RATS Agenda - Monday, July 26th – Session II

Room 8, RATS Session 1
Time zone: PDT (UTC-7)

14:30 : 14:35 **Agenda Bash & Logistics**
(5 min) Nancy Cam-Winget, Kathleen Moriarty, Ned Smith
14:35 : 14:40 **RATS Architecture and next steps**
(5 min) Michael Richardson
(draft-ietf-rats-architecture-12)
14:40 : 14:50 **EAT**
(10 min) Laurence Lundblade
(draft-ietf-rats-eat-10)
14:50 : 15:00 **CHARRA and RIV**
(10 min) Henk Birkholz, Guy Fedorkow
(draft-ietf-rats-yang-tpm-charra-08, draft-ietf-rats-tpm-based-network-device-attest-07)
15:00 : 15:10 **Reference Interaction Models and DAA**
(10 min) Henk Birkholz
(draft-ietf-rats-reference-interaction-models-03, draft-birkholz-rats-daa-01)
15:10 : 15:25 **Concise Reference Integrity Manifest**
(15 min) Henk Birkholz
(draft-birkholz-rats-corim-00)
15:25 : 15:30 **Attestation Sets**
(5 min) Kathleen Moriarty
(draft-moriarty-attestationsets)

IETF

RATS Architecture and next steps

- Michael Richardson

EAT Update

- Laurence Lundblade

IETF

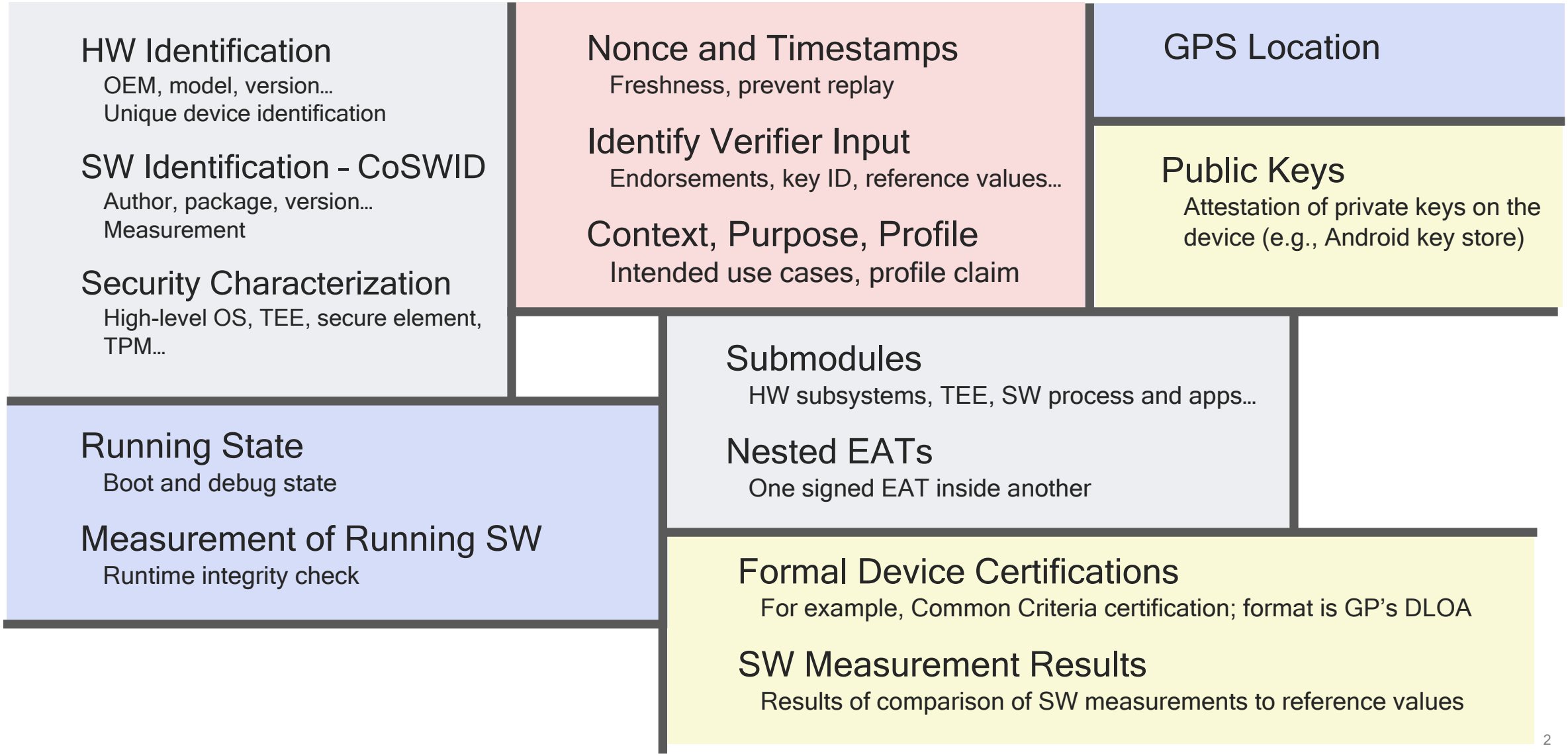
EAT Update:

- Draft Status
- Semi-permanent UEID and IDevID
- Attestation Results

Laurence Lundblade

IETF 111 July 2021

Planned Contents of an EAT – The Claims



Level of Completion in EAT Draft

- Ready for last call, no open issues
- Near completion, reviewed
- Draft text
- Proposed, Interest in


Progress & change since IETF 110. Draft -10


In Github, but not draft


HW Identification

OEM, model, version…
Unique device identification


SW Identification – CoSWID

Author, package, version…
Measurement

Security Characterization

High-level OS, TEE, secure element, TPM…

Nonce and Timestamps

Freshness, prevent replay

Identify Verifier Input

Endorsements, key ID, reference values…

Context, Purpose, Profile

Intended use cases, profile claim

GPS Location

Public Keys

Attestation of private keys on the device (e.g., Android key store)

Submodules

HW subsystems, TEE, SW process and apps…

Nested EATs

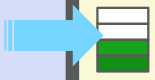
One signed EAT inside another

Running State

Boot and debug state


Measurement of Running SW

Runtime integrity check



Formal Device Certifications

For example, Common Criteria certification; format is GP's DLOA

SW Results

Results of comparison of SW measurements to reference values

EAT work needed beyond claims

- Rework introduction and related with respect to RATS Architecture
  - Use Architecture terminology: “Attester”, “Verifier”…
  - Remove most of the architecture-related text currently in EAT

- More examples

- Should a verification procedure be included?

Changes since IETF 110

- Added SUEID – Semi-permanent UEID
- Add appendix comparing IDevID to EAT
- Added section on use for Evidence and Attestation Results
- Fill in the key ID and endorsements identification section
- Remove origination claim as it is replaced by key IDs and endorsements
- Added manifests and software evidence claims (CoSWID, SUIT manifests)
- Add string labels and non-claim labels for use with JSON (e.g. label or members of location claim)
- EAN-13 HW versions are no longer a separate claim. Now they are folded in as a CoSWID version scheme.
- Lots of GitHub issues closed

CHARRA and RIV

- Henk Birkholz
- Guy Fedorkow

RATS YANG Module for Challenge-Response-based Remote Attestation Procedures using TPMs

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,

Michael Eckel <michael.eckel@sit.fraunhofer.de>,

Shwetha Bhandari <shwethab@cisco.com>,

Bill Sulzen <bsulzen@cisco.com>,

Eric Voit <evoit@cisco.com>,

Liang Xia (Frank) <frank.xialiang@huawei.com>,

Tom Laffey <tom.laffey@hpe.com>,

Guy C. Fedorkow <gfedorkow@juniper.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG

Document Status

- I-D depends on the RATS Architecture and RIV to clear
  - Made the reference to the RATS Interaction Models informative
- xml2rfc outdenting issue
  - Editorial issue that is probably not a blocker, tried working around that via kramdown-rfc2629 hotfixes in v1.5.5 with mixed success
- YANG Doctors comments seem to be all addressed, waiting for further feedback
- Next steps?

TPM-based Network Device Remote Integrity Verification

draft-ietf-rats-tpm-based-network-device-attest-07

IETF 111 RATS
26 Jul 2021

Guy Fedorkow - gfedorkow@juniper.net
Eric Voit - evoit@cisco.com
Jessica Fitzgerald-McKay - jmfitz2@nsa.gov

V1a

Objective

- Standardize operational model for today's existing but proprietary TPM-based router/switch Remote Attestation solutions.
  - Enables switches/routers to be appraised by non-proprietary controllers/Verifiers.
  - Gives Network Operators needed stability for interfacing operational systems.

Nonce based Background Check Model

From: draft-birkholz-rats-reference-interaction-model

What Evidence does RIV Appraise?

Section 2.1.1 outlines what we expect to attest with RIV, including:

- Code
  - Firmware, OS loader, OS kernel and applications
- Credentials
  - Keys used to authorize operation of routers, e.g. code-signing public keys or network-access private keys (e.g. VPN keys)
- Configuration
  - Security-sensitive configuration files

RIV is intended to secure the infrastructure, so that subsequent higher-level claims can be trusted.

Relationship to other WG drafts

Language

draft-ietf-rats-architecture
- Terminology
- Topological models
- Timing definitions

Enables WG discussion via shared context

draft-birkholz-rats-reference-interaction-model
- Interaction models

Profile

draft-ietf-rats-tpm-based-network-device-attest
- Use case
- Prerequisites/simplifying assumptions which enable operation
  - TPM1.2/TPM2.0/equivalent needs
  - Pre-established Key Types
  - Pre-configured endorsements
- RIV call flow
- Evidence evaluation
  - PCR allocations for network devices
  - Relevance/viability of KGVs for a subset of PCRs
  - Appraisal Policy for Evidence
  - Attester log type formats supportable

Peer Router Appraisal

Interface Specification

Defines operational pre-requisites for

draft-ietf-rats-yang-tpm-charra
- YANG definitions & RPCs for Attester

Attestation Evidence via Telemetry

draft-birkholz-rats-network-device-subscription
- Provably fresh events
- Subscribed YANG notifications

draft-voit-rats-trustworthy-path-routing
- Trustworthiness Vector
- Stamped Passport definition

Next Steps

- Forward RIV along with CHARRA for IESG review

Reference Interaction Models and DAA

- Henk Birkholz

RATS Reference Interaction Models for Challenge-Response/Time-Based/Streamed Remote Attestation

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,

Michael Eckel <michael.eckel@sit.fraunhofer.de>,

Wei Pan <william.panwei@huawei.com>,

Eric Voit <evoit@cisco.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG

Document Status

- Effective final issue was:
  - https://github.com/ietf-rats-wg/draft-ietf-rats-reference-interaction-models/issues/12
    (Authentication Secret)
- The proposal in the remaining PR #43 was vetted and is now considered to be out-of-scope. Some parts of it might move to a new document and some parts of it could move to existing I-Ds.
- Proposal for next step: request for WGLC

RATS Direct Anonymous Attestation

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Christopher Newton <cn0016@surrey.ac.uk>,
Liqun Chen <liqun.chen@surrey.ac.uk>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG

Document Status

- Around IETF 110, this I-D has been split out of:
  - https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
- -00 received a good amount of pre-adoption reviews and comments:
  - Thanks to Hannes, Thomas, Wei, Laurence, Ned, and Guy!
- Recent feedback is primarily reflected in new Privacy & Security Considerations content:
  - https://www.ietf.org/rfcdiff?url2=draft-birkholz-rats-daa-01.txt
- Dave Thaler joins the authors team. Welcome!
- Proposal for next step: Request for WG adoption call (WGAC)

Concise Reference Integrity Manifest

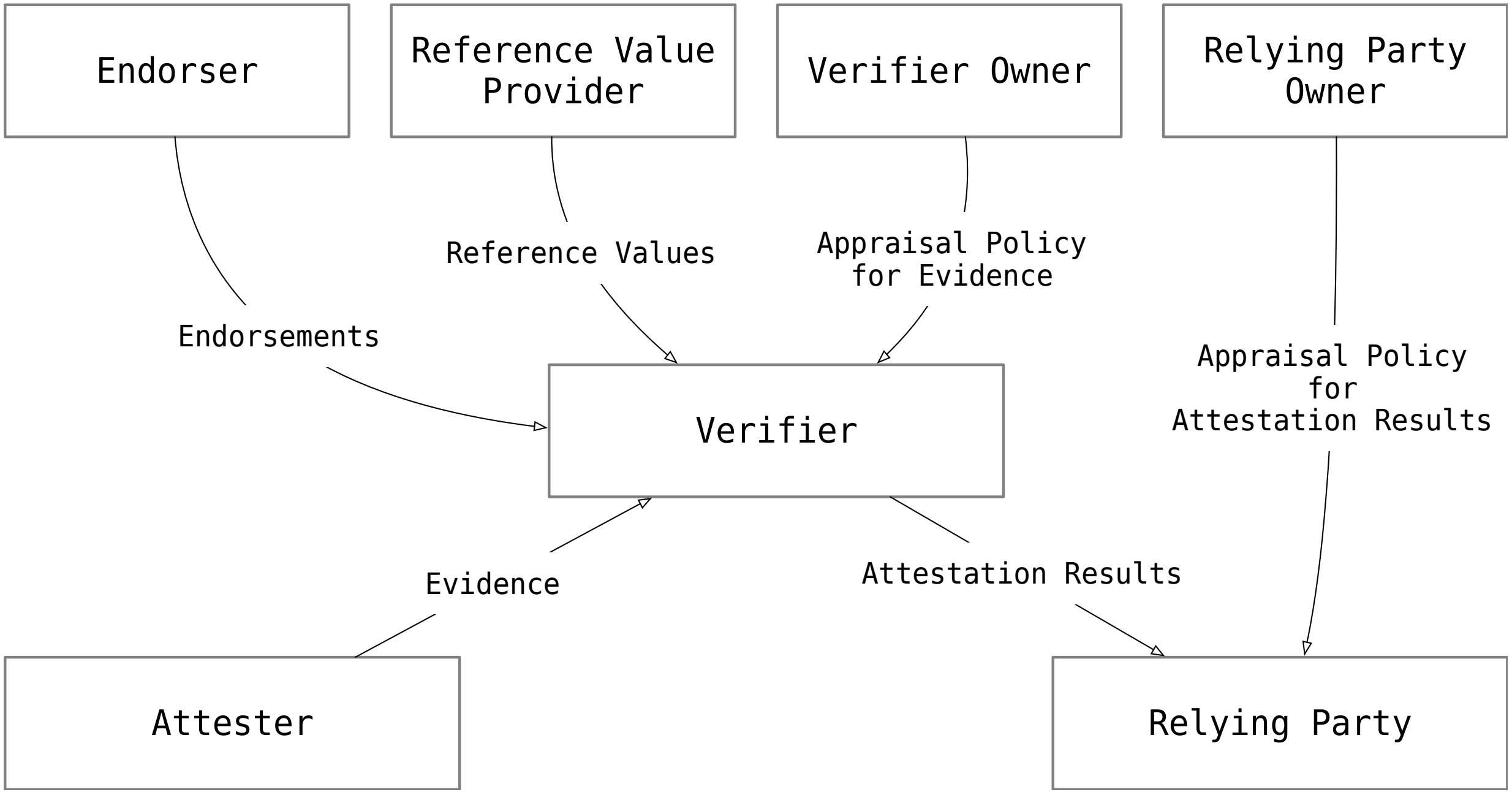
- Henk Birkholz

Describing Attesters to Verifiers:
Concise Reference Integrity Manifests

https://datatracker.ietf.org/doc/draft-birkholz-rats-corim/

Ned Smith <ned.smith@intel.com>,
Yogesh Deshpande <yogesh.deshpande@arm.com>,
Henk Birkholz <henk.birkholz@sit.fraunhofer.de>,
Wei Pan <william.panwei@huawei.com>,
Thomas Fossati <thomas.fossati@arm.com>,

IETF 111, notinsanfrancisco, July 26th 2021, RATS WG



RATS Architecture, Conceptual Data Flow in https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1

Problem Statement

One or more authorized supply chain actors (OEM, ISVs, SiPs, etc.) need to come together and "describe" an Attester to a Verifier. So, when Evidence from that Attester is passed on to the Verifier, it can use the attributes that apply to the Attester to appraise Evidence against the Appraisal Policy.

Without a standard Information Model / Data Model there is no standard tooling to reduce fragmentation or lower barriers to entry for the supply chain actors.

Problem Context & Scope

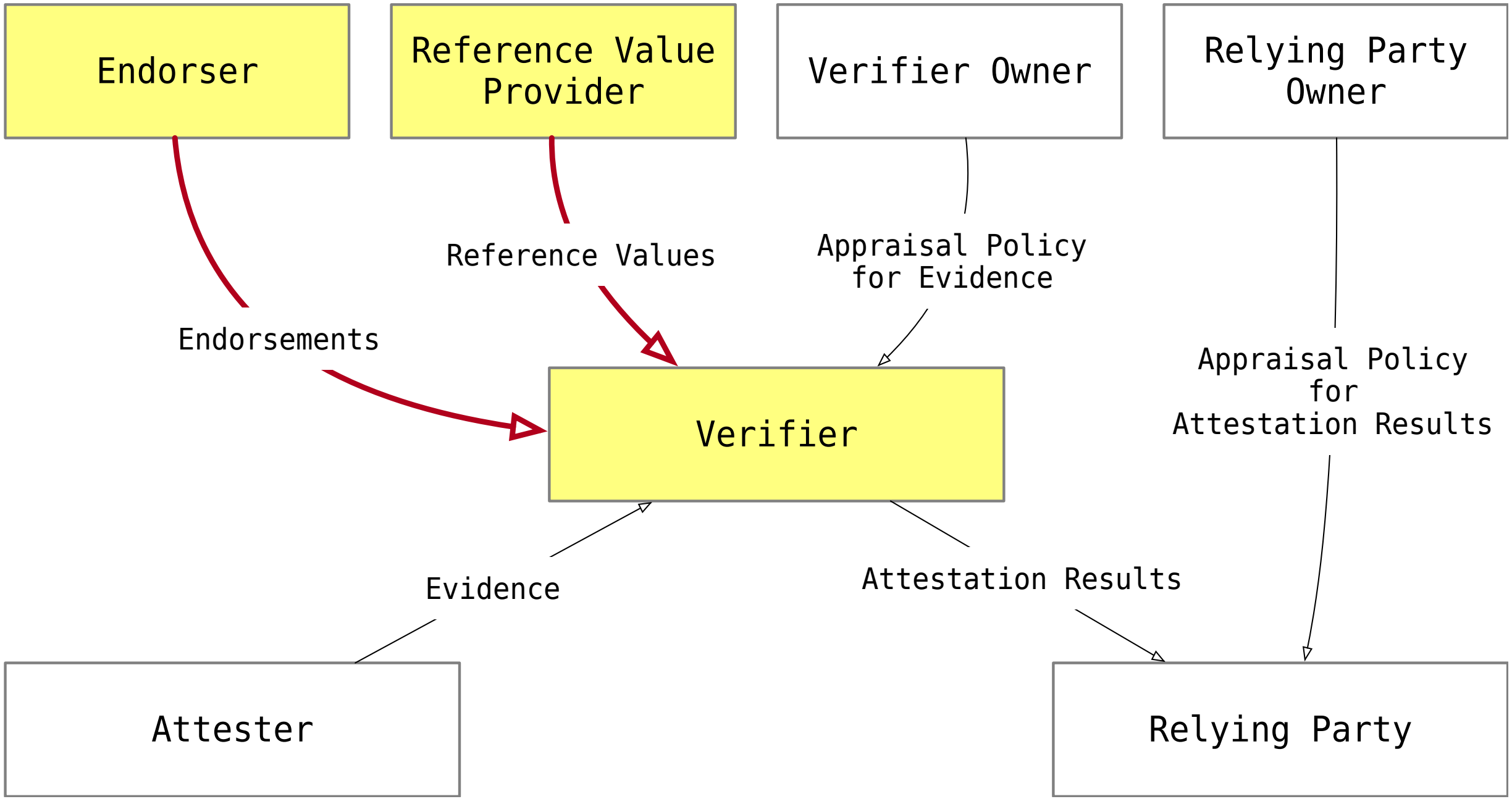
The descriptive material that flows from the supply chain to the Verifier can be, for example:

- Measurements, for example, FW – "Reference Values"
- Verification key material, certification status – "Endorsements"

It is also necessary to describe the composition of an Attester from its relevant parts (i.e., its Attesting and Target Environments):

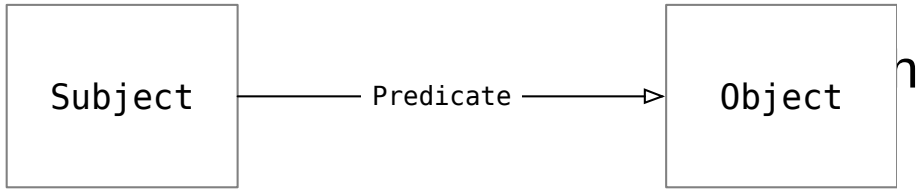
- This is not necessary for very simple attesters (AE:TE=1:1) but can come in handy for more complex topologies where the device structure is reflected in the Evidence structure (e.g., via submodules in EAT).
- Also, it can be useful for factoring out common parts that are reused across different Attesters.

Out of scope – at least for the moment – is the delivery of Verification Policies to the Verifier by the Verifier Owner.



RATS Architecture, Conceptual Data Flow in https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-1

High-Level Design

- Graph Data models (RDF-like) with its own specialized vocabulary and data types
- The "triple" 

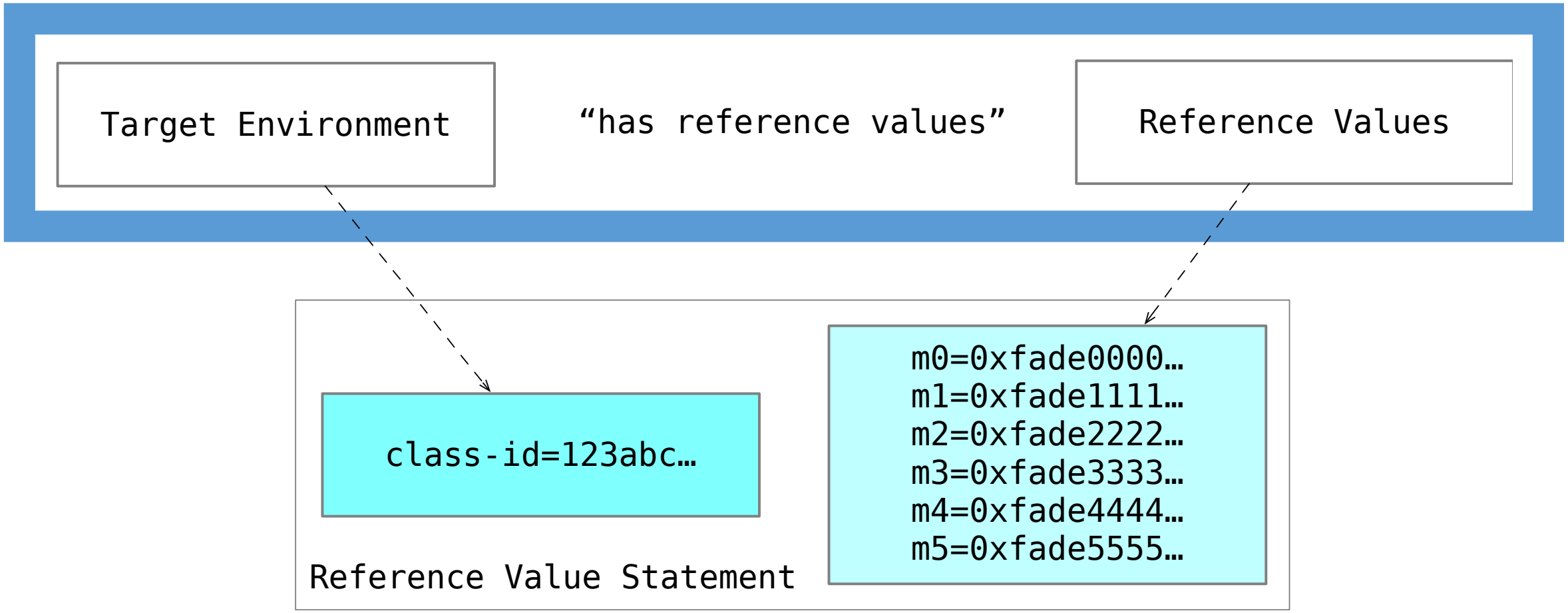
ne core pattern
- Used to define an Attester "ontology" (actually a simple directed property graph)
- Tracking triples provenance via explicit cryptographic methods
- **Co**ncise representations (**Co**MID, **Co**RIM)
  - Concise Module Identifier are the "hardware component" complement (including firmware) to CoSWID https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/, which are already used to represent software components.
  - Concise Reference Integrity Manifests are the trustworthy bundles of CoMID and CoSWID

What Kind of Triples Do We Need?

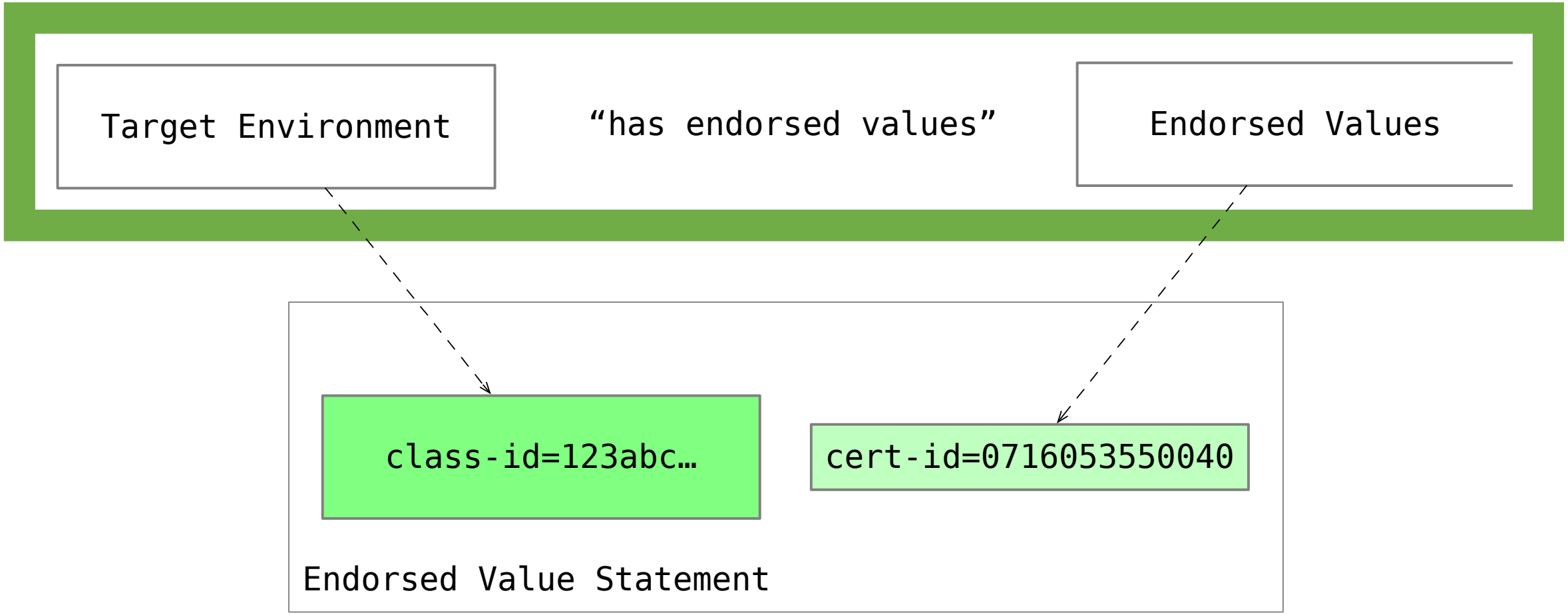
- Reference Values associated with a Target Environment
- Endorsements associated with an Attesting or a Target Environment
- Cryptographic identities associated with Attesting Environments
- Decomposition of a device in its constituent Attesting and Target Environments and their relational features
- Others that we haven’t yet anticipated (built-in extensibility)

- Examples (coming up in the next slides)

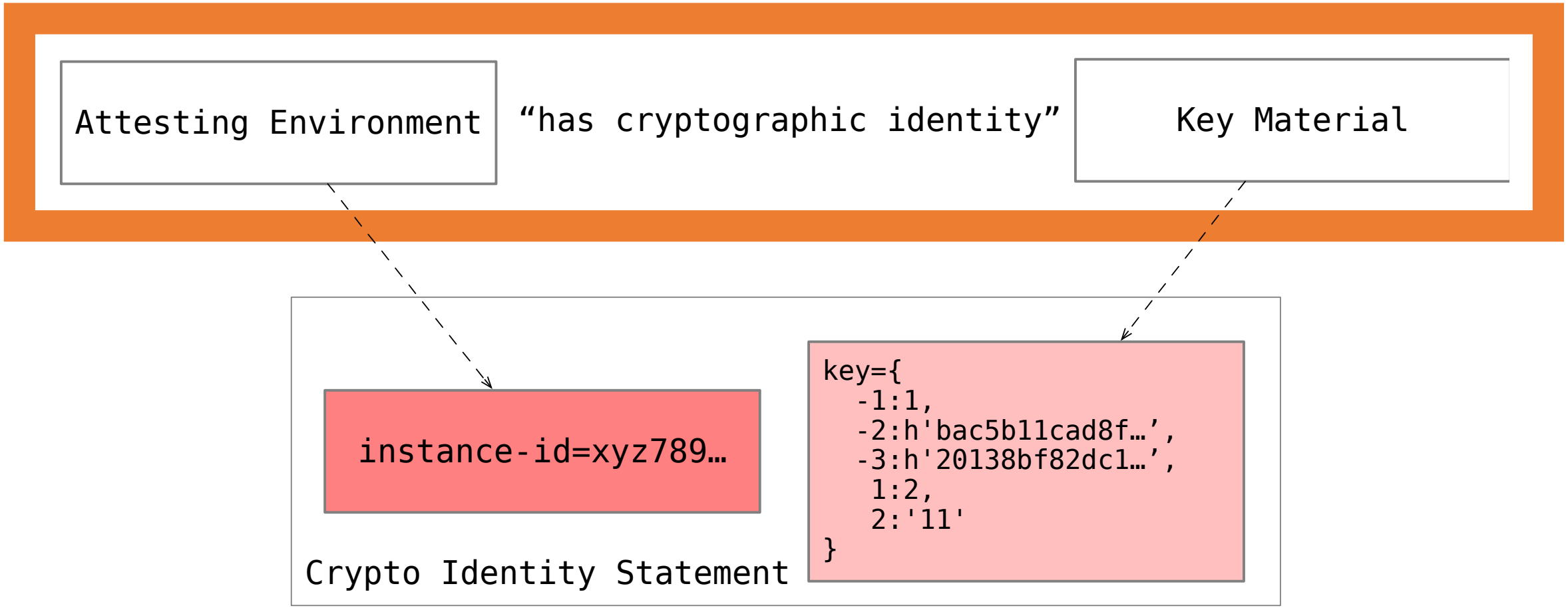
Reference Value Statements



Endorsed Value Statements

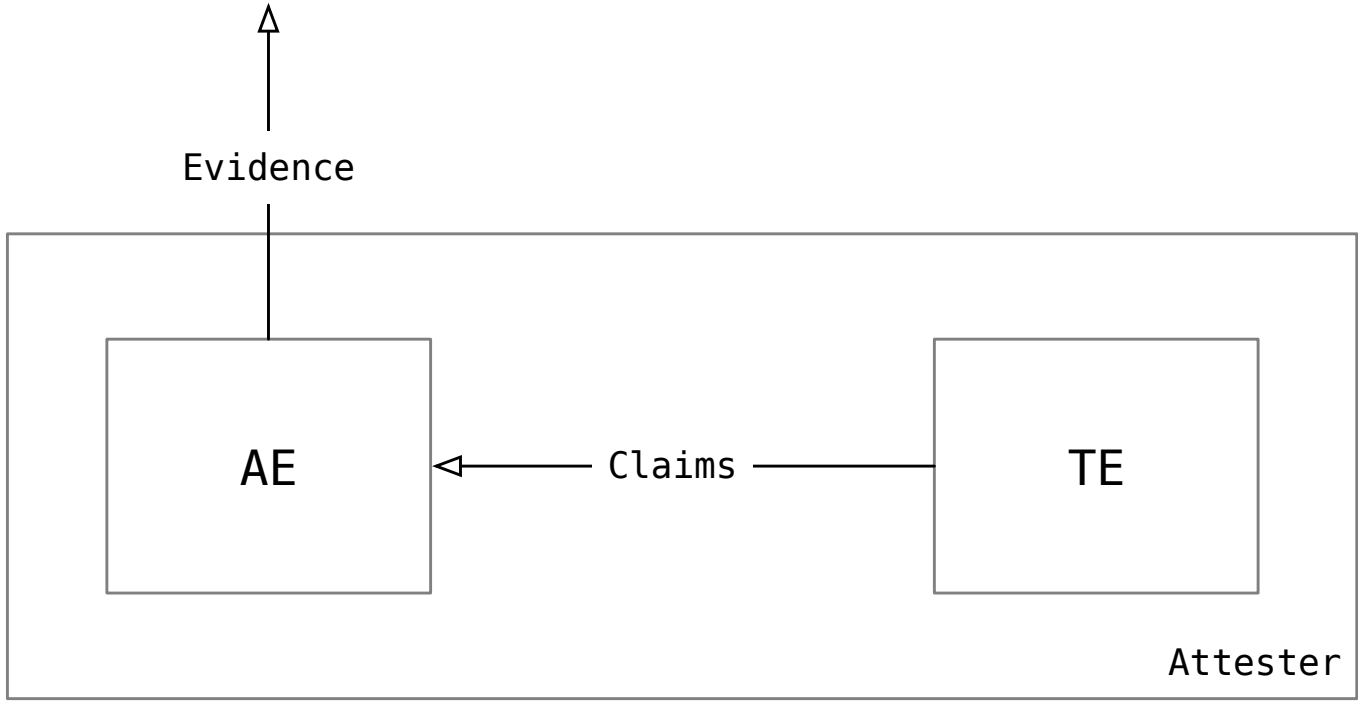


Cryptographic Identity Statement



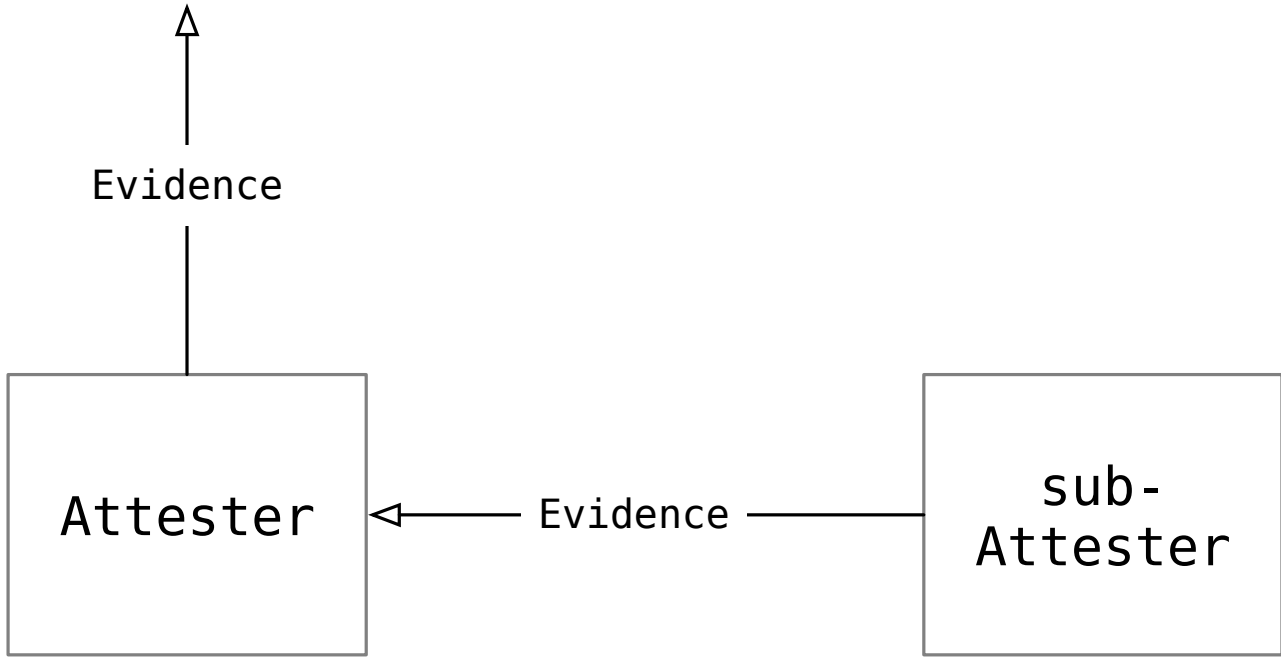
Next Step: Composition Patterns

- Attester (de)composition
  - i.e., relationships between Attesting and Target Environments within an Attester



Next Step: Composition Patterns (cont.)

- Device layering
  - i.e., how different Attesters come together in a composite device



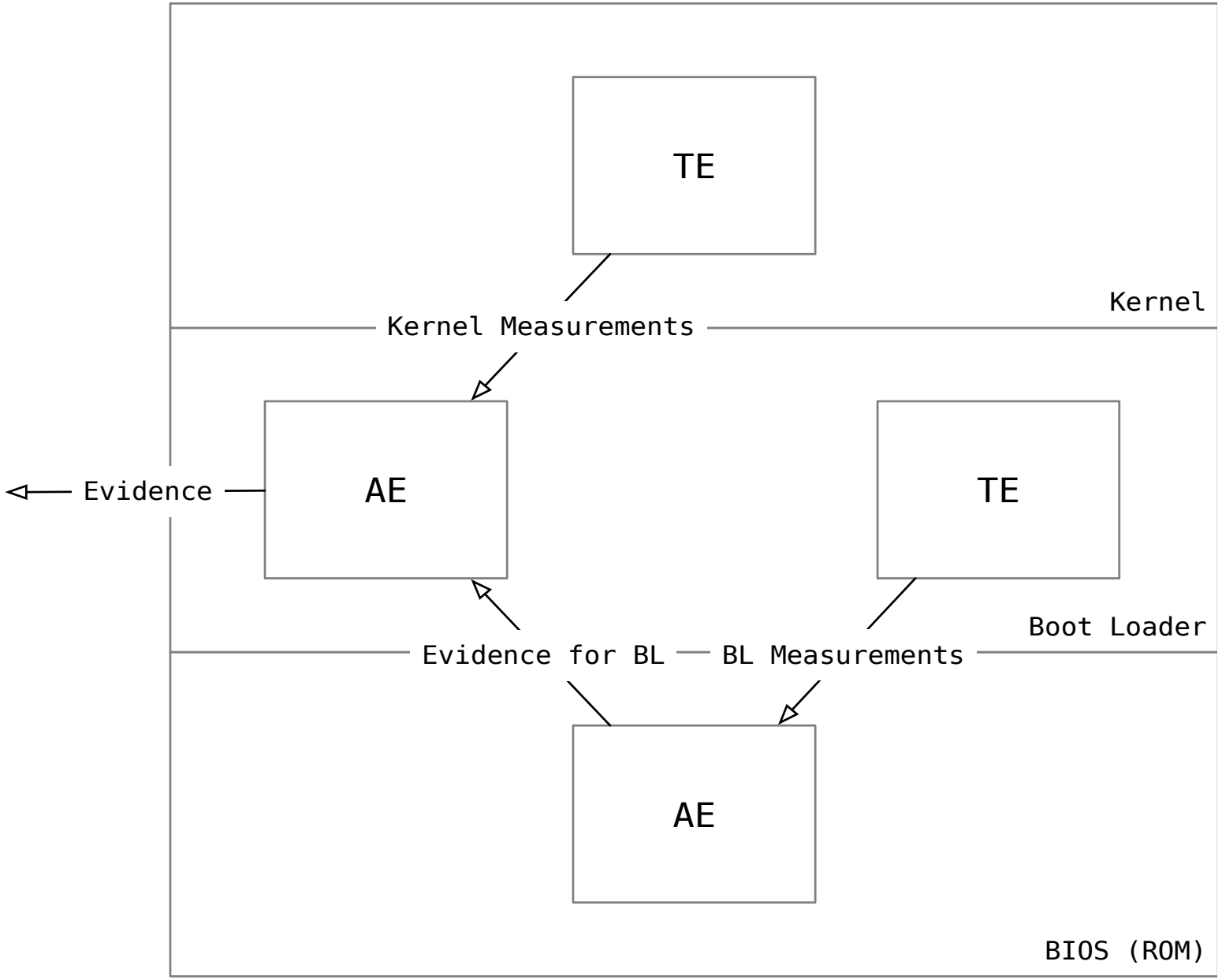
Next Step: Composition Patterns (cont.)

It turns out that both can be expressed with the same statement:

> *Attesting Environment {class-id} retrieves {"claims"|"evidence"} by {"active"|"passive" } collection over {"trusted"|"untrusted"} path from Environment {class-id}*

where the "object" Environment could be either a Target Environment or another Attesting Environment in a sub-Attester.

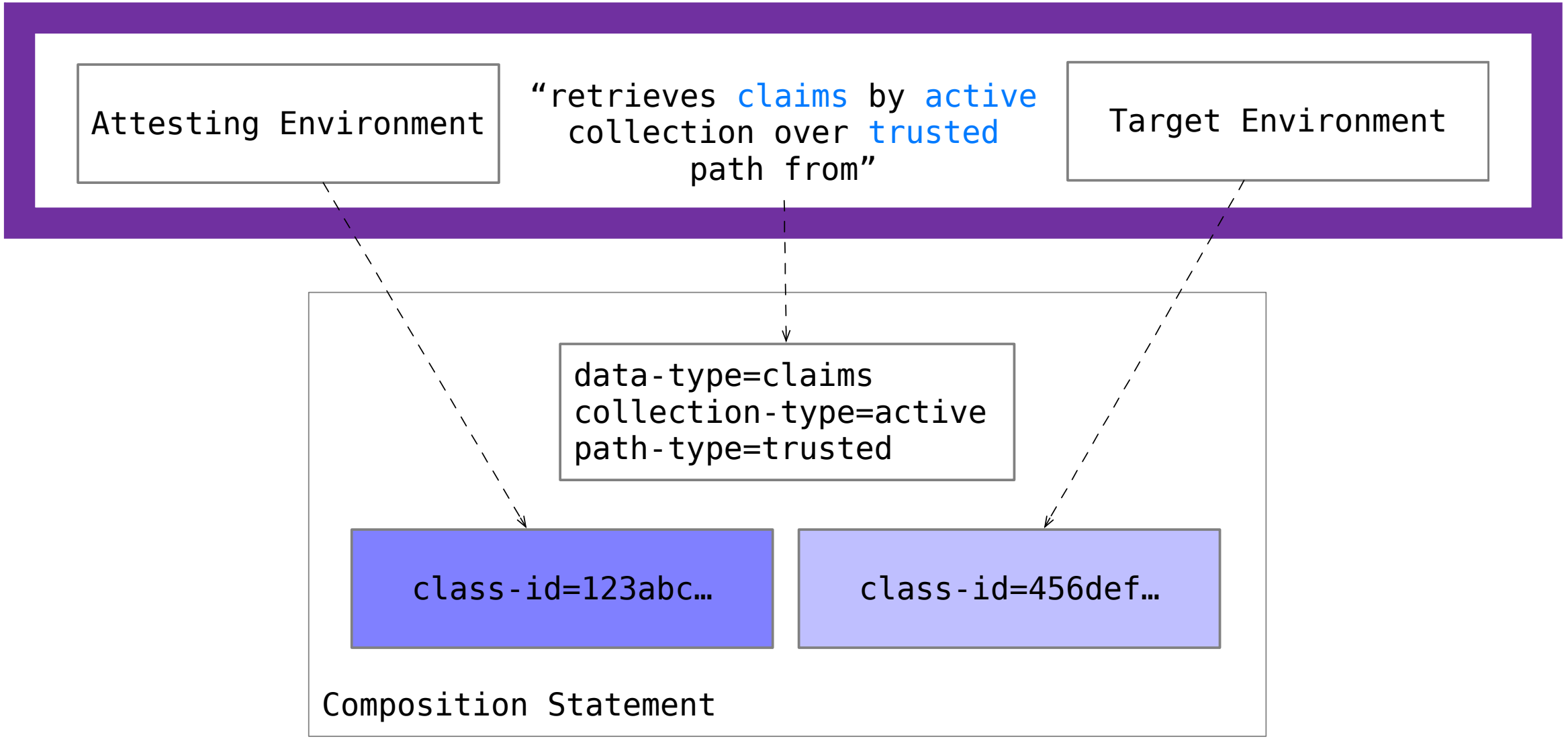
Note: There is also a separate statement to describe the environments that compose a certain Attester. (This is effectively just a grouping overlay on top of a device decomposition that can be fully described by the statement above.)



- BIOS retrieves claims by active collection over trusted path from Boot Loader
- Boot Loader retrieves evidence by active collection over trusted path from BIOS
- Boot Loader retrieves claims by active collection over trusted path from Kernel

Based on RATS Architecture, Layered Attester https://www.ietf.org/archive/id/draft-ietf-rats-architecture-12.html#figure-3

Next Step Example: Composition Statement



CoMID &CoSWID Usage: Grouping Statements

- Similar to CoSWID, CoMID tags are the wrapper around a bunch of statements, but pertain to hardware and firmware
- Like CoSWID tags, CoMID tags allow grouping, identification, typed linking (e.g., *supersedes*, *updates*) with other tags, plus some further encoding optimization in CoMID (e.g., if the statements subject is always the same it can be factored out)
- Grouping criteria are use-case specific. We can *suggest* a few (e.g., for handling FW updates), but we expect best practices to emerge with time and use

CoRIM Usage:
Grouping Groups of Statements

- CoMIDs and CoSWIDs are grouped into CoRIMs
- CoRIMs are signed by the relevant supply chain actor
- Used as the end-to-end conveyance payload (we don’t define the transport)
- The outer signature augments the triples in the CoMID statements with provenance:
  - “Supply chain actor X says ${CoMID-statement} and/or ${CoSWID-statement}”

Pulling All Together

Navigating the sea of triples allows a Verifier to construct a comprehensive device/attester description that it can use as the backdrop against which its Appraisal Policy for Evidence is evaluated.

TL;DR

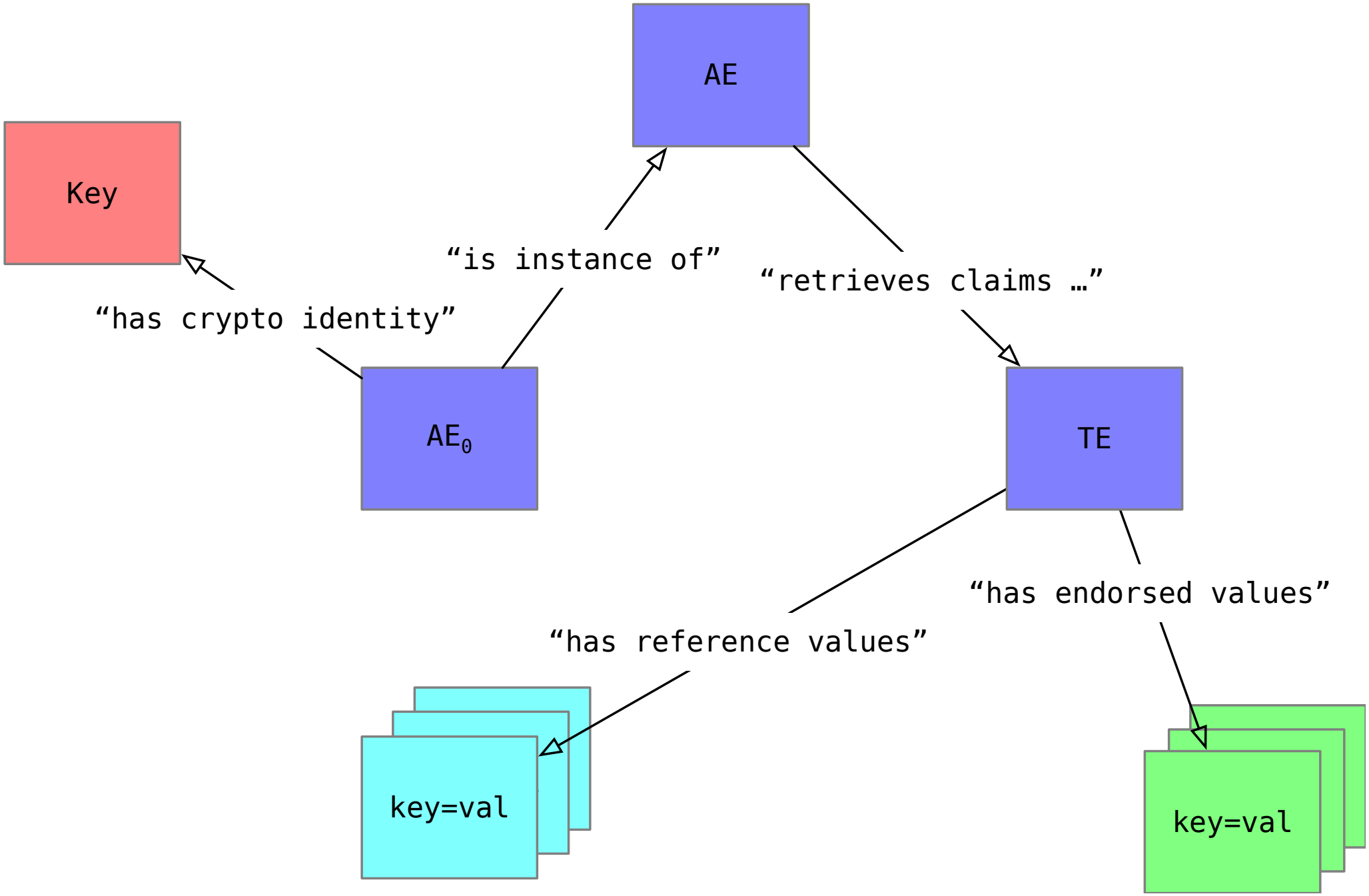
- Information Model Design Authority: TCG DICE WG
- work-in-progress
- Keep an eye on
  - https://github.com/ietf-rats/ietf-corim-cddl
  - https://github.com/ietf-rats/draft-birkholz-rats-corim
  - https://github.com/thomas-fossati/draft-psa-endorsements

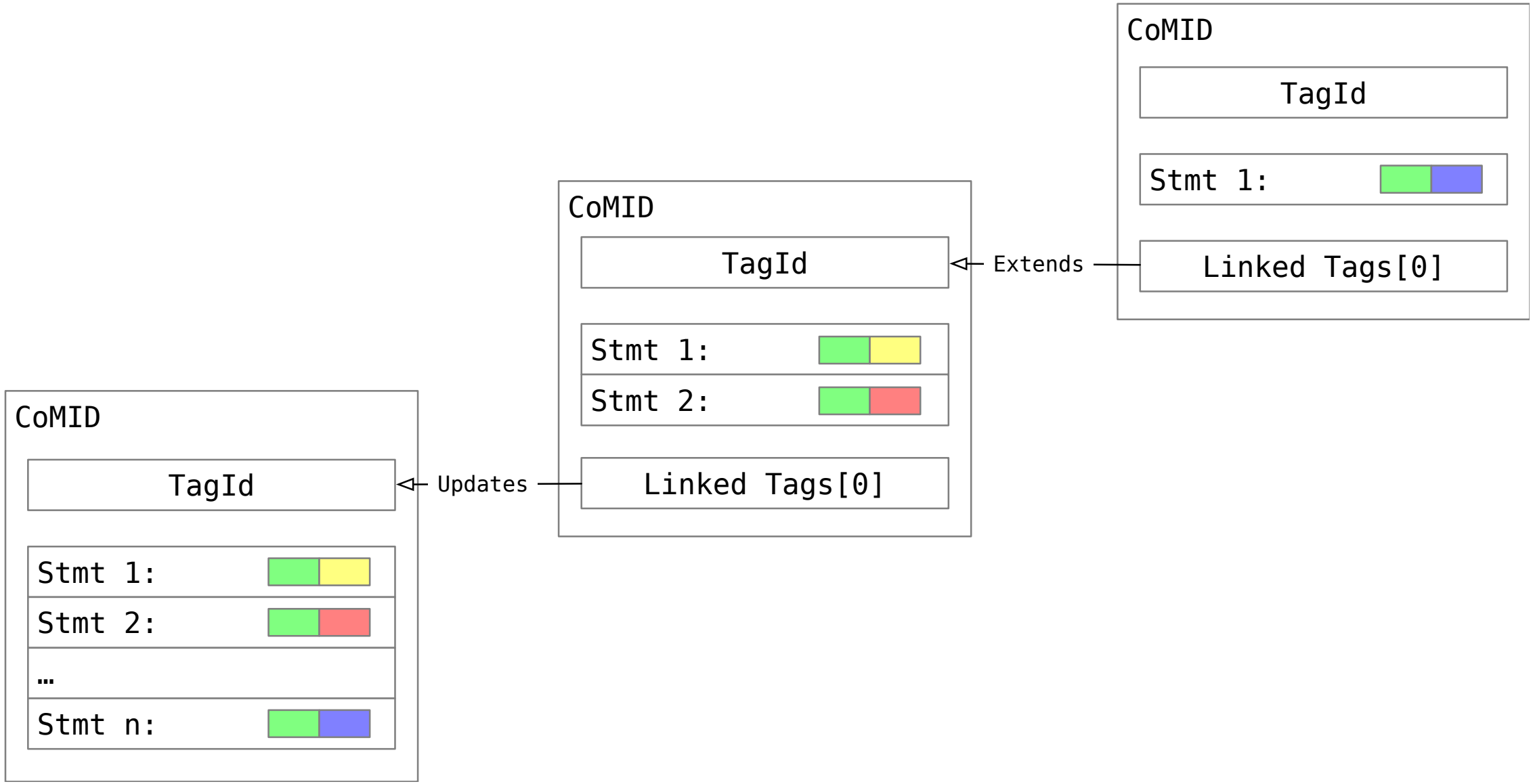
This slide is intentionally left...

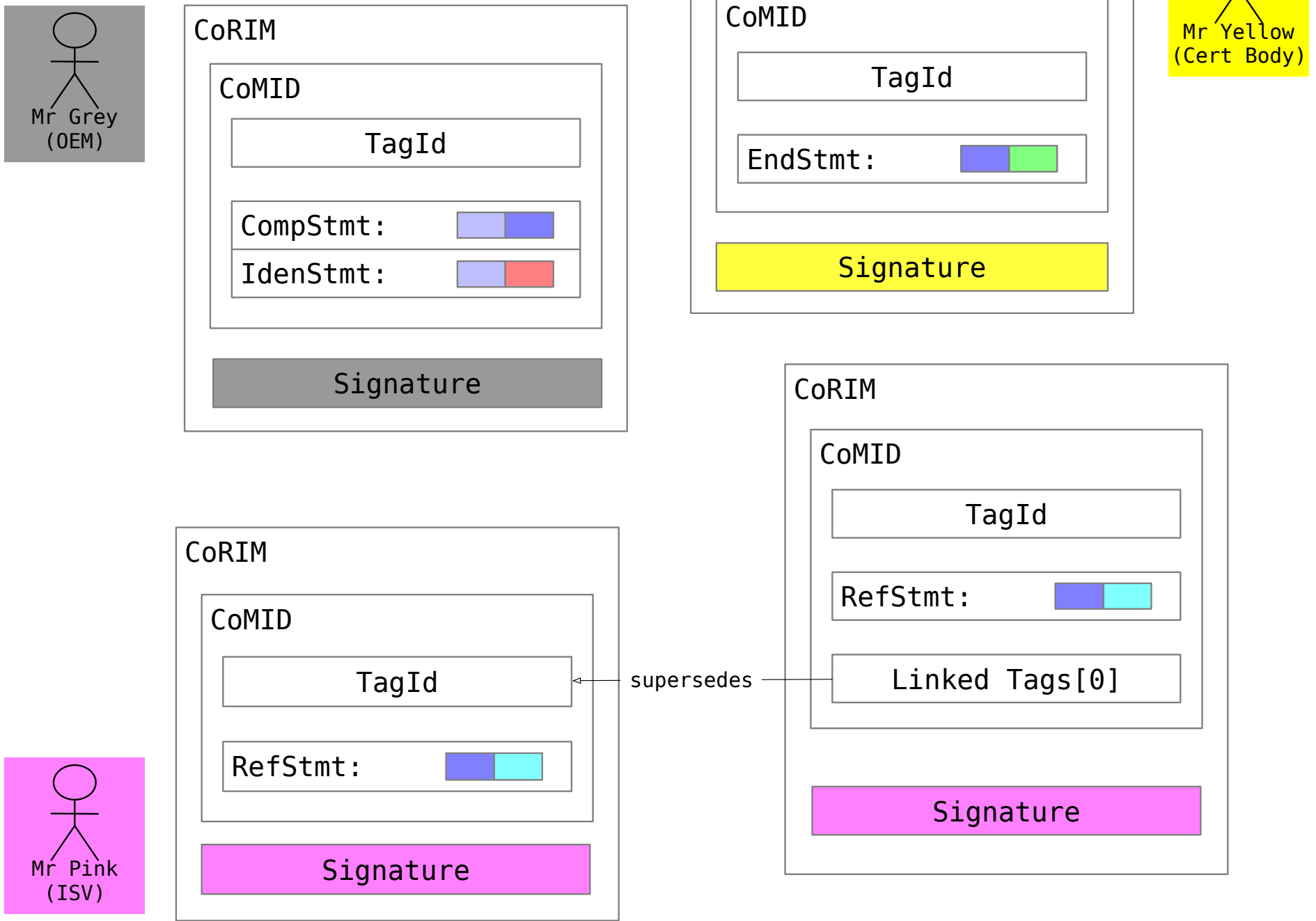
- ... almost blank

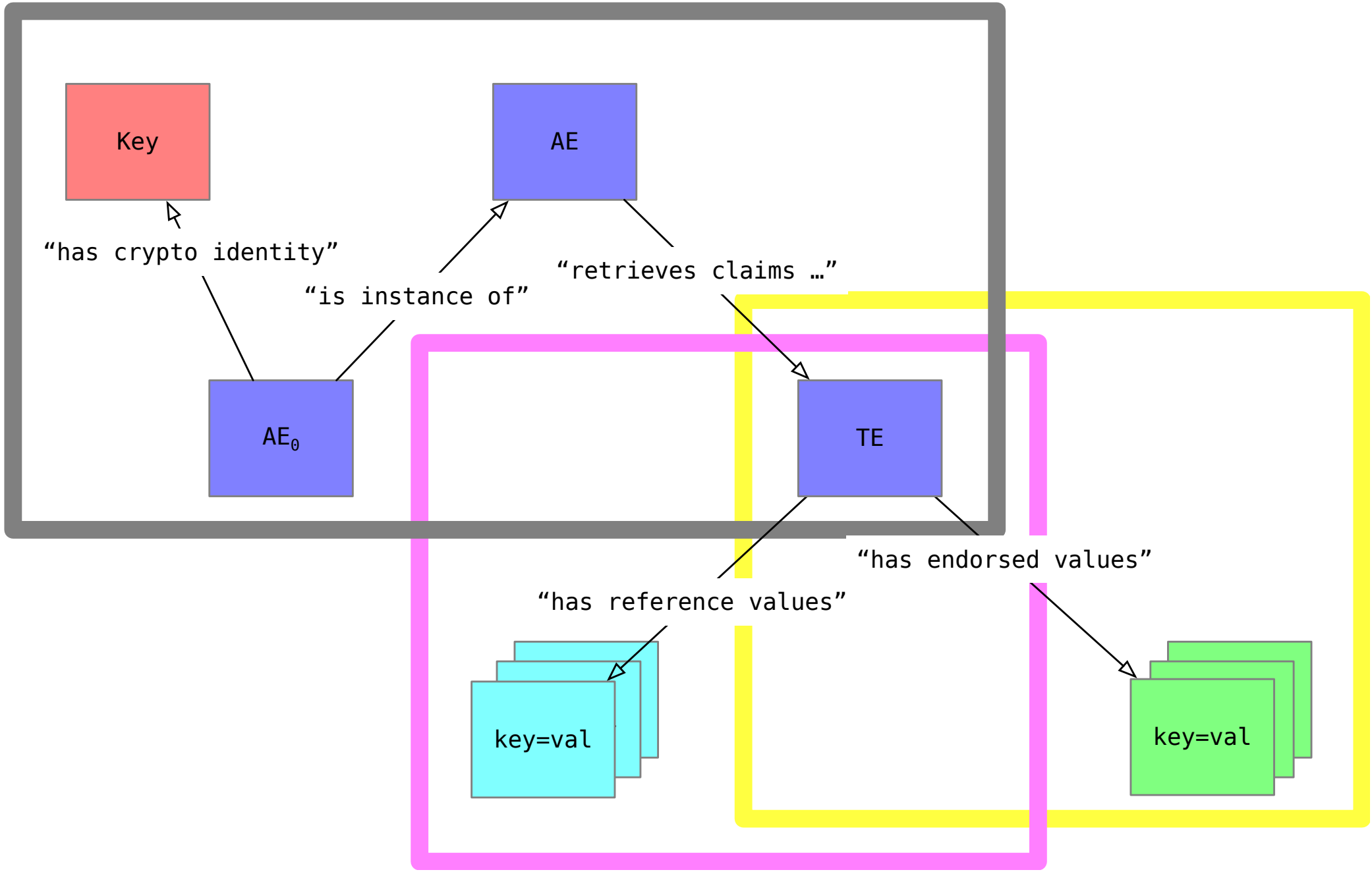
And a few more…

- Attester’s private key has certification path *x5chain*
- A and B are aliases for Attester
- Attester is a member of Group
- *<insert your statement here, the format is extensible>*


AE
Key
“is instance of”
“retrieves claims …”
“has crypto identity”
AE0
TE
“has endorsed values”
“has reference values”
key=val
key=val


CoMID
TagId
Stmt 1:
Linked Tags[0]
Extends
CoMID
TagId
Stmt 1:
Stmt 2:
Linked Tags[0]
Updates
CoMID
TagId
Stmt 1:
Stmt 2:
…
Stmt n:


Mr Grey
(OEM)
CoRIM
CoMID
TagId
CompStmt:
IdenStmt:
Signature
CoRIM
CoMID
TagId
EndStmt:
Signature
Mr Yellow
(Cert Body)
CoRIM
CoMID
TagId
RefStmt:
Linked Tags[0]
Signature
supersedes
CoRIM
CoMID
TagId
RefStmt:
Signature
Mr Pink
(ISV)


Key
AE
“has crypto identity”
“is instance of”
“retrieves claims …”
AE0
TE
“has endorsed values”
“has reference values”
key=val
key=val

Attestation Sets

- Kathleen Moriarty

Thank You!