TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG Attestation Framework

Part 1: Terminology, Concepts, and Requirements

Version 1.0
November 1, 2025

Contact: admin@trustedcomputinggroup.org

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

ACKNOWLEDGEMENTS

The writing of a specification, particularly a security specification, takes many hours for both development and review. TCG would like to acknowledge the contribution of those individuals (listed below) and the companies who allowed them to volunteer their time to the development of this specification. Special thanks are due to Henk Birkholz, Dennis Mattoon, and Ned Smith who served as Chairs of the Attestation Working Group during the development of this specification.

Contributors

Fabrizio Damato	Advanced Micro Devices, Inc.
Henk Birkholz	Fraunhofer Institute for Secure Information Technology (SIT)
Thomas Bowen	Intel Corporation
Ned Smith	Intel Corporation
James Borden	Kioxia Corporation
Frederick Knight	Kioxia Corporation
Ahmad Khalifeh	MediaTek, Inc.
Dennis Mattoon	Microsoft Corporation
Steven Bellock	NVIDIA Corporation
Eric Hibbard	Samsung Semiconductor, Inc.

CONTENTS

1 SCOPE

This document is a common source for attestation terminology, concepts, and requirements for designers of attestation systems that can be adopted and adapted by other TCG specifications.

Attestation in the TCG context refers to a process whereby a device is determined to be authentic, to have a known configuration, and to be running known software without unauthorized modifications.

Challenges for interoperable attestation include:

- timeliness of trustworthiness signals in dynamic environments,
- complete and accurate explicit representation of trustworthiness semantics, and
- supply chain dynamics that impact Attester trustworthiness.

The TCG publishes additional attestation related documents, see [1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

1.1 Key Words

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this document normative statements are to be interpreted as described in RFC-2119, Key words for use in RFCs to Indicate Requirement Levels.

1.2 Statement Type

Please note a very important distinction between different sections of text throughout this document. There are two distinctive kinds of text: informative comment and normative statements. Because most of the text in this specification will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, it can be considered a kind of normative statement.

EXAMPLE: Start of informative comment

This is the first paragraph of 1–n paragraphs containing text of the kind *informative comment* ...

This is the second paragraph of text of the kind *informative comment* ...

This is the nth paragraph of text of the kind *informative comment* ...

To understand the TCG specification the user must read the specification. (This use of MUST does not require any action).

End of informative comment

2 REFERENCES

[1] Trusted Computing Group, "Canonical Event Log Format," 2018. [Online]. Available: https://trustedcomputinggroup.org.

[2] Trusted Computing Group, "Implicit Identity Based Device Attestation," 2018. [Online]. Available: https://trustedcomputinggroup.org/.

[3] Trusted Computing Group, "TCG Trusted Attestation Protocol Information Model for TPM families 1.2 and 2.0 and DICE Family 1.0," 2019. [Online]. Available: https://www.trustedcomputinggroup.org.

[4] Trusted Computing Group, "DICE Layering Architecture," 2020. [Online]. Available: https://trustedcomputinggroup.org.

[5] Trusted Computing Group, "Reference Integrity Manifest Specification," 2020. [Online]. Available: https://trustedcomputinggroup.org.

[6] Trusted Computing Group, "TCG Platform Certificate Profile Specification," 2020. [Online]. Available: https://trustedcomputinggroup.org.

[7] Trusted Computing Group, "TCG Reference Integrity Manifest Information Model," 2020. [Online]. Available: https://trustedcomputinggroup.org.

[8] Trusted Computing Group, "DICE Endorsement Architecture," 2021. [Online]. Available: https://trustedcomputinggroup.org.

[9] Trusted Computing Group, "DICE Attestaiton Architecture," [Online]. Available: https://trustedcomputinggroup.org.

[10] Trusted Computing Group, "TCG PC Client Platform Firmware Integrity Measurement," 2021.

[11] Trusted Computing Group, "TCG Glossary," 2017. [Online]. Available: https://www.trustedcomputinggroup.com.

[12] Internet Engineering Task Force, "Remote Attestaton Procedures Architecture," 2020. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/.

[13] Internet Engineering Task Force, "Internet Security Glossary, Version 2," 2007. [Online]. Available: https://tools.ietf.org/html/rfc4949.

[14] Internet Engineering Task Force, "An Internet Attribute Certificate Profile for Authorization," 1 January 2010. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5755.

[15] IEEE, "802.1AR: Secure Device Identity," 2018. [Online]. Available: https://www.ieee.org/.

[16] GlobalPlatform Technology, "Root of Trust Definitions and Requirements," 2018. [Online]. Available: http://globalplatform.org.

[17] ISO/IEC JTC 1/SC6, "8824-1:2021, Information Technology, Abstract Syntax Notation One (ASN.1), Part 1: Specification of basic notation.," 2021. [Online]. Available: https://www.iso.org/standard/81416.html.

[18] Internet Engineering Task Force, "RFC8610, Concise Definition Langhage (CDDL)," June 2019. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8610.

[19] Trusted Computing Group, "Trusted Platform Module Library Family "2.0" Specification," 2019. [Online]. Available: https://trustedcomputinggroup.org.

[20] Trusted Computing Group, "Hardware Requirements for a Device Identifier Compostion Engine," 2020. [Online]. Available: https://trustedcomputinggroup.org/resource/hardware-requirements-for-a-device-identifier-composition-engine/.

[21] Internet Engineering Task Force, "The Transport Layer Security (TLS) Protocol," 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246.

[22] DMTF, "Security Protocol and Data Model (SPDM) Version 1.2.1," June 2022. [Online]. Available: https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.2.1.pdf.

[23] J. C. L. C. Ernie Brickell, "Direct Anonymous Attestation," 11 February 2004. [Online]. Available: https://eprint.iacr.org/2004/205.pdf. [Accessed 2022].

3 TERMS AND DEFINITIONS

This section builds on terminology contained in the Trusted Computing Group Glossary [11].

3.1 Glossary

Terms defined in this glossary are capitalized throughout this document to indicate use of a term that has special meaning for attestation. Terms with special significance for attestation that are defined in other glossaries are capitalized and italicized.

TERMS	DEFINITION
Actor	A computing entity (e.g., device, server, service) that hosts or implements one or more attestation Roles. See §5.1.
Appraisal of Attestation Results	Evaluation of Attestation Results for the purpose of determining Relying Party behavior based on the trustworthiness of an Attester. See §5.3.4 and [12].
Appraisal of Evidence	Evaluation of Evidence for the purpose of assessing trustworthiness of an Attester based on comparisons of Reference Values and Claims. See §5.3.1 and [12].
Appraisal Policy	A set of rules that direct the evaluation of Evidence (by a Verifier) or Attestation Results (by a Relying Party). See [13] and [12] .
Attestation	**Explicit**: A process whereby an Attester is determined to be authentic, to have a known configuration, and to be running known software without unauthorized modifications based on Evidence that is conveyed to a Verifier and compared to Reference Values as part of appraisal. **Implicit**: A process whereby an Attester is determined to be authentic and in a trustworthy state only upon successful use of a capability that cannot be used unless the device is the correct device and in a particular state that satisfies an Appraisal Policy. As a result, a Relying Party interprets successful use of that capability by the Attester as a successful attestation. See §7.
Attestation Result	The result of Evidence Appraisal generated by a Verifier. An Attestation Result also typically includes some information about an Attester. See §5.3.4 and [12].
Attester, Attester Role	A computing entity whose trustworthiness can be evaluated. An Attester Role implements attestation functions (e.g., collects Claims, protects Claims, and conveys Evidence to a Verifier). An Attester might be a Lead Attester that acts as a facilitator for internal Attesters. Lead Attesters convey Evidence to a Verifier on behalf of other Attesters. Lead Attesters might counter-sign Evidence from other Attesters signifying the Evidence transited the Lead Attester. Lead Attesters might proxy Evidence from other Attesters which could involve reformatting Evidence from other Attesters. See §5.2.1 and [12].
Attesting Environment (AE)	An Attesting Environment (AE) collects Claims about a Target Environment (TE), assembles collected Claims into Evidence, and integrity protects the Evidence, often by signing it. An AE protects keys and Claims prior to signing and/or conveyance of Evidence. An AE is hardened by Root of Trust or Trusted Computing Base (TCB) capabilities. An AE might rely on hardened storage capabilities such as a Root of Trust for Storage (RTS) or a storage TCB. An AE relies on Claims collection and/or integrity protection methods that cannot be impersonated by a TE or an intermediary. An AE cannot collect Claims about itself. See §5.2.1 and [12]
Attribute Certificate	An authenticatable and integrity protected structure containing Claims that complies with a standard certificate format and encoding such as [14]. See also Endorsement, Evidence, Measurement.

Assertion	An abstract expression (or information) describing a property that is used to appraise trustworthiness or integrity. See also Reference Value.
Chain of Trust	A sequence of trust dependencies. The sequence results from a series of execution environments, beginning with a Root of Trust, that are, in turn, measured (i.e., attested) by the previous environment. Except for the RoT, each environment begins as a Target Environment (TE). And, except for the last link in the Chain of Trust, each TE also will act as an Attesting Environment (AE). See also Transitive Trust [11]. Note that the term "trust chain" (See [13]) is not the same as a Chain of Trust. The term "trust chain" is typically used in reference to X.509 certificate paths.
Claim	An assertion about an Attester that has attributes, properties, measurements, identifiers, or trustworthiness properties that can be included in Evidence, Endorsements, or Attestation Results. See [13], [11] – Integrity Measurement (Metrics).
Endorsements, Endorsed Values	Claims about an Attester, that are authenticatable, that are supplied by an Endorser. For example, device certificates, see [15], [14], or manifests, see [5], [7], [8]. See also §5.3.2 and [12].
Endorser, Endorser Role	An entity that describes trustworthiness properties of an Attester that typically do not appear in Evidence. An Endorser Role refers to functionality that creates, provisions, or conveys trustworthiness properties, i.e., Endorsements, to Verifiers. See §5.2.2 and [12].
Evidence	Authenticatable Claims (e.g., measurements) related to one or more Target Environments that are asserted by an Attester and conveyed from the Attester to a Verifier. See §5.3.1 and [12].
Measurement	A assertion about an Attester that has trustworthiness properties, attributes, or identifiers.
Measurement TCB	A TCB that implements measurement functions, makes initial integrity Measurements, ensures the integrity of Measurements, and/or facilitates Protected State Transitions. Also, an Attesting Environment implemented within a TCB that collects or creates Measurements describing a Target Environment. See also [11] - RTM.
Protected State Transition	A transfer of control from one environment to another, prefaced by the collection of one or more measurements.
Reference Values	Trustworthiness properties that are expected to appear in Evidence. See §5.3.3 and [12].
Reference Value Provider, Reference Value Provider Role	An entity that provides Claims about trustworthiness properties that are expected to appear in Evidence. A Reference Value Provider Role supplies Reference Values to a Verifier. See §5.2.2 and [12].
Relying Party, Relying Party Role	An entity that manages resources or grants access based on trustworthiness assessments from a Verifier. A Relying Party Role takes Attestation Results from a Verifier as input and evaluates it. See §5.2.5 and [12].
Relying Party Owner, Relying Party Owner Role	An entity that authors and conveys Appraisal Policy used to control Relying Party behavior. For example, a Relying Party Owner might supply trust anchors to authenticate Verifier input. See [12].
Root of Trust	See [11] - Trust, Root of Trust, also [12] Bootstrapped Root of Trust.
Reporting TCB	An Attesting Environment implemented in a TCB that specializes in the production of Evidence, see [11].

Storage TCB	An Attesting Environment in a TCB that specializes in the storage of security relevant data such as Claims, Evidence, keys, secrets, nonces, or other security information, see [11].
Target Environment (TE)	The environment from which an Attesting Environment (AE) collects Claims. TE might possess some level of security hardening. A TE might also contain AE functionality enabling nested Attester compositions. Note: Appraisal of Attester trustworthiness can involve walking nested dependencies (see Chain of Trust). See §5.2.1 and [12].
Trusted Computing Base (TCB)	Environments that depend on one or more Roots of Trust to provide reliable collection and reporting of measurements that determine trustworthiness. See [11] - Trusted Building Block, Trusted Component, Trusted Device, and [16] - Bootstrapped Root of Trust.
Trustworthiness	See [11] and [12].
Verifier, Verifier Role	An entity that determines the trustworthiness of an Attester. A Verifier Role receives and processes Evidence, Reference Values, and Endorsements. A Verifier determines Attester trustworthiness by comparing Evidence to Reference Values to ensure the Reference Values match actual values. The Verifier then produces Attestation Results. See §5.2.4, [11], and [12].
Verifier Owner, Verifier Owner Role	An entity that authors and conveys Appraisal Policy or configuration data used to control Verifier behavior. For example, a Verifier Owner might supply trust anchors to authenticate Endorsers, Reference Value Providers and Attesters. See [12].

3.2 Acronyms

ABBREVIATIONS	DESCRIPTION
DDL	Data Definition Language [17], [18]
DICE	Device Identifier Composition Engine [11]
PCR	Platform Configuration Register [11]
RTS	Root of Trust for Storage [11]
TCB	Trusted Computing Base (§3.1)
TPM	Trusted Platform Module [11]

4 INTRODUCTION

This specification provides a general framework for attestation systems. Existing TCG specifications (see [19], [20]) define attestation information models for interoperable attestation systems containing both TPM and DICE Roots of Trust. Nevertheless, broadly interoperable attestation systems remain an industry challenge. Attestation systems depend on functionality that is deeply embedded in hardware as well as being tightly integrated into web, edge, and enterprise computing. The attestation framework facilitates the integration and interoperability of trusted systems.

Device trustworthiness, generally, relies on secure software, firmware, hardware, and manufacturing practices. Trust among a network of computers relies on the various endpoints being able to assess the quality of these security practices before placing data and computational resources that might be at risk due to participation in the network. Attestation provides the means for dynamic assessment of the quality of security capabilities of devices.

Suppliers of computing technology play a role by contributing data that describes expected security properties. Devices also play a role by disclosing operational information that is compared with the expected values to detect discrepancies. The attestation framework partitions attestation functionality into roles that can be applied to the various components of a trusted device. Such as: Attester, Verifier, Relying Party, Reference Value Provider, and Endorser. Attestation roles can be adapted to fit a variety of system designs. A common attestation vocabulary, concepts, and requirements facilitates the design of computing systems that are both interoperable and trustworthy.

5 ATTESTATION FRAMEWORK

The attestation framework consists of a set of Attestation Roles and the various system entities abstractly referred to as Actors.

5.1 Attestation Actors

An Actor is an entity such as a device, platform, or service that implements one or more Attestation Roles. Different deployments might coalesce multiple Roles onto a single Actor or divide a single Role across multiple Actors. Nevertheless, if inputs and outputs are consistent for a given Role, an attestation workflow is consistent regardless of which Actors are deployed. For example, two unrelated attestation systems might have very different Role-Actor deployments, but if both solutions have common data formats, they will be able to interoperate.

5.2 Attestation Roles

The attestation framework considers five Attestation Roles involved in the exchange of attestation information illustrated in Figure 1.

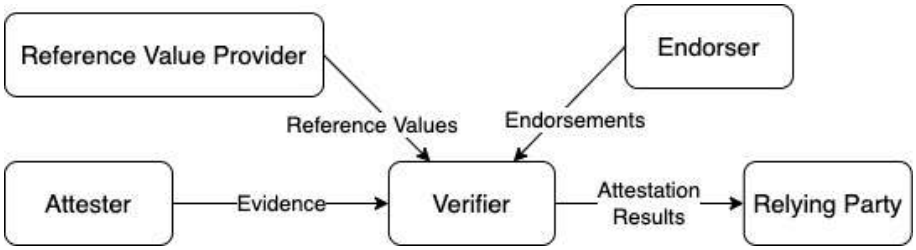

Figure 1: Attestation Roles and Messages

Not pictured in Figure 1 are Owner Roles. The Owner for a given Attestation Role provides policies and/or other data that govern the behavior of the respective Attestation Role. This specification presumes the existence of an Owner for each Attestation Role. Policies affecting Verifier appraisals are known as Appraisal Policy.

5.2.1 Attester Role

The Attester Role provides attestation Evidence to a Verifier. The Attester has access to at least one identity that is used to authenticate Evidence. Attester identities might be created as part of a device manufacturing process or a provisioning process as part of deployment. Attester identities, in the form of device credentials that belong to Actors that implement the Attester Role.

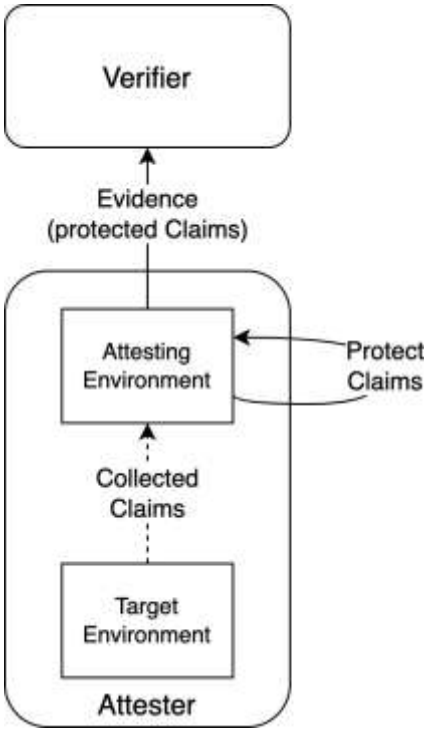

Figure 2: An Attesting Environment collects Claims from a Target Environment and protects them, creating Evidence

An Attester comprises at least one Attesting Environment (AE) and at least one Target Environment (TE), illustrated in Figure 2. An Attesting Environment collects Claims (as measurements) of the Target Environment, which are asserted with the AEs authority, by signing them using an attestation key. Claims are packaged as Evidence by the Attesting Environment, and they are integrity protected using a credential that authenticates the Attesting Environment. An Attester Role implements attestation functions (e.g., collects Claims, protects Claims, and conveys Evidence to a Verifier).

The Attesting Environment can also include Claims in Evidence such as a timestamp, nonce, or epoch marker. Device specific design can influence Evidence collection and reporting behavior. For example, the frequency that an AE collects Claims is a design consideration.

An Attester might be a Lead Attester that acts as a facilitator for internal Attesters. Lead Attesters convey Evidence to a Verifier on behalf of other Attesters. Lead Attesters might counter-sign Evidence from other Attesters signifying that Evidence transited the Lead Attester. Lead Attesters might proxy Evidence on behalf of other Attesters which could involve reformatting and re-signing Evidence.

5.2.1.1 Device Composition

An Attester device might be composed of multiple components or sub-components that each implement an Attester Role, as illustrated in Figure 3. A lead Attester might coordinate the gathering of Evidence from other Attesters. A lead Attester might describe the composition of a device based on the connectivity path to other Attesters. Additionally, Evidence might describe device composition using Measurement Claims where the Attester identifies the Target Environments from which Measurements were collected.

Attesters might be an assembly of discrete components. An Attester's trustworthiness is a function of the trustworthiness of its discrete components. Consequently, attestation Verifiers need to appraise trustworthiness of discrete components before arriving at an overall trustworthiness result.

Attester composition also provides context for understanding trust dependency. Components might depend on other components for trust establishment, such as provisioning secrets, collecting Measurements, and scheduling execution. A sequence of trust dependency is known as a Chain of Trust. Assessing a Chain of Trust is another aspect of Appraisal.

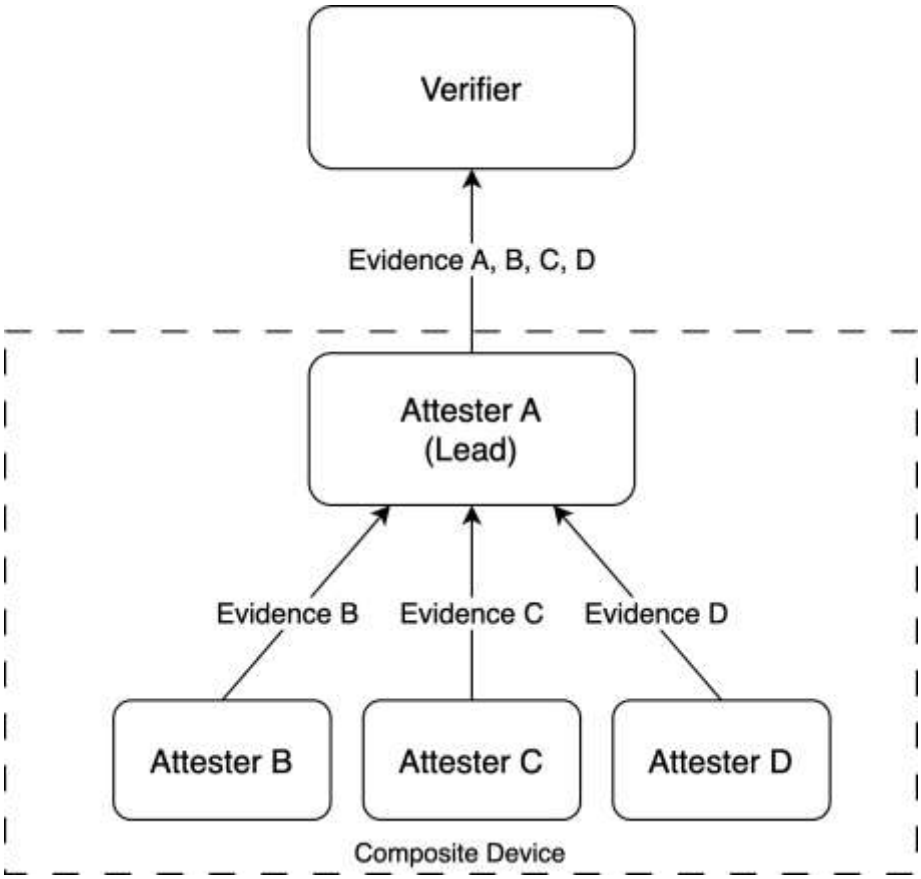

Figure 3 - Device composition with lead Attester (e.g., a composable server)

5.2.2 Reference Value Provider Role

The Reference Value Provider (RVP) Role is typically implemented by a supply chain entity that creates Reference Values. Reference Value Providers create Reference Values that are matched with Evidence to determine whether Evidence is trustworthy. RVPs are typically the same entity as the Attester's manufacturer, but where different, the RVP needs to coordinate with Attester's manufacturers to ensure Evidence can be matched with Reference Values. Nevertheless, these entities might not be the most trusted entities for supplying Reference Values. Consequently, Verifiers typically have Appraisal Policies that identify trustworthy Reference Value Providers.

5.2.3 Endorser Role

The Endorser Role is typically implemented by a supply chain entity that creates Endorsements. Endorsers implement manufacturing, productization, and/or other procedures that establish the trustworthiness properties of an Attesting Environment. Endorsements contain Assertions about the device's trustworthiness properties, such as conformance, compliance, and product design. For example, the enablement of a hardware-debug port might invalidate a compliant configuration, or the use of a physically unclonable function (PUF) might enhance security.

Endorsers also assert trustworthiness properties of an Endorsement. For example, a device manufacturer might be the best entity to assert properties of a hardware design. There might be multiple entities that vouch for the same Endorsement Claim. Of the potential Endorsers, some might not be as trusted as other entities for supplying a specific

Endorsement. Consequently, Verifiers and Relying Parties typically have Appraisal Policies that identify trustworthy Endorsers.

5.2.4 Verifier Role

A Verifier receives Endorsements, Reference Values, Evidence, and Appraisal Policy for Evidence; performs Appraisals; and conveys Attestation Results to one or more Relying Parties. A Verifier has Appraisal Policies for Evidence. For example, a configuration utility might provision the Verifier with trust anchors. The Verifier uses the Appraisal Policy for Evidence to determine Attester trustworthiness. The Verifier provides the Attestation Results, formatted in accordance with the Appraisal Policy, to the Relying Party.

5.2.5 Relying Party Role

The Relying Party Role is responsible for appraising Attestation Results according to Appraisal Policies. A Relying Party receives Attestation Results from a Verifier. A Relying Party has an Appraisal Policy for Attestation Results. The configuration and provisioning of a Relying Party also determines which Relying Party trusts Verifiers.

A Relying Party takes actions based on Appraisal of Attestation Results. For example, a Relying Party might admit or deny access, apply remediations, make entries in an audit log, or trigger other action. The exact actions taken are outside the scope of this specification.

5.3 Claims

Assertions about trustworthiness properties are implemented as Claims. Claims might be semantic-annotated values that can be explicitly realized in tag-value form or as expressions in a data definition language (DDL). See [17], [18].

Interoperability can be achieved when the syntax and semantics of the Claims are well-known. The choice of DDL can have a substantial impact and ought to be considered carefully. Ultimately, Verifiers need to ensure all Claims are semantically aligned before applying appraisal steps, otherwise different Verifier implementations that are supposed to agree will produce different results.

Claims that are from AEs that are part of the same Chain of Trust might need to stage appraisals so that components that depend on other components for trust are appraised in the correct order. For example, a device containing a TPM has a transitive trust chain [11] in which a module, such as a boot ROM, measures firmware which in turn measures a bootloader, and so forth. The TPM's PCRs contain Chain of Trust dependencies where each PCR in the chain has a trust dependency on another PCR.

5.3.1 Evidence

Evidence contains Claims about an Attester that originate from the Attester as illustrated in Figure 4. Evidence describes the current or historical operational state of a device. Evidence might describe an operational state that either cannot be anticipated by Reference Values or requires updated Reference Values before Appraisal will succeed. Evidence might also include freshness and/or recentness Claims (see Section 5.4.1).

Evidence might contain Claims that do not have corresponding Reference Values. For example, the presence of a pluggable storage device could be reported in Evidence, but its presence in the platform wasn't anticipated by the Reference Value Provider. The Relying Party might deny access based on the presence of this unexpected device.

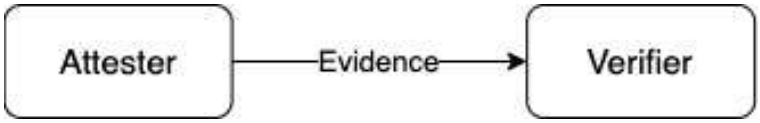

Figure 4: Evidence message from Attester to Verifier

5.3.2 Endorsements

Endorsements contain Claims that have been signed by an Endorser. Endorsements might indicate that the Attester possesses capabilities or properties that cannot (or will not) be reported in Evidence. Endorsements might consist of several types of information, including the initial operational state of a device. For example, if a debug mode is permanently disabled during manufacturing, the Endorser might assert this state independent of Evidence. The conveyance of this Role message is illustrated in Figure 5.

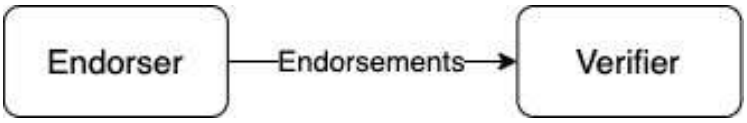

Figure 5: Endorsement message from Endorser to Verifier

Examples of Endorsement Claims include:

- Endorsed Values that are asserted by an Endorser, about an Attester, that Verifiers accept based on their trust in the Endorser.
- Device composition.
- Device identity properties.
- Manufacturing process assertions.

5.3.3 Reference Values

Reference Values describe various possible states that an Attester could enter. Appraisal of Evidence determines if the Attester is in one of these states.

Figure 6 - Reference Values message from Reference Value Provider to Verifier

Reference Values (e.g., [5], [7], [8]) are compared with Claims found in Evidence. Verifiers appraise Evidence using Reference Values.

5.3.4 Attestation Results

Attestation Results are the result of a Verifier's Appraisal of Evidence and Endorsements. Attestation Results are integrity-protected and possibly confidentiality-protected using Verifier credentials so that Relying Parties can verify the Attestation Results were asserted by the Verifier. Attestation Results assert Attester trustworthiness status in a format that is meaningful to the Relying Party's application-specific context. The conveyance of an Attestation Results message is illustrated in Figure 7.

Figure 7: Attestation Results message from Verifier to Relying Party

Verifiers might have policies that direct Attestation Results generation, which Claims are important within Attestation Results, which Relying Parties to trust, which cryptographic algorithms are acceptable for protecting Attestation Results.

5.4 Design Considerations

5.4.1 Properties of Measurement Claims

Measurement Claims are representations of Target Environment trustworthiness that an Attesting Environment can securely obtain. The quality of collected Claims is determined by the quality of the AE's design.

The following AE design challenges might be carefully considered:

- Measurability: the ability to reliably obtain TE Measurements.
- Mutability: the nature or design of the TE to accommodate change.
- Freshness: a mechanism that ensures TE state is current.

One overriding consideration for remote attestation is that Evidence accurately represents the operational state of an Attester's Target Environment, and that Claims in Evidence were collected at a well-defined point prior to or during runtime.

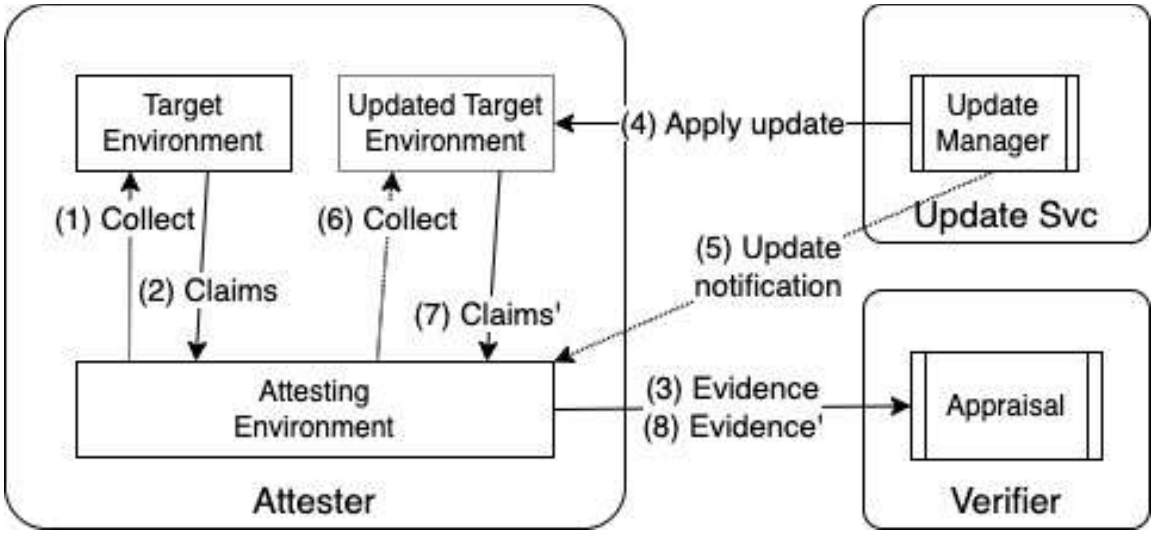

Figure 8 - Design considerations for keeping measurement Claims fresh

Evidence that accurately represents the state of a TE at the time of Appraisal is considered fresh. Evidence might become stale when, for example, a Target Environment (TE) is updated after initial Claims collection occurs. Figure 8 shows an example scenario involving an Attester with an Attesting Environment (AE) that initially collects measurement Claims describing a TE (steps 1 and 2). A Verifier receives an Evidence message from the AE in step 3. A service provider applies an update to the TE in step 4 resulting in the Evidence in step 3 becoming stale. The Update Service notifies the AE in step 5, that the TE Evidence is now stale. The AE collects new Claims in steps 6 and 7. The fresh Claims are reported in another Evidence message in step 8.

This example illustrates that as soon as the actual state of the TE changes, the Evidence that describes previous TE state is stale. The AE needs to collect Claims again to produce fresh Evidence. The Verifier needs to ensure the freshest available Evidence is appraised.

Note that there are situations in which the freshness of Evidence cannot be known for certain. In these situations, Verifiers use the recentness of Claims collection as an approximation of freshness. If a Verifier cannot know with certainty whether the state of the Attester is accurately represented by the Claims in Evidence, the Verifier can at least ensure that the Evidence was created as recently as possible, thereby increasing the likelihood of fresh Measurements by the Attester.

5.4.2 Timing

Attestation systems rely on techniques for collecting and reporting Claims that accommodate timing considerations but also provide Verifiers with Evidence that reflects the actual state of the Attester. The timing and frequency of Claims collection is a design consideration for attestation systems. Claims could be collected every time the Attesting Environment receives a request, as triggered by an event, scheduled at regular intervals, or by some combination thereof.

If an unanticipated change occurs and AE collects Claims at a regular interval, downstream trustworthiness appraisals will eventually detect the discontinuity. However, the amount of time it could take to detect the change would be determined by the attestation interval. More frequently collected Claims are less likely to be stale, but this might come with added computational cost. Attestation system designs need to balance the frequency of Claims collection and appraisal with the performance impact of more frequent interactions.

5.4.3 Root of Trust Semantics

A Root of Trust (RoT), by its nature, is described by an Endorsement because it cannot create meaningful Evidence about itself. A RoT typically contains a means for generating or storing cryptographic keys used by an Attesting Environment to sign Evidence. A RoT might also contain a means for observing Target Environment state such that an Attesting Environment can collect Claims without concern for spoofing attacks on behalf of the Target Environment. A Verifier needs an explicit understanding of not only the attributes of a Target Environment, but also the RoT within an Attester and its availability to a Target Environment.

5.4.4 Endorsement Lifecycle Management

Endorsers need a mechanism to account for all endorsable components within a product offering. This includes documenting system objects, expected behaviors, and composition of objects that impact trustworthiness. For examples of how to compose Endorsements, see [8]. An infrastructure that provides timely trustworthiness status is an important aspect of trusted information and cyber-physical systems.

6 INTERACTION MODELS

Attestation system interactions typically follow a few common models. This section describes some of these interaction models. Alternative interaction models are possible, and they could be combined in various ways.

6.1 Passport Model

The passport model, illustrated in Figure 9, is a sequence of message exchanges that is patterned after government-issued passports. In this analogy, a citizen (i.e., passport holder) presents identity information to the passport issuer who constructs the passport document and gives it to the passport holder. The passport contains markings or other factors that enable a border control agent to verify the passport document's authenticity and the passport holder's identity.

The passport model for attestation treats the Attester as the passport holder, who presents the passport (Attestation Results) to a Relying Party (the border agent).

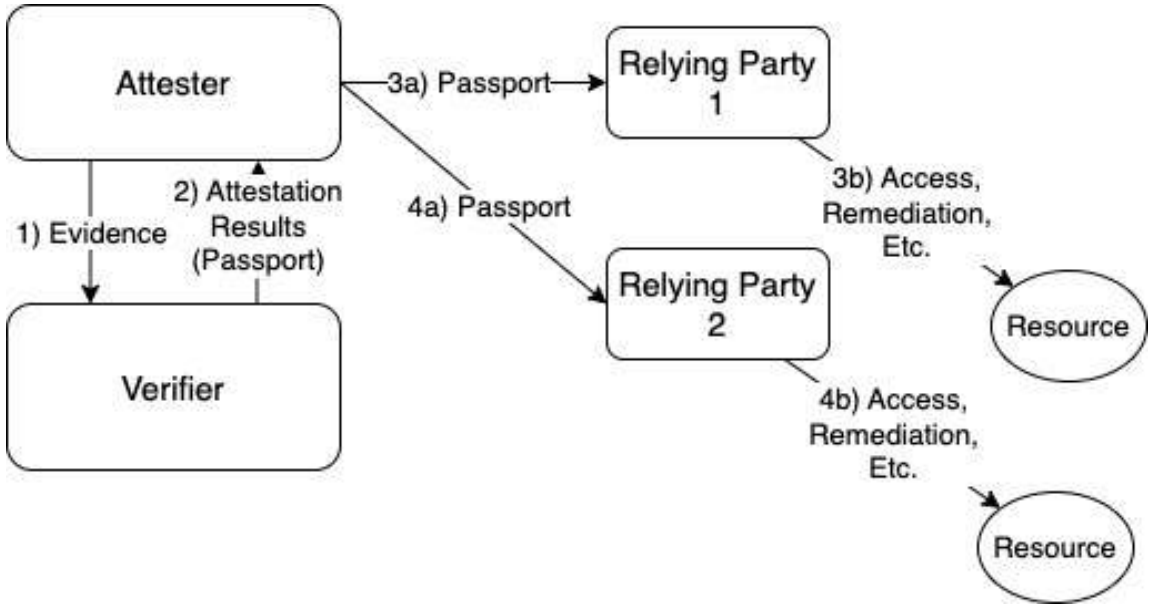

Figure 9: Passport model

The sequence of steps in the passport model for attestation comprises the following:

1) The Attester presents the Evidence message to a Verifier.
2) The Verifier checks message integrity and origin and might use a nonce (or some other method) to ensure recentness. The assertions within the message are evaluated based on an Appraisal Policy for Evidence. The Verifier creates an Attestation Results message (the passport) containing assertions about the Attester. The Attestation Results message is signed by the Verifier either directly or provided in an authenticated protocol such as TLS [21] or SPDM [22].
3) A Relying Party performs appraisal steps as follows:
    a. Verify that the passport is authentic and came from the Verifier.
    b. Apply an Appraisal Policy for Attestation Results to determine how the resource might be accessed or manipulated.
4) Relying Party 2 performs appraisals like step 3.

The passport model might scale well in applications where multiple relying parties are accessed over a short period of time.

6.2 Background Check Model

The background check model, illustrated in Figure 10, is a background check that occurs opaquely to the Attester.

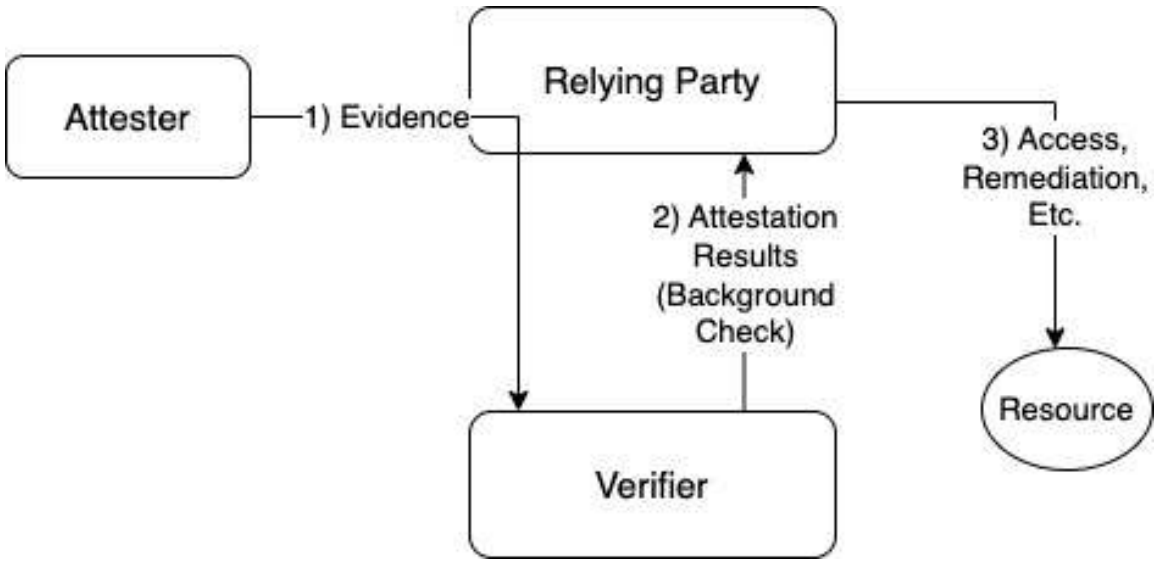

Figure 10: Background check model

The background check model comprises the following steps:

1) The Attester presents the Evidence message to a Relying Party. The Relying Party forwards the Evidence to the Verifier, which performs the background check.
2) The Verifier authenticates and appraises the Evidence. It might be necessary for the Verifier, by way of the Relying Party, to ensure the Evidence was created recently.
3) The Verifier delivers Attestation Results to the Relying Party. The Relying Party appraises the Attestation Results.

The background check model might scale well in applications where the Attester and Relying Party have a long-lived session.

6.3 Periodic Recheck Model

A periodic recheck model is an interaction model that employs a timer or other event-driven mechanism to initiate a remote attestation recheck signal. The recheck might cause the Attester to collect Claims and convey Evidence to a Verifier, or it might cause previously collected Claims to be reasserted as Evidence.

From the perspective of a Relying Party, the recheck might initiate the verification and appraisal of a previously asserted Attestation Results or might cause previously conveyed Attestation Results to be recreated or re-sent.

6.4 Subscription Model

A subscription model is an interaction model that uses a publish-subscribe method to convey Role messages. Verifiers subscribe to Evidence, Endorsements, and Appraisal Policy for Evidence; and publish Attestation Results. Relying Parties subscribe to Attestation Results and Appraisal Policies for Attestation Results. Attesters publish Evidence. Endorsers publish Endorsements, and so forth.

For example, a state change in an Attester device, like the device entering debug mode, might cause the Attester to publish updated Evidence to its subscribers (i.e., a Verifier). As another example, a change to software might cause an Endorser to publish updated reference values and a change to an Endorsement could result in a different appraisal outcome causing a Verifier to publish updated Attestation Results.

7 IMPLICIT ATTESTATION

Evidence Claims are Appraised to determine the degree of trustworthiness of an environment. Explicit attestation demonstrates trustworthiness using an external Verifier, whereas for an implicit attestation an external Verifier is not required. Instead, implicit attestation realizes contextual results that are only available if an Attester is in a trustworthy state.

In implicit attestation, an Actor (e.g., a manufacturer, component, device, platform) enables or installs an implicit attestation capability in an Attester. This implicit attestation capability serves a similar purpose to a Verifier and validates Attester state. If the local appraisal of this Evidence is successful, it need not be transmitted to external Verifiers. Successful use of the attestation capability implies successful attestation by the Attester. For example, a manufacturer might provision an internal Verifier and the policy that directs the implicit attestation in the form of an implicit attestation function, see Figure 11.

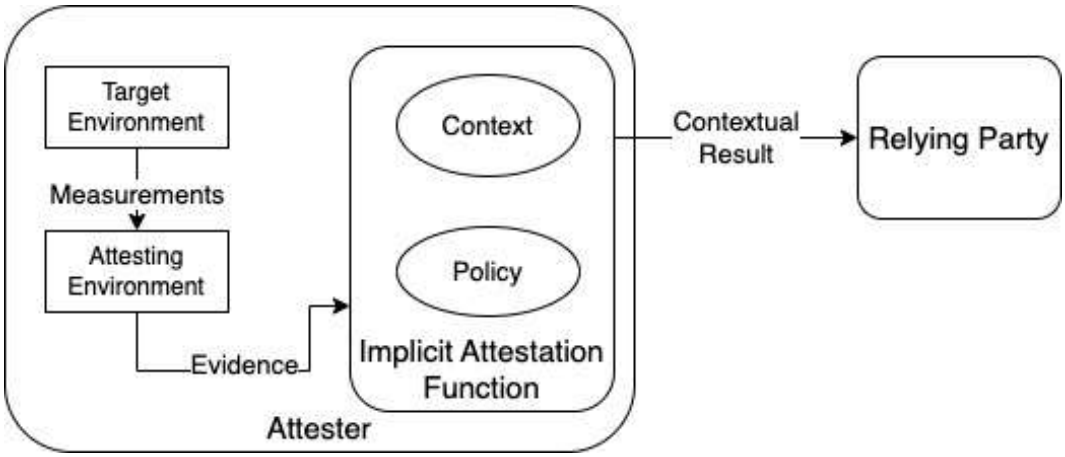

Figure 11: Implicit attestation model

An implicit attestation typically includes the ability to use a secret, such as an identity key or a decryption key. The availability (or not) of an implicit attestation is enforced by the platform's Root of Trust mechanisms. As a result, the availability of implicit attestation depends on the same trust mechanisms that are used in explicit attestation. If a platform can access and use the correct secret in an implicit attestation, the platform is in a particular operational state. As a result, the availability (or not) of an implicit attestation capability demonstrates whether the platform is trustworthy. An Attester might use the availability (or not) of an implicit attestation capability as explicit proof of attestation.

A Verifier or Relying Party might use explicit attestation to determine whether a platform has an implicit attestation capability that implies an acceptable degree of trustworthiness, deduce that a platform has an acceptable degree of trustworthiness, and enable or install an implicit attestation capability in the platform.

Relying Parties might be programmed to know that platforms cannot use an implicit attestation capability unless they have an acceptable degree of trustworthiness. Such Relying Parties do not require explicit attestation to determine whether a platform has an acceptable degree of trustworthiness.

An implicit attestation capability, by definition, is inoperable unless the host has the implied degree of trustworthiness, either ensured by design and manufacture, or verified via capabilities of Attesting Environments (such as Roots of Trust.

For example, if the platform is associated with a cryptographic identity document (e.g., X.509 certificate), then the presence or availability of the key material demonstrates successful implicit attestation. A Relying Party nevertheless

evaluates the platform's Endorsement record to verify the platform was manufactured with an implicit attestation capability. The Relying Party trusts that the implicit attestation capability cannot be circumvented.

8 ATTESTATION REQUIREMENTS

1) An attestation capability MUST contain a Root of Trust.

Start of informative comment

An Attester is a collection of hardware, software, and/or firmware, and a Root of Trust with the ability to provide reliable evidence (e.g., measurements) to a Verifier.

End of informative comment

2) An attestation capability Root of Trust MUST be Endorsed.

Start of informative comment

A Root of Trust is a component that is trusted to always behave in the expected manner because its misbehavior cannot be detected. For this reason, a Verifier can rely only on an Endorsement of an Attester's Root of Trust to establish trustworthiness.

End of informative comment

3) An implicit attestation capability MUST be Endorsed.

Start of informative comment

Without information from an Endorser (i.e., in the absence of explicit measurements to reconcile with Evidence), a Verifier may have no way of recognizing when an implicit attestation is successful. For example, if a Verifier is not aware that the derivation of a given DICE key is based on measurements of firmware, the Verifier may not be aware that the successful validation of a signature using that key confirms the Attester is in a known state. A Verifier needs to rely on an Endorsement to confirm that the successful use of a given Attester capability qualifies as a successful attestation.

End of informative comment

4) An explicit attestation capability that produces Evidence, MUST produce authenticatable and integrity protected Evidence.

Start of informative comment

A digital signature is a common way to satisfy this requirement. Signing Evidence integrity-protects it. If the identity of the signer (e.g., the Attester) is provided to and recognized by a Verifier (e.g., using an X.509 certificate containin the signing key), the Evidence is also authenticatable.

End of informative comment

5) An explicit attestation capability that produces Evidence MUST have a cryptographic key used to protect Evidence.

Start of informative comment

While use of explicit attestation implies the production of Evidence, this requirement is explicit. Evidence, including measurements, needs to be authenticatable and integrity-protected at minimum, and could require confidentiality. In this context "authenticatable" means to have certainty of the message origin. To achieve these requirements, methods involving the use of a cryptographic key are used.

End of informative comment

