       Using CBOR Web Tokens (CWTs) in Transport Layer Security (TLS) and
              Datagram Transport Layer Security (DTLS)
                      draft-tschofenig-tls-cwt-02

Abstract

   The TLS protocol supports different credentials, including pre-shared
   keys, raw public keys, and X.509 certificates. For use with public
   key cryptography developers have to decide between raw public keys,
   which require out-of-band agreement and full-fletched X.509
   certificates. For devices where the reduction of code size is
   important it is desirable to minimize the use of X.509-related
   libraries. With the CBOR Web Token (CWT) a structure has been
   defined that allows CBOR-encoded claims to be protected with CBOR
   Object Signing and Encryption (COSE).

   This document registers a new value to the "TLS Certificate Types"
   sub-registry to allow TLS and DTLS to use CWTs. Conceptually, CWTs
   can be seen as a certificate format (when with public key
   cryptography) or a Kerberos ticket (when used with symmetric key
   cryptography).

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 https://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 January 14, 2021.

Table of Contents

1. Introduction

   The CBOR Web Token (CWT) [RFC8392] was defined as the CBOR-based
   version of the JSON Web Token (JWT) [RFC7519]. JWT is used
   extensively on Web application and for use with Internet of Things

environments the believe is that a more lightweight encoding, namely
CBOR, is needed. CWTs, like JWTs, contain claims and those claims
are protected against modifications using COSE [RFC8152]. CWTs are
flexible with regard to the use of cryptography and hence CWTs may be
protected using a keyed message digest, or a digital signature. One
of the claims allows keys to be included, as described in
[I-D.ietf-ace-cwt-proof-of-possession]. This specification makes use
of these proof-of-possession claims in CWTs. This document mandates
a minimum number of claims to be present in a CWT. There may,
however, be a number of additional claims present in a CWT. An
example of a token with a larger number of claims is the Entity
Attestation Token (EAT), which may also be encoded as a CWT.

Fundamentally, there are two types of keys that can be used with
CWTs:

- Asymmetric keys: In this case a CWT contains a COSE_Key [RFC8152]
  representing an asymmetric public key. To protect the CWT against
  modifications the CWT also needs to be digitally signed.

- Symmetric keys: In this case a CWT contains the Encrypted_COSE_Key
  [RFC8152] structure representing a symmetric key encrypted to a
  key known to the recipient using COSE_Encrypt or COSE_Encrypt0.
  Again, to protect the CWT against modifications a keyed message
  digest is used.

The CWT also allows mixing symmetric and asymmetric crypto although
this is less likely to be used in practice.

Exchanging CWTs in the TLS / DTLS handshake offers an alternative to
the use of raw public keys and X.509 certificates. Compared to raw
public keys, CWTs allow more information to be included via the use
of claims. Compared to X.509 certificates CBOR offers an alternative
encoding format, which may also be used by the application layer
thereby potentially reducing the overall code size requirements.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in RFC
2119 [RFC2119].

3. The CWT Certificate Type

This document defines a new value to the "TLS Certificate Types" sub-
registry and the value is defined as follows.

```
      /* Managed by IANA */
       enum {
           X509(0),
           RawPublicKey(2),
           CWT(TBD),
           (255)
       } CertificateType;

       struct {
           select (certificate_type) {

               /* CWT "certificate type" defined in this document.*/
                case CWT:
                opaque cwt_data<1..2^24-1>;

                /* RawPublicKey defined in RFC 7250*/
               case RawPublicKey:
               opaque ASN.1_subjectPublicKeyInfo<1..2^24-1>;

               /* X.509 certificate defined in RFC 5246*/
               case X.509:
               opaque cert_data<1..2^24-1>;

                };

           Extension extensions<0..2^16-1>;
       } CertificateEntry;
```

4. Representation and Verification the Identity of Application Services

RFC 6125 [RFC6125] provides guidance for matching identifiers used in
X.509 certificates against a reference identifier, i.e. an identifier
constructed from a source domain and optionally an application
service type. Different types of identifiers have been defined over
time, such as CN-IDs, DNS-IDs, SRV-IDs, and URI-IDs, and they may be
carried in different fields inside the X.509 certificate, such as in
the Common Name or in the subjectAltName extension.

For CWTs issued to servers the following rule applies: To claim
conformance with this specification an implementation MUST populate
the Subject claim with the value of the Server Name Indication (SNI)
extension. The Subject claim is of type StringOrURI. If it is
string an equality match is used between the Subject claim value and
the SNI. If the value contains a URI then the URI schema must be
matched against the service being requested and the remaining part of
the URI is matched against the SNI in an equality match (since the
SNI only defines Hostname types).

For CWTs issued to clients the application service interacting with
the TLS/DTLS stack on the server side is responsible for
authenticating the client. No specific rules apply but the Subject
and the Audience claims are likely to be good candidates for
authorization policy checks.

Note: Verification of the Not Before and the Expiration Time claims
MUST be performed to determine the validity of the received CWT.

5. Security and Privacy Considerations

The security and privacy characteristics of this extension are best
described in relationship to certificates (when asymmetric keys are
used) and to Kerberos tickets (when symmetric keys are used) since
the main difference is in the encoding.

When creating proof-of-possession keys the recommendations for state-
of-the-art key sizes and algorithms have to be followed. For TLS/
DTLS those algorithm recommendations can be found in [RFC7925] and
[RFC7525].

CWTs without proof-of-possession keys MUST NOT be used.

When CWTs are used with TLS 1.3 [RFC8446] and DTLS 1.3
[I-D.ietf-tls-dtls13] additional privacy properties are provided
since most handshake messages are encrypted.

6. IANA Considerations

IANA is requested to add a new value to the "TLS Certificate Types"
sub-registry for CWTs.

7. References

7.1. Normative References

[I-D.ietf-ace-cwt-proof-of-possession]
          Jones, M., Seitz, L., Selander, G., Erdtman, S., and H.
          Tschofenig, "Proof-of-Possession Key Semantics for CBOR
          Web Tokens (CWTs)", draft-ietf-ace-cwt-proof-of-
          possession-11 (work in progress), October 2019.

[I-D.ietf-tls-dtls13]
          Rescorla, E., Tschofenig, H., and N. Modadugu, "The
          Datagram Transport Layer Security (DTLS) Protocol Version
          1.3", draft-ietf-tls-dtls13-33 (work in progress), October
          2019.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119,
               DOI 10.17487/RFC2119, March 1997,
               <https://www.rfc-editor.org/info/rfc2119>.

   [RFC7250]   Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J.,
               Weiler, S., and T. Kivinen, "Using Raw Public Keys in
               Transport Layer Security (TLS) and Datagram Transport
               Layer Security (DTLS)", RFC 7250, DOI 10.17487/RFC7250,
               June 2014, <https://www.rfc-editor.org/info/rfc7250>.

   [RFC8152]   Schaad, J., "CBOR Object Signing and Encryption (COSE)",
               RFC 8152, DOI 10.17487/RFC8152, July 2017,
               <https://www.rfc-editor.org/info/rfc8152>.

   [RFC8392]   Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig,
               "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392,
               May 2018, <https://www.rfc-editor.org/info/rfc8392>.

   [RFC8446]   Rescorla, E., "The Transport Layer Security (TLS) Protocol
               Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018,
               <https://www.rfc-editor.org/info/rfc8446>.

7.2. Informative References

   [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, DOI 10.17487/RFC6125, March
               2011, <https://www.rfc-editor.org/info/rfc6125>.

   [RFC7519]   Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token
               (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015,
               <https://www.rfc-editor.org/info/rfc7519>.

   [RFC7525]   Sheffer, Y., Holz, R., and P. Saint-Andre,
               "Recommendations for Secure Use of Transport Layer
               Security (TLS) and Datagram Transport Layer Security
               (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May
               2015, <https://www.rfc-editor.org/info/rfc7525>.

   [RFC7925]   Tschofenig, H., Ed. and T. Fossati, "Transport Layer
               Security (TLS) / Datagram Transport Layer Security (DTLS)
               Profiles for the Internet of Things", RFC 7925,
               DOI 10.17487/RFC7925, July 2016,
               <https://www.rfc-editor.org/info/rfc7925>.

7.3. URIs

    [1] mailto:tls@ietf.org

    [2] https://www1.ietf.org/mailman/listinfo/tls

    [3] https://www.ietf.org/mail-archive/web/tls/current/index.html

Appendix A. History

RFC EDITOR: PLEASE REMOVE THE THIS SECTION

- -01: Minor editorial bugfixes and reference updates; refreshing
  draft

- -00: Initial version

Appendix B. Working Group Information

The discussion list for the IETF TLS working group is located at the
e-mail address tls@ietf.org [1]. Information on the group and
information on how to subscribe to the list is at
https://www1.ietf.org/mailman/listinfo/tls [2]

Archives of the list can be found at: https://www.ietf.org/mail-
archive/web/tls/current/index.html [3]

Authors' Addresses

Hannes Tschofenig
Arm Limited

EMail: hannes.tschofenig@arm.com

Mathias Brossard
Arm Limited

EMail: Mathias.Brossard@arm.com