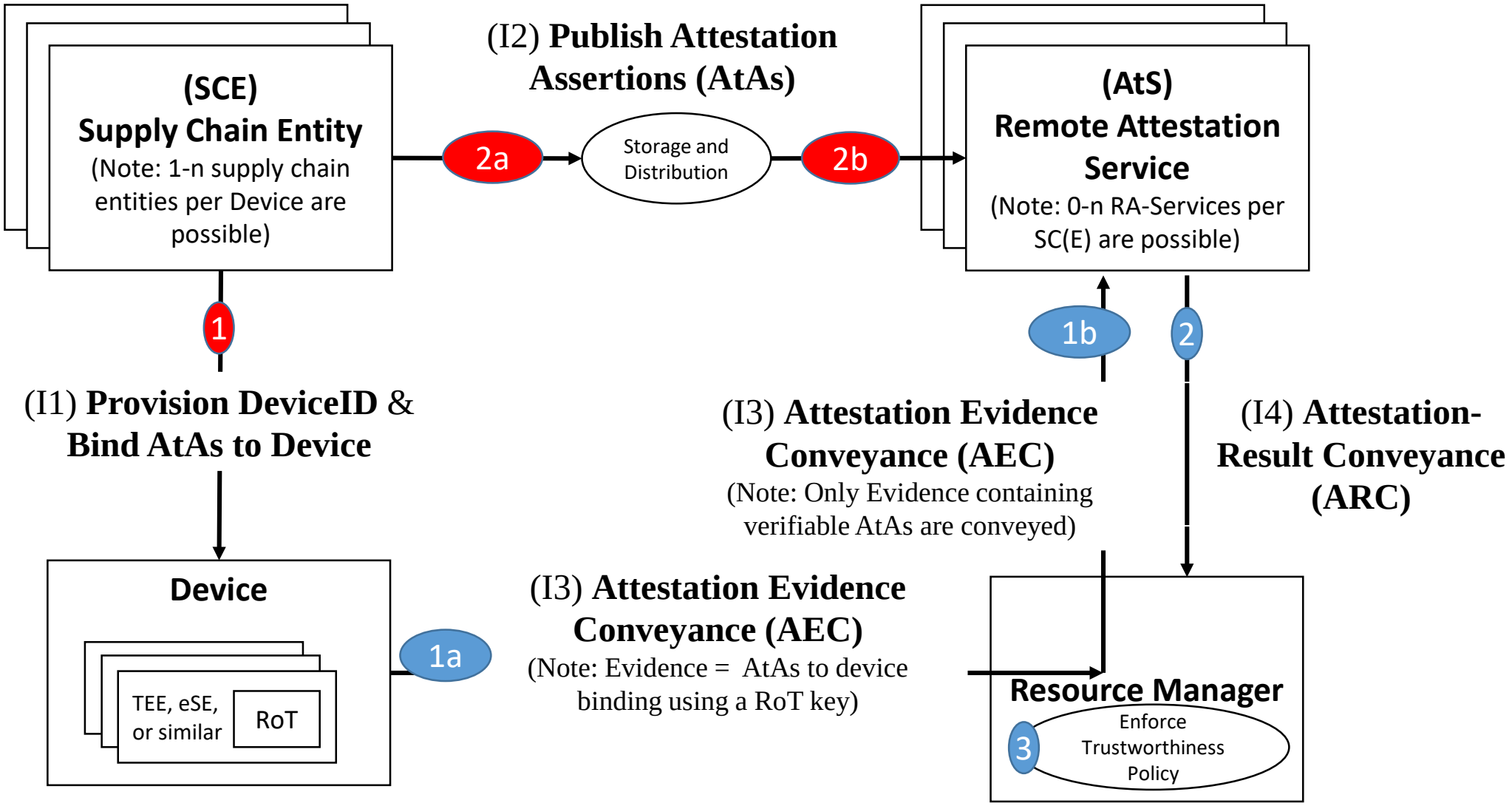
RATS Architecture & Terminology

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}

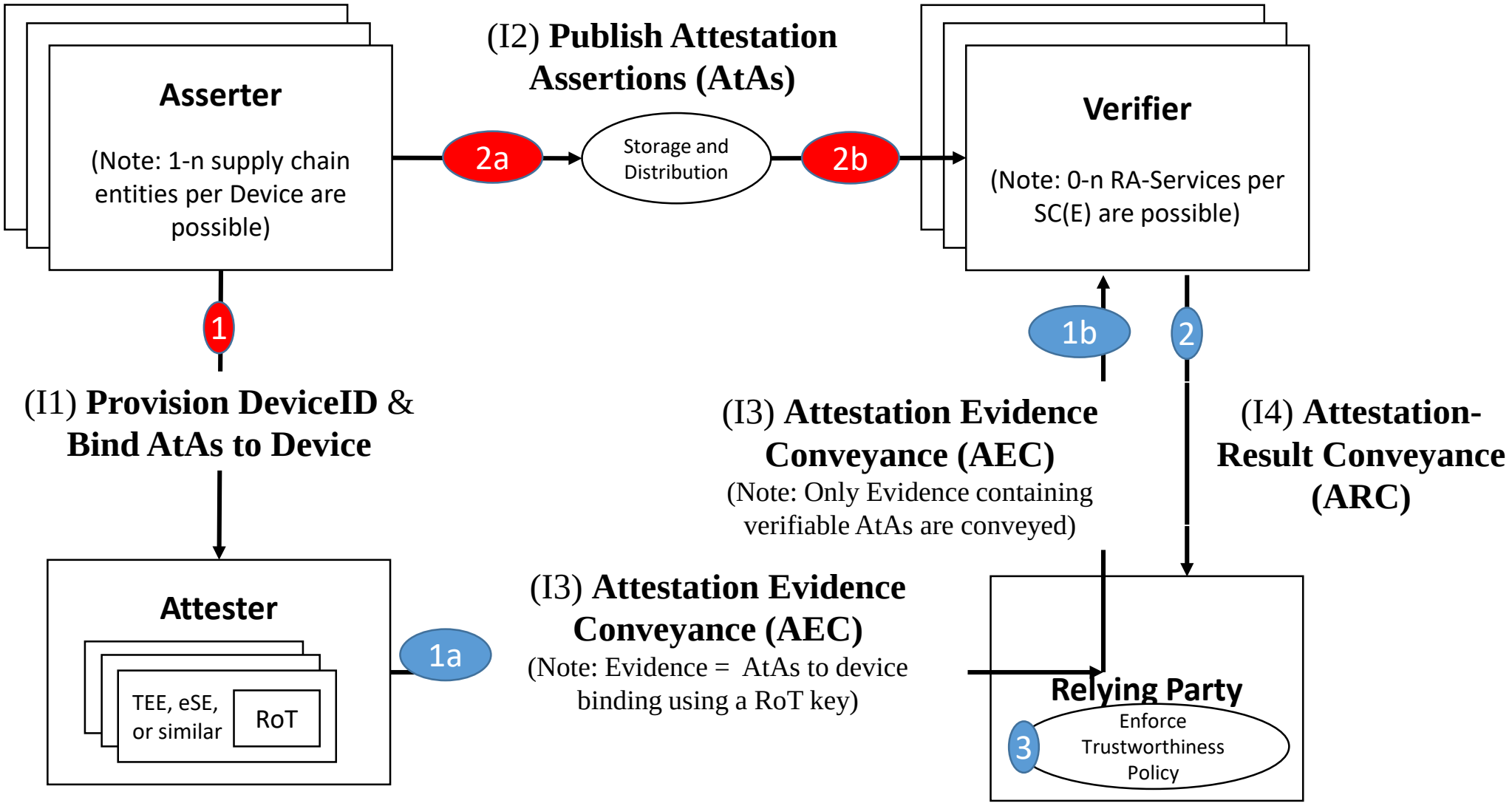
Ned Smith {ned.smith@intel.com}

IETF 105, Montreal, July 25th, RATS WG

RECAP: Current RATS Architecture: **Actors**



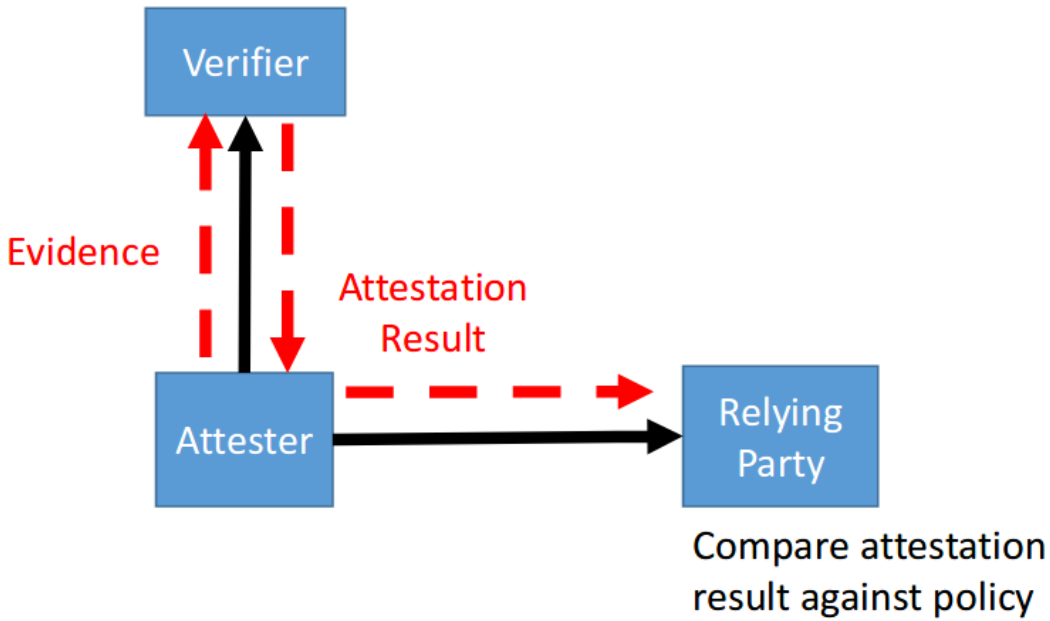
RECAP: Current RATS Architecture: **Roles**



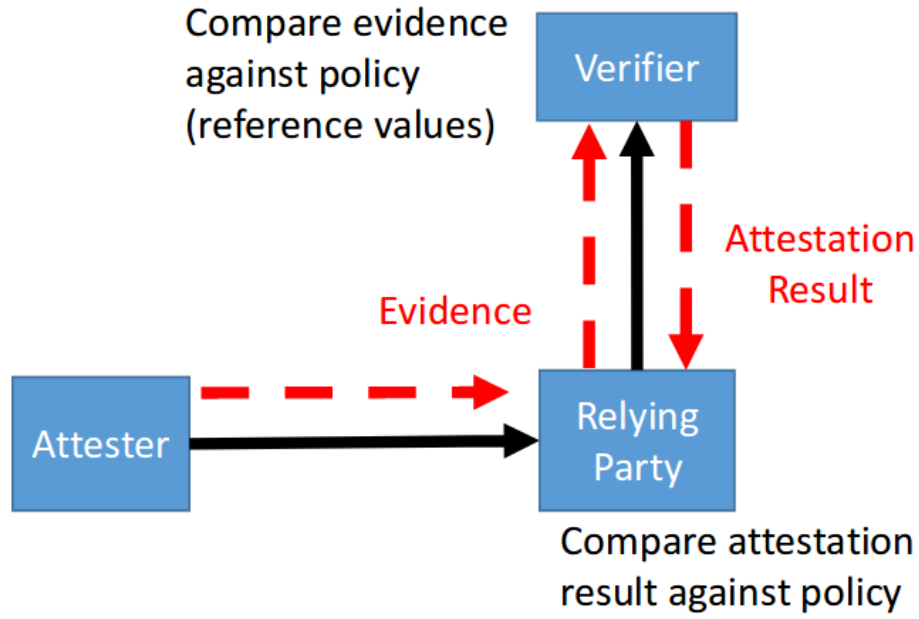
How **TEEP** sees **Rats Roles**

RATS models

"Passport" model:

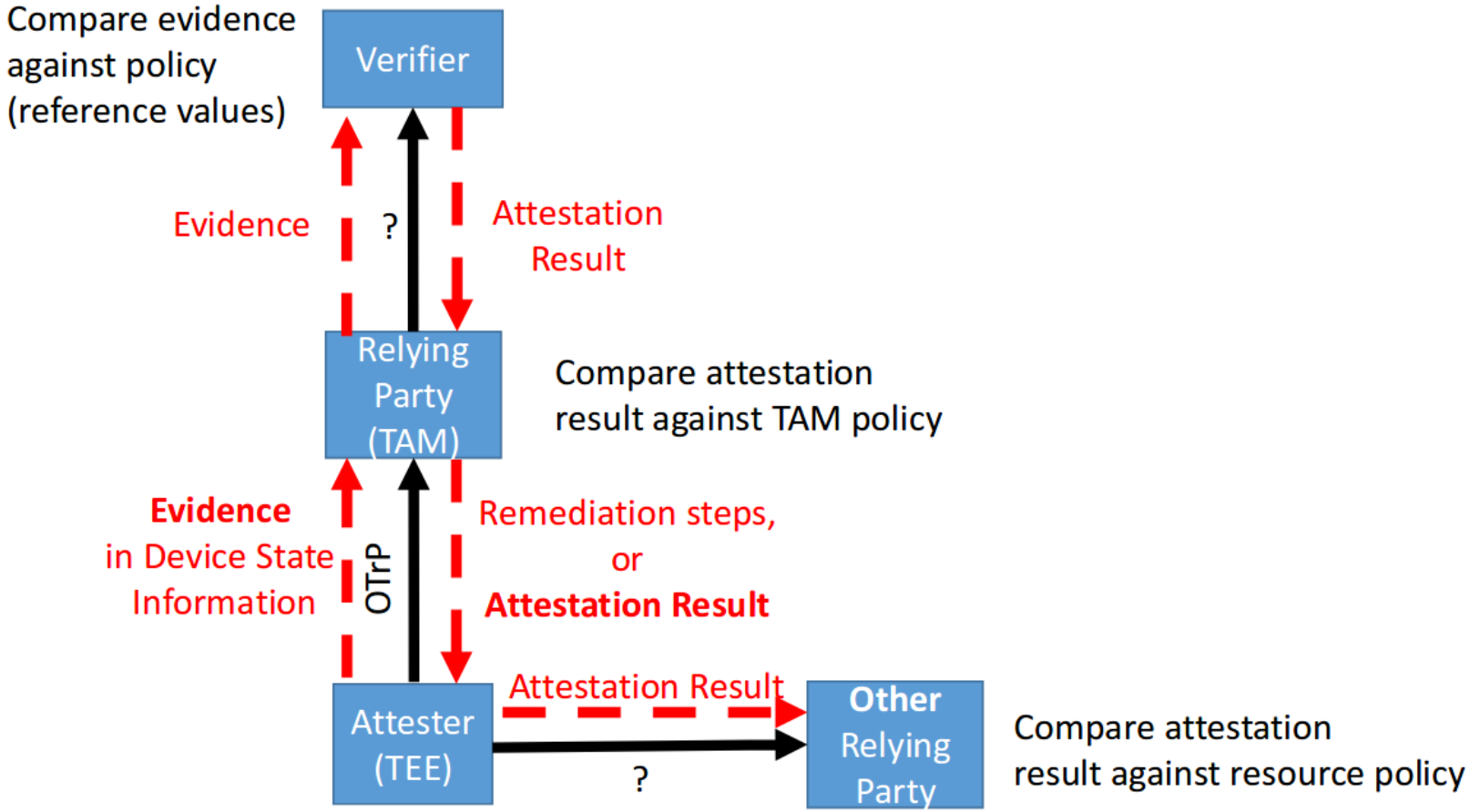


"Background check" model:



One options ow **TEEP** maps to **Rats Roles**

Advanced use of OTrP in “Passport model”



Call for Adoption?

- The TEEP WG was able to map the current architecture to their architecture quite intuitively:
  - https://datatracker.ietf.org/meeting/105/materials/slides-105-teep-sessb-teep-rats-alignment-01
- There where various comments about clarification and expansion to the I-D.

Reference Interaction Model for Challenge-Response-based Remote Attestation Procedures

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}
Michael Eckel {michael.eckel@sit.fraunhofer.de}

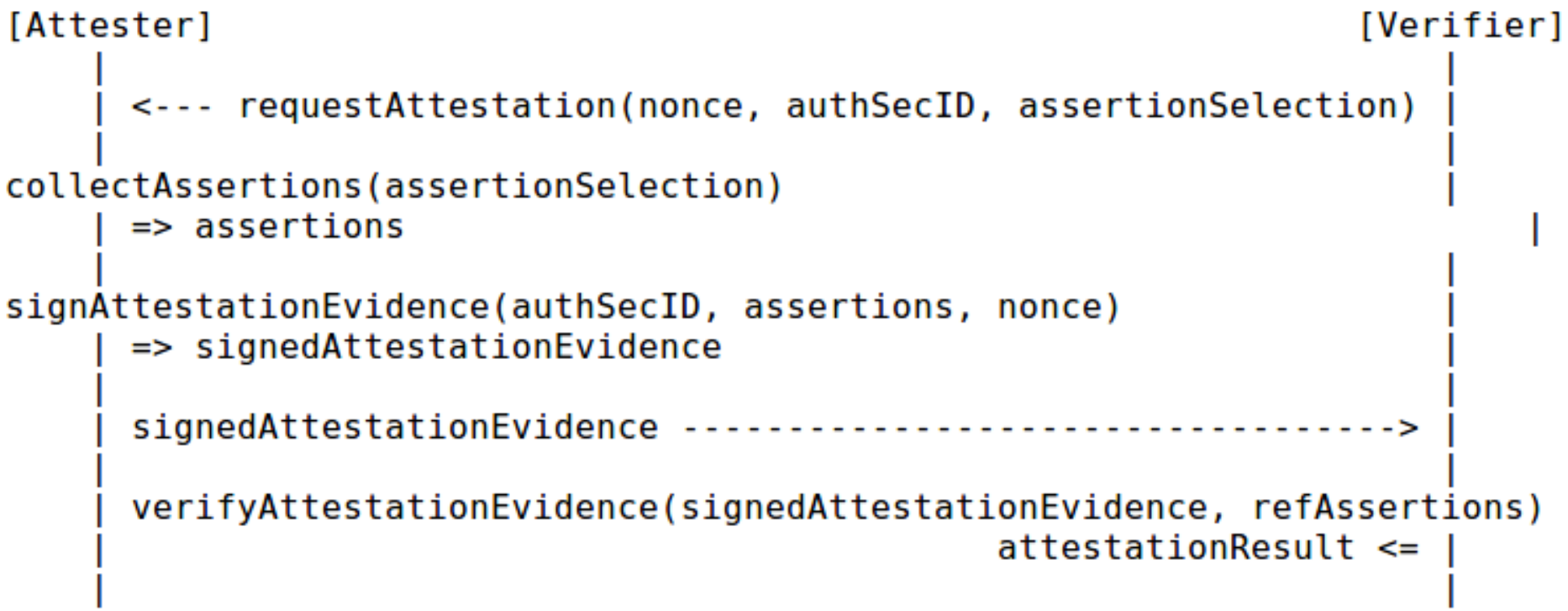
IETF 105, Montreal, July 25th, RATS WG

RECAP: What is the Purpose of this Doc?

- Background
  - Most **protocols** that require a **proof-of-freshness** use a **Challenge/Response**-based based interaction.
  - A **Nonce** that is provided by the challenger, processed cryptographically by the receiver and then returned to the challenger in a way that proofs that the response is a freshly composed set of information.
- Usage
  - This procedure is done at many places and in many protocols **already** 👍
  - This procedure is mostly “re-”explained and illustrated **over and over again** 👎
- Contribution
  - By describing and illustrating this essential concept in an elaborate and use-case agnostic fashion will **prevent “cloning” this normative text** over and over again.
- In consequence, this common basis will reduce the risk of **code-cloning**.

The State of the Document

- Update to the terms used in the Interaction Model



The State of the Document

- There is now Proof-of-Concept code available:
  - Code is monolithic link-able
  - Basically no dependencies, but libcoap and tinycbor
  - POSIX is also not a requirement -> support of implementability in firmware blobs or partitions without an OS
- New Addition: an exemplary CDDL spec for CoAP FETCH Bodies
  - Providing the basis for the PoC implementation
- Current applications:
  - I-D. birkholz-yang-basic-remote-attestation
  - http://github.com/fraunhofersit/charra (BSD clause 3)
- Upcoming features:
  - Adding CoAP block-wise transfer for PoC code

YANG Module for Basic Challenge-Response-based Remote Attestation Procedures

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.de}

IETF 105, Montreal, July 25th, RATS WG

RECAP: What is the Purpose of this Doc?

- Background
  - A lot of **network equipment devices** provide YANG-based management interfaces.
  - A lot of corresponding **agents already exist**.
  - YANG provides an RPC interface that can **implement the Reference Interaction Model**.
- Usage
  - **YANG is widely used and deployed**, especially on network equipment and virtual services.
  - Adding Remote Attestation as procedures to **existing and implemented management interfaces** significantly reduces the threshold of adoption.
- Contribution
  - This YANG module provides an **RPC** implementing the **Reference Interaction Model for Challenge/Response based RATS** (i.e. “nonce-based”).
  - The YANG module also supports multiple **Roots-of-Trust for Reporting** in a **composite device** to create remote attestation evidence about integrity and therefore trustfulness of network equipment (or VNF, respectively). I.e. enabling **trustworthy continuous telemetry.**

The State of the Document

- Current Work
  - Added support for **legacy hardware** (effectively splitting the RPCs into two)
  - Addressed **input from the list** (where possible, a few might still be open)
- Upcoming Features:
  - Some required polish on support structures remains.
  - Adding more English text: e.g. **usage guidance** & work on **Security Considerations**
- Next Steps:
  - Call for Adoption?

RATS Information Model

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}
Michael Eckel {michael.eckel@sit.fraunhofer.de}
Ned Smith {ned.smith@intel.com}

IETF 105, Montreal, July 25th, RATS WG

Food for Discussion (I)

- What is the purpose of an **Information Model** about **Attestation Assertions** (**AtAs** – the generalization of **Web Token Claims**)?
  - **Assertion**: A statement made by an entity **without** accompanying **evidence of its validity** [X.1252]
  - **Claim**: A piece of information **asserted** about a subject. A claim is represented as a name/value pair consisting of a Claim Name and a Claim Value. [RFC7519]
  - "The [**ITU defined**] terms assertion and claim are agreed to be **very similar**." [X.1252]
- **But!** these details on terms here are most "frosting" – there seems to be agreement on the intent und use of **Information Element Definitions**.

Food for Discussion (II)

- Why we need an Information Model is clear:
  Different solutions can convey “attestation information” in various, **data model specific** ways. We have to make sure they are **interoperable** on a semantic level, when two or more **different data models** are used in concert.
- The prominent open question is:
  How and where to put the Information Elements?
  - E.g. https://datatracker.ietf.org/doc/draft-birkholz-rats-information-model/
  - E.g. https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
- More detailed sub-aspects of this open question on the next slide…

Food for Discussion (III)

- **Scope…** when do we know that we have a viable minimal set of information elements?
- **Source…** how & where do we discover differentiable information elements?
- **Structure…** how do we express a {primitive|composite} information element in a document so it is useful for the purpose of enabling interoperability between different solutions?
- **Semantics…** how do we capture the intent and scope of application of the things that are conveyed via Interactions between Roles – without pontificating?
- **Super-Elements…** how do we define a minimal set of categories that an information element fits into? (Taxonomy, Actor-Types, Application-Scope,…?)