CWT (CBOR Web Token)

Erik Wahlström

Mike Jones

Hannes Tschofenig

Agenda

- CWT introduction
- Example
- Open issues
- Next step

CWT introduction

- https://tools.ietf.org/html/draft-wahlstroem-ace-cbor-web-token-00
- Profile of JSON Web Token (JWT)
  - CBOR/COSE vs JSON/JOSE.
- Optimzed for constrained IoT devices
- Transfer claims between two parties.
  - Name/value pairs
- ”cot”, yes Justin that means it’s a ”cosy cot” ☺

```
{
   "iss": "coap://as.example.com",
   "aud": "coap://light.example.com",
   "sub": "erikw",
   "exp": 1444064944,
   "nbf": 1443944944,
   "iat": 1443944944,
   "cti": 2929,
   "cks":
     [
       {
         "kty": "EC",
         "kid": "11",
         "crv": 1, // using P-384
         "x": h'bac5b11cad8f99f9c72b05cf4b9e26d244dc189f745228255a219a86d6a09eff',
         "y": h'20138bf82dc1b6d562be0fa54ab7804a3a64b6d72ccfed6b6fb6ed28bbfc117e'
       }
     ],
   "aif": [["/s/light", 1], ["/a/led", 5], ["/dtls", 2]]
 }
```

CWT defines mapping to CBOR

Claim	CBOR encoded claim key	CBOR major type of value
iss	1	3
sub	2	3
aud	3	3
exp	4	6 tag value 1
nbf	5	6 tag value 1
iat	6	6 tag value 1
cti	7	3

```
{
  1: "coap://as.example.com",
  3: "coap://light.example.com",
  2: "erikw",
  4: 1(1444064944),
  5: 1(1443944944),
  6: 1(1443944944),
  7: 2929,
  8: [
    {
      1: 2,
      2: "11",
      -1: 1,
      -2: h'bac5b11cad8f99f9c72b05cf4b9e26d244dc189f745228255a219a86d6a09eff',
      -3: h'20138bf82dc1b6d562be0fa54ab7804a3a64b6d72ccfed6b6fb6ed28bbfc117e'
    }
    ],
  9: [["/s/light", 1], ["/a/led", 5], ["/dtls", 2]]
}
```

Open issues at https://github.com/erwah/ietf/

1. Add signed and encrypted examples.
2. Make ”cti” binary.
3. Use numeric date instead of major type 6, minor type 1.
4. New section about creating and validating CWT’s.
5. Register a new content type for CWT.
6. Truncate binary values for readability.
7. s/re-used/used

Next steps

- Security AD decided that ACE is the place for CWT.
- Adoption
- Define extensions parallell to JWT extensions like the cnf claim.