TRUSTED® COMPUTING GROUP

TCG Attestation Framework

and

IETF Remote Attestation Procedures

An Overview of TCG and IETF Attestation Working Groups

Presenter: Ned Smith – Intel Corp.

TRUSTED® COMPUTING GROUP

Attestation Use Cases

Authentication

Trustworthiness

Integrity & Posture Assurance

Origin Provenance

Interoperability is Essential

TRUSTED® COMPUTING GROUP

What is Attestation?

NIST defines attestation two ways:

Definition 1:

> "The process of providing a digital signature for a set of measurements securely stored in hardware, and then having the requester validate the signature and the set of measurements."

Definition 2:

> "The issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated."

Note: Definition 2 is typically associated with origin provenance e.g.: SW Bill of Materials (SBOM).

TRUSTED® COMPUTING GROUP

TCG Attestation WG Focus

- Define attestation terminology, concepts, requirements, and deployment patterns
- Deliverables:
  - TCG Attestation Framework Part 1
    - Terminology, Concepts, and Requirements
  - TCG Attestation Framework Part 2
    - Deployment Patterns

TCG Attestation Framework Goals

- Encourage other TCG work groups to use attestation terms consistently
- Expand the attestation concepts to include evolving trusted computing technology
  - TPM, DICE, MARS, others...
- Provide greater industry awareness of attestation related technology

TRUSTED® COMPUTING GROUP

Multiple Industry Groups Actively Define Attestation Technology

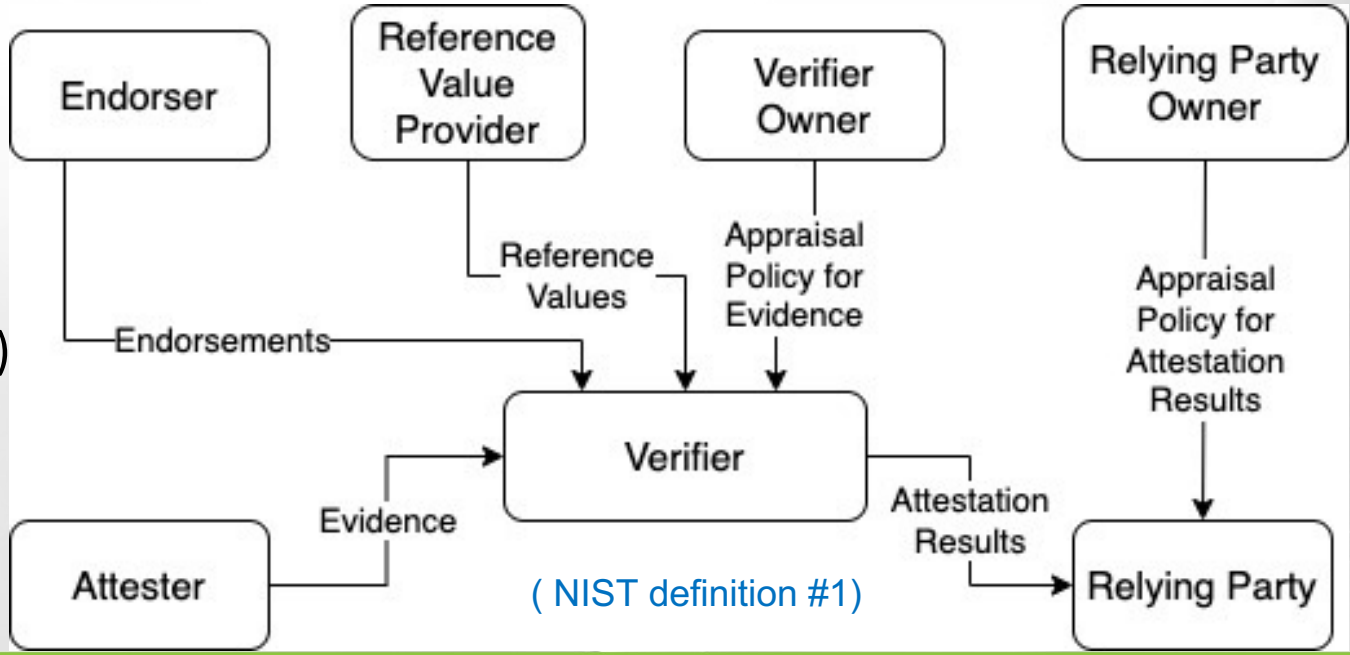
- Internet Engineering Task Force (IETF)
- Distributed Management Task Force (DMTF)
- Open Compute Project (OCP)
- Open-Source Security Foundation (OpenSSF)
- Etc...

TRUSTED® COMPUTING GROUP

Framework Overview

- Remote attestation as a *workflow* model

- Roles & Role Messages
- Messages flow from one role to another
- Flow terminates at the Relying Party(RP)
- The RP performs actions that are informed by Attestation results



TRUSTED® COMPUTING GROUP

Verifier Objectives

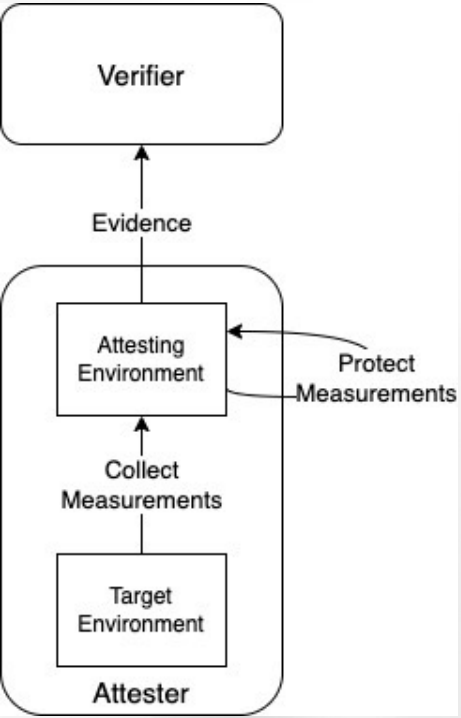
- Collect & evaluate inputs and produce a result that describes Attester's trust attributes
- Reference Values (golden measurements) will match Evidence (actual values) from Attester
- Apply appraisal policies that simplify posture, such as *trusted* or *not-trusted;* or expose specific attributes that are most relevant to Relying Parties

TRUSTED® COMPUTING GROUP

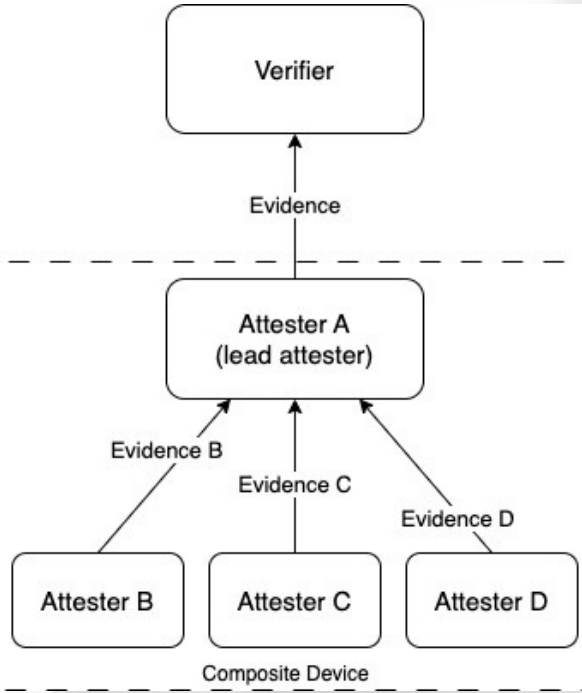
Attester Composition

- Attestation needs to describe the internal makeup of the Attester device.
  - A.k.a., “Turtles all the way down”
- The Framework defines terminology for describing various attestable components called Target Environments (TE).
- TEs are anything that can be attested (i.e., “measured”).
- Attesting Environments (AE) are anything that can collect measurements from TEs and report them to a Verifier.
- AE can also be TEs.
- The bottom AE typically is a Root-of-Trust.
  - E.g., TPM, DICE, DPE, MARS, etc...

Example Device Composition

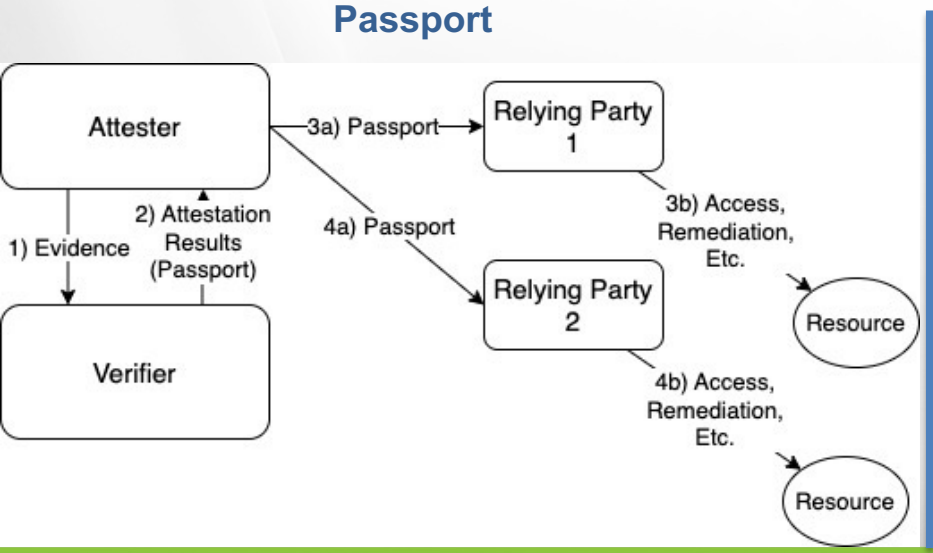


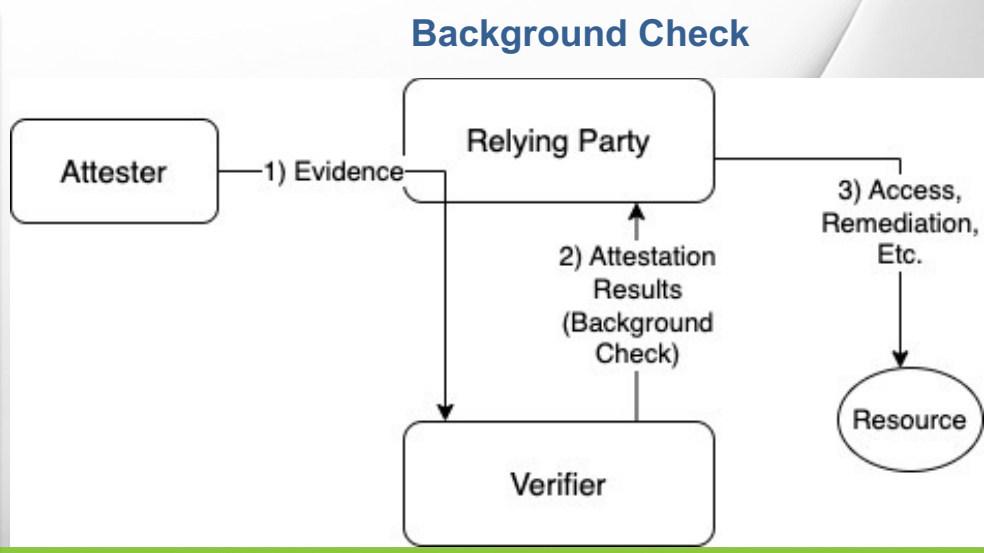
- Attesters may be composed of multiple environments
- ‘Attester’ is a role, hence a device may have multiple Attesters
- Device composition can involve multiple ”devices” – e.g., CPUs, storage, accelerators,...



Deployment Patterns

- Roles may be implemented by nodes that don't have direct connections to an intended recipient.
- Deployment patterns describe common cases where Role Messages may be redirected based on connectivity limitations

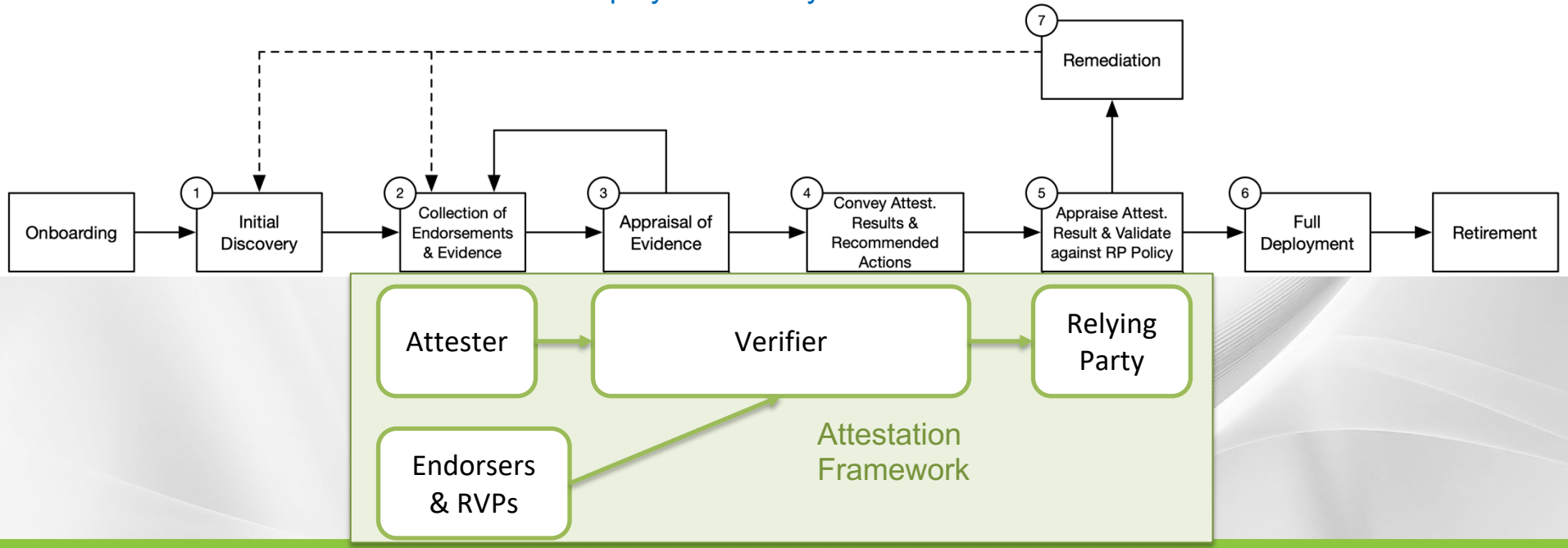




TRUSTED® COMPUTING GROUP

Attestation Framework Aligns with IWG Architecture

IWG Device Deployment Lifecycle Model with Attestation



TCG has Several Attestation Specs

- Infrastructure WG
  - TCG Reference Integrity Manifest Information Model
  - TCG Trusted Attestation Protocol (TAP) Use Cases
  - TCG Trusted Attestation Protocol (TAP) Information Model
  - Canonical Event Log Format
  - TPM 2.0 Keys for Device Identity and Attestation
- DICE WG
  - DICE Attestation Architecture
  - DICE Layering Architecture
  - DICE Concise Evidence Binding for SPDM
  - Symmetric Identity Based Device Attestation
  - Hardware Requirements for a Device Identifier Composition Engine
  - Implicit Identity Based Device Attestation
  - DICE Endorsement Architecture
- PC Client
  - TCG PC Client Platform Firmware Integrity Measurement
- MARS WG
  - Measurement and Attestation RootS Serialization Interface Specification
- Network Equipment
  - TCG SNMP MIB for TPM-Based Attestation
- Etc...

TRUSTED® COMPUTING GROUP

TCG Attestation Framework is Aligned with IETF

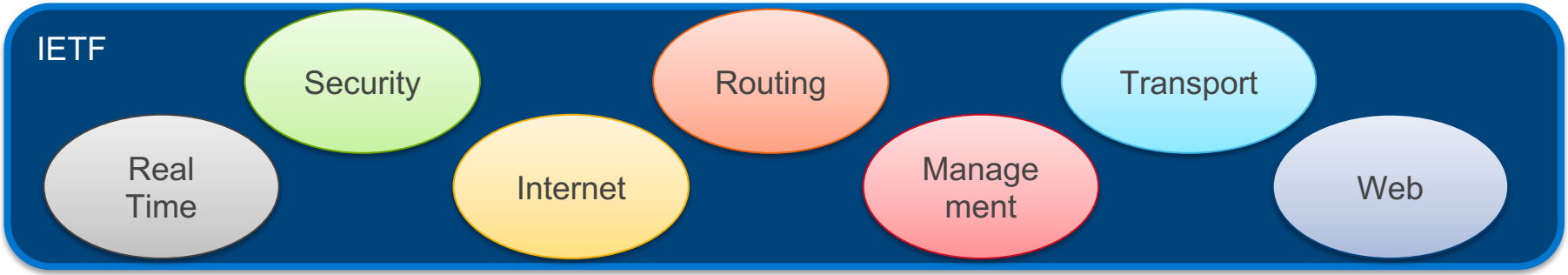
- TCG Framework is aligned with IETF RFC9334.
- The IETF Remote Attestation Procedures (RATS) working group has several attestation specifications under development.
- Other IETF working groups are incorporating attestation into their specifications.

IETF Mission

Make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

The IETF is a Standards Setting Organization

It is divided into several “Areas”:



- Building-block attestation standards are defined by the Remote Attestation Procedures (RATS) working group.

RATS specifications target four main areas:

- Architecture
- Protocols
- Data Structures
- Miscellaneous

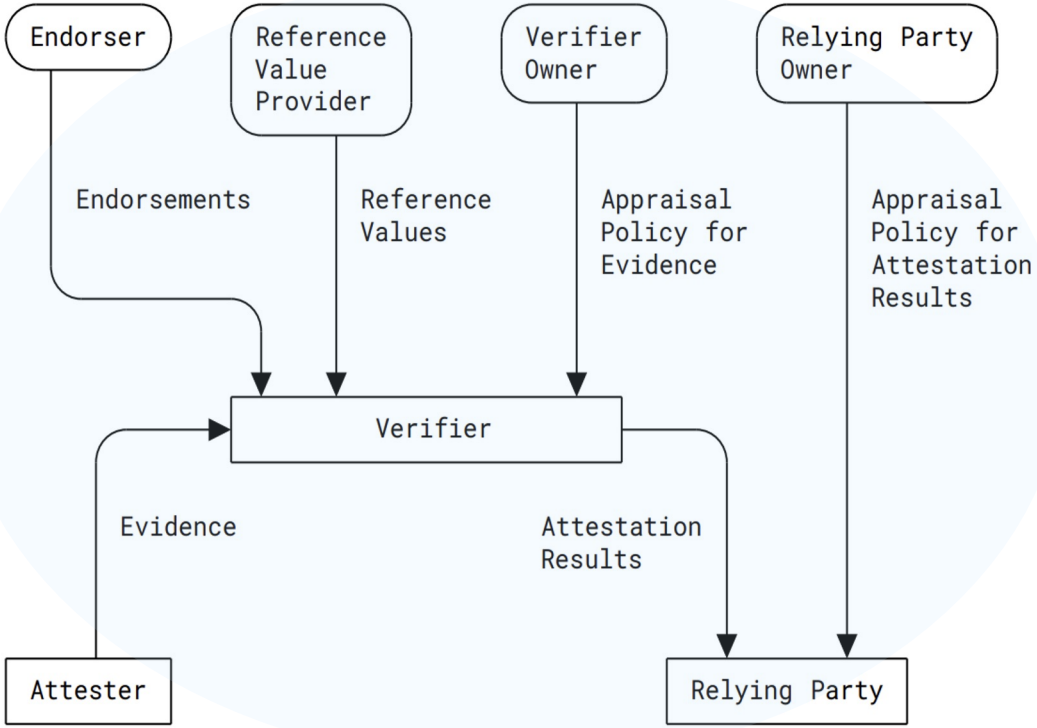
- Other IETF working groups incorporate attestation into their standards.

IETF Remote ATestation procedureS (RATS)

RATS Architecture is published as RFC9334

RATS Architecture:

- Roles
  - Attester
  - Verifier
  - Relying Party
  - Endorser
  - Reference Value Provider
  - Verifier Owner
  - Relying Party Owner
- Conceptual Messages
  - Evidence
  - Attestation Results
  - Endorsement
  - Reference Values



(NIST definition #1)

RATS Working Group Link: https://datatracker.ietf.org/wg/rats/about/

Attestation Claims for IETF Tokens

“Claims” are the payload of a Token

Entity Attestation Token (EAT)

- Defines attestation claims for **JOSE Web Token (JWT)** or **CBOR Web Token (CWT)**
- Also supports token and submodule nesting
- Detached signatures
- Current Status: *IESG Reviewing prior to publication as an RFC*

Example EAT Token (in CBOR Diagnostic format)

```
{
     / nonce (cti) /            7:h'948f8860d13a463e8e',
     / UEID /                   8:h'0198f50a4ff6c05861c8860d13a638ea4fe2f',
     / boot_state /            12:{true, true, true, true, false}
     / time stamp (iat) /       6:1526542894,
}
```

Only the COSE payload is shown.

This slide originally appeared in Orange Workshops: Attestation and it’s Applications, Nov 13-14, 2023

Active RATS Working Group Documents

Architectural

- RATS Endorsements draft-ietf-rats-endorsements/
- Reference Interaction Models draft-ietf-rats-reference-interaction-models/
- Direct Anonymous Attestation for the RATS Architecture draft-ietf-rats-daa/

Data Definition

- EAT Media Types draft-ietf-rats-eat-media-type/
- Concise Reference Integrity Manifest draft-ietf-rats-corim/
- Conceptual Message wrapper draft-ietf-rats-msg-wrap
- A CBOR Tag for Unprotected CWT Claims Sets draft-ietf-rats-uccs/
- Attestation Event Stream Subscription draft-ietf-rats-network-device-subscription/
- Attestation Results for Secure Interactions draft-ietf-rats-ar4si/
- Concise TA Stores (CoTS) draft-ietf-rats-concise-ta-stores/

Active RATS Working Group Documents Cont.

Profiles

- ARM PSA Verifier draft-fdb-rats-psa-endorsements/
- ARM PSA Token draft-tschofenig-rats-psa-token-20/
- Intel CoRIM Profile draft-cds-rats-intel-corim-profile/
- Intel TDX Attestation Results Profile draft-kdyxy-rats-tdx-eat-profile/

Misc.

- TPM-based Network Device Remote Integrity Verification draft-ietf-rats-tpm-based-network-device-attest/

Additional drafts under consideration for adoption

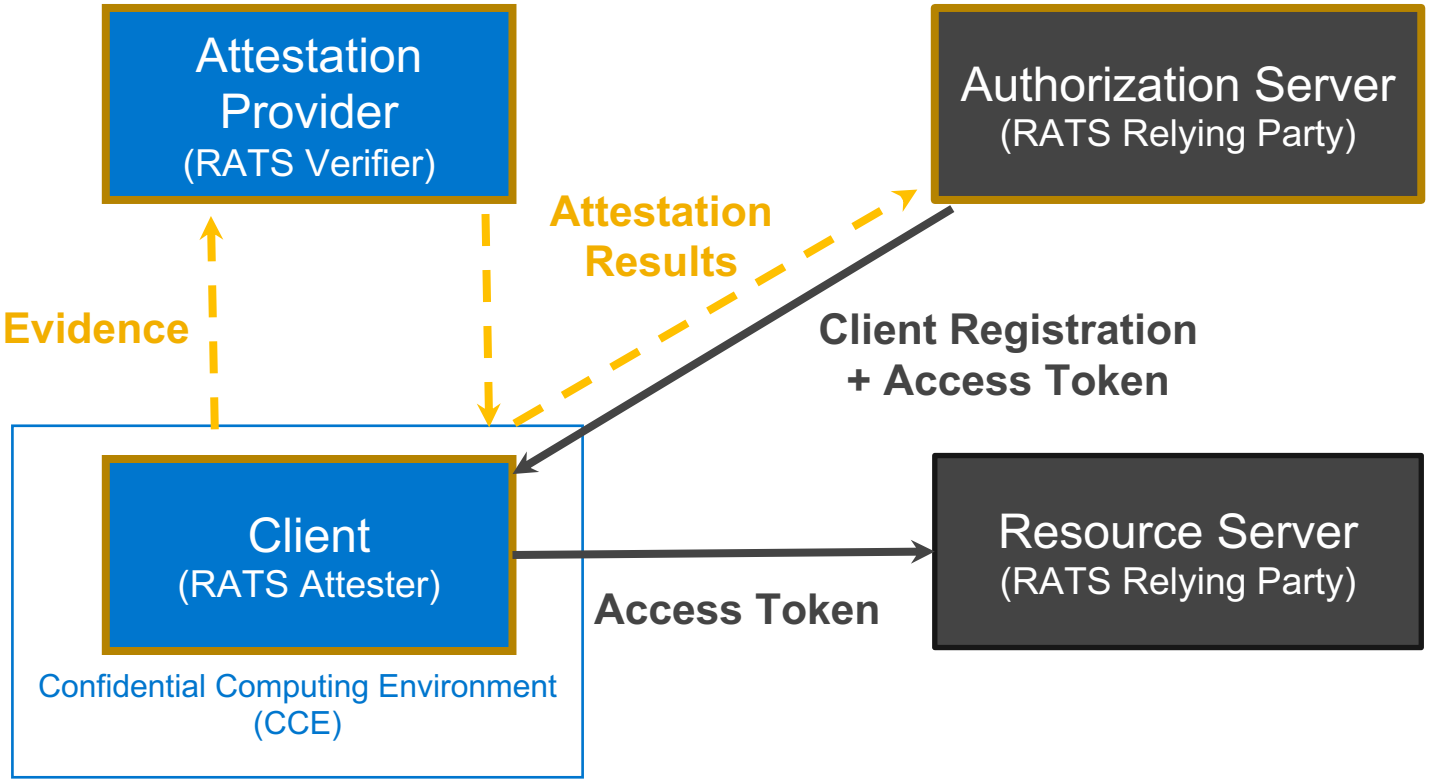
- Trusted path routing draft-voit-rats-trustworthy-path-routing/
- X.509-based Evidence draft-ounsworth-rats-x509-evidence/
- EAT Attestation Results draft-fv-rats-ear/

Other IETF Working Groups are Incorporating RATS Technology

- OAuth Working Group
  - Adding attestation to web authorization protocols
- TLS Working Group
  - Attested TLS
- Limited Additional Mechanisms for PKIX and SMIME (LAMPS)
  - Adding attestation to certificate signing request (CSR) protocols
- Trusted Execution Environment Protocols (TEEP)
  - Adding attestation to TEE management protocols
- Privacy Pass Architecture
  - Focuses on attestation that preserves privacy on the web

Example: OAuth2 Client Registration

Ref: draft-tschofenig-oauth-attested-dclient-reg/



Access Token might not be issued if Attestation Results are not as expected

Resource access might not be granted if the Token's trust properties are not as expected

Passport Model overlay

Links to IETF Working Groups

Other Relevant IETF Working Groups

- Transport Layer Security (TLS)
  - https://datatracker.ietf.org/group/tls/about/
- Trusted Execution Environment Provisioning (TEEP)
  - https://datatracker.ietf.org/wg/teep/about/
- Software Update For Internet of Things (SUIT)
  - https://datatracker.ietf.org/wg/suit/about/
  - Manifest format defined in SUIT used in TEEP
- Limited Additional Mechanisms for PKIX and SMIME (LAMPS)
  - https://datatracker.ietf.org/wg/lamps/about/
- Web Authorization Protocol (OAuth)
  - https://datatracker.ietf.org/wg/oauth/about/
- Privacy Pass
  - https://datatracker.ietf.org/wg/privacypass/about/

Internet Drafts (I-D) benefit from additional review and collaboration to solve problems in scope.

Mailing list information is on each WG page (join or view archive).

Overview of Attestation Specs

TRUSTED COMPUTING GROUP

Framework 1 & 2

TAP Use Cases

IWG Architecture

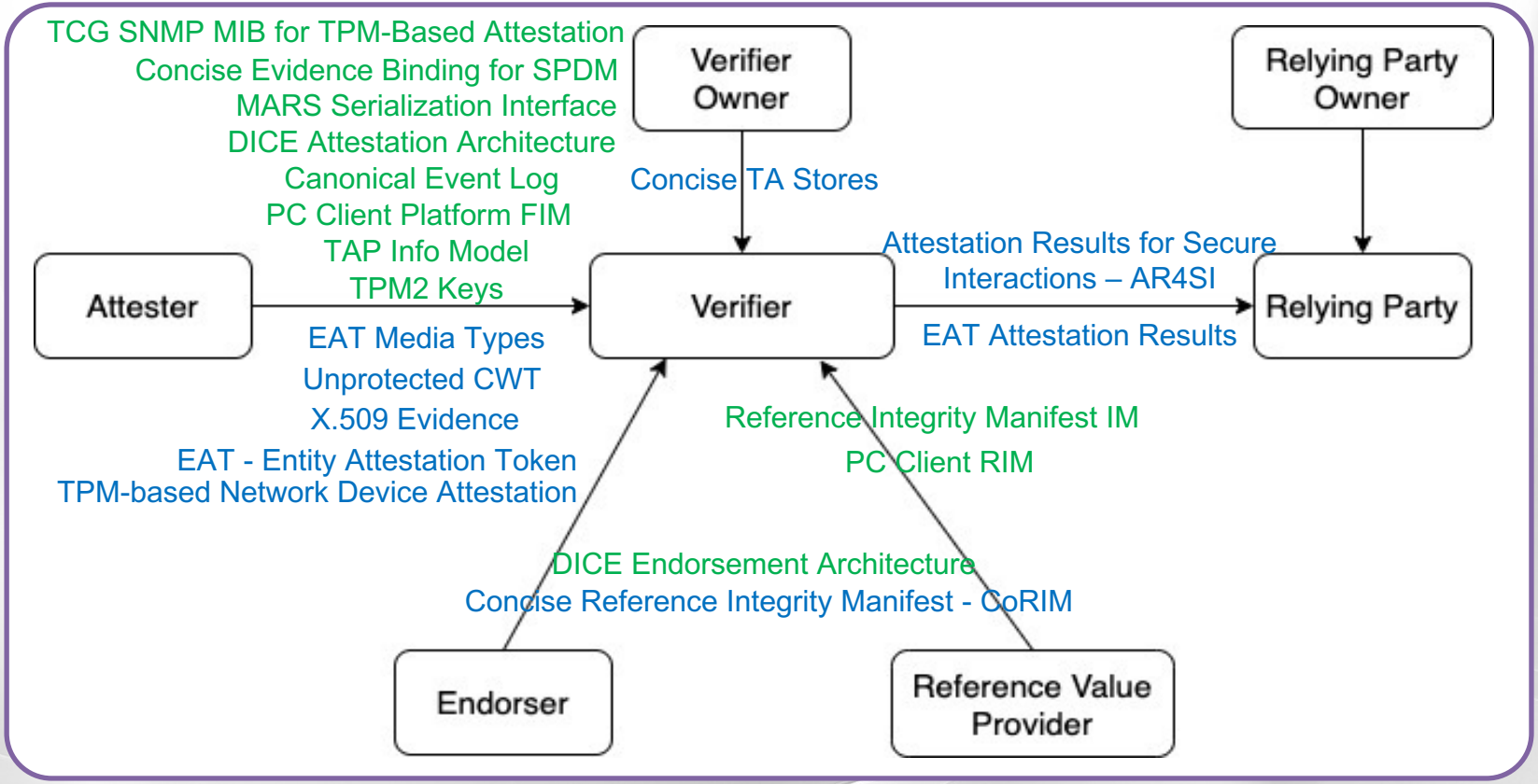
RFC9334

Reference Interactions

DAA for RATS Architecture

Conceptual Message Wrapper

Network Device Subscription



TCG*

IETF*

*not an exhaustive list

TRUSTED® COMPUTING GROUP

Thank You!

Contact Info: ned.smith@intel.com

TRUSTED® COMPUTING GROUP

Abstract

Trust and attestation are gaining in popularity and importance for cloud, edge, and distributed computing. Attestation capabilities in the platform as well as attestation services in the cloud, edge, and IT enterprise need to interoperate to minimize costs and maximize reach. Many standards are actively defining attestation technologies, but interoperability isn’t guaranteed. This talk provides an overview of work in the TCG Attestation and IETF Remote Attestation Procedures (RATS) working groups.