Composite Attesters (a taxonomy)

Michael Richardson <mcr+ietf@sandelman.ca>,
Henk Birkholz <henk.birkholz@ietf.contact>,
Yogesh Deshpande <yogesh.deshpande@arm.com>

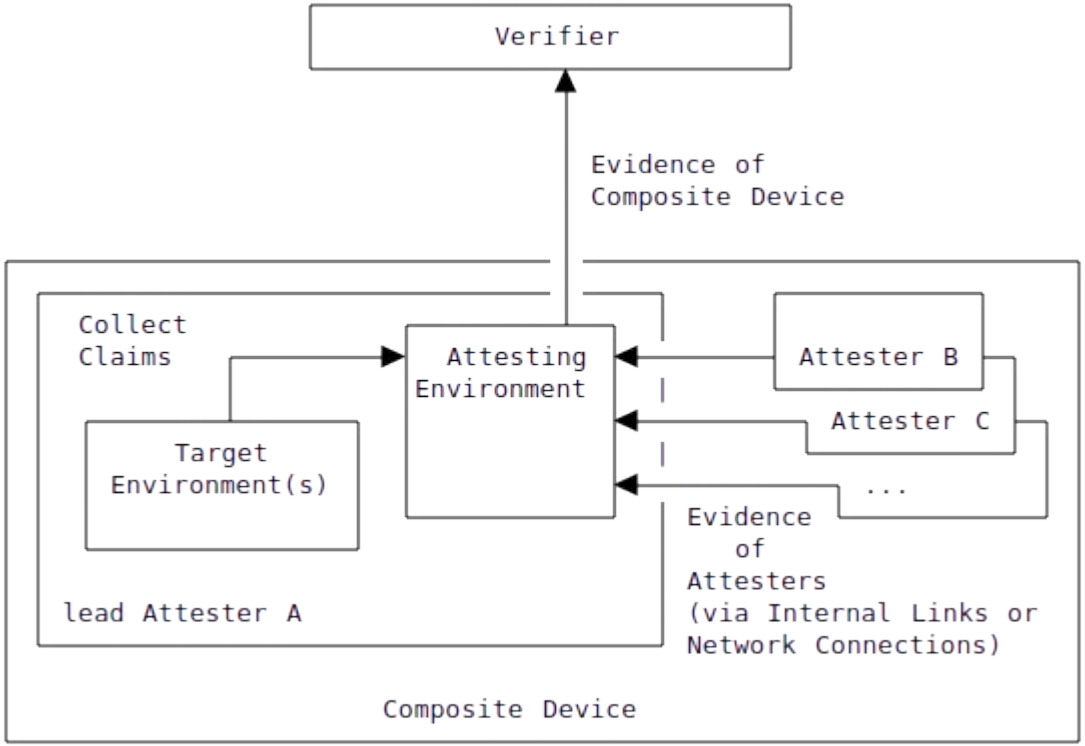
IETF124, RATS, Montreal

Purpose of this document

RFC9334 section 3.3, Figure 4 defined Composite Attester.

This diagram is accurate, but does not capture the emergent variety of different ways to compose things. This has led to difficulty in communicating.

This draft aims to document a standards based terminology and multiple possible compositions of Attesters, mapping it to real-world industry situations



Seven Classes … so far

- A class represents a category or a type of composition
- We are not strongly attached to the word “class”
- The classes are numbered/lettered, with bigger numbers being more complex, but there is also not a strong attachment
- Quite likely that there are new, unique classes that are missing
- There is some overlap between some classes, but also some subtle distinctions
- All classes are pluggable, and any level could be composed of composites
    - Some turtles, but there is some bottom turtle

- Class 0 Composite Attester
- Class 1 Composite Attester
- Class 2 Composite/Hybrid Attester
- Class 3B Composite Background-Check Attester
- Class 3P Composite Passport-Model Attester
- Class 4 Dual Composite Attester
- Class 5 Mixed Composite Attester

Next slides have diagrams for each of these.

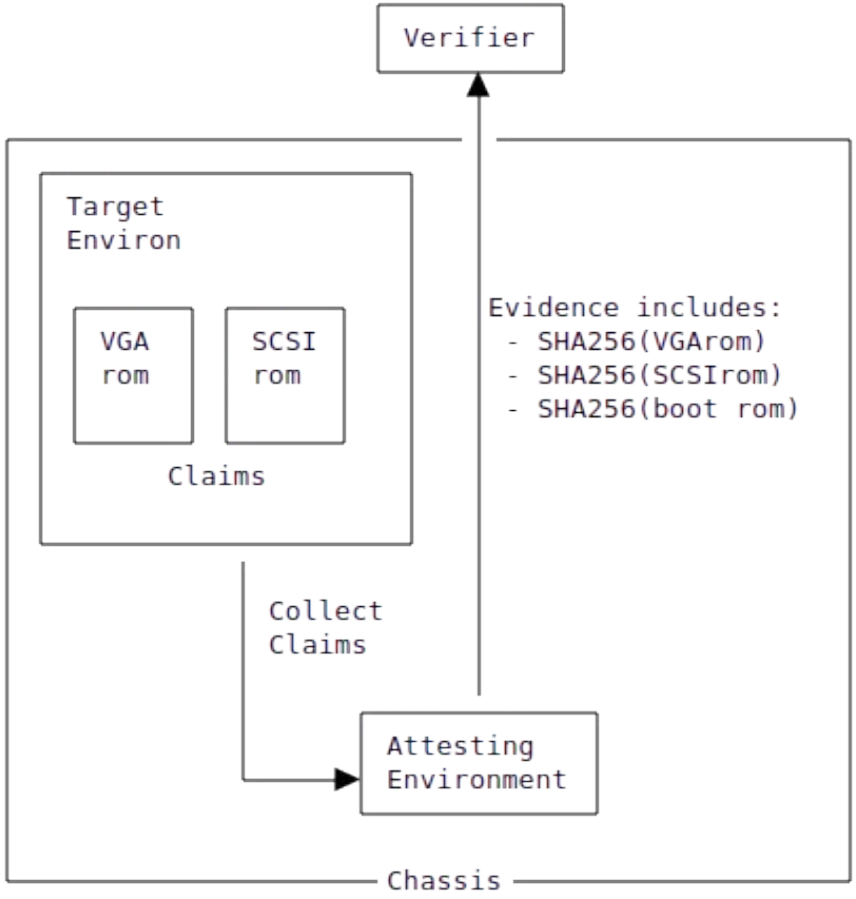
Will stop for very short clarification questions.

Save discussion for Slide 11/12.

Class 0 Composite Attester

Many components, but not really a composite at all.

Think 286/386 ISA/MCA, PCI-33: plug peripherals have ROMs that change the behaviour of CPU. But do **not** have roots of trust. Swapping a Cirrus Logic SVGA for a Trident SVGA would change PCRs, so treat it as a composite to simplify combinatorics.



Class 1 Composite Attester

This is diagram from RFC9334.

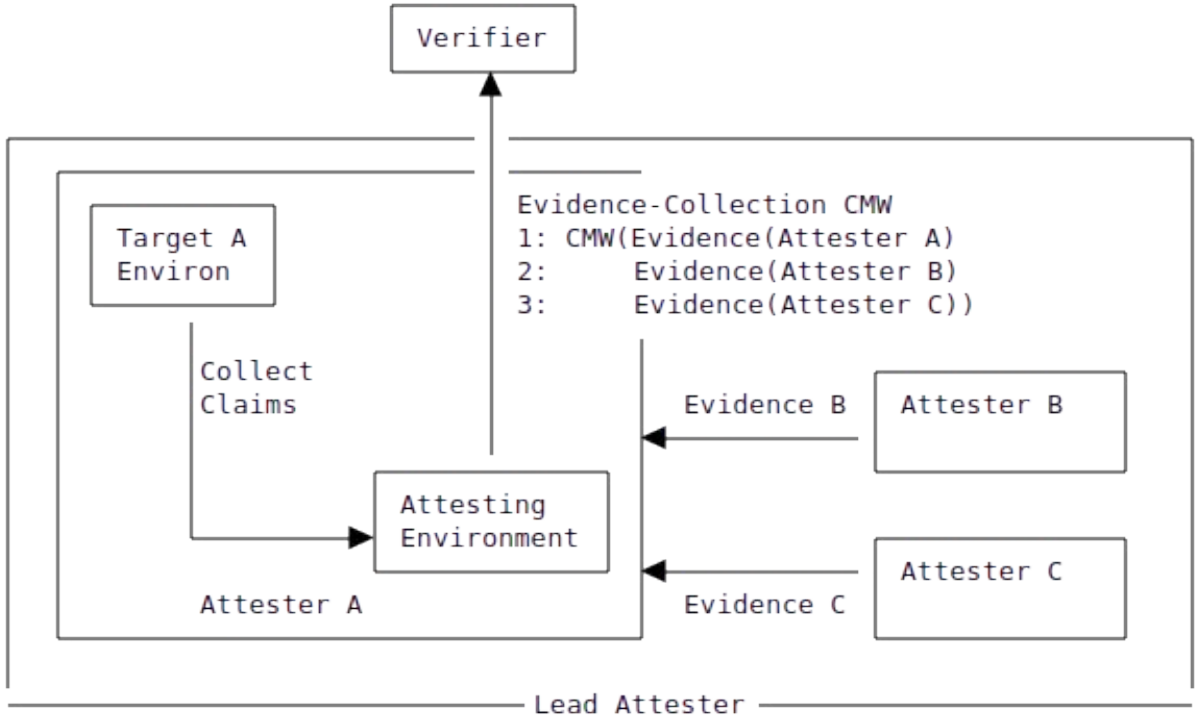
For example, Attester B and C are line cards in a routing chassis.

- They have a control planes which boots with its own RoT.
- They are from the same vendor, so have a single Verifier
- The inventory varies, including being hotplugged.

Attester A also performs a role of Lead Attester.

It has own Claims like Attester B and Attester C

Lead Attester(LA) Collects all Evidence (A,B,C) and may provide protection through an Outer Signature for LA.

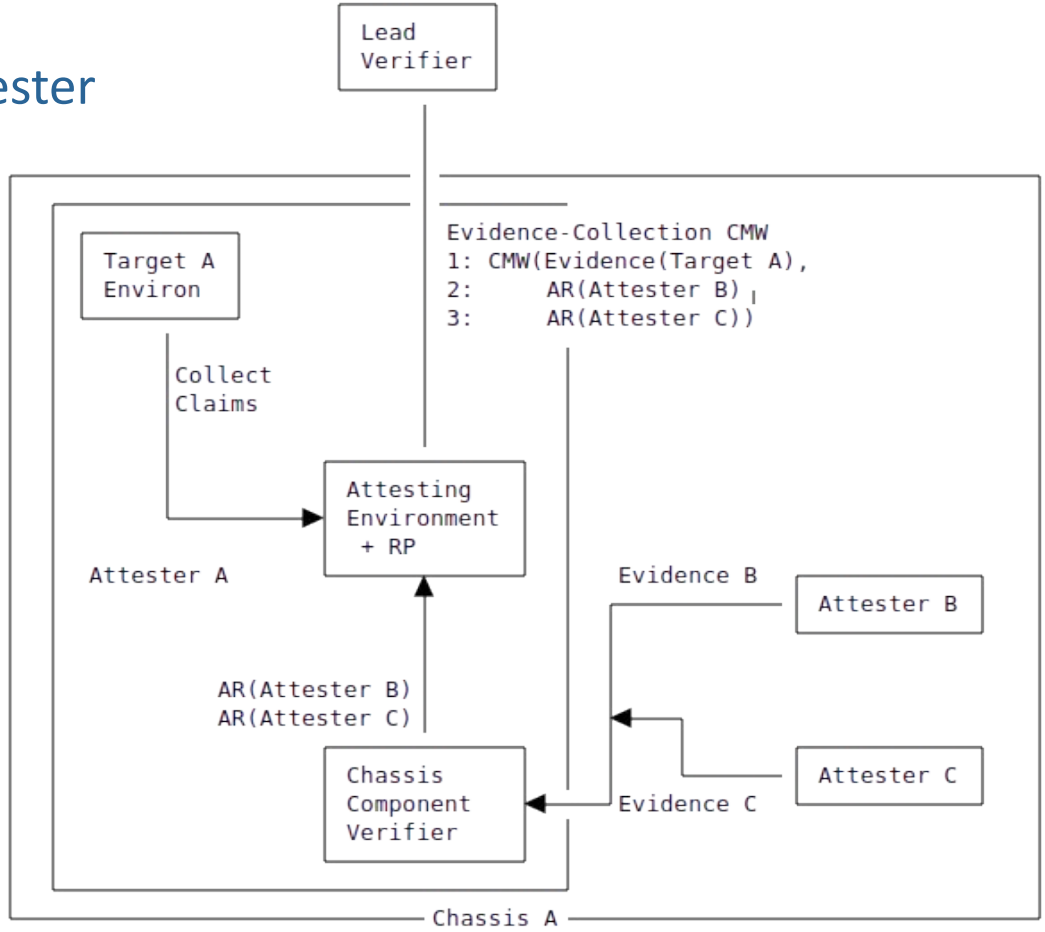


Class 2 Composite/Hybrid Attester

This differs from Class 1, because the evidence from the components ("line cards"), is evaluated within the Lead Attester.

Attestation Results are provided to the Lead Verifier, rather than Evidence!

- Lead Verifier acts as RP for B/C
  - AR for A might not mention B/C.
- Signature on AR is from Attester A.
  - Maybe same as AK-A
  - Maybe a different key
- Component Verifier
  - could be in a TEE
  - could be part of Target A environment.



Class 3B Composite Background-Check Attester

Similar shape to Class 1, (see slide later)

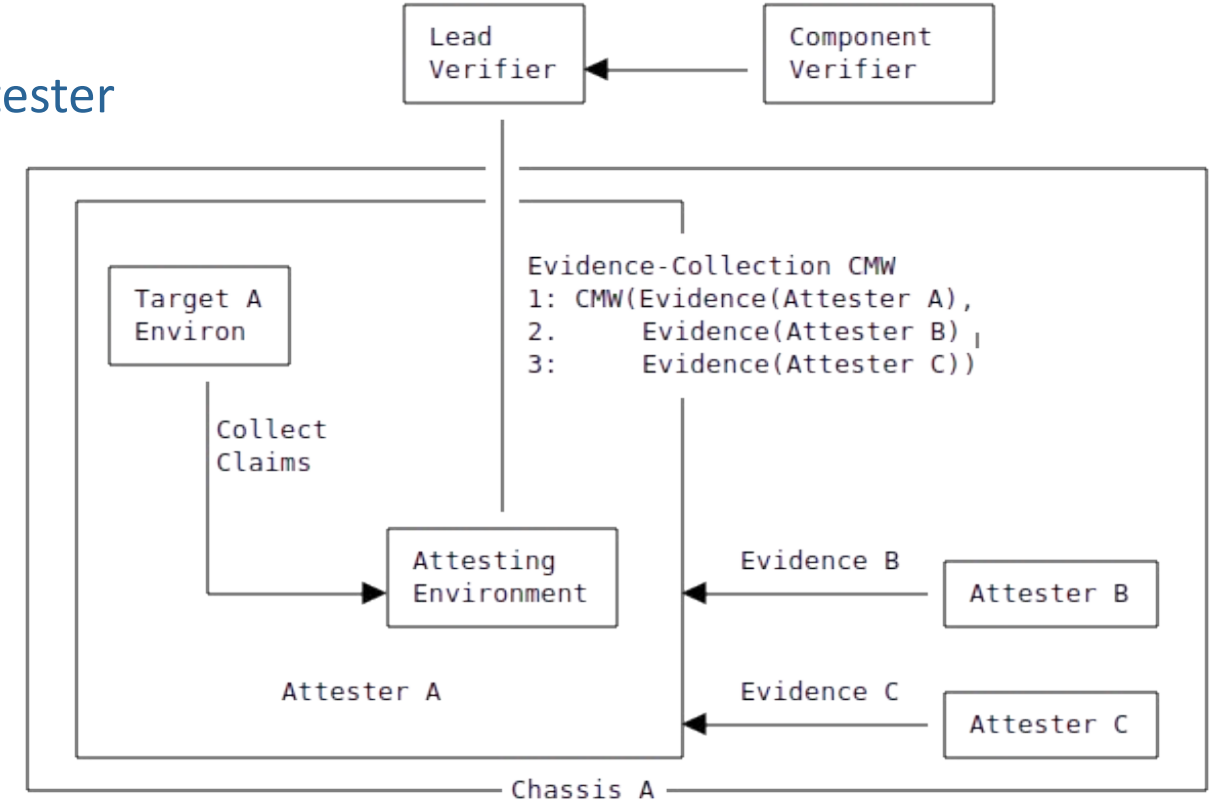
But, Component Verifier(s) are external to Lead Verifier.

- Likely multi-vendor
- GPU
- NeuralProcessorUnit

B/C have to treat Lead Verifier as a RP, possibly encrypting evidence.

How does Lead Verifier pick Component Verifier?

- A problem across **all** Background check models
  - Cf: LAMPS CSR Attestation "hint" debate.



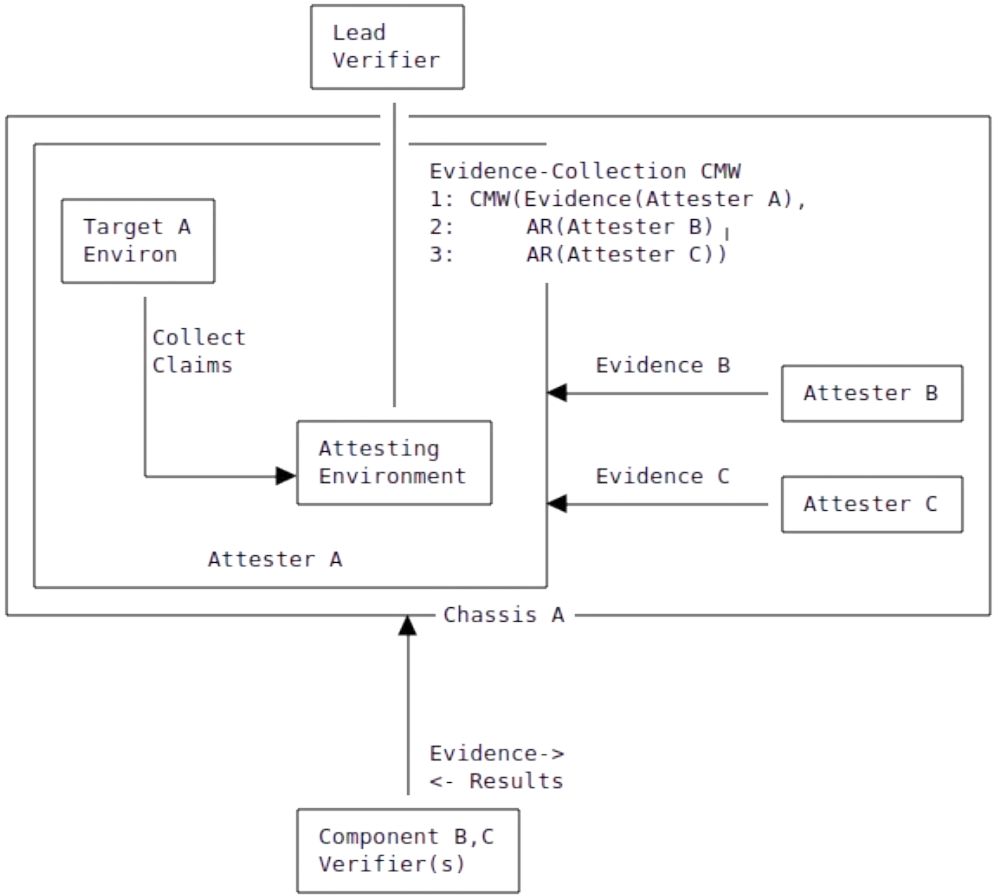
Class 3P Composite

Passport-Model Attester

Similar in shape to class 2.

Lead Attesting Environment A picks Component B/C Verifiers, collects signed AR.

- AR might use selective disclosure to make some details private, but auditable.

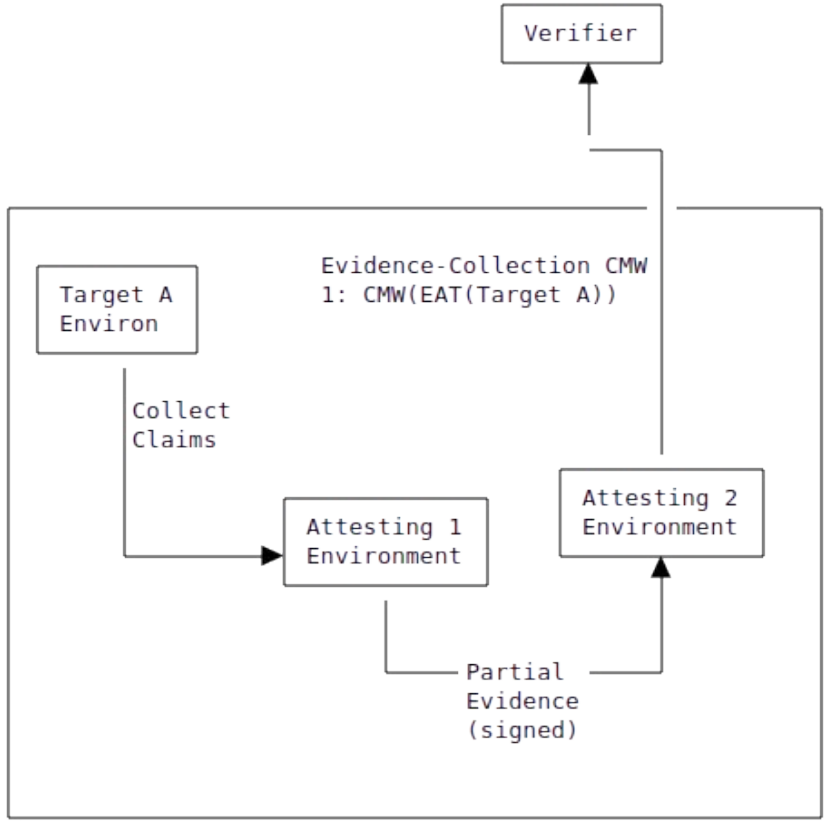


Class 4 Dual Composite Attester

- Two Root of Trusts in the system
- One acts as a Primary and the other as Secondary
- Evidence is presented from Secondary AE (AE1) to Primary AE (AE2)
- Primary AE is responsible for preparing the final Attestation Evidence using the information presented from Secondary AE

Deployment and Configuration drives the choice of Primary and Secondary AE

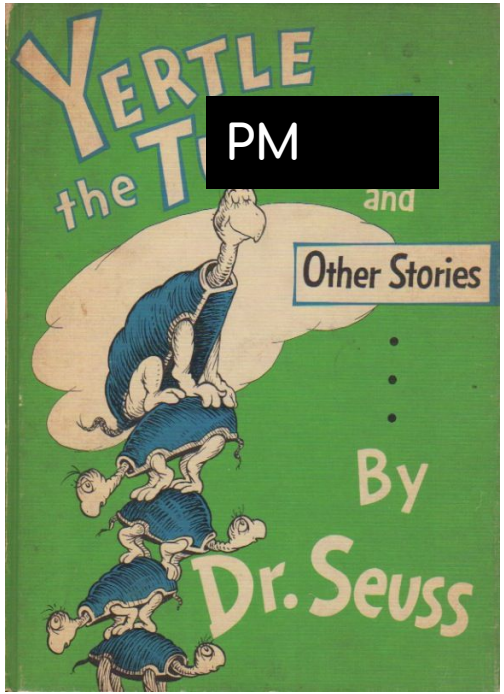
Example: A CPU with a built-in RoT integrated in a TPM System



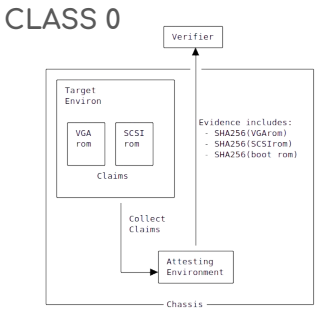
Class 5 Mixed Composite Attester

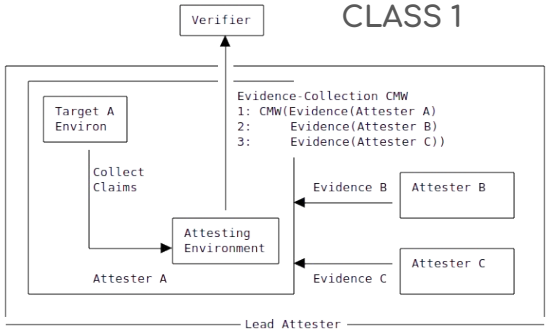
Each class has components that can be themselves compound.

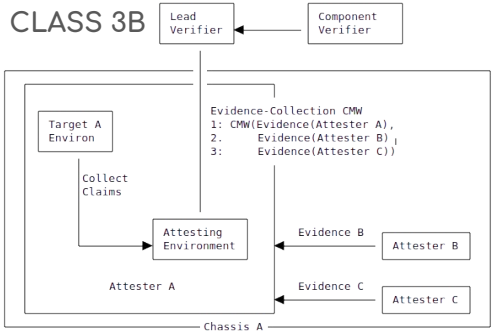
No Diagram Yet

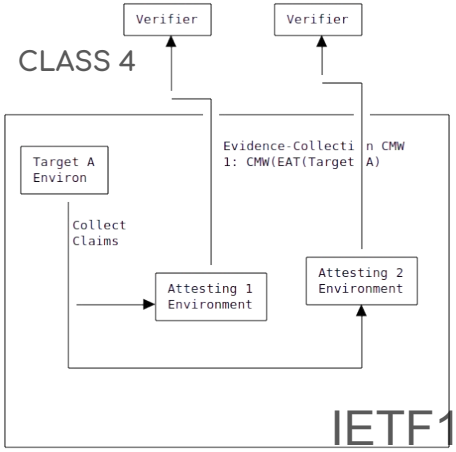


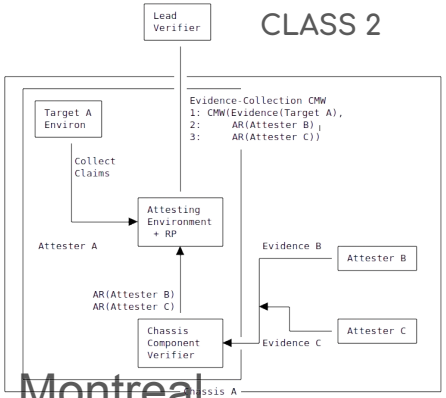
All Composites -- MIC Time

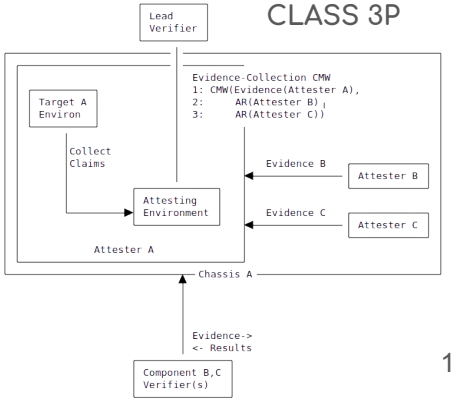




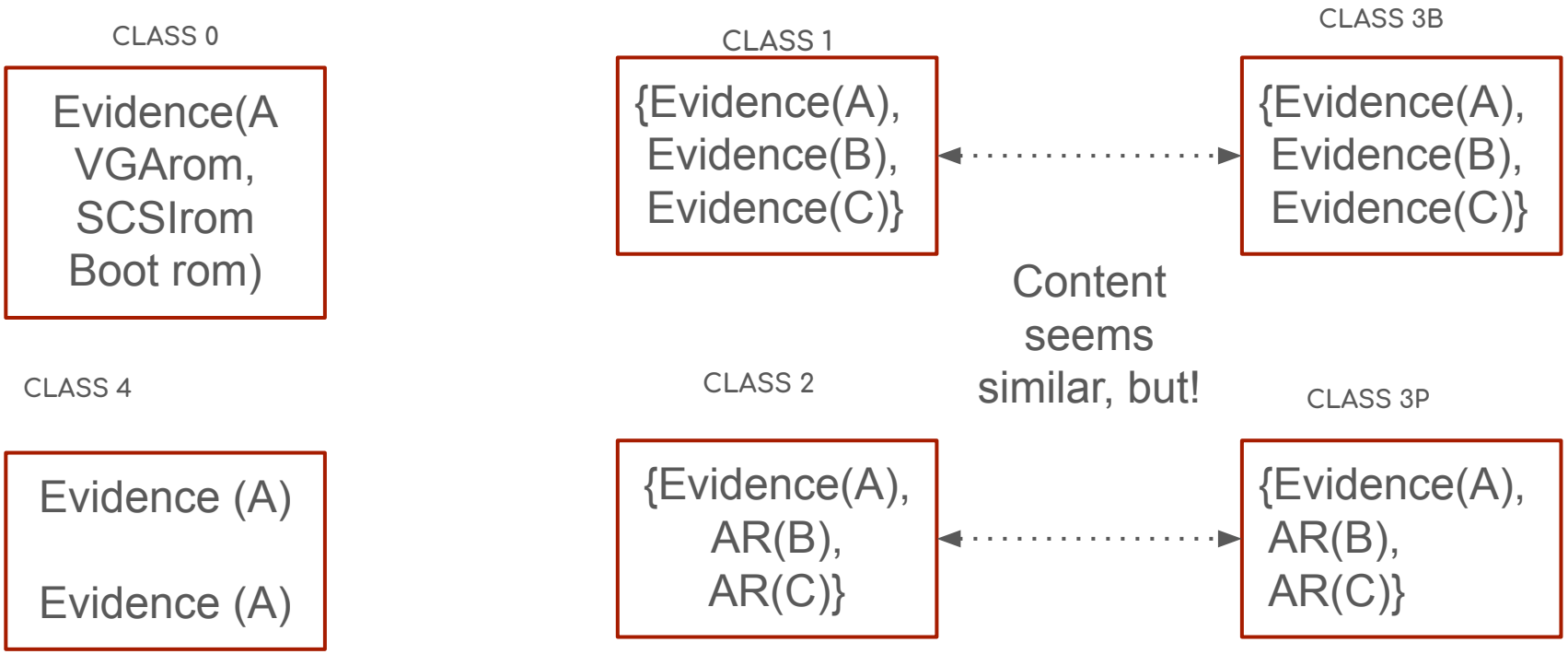








All Composites -- by Attesting Environment/Verifier Arc



Further Discussion

- A section in the document starts to deal with freshness flow for these composites.
  - Generally, the Verifier needs to create the nonce, if you are going that way.
  - So there needs to be a flow in the opposite direction!
  - Requires a second set of diagrams
- Likely some additional classes!
  - Hypervisor + VM?
- Maybe some classes are degenerate

Adopt?

Amends/Updates/Extends

RFC9334