step given below first, and then proceed with the steps in Section 7.1 of [8] (Gurbani, V., Lawrence, S., and A. Jeffrey, “Domain Certificates in the Session Initiation Protocol (SIP),” November 2007.).
The Extended Key Usage value(s), if any, MUST be examined to determine whether or not the certificate is valid for use in SIP:

* 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.

*If the certificate contains the id-kp-sipDomain EKU extension, then the certificate MUST be accepted as valid 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 accept it for use as a SIP certificate.

*If the certificate does not contain the id-kp-sipDomain EKU value, but does contain either the id-kp-serverAuth or id-kp-clientAuth EKU values, it is a matter of local policy whether or not to accept it for use as a SIP certificate.

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

---

5. Guidelines for a Certification Authority

TOC

The procedures and practices employed by the 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.

---

6. Security Considerations

TOC

This memo defines an EKU X.509 certificate extension that enables the holder of a certificate to be authoritative for a SIP service belonging to an autonomous domain. Relying parties may 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. At the very most, it simply allows the relying party to know that the holder of the certificate is authoritative for the SIP service in a certain domain. In the absence of the id-kp-sipDomain EKU value, this information can be collected over time by a peer in any case.

---

7. IANA Considerations

TOC

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

---

8. Acknowledgments

TOC

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, 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.

---

9. References

TOC

9.1. Normative References

TOC

[1]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” RFC 2119, March 1997 (TXT).
[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 (TXT).
[3]	Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” RFC 3280, April 2002 (TXT).
[4]	International International Telephone and Telegraph Consultative Committee, “Information Technology - Open Systems Interconnection - The Directory: Authentication Framework,” CCITT Recommendation X.509, November 1988.
[5]	International International Telephone and Telegraph Consultative Committee, “Specification of Abstract Syntax Notation One (ASN.1): Specification of Basic Notation,” CCITT Recommendation X.680, July 1994.
[6]	International Telecommunications Union, “Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER),” ITU-T Recommendation X.690, 1994.

[7]	Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Location SIP Servers,” RFC 3263, June 2002 (TXT).

9.2. Informative References

TOC

[8]	Gurbani, V., Lawrence, S., and A. Jeffrey, “Domain Certificates in the Session Initiation Protocol (SIP),” draft-ietf-sip-domain-certs-00.txt (work in progress), November 2007 (TXT).

Appendix A. ASN.1 Module

TOC

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- OID Arcs

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

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

id-aca  OBJECT IDENTIFIER  ::=
   { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) 10 }

-- Extended Key Usage Values

id-kp-sipDomain  OBJECT IDENTIFIER  ::=  { id-kp VALUE-TBD }

END
```

Authors' Addresses

TOC

	Scott Lawrence
	Bluesocket Inc.
	10 North Ave.
	Burlington, MA 01803
	USA
Phone:	+1 781 229 0533
Email:	slawrence@bluesocket.com
	Vijay K. Gurbani
	Bell Laboratories, Alcatel-Lucent
	2701 Lucent Lane
	Room 9F-546
	Lisle, IL 60532
	USA
Phone:	+1 630 224-0216
Email:	vkg@alcatel-lucent.com

Full Copyright Statement

TOC

Intellectual Property

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.