TOC

SIP WG	V. Gurbani
Internet-Draft	Bell Laboratories, Alcatel-Lucent
Intended status: BCP	S. Lawrence
Expires: May 11, 2008	Bluesocket Inc.
	A. Jeffrey
	Bell Laboratories, Alcatel-Lucent
	November 08, 2007

Domain Certificates in the Session Initiation Protocol (SIP) DOCNAME

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 May 11, 2008.

Abstract

This document describes how to interpret certain information in a X.509 PKIX-compliant certificate used in a Transport Layer Security (TLS) connection. More specifically, it describes how to find the right identity for authentication in such certificates and how to use it for mutual authentication.

Table of Contents

1. Terminology
    1.1. Key Words
2. Introduction
3. Problem statement
4. SIP domain to host resolution
5. The need for mutual interdomain authentication
6. Guidelines for a service provider
7. Behavior of SIP entities
    7.1. Finding SIP Identities in a Certificate
    7.2. Comparing SIP Identities
    7.3. Client behavior
    7.4. Server behavior
    7.5. Proxy behavior
    7.6. Registrar behavior
    7.7. Redirect server behavior
    7.8. Virtual SIP Servers and Certificate Content
8. Security Considerations
    8.1. Connection authentication using Digest
9. IANA Considerations
10. Acknowledgments
11. References
    11.1. Normative References
    11.2. Informative References
§ 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].

TOC

2. Introduction

Transport Layer Security (TLS) [3] (Dierks, T. and C. Allen, “The TLS Protocol Version 1.0,” January 1999.) has started to appear in an increasing number of Session Initiation Protocol (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.) implementations. In order to use the authentication capabilities of TLS, certificates as defined by the Internet X.509 Public Key Infrastructure 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.) [4] are required.

Existing SIP specifications do no sufficiently specify how to use certificates for domain (as opposed to host) authentication. This document provides 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

TOC

TLS uses X.509 Public Key Infrastructure [4] (Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” April 2002.) 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 per-hop 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 shows how the certificates are to be used for mutual authentication when both the client and server possess appropriate certificates. It also contains 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] (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 compliant with RFC 3280, a spec that is 5 years old.) instead of the currently used Subject Alternative Names (subjectAltName) extension. Furthermore, it is permissible for a certificate to contain multiple identifiers for the Subject via the subjectAltName extension. As such, this document specifies appropriate matching rules to encompass various Subject identity representation options. And finally, this document also provides guidelines 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 (The need for mutual interdomain authentication) 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 7 (Behavior of SIP entities) provides normative behavior on the SIP entities (user agent clients, user agent servers, registrars, redirect servers, and proxies) that need perform authentication based on X.509 certificates. Section 8 (Security Considerations) includes the security considerations.

---

4. SIP domain to host resolution

TOC

Routing in SIP is performed by having the client execute RFC 3263 (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Location SIP Servers,” June 2002.) [5] procedures on a URI, called the "Application Unique String (AUS) (c.f. Section 8 of RFC 3263 (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Location SIP Servers,” June 2002.) [5]). 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 to 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 extract identifiers from the Subject and subjectAltName extension in the certificate (see Section 7.1 (Finding SIP Identities in a Certificate)) and compare these values to the AUS. If any identifier 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 7.3 (Client behavior).
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", so that is 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 asserting an identity of "sip:example.com". Since the host portion of the SIP AUS matches the subject of the certificate, the server is authenticated.

> SIPS borrows this behavior from HTTPS. However, to be pedantic, RFC 2818 (Rescorla, E., “HTTP Over TLS,” May 2000.) [6] prefers that the identity be conveyed as a subjectAltName extension of type dNSName instead of the commonly used practice of conveying the identity in the CN field of the Subject field. Similarly, this document RECOMMENDS that the SIP identity be conveyed as a subjectAltName extension of type uniformResourceIdentifier (c.f. Section 6 (Guidelines for a service provider), Section 7.1 (Finding SIP Identities in a Certificate)).
>
> 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

TOC

Consider the SIP trapezoid shown in Figure 1 (SIP Trapezoid).

```
proxyA.example.com ------------ proxyB.example.net
       |                            |
       |                            |
       |                            |
       |                          +---+
     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 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.) [5] 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.

> 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] section 26.3.2.2 "Interdomain Requests" states that when a TLS connection is created between two proxies, each should authenticate the other by validating the certificates exchanged during the TLS handshake and by comparing the subject of those certificates to the expected domain name. However, RFC3261 does not make any reference to using an identifier extracted specifically from the Subject field as opposed to the subjectAltName when comparing against the domain name.

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] ((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.) Normative behavior for proxyA is outlined in Section 7.3 (Client behavior).

The problem for proxyB is slightly more complex since it accepted the TLS request passively. Thus, it does not possess an equivalent AUS that proxyA did; instead, it uses local policies to consider the client authenticated. The normative behavior for servers is provided in Section 7.4 (Server behavior).

6. Guidelines for a service provider

TOC

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.

Service providers MAY continue the practice of using existing certificates for SIP usage with the identity conveyed in the Subject field; however, such usage is NOT RECOMMENDED for new certificates, which MUST contain the identity in the subjectAltName extension.

7. Behavior of SIP entities

TOC

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

7.1. Finding SIP Identities in a Certificate

TOC

Procedures for constructing a certificate path and checking revocation status to determine the validity of a certificate are described in 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.) [4]; implementations must follow checks as prescribed therein. This document adds additional rules for interpreting an X.509 certificate for use in SIP.

I-D.sip-eku (Lawrence, S. and V. Gurbani, “Using Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates,” 2007.) [9] describes the method to validate any Extended Key Usage values found in the certificate for a SIP domain. Implementations MUST perform the checks prescribed by that specification.

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 one or more identities that are valid for use in SIP.

1. 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 (Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” April 2002.) [4]. The subjectAltName field may not be present or it may contain one or more identities. 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.

2. If and only if the subjectAltName does not appear in the certificate, 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 7.3 (Client behavior)) and a server uses them to authenticate a client (see Section 7.4 (Server behavior)).

7.2. Comparing SIP Identities

TOC

When comparing two values as SIP identities:

> Implementations MUST compare only that part of each identifier (from the procedure defined in Section 7.1 (Finding SIP Identities in a Certificate) 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". [Comment.3] ((authors): RFC 2818 (HTTP over TLS) allows the dNSName component to contain a wildcard; e.g., "DNS:*.example.com". RFC 3280, 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.)

7.3. Client behavior

TOC

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 (SIP domain to host resolution) for an overview.)
The SIP server, when establishing 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 7.1 (Finding SIP Identities in a Certificate). Then, the client MUST compare the original SIP domain name (the AUS) used as input to the server location procedures [5] (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Location SIP Servers,” June 2002.) to the SIP domain identities obtained from the certificate.

- If there were no identities found in the server certificate, the server is not authenticated.

- If the AUS matches any SIP domain identity obtained from the certificate when compared as described in section Section 7.2

(Comparing SIP Identities), the server is authenticated for the domain.

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

7.4. Server behavior

TOC

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 8.1 (Connection authentication using Digest)).
>
> 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 7.1 (Finding SIP Identities in a Certificate). Because the server accepted the TLS connection passively, unlike a client, it does not possess an AUS for comparison. Nonetheless, 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 client domain is independent of whether or not the connection is authenticated; the connect-reuse (Mahy, R., Gurbani, V., and B. Tate,

“Connection Reuse in the Session Initiation Protocol,” October 2007.) [10] draft discusses this aspect in more detail.

7.5. Proxy behavior

TOC

A proxy MUST use the procedures defined for a User Agent Server (UAS) in Section 7.4 (Server behavior) when authenticating a connection from a client.

A proxy MUST use the procedures defined for a User Agent Client (UAC) in Section 7.3 (Client behavior) 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.

7.6. Registrar behavior

TOC

A SIP registrar, acting as a server, follows the normative behavior of Section 7.4 (Server behavior). When it accepts a TLS connection from the client, it present its certificate. Depending on the registrar policies, it may challenge the client with HTTP Digest.

7.7. Redirect server behavior

TOC

A SIP redirect server follows the normative behavior of Section 7.4 (Server behavior). It may accept a TLS connection from the client, present its certificate, and then challenge the client with HTTP Digest.

7.8. Virtual SIP Servers and Certificate Content

TOC

The closest guidance in SIP today regarding certificates and virtual SIP servers occurs in SIP Identity ([8] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.), 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 is incorrect, in that it implies that one certificate can have multiple subjectAltName (or Subject) fields, each corresponding to a discrete virtual server that represents a single domain; actually, a PKIX-compliant certificate has exactly one Subject field and at most one subjectAltName (the subjectAltName 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 certificate.

The TLS extended client hello [7] (Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, “Transport Layer Security (TLS) Extensions,” April 2006.) 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.

8. Security Considerations

TOC

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 be read only 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 verifiable by a certificate chain leading to a (locally configured) trust anchor.

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; 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).

8.1. Connection authentication using Digest

TOC

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.

9. IANA Considerations

TOC

This memo does not contain any considerations for IANA.

10. 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. Special acknowledgement goes to

Stephen Kent for extensively reviewing draft versions and suggesting invaluable feedback, edits, and comments.

11. References

TOC

11.1. 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] Dierks, T. and C. Allen, “The TLS Protocol Version 1.0,” RFC 2246, January 1999 (TXT).

[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 (TXT).

11.2. Informative References

TOC

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

[6] Rescorla, E., “HTTP Over TLS,” RFC 2818, May 2000 (TXT).

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

[8] Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” RFC 4474, August 2006 (TXT).

[9] Lawrence, S. and V. Gurbani, “Using Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates,” draft-ietf-sip-eku-00.txt (work in progress), 2007 (TXT).

[10] Mahy, R., Gurbani, V., and B. Tate, “Connection Reuse in the Session Initiation Protocol,” draft-ietf-sip-connect-reuse-08.txt (work in progress), October 2007 (TXT).

Editorial Comments

TOC

Stephen Kent: PKIX standards made an exception for RFC 822 names in legacy certificates, but not for DNS names

Comment. 1:	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 compliant 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.
Comment. 3:	(authors): RFC 2818 (HTTP over TLS) allows the dNSName component to contain a wildcard; e.g., "DNS:*.example.com". RFC 3280, 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.

Authors' Addresses

TOC

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

Scott Lawrence
Bluesocket Inc.
10 North Ave.
Burlington, MA 01803
USA
Phone: +1 781 229 0533
Email: slawrence@bluesocket.com

Alan S.A. Jeffrey
Bell Laboratories, Alcatel-Lucent
2701 Lucent Lane
Room 9F-534
Lisle, IL 60532
USA
Email: ajeffrey@alcatel-lucent.com

Full Copyright Statement

TOC

Intellectual Property