Attestation Verifier Theory of Operation

Ned S., Henk B., Andrew D., Yogesh D., Thomas F.

IETF 119 - Brisbane

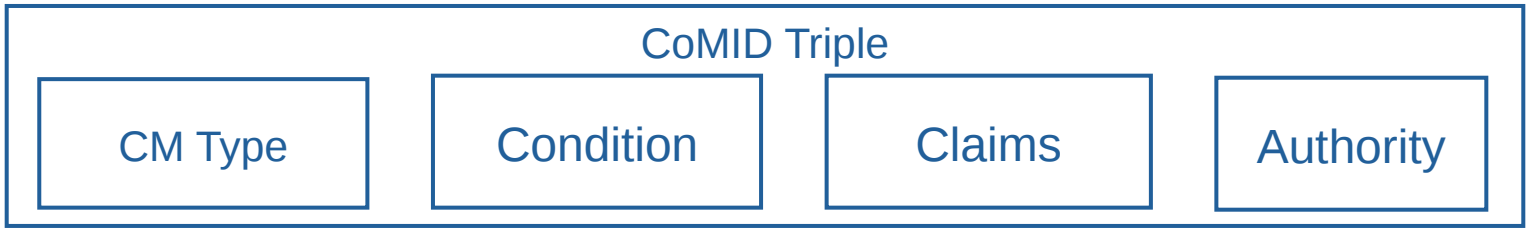
Recap of Verifier Inputs

- 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:



Conceptual Message Type

- EV : Evidence
- RV : Reference Values
- EN : Endorsements
- AR: Attestation Results
- Etc...

Condition

- Claims (state) about an Attester that are true (accepted) and are a precondition for accepting additional Claims

Claims

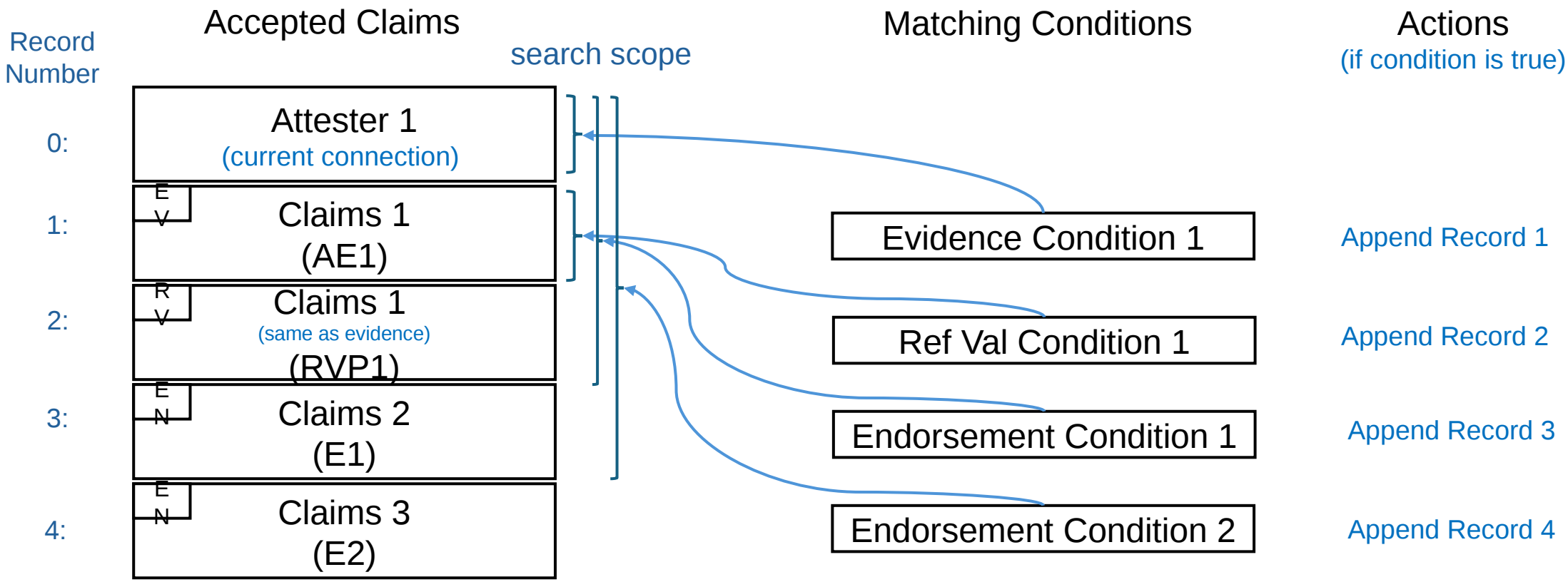
- New Claims about the Attester given the matching condition is satisfied.
- Note: a Claim identifies a Target Environment and its associated measurements.

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



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
  - (<condition>, <claims>, <authority>) => The record to append to Accepted Claims
- Evidence
  - (<Attester 1>,
  - <env-id=.3.2.1 : digest=h'FED4'>,
  - <key-id=h'01'>) =>

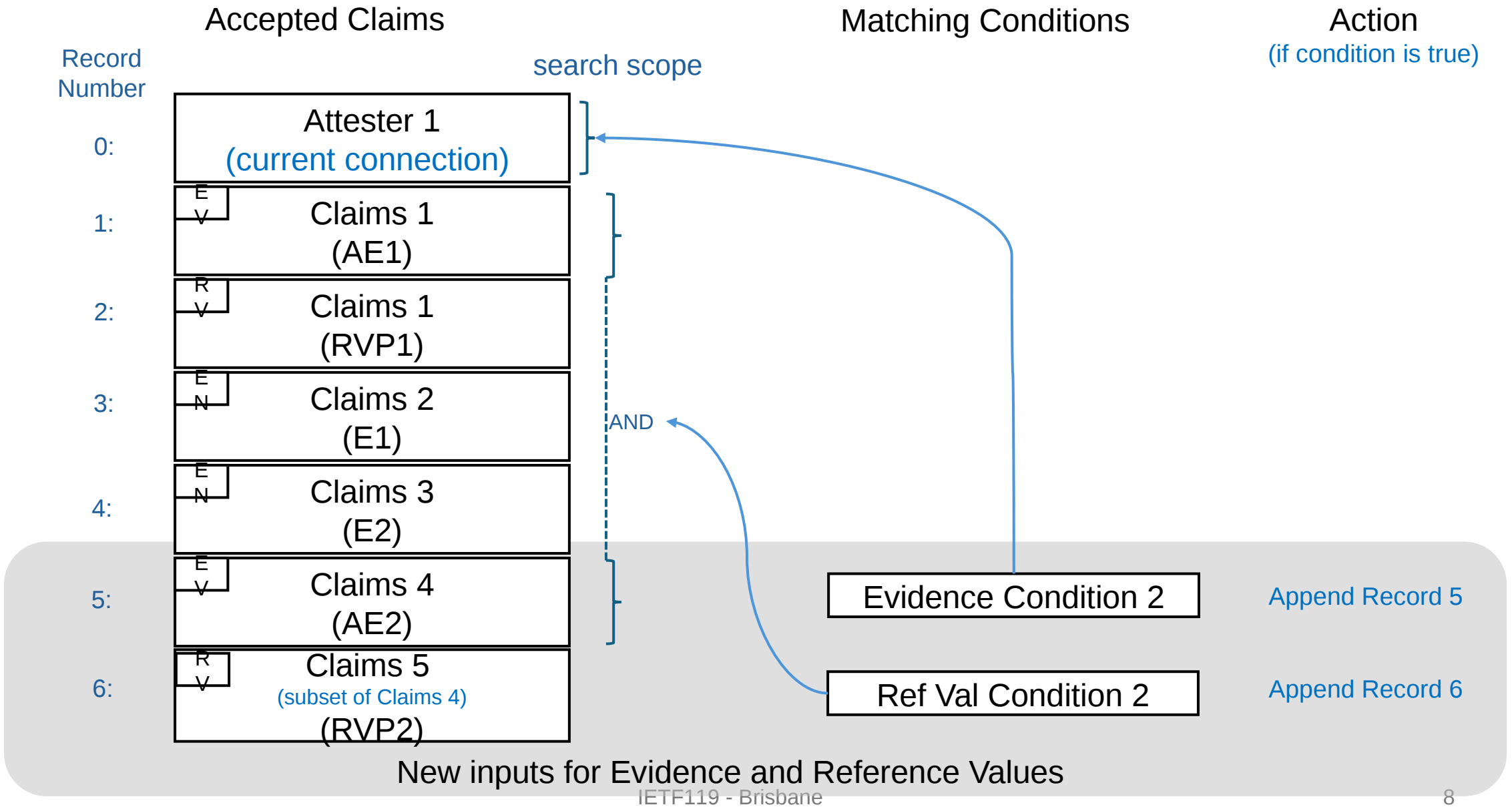
  Type: Evidence
  Claim: [env-id=.3.2.1 : digest=h'FED4']
  Authority: key-id=h'01' /Attester 1/
- RVP
  - (<env-id=.3.2.1 : digest=h'FED4'>,
  - <env-id=.3.2.1 : digest=h'FED4'>,
  - <key-id=h'02'>) =>

  Type: RV
  Claim: [env-id=.3.2.1 : digest=h'FED4']
  Authority: key-id=h'02' /RVP 1/
- Endorsement #1
  - (<env-id=.3.2.1 : digest=h'FED4', key-id=h'02'>
  - <env-id=.3.2.1 : svn=7>,
  - <key-id=h'03'>) =>

  Type: Endorsement
  Claim: [env-id=.3.2.1 : svn=7]
  Authority: key-id=h'03' /Endorser 1/
- Endorsement #2
  - (<env-id=.3.2.1 : svn=7, key-id=h'03'>,
  - <env-id=.3.2.2 : version="1.0">,
  - <key-id=h'04'>) =>

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

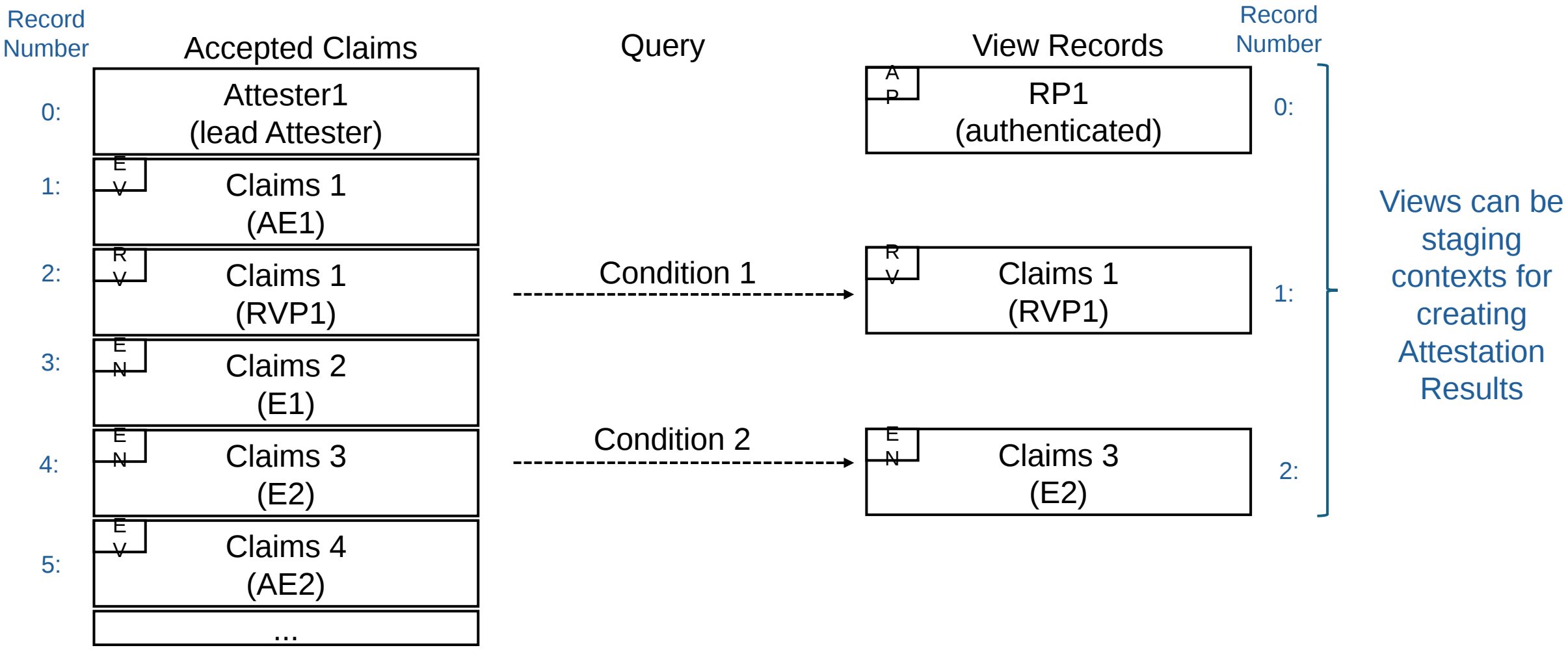
What if more inputs show up?



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



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/