TLS
Internet-Draft
Intended status: Standards Track
Expires: September 9, 2014

M. Thomson
Mozilla

March 8, 2014

# Client Authentication Request Extension for (D)TLS
## draft-thomson-tls-care-00

Abstract

This document describes an extension to Transport Layer Security (TLS) and Datagram TLS (DTLS) that allows a client to indicate that it wants to provide a client certificate.

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 September 9, 2014.

Table of Contents



## 1. Introduction

In Transport Layer Security (TLS) [RFC5246] and Datagram TLS (DTLS) [RFC5764] the server decides whether or not to request a certificate from clients.

In TLS versions 1.2 and earlier, the Certificate message from a client is not encrypted and is therefore not confidential. TLS renegotiation is frequently used to provide confidentiality for client credentials, since renegotiation handshakes are encrypted with the TLS session keys.

A client that is aware of a need to authenticate can initial renegotiation, but is unable to induce a CertificateRequest from the server. The decision to request client authentication is one that can only be made by a server.

This document defines a client authentication request extension that can be used by a client to request that the server send a CertificateRequest in its handshake.

### 1.1. Conventions and Terminology

At times, this document falls back on shorthands for establishing interoperability requirements on implementations: the capitalized words "MUST", "SHOULD" and "MAY". These terms are defined in [RFC2119].

## 2. Client Authentication and TLS Renegotiation

Renegotiation has the potential to create confusion at higher layers about the security properties that apply to the byte stream. This is especially difficult when there are protocol constructs that span the ChangeCipherSpec messages that represent a switch between states.

For that reason, a client can initiate a new connection when it detects a need to authenticate, initiating renegotiation to establish authentication credentials immediately after the initial handshake.

Since the server only conditionally requests client authentication and it has no context with which to decide that authentication is needed, the client needs to provide some indication that it might need to be authentication. The second, renegotiation handshake can contain the client authentication request extension (Section 3) to provide this indication. As long as no application data is sent on the connection prior to completing renegotiation and sending the corresponding ChangeCipherSpec, there is no possibility for confusion over the security properties of application content.

This behavior could need to be triggered by a higher level protocol. This document does not define how that happens.

## 3. Client Authentication Request Extension

A new extension type ("client_authentication_request(TBD)") is defined. If a client includes this extension in its ClientHello to indicate that it wishes the server to issue a CertificateRequest.

```
enum {
    client_authentication_request(TBD), (65535)
} ExtensionType;
```

The "extension_data" field of this extension MUST be empty.

A server that supports client authentication based on certificates can use the presence of this extension to decide to include a CertificateRequest. The server MAY choose to ignore this extension.

A server MUST NOT send this extension to a client.

## 4. Security Considerations

This document is entirely about security.

## 5. IANA Considerations

IANA has allocated a TLS extension code point of (TBD) for this extension.

## 6. Acknowledgements

Eric Rescorla helped identify the problem and formulate this mechanism.

## 7. Normative References

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

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

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, May 2010.

Author's Address

Martin Thomson
Mozilla
Suite 300
650 Castro Street
Mountain View, CA 94041
US

Email: martin.thomson@gmail.com