UTA
Internet-Draft
Updates: 6125 (if approved)
Intended status: Standards Track
Expires: 14 September 2021

R. Salz
Akamai Technologies

13 March 2021

Update to Verifying TLS Server Identities with X.509 Certificates draft-rsalz-use-san-01

Abstract

In the decade since [RFC6125] was published, the subjectAlternativeName extension (SAN), as defined in [RFC5280] has become ubiquitous. This document updates [RFC6125] to specify that the fall-back techniques of using the commonName attribute to identify the service must not be used. This document also places some limitations on the use of wildcards in SAN fields.

The original context of [RFC6125], using X.509 certificates for server identity with Transport Layer Security (TLS), is not changed.

Discussion Venues

This note is to be removed before publishing as an RFC.

This draft is discussed in the UTA working group, https://datatracker.ietf.org/wg/uta/.

Source for this draft and an issue tracker can be found at https://github.com/richsalz/draft-rsalz-use-san.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 14 September 2021.

Table of Contents

1. Introduction

In the decade since [RFC6125] was published, the subjectAlternativeName extension (SAN), as defined in [RFC5280] has become ubiquitous. This document updates [RFC6125] to specify that the fall-back techniques of using the commonName attribute to identify the service must not be used. This document also places some limitations on the use of wildcards in SAN fields.

The original context of [RFC6125], using X.509 certificates for server identity with Transport Layer Security (TLS), is not changed. In addition to the examples in that document, the Baseline Requirements of the CA/Browser Forum, [CABBR], might also be useful.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The terminology from [RFC6125] is used here. Specifically, the following terms and brief definition (as a reminder):

* CN-ID: the Common Name element of a Distingiushed Name.

* DNS-ID: a domain name entry in a SAN extension.

3. The New Rules

The CN-ID MUST NOT be used. The appropriate value in the SAN extension MUST be used to get the presented identity of the server.

While not discussed in [RFC6125] this section also implicitly prohibits the use of the Domain Component or emailAddress RDN's.

The following sections repeat the above rule in other forms, for the purpose of updating [RFC6125].

3.1. Designing Application Protocols

Applications should determine which form of name they want to use, and specify the appropriate SAN extension. Unless there are reasons to do otherwise, applications SHOULD use the DNS-ID form.

3.2. Representing Server Identity

Servers MUST NOT request certificates that contain CN-ID in the subject. If the Common Name RDN must be present in the certificate, it MUST be in a form that cannot be mistaken for a CN-ID.

3.3. Verifying Service Identity

When constructing a list of reference identifiers, the client MUST NOT include any CN-ID present in the certificate. This means that section 6.4.4 of [RFC6125] MUST be ignored.

4. Constraints on Wildcards

Wildcard certificates are discussed in section 7.2 of [RFC6125], which says that the specifications "are not clear or consistent" about where a wildcard can appear.

This documents specifies that a wildcard can appear

* only as the left-most label; or

* as the last character in a left-most label

5. Security Considerations

The CN-ID, domainComponent, and emailAddress RDN fields are unstructured free text, and using them is dependant on ordering and encoding concerns. In addition, their evaluation when PKIX nameConstraints are present is ambiguous. This document removes those fields from use, so a source of possible errors is removed.

Because of the ambiguity around wildcards, [RFC6125] mentions that it is possible to have exploitable differences in behavior. By simplifying those practices to one rule, this source of errors should be avoided.

All other security considerations of [RFC6125] and its dependant documents are still relevant.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] 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, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. Informative References

[CABBR] CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", 2020, <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.7.3.pdf>.

Author's Address

Rich Salz
Akamai Technologies
United States of America

Email: rsalz@akamai.com