RATS Architecture Design Team Status and Walkthrough

WHO:

- Henk Birholz(*)
- Thomas Fossati
- Andrew Guinn
- Thomas Hardjono
- Sarah C. Helble
- Eliot Lear
- Peter Loscocco
- Laurence Lundblade
- Nicolae PALADI
- Wei (William) Pan(*-new)
- Michael Richardson(*)
- Paul Rowe
- Ned Smith(*)
- Dave Thaler(*)
- Eric Voit
- Monty Wiseman
- Ling (Frank) Xia

WHEN: Tuesdays 10am EST.
(+ a few Fridays/adhoc)

14 meetings since IETF106

ISSUES: 13 open, 20 closed

Pull requests:

2 open, 39 closed

(*)-listed author

Overview of presentation

1) Table of Contents
2) Summary of Open Issues
3) Work since IETF106 and last Virtual Interim meeting
4) Walk through

Table of Contents

Open Issues / Pull Requests

- #73 What are "role compositions"?
  - https://github.com/ietf-rats-wg/architecture/issues/73
- **#71 Section 4.2 and 4.3 should use similar conventions for section names and figures**
  - **https://github.com/ietf-rats-wg/architecture/issues/71**
- #69 create pull requests with time-sequence and table of time points
  - https://github.com/ietf-rats-wg/architecture/issues/69
  - #75 Time considerations https://github.com/ietf-rats-wg/architecture/pull/75
- **#67 Class of claims for messages that 'transit' entities involved in Role interactions**
  - https://github.com/ietf-rats-wg/architecture/issues/67
- #66 Have preferred serialization formats
  - https://github.com/ietf-rats-wg/architecture/issues/66
- #65 More thorough definition of Endorser or Endorsement
  - https://github.com/ietf-rats-wg/architecture/issues/65
- #57 Trust Model Section, Evidence consumed by an Endorser
  - https://github.com/ietf-rats-wg/architecture/issues/57
- #55 Evidence description misses the mark
  - https://github.com/ietf-rats-wg/architecture/issues/55
- #54 Attestation Results description too limited
  - https://github.com/ietf-rats-wg/architecture/issues/54
- #42 to what extent does the security considerations talk about how long things are valid?
  - https://github.com/ietf-rats-wg/architecture/issues/42
- #39 It seems to miss a final conclusion for the second paragragh in section 5.1
  - https://github.com/ietf-rats-wg/architecture/issues/39
- #19 Entity and Sub-Entity & Composite Device and Component
  - https://github.com/ietf-rats-wg/architecture/issues/19
- #18 Claim is used heavily but not in the terminology section
  - https://github.com/ietf-rats-wg/architecture/issues/18
  - #74 Define claim https://github.com/ietf-rats-wg/architecture/pull/74
- #60 Update Trust Model with Implicit Trust Example
  - https://github.com/ietf-rats-wg/architecture/pull/60

Previously Open Issues

- ~~Introduction!~~
- ~~Terminology discussion mostly done~~
  - Last argument is about “Claim”
- ~~Need to get consensus on Layered approach pull request~~
- Published -02: feature complete.
  - Not all issues are show stoppers, some may be unresolvable.

Walkthrough: Conceptual Data Flow

Endorsements come from an external authority

- (e.g., OEM, owner)

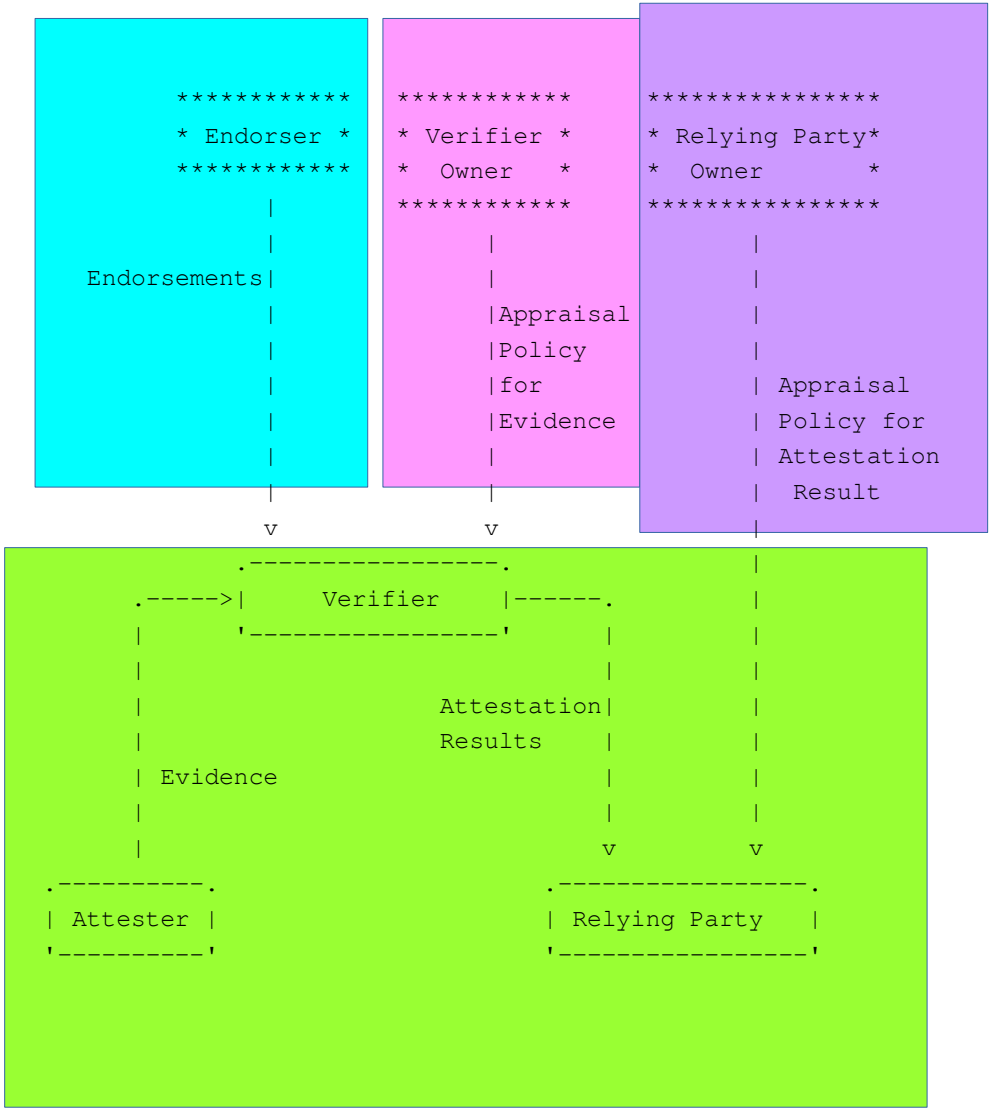
Appraisal Policy is set by Operator

Relying Party sets its own policy

Not in current charter for IETF RATS WG

Attester, Verifier, and Relying Party are connected by Evidence and Attestation Results

In Scope



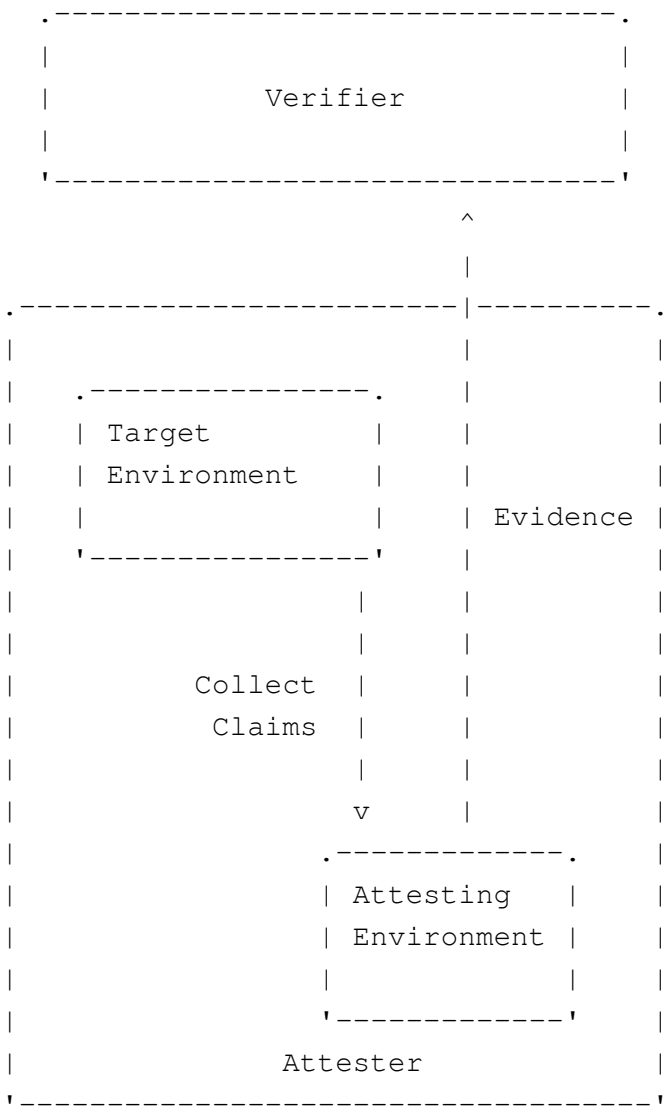
Two Types of Environments

Target Environment

- this is the thing we care about

Attesting Environment

- this is the thing that does the caring



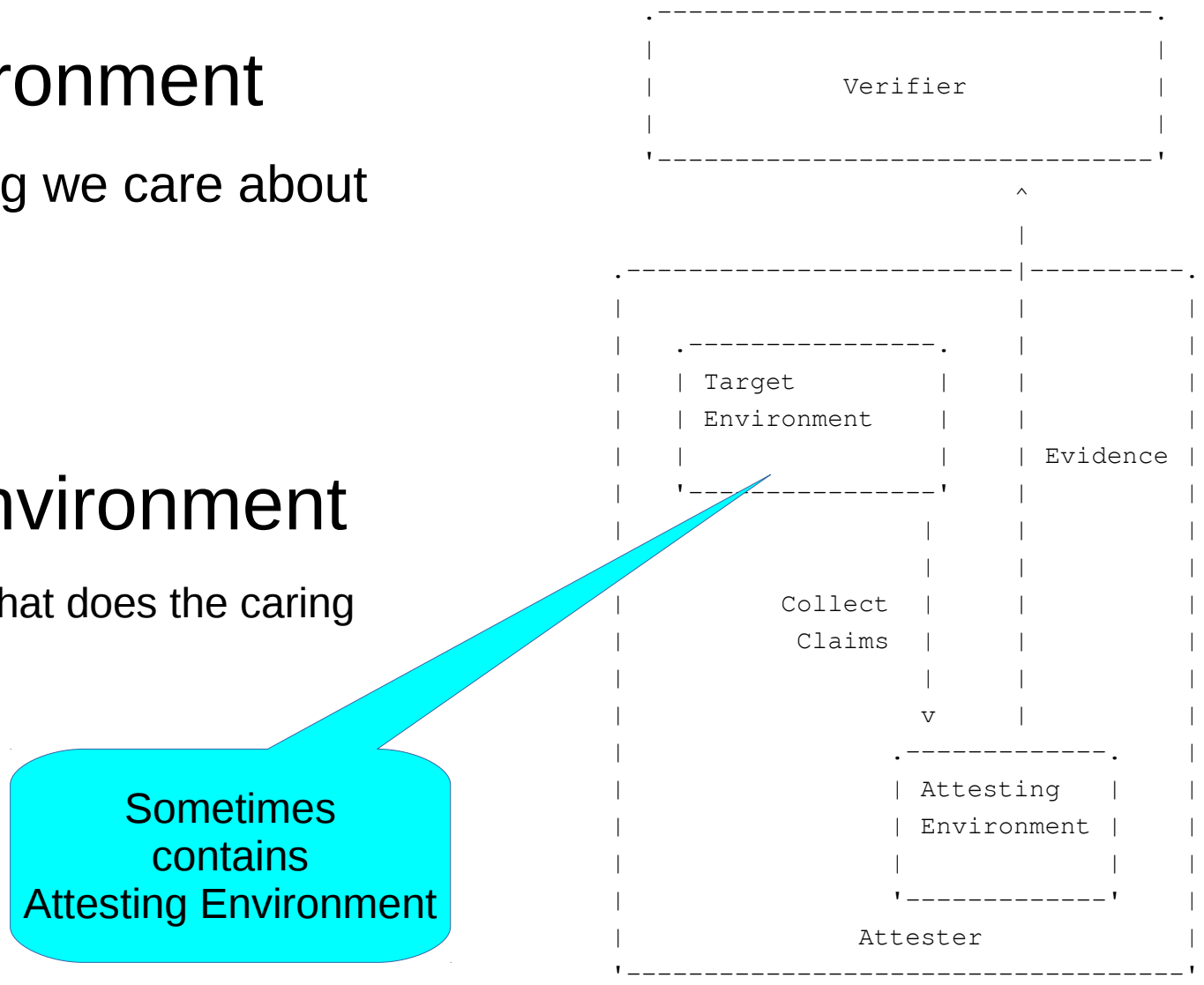
Two Types of Environments

Target Environment

- this is the thing we care about

Attesting Environment

- this is the thing that does the caring



Two Types of Environments

Target Environment

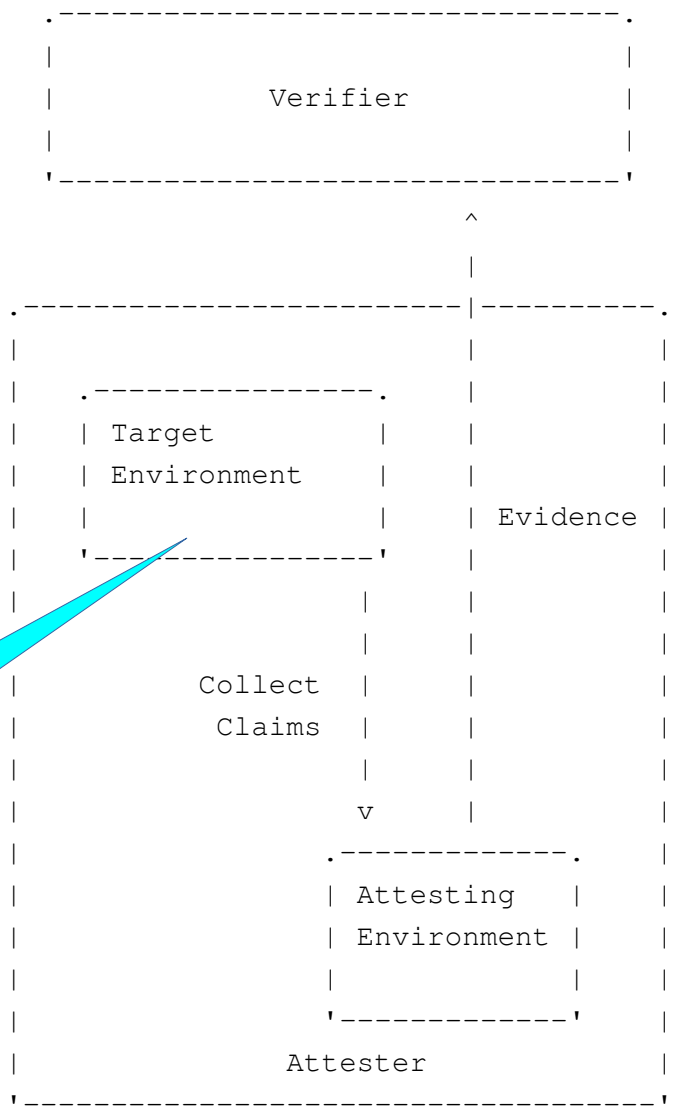
- this is the thing we care about

Attesting Environment

- this is the thing that does the caring

Some people ask:
can the measurements
be trusted?

Sometimes
contains
Attesting Environment



Two Types of Environments

It does not always make sense, but **VERIFIER** is responsible To decide this

Target Environment

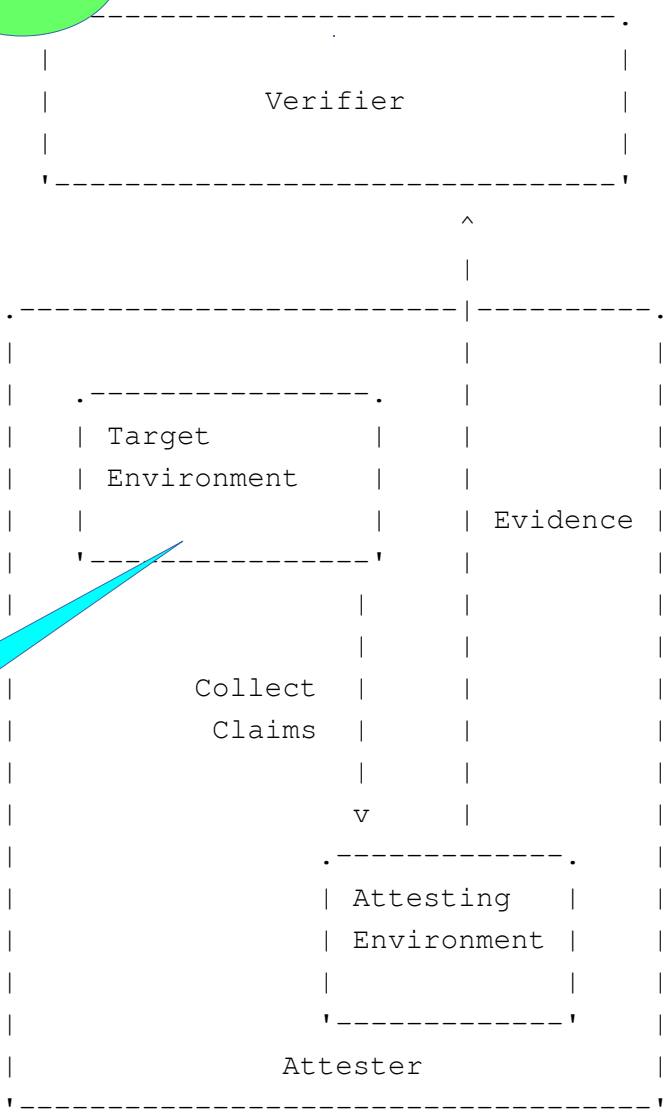
- this is the thing we care about

Some people ask: can the measurements be trusted?

Attesting Environment

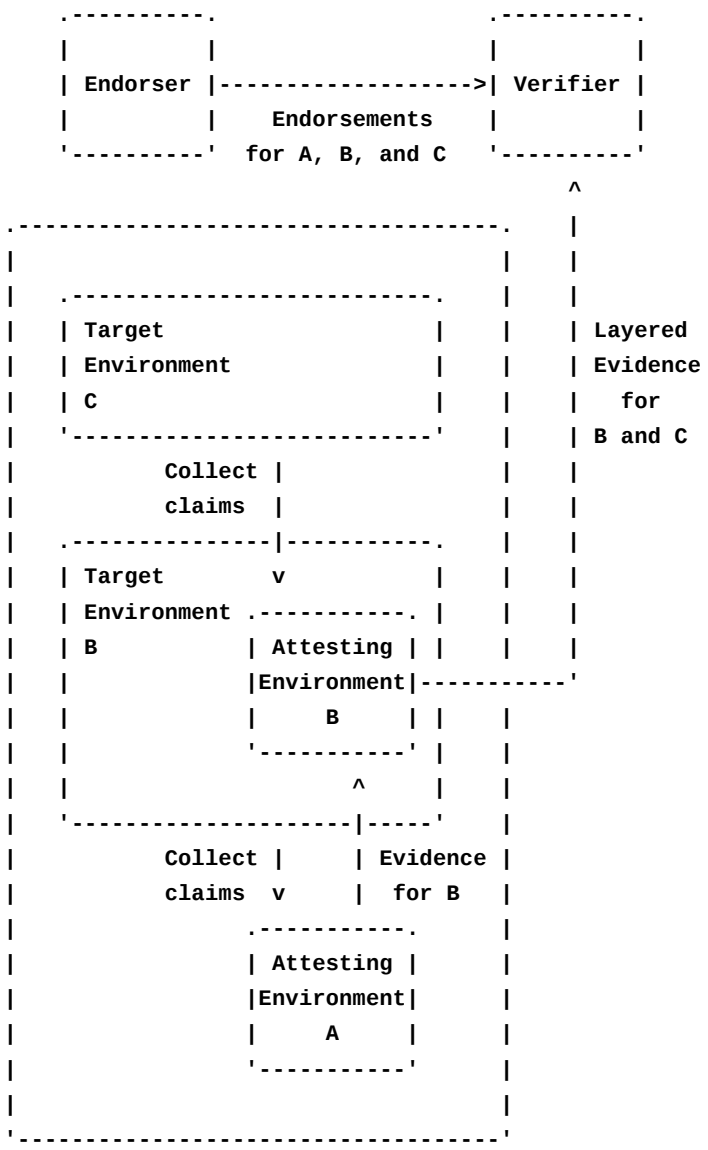
- this is the thing that does the caring

Sometimes contains Attesting Environment



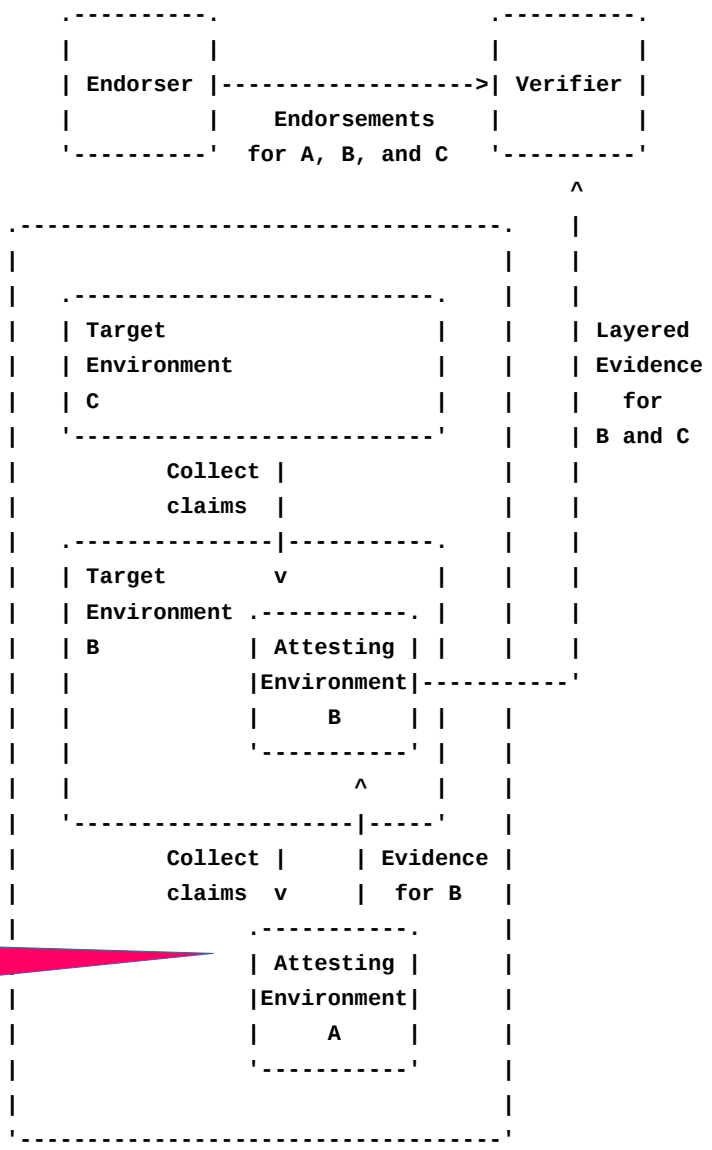
Layered Attestation

- each layer is the Attesting Environment for the next layer
- “trusted boot”



Layered Attestation

- each layer is the Attesting Environment for the next layer
- “trusted boot”



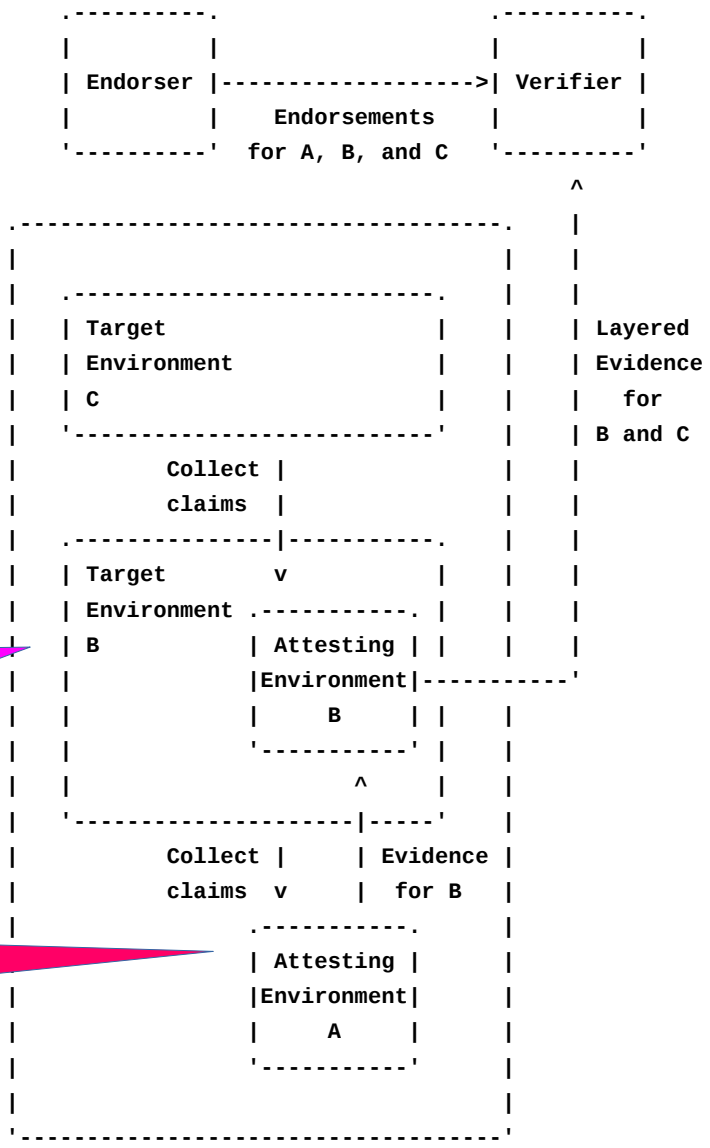
such as the (U)EFI, BIOS, Firmware

Layered Attestation

- each layer is the Attesting Environment for the next layer
- “trusted boo

e.g., Linux, Windows, Android, VxWorks, OpenWSN, Zephyr..

such as the (U)EFI, BIOS, Firmware



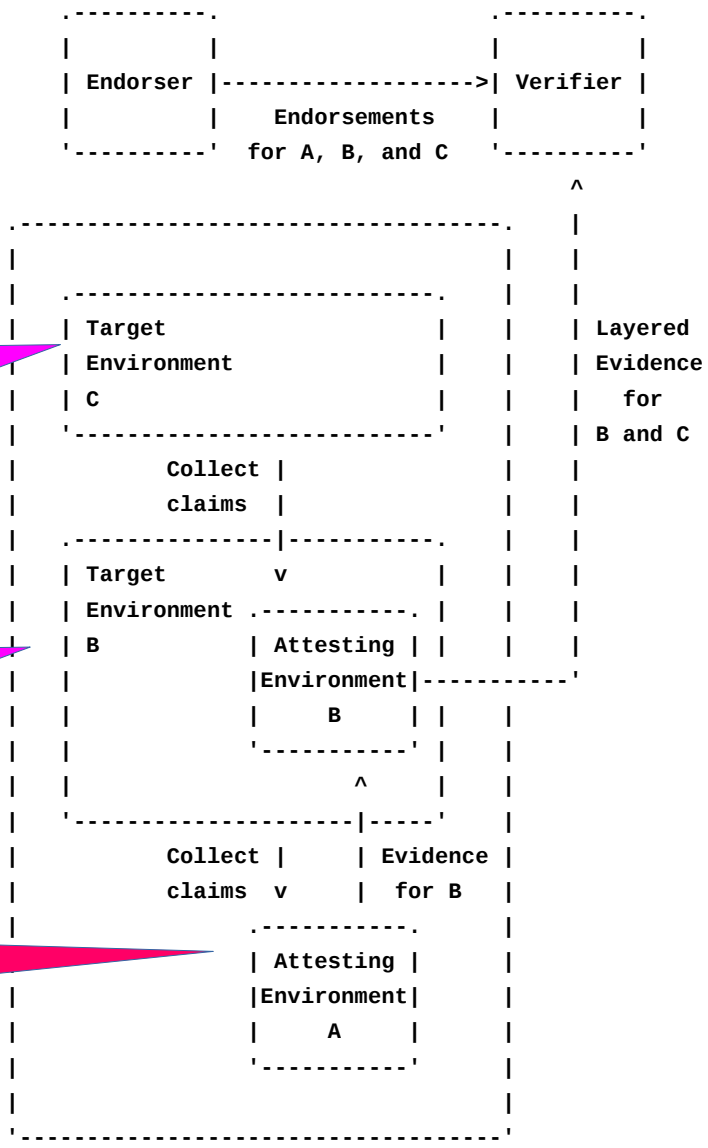
Layered Attestation

- each layer is the Attesting En for the next
- “trusted boo

some target application/configuration or set of processes

e.g., Linux, Windows, Android, VxWorks, OpenWSN, Zephyr..

such as the (U)EFI, BIOS, Firmware



Layered Attestation

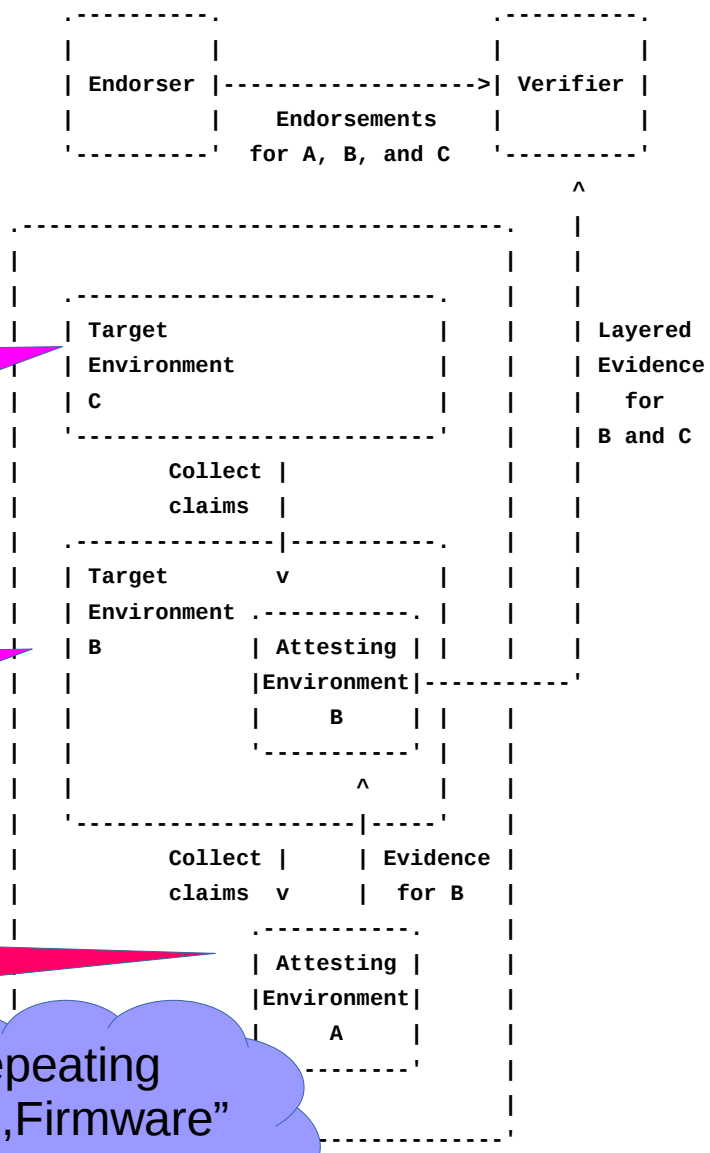
- each layer is the Attesting En for the next
- “trusted boo

some target application/configuration or set of processes

e.g., Linux, Windows, Android, VxWorks, OpenWSN, Zephyr..

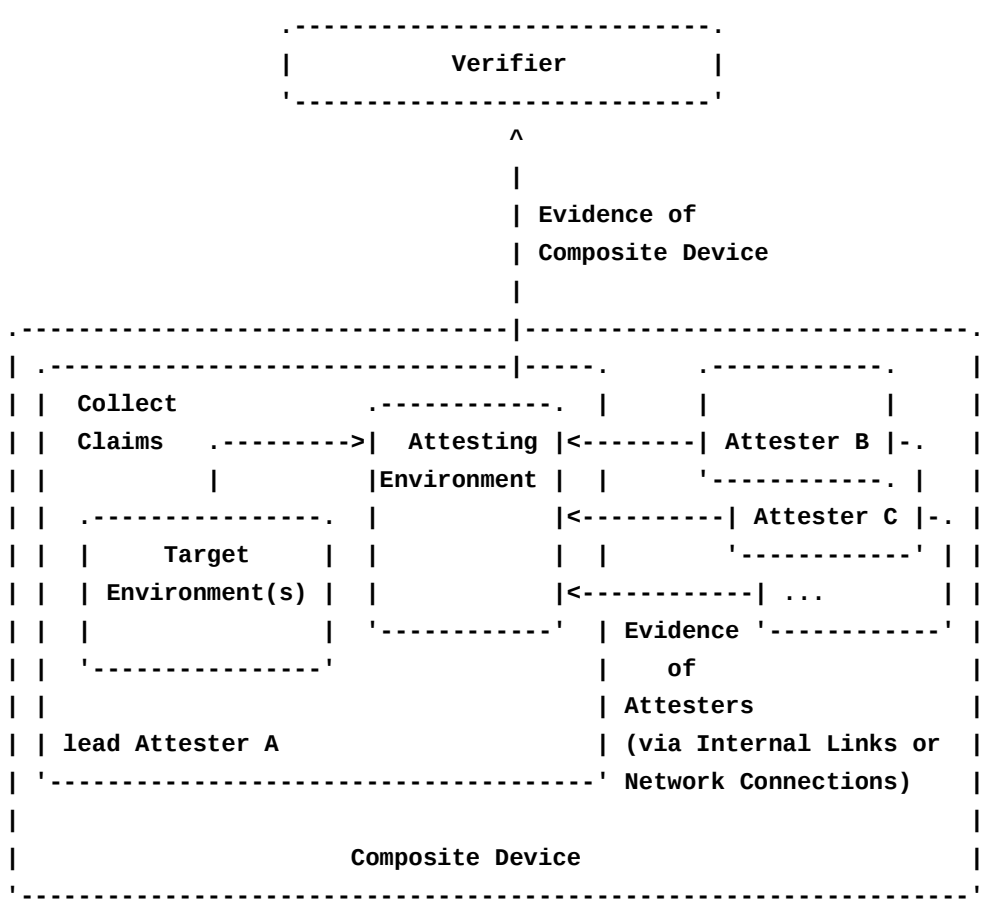
such as the (U)EFI, BIOS, Firmware

We hate repeating “(U)EFI,BIOS,Firmware” please find us a better, but inclusive term

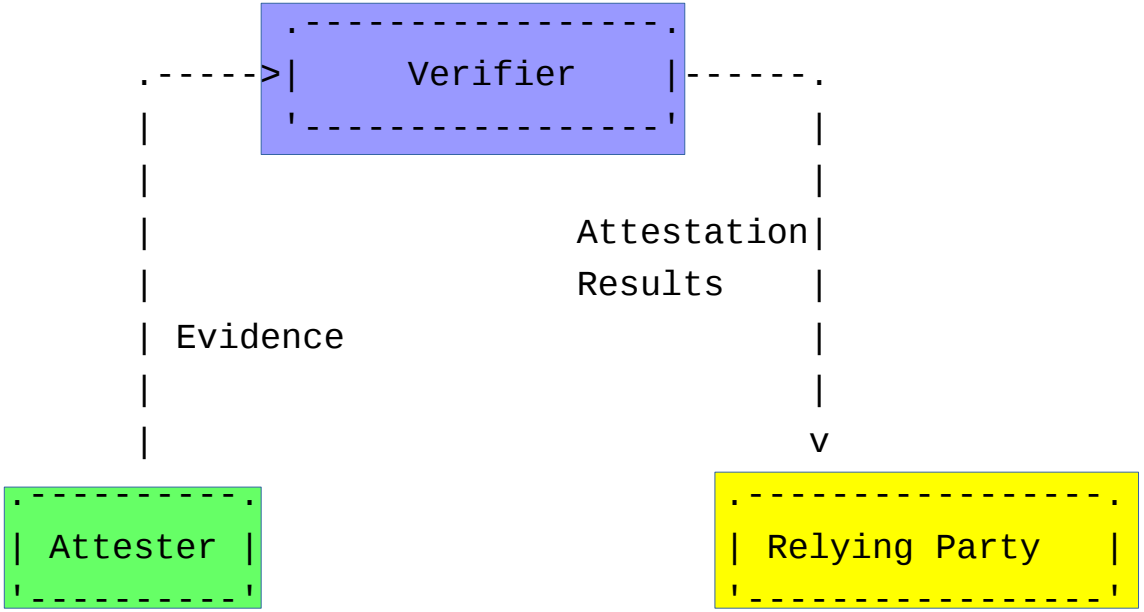


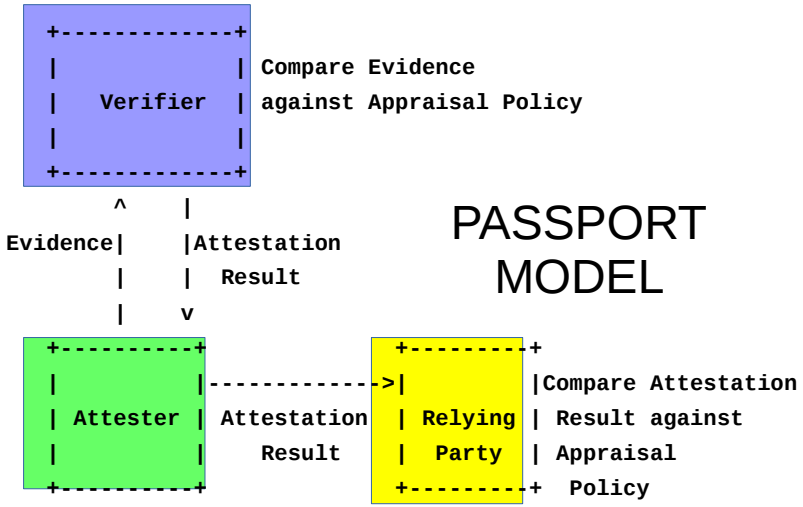
Composite Device

- lead Attester has connection to Verifier
- other components may be:
  - line cards in a chassis
  - aggregates of similar systems
  - Smartphone (main CPU relays evidence from broadband CPU)
  - Devices attached to system bus (each device has firmware)
  - ...



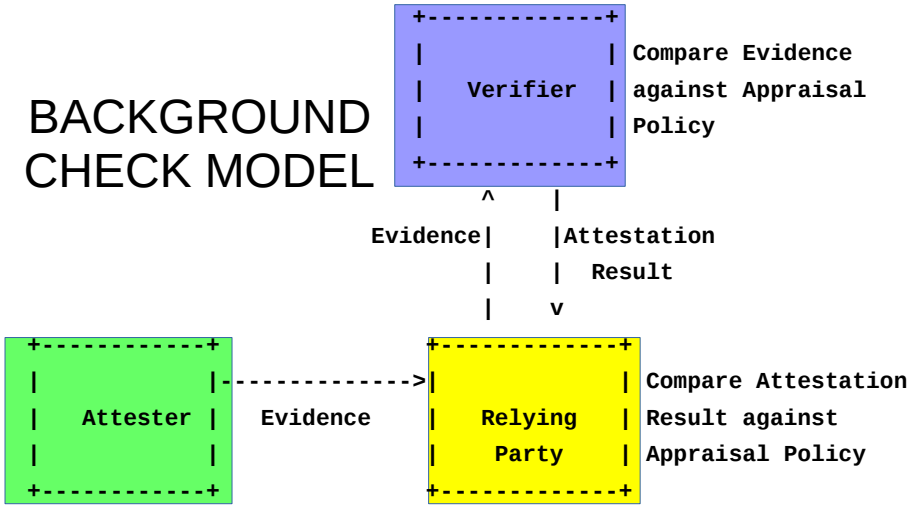
Topology models



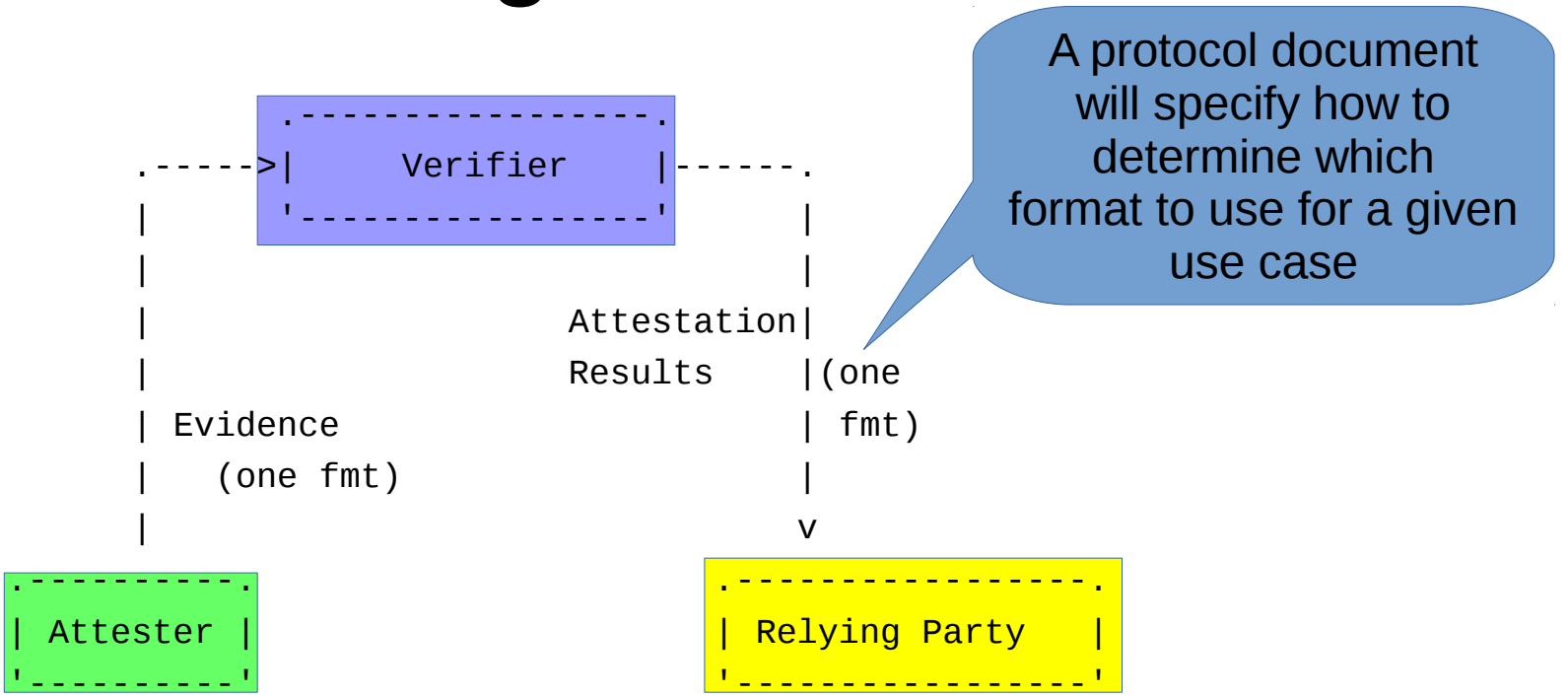


PASSPORT MODEL

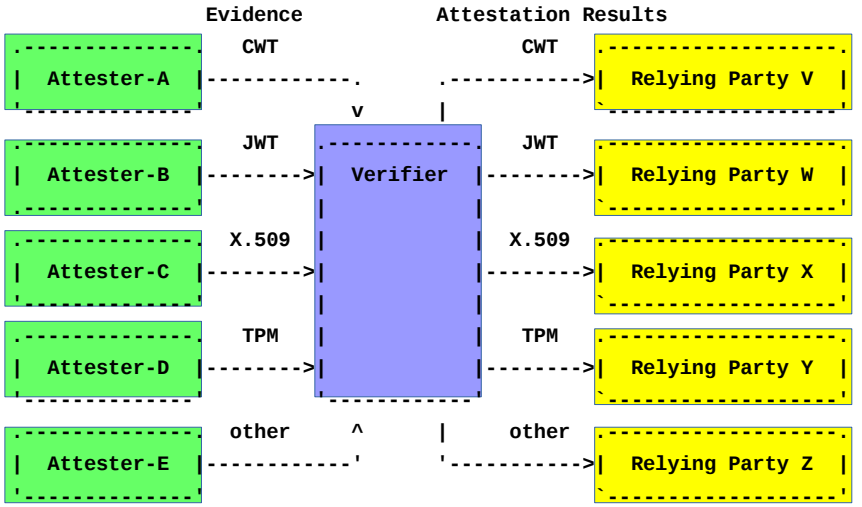
BACKGROUND CHECK MODEL



Encoding Formats



- Attester produces a specific format
- Relying Party demands a specific format
- Either the protocol specifies the format, or it specifies a way to negotiate it dynamically



Here is an example of applying this architecture

- Passport with negotiation

Here is another example of applying this architecture

- Background check, no negotiation