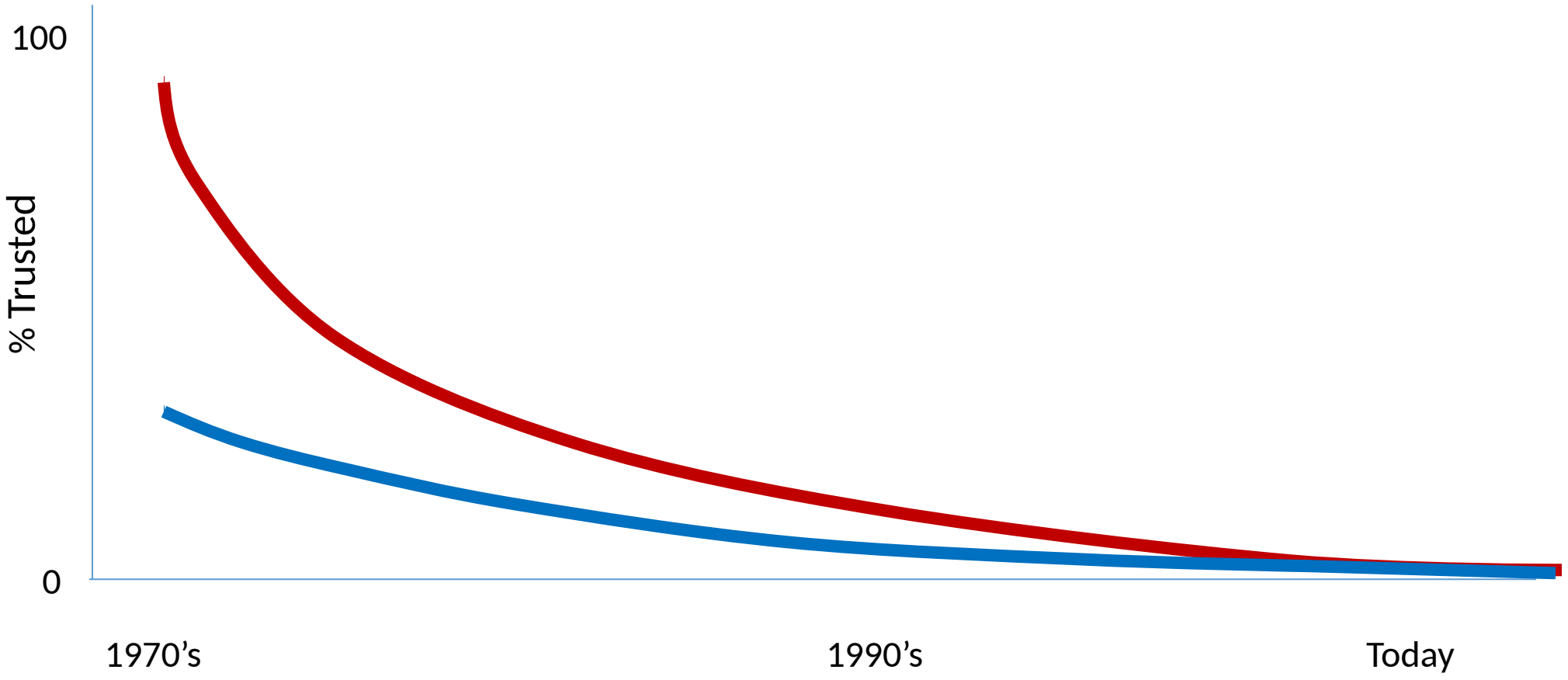
Remote ATtestation ProcedureS (RATS)

IETF 103, November 6, 2018 - Bangkok

Henk Birkholz (henk.birkholz@sit.fraunhofer.de),
Ned Smith (ned.smith@intel.com),
Monty Wiseman (monty.wiseman@ge.com),
Eric Voit (evoit@cisco.com)

Trends in Trust



Problem ⊒ Need

- Problem
  - Desire to understand host characteristics of peers to prevent communications with peers of compromised integrity
  - But the integrity of assertions about host characteristics cannot be assured with software-based approaches alone (e.g. Network Endpoint Assessment)
- Need
  - Assertions about characteristics of peers anchored in hardware roots of trust
  - Means to convey assertions in a timely and secure fashion

Host Characteristics

- Hosts ⊑ System Components [RFC4949]
- Host Characteristics = Assertions [ITU X.1252] that can be signed

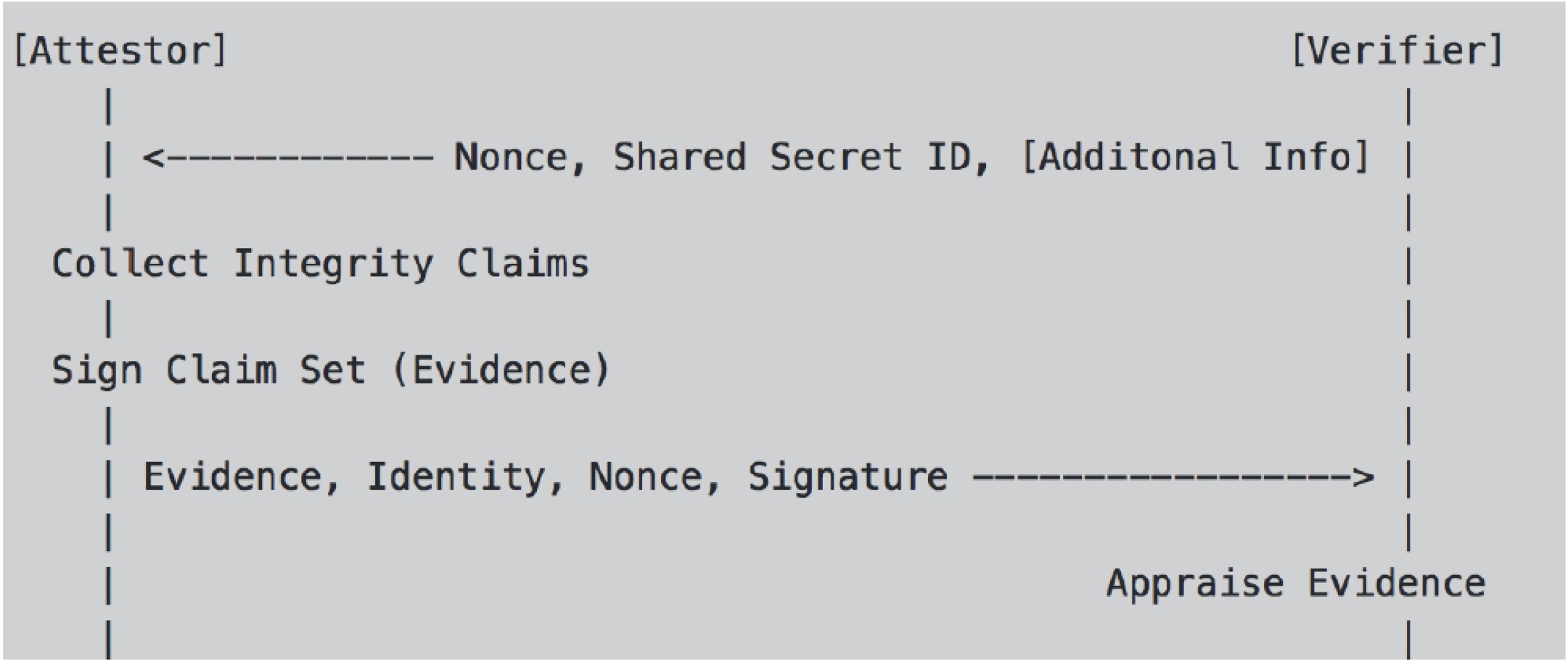
Root of Trust (RoT)

- NIST SP 800-164
  - “Security **primitives** composed of hardware, firmware and/or software that provide a set of trusted, security-critical functions. They must always **behave in an expected manner** because their **misbehavior cannot be detected**. As such, RoTs need to be secured by their design”
- “Trusting” a Root of Trust is a **decision** made by the relying party.

Conveyance of Assertions

- **Network Protocols** have to address requirements for secure conveyance of assertions
- **Message Formats** (e.g. data models) have to address requirements for secure conveyance of assertions
- Definition of the demarcation line is part of the work
- Some requirements:
  - Freshness
  - Integrity
  - Confidentiality
  - Privacy

The General Model for Remote Attestation
(in ASCII Art)



Proposed Remote Attestation Model