Attestation Verifier
Theory of Operation

Ned S., Henk B., Andrew D., Yogesh D., Thomas F.
IETF 119 - Brisbane
Recap of Verifier Inputs

• Evidence is a set of Claims from an Attester
  • Verifier accepts Evidence if it's authenticated to the Attester.

• Reference Values are a set of Claims from an RVP
  • Verifier accepts RV Claims with the expectation they will match Evidence

• Endorsements are a set of Claims from an Endorser
  • Verifier accepts Endorsement Claims with the expectation that the Attester is valid
Verifier Inputs have a Matching Condition

- **Endorsement example:**
  - If Attester has a digest value X, then assert a CVE Endorsement Claim

- **RV example:**
  - If all the RV Claims match Evidence, then the Attester is valid

- **Evidence example:**
  - If Evidence was signed by the Attester, then its OK to accept it
  - The matching condition is simply that the Verifier knows which Attester it is appraising.
CoMID Triples can be Abstracted as follows:

- **CoMID Triple**
  - **CM Type**
    - Conceptual Message Type
      - EV: Evidence
      - RV: Reference Values
      - EN: Endorsements
  - **Condition**
    - Claims (state) about an Attester that are true (accepted) and are a precondition for accepting additional Claims
  - **Claims**
    - New Claims about the Attester given the matching condition is satisfied.
    - Note: a Claim identifies a Target Environment and its associated measurements.
  - **Authority**
    - The entity that asserted the triple (e.g., a key)

• Accepted Claims records have the same structure as triple records, minus the **Condition**
How to Process Conditions

<table>
<thead>
<tr>
<th>Record Number</th>
<th>Accepted Claims</th>
<th>Matching Conditions</th>
<th>Actions (if condition is true)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:</td>
<td>Attester 1 (current connection)</td>
<td>Evidence Condition 1</td>
<td>Append Record 1</td>
</tr>
<tr>
<td>1:</td>
<td>Claims 1 (AE1)</td>
<td>Ref Val Condition 1</td>
<td>Append Record 2</td>
</tr>
<tr>
<td>2:</td>
<td>Claims 1 (same as evidence)</td>
<td>Endorsement Condition 1</td>
<td>Append Record 3</td>
</tr>
<tr>
<td>3:</td>
<td>Claims 2 (E1)</td>
<td></td>
<td>Append Record 4</td>
</tr>
<tr>
<td>4:</td>
<td>Claims 3 (E2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A Note on Scalability

• Horn Clause Scalability - If updates are limited to conjunction, then processing complexity is polynomial
  • Updates to Accepted Claims can be appended because position in the set doesn't have significance

• Condition processing efficiency can be improved with indexed search

• If a condition doesn’t match, then it can be tried again
  • Maybe a different record will be added that satisfies the condition

• The Verifier can stop accepting inputs as needed, based on operational conditions
A Few Examples

• Pattern
  • \( (<\text{condition}>, <\text{claims}>, <\text{authority}>) \Rightarrow \text{The record to append to Accepted Claims} \)

• Evidence
  • \((<\text{Attester 1}>,
    \langle \text{env-id=.3.2.1 : digest=h'FED4'}>,
    \langle \text{key-id=h'01'}> \) \Rightarrow \)
  
  \text{Type: Evidence}  
  \text{Claim: [env-id=.3.2.1 : digest=h'FED4']}  
  \text{Authority: key-id=h'01' /Attester 1/}

• RVP
  • \((<\text{env-id=.3.2.1 : digest=h'FED4'}>,
    \langle \text{env-id=.3.2.1 : digest=h'FED4'}>,
    \langle \text{key-id=h'02'}> \) \Rightarrow \)
  
  \text{Type: RV}  
  \text{Claim: [env-id=.3.2.1 : digest=h'FED4']}  
  \text{Authority: key-id=h'02' /RVP 1/}

• Endorsement #1
  • \((<\text{env-id=.3.2.1 : digest=h'FED4', key-id=h'02'}>,
    \langle \text{env-id=.3.2.1 : svn=7}>,
    \langle \text{key-id=h'03'}> \) \Rightarrow \)
  
  \text{Type: Endorsement}  
  \text{Claim: [env-id=.3.2.1 : svn=7]}  
  \text{Authority: key-id=h'03' /Endorser 1/}

• Endorsement #2
  • \((<\text{env-id=.3.2.1 : svn=7, key-id=h'03'}>,
    \langle \text{env-id=.3.2.2 : version="1.0"}>,
    \langle \text{key-id=h'04'}> \) \Rightarrow \)
  
  \text{Type: Endorsement}  
  \text{Claim: [env-id=.3.2.2 : version="1.0"]}  
  \text{Authority: key-id=h'04' /Endorser 2/}
What if more inputs show up?

- **Record Number**: 0, 1, 2, 3, 4, 5, 6
- **Accepted Claims**:
  - 0: Attester 1 (current connection)
  - 1: Claims 1 (AE1)
  - 2: Claims 1 (RVP1)
  - 3: Claims 2 (E1)
  - 4: Claims 3 (E2)
  - 5: Claims 4 (AE2)
  - 6: Claims 5 (subset of Claims 4) (RVP2)
- **Evidence Condition 2**: AND
- **Ref Val Condition 2**: Append Record 5
- **Append Record 6**

**New inputs for Evidence and Reference Values**

**Action** (if condition is true):
- Append Record 5
- Append Record 6
Accepted Claims Restriction using Views

- **View** – Typically, it’s a subset of the Accepted Claims:
  - **View tuple: (view-name, condition, authority) => results**
    - **view-name** - A context for putting view results
    - **condition** - Interesting Claims
    - **authority** - The Relying Party requesting the View
    - **results** - The Accepted Claims records selected by the condition

- If the condition is met, matched Claims are copied into the View

- Receipt of a View request can trigger processing
  - If the Verifier is still processing inputs, then View results may differ each time the view request is processed.

- The Verifier can append its own claims from appraisal policy
  - Example: AR4SI
Processing a View Request

accepted Claims

<table>
<thead>
<tr>
<th>Record Number</th>
<th>Accepted Claims</th>
<th>Query</th>
<th>View Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:</td>
<td>Attester1 (lead Attestor)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:</td>
<td>Claims 1 (AE1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:</td>
<td>Claims 1 (RVP1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td>Claims 2 (E1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:</td>
<td>Claims 3 (E2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:</td>
<td>Claims 4 (AE2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Condition 1

Condition 2

Views can be staging contexts for creating Attestation Results
View Examples

• The view example selects records asserted by RVP_1 and Endorser_2
• View request has the following structure:
  • View Name
  • Condition
  • Authority (of requester – e.g., a Relying Party)

View Results:

• View: view-name="MyView"
• Authority: key-id=h'06' / RP_1/
• Condition: [OR[Asserters=[key-id=h'02' / RVP_1/], [key-id=h'04' / Endorser_2/]]]
• Records copied:
  Type: RV
  Claim: [env-id=.3.2.1 : digest=h'FED4']
  Authority: key-id=h'02' /RVP 1/

  Type: Endorsement
  Claim: [env-id=.3.2.2 : version="1.0"]
  Authority: key-id=h'04' /Endorser 2/