Measured Components

draft-fft-rats-eat-measured-component

IETF 119 Brisbane, RATS WG
EAT Measurements

EAT defines an extensible Measurements claim, which:

"[c]ontains descriptions, lists, evidence or measurements of the software that exists on the entity or any other measurable subsystem of the entity."

Currently, CoSWID is the only format supported.

CoSWID is not a good fit for environments that do not have a file system onto which measurements can be anchored.
PSA Software Components

The PSA profile has defined its own "software components" format:

```
psa-software-component = {
  ? &(measurement-type: 1)  => text
  &(measurement-value: 2) => psa-hash-type
  ? &(version: 4)           => text
  &(signer-id: 5)         => psa-hash-type
  ? &(measurement-desc: 6)  => text
}
```
Generalising psa-software-component

Refactor psa-software-component to take into account the recommendations for "new claims design considerations" in Appendix E of EAT:

✅ Interoperability and Relying Party Orientation
✅ Operating System and Technology Neutral
✅ Security Level Neutral
✅ Reuse of Extant Data Formats
# Measured Component Information Model

<table>
<thead>
<tr>
<th>Information Element</th>
<th>Description</th>
<th>Requirement Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Name</td>
<td>The name given to a measured component. It is important that this name remains consistent across different releases to allow for better tracking of the same measured item across updates. When combined with a consistent versioning scheme, it enables better signaling from the appraisal procedure to the relying parties.</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>Component Version</td>
<td>A value representing the specific release or development version of the measured component. Using Semantic Versioning is RECOMMENDED.</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>Digest Value</td>
<td>Hash of the invariant part of the component that is loaded in memory at startup time.</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>Hash algorithm used to compute the Digest Value.</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>Signer</td>
<td>A unique identifier of the entity authorizing installation of the measured component.</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>Countersigners</td>
<td>One or more unique identifiers of further authorizing entities for component installation.</td>
<td>OPTIONAL</td>
</tr>
</tbody>
</table>
Measured Component Information Model (cont.)

Anything missing? E.g., SVN
Measured Component Data Model

Reuse COSE Key Thumbprint, CoSWID software name and version, CoRIM digest.

measured-component = [
    id: component-id
    measurement: corim.digest
    signer: ckt
    ? countersigners: [ + ckt ]
]
EAT sockets

CBOR & JSON serialisations

mc-cbor = bstr .cbor measured-component
mc-json = tstr .json measured-component

EAT CBOR (.feature "cbor")

$measurements-body-cbor /= mc-cbor ; native
$measurements-body-cbor /= tstr .b64u mc-json ; tunnel

EAT JSON (.feature "json")

$measurements-body-json /= mc-json ; native
$measurements-body-json /= tstr .b64u mc-cbor ; tunnel
Relation with other drafts

X.509-based Attestation Evidence

Potential reuse of the info model
adopt me?