Common Access Token

Chris Lemmons

CTA WAVE CAT WG for the IETF CDNI WG

2022-03-22

Outline

- Who is doing this?
- What are they doing?
- Why do we care?

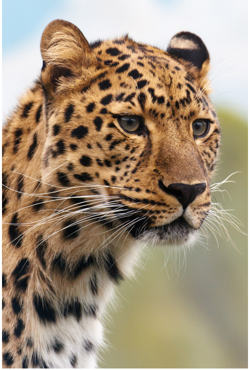
Who

- Consumer Technology Association (CTA)
- Web Application Video Ecosystem (WAVE)
- Primary Use Case: Streaming Media
- Goal: Single token that covers existing usage

How is this different?

- CWT-based
- Receivers get more MUSTs
- No built-in support for delegation
- Generally more claims and greater complexity

Encrypted Claims



- Uses a COSE object directly instead of a base64ed string
- Avoids repeated base64ing
- Can't use sub claim, because that's a string
- Must encrypt sensitive claims:
  - Network/IP Address
  - Subject
  - Detailed Geography

Additional Claims

- HTTP Method
- ALPN
- Headers
- Geography claims
- TLS Public Key (a la OAUTH mTLS)
- Nestable Compositions (and, or, nor)
- Actions that modify rejections

Claims with Types

- Critical Claim: Array
- Encrypted Claims: COSE_Encrypt or COSE_Encrypt0
- Network Claim: Array of RFC9164 tags

Some Very Generic Claims

- ALPN, Method, Headers, and Compositions
- Encrypted Subject
- Critical Claim
- These are potentially generally useful
- Maybe try to define them generally?

Some Overlapping Utility

- All URI Signing Tokens can be represented as CATs
- Any successor token is likely to use at least some of these claims

Takeaway

- No real takeaway
- No action items
- Just food for thought
- And some Public Domain cats