Using CBOR Web Tokens (CWTs) in TLS and DTLS
(draft-tschofenig-tls-cwt-00)

H. Tschofenig, M. Brossard
CWT History

• JSON Web Tokens (JWTs) have been defined in RFC 7519 and proof-of-possession key claim in RFC 7800.
• CBOR Web Token (CWT) has been published in RFC 8392 and PoP extension is available with <draft-ietf-ace-cwt-proof-of-possession>.
• JWTs (as bearer tokens) are in widespread use; initial usage was for OAuth-based applications.
• CWTs aim for the IoT use case.
• Tokens contain claims registered with IANA.
• Tokens are protected with JOSE (for JWTs) and with COSE (for CWTs).
• Works with symmetric as well as asymmetric keys.
CWT Example
(in diagnostic syntax with asymmetric PoP key)

{
/iss/ 1 : "coaps://server.example.com",
/aud/ 3 : "coaps://client.example.org",
/exp/ 4 : 1361398824,
/cnf/ 8 :{
/COSE_Key/ 1 :{
/kty/ 1 : /EC/ 2,
/crv/ -1 : /P-256/ 1,
/x/-2 : h'd7cc072de2205bdc1537a543d53c60a6acb62eccd890c7fa27c9 e354089bbbe13',
/y/-3 : h'f95e1d4b851a2cc80fff87d8e23f22af8725d535e515e020731e 79a3b4e47120'
}
}
}
Certificate Types History

• RFC 5081/RFC 6091 “Using OpenPGP Keys in TLS” created the “TLS Certificates Types” registry and RFC 7250 extended the extension and populated the registry with the “raw public key” format.

• Raw public keys are obviously quite efficient (over-the-wire and in terms of code size).
CWTs

• Is there something that is smaller than X.509 certs but more sophisticated than raw public keys?

• Our approach: Let’s experiment with CWTs

• Plan to implement prototype to determine
  • Implementation complexity,
  • Code size requirements,
  • Ram requirements, and
  • Over-the-wire overhead.
Draft Content

• Simple document.

• Registers CWT to the TLS Certificate Types registry

• Talks about how to match the subject claim in the CWT with the value provided by the SNI (for server-to-client authentication).

• Focuses only on PoP tokens and not bearer tokens.
Next steps

• Technically quite easy but difficult to deploy → Not ready for prime time yet.

• We plan to come back with performance numbers and implementation feedback to the next IETF meeting.

• If you are interested in this work, please let us know.