Composite Claims

Chris Lemmons

IETF COSE WG

2023-11-07

Composite Claims

- I have a CWT bearer token that embeds policy:
  - Application-specific claims
  - General claims defined in RFCs
  - **A way to flexibly put all of them together.**

This last point is what I'm here about.

Logical Claims

I can do a simple claim:

```
{ /uri/ ?: { /ext/ 8: { /=/ 0: ".m3u8" } } }
```

But sometimes the policy needs to be more flexible:

```
{ /or/ ?: [
  {{ /uri/ ?: { /ext/ 8: { /=/ 0: ".m3u8" } } }},
  {{ /uri/ ?: { /ext/ 8: { /=/ 0: ".ts" } } }},
]}
```

Enveloped Claim

Sometimes, bearer tokens traverse unsafe places, like in URIs.

```
{ /sub/ 2: "123456789" }
```

This isn't great. We can do better:

```
{ /env/ ?: { /sub/ 2: <COSE_Encrypt1> } }
```

Now, without opening the evelope, we don't know the account id.

Crit Claim

And sometimes, we need to know if the data is important:

```
{ /env/ ?: {
    /private1/ ?: <COSE_Encrypt1>,
    /private2/ ?: <COSE_Encrypt1>
  },
  /crit/ ?: [/private2/ ?]
}
```

If we get one of these, we know that we have to unwrap the envelope and must understand private2, but we can leave private1 alone if we don't know or care about it.

Why am I here

I have two options:

- Define these in the Expert Review section.
- Bring the work here because it's generic and we shouldn't each build our own building blocks.

Questions

- Questions.