Network Working Group	S. Josefsson	
Internet-Draft	SJD AB	
Intended status: Standards Track	August 23, 2010	
Expires: February 24, 2011		

TOC

Confirming the Certificate structure in TLS with Secure DNS
draft-josefsson-keyassure-tls-00

Abstract

TLS supports X.509 and OpenPGP certificate based mechanisms to authenticate a server. Users want their applications to verify that the certificate provided by the TLS server is in fact associated with the domain name they expect. Instead of trusting a certificate authority to have made this association correctly, and an X.509/OpenPGP implementation to validate that properly, the user might instead trust the authoritative DNS server for the domain name to make that association. This document describes how to use secure DNS to associate the certificate chain transferred by TLS with the intended domain name.

Status of this Memo

Copyright Notice

Table of Contents

---

1. Introduction and Background

TOC

This document provides Transport Layer Security (TLS) (Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” August 2008.) [RFC5246] clients with an alternative way to authenticate the binding between the server's certificate and the domain name expected by the user.

TLS transfers the certificate from the server to the client using the Certificate structure, see section 7.4.2 of RFC 5246. We treat this structure as an opaque value, which results in that we support both X.509 and OpenPGP certificates directly.

Normally the binding between certificate and domain name is verified by using the normal PKIX (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,” May 2008.) [RFC5280] or OpenPGP (Mavrogiannopoulos, N., “Using OpenPGP Keys for Transport Layer Security (TLS) Authentication,” November 2007.) [RFC5081] validation algorithm, possibly together with an application protocol profile. A good overview of the current state is given by [I-D.saintandre-tls-server-id-check] (Saint-Andre, P. and J. Hodges, “Representation and Verification of Domain-Based Application Service Identity in Certificates Used with Transport Layer Security,” August 2010.).

This document specify a way to directly authenticate the server certificate provided by a TLS server using DNSSEC (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, “DNS Security Introduction and Requirements,” March 2005.) [RFC4033] using the CERT record (Josefsson, S., “Storing Certificates in the Domain Name System (DNS),”

March 2006.) [RFC4398]. We specify a new CERT RR type to hold a hash of the Certificate structure sent by a TLS server to a client.

---

2. The TLSCERT Certificate Type of the CERT RR

TOC

The CERT RR [RFC4398] allows expansion by defining new certificate types. The new certificate type "TLSCERT" is defined here. A query on a domain name for the CERT RR may return records of the type CERT, and zero or more of those CERT responses can be of type TLSCERT.
The format of the TLSCERT certificate type is binary. The record contains the SHA-256 (National Institute of Standards and Technology, "Secure Hash Standard," August 2002.) [FIPS.180-2.2002] hash of the Certificate structure as transferred from the TLS server to the client, including the length field.
[[Rationale: Use of the SHA-256 provides an yet unbroken hash of the data, and stronger hashes are of questionable utility with this method given that Secure DNS normally has other weaker parts due to performance reasons. Of course this approach is open for discussion.]]
The protocol (TCP or UDP) and port number is specified as part of the resource domain name as follows:

```
_443._tcp.example.com. IN CERT TLSCERT 0 0
                          IN1eoUHi9eb9nkCeROH5FmkdTKXQ/hmOM0mXjC2LM/I=
_5060._udp.example.com. IN CERT TLSCERT 0 0
                          R4UWsL/fwtOZp62gFHspEQY5v8iczDI20ZBOwMBQ1Hw=
```

[[Rationale: Letting the protocol and port number be part of the owner name reduces transfer sizes of the CERT record in situations where there would otherwise be multiple CERT records for unrelated services on the same domain name.]]

---

3. IANA Considerations

TOC

The IANA is requested to register and allocate a number for a new CERT RR certificate type TLSCERT.

---

4. Acknowledgements

TOC

Inspiration for this solution was drawn on earlier works in this area. Further, text were borrowed from draft-hoffman-keys-linkage-from-dns-00.

5. Security Considerations

TOC

TBW

6. References

TOC

6.1. Normative References

TOC

[RFC4033]	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements," RFC 4033, March 2005 (TXT).
[RFC4398]	Josefsson, S., "Storing Certificates in the Domain Name System (DNS)," RFC 4398, March 2006 (TXT).
[RFC5246]	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008 (TXT).
[FIPS.180-2.2002]	National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180-2, August 2002.

6.2. Informative References

TOC

[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 (TXT).
[RFC5081]	Mavrogiannopoulos, N., "Using OpenPGP Keys for Transport Layer Security (TLS) Authentication," RFC 5081, November 2007 (TXT).
[I-D.saintandre-tls-server-id-check]	Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity in Certificates Used with Transport Layer Security," draft-saintandre-tls-server-id-check-09 (work in progress), August 2010 (TXT).

Author's Address

TOC

	Simon Josefsson

	Simon Josefsson Datakonsult AB
	Hagagatan 24
	Stockholm 113 47
	Sweden
Email:	simon@josefsson.org
URI:	http://josefsson.org/