Internet Engineering Task Force (IETF)
Request for Comments: 7218
Updates: 6698
Category: Standards Track
ISSN: 2070-1721

O. Gudmundsson
Shinkuro Inc.

April 2014

Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)

Abstract

Experience has shown that people get confused when discussing the three numeric fields of the TLSA record. This document specifies descriptive acronyms for the three numeric fields in TLSA records. This document updates the format of the IANA registry created by RFC 6698.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7218.

Table of Contents

1. Introduction

During discussions on how to add DNS-Based Authentication of Named Entities (DANE) [RFC6698] technology to new protocols and services, people were repeatedly confused as to what the numeric values stood for and even the order of the fields of a TLSA record (note that TLSA is not an acronym but a name). This document updates the IANA registry definition for the TLSA record to add a column containing an acronym for each specified field, in order to reduce confusion. This document does not change the DANE protocol in any way.

It is expected that DANE parsers in applications and DNS software can adopt parsing the acronyms for each field.

2. IANA Considerations

This document applies to the "DNS-Based Authentication of Named Entities (DANE) Parameters" registry located at <http://www.iana.org/assignments/dane-parameters>. IANA has added a column with an acronym to each of the sub-registries.

[RFC6698] and this document are the referenced documents for the three sub-registries.

As these acronyms are offered for human consumption, case does not matter; it is expected that software that parses TLSA records will handle upper-, mixed-, or lower-case characters as input.

2.1. TLSA Certificate Usages Registry

The reference for this registry has been updated to include both [RFC6698] and this document.

Value	Acronym	Short Description	Reference
0	PKIX-TA	CA constraint	[RFC6698]
1	PKIX-EE	Service certificate constraint	[RFC6698]
2	DANE-TA	Trust anchor assertion	[RFC6698]
3	DANE-EE	Domain-issued certificate	[RFC6698]
4-254		Unassigned	
255	PrivCert	Reserved for Private Use	[RFC6698]

Table 1: TLSA Certificate Usages

2.2. TLSA Selectors

The reference for this registry has been updated to include both [RFC6698] and this document.

Value	Acronym	Short Description	Reference
0	Cert	Full certificate	[RFC6698]
1	SPKI	SubjectPublicKeyInfo	[RFC6698]
2-254		Unassigned	
255	PrivSel	Reserved for Private Use	[RFC6698]

Table 2: TLSA Selectors

2.3. TLSA Matching Types

The reference for this registry has been updated to include both [RFC6698] and this document.

Value	Acronym	Short Description	Reference
0	Full	No hash used	[RFC6698]
1	SHA2-256	256 bit hash by SHA2	[RFC6234]
2	SHA2-512	512 bit hash by SHA2	[RFC6234]
3-254		Unassigned	
255	PrivMatch	Reserved for Private Use	[RFC6698]

Table 3: TLSA Matching Types

3. Examples of Usage

Two examples are described below.

3.1. TLSA Records Using/Displaying the Acronyms

```
_666._tcp.first.example.  TLSA PKIX-TA CERT SHA2-512 {blob}
_666._tcp.second.example.  TLSA DANE-TA SPKI SHA2-256 {blob}
```

3.2. Acronym Use in a Specification Example

Protocol FOO only allows TLSA records using PKIX-EE and DANE-EE, with selector SPKI, and using SHA2-512.

4. Security Considerations

This document only changes registry fields and does not change the behavior of any protocol. The hope is to reduce confusion, which would lead to better specification and operations.

5. Acknowledgements

Scott Schmit offered really good suggestions to decrease the possibility of confusion. Viktor Dukhovni provided comments from the expert point of view. Jim Schaad, Wes Hardaker, and Paul Hoffman provided feedback during WGLC. Dan Romascanu and Tobias Gondrom pointed out a few defects during the IESG last call.

6. References

6.1. Normative References

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

6.2. Informative References

[RFC6234] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, May 2011.

Author's Address

Olafur Gudmundsson
Shinkuro Inc.
4922 Fairmont Av, Suite 250
Bethesda, MD 20814
USA

EMail: ogud@ogud.com