SIP WG
Internet-Draft
Updates: 3261 (if approved)
Intended status: Best Current Practice
Expires: January 10, 2008

V. Gurbani
Bell Laboratories, Alcatel-Lucent
S. Lawrence
Pingtel Corp.
A. Jeffrey
Bell Laboratories, Alcatel-Lucent

July 9, 2007

Domain Certificates in the Session Initiation Protocol (SIP)
draft-gurbani-sip-domain-certs-06

Status of this Memo

Copyright Notice

Abstract

This document provides a profile of PKIX-compliant certificates for the purpose of domain authentication in the Session Initiation Protocol (SIP).

Table of Contents

1. Terminology 3
1.1. Key Words 3
1.2. Abstract syntax notation 3
2. Introduction 3
3. Problem statement 3
4. SIP domain to host resolution 4
5. The need for mutual interdomain authentication 5
5.1. Restricting usage to SIP 6
5.1.1. Extended Key Usage values for SIP domains 6
6. Guidelines for a Certification Authority 7
7. Guidelines for a service provider 7
8. Behavior of SIP entities 8
8.1. Finding SIP Identities in a Certificate 8
8.2. Comparing SIP Identities 9
8.3. Client behavior 10
8.4. Server behavior 10
8.5. Proxy behavior 11
8.6. Registrar behavior 11
8.7. Redirect server behavior 11
8.8. Virtual SIP Servers and Certificate Content 12
9. Security Considerations 12
9.1. Connection authentication using Digest 13
10. Acknowledgments 13
11. References 14
11.1. Normative References 14
11.2. Informative References 14
Editorial Comments . . . . . .
Appendix A. ASN.1 Module 15
Authors' Addresses 16
Intellectual Property and Copyright Statements 17

1. Terminology

1.1. 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].

1.2. Abstract syntax notation

All X.509 certificate X.509 [5] extensions are defined using ASN.1 X.680 [6],X.690 [7].

2. Introduction

Transport Layer Security (TLS) [3] has started to appear in an increasing number of Session Initiation Protocol (SIP) [2] implementations. In order to use the authentication capabilities of TLS, certificates as defined by the Internet X.509 Public Key Infrastructure RFC 3280 [4] are required.

Existing SIP specifications do no sufficiently specify how to use certificates for domain (as opposed to host) authentication. This document attempts to provide sufficient guidance to ensure interoperability and uniform conventions for the construction of SIP domain certificates.

The discussion in this document is pertinent to an X.509 PKIX-compliant certificate used for a TLS connection; it may not apply to use of such certificates with S/MIME, for instance.

3. Problem statement

TLS uses X.509 Public Key Infrastructure [4] to bind an identity, or a set of identities, to the subject of a X.509 certificate. Accordingly, the recommendations of the SIP working group have been to populate the X.509v3 subjectAltName extension with an identity. However, this is under-specified in RFC 3261, which mentions subjectAltName in conjunction with S/MIME only and not TLS. The security properties of TLS and S/MIME as used in SIP are different: X.509 certificates used for S/MIME are generally used for end-to-end authentication and encryption, thus they serve to bind the identity of a user to the certificate. On the other hand, X.509 certificates used for TLS serve to bind the identities of the domain sending or receiving the SIP messages.

While RFC3261 provides adequate guidance on the use of X.509 certificates used for S/MIME, it is relatively silent on the use of such certificates for TLS. The concept of what should be contained in a site (or domain) certificate in RFC3261 is quoted below (Section 26.3.1):

> Proxy servers, redirect servers and registrars SHOULD possess a site certificate whose subject corresponds to their canonical hostname.

The lack of specifications leads to problems when attempting to interpret the certificate contents for TLS connections in a uniform manner.

This document addresses two concerns related to X.509 certificates used in SIP. First, it shows how the certificates are to be used for mutual authentication when both the client and server possess appropriate certificates; and second, it provides normative behavior for matching the DNS query string with an identity stored in the X.509 certificate (following the accepted practice of the time, legacy X.509 certificates may store the identity in the Common Name (CN) field of the certificate [Comment.1] instead of the currently used subjectAltName extension. Furthermore, it is permissible for a certificate to contain multiple identifiers for the Subject. As such, this document specifies the appropriate matching rules.) And finally, this document also provides guidelines for a Certification Authority (CA) for issuing certificates to be used with SIP and to service providers for assigning certificates to SIP servers.

The rest of this document is organized as follows: the next section provides an overview of the most primitive case of a client using DNS to access a SIP server and the resulting authentication steps. Section 5 looks at the reason why mutual inter-domain authentication is desired in SIP, and the lack of normative text and behavior in RFC3261 for doing so. Section 6 outlines general guidelines for the CA. Section 8 provides normative behavior of the SIP entities (user agent clients, user agent servers, registrars, redirect servers, and proxies) that need perform authentication based on X.509 certificates. Section 9 includes the security considerations.

4. SIP domain to host resolution

Routing in SIP is performed by having the client execute RFC 3263 [8] procedures on a URI, called the "Application Unique String (AUS) (c.f. Section 8 of RFC 3263 [8]). These procedures take as input a SIP AUS (the SIP domain) and return an ordered set containing one or more IP addresses, and a port number and transport corresponding to

each IP address in the set (the "Expected Output") by querying an Domain Name Service (DNS). If the transport indicates the use of TLS, then a TLS connection is opened towards the server on a specific IP address and port. The server presents an X.509 certificate to the client for verification as part of the initial TLS handshake.

The client should determine the subjects of the certificate (see Section 8.1) and compare these values to the AUS. If any subject match is found, the server is considered to be authenticated and subsequent signaling can now proceed over the TLS connection. Matching rules for X.509 certificates and the normative behavior for clients is specified in Section 8.3.

As an example: a request is to be routed to the SIP address "sips:alice@example.com". This address requires a secure connection to the SIP domain "example.com", which is used as the SIP AUS value. Through a series of untrusted DNS manipulations, that AUS is mapped to a set of host addresses and transports, from which an address appropriate for use with TLS is selected. A connection is established to that server, which presents a certificate with the subject "sip:example.com". Since the SIP AUS matches the subject of the certificate, the server is considered authenticated.

> This is the way HTTPS operates, and SIPS simply borrows this behavior from HTTP.
>
> A domain name in an X.509 certificates is properly interpreted only as a sequence of octets to be compared to the URI used to reach the host. No inference should be made based on the DNS name hierarchy.

5. The need for mutual interdomain authentication

RFC 3261 [2] section 26.3.2.2 "Interdomain Requests" discusses the requirement that when a TLS connection is created between two proxies, those proxies should each authenticate the other by validating the certificate presented by the other during the TLS handshake and comparing the subject of those certificates to the expected domain name.

For example, suppose 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 [8] resolution and finds that proxyB.example.net is a valid proxy for example.net using TLS.

proxyA.example.com requests a TLS connection to proxyB.example.net, and each presents a certificate to authenticate that connection.

The authentication problem for proxyA is straightforward - if we assume secure DNS, then proxyA already knows that proxyB is a valid proxy for the SIP domain example.net, so it only needs a valid certificate from proxyB that contains the fully qualified host name proxyB.example.net, or a SIP URI that asserts proxy B's authority over example.net domain, i.e., a certificate that asserts the identity "sip:example.net". [Comment.2]

The problem for proxyB is different, however; 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.

5.1. Restricting usage to SIP

The intent of this draft is to define certificate usage for binding a SIP domain name to a connection. 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 may well 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 [4] 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.

5.1.1. Extended Key Usage values for SIP domains

RFC 3280 [4] specifies the extended key usage 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

extended key usage 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 crytographic way.

The extended key usage 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 DNS name(s) in question. 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 8.1 for how the presence of an id-kp-sipDomain value affects the interpretation of the certificate.

6. Guidelines for a Certification Authority

The procedures and practices employed by the certification authority (CA) MUST ensure that the correct values for the extended key usage extension and subjectAltName are inserted in each certificate that is issued.

7. Guidelines for a service provider

When assigning certificates to proxy servers, registrars, and redirect servers, a service provider MUST ensure that the SIP AUS used to address the server is present as an identity in the subjectAltName field of the certificate.

8. Behavior of SIP entities

This section is normative; it specifies the behavior of SIP entities when using X.509 certificates to determine an authenticated SIP domain identity.

8.1. Finding SIP Identities in a Certificate

Procedures for determining a certificate's validity period, its certification path, its presence on a certificate revocation list, and other checks are described in RFC 3280 [4]; implementations must follow checks as prescribed in RFC3280. This document adds rules for interpreting an X.509 certificate for use in SIP.

Given an X.509 certificate that the above checks have found to be acceptable, the following describes how to determine what SIP identity or identities it contains. Note that a single certificate MAY serve more than one purpose - that is, it MAY contain identities not valid for use in SIP, and/or MAY contain more than one identity for use in SIP.

1. The extendend 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 contains any extended key usage (EKU) value other than id-kp-sipDomain, and does not contain the id-kp-sipDomain value, then the certificate MUST NOT be accepted as valid for use as a SIP certificate, and none of the identities it contains are acceptable for SIP domain authentication.

   * If the certificate does not contain any EKU values, it is a matter of local policy whether or not to accept it for use as a SIP certificate.

2. Examine the values in the subjectAltName field. The contents of subjectAltName field and the constraints that may be imposed on them are defined in Section 4.2.1.7 of RFC 3280 [4]. The subjectAltName field may be empty, or may not exist at all, or it may contain more than one identity. Each value in the subjectAltName has a type; the only types acceptable for encoding a SIP domain identity are:

   URI If the scheme of the URI value is 'sip' (URI scheme tokens are always case insensitive), and there is no userinfo component in the URI (there is no '@'), then the hostpart is a SIP domain identity. A URI value that does contain a userpart MUST NOT be used as a domain identity (such a certificate identifies an individual user, not a server for the domain).

DNS A domain name system identifier MAY be accepted as a SIP domain identity. An implementation MAY choose to accept a DNS name as a domain identity, but only when no identity is found using the URI type above.

3. If and only if the subjectAltName is empty or does not exist, the client MAY examine the Subject Common Name (CN) field of the certificate. If a valid DNS name is found there, the implementation MAY use this value as a SIP domain identity. The use of the CN value is allowed for backward compatibility, but is NOT RECOMMENDED.

The above procedure yields a set containing zero or more identities from the certificate. A client uses these identities to authenticate a server (see Section 8.3) and a server uses them to authenticate a client (see Section 8.4).

8.2. Comparing SIP Identities

When comparing two values as SIP identities:

Implementations MUST compare only that part of each identifier (from the procedure defined in Section 8.1 that is a DNS name. Any scheme or parameters extracted from an identifier MUST NOT be used in the comparison procedure described below.

The values MUST be compared as DNS names, which means that the comparison is case insensitive.

The match MUST be exact:

A suffix match MUST NOT be considered a match. For example, "foo.example.com" does not match "example.com".

Any form of wildcard, such as a leading "." or "*.", MUST NOT be considered a match. For example, "foo.example.com" does not match ".example.com" or "*.example.com".

Note: RFC 2818 [9] (HTTP over TLS) allows the dNSName component to contain a wildcard; e.g., "DNS:*.example.com". RFC 3280 [4], while not disallowing this explicitly, leaves the interpretation of wildcards to the individual specification.

RFC 3261 does not provide any guidelines on the presence of wildcards in certificates. The consensus from the working group discussion leans in the favor of not using them in SIP.

8.3. Client behavior

A client uses the SIP AUS (the SIP domain name) to query a (possibly untrusted) DNS to obtain a result set, which is a one or more SRV and A records identifying the server for the domain (see Section 4 for an overview.)

The SIP server, when accepting a TLS connection, presents its certificate to the client for authentication. The client MUST determine the SIP identities in the server certificate using the procedure in Section 8.1. Then, the client MUST compare the original SIP domain name (the AUS) used as input to the server location procedures [8] to the set of SIP domain identities obtained from the certificate.

- If the set of SIP identities is empty, the server is not authenticated.

- If the AUS matches any SIP domain identity in the set, the server is authenticated for the domain (SIP identity matching rules are described in Section 8.2.)

If the server is not authenticated, the client MUST close the connection immediately.

8.4. Server behavior

When a server accepts a TLS connection, it presents its own X.509 certificate to the client. To authenticate the client, the server asks the client for a certificate. If the client possesses a certificate, it is presented to the server. If the client does not present a certificate, it MUST NOT be considered authenticated.

Whether or not to close a connection if the client cannot present a certificate is a matter of local policy, and depends on the authentication needs of the server for the connection. Some currently deployed servers use Digest authentication to authenticate individual requests on the connection, and choose to treat the connection as authenticated by those requests for some purposes (but see Section 9.1).

If the server requires client authentication for some local purpose, then it MAY implement a policy of allowing the connection only if the client is authenticated. For example, if the server is an inbound proxy that has peering relationships with the outbound proxies of other specific domains, it might only allow connections authenticated as coming from those domains.

The server MUST obtain the set of SIP domain identities from the client certificate as described in Section 8.1. Because the server accepted the TLS connection passively, unlike a client, it does not possess an AUS for comparison. Instead, server policies can use the authenticated SIP domain identity to make authorization decisions.

For example, a very open policy could be to accept any X.509 certificates and validate them using the procedures in RFC 3280; if they validate, the identity is accepted and logged. Alternatively, the server could have a list of all SIP domain names is allowed to accept connections from; when a client presents its certificate, for each identity in the client certificate, the server searches for it in the list of acceptable domains to decide whether or not to accept the connection. Other policies that make finer distinctions are possible.

Note that the decision of whether or not the authenticated connection to the client is appropriate for use to route new requests to the authenticated domain is independent of whether or not the connection is authenticated; the normal routing rules for SIP as defined elsewhere MUST be used.

8.5. Proxy behavior

A proxy MUST use the procedures defined for a User Agent Server (UAS) in Section 8.4 when authenticating a connection from a client.

A proxy MUST use the procedures defined for a User Agent Client (UAC) in Section 8.3 when requesting an authenticated connection to a UAS.

If a proxy adds a Record-Route when forwarding a request with the expectation that the route is to use secure connections, it MUST insert into the Record-Route header a URI that corresponds to an identity for which it has a certificate; if it does not, then it will not be possible to create a secure connection using the value from the Record-Route as the AUS.

8.6. Registrar behavior

A SIP registrar, acting as a server, follows the normative behavior of Section 8.4. It may accept a TLS connection from the client, present its certificate, and then challenge the client with HTTP Digest.

8.7. Redirect server behavior

A SIP redirect server follows the normative behavior of Section 8.4. It may accept a TLS connection from the client, present its

certificate, and then challenge the client with HTTP Digest.

8.8. Virtual SIP Servers and Certificate Content

The closest guidance in SIP today regarding certificates and virtual SIP servers occurs in SIP Identity ([11], Section 13.4). The quoted section states that, "... certificates have varying ways of describing their subjects, and may indeed have multiple subjects, especially in the 'virtual hosting' cases where multiple domains are managed by a single application."

The above quote appears to imply that a certificate that is shared among virtual servers will have multiple identifiers in the subjectAltName field, each corresponding to a discrete virtual server that represents a single domain (PKIX-compliant certificates have exactly one Subject field and at most one subjectAltName field, which may contain multiple identifiers for the Subject.)

Since only one certificate is needed for multiple domains, the keying material management is straightforward, but such a certificate MUST be revoked if ANY identifier in the certificate is no longer associated with the holder of the private key for the the certificate.

The TLS extended client hello [10] allows a TLS client to provide to the TLS server the name of the server to which a connection is desired. Thus, the server can present the correct certificate to establish the TLS connection.

9. Security Considerations

The goals of TLS (when used with X.509 certificates) include the following security guarantees at the transport layer:

Confidentiality: packets tunneled through TLS can only be read by the sender and receiver.

Integrity: packets tunneled through TLS cannot be undetectably modified on the connection between the sender and receiver.

Authentication: each principal is authenticated to the other as possessing a private key for which a certificate has been issued. Moreover, this certificate has not been revoked, and is backed by a certificate chain leading to a trusted certification authority.

We expect appropriate processing of domain certificates to provide the following security guarantees at the application level:

Confidentiality: SIPS messages from alice@example.com to bob@example.edu can be read only by alice@example.com, bob@example.edu, and SIP proxies issued with domain certificates for example.com or example.edu.

Integrity: SIPS messages from alice@example.com to bob@example.edu cannot be undetectably modified on the links between alice@example.com, bob@example.edu, and SIP proxies issued with domain certificates for example.com or example.edu.

Authentication: alice@example.com and proxy.example.com are mutually authenticated, and moreover proxy.example.com is authenticated to alice@example.com as an authoritative proxy for domain example.com. Similar mutual authentication guarantees are given between proxy.example.com and proxy.example.edu and between proxy.example.edu and bob@example.edu. As a result, alice@example.com is transitively mutually authenticated to bob@example.edu (assuming trust in the authoritative proxies for example.com and example.edu).

9.1. Connection authentication using Digest

Digest authentication in SIP provides for authentication of the message sender to the challenging UAS. As commonly deployed, it provides only very limited integrity protection of the authenticated message. Many existing deployments have chosen to use the Digest authentication of one or more messages on a particular connection as a way to authenticate the connection itself - and by implication, authenticating other (unchallenged) messages on that connection. Some even choose to similarly authenticate a UDP source address and port based on the Digest authentication of a message received from that address and port. This use of Digest goes beyond the assurances it was designed to provide, and is NOT RECOMMENDED. Authentication of the domain at the other end of a connection SHOULD be accomplished using TLS and the certificate validation rules described by this specification instead.

10. 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, and Stephen Kent.

11. References

11.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", 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] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[4] 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.

[5] International International Telephone and Telegraph Consultative Committee, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", CCITT Recommendation X.509, November 1988.

[6] 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.

[7] 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.

11.2. Informative References

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

[9] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[10] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006.

[11] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-sip-identity-06.txt (work in progress), October 2005.

Editorial Comments

[Comment.1] Stephen Kent: PKIX standards made an exception for RFC 822 names in legacy certificates, but not for DNS names or URIs! There is a private extension, developed by Netscape for representing a DNS name in a certificate prior to the advent of SAN. I think it's rather late to be accomodating certificates that are not compiant with RFC 3280, a spec that is 5 years old.

[Comment.2] (authors) and Stephen Kent: Actually, even if DNSSEC provides a trusted host name, it is sufficient for proxyB to have presented a certificate that contains a SIP identity for example.net, so authentication of just the proxyB hostname has little value since it would not be sufficient without DNSSEC.

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(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

Vijay K. Gurbani
Bell Laboratories, Alcatel-Lucent
2701 Lucent Lane
Room 9F-546
Lisle, IL 60532
USA

Phone: +1 630 224-0216
Email: vkg at bell hyphen labs dot com

Scott Lawrence
Pingtel Corp.
400 West Cummings Park
Suite 2200
Woburn, MA 01801
USA

Phone: +1 781 938 5306
Email: slawrence@pingtel.com

Alan S.A. Jeffrey
Bell Laboratories, Alcatel-Lucent
2701 Lucent Lane
Room 9F-534
Lisle, IL 60532
USA

Email: ajeffrey at bell hyphen labs dot com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).