Measured Components

draft-fft-rats-eat-measured-component

IETF 120 Vancouver, 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:

```plaintext
code
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>IE</th>
<th>Description</th>
<th>Requirement Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Name</td>
<td>The name given to the 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 measured component.</td>
<td>REQUIRED</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>Hash algorithm used to compute the Digest Value. REQUIRED</td>
<td></td>
</tr>
<tr>
<td>Signers</td>
<td>One or more unique identifiers of entities signing the measured component.</td>
<td>OPTIONAL</td>
</tr>
</tbody>
</table>
Measured Component Information Model (cont.)

Are we missing anything absolutely required? (SVN?)
Measured Component Data Model

```
measured-component = [  
    id:               component-id  
    measurement:      corim.digest  
    ? signers:        [ + signer-type ]  
]  

component-id = [  
    name:      text  
    ? version: eat.sw-version-type  
]  
```

IETF 120 Vancouver, RATS WG
EAT sockets

The document defines how the Measurements extension is consumed by EAT.

CBOR & JSON serialisations:

\[
\begin{align*}
\text{mc-cbor} &= \text{bstr .cbor measured-component} \\
\text{mc-json} &= \text{tstr .json measured-component}
\end{align*}
\]
EAT sockets (CBOR)

CBOR EAT(.feature "cbor")

$measurements-body-cbor /= mc-cbor ; native
$measurements-body-cbor /= tstr .b64u mc-json ; tunnel
EAT sockets (JSON)

JSON EAT (.feature "json")

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

Covers a gap for early boot measurements, which CoSWID does not address well

Extends EAT, reusing the available type system as much as possible

Proven data format based on experience with PSA
adopt me?