Entity Attestation Token (EAT) Collection Type

draft-frost-rats-eat-collection-01
IETF 114, July 2022, RATS WG

Simon Frost
Arm
simon.frost@arm.com
EAT Collections Draft Introduction

• Purpose: an extension for EAT top level object for use cases where there may be no top level signer

• Current EAT needs top level object to be CWT / JWT / DEB
  • exception is UCCS extension, but that is for tightly defined use case

• The Collection extension is used where the overall token is made up of multiple independent tokens with an internally defined integrity relationship

• In particular where the number of tokens present may change
  • or the definition of the leaf signer may vary by deployment

• e.g. migrating info currently defined as x.509 certificate chain to EAT

• e.g. platform / workload token parts from Arm CCA
CCA ‘Direct Sign’ model

<table>
<thead>
<tr>
<th>Platform (EAT)</th>
<th>Workload (EAT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>...claims...</td>
<td>...claims...</td>
</tr>
<tr>
<td>Challenge: H(workload claims)</td>
<td>Challenge: RP nonce</td>
</tr>
</tbody>
</table>

Platform Key

CCA ‘Delegated Sign’ model

<table>
<thead>
<tr>
<th>Platform (EAT)</th>
<th>Workload (EAT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>...claims...</td>
<td>...claims...</td>
</tr>
<tr>
<td>Challenge: H(RAK_{pub})</td>
<td>Challenge: RP nonce</td>
</tr>
</tbody>
</table>

Platform Key

RAK

Future potential to add additional token(s)

Could format into single EAT DEB...

Could format into top level workload with Platform as submod

Significant format & (hence code) change for subtle differences by deployment

...instead, treat as Collection entries

TBD...
EAT Collections Format

- Tagged Map containing:
- Collection Identifier (optional) -> EAT profile claim
- One or more entries consisting of CWT / JWT / DEB
  - Tags on map entries may be meaningful to the profile
- Each entry must have its own integrity and an integrity relationship to other entries
  - Custom (profile) defined
  - 1:1 or 1:n
EAT Collections Draft Status

• draft-00 released to WG
• draft-01 released addressing review comments from -00
  • CDDL embracing multiple formats for member tokens
  • CDDL allowing 1+ members rather than 2+
  • Greater emphasis on security considerations