

SIP WG	S. Lawrence	
Internet-Draft	Nortel Networks, Inc.	
Intended status: Experimental	V. Gurbani	
Expires: April 23, 2010	Bell Laboratories, Alcatel-Lucent	
	October 20, 2009	

[TOC](#)

**Using Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates  
draft-ietf-sip-eku-08**

**Status of this Memo**

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

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 April 23, 2010.

**Copyright Notice**

Copyright (c) 2009 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 in effect on the date of

publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

## 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.

---

## 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.](#) Implications for a Certification Authority
- [6.](#) Security Considerations
- [7.](#) IANA Considerations
- [8.](#) Acknowledgments
- [9.](#) Normative References
- [Appendix A.](#) ASN.1 Module
- [§](#) Authors' Addresses

---

## 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].

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.

---

## 1.2. Abstract syntax notation

[TOC](#)

All X.509 certificate [X.509 \(International Telecommunications Union, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," March 2000.\)](#) [4] extensions are defined using ASN.1 [X.680 \(International International Telephone and Telegraph Consultative Committee, "Abstract Syntax Notation One \(ASN.1\): Specification of basic notation," July 2002.\)](#) [5], [X.690 \(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 \(DER\)," July 2002.\)](#) [6].

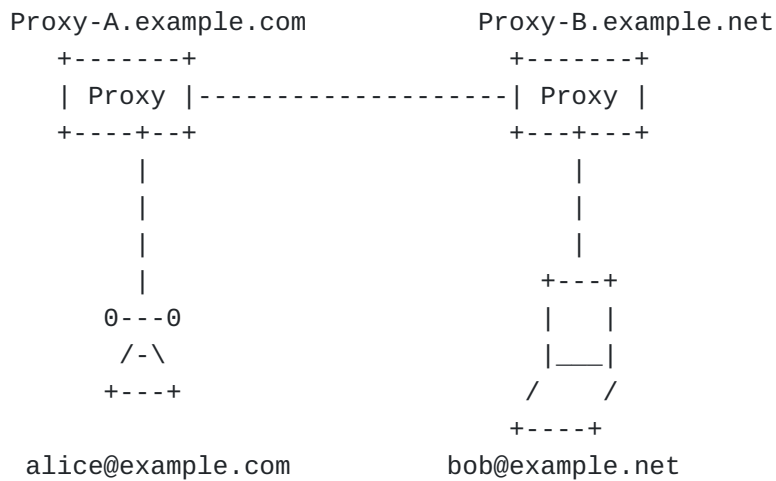
---

## 2. Problem statement

[TOC](#)

Consider the SIP [RFC 3261 \(Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.\)](#) [2] actors 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 her INVITE arrived at an outbound proxy `Proxy-A.example.com`. In order to route the request onward, Proxy-A uses [RFC 3263 \(Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol \(SIP\): Location SIP Servers," June 2002.\)](#) [7] resolution and finds that `Proxy-B.example.net` is a valid proxy for `example.net` that uses TLS. Proxy-A.example.com requests a TLS connection to Proxy-B.example.net, and in the TLS handshake each 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 \(SIP\) \(Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol \(SIP\)," May 2009.\)](#) [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.

---

### 3. Restricting usage to SIP

[TOC](#)

This memo defines a certificate profile for restricting the usage of a domain name binding to usage as a SIP domain name. [RFC 5280 \(Cooper, D., Santesson, S., Farrell, S., Boyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile," May 2008.\)](#) [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 3.1 \(Extended Key Usage values for SIP domains\)](#)).

---

#### 3.1. Extended Key Usage values for SIP domains

[TOC](#)

[RFC 5280 \(Cooper, D., Santesson, S., Farrell, S., Boyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile," May 2008.\)](#) [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 }
```

---

#### 4. Using the SIP EKU in a certificate

[TOC](#)

Section 7.1 of [Domain Certificates in the Session Initiation Protocol \(Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol \(SIP\)," May 2009.\)](#) [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 step given below as a part of the certificate validation:

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

\*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.

---

## 5. Implications for a Certification Authority

[TOC](#)

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.

---

## 6. Security Considerations

[TOC](#)

This memo defines an EKU X.509 certificate extension that restricts the 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.

---

## 7. IANA Considerations

[TOC](#)

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.

---

## 8. Acknowledgments

[TOC](#)

The following IETF contributors provided substantive input to this document: Jeroen van Bommel, 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.

---

## 9. Normative References

[TOC](#)

[1]	Bradner, S., " <a href="#">Key words for use in RFCs to Indicate Requirement Levels</a> ," RFC 2119, March 1997 ( <a href="#">TXT</a> ).
[2]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, " <a href="#">SIP: Session Initiation Protocol</a> ," RFC 3261, June 2002 ( <a href="#">TXT</a> ).
[3]	Cooper, D., Santesson, S., Farrell, S., Boyen, S., Housley, R., and W. Polk, " <a href="#">Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile</a> ," RFC 5280, May 2008 ( <a href="#">TXT</a> ).
[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, " <a href="#">Session Initiation Protocol (SIP): Location SIP Servers</a> ," RFC 3263, June 2002 ( <a href="#">TXT</a> ).
[8]	Gurbani, V., Lawrence, S., and A. Jeffrey, " <a href="#">Domain Certificates in the Session Initiation Protocol (SIP)</a> ," draft-ietf-sip-domain-certs-04.txt (work in progress), May 2009 ( <a href="#">TXT</a> ).

---

[TOC](#)



## 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

[TOC](#)

	Scott Lawrence
	Nortel Networks, Inc.
	600 Technology Park
	Billerica, MA 01821
	USA
Phone:	+1 978 248 5508
Email:	<a href="mailto:scott.lawrence@nortel.com">scott.lawrence@nortel.com</a>
	Vijay K. Gurbani
	Bell Laboratories, Alcatel-Lucent
	1960 Lucent Lane
	Room 9C-533
	Naperville, IL 60566
	USA
Phone:	+1 630 224-0216
Email:	<a href="mailto:vkg@bell-labs.com">vkg@bell-labs.com</a>