Introduction

Relying parties require evidence about the trustworthiness of remote system components [RFC4949] they interact with. Remote attestation procedures (RATS) enable relying parties to establish a level of confidence in the trustworthiness of remote system components by creating and processing attestation evidence. A relying party can then decide whether to consider a remote system component trustworthy or not.

To improve the confidence in a system component's trustworthiness a relying party may require evidence about:

- system component identity,
- composition of system components, including nested components,
- roots of trust,
- assertion/claim origination or provenance,
- manufacturing origin,
- system component integrity,
- system component configuration, or
- operational state and measurements of steps which led to the operational state.

While domain-specific attestation mechanisms such as Trusted Computing Group (TCG) Trusted Platform Module (TPM)/Trusted Software Stack (TSS), Fast Identity Online (FIDO) Alliance attestation and Android Keystore attestation exist, there is no interoperable way to create and process attestation evidence to make determinations about system components among relying parties of different manufactures and origins.

Goals

This WG will standardize formats for describing assertions/claims about system components and associated evidence; and procedures and protocols to convey these assertions/claims tothe relying parties. While a relying party may use reference values to assess the assertions/claims the procedures for this activity are out of scope for this WG.

The working group will cooperate and coordinate with other IETF WG such as TEEP, SUIT and SACM as appropriate. The WG will also evaluate prior work such as NEA and proprietary attestation technologies.

Program of Work

The working group will develop standards supporting interoperable remote attestation procedures for system components. The main deliverables are as follows.

1. Specify a terminology, architecture and use cases that enable explicit (a set of verifiable assertion/claims is transported in the attestation) and implicit (a set of assertions/claims is implied by possession of a secret) attestation techniques. The architecture may include a system security model for the signing key material and involve at least the system component, system component provider, and the relying authority.

2. Standardize an information model for assertions/claims which provide information about system components characteristics scoped by the specified use-cases.

3. Standardize data models that implements and secures the defined information model (e.g., CBOR Web Token structures [RFC8392], JSON Web Token structures [RFC7519]).

4. Standardize interoperable protocols to securely convey assertions/claims.

5.