DANE
Internet-Draft
Intended status: Informational
Expires: August 18, 2014

O. Gudmundsson
Shinkuro Inc.

February 14, 2014

# Harmonizing how applications specify DANE-like usage
# draft-ogud-dane-vocabulary-02

Abstract

There is no standard terminology as how to talk about use of DNS in various application contexts, this document goal is to facilitate creation of such a vocabulary/taxonomy.

This document started out as proposal for specific word usage for specifications of adding DANE like technology by different protocols/services. DANE is a method for specifying in DNS records acceptable keys/certificates for application servers.

The terms defined in this document should be applicable to all uses of service specification that uses DNS records.

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 http://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 August 18, 2014.

Table of Contents



## 1. Introduction

DNS [RFC1034] is being used by many protocols to express where services are located on the internet, today there is no good way to express exactly what people have in mind when specifying a new service/protocol exactly and in concise manner how the service is looked up in the DNS.

DANE [RFC6698] is a powerful new way to provide/amend how authentication/authorization/confidentiality of a connection to a server can be protected by leveraging DNSSEC [RFC4033] [RFC4034] [RFC4035] for the establishment of TLS connection [RFC5246] [RFC6347] which in many cases uses PKIX [RFC5280]. All of these technologies are complicated. People familiar with one or two are not necessarily familiar with all the parts that needed to apply DANE like mechanism to other protocols.

The goal of this document is three fold:

- To provide common vocabulary for usage of DNS records in service specification.

- To provide an overview of the non protocol specific parts needed to specify an DANE like addition.

- To provide a common framework for such specifications making it easy to review/compare the specifications. An important goal is to allow the new specifications to avoid repeating explanations and/or definitions.

Number of RFC's in the past have tried to use consistent terminology when specifying how to access services both in the context of security TLS with X.509 [RFC6125] and without security [RFC2782]. The terminology in this document is not identical but concepts are similar. The hope is that once the standard terminology is specified, as simple documents can provide a mapping if one is needed.

This version of the document aims to hide complexity and focus on generalities. This is done to make it easier for the reader to decide if the terms here are of use and if it is worthwhile for the DANE WG to adopt this document. Descriptions of complexities can be added in later versions if the WG decides that is needed.

When notation "foo/bar" is used below that is because the editor is not sure if both apply or which one is more appropriate, please advise.

## 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. Proposed Terms

The terms below are being proposed to avoid confusion when reading protocol specifications related to DNS and DANE, for various application protocols.

At this point all the terms below are proposals and better terms are welcome.

### 2.1. DNS Navigation Records

DNS Navigation refers to any records used to traverse the DNS tree to find the records requested. This includes

NS records: that provide a referral to DNS servers for more specific part of the name being looked up. Example: name server for "example." will hand out a referral to server for "bar.example." when asked about "foo.bar.example."

CNAME records: records that change the location of an record, this for all practical purposes a pointer that only applies to that specific name.

DNAME records: specify a rewrite rule for a name to a new name. Example: "bar.example." DNAME "foo.example." means that "www.bar.example." is to be looked up as "www.foo.example". DNAME applies to names that are longer than the name it, i.e. "bar.example." is not rewritten but "www.bar.example." is.

DANE specification explicitly requires all of these records to be validated by DNSSEC.

See section Section 2.2

While traversing the DNS tree other records like A and AAAA are used but these records do not change the "navigation", these records do not explicitly need to be protected as the data retrieved from the addresses is expected to be protected.

## 2.2. DNS Integrity

DNSSEC defines a records and procedures to provide integrity and authentication to data stored in DNS [RFC4034]. The records used to provide the keying information and chain of trust are DNSKEY, DS records. NSEC/NSEC3 provide information about existence/non-existence of the requested information. RRSIG provides a digital signature for a RRset.

DNSSEC provides both Integrity and Authenticity i.e. it says the records came from the right source and have not been changed.

Any DNS record that is DNS Integrity protected, will pass DNSSEC validation for all DNS Navigation records leading to the name and the record itself also passes DNSSEC validation.

In the case of CNAME and DNAME that go "sideways" i.e. to a different branch of the DNS tree, both branches MUST be validated.

## 2.3. Service Specification Records (SSR)

Protocols have different ways to express servers.

- Web servers are frequently specified by name i.e. the "www" prefix, thus its service specification record is: "address record stored at www.<domain>".

- Email servers have a special RR type (MX): SRR= "MX record at <domain>"),

- Jabber uses SRV records: SSR="SRV record at _xxmp-server.tcp.<domain>",

- ENUM uses NAPTR records etc.

- In addition there are also protocols that use a combination like S-NAPTR a schema where NAPTR records are used to specify where to look for SRV records. For all practical purposes NAPTR + SRV should combined be treated as the Service Specification.

For a DANE like specification it has to be clear as what the service specification records are and these records require DNS Integrity.

NOTE: when a client supplies a string to the server as a indicator of what service the the client wants, the string supplied MAY depend on redirection in DNS navigation as well as results of NAPTR records, etc. See section Section 2.6.

NOTE: when NAPTR records as are used they should be treated same way as DNS Navigation records even though strictly speaking it is the application that evaluates the NAPTR record.

NOTE: When there is a CNAME at the name service is expected to be specified at, that can be either a DNS Navigation record or a Service Specification Record. Protocol specification should provide guidance on interpretation.

## 2.4. Service Address Records (SAR)

These are the address records for the servers that offer the service.

In some cases the Service Specification records reside at the same name or are the same as the Service Address records. Example: original TLS/DANE[RFC6698], thus both SSR and SAR records are covered by the same DNS integrity rule.

## 2.5. Application Authentication Records (AAR)

This term refers to the records that provide information about what are acceptable keys or certificates for the servers to offer.

Application Authentication Records MUST be protected by DNS Integrity and each protocol specification MUST explicitly state where/how to look up the Authentication records.

In some cases all the servers for a service will have the same authentication information, in other cases it is going to be on a server by server case. In the first case it is "natural" to store the Authentication records "at" the Service Specification records. In the second case it more natural to store them "at" the Address Records. In this context "at" means the authentication records are stored at name that is an extension of the location example: "_443._tcp.www.example.com" for [RFC6698]. It is possible that neither of these locations is the right one and in that case the specification MUST explicitly express rules as how to find the Authentication Records.

Note: above that there is no a requirement that the Application Address records be covered by DNS Integrity. This is because when the Application Authentication records reside "at" the address records, DNS Integrity is inherited. On the other hand when when Application Authentication Records are stored "at" the Service Specification Record, DNS Integrity for the address records is optional, as any connection to a bogus/wrong server should fail the Authentication tests performed at connection time.

Note: When a Address record search has a CNAME at or DNAME above, the name queried, where should the Authentication Records reside ? With CNAME or with final address record ?

## 2.6. Offered Name: Name used when indirection records are used

In many protocols one of the first items presented by the application is a <name> that is "related to"/"derived from" the original query name. When DNAME is used the name queried for might be required to be rewritten into a new name.

To disambiguate these cases following prefix terms are defined. Similar rules apply NAPTR + SRV combinations. It is important for many applications to be able to express what name is presented by the application to the server at connection time.

Query: The name the application issued the query for to discover SSR /service.

Final: The name after all the indirection records have been applied.

SRV The name on the SRV record used.

NAPTR The name on the first NAPTR record used, prefix with Final if that is the one wanted.

Intermediate A particular location in the indirection chain. The specification needs to handle this case if it ever occurs. NOTE: not sure this is needed???ogud???

## 3. Example specification

This section is an short example for a protocol that is like SSH [RFC4253] we will call this protocol HISS. This is not an actual full specification, just here to give an idea of how to go about extending DANE-like to a random protocol using the terminology from this document.

Location of HISS protocol DNS records:

Service Specification Records:
HISS uses address records as the service specification record. This record MUST have "DNS Integrity" as explained in RFC-to-be-this-document. CNAME/DNAME are treated as a DNS Navigation record.

Service Address Records:
see: Service Specification Records.

Application Authentication Records:
The protocol uses the DNS HISSFP that is stored at the same name as the service is specified. The HISSFP record, if present, takes precedence over keys stored in client cache.

Offered Name
Not used.

The HISS protocol and HISSFP DNS RR do not exist

## 4. IANA considerations

None

[RFC Editor: Please remove this section before publication ]

## 5. Security considerations

This documents goal is to improve specifications of adding security via DANE technology to protocols, thus the overwriting goal is to decrease confusion and increase clarity, with the end goal of improving security. This document does not specify a protocol. XX Needs more work XX

## 6. Internationalization Considerations

When selecting terms to use in standards documents it is important to select works that do not confuse international readers. This document goes out of its way in selecting English terms that are dissimilar to avoid confusions.

## 7. Acknowledgements

Number of people have commented that this is interesting work. Peter Saint-Andre tried to apply the terms to one of his documents and provided many good suggestions.

## 8. References

### 8.1. 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.

### 8.2. Informative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4253] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[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, May 2008.

[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, March 2011.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

## Appendix A. Document history

[RFC Editor: Please remove this section before publication ]

02 Textual improvements, applied comments from Peter Saint-Andre.

01 Added definition of offered names, expanded DNAME/CNAME text added NAPTR and SRV.

00 Initial version

## Author's Address

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

Email: ogud@ogud.com