DANE
Internet-Draft
Updates: 6698 (if approved)
Intended status: Standards Track
Expires: March 23, 2014

O. Gudmundsson
Shinkuro Inc.

September 19, 2013

Adding acronyms to simplify DANE conversations
draft-ietf-dane-registry-acronyms-00

Abstract

Experience has show that people get confused using the three numeric fields the TLSA record. This document specifies descriptive acronyms for the three numeric fields in the TLSA records.

Status of This Memo

This Internet-Draft will expire on March 23, 2014.

Copyright Notice

Table of Contents

1. Introduction

During discussions on how to add DANE [RFC6698] technology to new protocols/services people repeatedly have got confused as what the numeric values stand for and even the order of the fields of a TLSA record. This document updates the IANA registry definition for TLSA record to add a column with 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 parser's in applications and DNS software MAY adopt parsing the acronyms for each field, installed base MAY NOT get updated.

1.1. Requirements notation

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 [RFC2119].

2. IANA considerations

This document applies to "DNS-Based Authentication of Named Entities (DANE) Parameters" located at "http://www.iana.org/assignments/dane-parameters/dane-parameters.xhtml". Each one of the Sub-registries will add a column with an acronym for that field.

[RFC6698] and this document are both to be the reference documents for the three sub-registries.

As these acronyms are offered for human consumption, case does not matter, it is expected that software the parses TLSA records will handle any case use in the input> The expectation is that by using

the acronyms in production systems fewer bad TLSA records will be published.

2.1. TLSA Certificate Usages

Value	Acronym	Short Description	Reference
0	PKIX-CA	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

Note: should the short description be updated to be more expressive ?

Other options suggested for 0: PKIX-TA

2.2. TLSA Selectors

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

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

Table 3: TLSA Matching types

3. Examples of usage

TLSA records using/displaying the acronyms:

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

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 and lead to better specification and operations.

5. Acknowledgements

Scott Schmit offered real good suggestions to decrease the possibility of confusion. Viktor Dukhovni provided comments from expert point of view.

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

Appendix A. Document history

[RFC Editor: Please remove this section before publication]

00 Initial version

01 Updated version based on some comments ready for WGLC

00 WG version almost identical to 01

Author's Address

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

Email: ogud@ogud.com