TCG Credential Profiles
For TPM Family 1.2; Level 2

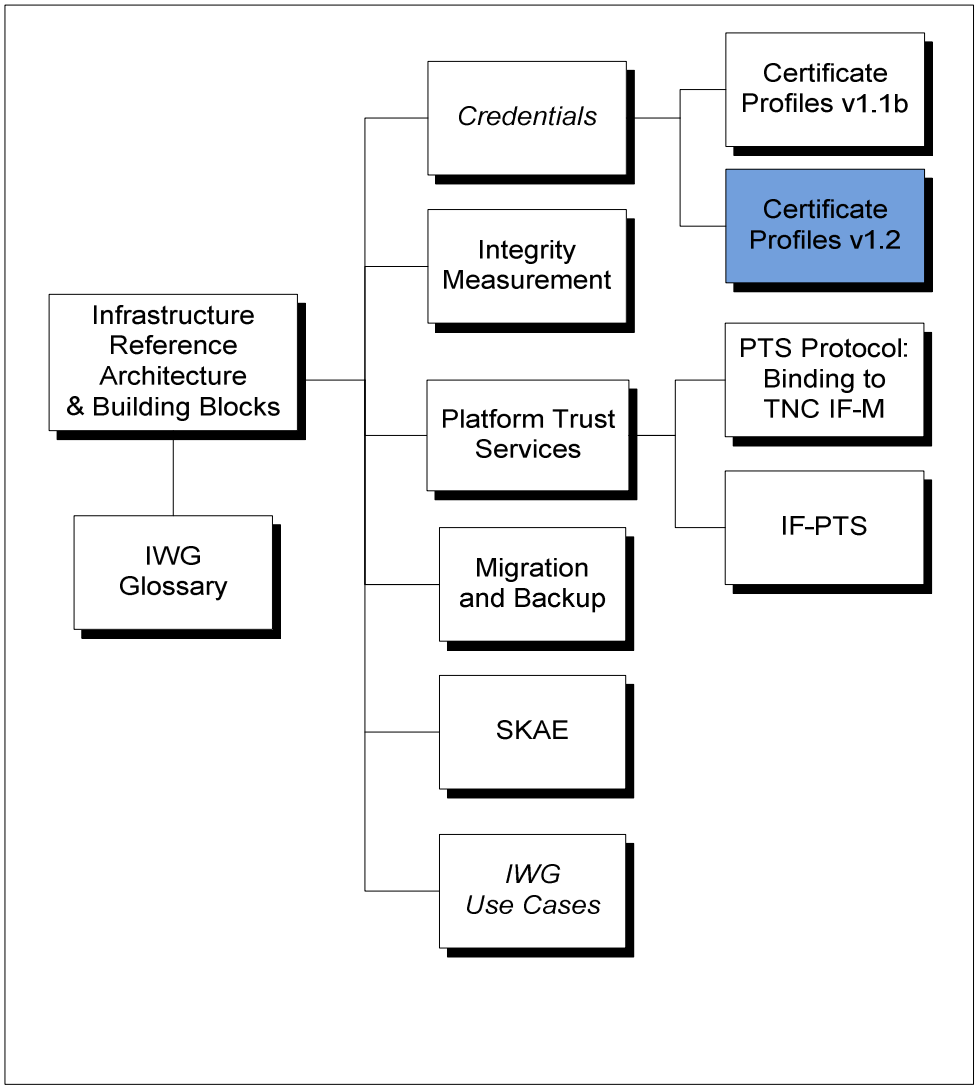
Specification Version 1.2
Revision 8
3 July 2013
Published

Contact:
admin@trustedcomputinggroup.org

TCG PUBLISHED

TCG

IWG Document Roadmap



Acknowledgement

The TCG wishes to thank those who contributed to this specification. This document builds on considerable work done in the various working groups in the TCG.

Special thanks to the members of the IWG group and others contributing to this document:

Name	Member Company
Carolin Latze	89grad
Geoffrey Strongin	AMD
Dean Liberty	AMD
Randy Mummert	Atmel
Malcolm Duncan	CESG
Kazuaki Nimura	Fujitsu
Graeme Proudler	Hewlett-Packard
Takeuchi Keisuke	Hitachi
Hisanori Mishima	Hitachi
Diana Arroyo	IBM
Lee Terrell	IBM
Roger Zimmermann	IBM
Markus Gueller	Infineon
Johann Schoetz	Infineon
David Grawrock	Intel
Ned Smith	Intel
Monty Wiseman	Intel
Daniel Wong	Microsoft
Mark Williams	Microsoft
Mark Redman	Motorola
Sue Roddy	NSA
Laszlo Elteto	SafeNet
Manuel Offenberg	Seagate Technology
Brad Andersen	SignaCert
Nicholas Szeto	Sony
Wyllys Ingersoll (IWG co-chair)	Sun Microsystems
Jeff Nisewanger	Sun Microsystems
Paul Sangster (Editor and IWG co-chair)	Symantec Corporation
Thomas Hardjono	Wave Systems
Greg Kazmierczak	Wave Systems
Len Veil	Wave Systems
Mihran Dars	Wave Systems

Table of Contents

1 Introduction

This section summarizes the purpose, scope, and intended audience for this document.

1.1 Purpose

The purpose of this document is to collect, in one document, definitions for three of the abstract credential types identified in the v1.1b TCPA Main specification[5]. These are the Endorsement Key (EK) Credential, the Attestation Identity Key (AIK) Credential, and the Platform Endorsement (Platform) Credential. This specification describes the contents of these abstract credentials and then provides an X.509 instantiation of each of the three credentials that product vendors and customers could use with their products. Version 1.1 of this specification adds a fourth certificate instantiation called the Unified Certificate which blends the formats of each certificate type into a single definition and enables references.

This specification establishes the use of these three abstract credential types for trusted platforms that include 1.1 and 1.2 family TPMs.

TCPA defined a fourth type of credential, a Conformance Credential, in Section 4.32.3, Evidence of Platform Conformance[5]. A fifth credential type known as a Validation Credential is defined in Section 4.32.4[5]. The Conformance Credential and the Validation Credential are not profiled in the current document.

Version 1.1 of this specification builds upon 1.0[12] by adding:

- A “unified” credential format (and X.509 instantiation) capable of representing all of the information present in version 1.0 EK, AIK and Platform credentials. It is not our expectation that a single unified credential would be deployed including all this information, but rather this format allows for a single type of credential to be used and parsed throughout the supply chain. The associated unified certificate format would be a normal end entity certificate so would eliminate the need for issuing attribute certificates like the 1.0 Platform Credential.
- New fields within the unified credential that enable referencing of information present in other credentials or signed documented (e.g. an XML-based Reference Manifest.) This addition makes it possible for information not unique to a single platform to be shared (thus not duplicated) in a number of credentials. This addition to the credential is included as a new extension to the X.509 certificate instantiation.

The use of credentials described in the 1.0 specification is not deprecated, so the 1.1 specification is merely adding additional options/flexibility. The TCG encourages the use of the new unified credential even if it is referencing other 1.0 compliant credentials for much of its contents.

1.2 Scope and Document Time-Line

This document specifies a full definition of the EK Credential, the AIK Credential, and the Platform Credential for use with Family 1.1 and Family 1.2 TPMs. Credentials unique to the 1.2 family such as Direct Anonymous Attestation (DAA) will be specified in a future document.

For all three credential types, this specification describes the abstract definition of the credential and specifically how each credential would appear as an X.509 certificate. Other documents may describe the mapping of these credentials to other formats such as those based on XML. Version 1.1 of this specification includes a fourth credential type that can replace/represent any of the three 1.0 credentials, thus enabling a common format to be used.

1.3 Relationship to Other TCG Specifications

1. A TPM claiming adherence to this specification MUST be compliant with the TPM Specification; Family 1.1; Level 1; Revision 2.0[5] or later.

2. This specification is known to be compatible with the PC Client Implementation Specification for Conventional BIOS Version 1.0[6].

1.4 Keywords

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119[7].

1.5 Intended Audiences

The intended audience for this document is people who work for the entities, such as Privacy-CAs (AKA Attestation CAs), who are expected to participate in the TCG infrastructure. People who work for computer OEMs and the companies in the OEM supply chain, such as TPM vendors and software vendors, are also intended audiences for this document.

This document specifies one aspect of an architectural framework that can be found in the latest draft of the document entitled “TCG Infrastructure Working Group Reference Architecture for Interoperability”[2] In particular, see sections 3, 4, 5, and 6.

1.6 Specification Design Goals

The completeness of the credential type specifications in this document will be judged using the following criteria:

- Interoperability
- Backward compatibility with Section 4.32, Credentials, and Section 9.5, Instantiation of Credentials as Certificates, in the 1.1b TCPA Main Specification[5]. This specification is fully backwards compatible except where specifically noted.
- Trusted Platform owner and user privacy protection

1.7 Definition of Terms

The TCG Technical Committee Glossary contains a few definitions that are fundamental to this document.

The following operational definitions, however, are specific to this specification.

Certificate – A certificate is an instantiation of a credential using the industry-standard certificate structure from ISO/IEC/ITU-T X.509 version 3. Certificate generation consists of (a) assembling values for the credential fields and (b) signing over the assembled fields.

Credential – A credential is an abstract proof that must be instantiated as a certificate before it can be exchanged between entities.

2 TCG 1.0 Credential Overview

This section describes three TCG credential types, and summarizes the relationships between them.

It is useful to differentiate two categories of TCG credentials:

- Credentials used for platform identity management; typically, this type of TCG credential contains the public key of a public/private key pair that is held inside a TPM. The TPM EK Credential and the AIK Credential are used for platform identity management.
- Credentials used for platform integrity management; typically, this type of TCG credential does not contain a public key. The Platform Credential is used for platform integrity management. It represents the Trusted Building Block (TBB) of the platform.

2.1 Relationships between the 1.0 TCG Credentials

Figure 1 shows the relationship between the TCG credential types as defined in the version 1.0 of this specification. Note that not all fields are shown for the credential types in the diagram, but all fields that reference other credential types are shown.

- The Platform Credential references the EK Credential for the TPM that is bound to the platform, shown as “A” in the diagram. This links the Platform and EK Credential to a single platform and establishes assertions about that particular platform.
- The AIK Credential shares information with both the EK Credential and the Platform Credential. A challenger could use this information, along with other information that is in the AIK Credential, to trust the platform via an attestation protocol.
    - Specifically, the AIK Credential contains a description of the TPM manufacturer, model, and version in the EK Credential, shown as “C” in the diagram. Note that the AIK Credential does not reference the privacy-sensitive public Endorsement Key that is also part of the EK Credential.
    - The AIK Credential also includes the platform root of trust manufacturer, model, and version in the Platform Credential, shown as “B” in the diagram. Note that this common information is not unique to a single Platform Credential; instead, it is a reference to (or integration of) the information contained within the Platform Credential that is not privacy-sensitive.

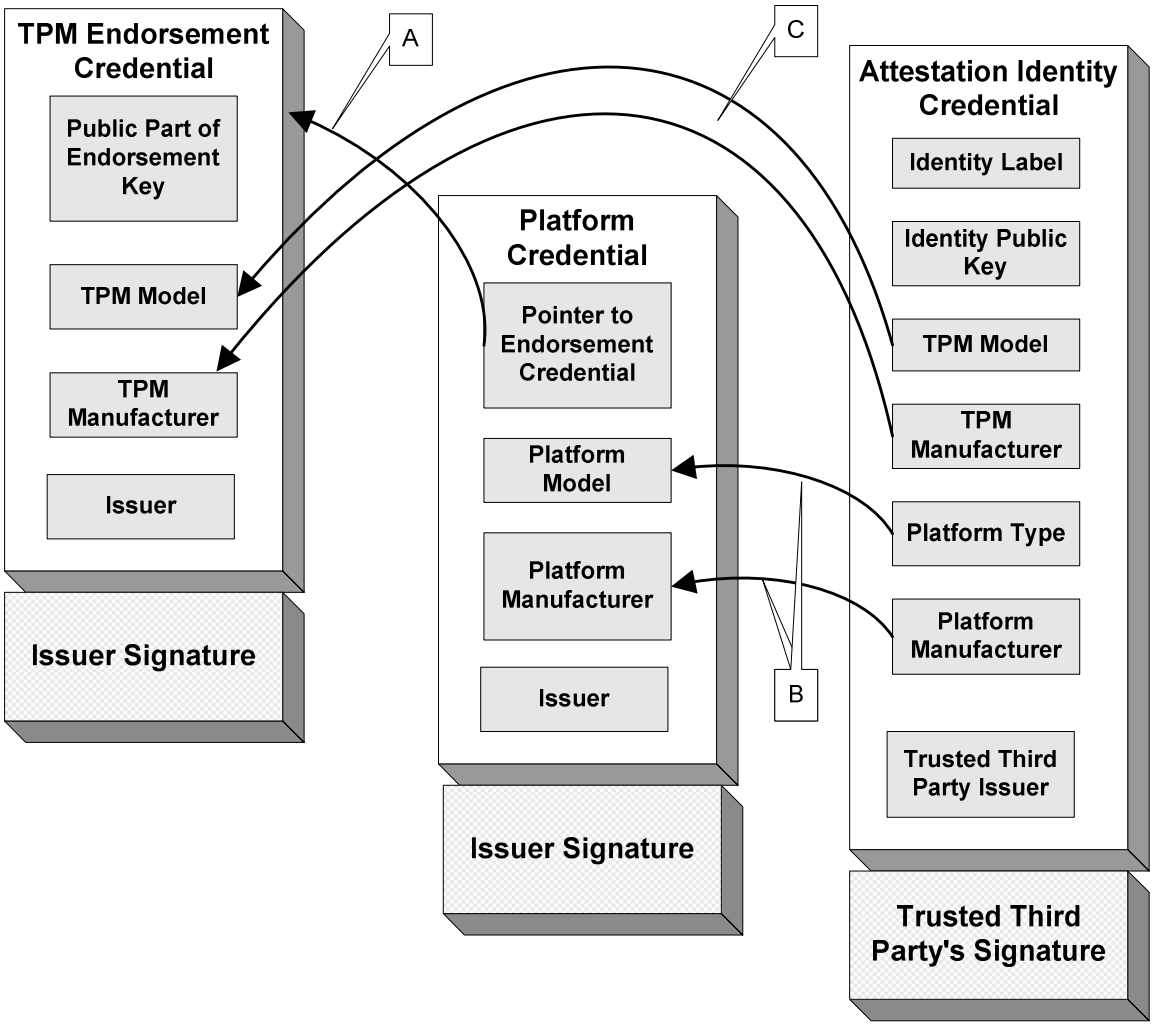


Figure 1: Credential Relationship Diagram

2.2 Relationships between the 1.1 TCG Credentials

Version 1.1 of this specification introduces a new credential type called the Unified Credential that expands the relationships that can be represented between credentials. The following diagram shows an example of how the Unified Credential increases the flexibility of relationships in part by including lists of references to other Credentials and relevant documents (e.g. Reference Manifests.)

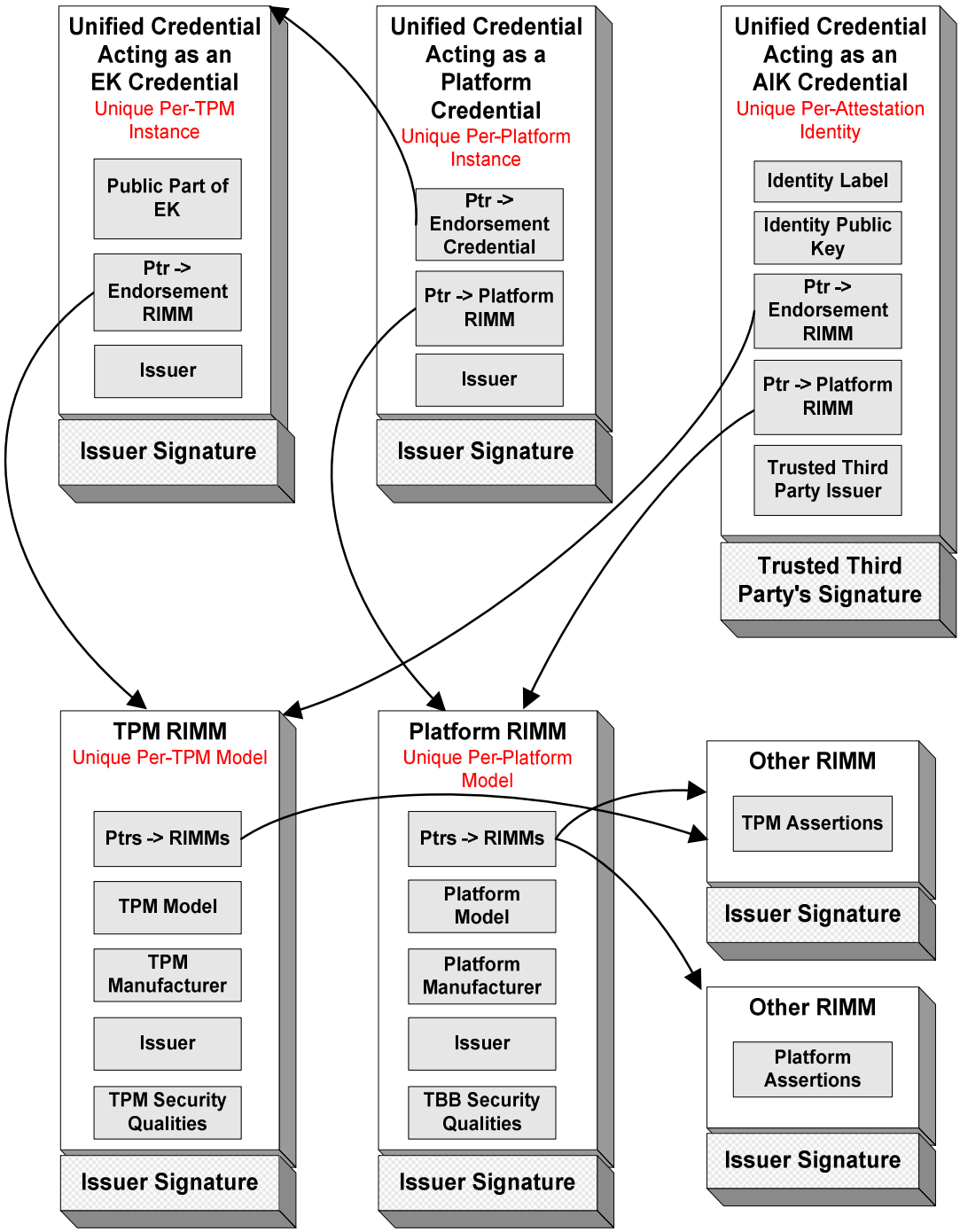


Figure 2: Credential Relationships based upon a Unified Credential

In Figure 2, this example shows three Unified Credentials and four Reference Manifests acting in concert to describe an AIK credential associated with a particular platform. The three Unified Credentials are fulfilling the equivalent roles of the EK, Platform and AIK Credentials from Figure 1 but this time much of the information is not directly included in the credentials. Instead the information is included by reference to another Credential or Reference Manifest allowing sharing of

information. In particular, this example shows two Reference Manifests that are asserting information common to all instances of a TPM or Platform Model that a manufacturer might issue one time during the lifetime of a model. These Reference Manifests might leverage references to other Reference Manifests offering assertions common to many models. Later as each instance of TPM part or Platform Model is manufactured, it is given a minimal sized credential that includes some instance specific information (e.g. EK Public Key) and a reference to the common model information. While not shown on this diagram, the Unified Credentials are capable of referencing older 1.0 or 1.1 formatted credentials allowing for credential re-issuance while maintaining some properties of the original credential. For example, a Unified Credential acting as an EK Credential, may reference previous EK Credentials for the TPM issued by other parties which might occur if an OEM needed to re-issue the EK Credential yet wanted to link it to the TPM Manufacturer created EK Credential.

2.3 Fields Common to All Four TCG Credential Types

The following four fields MUST be included directly or via reference in all four credential types in this specification and are collectively called “common fields.”

- Credential type label: The label enables the Issuer to sign the credential with a key that is not reserved exclusively for a particular credential type.
- Issuer: Identifies the entity that signed and issued the credential
- TCG specification version: Identifies the TPM or platform-specific specifications implemented by the TPM or platform TBB which is represented by the credential
- Signature value: The signature of the issuer over the other fields in the credential

All other fields in a TCG credential type are called, collectively, “information fields.” Some information fields are mandatory and some are optional. The credential-specific information fields for each of the four TCG credential types are summarized in this section below.

2.4 Endorsement Key (EK) Credential

The EK Credential contains the public Endorsement Key, so an EK Credential cannot be issued until the unique EK public/private key pair is established inside the TPM. The pair can be established inside the TPM at any point in the Trusted Platform supply chain; for more information, see section 6.4, Examples of Credentials in the TP Lifecycle[2].

If the EK pair is generated after delivery of the platform to a customer, the conditions in which the key was created may impact the endorsement that can be provided.

The EK public key, though public, may be privacy-sensitive due to the fact that it uniquely identifies the TPM and by extension the platform.

2.4.1 Who Uses an EK Credential?

A Privacy-CA (Attestation CA) is the primary user of an EK Credential although it may have other uses. For example, protocols that manage TPM ownership may utilize the EK Credential.

2.4.2 Who Issues an EK credential?

Several different types of entities in the platform manufacturing process may sign an EK credential. For more information, see Section 3, The Trusted Platform Lifecycle[2].

2.4.3 EK Credential Privacy Protection Requirements

If the EK Credential is stored on a platform after an Owner has taken ownership of that platform, it SHALL exist only in storage to which access is controlled and that is available only to entities authorized by the Owner; this is to protect the privacy of the platform owner and the privacy of users of the platform.

2.4.4 EK Credential Creation Requirements

An entity SHALL NOT create an EK credential for a TPM unless the entity is satisfied that the public key referenced in the EK credential was either:

- returned in response to a TPM_CreateEndorsementKeyPair or TPM_CreateRevocableEK command by an implementation of protected capabilities and shielded locations that meets the TCG specification
- generated outside the TPM and inserted by a process defined in the Target of Evaluation (TOE) of the security target in use to evaluate the TPM.

2.4.5 Revocation of an EK Credential

If the private key of the EK is compromised, the EK Credential SHOULD be revoked.

An EK Credential MAY be revoked if an assertion changes and is no longer valid.

An EK Credential MAY be reissued if an assertion changes and is no longer valid.

When a discrepancy in a credential's assertion is determined to exist, the Privacy CA's policy SHOULD dictate how to resolve the discrepancy. For example, if the TPM's version changes (possibly due to a field upgrade) and therefore no longer matches the TPM Model field in the EK Credential, the Privacy CA may rely upon the TPM reported version information when determining if it trusts the requesting platform. This TPM reported version could also be substituted in subsequent AIK Credentials issued for the requestor.

2.4.6 Validity Period of an EK Credential

An EK Credential MAY contain field(s) that express the validity period of the credential. An EK Credential is not expected to expire during the normal life expectancy of the platform.

2.4.7 Assertions Made By an EK Credential

In general, an EK Credential asserts that the holder of the private EK is a TPM conforming to TCG specifications. Since the EK Credential is a public key credential, then by definition the signature of the issuer binds the public key material and the subject of the credential, which is a particular TPM model.

More specifically, an EK Credential asserts:

- Mandatory TPM specification compliance: The TPM model correctly implements the protected capabilities and shielded locations according to a particular version of the TCG specification set, especially the protection of the private Endorsement Key (EK). The “TPM model” must be fully described by the following three data items: TPM manufacturer, TPM model, and TPM version number. The TPM model values are manufacturer-specific.

- Optional TPM security assertions: The EK Credential may include assertions that it meets various evaluation conformance criteria or that it was manufactured or initialized under certain specified conditions.

To meet the assertion requirements listed above, an EK Credential MUST contain the following information fields:

- EK public key
- TPM model (TPM manufacturer, TPM model, and TPM version)

Note that the Unified Credential maybe used instead of an EK Credential in a deployment. The requirements for a Unified Credential are described in 2.7 and are different then the table below.

Field Name	Description	Field Status
Credential Type Label	Distinguish credential types issued under a shared key	MUST
Public EK	The TPM public Endorsement Key value	MUST
TPM Model	Manufacturer-specific identifier of the TPM component associated with the credential.	MUST
Issuer	Identifies the issuer of the credential	MUST
TPM Specification	Identifies the TPM Family and revision of the specification that this TPM implements	MUST
Signature Value	Signature of the issuer over the other fields	MUST
TPM Assertions	Security-related assertions about the TPM. This item maybe instantiated as in-line assertions within the credential or using the Unified Credentials as a reference to external information stored in another signed object (e.g. Reference Manifest or other credential.)	MAY
Validity Period	Time period when credential is valid	MAY
Policy Reference	Credential policy reference	MAY
Revocation Locator	Identifies source of revocation status information	MAY

Table 1: EK Credential Fields

2.4.7.1 Credential Type Label

The label enables the issuer to sign the credential with a key that is not reserved exclusively for signing an EK credential. It allows different types of credentials to be reliably distinguished from each other. TCPA reserved this flexible key re-purposing capability and the credential labels have been retained for compatibility.

For EK credentials, the value of this field must be the string, “TCPA Trusted Platform Module Endorsement”. Version 1.1 of this specification adds the Unified Credential (see section 2.7) which uses a numeric value (OID in an X.509 instance) to represent the credential type instead of a string. This new encoding MUST NOT be used in 1.0 credentials as it is specific to the new Unified Credential.

2.4.7.2 Public EK

The TPM public Endorsement Key value.

2.4.7.3 TPM Model

Identifies the implementation of the TPM when the Endorsement Key was first generated or inserted into the TPM.

There are three logical sub-fields: TPM manufacturer, TPM model, and TPM version.

TPM manufacturer identifies the manufacturer of the TPM. This value SHOULD be derived from the tpmVendorID field of the TPM_CAP_PROP_MANUFACTURER structure reported by the TPM[3].

The TPM model is encoded as a string and is manufacturer-specific.

The TPM version information is a manufacturer-specific implementation version of the TPM. This value SHOULD be derived from the revMajor and revMinor fields of the TPM_VERSION structure reported by the TPM[3].

2.4.7.4 Issuer

Identifies the entity that signed and issued the EK credential.

2.4.7.5 TPM Specification

Identifies the version of the TPM specification the implementation of the TPM was built to. The identification will be based on family level and revision.

2.4.7.6 Signature Value

The signature of the issuer over the other fields in the credential.

2.4.7.7 TPM Assertions

This field may contain assertions about the security properties of the issuance process and evaluations the manufacturing process or component have undertaken. For example, this field can declare: how the EK keys were generated, whether ISO 9000 processes were used/certified by the TPM manufacturer and information about Common Criteria evaluations performed.

Version 1.1 of this specification broadens how this information is associated with the credential by allowing the use of references to other credentials or signed documents which include this information. These references are beneficial in a number of situations such as avoiding the need for copying the assertions into many credentials associated with the same type of TPM component (manufacturer, model, version.) This way a TPM vendor might create per-TPM credentials that each reference a common signed objects with the shared assertions.

For more information, see Section 5, Entities, Assertions, and Signed Structures[2].

2.4.7.8 Validity Period

Enables the credential user to determine whether the EK Credential has begun to be valid and/or has expired. This is optional, so if it is not present then the credential is always valid from the time of issuance.

2.4.7.9 Policy Reference

Enables the credential user to identify the credential issuance policy of the EK Credential issuer.

2.4.7.10 Revocation Locator

Enables the credential user to determine whether the EK Credential has been revoked.

2.5 Platform Credential

A Platform Credential, also known as a “Platform Endorsement Credential” attests that a specific platform contains a unique TPM and Trusted Building Block (TBB).

A TBB consists of the parts of the Root of Trust that do not have shielded locations or protected capabilities. Normally, this includes just the Core Root of Trust for Measurement (CRTM) and the TPM initialization functions. The definition of a TBB is typically platform specific. One example of a TBB, specific to the PC Client platform, is the combination of CRTM, connection of the CRTM storage to the motherboard, and mechanisms for determining Physical Presence.

In general, the issuer of a Platform Credential is the platform manufacturer (for example, an OEM). An entity should not generate a Platform Credential unless the entity is satisfied that the platform contains the TPM referenced inside the credential. Platform Credentials only contain assertions about trust that a host platform manufacturer can typically make.

The consumer of a Platform Credential is a Privacy-CA. A Platform Credential contains information that the Privacy-CA may use in attesting to the integrity characteristics of a platform. The Privacy-

CA may copy field entries from the Platform Credential to a new AIK Credential that the Privacy-CA creates for a trusted platform.

2.5.1 Who Uses a Platform Credential?

A Privacy-CA is the only user of a Platform Credential. For more information, refer to section 6.2, Platform Credential[2].

2.5.2 Who Issues a Platform Credential?

Several different types of entities in the platform manufacturing supply chain may sign a Platform Credential. For more information, refer to section 3[2].

2.5.3 Platform Credential Privacy Protection Requirements

If the Platform Credential is stored on a platform after an Owner has taken ownership of that platform, it SHALL exist only in storage to which access is controlled and is available to authorized entities; this is to protect the privacy of the platform owner and the privacy of users of the platform. Access SHOULD be limited to those authorized to obtain an AIK Credential on the platform.

Access to the Platform Credential must be restricted to entities that have a "need to know." This is for reasons of privacy protection.

2.5.4 Revocation of a Platform Credential

If the platform is patched or upgraded, the existing Platform Credential SHOULD be invalidated and MAY be revoked. A replacement Platform Credential SHOULD be issued.

A Platform credential MAY be revoked if an assertion changes and is no longer valid.

A Platform credential MAY be reissued if an assertion changes and is no longer valid.

2.5.5 Validity Period of a Platform Credential

A Platform Credential is not expected to expire during the normal life expectancy of the platform.

2.5.6 Assertions Made by a Platform Credential

The following table lists all the fields that are central to the use of this credential type by TCG and which MUST or MAY be in a Platform Credential. Version 1.1 of this specification introduces the Unified Credential which might be used to carry the information normally housed in a Platform Credential. For Unified Credentials only, the meaning of the Field Status changes from requiring each field be present in the credential to the field needing to be present in the credential or one of its referenced items (e.g. other credentials.) See section 2.7 for the field requirements of the Unified Credential when replacing a Platform Credential.

Field Name	Description	Field Status
Credential Type Label	Distinguish credential types issued under a shared key	MUST
EK Credential	Identifies the associated EK Credential	MUST
Platform Model	Manufacturer-specific identifier	MUST
Issuer	Identifies the issuer of the credential	MUST
Platform Specification	Platform specification to which this platform is built	MUST
Signature Value	Signature of the issuer over the other fields	MUST

Field Name	Description	Field Status
Platform Assertions	Security assertions about the platform	MAY
Validity Period	Time period when credential is valid	MAY
Policy Reference	Credential policy reference	MAY
Revocation Locator	Identifies source of revocation status information	MAY

Table 2: Platform Credential Fields

2.5.6.1 Credential Type Label

The label enables the issuer to sign the credential with a key that is not reserved exclusively for signing a platform credential. It allows different types of credentials to be reliably distinguished from each other by this label instead of based on which signer key was used. TCPA reserved this flexible key re-purposing capability and the credential labels have been retained for compatibility.

For platform credentials, the value of this field must be the string, “TCPA Trusted Platform Endorsement”. Version 1.1 of this specification adds the Unified Credential (see section 2.7) which uses a numeric value (OID in an X.509 instance) to represent the credential type instead of a string. This new encoding MUST NOT be used in 1.0 credentials as it is specific to the new Unified Credential.

2.5.6.2 EK Credential

Used by the Privacy-CA to verify that the platform contains a unique TPM referenced by this Platform Credential.

This SHALL be an unambiguous indication of the EK Credential of the TPM incorporated into the platform.

2.5.6.3 Platform Model

Identifies the specific implementation of the platform. This is used by a Privacy-CA to verify that the platform contains a specific root of trust implementation.

There are three sub-fields: platform manufacturer, platform model, and platform version.

The platform manufacturer is encoded as a string and is manufacturer-specific.

The platform model is encoded as a string and is manufacturer-specific.

The platform version is encoded as a string and is the manufacturer-specific implementation version of the platform.

2.5.6.4 Issuer

Identifies the entity that signed and issued the Platform Credential.

2.5.6.5 Platform Specification

Identifies the TCG platform-specific specification the implementation of the platform was built to. This describes the platform class as well as the major and minor version number and the revision level.

2.5.6.6 Signature Value

The signature of the issuer over the other fields in the credential.

2.5.6.7 Platform Assertions

This field may contain assertions about the general security properties of the platform. This may be used by the credential user to verify that the platform implements acceptable security policies.

For more information, see Section 5, Entities, Assertions, and Signed Structures[2].

2.5.6.8 Validity Period

Enables the credential user to determine whether the Platform Credential has begun to be valid or has expired.

2.5.6.9 Policy Reference

Enables the credential user to identify the credential issuance policy of the Platform Credential issuer.

2.5.6.10 Revocation Locator

Enables the credential consumer to determine whether the Platform Credential has been revoked and should no longer be used as the basis for a trust decision.

2.6 Attestation Identity Key (AIK) Credential

An Attestation Identity Key (AIK) Credential contains the AIK public key and, optionally, any other information deemed useful by the issuer.

AIK Credentials are issued by a service known as a Privacy-CA that is trusted to verify the various credentials it receives during AIK issuance and to preserve privacy policies of the client. By issuing the AIK Credential, the signer attests to TPM authenticity by proving facts about the TPM. Goals of the proof are that the TPM owns the AIK and the AIK is tied to a valid EK Credential and a valid Platform Credential.

The trusted party that issues an AIK Credential further guarantees that it will abide by the privacy policies embodied in the Credential Practices Statement (CPS) document. For more information, refer to section 6.3, Attestation Identity (AIK) Credential[2] and section 3.3.4, Platform Identity Registration[2].

2.6.1 Who Uses an AIK Credential?

An AIK Credential is used in a Requestor-Verifier-Relying party protocol. The AIK credential is most commonly used to sign the quote information sent as part of an attestation.

For more information, see section 4, TP Deployment Infrastructure[2]. In particular, see section 4.5, Detailed Architecture for Deployment, section 4.5, [Platform Authentication] Abstract Entities, and section 4.6, Platform Authentication Flows. Also, see section 6.3, Attestation Identity Certificate, and section 8.5, Subject Key Attestation Evidence (SKAE). See the SKAE[4] specification for one use of an AIK Credential.

2.6.2 Who Issues an AIK Credential?

A Privacy-CA issues an AIK Credential upon a request from a TPM Owner provided the request meets the security requirements, AIK usage and other policies of the Privacy-CA. For more information, see section 3.3.4, Platform Identity Registration, and section 3.4.3[2].

2.6.3 Revocation of an AIK Credential

An AIK Credential MAY contain field(s) that enable revocation of the credential.

If the private key of the AIK is compromised or the private key of the TPM EK is compromised, the AIK credential SHOULD be revoked.

An AIK credential MAY be revoked if an assertion changes and is no longer valid.

An AIK credential MAY be reissued if an assertion changes and is no longer valid.

An example reason for a Privacy-CA to revoke an AIK Credential is the loss of the Privacy-CA signing key, an extremely low-probability event. Another example would be the exposure of the private TPM Endorsement Key value.

A TPM owner or Privacy-CA may choose to withdraw a previously-issued AIK Credential and issue a new replacement if the association of the AIK Credential to the EK or other AIK Credentials issued under the same EK becomes known. Rather than revoking the old credential it might simply be discarded and allowed to expire.

2.6.4 Validity Period of an AIK Credential

An AIK Credential MAY contain fields that express the validity period of the credential.

2.6.5 Assertions Made By an AIK Credential

An AIK Credential provides aliasing of platform identity; an AIK Credential is presented whenever an entity requires proof that an identity belongs to a platform that contains a platform root of trust of a general assurance level. In TCG terminology, a “platform root of trust” is the logical/physical binding of the Root of Trust for Measurement (RTM), Root of Trust for Storage (RTS), Root of Trust for Reporting (RTR), Root of Trust for Verification (RTV) and the Trusted Building Block (TBB).

In general, an AIK Credential asserts that the public AIK is associated with a valid TPM on a platform. More specifically, an AIK Credential contains the following four assertions:

- TPM properties: The AIK Credential contains an assertion by the Privacy-CA that an AIK is controlled by a TPM and, furthermore, attests to the properties of the TPM implementation that holds the AIK.
- TPM specification conformance: The AIK Credential contains an assertion by the Privacy-CA that the TPM bound to a platform conforms to TPM specifications for protected capabilities and shielded locations.
- Uniqueness: The AIK Credential contains an assertion by the Privacy-CA that the TPM contains a unique AIK pair.
- Privacy-CA evaluation process review: The AIK Credential contains an assertion by the Privacy-CA that a reviewable evidentiary path exists to support the above three assertions. For example, this could be proof that the Privacy-CA maintains an audit trail of the credential issuance process along with a reference to an audit trail maintained by the TPM manufacturer.

A Privacy-CA makes these and potentially other assertions in an AIK Credential.

This following table lists all the fields that must or may be in an AIK Credential. When a Unified Credential is used to replace an AIK (see section 2.7) it relaxes the requirement that these fields be directly included in the credential by allowing them to be inherited from other referenced credentials or Reference Manifests.

An AIK Credential MAY contain as much or as little information as dictated by requester and Privacy-CA issuer policy. The Privacy-CA must consult policy associated with the requestor to determine what information to include in the credential considering potential privacy matters. For instance, the Privacy-CA might decide to not include information about unique information about the platform in a Unified Credential filling the role of an AIK. TCG recommends that Privacy-CAs not include a reference to a Platform Credential or EK Credential (1.0 or Unified) that includes information unique to a specific platform for privacy reasons.

Field Name	Description	Field Status
Credential Type Label	Distinguish credential types issued under a shared key	MUST

Field Name	Description	Field Status
Public AIK	The public AIK value	MUST
TPM Model	Manufacturer-specific identifier	MUST
Platform Model	Manufacturer-specific identifier	MUST
Issuer	Identifies the issuer of the credential	MUST
TPM Specification	Identifies the specification this TPM conforms to	MUST
Platform Specification	Identifies the specification this platform conforms to	MUST
Signature Value	Signature of the issuer over the other fields	MUST
Identity Label	String associated with the AIK by the issuer	SHOULD
TPM Assertions	Security assertions about the TPM	MAY
Platform Assertions	Security assertions about the platform	MAY
Validity Period	Time period when credential is valid	MAY
Policy Reference	Credential policy reference	MAY
Revocation Locator	Identifies source of revocation status information	MAY

Table 3: AIK Credential Fields

2.6.5.1 Credential Type Label

The label enables the issuer to sign the credential with a key that is not reserved exclusively for signing an AIK credential. It allows different types of credentials to be reliably distinguished from each other by this label instead of based on which signer key was used. TCPA reserved this flexible key re-purposing capability and the credential labels have been retained for compatibility.

For AIK credentials, the value of this field must be the string, “TCPA Trusted Platform Identity”. Version 1.1 of this specification adds the Unified Credential (see section 2.7) which uses a numeric value (OID in an X.509 instance) to represent the credential type instead of a string. This new encoding MUST NOT be used in 1.0 credentials as it is specific to the new Unified Credential.

2.6.5.2 Public AIK

The public Attestation Identity Key.

2.6.5.3 TPM Model

This is a TPM model attribute, with field values correctly reflecting the current TPM implementation at the time of credential issuance.

This is expected to be a copy of the TPM model information from the EK credential. When the Unified Credential is used in the role of an AIK Credential, the model information can be established via references to other credentials. See section 2.7 for more information on the Unified Credential.

The AIK issuer includes the latest model information available at the time of issuance. This may differ from the model information presented to the Privacy-CA in the platform or EK credentials if the Privacy-CA can determine that the TPM has since been field upgraded to a later version.

2.6.5.4 Platform Model

For version 1.0 credentials, this is a copy of the platform model information from the platform credential. When a Unified Credential is deployed to fill the role of the platform credential, this platform model information could be missing and a verifier learns this information from a referenced credential or Reference Manifest. Because the platform model is not unique to a particular system (many systems of a particular model are normally manufactured) this allows each system to reference a common platform model description included in a Reference Manifest or previously issued credential. See section 2.7 for information about when a Unified Credential can be purposed to fill the role of an AIK Credential.

2.6.5.5 Issuer

Identifies the entity that signed and issued the AIK credential.

2.6.5.6 TPM Specification

Identifies the version of the TCG TPM specification the implementation of the TPM was built to.

The AIK issuer includes the latest version information available at the time of issuance. This may differ from the information presented to the Privacy-CA in the platform or EK certificates if the Privacy-CA can determine that the TPM has since been field upgraded to a later version.

2.6.5.7 Platform Specification

Identifies the version of the TCG platform-specific specification that the platform was built to meet (e.g. PC Client.) This describes the platform class as well as the major and minor version number and the revision level.

2.6.5.8 Signature Value

The signature of the issuer over the other fields in the credential.

2.6.5.9 Identity Label

Used by the issuer to associate this identity string with the AIK.

2.6.5.10 TPM Assertions

This field may contain assertions about the security properties of the TPM included within the platform associated with the credential. Generally these assertions are copied from the EK filtered by applicable privacy policies. These assertions can include information about how the EK keys were generated, independent assessment of the manufacturing processes (e.g. ISO 9000) and security evaluations (e.g. Common Criteria.)

Version 1.1 of this specification allows for Unified Credentials instances (e.g. X.509 Unified Certificate) to reference other credentials or signed documents (e.g. Security Qualities schema included in a Reference Manifest) that include this information avoiding the need to copy the information into each AIK credential.

2.6.5.11 Platform Assertions

This field may contain assertions about the general security properties of the platform. It may also describe the conformance evaluation process for the design and implementation of the platform. This may be used by a Privacy-CA to verify that the platform implements security policies in conformance with its CPS.

Version 1.1 introduces the Unified Credential that is capable of referencing other credentials and Reference Manifests containing Security Qualities that might include the Platform Assertions relevant to this AIK credential.

For more information, see Section 5, Entities, Assertions, and Signed Structures[2].

2.6.5.12 Validity Period

Enables the consumer of a Credential to determine whether the AIK Credential is currently valid (e.g. within the time range when it is valid.)

2.6.5.13 Policy Reference

Enables the consumer of an AIK Credential to determine the issuance policies followed by the Credential's issuer. . .

2.6.5.14 Revocation Locator

If present, enables the Credential user to determine whether the AIK credential has been revoked.

2.7 Unified Trust Credential

This new credential type is introduced in version 1.1 of this specification. The goal of this credential type is to offer a superset of the contents of the other credentials so they may all be represented in this single format easing credential issuance and parsing. This means that the supply chain and deployers have an alternative format to those described in 1.0 of this specification for describing the TPM, platform and attestation identities. Instances of the Unified Credential (e.g. X.509 below) will also include the ability to reference other credential's contents including other Unified Credentials, 1.0 credentials or even Reference Manifests (signed XML documents.)

The ability to reference instead of explicitly include allows the larger Unified Credential to actually be quite small since many of its fields are optional and possibly already asserted in another credential. For example, a Privacy CA might issue a Unified Credential acting as an AIK Credential with minimal information included instead leveraging sets of references to the non-platform unique (e.g. not including the public keys) qualities asserted in a Reference Manifest for the platform and/or TPM.

2.7.1 Who Uses a Unified Credential?

The Unified Credential can be consumed by wide variety of relying parties that typically use any of the three previously described version 1.0 TCG credentials. Because the Unified Credential might contain a wide variety of types of information, it is important that the credential consumer consider the role the particular Unified Credential is intending to fill (e.g. was it issued by a TPM manufacturer only asserting TPM properties.) Credential consumers benefit from this type of credential as it unifies the parsing code necessary to leverage its many possible contents.

2.7.2 Who Issues a Unified Credential?

The Unified credential can be created by a variety of parties in the supply chain. These parties are generally the same as those who created the EK, Platform and AIK Credentials in the pure 1.0 ecosystem as described in the TCG Infrastructure WG Reference Architecture document[2].

For example, a TPM manufacturer might issue a Unified Credential for each TPM instance it constructs. These credentials might all reference a single common Reference Manifest which asserts the security qualities of the entire model line. Later an OEM including the TPM into a platform might issue another Unified Credential which references the TPM manufacturer's Unified Credential creating a credential list. Finally, an IT department might decide to issue its own Unified Credential including deployment specific assertions about the platform and also includes references to the OEM and TPM manufacturers' credentials.

2.7.3 Revocation of a Unified Credential

A Unified Credential MAY contain field(s) that enable revocation of the credential.

If the private key of the Unified Credential is compromised or the private key signer of the credential is compromised, the Unified credential SHOULD be revoked.

Unified Credentials frequently include or reference information (e.g. security assertions.) Over time this information may change and no longer represent an accurate depiction of the security

properties of the component. Should this occur, a new credential MAY be issued and the prior credential SHOULD be revoked if it poses a potential security risk.

An example reason for a Privacy-CA to revoke a Unified Credential acting as an AIK Credential is the compromise of the Privacy-CA signing key potentially allowing an untrustworthy party to forge credentials. Another example would be the exposure of the private TPM Endorsement Key value.

A TPM owner or Privacy-CA may choose to withdraw a previously-issued AIK Credential and issue a new replacement if the association of the AIK Credential to the EK or other AIK Credentials issued under the same EK becomes known. Rather than revoking the old credential it might simply be discarded and allowed to expire.

2.7.4 Validity Period of an Unified Credential

An AIK Credential MAY contain fields that express the validity period of the credential. This establishes an upper bound on the time a credential may be relied upon and might ease the length of time a revoked credential needs to be maintained on a CRL or OCSP server.

2.7.5 Assertions Made by a Unified Credential

A Unified Credential is largely a union of the information that can be included in an EK, AIK and Platform Credential. Therefore the set of assertions which can be made by those credentials represents the list of assertions possible in a Unified Credential. See sections 2.3.7, 2.4.6 and 2.5.5 for a complete description of the assertions possible with each credential type.

3 X.509 ASN.1 Definitions

This section contains the format for each credential instantiated as an X.509 certificate for all the common and information fields in all four TCG credential types defined in this specification. All fields are defined in ASN.1 and encoded using DER.

Version 1.1 of this specification introduces the Unified Credential that offers a common format across all the credentials and may be issued instead of the 1.0 EK, Platform and AIK Credentials. The Unified Credential also offers more flexibility in leveraging information stored in other documents and credentials relevant to the described entity.

Version 3 of the X.509 certificate structure can be leveraged to dovetail TCG credentials into existing PKI tools and services. TCG credential profiles do not utilize all aspects of X.509 defined fields and some fields are overloaded with TCG specific interpretations. The following sections define TCG interpretations for X.509 certificates.

The TCG EK and AIK certificate syntax conforms to the definition for public key certificates in X.509. The TCG Platform syntax conforms to the definition for attribute certificates in X.509.

TCG defines a number of new attribute value types to hold TCG-specific values. When present in a public key certificate they are carried in a Subject Directory Attributes extension.

This specification is a profile of RFC 3280[9] and RFC 3281[10] which are themselves profiles of the ISO/IEC/ITU-T X.509 specifications for public key and attribute certificates. All syntax and semantics are inherited from those specifications unless explicitly documented otherwise below.

3.1 TCG Attributes

3.1.1 Security Qualities

This attribute describes the TPM security qualities in the EK certificate or the platform security qualities in the platform certificate.

The text string describing the qualities of the TPM is manufacturer-specific. This attribute is deprecated but is retained for compatibility with TCPA. If present, the security qualities attribute, which has manufacturer-specific syntax, should be consistent with any TPM Assertions(Table 4) or Platform Assertions(Table 5) attributes in the certificate.

```
securityQualities ATTRIBUTE ::= {
    WITH SYNTAX SecurityQualities
    ID tcg-at-tpmSecurityQualities }

SecurityQualities ::= SEQUENCE {
    version INTEGER,
    -- version 0 defined by TCPA 1.1b
    statement UTF8String }
```

3.1.2 TPM and Platform Assertions

These two attributes describe security-related assertions about the TPM or platform TBB.

These attributes replace the Security Qualities attribute from TCPA 1.1b which has been deprecated but retained for compatibility.

Each attribute begins with a version number which identifies the version of the assertion syntax. Future versions of this profile may add new assertions by appending new fields at the end of the

ASN.1 SEQUENCE and increasing the version number to identify which version of the assertion syntax is encoded.

The **fieldUpgradable** BOOLEAN indicates whether the TPM is capable of having its firmware upgraded after manufacturing.

The **ekGenerationType** indicates how the Endorsement Key in the TPM was created. It may be internally generated within the TPM, generated externally and then inserted under a controlled environment during manufacturing. The revocable variants indicate whether the EK was created consistent with the TPM_CreateRevocableEK command.

The **MeasurementRootType** indicates which types of Root of Trust for Measurement are implemented as part of the platform TBB. A Static RTM is required and support for a dynamic RTM is optional.

In the **CommonCriteriaMeasures**, the profile and target for the evaluation can be described by either an OID, a URI to a document describing the value, or both. If both are present, they must represent consistent values. The URI values are included in an **URIReference** which describes the URI to the document and a cryptographic hash value which identifies a specific version of the document.

URIMAX is a constant used to provide an upper bound on the length of a URI included in the certificate. This upper bound may be helpful to consumers of the extension and also helps limit the overall size of the certificate. In order to provide a reasonable upper bound for ASN.1 parsers, URIMAX SHOULD NOT exceed a value of 1024. This value was selected as it matches the length limit for <A> anchors in HTML as specified by the SGML declaration (LITLEN) for HTML[13].

STRMAX is a constant defining the upper bound on the length of a string type. Like the URIMAX this is to aid ASN.1 parsers and help limit the upper bound on the length of the certificate. Based on the expected sizes of the strings in the ASN.1 in this document an upper bound of 256 was selected. STRMAX SHOULD NOT exceed a value of 256.

```
Version ::= INTEGER { v1(0) }

tPMSecurityAssertions ATTRIBUTE ::= {
    WITH SYNTAX TPMSecurityAssertions
    ID tcg-at-tpmSecurityAssertions }

TPMSecurityAssertions ::= SEQUENCE {
    version Version DEFAULT v1,
    fieldUpgradable BOOLEAN DEFAULT FALSE,
    ekGenerationType [0] IMPLICIT EKGenerationType OPTIONAL,
    ekGenerationLocation [1] IMPLICIT EKGenerationLocation OPTIONAL,
    ekCertificateGenerationLocation [2] IMPLICIT
        EKCertificateGenerationLocation OPTIONAL,
    ccInfo [3] IMPLICIT CommonCriteriaMeasures OPTIONAL,
    fipsLevel [4] IMPLICIT FIPSLevel OPTIONAL,
    iso9000Certified [5] IMPLICIT BOOLEAN DEFAULT FALSE,
    iso9000Uri IA5STRING (SIZE (1..URIMAX) OPTIONAL }

tBBSecurityAssertions ATTRIBUTE ::= {
    WITH SYNTAX TBBSecurityAssertions
```

```
    ID tcg-at-tbbSecurityAssertions }

TBBSecurityAssertions ::= SEQUENCE {
    version Version DEFAULT v1,
    ccInfo [0] IMPLICIT CommonCriteriaMeasures OPTIONAL,
    fipsLevel [1] IMPLICIT FIPSLevel OPTIONAL,
    rtmType [2] IMPLICIT MeasurementRootType OPTIONAL,
    iso9000Certified BOOLEAN DEFAULT FALSE,
    iso9000Uri IA5STRING (SIZE (1..URIMAX) OPTIONAL }

EKGenerationType ::= ENUMERATED {
    internal (0),
    injected (1),
    internalRevocable(2),
    injectedRevocable(3) }

EKGenerationLocation ::= ENUMERATED {
    tpmManufacturer (0),
    platformManufacturer (1),
    ekCertSigner (2) }

EKCertificateGenerationLocation ::= ENUMERATED {
    tpmManufacturer (0),
    platformManufacturer (1),
    ekCertSigner (2) }

-- V1.1 of this specification adds hybrid and physical.
-- Hybrid means the measurement root is capable of static AND dynamic
-- Physical means that the root is anchored by a physical TPM
-- Virtual means the TPM is virtualized (possibly running in a VMM).
-- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
-- the capabilities of the platform.
MeasurementRootType ::= ENUMERATED {
    static (0),
    dynamic (1),
    nonHost (2),
    hybrid (3),
    physical (4),
    virtual (5) }


-- common criteria evaluation
```

```
        CommonCriteriaMeasures ::= SEQUENCE {
            version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined
by CC
            assurancelevel EvaluationAssuranceLevel,
            evaluationStatus EvalutionStatus,
            plus BOOLEAN DEFAULT FALSE,
            strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
            profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
            profileUri [2] IMPLICIT URIReference
         OPTIONAL,
            targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
            targetUri [4] IMPLICIT URIReference OPTIONAL }

        EvaluationAssuranceLevel ::= ENUMERATED {
            level1 (1),
            level2 (2),
            level3 (3),
            level4 (4),
            level5 (5),
            level6 (6),
            level7 (7) }

        StrengthOfFunction ::= ENUMERATED {
            basic (0),
            medium (1),
            high (2) }

        -- Reference to external document containing information relevant to this subject.
        -- The hashAlgorithm and hashValue MUST both exist in each reference if either
        -- appear at all.
        URIReference ::= SEQUENCE {
            uniformResourceIdentifier IA5String (SIZE (1..URIMAX),
            hashAlgorithm AlgorithmIdentifier OPTIONAL,
            hashValue BIT STRING OPTIONAL }

        EvaluationStatus ::= ENUMERATED {
            designedToMeet (0),
            evaluationInProgress (1),
            evaluationCompleted (2) }

        -- fips evaluation

        FIPSLevel ::= SEQUENCE {
```

```
    version IA5STRING (SIZE (1..STRMAX)), -- "140-1" or "140-2"
    level SecurityLevel,
    plus BOOLEAN DEFAULT FALSE }

SecurityLevel ::= ENUMERATED {
    level1 (1),
    level2 (2),
    level3 (3),
    level4 (4) }
```

3.1.3 Conformance Attributes

The syntax of the protection profile and security target attributes. These attributes are deprecated and replaced with the TPM and Platform Assertion attributes. They MAY be present for compatibility with TCPA.

```
ProtectionProfile ::= OBJECT IDENTIFIER
SecurityTarget ::= OBJECT IDENTIFIER

TPMProtectionProfile ATTRIBUTE ::= {
    WITH SYNTAX ProtectionProfile
    ID tcg-at-tpmProtectionProfile }

TPMSecurityTarget ATTRIBUTE ::= {
    WITH SYNTAX SecurityTarget
    ID tcg-at-tpmSecurityTarget }

TBBProtectionProfile ATTRIBUTE ::= {
    WITH SYNTAX ProtectionProfile
    ID tcg-at-tbbProtectionProfile }

TBBSecurityTarget ATTRIBUTE ::= {
    WITH SYNTAX SecurityTarget
    ID tcg-at-tbbSecurityTarget }
```

3.1.4 Name Attributes

The following definitions define the syntax of the relative distinguished names (RDNs) used in the subject alternative name extension to identify the type of the TPM and the platform.

The value of the **TPMManufacturer** attribute SHOULD be the ASCII representation of the hexadecimal value of the 4 byte vendor identifier defined in 2.3.7.3, TPM Model. Each byte is represented individually as a two digit unsigned hexadecimal number using the characters 0-9 and A-F. The result is concatenated together to form an 8 character name which is appended after the lower-case ASCII characters "id:". The attribute MAY instead use a manufacturer-specific name for backwards compatibility with earlier practice.

For example, the vendorId 0x12 0x34 0x56 0xEF would be encoded as "id:123456EF".

Likewise, the value of the **TPMVersion** attribute SHOULD be the ASCII representation of the hexadecimal value of the 2 bytes derived from "revMajor" and "revMinor" as defined in 2.3.7.3, TPM Model. Each byte is represented individually as a two digit unsigned hexadecimal number

using the characters 0-9 and A-F. The result is concatenated together to form a 4 character name which is appended after the lower-case ASCII characters “id:”. The attribute MAY instead use a manufacturer-specific name for backwards compatibility with earlier practice.

For example, a revMajor of 0x02 and revMinor of 0x08 would be encoded as “id:0208”.

The value of the **`TPMModel`** attribute is a UTF 8 string with manufacturer-specific values.

The value of the **`PlatformManufacturer`**, **`PlatformModel`**, and **`PlatformVersion`** attributes are UTF 8 strings with manufacturer-specific values.

```
TPMManufacturer ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-tpmManufacturer }

TPMModel ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-tpmModel }

TPMVersion ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-tpmVersion }

PlatformManufacturer ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-platformManufacturer }

PlatformModel ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-platformModel }

PlatformVersion ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-platformVersion }
```

3.1.5 TCG Specification Attributes

The following definitions define the syntax of the TPM and platform-specific specification attributes.

The **`TCPASpecVersion`** attribute identifies the specification implemented by the TPM at the time of Endorsement Key generation. It has been deprecated in favor of new TPM and platform-specific attributes which support newer TCG specification naming conventions.

```
tCPASpecVersion ATTRIBUTE ::= {
    WITH SYNTAX TCPASpecVersion
    ID tcg-tcpaSpecVersion }

TCPASpecVersion ::= SEQUENCE {
    major INTEGER,
```

```
    minor INTEGER }
```

The **TPMSpecification** attribute identifies the TPM family, level and revision of the TPM specification with which a TPM implementation is compliant. The family value of "1.1" with level 1 and revision 2 identifies a TPM compliant with TCPA 1.1b. A family value of "1.2" with level 2 and revision 85 identifies a newer public TPM specification published by TCG. The family value is encoded in a UTF 8 string but the current defined standard values fall within the ASCII character set.

```
tPMSpecification ATTRIBUTE ::= {
    WITH SYNTAX TPMSpecification
    ID tcg-at-tpmSpecification }

TPMSpecification ::= SEQUENCE {
    family UTF8String (SIZE (1..STRMAX)),
    level INTEGER,
    revision INTEGER }
```

The **TCGPlatformSpecification** attribute identifies the platform class, version and revision of the platform-specific specification with which a platform implementation is compliant. Standardized four byte platform class values are defined in each platform-specific specification document.

```
tCGPlatformSpecification ATTRIBUTE ::= {
    WITH SYNTAX TCGPlatformSpecification
    ID tcg-at-tcgPlatformSpecification }

TCGSpecificationVersion ::= SEQUENCE {
    majorVersion INTEGER,
    minorVersion INTEGER,
    revision INTEGER }

TCGPlatformSpecification ::= SEQUENCE {
    Version TCGSpecificationVersion,
    platformClass OCTET STRING SIZE(4) }
```

3.1.6 References to Other Relevant Credentials

Version 1.1 of this specification adds the notion of referencing pre-existing credentials or signed assertions relevant to this platform (or component.) Because the new Unified Credential may be issued multiple times during the supply chain (e.g. by an IT department) it may wish to reference assertions made in prior credentials or Reference Manifests potentially signed by a more credible party.

For instance a well known TPM vendor may create an EK credential containing information unique to this TPM and a Reference Manifest with assertions pertaining to all TPMs of this model/version. Each of the TPM instance specific Unified Credentials can reference the single Reference Manifest describing common properties of the component.

Later in the supply chain, an OEM including this TPM part in a platform may wish to issue its own Unified Credential and offer its own Reference Manifest covering common security properties of the

platform. This newly issued credential could reference the prior TPM vendor issued credential and Reference Manifest to give strength to its claims about the security of the TPM attached to the platform (rather than copying the attributes into a credential signed by the OEM.)

Much later an IT department may wish to issue a unified credential that references some or all of the prior credentials and Reference Manifests and for the same reason not wish to copy their authoritative information into the new credential covered by the IT department's signature.

The unordered list of references to other credentials or manifests may be included in the TCG defined Relevant Certificates and Relevant Manifests X.509 extensions. The list of prior credentials can be identified by the OID tcg-ce-relevantCredentials value. Similarly the list of relevant Reference Manifests can be recognized by the OID tcg-ce-relevantManifests. The associated data element for each OID is a list of references to other data objects that contain relevant information. Each reference SHOULD include a hash value of the document that reflects the content of the document at the time of certificate issuance. This allows a verifier to determine if the currently referenced document differs and might make different assertions about the subject.

The detailed content of the URI references is not specified and is likely to be situation dependent. It's expected that when a reference is to another certificate, the URI MAY contain information about the certificates CA issuer and its serial number to aid in lookup and recognition of the certificate.

The use of references rather than in-lined data within the certificate implies that relying parties have the ability to fetch (or pre-store) this information via some mechanism, thus it is likely that additional infrastructure is necessary.

The following ASN.1 describes the list of URI references to information about the subject that may be included in a Relevant Certificates or Relevant Manifests certificate extension:

```
HashAlgAndValue ::= SEQUENCE {
   hashAlg         AlgorithmIdentifier,
   hashValue       OCTET STRING }

HashedSubjectInfoURI  ::=  SEQUENCE {
   documentURI IA5String (SIZE (1..URIMAX)),
   documentAccessInfo OBJECT IDENTIFIER OPTIONAL,
   documentHashInfo HashAlgAndValue OPTIONAL }

SubjectInfoURIList  ::=
   SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI

TCGRelevantCredentials ::=

   SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI


TCGRelevantManifests   ::=

   SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI
```

REFMAX is a constant used to provide an upper bound on the URI list. This upper bound may be helpful to consumers of the extension and also helps limit the overall size of the certificate. In order to provide a reasonable upper bound for ASN.1 parsers, REFMAX SHOULD NOT exceed a value of 32.

Because a URI might be a reference to a specific document or certificate or may reference an intermediary service interface that is used to provide the desired information, each HashedSubjectInfoURI MAY include information about what type of reference is provided (encoded as an OID in the documentAccessInfo element. For TCGRelevantCredentials this might be the certificate type OID allowing for verifiers to keep separate databases of each certificate to ease processing.

If the TCGRelevantCredentials is included in a certificate it MUST include a set of references to existing X.509 certificates that contain relevant information to this subject of the certificate. Ideally

the information included in these referenced certificates would not overlap with this parent level certificate or other referenced certificates, but should this occur the relying parties MUST consider the most recently issued certificate's information as authoritative (normally this is the parent.) This is essential for consistent evaluation of an entity's credentials across different situations and relying parties.

Equivalent to the TCGRelevantCredentials extension is the TCGRelevantManifests list of references which is optional but if present MUST include a set of references to Reference Manifests containing relevant information to this subject of this certificate. Duplicate information must be treated in the same way as described for the certificates in the prior paragraph.

3.2 EK Certificate

This section contains the format for an EK Credential conforming to version 1.0 of this specification. The specification of the Unified Credential which may also fill this role is defined in section 3.5.

An X.509 EK certificate is an instantiation of the TPM EK Credential defined in section 2.3.

Notes:

- Some fields are assigned a value even though the certificate user performs no action based on that value. In such cases, the intention is to inhibit non-TCG implementations from making inappropriate use of the certificate.
- It is intended that the lifetime of a TPM will be shorter than the crypto-period of the TPM endorsement public and private keys. Therefore, keys are not "rolled-over".

The value Standard in Field Status column in the table below means the field is an inherent component of the standard certificate syntax and is not optional.

Field/Extension Name	Description	Field Status
Version	Certificate syntax version number	Standard
Serial Number	Positive integer value unique relative to the issuer	Standard
Signature Algorithm	Algorithm used by the issuer to sign this certificate	Standard
Issuer	Distinguished name of the EK certificate issuer	Standard
Validity	Time interval during which the certificate is valid	Standard
Subject	Distinguished name of the certificate	Standard
Public Key Info	Identifier of the algorithm for the public key	Standard
Extensions	Contains a set of additional attributes to be associated with the certificate's entity.	MUST
Certificate Policies	Policy terms under which the certificate was issued	MUST
Subject Alternative Name	Name forms other than directory distinguished names for entity represented by certificate	MUST
Basic Constraints	CA certificate indicator and path constraints	MUST

Field/Extension Name	Description	Field Status
Subject Directory Attributes	Various device characteristics	MUST
Authority Key Id	Identifies the subject public key of the certificate issuer	SHOULD
Authority Info Access	Indicates how to access CA information	MAY
CRL Distribution	Indicates how to access CRL information	MAY
Key Usage	Indicates the intended use of the subject public key	SHOULD NOT
Extended Key Usage	Indicates the intended use of the subject public key	SHOULD NOT
Subject Key Id	Identifies the subject public key of the certificate	SHOULD NOT
Issuer Alternative Name	Used to associate Name forms other than distinguished names for the issuer of the certificate	SHOULD NOT
Freshest CRL	Identifies how delta CRL information is obtained	SHOULD NOT
Subject Information Access	Indicates how to access additional information and services associated with the certificate entity.	SHOULD NOT
Subject Unique Id	Unique value when using a shared a subject name	SHOULD NOT
Issuer Unique Id	Unique value when using a shared a issuer name	SHOULD NOT
Virtual Platform Backup Service URI	Provides a URI to the virtualized TPM backup service in case a remote challenger wishes to evaluate the restore policies to avoid rollback attacks. This extension also includes the restoreAllowed flag to indicate if a restore is possible under any circumstances.	SHOULD only for virtualized TPM with a backup authority

Table 4: EK Certificate Fields

3.2.1 Version

This field contains the version of the certificate syntax. Since EK certificates always contain mandatory extensions the version number must be set to 3 (which is encoded as the value 2 in ASN.1).

3.2.2 Serial Number

The serial number MUST be a positive integer which is uniquely assigned to each EK certificate by the issuer. The combination of an issuer's DN and the serial number MUST uniquely describe a single certificate.

3.2.3 Signature Algorithm

This OID identifies the algorithm used by the EK certificate issuer to sign the certificate. EK certificate verifiers MUST support certificates signed using a 2048 bit key with the algorithm sha-

1WithRSAEncryption which has the OID value shown below. The AlgorithmIdentifier parameters field MUST be the ASN.1 type NULL.

```
sha-1WithRSAEncryption OBJECT IDENTIFIER  ::=  {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5  }
```

3.2.4 Issuer

This field contains the distinguished name of the TPM endorsement entity which is the entity that asserts that the subject TPM conforms to the TCG specification. (Note: this may not always be the TPM manufacturer. See section 3 of the TCG Reference Architecture for Interoperability[2].

3.2.5 Validity

The period when the binding of the certificate's contents is valid is represented by two date values named notBefore and notAfter. Issuers SHOULD assign notBefore to the current time when the EK certificate is issued and notAfter to the last date that the certificate will be considered valid. Both notBefore and notAfter MUST use the appropriate time format as indicated by RFC 3280, section 4.1.2.5.

3.2.6 Subject

The subject distinguished name MUST be empty.

Issuers MUST use the subject alternative name extension instead.

3.2.7 Public Key Info

Describes the public Endorsement Key algorithm and key value.

The algorithm OID shown below MUST be supported for interoperability.

```
id-RSAES-OAEP OBJECT IDENTIFIER  ::=  {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 7 }
```

The AlgorithmIdentifier parameters field MUST be present, and the parameters field MUST contain RSAES-OAEP-params as defined in section A.2.1 of RFC 3447[11]. The "pSourceFunc" parameters field MUST contain the OID id-pSpecified with an octet string value of "TCPA" as required by the TPM Design Principles in section 31.1.1[3]. For backwards compatibility, a terminating zero-valued character in such a string should be ignored if it is present.

3.2.8 Certificate Policies

Indicates policy terms under which the certificate was issued.

Assign "critical" the value TRUE. Assign policyIdentifier at least one object identifier. Assign the cPSuri policy qualifier the value of an HTTP URL at which a plain language version of the TPM endorsement entity's certificate policy may be obtained. Assign the explicit text userNotice policy qualifier the value "TCPA Trusted Platform Module Endorsement".

During certificate path validation, check that at least one acceptable policyIdentifier value is present. The Privacy-CA SHOULD transfer the acceptable policyInformation value to the AIK certificate "certificate policies" extension.

3.2.9 Subject Alternative Names

This contains the alternative name of the entity associated with this certificate. Assign "critical" the value TRUE. Include the TPM identity, using the directory name-form with RDNs for the TPM manufacturer, model and version numbers. During certificate validation, the Privacy-CA MUST check that the TPM manufacturer, model and version numbers are acceptable. If so, it should transfer to the new TPM identify certificate the "subject alternative name" extension value for the TPM.

3.2.10 Basic Constraints

This indicates whether the subject is a CA. Assign “critical” the value TRUE. Assign “CA” the value FALSE.

3.2.11 Subject Directory Attributes

The extension includes miscellaneous properties and security assertions about the entity. The extension SHOULD be non-critical.

The following attribute MUST be included in a Subject Directory Attributes extension in the EK Certificate:

- The “TPM Specification” attribute which identifies the family and revision of the TCG TPM specification to which the TPM was designed.

The following attributes SHOULD be included in a Subject Directory Attributes extension in the EK Certificate:

- The multi-valued attribute “supported algorithms” (see X.509) which SHOULD include object identifiers for the algorithms RSAES-OAEP, SHA-1 (1.3.14.3.2.26), and other algorithms implemented by the TPM.
- The “TPM Security Assertions” attribute which describes various assertions about the security properties of the TPM and the conditions under which the Endorsement Key was generated.

The following attributes are documented for compatibility with TCPA but SHOULD NOT be included in EK Certificates (see Changes Since TCPA 1.1b):

- The "TCPA Specification Version" attribute, with field values correctly reflecting the highest version of the TCG specification with which the TPM implementation conforms.
- The "security qualities" attribute with a text string reflecting the security qualities of the TPM.

3.2.12 Authority Key Id

This identifies the subject public key of the certificate issuer. Assign “critical” the value FALSE. Assign the value of “subject key identifier” from the issuer’s public-key certificate, if available, else omit.

3.2.13 Authority Info Access

This contains additional information about the issuer. This extension MAY be omitted. If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 3280[9]) and the accessLocation value SHOULD point to the access value of the OCSP responder (HTTP URI).

The relying party can access the certificate status for this certificate by sending a properly formatted OCSPRequest to the URI. If both a CDP and OCSP AIA extension are present in the certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

3.2.14 CRL Distribution

This provides the location of the subject’s revocation information. The relying party can access the CRL for this certificate from this URI. If both a CDP and OCSP AIA extension are present in the certificate, then relying parties SHOULD use OCSP as the primary validation mechanism.

3.2.15 Key Usage

If present, this extension indicates the intended purpose of the subject public key. It SHOULD NOT be included in EK certificates. If present, the key encipherment bit SHOULD be set and the extension SHOULD be marked critical.

3.2.16 Extended Key Usage

If present, this extension indicates the intended purpose of the subject public key. It SHOULD NOT be included in EK certificates. If a certificate includes this extension and it is marked CRITICAL then reject the certificate during path validation if the extended key usage is not understood.

3.2.17 Subject Key Id

Identifies the public key of the certificate. This extension SHOULD NOT be included in EK certificates.

3.2.18 Issuer Alternative Names

This is used to associate Internet style identities with the certificate issuer. This extension SHOULD NOT be included in EK certificates.

3.2.19 Freshest CRL

The freshest CRL extension identifies how delta CRL information is obtained. This extension SHOULD NOT be included in EK certificates.

3.2.20 Subject Information Access

The subject information access extension indicates how to access information and services for the subject of the certificate in which the extension appears. This extension SHOULD NOT be included in EK certificates.

3.2.21 Subject and Issuer Unique Ids

These uniquely identify certificates which share names with other certificates issued by the same issuer. Under this specification these fields MUST be omitted.

3.2.22 Virtual Platform Backup Service

This extension is only for use in EK and AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI to the backup authority if one exists that is capable of restoring a complete virtualized TPM instance. The restore of a TPM instance could pose a rollback attack, so remote challengers may wish to attest the operation and policies of the backup authority as part of its trust decisions. The restoreAllowed element indicates whether the virtual TPM associated with this entity could ever have a restored VPM instance (thus a potential rollback concern).

3.3 Platform Certificate

This section contains the format for a Platform Credential conforming to version 1.0 of this specification. The specification of the Unified Credential which may also fill this role is defined in section.

The Platform Certificate makes the assertions listed in section 2.4.6. The platform certificate format is a profile of RFC 3281[10] and all requirements and limitations from that specification apply unless otherwise noted.

Note: some fields are assigned a value even though the certificate user performs no action with that value. In such cases, the intention is to inhibit non-TCG implementations from making inappropriate use of the certificate.

Field Name	Description	Field Status
Version	Certificate syntax version number	Standard
Serial Number	Positive integer value unique relative to the issuer	Standard
Signature Algorithm	Algorithm used by the issuer to sign this certificate	Standard
Holder	Identity of the associated TPM EK Certificate	Standard
Issuer	Distinguished name of the platform certificate issuer	Standard
Validity	Time interval during which the certificate is valid	Standard
Attributes	Information about the platform of this certificate	Standard
Extensions	Includes additional attributes associated with certificate	MUST
Certificate Policies	Policy terms under which the certificate was issued	MUST
Subject Alternative Names	Name forms other than directory distinguished names.	MUST
Authority Key Id	Identifies the subject public key of the certificate issuer	SHOULD
Authority Info Access	Indicates how to access CA information	MAY
CRL Distribution	Indicates how to access CRL information	MAY
Issuer Unique Id	Unique value when using a shared issuer name	SHOULD NOT

Table 5: Platform Certificate Fields

3.3.1 Version

This field contains the version of the certificate syntax. Since platform certificates always contain mandatory extensions the version number must be set to 2 (which is encoded as the value 1 in ASN.1).

3.3.2 Serial Number

The serial number MUST be a positive integer which is uniquely assigned to each certificate by the issuer. The combination of an issuer's DN and the serial number MUST uniquely describe a single certificate.

Assign a value unique per instance of a TBB amongst all certificates issued by "issuer".

3.3.3 Signature Algorithm

This OID identifies the algorithm used by the platform certificate issuer to sign the certificate. Platform certificate verifiers MUST support certificates signed using a 2048 bit key with the algorithm sha-1WithRSAEncryption which has the OID value shown below. The AlgorithmIdentifier parameters field MUST be the ASN.1 type NULL.

```
sha-1WithRSAEncryption OBJECT IDENTIFIER  ::=  {
```

```
iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5  }
```

3.3.4 Holder

This contains a reference to the X.509 certificate of the TPM EK certificate. The BaseCertificateID choice MUST be used.

3.3.5 Issuer

This field contains the distinguished name of the entity that issued this platform certificate. This is the entity that asserts that the platform incorporates a TPM and RTM in a manner that conforms to the TCG specification.

3.3.6 Validity

This contains the period during which the binding between the attributes and TPM EK certificate is considered valid. It is represented by two date values named notBefore and notAfter. Issuers should assign notBefore to the current time when the certificate is issued and notAfter to the last date that the certificate will be considered valid. Both notBefore and notAfter MUST use the appropriate time format as indicated by RFC 3280, section 4.1.2.5.

3.3.7 Certificate Policies

Indicates policy terms under which the certificate was issued.

Assign “critical” the value TRUE. Assign policyIdentifier at least one object identifier. Assign the cPSuri policy qualifier the value of an HTTP URL at which a plain language version of the platform endorsement entity’s certificate policy may be obtained. Assign the explicit text userNotice policy qualifier the value “TCPA Trusted Platform Endorsement”.

During certificate path validation, check that at least one acceptable policyIdentifier value is present. The Privacy-CA SHOULD transfer the acceptable policyInformation value to the AIK certificate “certificate policies” extension.

3.3.8 Subject Alternative Names

This contains the alternative name of the entity associated with this certificate. Assign "critical" the value TRUE. Include the platform model, using the directory name-form with RDNs for the platform manufacturer, model and version numbers.

During certificate validation, the Privacy-CA MUST check that the platform manufacturer, model and version numbers are acceptable. If so, it should transfer these values to the “subject alternative name” extension of the new AIK certificate.

3.3.9 Attributes

The following attributes SHOULD be included:

- The “TCG Platform Specification” attribute references the platform class, version and revision level of the TCG platform-specific specification to which the platform was designed.
- The platform “TBB Security Assertions” attribute describes various assertions about the security properties of the TBB of the platform.

The following attributes are documented for compatibility with TCPA but SHOULD NOT be included in Platform Certificates (see Changes Since TCPA 1.1b):

- The "TCPA Specification Version" attribute, with field values correctly reflecting the highest version of the TCG specification with which the TPM implementation conforms.
- If the TPM has been successfully evaluated against a Common Criteria protection profile, then include the TPM protection profile identifier attribute.

- If the TPM has been successfully evaluated against a Common Criteria security target, then include the TPM security target identifier attribute.
- If the RTM and the means by which the TPM and RTM have been incorporated into the platform have been successfully evaluated against a Common Criteria protection profile, then include the "TBB protection profile" identifier attribute.
- If the RTM and the means by which the TPM and RTM have been incorporated into the platform have been successfully evaluated against a Common Criteria security target, then include the "TBB security target" identifier attribute.
- Optionally, include the "security qualities" attribute with a text string reflecting the security qualities of the platform.

3.3.10 Authority Key Identifier

This identifies the subject public key of the certificate issuer. Assign “critical” the value FALSE. Assign the value of “subject key identifier” from the issuer’s public-key certificate, if available, else omit.

3.3.11 Authority Info Access

This contains additional information about the issuer. It MAY be omitted. If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 3280[9]) and the accessLocation value SHOULD point to the access value of the OCSP responder (HTTP URI).

The relying party can access the certificate status for this certificate by sending a properly formatted OCSPRequest to the URI. If both a CDP and OCSP AIA extension are present in the certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

3.3.12 CRL Distribution

This provides the location of the subject’s revocation information. The relying party can access the CRL for this certificate from this URI. If both a CDP and OCSP AIA extension are present in the certificate, then relying parties SHOULD use OCSP as the primary validation mechanism.

3.3.13 Issuer Unique Id

These uniquely identify certificates which share names with other certificates issued by the same issuer. Under this specification these fields MUST be omitted.

3.4 AIK Certificate

This section contains the format for an AIK Credential conforming to version 1.0 of this specification. The specification of the Unified Credential which may also fill this role is defined in section 3.5.

In the case of the TPM AIK certificate, the ***issuer*** is the Privacy-CA and the ***user*** is typically an integrity verifier. Large enterprises or government agencies with “closed environments” may operate an internal Privacy-CA (see the TCG Reference Architecture for Interoperability section 6.3[2]).

Note:

Some fields are assigned a value even though the certificate user performs no action with that value. In such cases, the intention is to inhibit non-TCG implementations from making inappropriate use of the certificate and/or using the certificate incorrectly (for example, using it for SMIME).

Field/Extension Name	Description	Field Status
Version	Certificate syntax version number	Standard
Serial Number	Positive integer value unique relative to the issuer	Standard
Signature Algorithm	Algorithm was used by the issuer to sign this certificate	Standard
Issuer	Distinguished name of the AIK certificate issuer	Standard
Validity	Time interval during which the certificate is valid	Standard
Subject	Distinguished name of the certificate. MUST be empty.	Standard
Public Key Info	Identifier of the algorithm for the public key	Standard
Extension	Contains a set of additional attributes to be associated with the certificate's entity.	MUST
Certificate Policies	Policy terms under which the certificate was issued	MUST
Subject Alternative Names	Name forms other than directory distinguished names for the certificate.	MUST
Basic Constraints	CA certificate indicator and path constraints	MUST
Subject Directory Attributes	Various device characteristics	MUST
Authority Key Id	Identifies the subject public key of the certificate issuer	SHOULD
Authority Info Access	Indicates how to access CA information	MAY
CRL Distribution	Indicates how to access CRL information	MAY
Key Usage	Indicates the intended use of the subject public key	SHOULD NOT
Extended Key Usage	Indicates the intended use of the subject public key	SHOULD NOT
Issuer Alternative Name	Used to associate Name forms other than distinguished names for the issuer of the certificate	SHOULD NOT
Freshest CRL	Identifies how delta CRL information is obtained	SHOULD NOT
Subject Information Access	Indicates how to access additional information and services associated with the certificate entity.	SHOULD NOT
Subject Key Id	Identifies the subject public key of the certificate	SHOULD NOT
Subject Unique Id	Unique value when using a shared subject name	SHOULD NOT

Field/Extension Name	Description	Field Status
Issuer Unique Id	Unique value when using a shared issuer name	SHOULD NOT
Virtual Platform Attestation Service	This URI indicates how the remote challenger may contact the attestation service of the layer below the holder of this credential (typically the virtual machine). This extension is only for use with virtualized trusted platforms.	SHOULD only on virtualized trusted platforms
Migration Controller Attestation Service	This URI provides the location of the attestation service for the migration controller associated with the component holder of this credential. For example, this could be a virtual machine which could be moved to another platform by the migration controller. Remote challengers concerned about the trustworthiness of the migration controller can use this URI to request an attestation.	SHOULD only when a migration controller associated with the credential holder is present
Migration Controller Registration Service	This extension includes a URI to the migration controller's event notification service. This is useful when a VM is being attested and the remote challenger would like proactive notification when the VM has been moved to a different platform in case its security properties have changed.	SHOULD only when a migration controller associated with the credential holder is present
Virtual Platform Backup Service URI	Provides a URI to the virtualized TPM backup service in case a remote challenger wishes to evaluate the restore policies to avoid rollback attacks. This extension also includes the restoreAllowed flag to indicate if a restore is possible under any circumstances.	SHOULD only for virtualized TPM with a backup authority

Table 6: AIK Certificate Fields

3.4.1 Version

This field contains the version of the certificate syntax. Since AIK certificates always contain mandatory extensions the version number must be set to 3 (which is encoded as the value 2 in ASN.1).

3.4.2 Serial Number

The serial number MUST be a positive integer which is uniquely assigned to each AIK certificate by the issuer. The combination of an issuer's DN and the serial number MUST uniquely describe a single certificate.

3.4.3 Signature Algorithm

This OID identifies the algorithm used by the AIK certificate issuer to sign the certificate. AIK certificate verifiers MUST support certificates signed using a 2048 bit key with the algorithm sha-1WithRSAEncryption which has the OID value shown below. The AlgorithmIdentifier parameters field MUST be the ASN.1 type NULL.

```
sha-1WithRSAEncryption OBJECT IDENTIFIER  ::=  {
```

```
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5  }
```

3.4.4 Issuer

This is the distinguished name of the Privacy-CA. This is the entity that asserts that the subject AIK conforms to the TCG specification.

3.4.5 Validity

This contains the period during which the binding between the attributes and TPM EK certificate is considered valid. It is represented by two date values named notBefore and notAfter. Issuers should assign notBefore to the current time when the AIK certificate is issued and notAfter to the last date that the certificate will be considered valid. Both notBefore and notAfter MUST use the appropriate time format as indicated by RFC 3280, section 4.1.2.5.

3.4.6 Subject

The subject distinguished name MUST be empty.

Issuers MUST use the subject alternative name extension instead.

3.4.7 Public Key Info

Describes the public Attestation Identity Key algorithm and key value.

The algorithm OID shown below MUST be supported for interoperability.

```
id-RSAEncryption OBJECT IDENTIFIER  ::=  {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
```

3.4.8 Certificate Policies

Indicates policy terms under which the certificate was issued.

Assign “critical” the value TRUE. Assign policyIdentifier at least one object identifier. Optionally, assign the cPSuri the value of an HTTP URL at which a plain language version of the Privacy-CA’s certificate policy may be obtained. Assign the explicit text userNotice policy qualifier the value “TCPA Trusted Platform Identity”. Also, include the policyInformation values from the certificate policies extensions of the TPM EK and platform certificates provided in the TPM identity request message

During certificate path validation, check that at least one acceptable Privacy-CA policyIdentifier value is present. Optionally, check that at least one acceptable EK, and one acceptable platform certificate policyIdentifier value are present.

3.4.9 Subject Alternative Names

This contains the alternative name of the entity associated with this certificate. Assign “critical” the value TRUE. Include three values in the extension:

The TPM manufacturer, model and version numbers from the TPM EK certificate “Subject Alternative Name” extension.

The platform manufacturer, model and version numbers from the platform certificate “subject alternative name” extension.

The TPM identity label provided to the Privacy-CA by the TPM owner encoded as a TPMIdLabel other-name. The TPM owner should choose a label syntax and semantics that are understood by the integrity verifier. (Note: the specified syntax accommodates multi-byte character sets).

3.4.10 Basic Constraints

This indicates whether the subject is a CA. Assign “critical” the value TRUE. Assign “CA” the value FALSE.

3.4.11 Subject Directory Attributes

The extension includes miscellaneous properties and security assertions about the entity. This SHOULD be non-critical.

The following attributes MUST be included in a Subject Directory Attributes extension in the AIK certificate:

- The “TPM Specification” attribute which identifies the family and revision of the TCG TPM specification to which the TPM was designed.
- The “TCG Platform Specification” attribute references the platform class, version and revision level of the TCG platform-specific specification to which the platform was designed.

The following attributes SHOULD be included in a Subject Directory Attributes extension in the AIK certificate:

- The multi-valued attribute “supported algorithms” (see X.509) which SHOULD include object identifiers for the algorithms RSAES-OAEP, SHA-1 (1.3.14.3.2.26), and other algorithms implemented by the TPM.
- The “TPM Security Assertions” attribute which describes various assertions about the security properties of the TPM and the conditions under which the Endorsement Key was generated.
- The platform “TBB Security Assertions” attribute describes various assertions about the security properties of the TBB of the platform.

The following attributes are documented for compatibility with TCPA but SHOULD NOT be included in AIK Certificates (see Changes Since TCPA 1.1b):

- The "TCPA Specification Version" attribute, with field values correctly reflecting the highest version of the TCG specification with which the TPM implementation conforms.
- If the TPM has been successfully evaluated against a Common Criteria protection profile, then include the TPM protection profile identifier attribute.
- If the TPM has been successfully evaluated against a Common Criteria security target, then include the TPM security target identifier attribute.
- If the RTM and the means by which the TPM and RTM have been incorporated into the platform have been successfully evaluated against a Common Criteria protection profile, then include the "TBB protection profile" identifier attribute.
- If the RTM and the means by which the TPM and RTM have been incorporated into the platform have been successfully evaluated against a Common Criteria security target, then include the "TBB security target" identifier attribute.
- The "security qualities" attribute with a text string reflecting the security qualities of the TPM.
- The "security qualities" attribute with a text string reflecting the security qualities of the platform.

3.4.12 Authority Key Id

This identifies the subject public key of the certificate issuer. Assign “critical” the value FALSE. Assign the value of “subject key identifier” from the Privacy-CA’s public-key certificate, if available, else omit.

3.4.13 Authority Info Access

This contains additional information about the issuer. It MAY be omitted. If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 3280) and the accessLocation value SHOULD point to the access value of the OCSP responder (HTTP URI).

The relying party can access the certificate status for this certificate by sending a properly formatted OCSPRequest to the URI. If both a CDP and OCSP AIA extension are present in the certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

3.4.14 CRL Distribution

This provides the location of the subject's revocation information. The relying party can access the CRL for this certificate from this URI. If both a CDP and OCSP AIA extension are present in the certificate, then relying parties SHOULD use OCSP as the primary validation mechanism.

If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 3280) and the accessLocation value SHOULD point to the location of the OCSP responder (HTTP URI).

3.4.15 Key Usage

If present, this extension indicates the intended purpose of the subject public key. If present, the digital signature bit SHOULD be set and the extension SHOULD be marked critical.

3.4.16 Extended Key Usage

If present, this extension indicates the intended purpose of the subject public key. It SHOULD NOT be included in AIK certificates. If a certificate includes this extension and it is marked CRITICAL then reject the certificate during path validation if the extended key usage is not understood.

3.4.17 Issuer Alternative Names

This is used to associate Internet style identities with the certificate issuer. This extension SHOULD NOT be included in AIK certificates.

3.4.18 Freshest CRL

The freshest CRL extension identifies how delta CRL information is obtained. This extension SHOULD NOT be included in AIK certificates.

3.4.19 Subject Information Access

The subject information access extension indicates how to access information and services for the subject of the certificate in which the extension appears. This extension SHOULD NOT be included in AIK certificates.

3.4.20 Subject Key Id

Identifies the public key of the certificate. This extension SHOULD NOT be included in AIK certificates.

3.4.21 Subject and Issuer Unique Ids

These uniquely identify certificates which share names with other certificates issued by the same issuer. Under this specification these fields MUST be omitted.

3.4.22 Virtualized Platform Attestation Service

This extension is only for use in AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI that provides a linkage between the layer holding this credential (typically a virtual machine) and the layer below it such as a VMM. This extension is intended to be used by a remote challenger wishing to attest not only the entity holding this credential, but also the layer below it. This extension is identified using the tcg-ce-virtualPlatformAttestationService OID and includes a single URI (not hashed like other potential URIs in the credential)

For example, a virtual machine (VM) could have a virtualized trusted platform associated with it. The virtualized trusted platform would offer trusted computing features such as a TPM and CRTM, so the AIK credential could refer (or contain) information about a virtualized EK credential. A remote challenger may wish to attest the VMM layer that is supporting the VM, since it runs in a more privileged environment and therefore might be able to compromise the VM without its knowledge (so would not be detectable by attesting the VM). This extension's URI defines how to reach that VMM's (or generically the layer below's) attestation service. By generically thinking about this as "the layer below", it enables support for having multiple virtualization layers below the VM and the remote challenger being able to walk the layer stack.

3.4.23 Migration Controller Attestation Service

This extension is only for use in AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI to identify the migration authority controlling movement of the credential holder. This movement (migration) is not always possible even in virtualized trusted platform usages, so this extension should only present when migration is possible and the controller may provide attestations to remote challengers. This extension is identified using the tcg-ce-migrationControllerAttestationService OID and includes a single URI.

For example, a virtualized trusted platform associated with a VM could be moved for various reasons (e.g. addressing capacity issues) to another trusted platform while servicing remote parties. Those parties may have initially attested and determined the VM and its underlying platforms are trustworthy, but now the migration controller moves it to a different platform. This extension allows the remote challenger to ensure the migration controller's policies and that it is trustworthy as well.

3.4.24 Migration Controller Registration Service

This extension is only for use in AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI to identify the migration event registration service on the migration authority controlling movement of the credential holder. This service is responsible for notifying all registered parties when a VM of interest in about to be moved in case the party would like to re-attest the VM after it has been migrated before continuing to trust its operation. This extension is identified using the tcg-ce-migrationControllerRegistrationService OID and includes a single URI

For example, a remote challenger performs a deep attestation of a VM prior to trusting it to perform a transaction. After the successful attestation, the party starts to use the VM's services but the data center owner decides the VM needs to be immediately migrated to another physical platform so the current one can have maintenance performed. Some remote parties may choose to continue to trust the VM, but others may wish to re-attest the VM once it has been instantiated on the new physical platform. This URI provides a mechanism for interested parties to be notified when a migration is about to occur, so it can re-attest the VM.

3.4.25 Virtual Platform Backup Service

This extension is only for use in EK and AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI to the backup authority if one exists that is capable of restoring a complete virtualized TPM instance. The restore of a TPM instance could pose a rollback attack, so remote challengers may wish to attest the operation and policies of the backup authority as part of its trust decisions. The restoreAllowed element indicates whether the virtual TPM associated with this entity could ever have a restored VPM instance (thus a potential rollback concern).

3.5 Unified Trust Certificate

This section describes the X.509 instantiation of a Unified Credential as described above in section 2. This type of credential/certificate was introduced in Version 1.1 of this specification to allow a

common formatted certificate to be used throughout the supply chain to represent each of the 1.0 specification credential types. As noted, it is not expected that a single instance of a Unified credential will be created/deployed that contains the contents of each of the 1.0 credentials simultaneously. This might pose privacy concerns if an AIK equivalent Unified credential also included the EK public key.

During the supply chain of a Trusted Platform its security components are controlled by various parties from the TPM manufacturer to the OEM and ultimately to an IT department. All of the parties in the supply chain may wish to issue a certificate to assert qualities they believe are present in the platform. The Unified Certificate allows a single format for each of these entities to assert their claims, so its important for relying parties to observe the credential type before making decisions based upon the certificates contents.

Field/Extension Name	Description	Field Status
Version	Certificate syntax version number	Standard
Serial Number	Positive integer value unique relative to the issuer	Standard
Signature Algorithm	Algorithm used by the issuer to sign this certificate	Standard
Issuer	Distinguished name of the party that created this certificate	Standard
Validity	Time interval during which the certificate is valid	Standard
Subject	Distinguished name of the certificate. MUST be empty.	Standard
Public Key Info	Identifier of the algorithm for the public key	Standard
Extensions	Contains a set of additional attributes to be associated with the certificate's entity.	MUST
Certificate Policies	Policy terms under which the certificate was issued	MAY
Subject Alternative Names	Name forms other than directory distinguished names.	MUST
Basic Constraints	CA certificate indicator and path constraints	MUST
Subject Directory Attributes	Various characteristics about component	SHOULD
Authority Key Id	Identifies the subject public key of the certificate issuer	SHOULD
Authority Info Access	Indicates how to access CA information	MAY
CRL Distribution	Indicates how to access CRL information	MAY
Key Usage	Indicates the intended use of the subject public key	SHOULD NOT

Field/Extension Name	Description	Field Status
Extended Key Usage	Indicates the intended use of the subject public key and the type of credential (AIK, EK, Platform.)	MUST
Subject Key Id	Identifies the subject public key of the certificate	SHOULD NOT
Issuer Alternative Name	Used to associate Name forms other than distinguished names for the issuer of the certificate	SHOULD NOT
Freshest CRL	Identifies how delta CRL information is obtained	SHOULD NOT
Subject Information Access	Indicates how to access additional information and services associated with the certificate entity.	SHOULD NOT
Subject Unique Id	Unique value when using a shared subject name	SHOULD NOT
Virtual Platform Attestation Service	This URI indicates how the remote challenger may contact the attestation service of the layer below the holder of this credential (typically the virtual machine). This extension is only for use with virtualized trusted platforms.	SHOULD only on virtualized trusted platforms
Migration Controller Attestation Service	This URI provides the location of the attestation service for the migration controller associated with the component holder of this credential. For example, this could be a virtual machine which could be moved to another platform by the migration controller. Remote challengers concerned about the trustworthiness of the migration controller can use this URI to request an attestation.	SHOULD only when a migration controller associated with the credential holder is present
Migration Controller Registration Service	This extension includes a URI to the migration controller's event notification service. This is useful when a VM is being attested and the remote challenger would like proactive notification when the VM has been moved to a different platform in case its security properties have changed.	SHOULD only when a migration controller associated with the credential holder is present
Virtual Platform Backup Service URI	Provides a URI to the virtualized TPM backup service in case a remote challenger wishes to evaluate the restore policies to avoid rollback attacks. This extension also includes the restoreAllowed flag to indicate if a restore is possible under any circumstances.	SHOULD only for virtualized TPM with a backup authority
Issuer Unique Id Relevant Credentials	Unique value when using a shared issuer name Unordered list of references to other certificates associated with the subject components.	SHOULD NOT MAY

Field/Extension Name	Description	Field Status
Relevant Manifests	Unordered list of references to Reference Manifests describing aspects of the subject components.	MAY

Table 7: Unified Trust Certificate Fields

3.5.1 Version

This field contains the version of the certificate syntax. Since Unified Trust certificates always contain mandatory extensions the version number MUST be set to 3 (which is encoded as the value 2 in ASN.1).

```
Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
```

3.5.2 Serial Number

The serial number MUST be a positive integer which is uniquely assigned to each unified certificate by the issuer. The combination of the issuer's DN and the serial number MUST uniquely identify the certificate (this might be leveraged within a reference.)

3.5.3 Signature Algorithm

This OID identifies the algorithm used by the certificate issuer to sign the certificate. Certificate verifiers MUST support certificates signed using a 2048 bit key with the algorithm sha-1WithRSAEncryption which has the OID value shown below. The AlgorithmIdentifier parameters field MUST be the ASN.1 type NULL.

```
sha-1WithRSAEncryption OBJECT IDENTIFIER  ::=  {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5  }
```

3.5.4 Issuer

This is the distinguished name of the entity that created this certificate. This entity (TPM vendor, OEM, IT department's Privacy CA) will vary depending on the phase of the supply chain when the certificate was minted. For instance, the Privacy-CA normally would sign a certificate intending to be used with an attestation (parallels a 1.0 AIK credential.) This is the entity that asserts that the subject DN conforms to the TCG specification.

3.5.5 Validity

The period when the binding of the certificate's contents is valid is represented by two date values named notBefore and notAfter. Issuers should assign notBefore to the current time when the EK certificate is issued and notAfter to the last date that the certificate will be considered valid. Both notBefore and notAfter MUST use the appropriate time format as indicated by RFC 3280, section 4.1.2.5.

3.5.6 Subject

The subject distinguished name MUST be empty.

Issuers MUST use the subject alternative name extension instead.

3.5.7 Public Key Info

Describes the public key algorithm associated with the key included in this certificate and the actual key value. The value to use varies depending on the role (e.g. acting as a 1.0 EK Certificate equivalent) of the certificate.

Certificates of the type EK Certificate (tcg-kp-EKCertificate), the following OID MUST be supported:

- `id-RSAES-OAEP OBJECT IDENTIFIER  ::=  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 7 }`

- The “pSourceFunc” parameters field MUST contain the OID id-pSpecified with an octet string value of “TCPA” as required by the TPM Design Principles in section 31.1.1[5]. For backwards compatibility, a terminating zero-valued character in such a string should be ignored if it is present.

Certificates of the type Platform Certificate (tcg-kp-PlatformCertificate),

- Because the traditional Platform Certificate does not include a public key, the use of an X.509v3 Unified Certificate to represent it raises the question of what to include in the Public Key Info mandatory base field. This specification allows for two uses of this field:
    - No public key info – An issuer SHOULD mark this certificate field as not containing public key information by using the tcg-algorithm-null OID in the field SubjectPublicKeyInfo’s “algorithm” OID and including a zero length subjectPublicKey. Clearly this is not a well known algorithm OID so TCG-aware software (verifiers) seeing this OID MUST interpret it as meaning no public key information is included so verifiers MUST ignore the other contents of the Pubic Key Info field.
    - EK public key info – An issuer MAY use this base certificate field to contain the EK public key information under specific circumstances in order to make EK decryption more convenient (possibly in lieu of a separate EK certificate). The EK certificate’s SubjectPublicKeyInfo (or the equivalent information if known by the issuer) MAY be placed into this field as long as this new certificate doesn’t relax the restrictions on the EK public key usage from the original referenced EK certificate. For example, if the original EK certificate contains NotAfter date during 2010 and by copying the EK public key into this new certificate it becomes associated with information that doesn’t expire until 2015, thus effectively lengthening its lifetime.) Because the X.509 certificate does not include a NotAfter date for its contents and a separate NotAfter date for the Public Key Info care should be used when copying the keys.

Certificates of the type AIK Certificate (tcg-kp-AIKCertificate), the following OID MUST be supported:

- **id-RSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }**

3.5.8 Certificate Policies

Indicates policy terms under which the certificate was issued. The decision of whether to mark this extension as “critical” is determined by the certificate issuer and no longer mandated by this specification. Previous TCG certificates required this extension to set critical to TRUE, but this is no longer necessary as the critical information (certificate type) has been moved out of this extension for the Unified Certificate.

When this extension is present in a certificate, it MUST include at least one policyIdentifier. An issuer MAY assign the CPS pointer qualifier, cPSuri, the value of an HTTP URL at which a plain language version of the issuing CA’s certificate policy may be obtained.

Unlike version 1.0 of this specification, the Certificate Policies are no longer used to hold the certificate type in the explicitText field within this extension (see Extended Key Usage extension.) Therefore in order to avoid potentially conflicting information, certificate issuers SHOULD NOT include a 1.0 style certificate label in this extension and verifiers MUST ignore such information if it happens to be present.

This extension remains useful in Unified Certificates to include the PolicyInformation values from the certificate policies extensions of the TPM EK and platform certificates provided in the TPM identity request message if those credentials are not directly referenced by this certificate.

During certificate path validation if this extension is present, check that at least one acceptable Privacy-CA policyIdentifier value is present. Optionally depending on the type of certificate, check that at least one acceptable EK, and one acceptable platform certificate policyIdentifier value are present if no accessible reference to a relevant EK or Platform credential is included in the certificate. EK type certificates would not include references to Platform information. This information MAY be asserted by another referenced certificate.

3.5.9 Subject Alternative Names

This contains the alternative name of the entity associated with this certificate. Assign “critical” the value TRUE (since the Subject field is empty.) Depending on the type of certificate (see EKU discussion in 3.5.16 below) this field MUST contain different lists of names in the SubjectAltName extension (which is a sequence of GeneralNames identified by an OID.)

Which name types are included depend on the timing in the supply chain, intended use of the certificate, and whether other relevant names are included in other credentials referenced in the Subject Directory Attributes of this certificate.

Certificates of the type EK Certificate (tcg-kp-EKCertificate) -

- MUST include:
    - TPM Manufacturer Info – TPM manufacturer, model and version numbers

Certificates of the type Platform Certificate (tcg-kp-PlatformCertificate) –

- MUST include:
    - Platform Manufacturer Info – Platform manufacturer, model and version numbers
- MUST include or reference in an extension other Credentials containing:
    - TPM Manufacturer Info – TPM manufacturer, model and version numbers

Certificates of the type AIK Certificate (tcg-kp-AIKCertificate) –

- MUST include:
    - TPM Identity Label Info – Attestation identity label provided to the Privacy-CA by the TPM owner as a TPMIdLabel other-name. The TPM owner should choose a label syntax and semantics that are understood by the integrity verifier.
- MUST include or reference in an extension other Credentials containing:
    - TPM Manufacturer Info – TPM manufacturer, model and version numbers

o Platform Manufacturer Info – Platform manufacturer, model and version numbers

3.5.10 Basic Constraints

This indicates whether the subject is a CA. Assign “critical” the value TRUE. Assign “cA” the value FALSE.

3.5.11 Subject Directory Attributes

The extension SHOULD be non-critical.

This attribute extension is included within the TCG credentials as a place to store security oriented assertions about the component described by the certificate. In version 1.1 of this specification, the Unified Certificate is defined allowing for multiple types of 1.0 credentials to share a common format and the ability to reference other credentials (or signed documents) which add to the assertions made by this distributed credential. Because of this the contents of some common fields (including

Subject Directory Attributes) vary depending on the type of certificate (see EKU discussion in 3.5.16 below) this section defines the requirements for this field based on the certificate type.

Certificates of the type EK Certificate (tcg-kp-EKCertificate) -

- MUST include or reference in an extension other Credentials containing:
    - The “TPM Specification” attribute which identifies the family and revision of the TCG TPM specification to which the TPM was designed.
- SHOULD include or reference in an extension other Credentials containing:
    - The multi-valued attribute “supported algorithms” (see X.509) which SHOULD include object identifiers for the algorithms RSAES-OAEP, SHA-1 (1.3.14.3.2.26), and other algorithms implemented by the TPM.
    - The “TPM Security Assertions” attribute which describes various assertions about the security properties of the TPM and the conditions under which the Endorsement Key was generated.

Certificates of the type Platform Certificate (tcg-kp-PlatformCertificate) -

- MUST include or reference in an extension the items from above Unified EK Certificate
- MUST also include or reference in an extension other Credentials containing:
    - The “TCG Platform Specification” attribute references the platform class, version and revision level of the TCG platform-specific specification to which the platform was designed.
- SHOULD also include or reference in an extension other Credentials containing:
    - The platform “TBB Security Assertions” attribute describes various assertions about the security properties of the TBB of the platform.

Certificates of the type AIK Certificate (tcg-kp-AIKCertificate) -

- MUST include or reference in an extension the items from above Unified Platform Certificate
- No additional AIK specific attributes are defined at this time.

The use of legacy TCPA attributes described at the end of section 3.4.11 MUST NOT be used in a Unified Certificate.

3.5.12 Authority Key Id

This identifies the subject public key of the certificate issuer. Assign “critical” the value FALSE. Assign the value of “subject key identifier” from the issuer’s public-key certificate, if available, else omit.

3.5.13 Authority Info Access

This contains additional information about the issuer. It MAY be omitted. If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 3280) and the accessLocation value SHOULD point to the access value of the OCSP responder (HTTP URI).

The relying party can access the certificate status for this certificate by sending a properly formatted OCSPRequest to the URI. If both a CDP and OCSP AIA extension are present in the certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

3.5.14 CRL Distribution

This provides the location of the subject's revocation information. The relying party can access the CRL for this certificate from this URI. If both a CDP and OCSP AIA extension are present in the certificate, then relying parties SHOULD use OCSP as the primary validation mechanism.

If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 3280) and the accessLocation value SHOULD point to the location of the OCSP responder (HTTP URI).

3.5.15 Key Usage

If present, this extension indicates the intended purpose of the subject public key. If present, the value should reflect the purpose of the key. This extension SHOULD NOT be used since it potentially causes confusion around the use of the key should it conflict with the mandated EKU extensions content. If this field is used the following values MUST be used:

Certificates of the type EK Certificate (tcg-kp-EKCertificate) -

- This attribute should contain "keyEncipherment".

Certificates of the type Platform Certificate (tcg-kp-PlatformCertificate) -

- This attribute should contain "keyEncipherment".

Certificates of the type AIK Certificate (tcg-kp-PlatformCertificate) -

- This attribute should contain "digitalSignature".

For EK and Platform Certificates (containing a type of tcg-kp-EKCertificate or tcg-kp-PlatformCertificate in the EKU), this attribute should contain "keyEncipherment".

For AIK Certificates (tcg-kp-AIKCertificate), this attribute should contain "digitalSignature".

3.5.16 Extended Key Usage

This extension indicates the intended purpose of the meta-data stored in the certificate. This extension MUST exist in all Unified Credentials to indicate the type of certificate being represented. Other EKU OIDs defined in RFC 3280 MAY be used in addition to the certificate label define in version 1.1 of this specification.

The introduction of the Unified Certificate capable of being used as an EK, AIK or Platform Certificate raises the need for a clear, easy to locate/parse credential type label. Unlike the 1.0 certificates described above (that were based on the TPM 1.1b credential definitions), this certificate stores the type information in the EKU extension as an OID.

The tcg-kp-EKCertificate, tcg-kp-PlatformCertificate and tcg-kp-AIKCertificate OIDS defined below in the ASN.1 are the Credential Labels (described above) for the Unified Certificate. Due to the large number of common fields within an EK, Platform and AIK certificate and privacy concerns, it is not expected that multiple of these labels will be present in the certificate. If multiple labels or no label appears in the unified certificate, verifiers are unable to determine the role of this certificate and therefore MUST treat this as a fatal error.

If a certificate contains both the EKU and the KU extensions, the EKU semantics MUST be used. If the KU field states an inconsistent usage for the certificate type (as indicated in the EKU) the verifier MAY consider this a fatal error (or merely ignore the KU type information.)

3.5.17 Subject Key Id

Identifies the public key holder of the certificate. This extension SHOULD NOT be included in TCG certificates.

3.5.18 Issuer Alternative Name

This is used to associate Internet style identities with the certificate issuer. This extension SHOULD NOT be included in Unified certificates.

3.5.19 Freshest CRL

The freshest CRL extension identifies how delta CRL information is obtained. This extension SHOULD NOT be included in Unified certificates.

3.5.20 Subject Information Access

The subject information access extension indicates how to access information and services for the subject of the certificate in which the extension appears. This extension SHOULD NOT be included in Unified certificates. A similar extension is defined for TCG certificates allowing information to be associated with the subject (Relevant Credentials, Relevant Manifests.)

3.5.21 Subject and Issuer Unique Ids

These uniquely identify certificates which share names with other certificates issued by the same issuer. Under this specification these fields MUST be omitted.

3.5.22 Virtualized Platform Attestation Service

This extension is only for use in AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI that provides a linkage between the layer holding this credential (typically a virtual machine) and the layer below it such as a VMM. This extension is intended to be used by a remote challenger wishing to attest not only the entity holding this credential, but also the layer below it. This extension is identified using the tcg-ce-virtualPlatformAttestationService OID and includes a single URI (not hashed like other potential URIs in the credential)

For example, a virtual machine (VM) could have a virtualized trusted platform associated with it. The virtualized trusted platform would offer trusted computing features such as a TPM and CRTM, so the AIK credential could refer (or contain) information about a virtualized EK credential. A remote challenger may wish to attest the VMM layer that is supporting the VM, since it runs in a more privileged environment and therefore might be able to compromise the VM without its knowledge (so would not be detectable by attesting the VM). This extension's URI defines how to reach that VMM's (or generically the layer below's) attestation service. By generically thing about this as "the layer below", it enables support for having multiple virtualization layers below the VM and the remote challenger being able to walk the layer stack.

3.5.23 Migration Controller Attestation Service

This extension is only for use in AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI to identify the migration authority controlling movement of the credential holder. This movement (migration) is not always possible even in virtualized trusted platform usages, so this extension should only present when migration is possible and the controller may provide attestations to remote challengers. This extension is identified using the tcg-ce-migrationControllerAttestationService OID and includes a single URI.

For example, a virtualized trusted platform associated with a VM could be moved for various reasons (e.g. addressing capacity issues) to another trusted platform while servicing remote parties. Those parties may have initially attested and determined the VM and its underlying platforms are trustworthy, but now the migration controller moves it to a different platform. This extension allows the remote challenger to ensure the migration controller's policies and that it is trustworthy as well.

3.5.24 Migration Controller Registration Service

This extension is only for use in AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI to identify the migration event registration service on the migration authority controlling movement of the credential holder. This service is responsible for notifying all registered parties when a VM of interest in about to be moved in case the party would like to re-attest the VM after it has been migrated before continuing to trust its operation. This extension is identified using the tcg-ce-migrationControllerRegistrationService OID and includes a single URI

For example, a remote challenger performs a deep attestation of a VM prior to trusting it to perform a transaction. After the successful attestation, the party starts to use the VM's services but the data center owner decides the VM needs to be immediately migrated to another physical platform so the current one can have maintenance performed. Some remote parties may choose to continue to trust the VM, but others may wish to re-attest the VM once it has been instantiated on the new physical platform. This URI provides a mechanism for interested parties to be notified when a migration is about to occur, so it can re-attest the VM.

3.5.25 Virtual Platform Backup Service

This extension is only for use in EK and AIK (and Unified) Credentials associated with virtualized trusted platforms in order to provide a URI to the backup authority if one exists that is capable of restoring a complete virtualized TPM instance. The restore of a TPM instance could pose a rollback attack, so remote challengers may wish to attest the operation and policies of the backup authority as part of its trust decisions. The restoreAllowed element indicates whether the virtual TPM associated with this entity could ever have a restored VPM instance (thus a potential rollback concern).

3.5.26 Relevant Certificates

This extension includes a list of URIs used to reference existing certificates that offer information (e.g. assertions) relevant to the subject component. If present, this extension SHOULD be marked as critical.

This extension is recognized by the presence of the tcg-ce-relevantCredentials OID. This extension includes a list of URI references to other previously issued certificates that assert information relevant to this TPM, platform or identity (depending on the type of certificate.) These references MAY point to 1.0 type credentials, other Unified Credentials or both.

An optional hash SHOULD be used to enable verifiers to detect when a different certificate has been returned via the URI reference. This might occur if there was any vagueness in identifying the target certificate (e.g. the URI wasn't precise in its description) or if an attacker was attempting to substitute a different certificate. The contents of the URI itself are not standardized but it's envisioned that it would include the serial number and name of the issuer to help uniquely identify the certificate.

The reference also includes an optional hint (OID) at the semantics of the certificate being referenced. This hint is included in the documentAccessInfo field. This OID SHOULD contain the type of certificate being referenced (EK, Platform, AIK) using the certificate type OIDs defined below (and used in the EKU of the Unified Credential.)

3.5.26.1 Determining Most Recent Certificate

One issue raised by the introduction of references to other certificates is the possibility of overlapping information. In order to have a consistent, interoperable way to address conflicts, verifiers SHOULD ignore overlapping information contained in older certificates. This assures only the latest information contained in the distributed certificates is applied. However entities issuing certificates containing overlapping and conflicting information need to assure this information is correct, particularly when they are changing an assertion made by a potentially more authoritative entity (e.g. an IT department overriding an assertion made by a TPM manufacturer.)

Because X.509 certificates do not include an explicit issuance date, the processing rules for determining which certificate is more recent are more difficult. Three interesting cases exist where overlapping information may occur, each with varying levels of complexity to determine which is authoritative:

1 A unified certificate includes information that overlaps and conflicts with information contained in certificates it directly references.

2 Multiple referenced certificates contain conflicting information but only one certificate is currently valid (within its Validity period notBefore thru notAfter) and has not been revoked.

3 Multiple referenced certificates contain conflicting information and are currently within their Validity period (and not revoked.)

The processing rules to be used to determine which of the conflicting information SHOULD be considered authoritative is as follows:

Case 1: Verifier SHOULD consider the base unified certificate referencing the other conflicting certificates as authoritative (most current.) Because the base certificate references other existing certificates, it must be newer than those referenced. For efficiency, this also allows verifiers to only look to the referenced relevant certificates for additional information not asserted by the base certificate.

Case 2: Verifier SHOULD consider the non-expired and not revoked certificate as authoritative. Information in revoked certificate MUST be ignored. Therefore, revoked certificates should be ignored for all processing including any references it may include. Expired certificate information SHOULD NOT be used unless local policy allows for its use when no other information is available.

Case 3: Verifier SHOULD identify the valid referenced certificate that contains the latest notBefore date. This certificate is considered authoritative for conflicting information amongst referenced certificates from a common base certificate. Because the notBefore field wasn't intended to be used as an issuance date, some deployments may wish to pre-issue certificates with later (non-current) notBefore dates.

In order for this set of processing rules to correctly recognize the latest certificate when resolving conflicts between overlapping referenced certificates, issuers MUST NOT re-issue TCG certificates for an entity with a notBefore date earlier then the current date/time unless the issuer knows no pre-existing certificates for the entity are valid and contain conflicting assertion information. Doing so might confuse this processing and consider the pre-existing information to be authoritative over the new certificate.

3.5.27 Relevant Manifests

This extension includes an unordered list of URIs to existing Reference Manifests that may define qualities present in the subject component described by this certificate. When present, this extension SHOULD be marked as critical.

This extension is recognized by the presence of the tcg-ce-relevantManifests OID. This extension includes a list of URI references to other previously issued Reference Manifests (signed XML documents) that assert information relevant to this TPM, platform or identity (depending on the type of manifest.)

An optional hash SHOULD be used to enable verifiers to detect when a different Reference Manifest has been located via the URI reference. This might occur should there be any vagueness in identifying the target manifest (e.g. the URI wasn't precise in its description) or if an attacker was attempting to substitute a different manifest.

The reference also includes an optional hint (OID) at the access method (in documentAccessInfo) available for fetching the Reference Manifest. Future revisions of this specification will define such values.

3.5.27.1 Determining Most Recent Manifest

One issue raised by the introduction of references to multiple manifests is the possibility of overlapping information with each other. In order to have a consistent, interoperable way to address conflicts, verifiers SHOULD ignore conflicting (overlapping) information contained in older manifests. This assures only the latest information contained in the collection of manifests is applied.

In order to determine which reference manifest to consider authoritative when multiple provide overlapping information, the Verifier MUST consult the RimmType's RevLevel attribute. Because the creators of RimmType documents are required to increment the RevLevel when re-issuing a reference manifest for a component, verifiers can determine which reference manifest is most current (highest value in RevLevel.) If for some reason the RevLevel is the same (which should not happen), the verifier MAY consult the optional SignerInfo complex type and compare the included dateTime attribute. If the dateTime is present in the RimmType it would also be helpful in addressing conflicts between a reference manifest and other referenced certificates.

4 Changes Since TCPA 1.1b

This chapter provides a summary of significant changes versus the credentials and certificate definitions in the TCPA Main Specification 1.1b.

- The critical flag on the Subject Alt Name extension in the X.509 certificate definitions has been changed from FALSE to TRUE. This was changed to be consistent with RFC 3280 which requires the extension to be critical when the Subject field is empty. Since the Subject field was previously required to be empty and the Subject Alt Name was previously required to be present in TCPA 1.1b this change should be backwards compatible.
- In TCPA 1.1b, there are defined attributes which optionally carry the ASN.1 Object Identifiers for the protection profile and security target of the TPM and platform inside of the Platform and AIK certificates but not the EK certificate. In addition, all three certificates may optionally carry a SecurityQualities attribute. In the current document, the SecurityQualities attribute has been deprecated in favor of the new “TPM Security Assertions” and “TBB Security Assertions” ASN.1 attributes which include any relevant protection profile and security target information.
- TCG has introduced a new specification naming convention to identify the TPM and platform-specific specifications. New “TPM Specification” and “TCG Platform Specification” attributes have been introduced to describe these values within TCG credentials and certificates. Certificates issued under this profile should include the new attributes and may include the old “TCPA Specification Version” for backwards compatibility.
- The X.509 “supported algorithms” attribute in a Platform Certificate is deprecated since there are no standard platform-specific algorithms beyond those that would be documented in a EK Certificate “supported algorithms” attribute.
- It is now recommended that the platform credential carry only platform-specific attributes and assertions to avoid duplicating information already present in the TPM credential.
- Version 1.1 of this specification added a new Unified Credential (and Certificate) offering a common format for each of the 3 types of credentials. The Unified Credential also includes 2 lists of URI references allowing credentials to be linked with other previously issued credentials or Reference Manifests. This enables sharing (via references) of most of the non-instance specific information thus allowing for smaller overall credential sizes.
- Addition of new elements to reference virtualization oriented components (e.g. URI of Deep Attestation Service for layer below holder of credential). This enables attestation traversing several virtualized platform layers by the relying party and interacting with the virtualization infrastructure components.

5 X.509 ASN.1 Structures and OIDs

TCG has registered an object identifier (OID) namespace as an “international body” in the ISO registration hierarchy. This leads to shorter OIDs and gives TCG the ability to manage its own namespace. The OID namespace is inherited from TCPA. These definitions are intended to be used within the context of an X.509 v3 certificate specifically leveraging the profile described in RFC 3280.

```
-- TCG specific OIDs
tcg OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) international-organizations(23) tcg(133) }

tcg-tcpaSpecVersion OBJECT IDENTIFIER ::= {tcg 1}
tcg-attribute OBJECT IDENTIFIER ::= {tcg 2}
tcg-protocol OBJECT IDENTIFIER ::= {tcg 3}
tcg-algorithm OBJECT IDENTIFIER ::= {tcg 4}
tcg-ce OBJECT IDENTIFIER ::= {tcg 6}
tcg-kp OBJECT IDENTIFIER ::= {tcg 8}

-- TCG Attribute OIDs
tcg-at-tpmManufacturer OBJECT IDENTIFIER ::= {tcg-attribute 1}
tcg-at-tpmModel OBJECT IDENTIFIER ::= {tcg-attribute 2}
tcg-at-tpmVersion OBJECT IDENTIFIER ::= {tcg-attribute 3}
tcg-at-platformManufacturer OBJECT IDENTIFIER ::= {tcg-attribute 4}
tcg-at-platformModel OBJECT IDENTIFIER ::= {tcg-attribute 5}
tcg-at-platformVersion OBJECT IDENTIFIER ::= {tcg-attribute 6}

tcg-at-securityQualities OBJECT IDENTIFIER ::= {tcg-attribute 10}
tcg-at-tpmProtectionProfile OBJECT IDENTIFIER ::= {tcg-attribute 11}
tcg-at-tpmSecurityTarget OBJECT IDENTIFIER ::= {tcg-attribute 12}
tcg-at-tbbProtectionProfile OBJECT IDENTIFIER ::= {tcg-attribute 13}
tcg-at-tbbSecurityTarget OBJECT IDENTIFIER ::= {tcg-attribute 14}
tcg-at-tpmIdLabel OBJECT IDENTIFIER ::= {tcg-attribute 15}
tcg-at-tpmSpecification OBJECT IDENTIFIER ::= {tcg-attribute 16}
tcg-at-tcgPlatformSpecification OBJECT IDENTIFIER ::= {tcg-attribute 17}
tcg-at-tpmSecurityAssertions OBJECT IDENTIFIER ::= {tcg-attribute 18}
tcg-at-tbbSecurityAssertions OBJECT IDENTIFIER ::= {tcg-attribute 19}

-- TCG Algorithm OIDs
tcg-algorithm-null OBJECT IDENTIFIER ::= {tcg-algorithm 1}

-- TCG Key Purposes OIDs
tcg-kp-EKCertificate OBJECT IDENTIFIER ::= {tcg-kp 1}
tcg-kp-PlatformCertificate OBJECT IDENTIFIER ::= {tcg-kp 2}
tcg-kp-AIKCertificate OBJECT IDENTIFIER ::= {tcg-kp 3}

-- TCG Certificate Extensions
tcg-ce-relevantCredentials OBJECT IDENTIFIER ::= {tcg-ce 2}
tcg-ce-relevantManifests OBJECT IDENTIFIER ::= {tcg-ce 3}
tcg-ce-virtualPlatformAttestationService OBJECT IDENTIFIER ::= {tcg-ce 4}
tcg-ce-migrationControllerAttestationService OBJECT IDENTIFIER ::= (tcg-ce 5}
tcg-ce-migrationControllerRegistrationService OBJECT IDENTIFIER ::= (tcg-ce 6}
tcg-ce-virtualPlatformBackupService OBJECT IDENTIFIER ::= (tcg-ce 7}

-- TCG Protocol OIDs
tcg-prt-tpmIdProtocol OBJECT IDENTIFIER ::= {tcg-protocol 1}

-- tcg specification attributes for tpm and platform

tPMSpecification ATTRIBUTE ::= {
    WITH SYNTAX TPMSpecification
    ID tcg-at-tpmSpecification }
```

```
TPMSpecification ::= SEQUENCE {
    family UTF8String (SIZE (1..STRMAX)),
    level INTEGER,
    revision INTEGER }

tCGPlatformSpecification ATTRIBUTE ::= {
    WITH SYNTAX TCGPlatformSpecification
    ID tcg-at-tcgPlatformSpecification }

TCGSpecificationVersion ::= SEQUENCE {
    majorVersion INTEGER,
    minorVersion INTEGER,
    revision INTEGER }

TCGPlatformSpecification ::= SEQUENCE {
    Version TCGSpecificationVersion,
    platformClass OCTET STRING SIZE(4) }

-- tcpa tpm specification attribute (deprecated)

tCPASpecVersion ATTRIBUTE ::= {
    WITH SYNTAX TCPASpecVersion
    ID tcg-tcpaSpecVersion }

TCPASpecVersion ::= SEQUENCE {

    major INTEGER,

    minor INTEGER }


-- manufacturer implementation model and version attributes

TPMManufacturer ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-tpmManufacturer }

TPMModel ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-tpmModel }

TPMVersion ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-tpmVersion }

PlatformManufacturer ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-platformManufacturer }

PlatformModel ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-platformModel }

PlatformVersion ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-platformVersion }


-- tpm and platform tbb security assertions

Version ::= INTEGER { v1(0) }

tPMSecurityAssertions ATTRIBUTE ::= {
    WITH SYNTAX TPMSecurityAssertions
    ID tcg—at-tpmSecurityAssertions
}
```

```
TPMSecurityAssertions ::= SEQUENCE {
    version Version DEFAULT v1,
    fieldUpgradable BOOLEAN DEFAULT FALSE,
    ekGenerationType [0] IMPLICIT EKGenerationType OPTIONAL,
    ekGenerationLocation [1] IMPLICIT EKGenerationLocation OPTIONAL,
    ekCertificateGenerationLocation [2] IMPLICIT
        EKCertificateGenerationLocation OPTIONAL,
    ccInfo [3] IMPLICIT CommonCriteriaMeasures OPTIONAL,
    fipsLevel [4] IMPLICIT FIPSLevel OPTIONAL,
    iso9000Certified [5] IMPLICIT BOOLEAN DEFAULT FALSE,
    iso9000Uri IA5STRING (SIZE (1..URIMAX)) OPTIONAL }


tBBSecurityAssertions ATTRIBUTE ::= {
    WITH SYNTAX TBBSecurityAssertions
    ID tcg—at-tbbSecurityAssertions }


TBBSecurityAssertions ::= SEQUENCE {
    version Version DEFAULT v1,
    ccInfo [0] IMPLICIT CommonCriteriaMeasures OPTIONAL,
    fipsLevel [1] IMPLICIT FIPSLevel OPTIONAL,
    rtmType [2] IMPLICIT MeasurementRootType OPTIONAL,
    iso9000Certified BOOLEAN DEFAULT FALSE,
    iso9000Uri IA5STRING (SIZE (1..URIMAX)) OPTIONAL }


EKGenerationType ::= ENUMERATED {
    internal (0),
    injected (1),
    internalRevocable(2),
    injectedRevocable(3) }


EKGenerationLocation ::= ENUMERATED {
    tpmManufacturer (0),
    platformManufacturer (1),
    ekCertSigner (2) }


EKCertificateGenerationLocation ::= ENUMERATED {
    tpmManufacturer (0),
    platformManufacturer (1),
    ekCertSigner (2) }


-- V1.1 of this specification adds hybrid and physical.
-- Hybrid means the measurement root is capable of static AND dynamic
-- Physical means that the root is anchored by a physical TPM
-- Virtual means the TPM is virtualized (possibly running in a VMM)

-- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
-- the capabilities of the platform.
MeasurementRootType ::= ENUMERATED {

    static (0),

    dynamic (1),

    nonHost (2),

    hybrid (3),

    physical (4),

    virtual (5) }



-- common criteria evaluation

CommonCriteriaMeasures ::= SEQUENCE {
```

```
            version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined
by CC
            assurancelevel EvaluationAssuranceLevel,
            evaluationStatus EvalutionStatus,
            plus BOOLEAN DEFAULT FALSE,
            strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
            profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
            profileUri [2] IMPLICIT URIReference OPTIONAL,
            targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
            targetUri [4] IMPLICIT URIReference OPTIONAL }


        EvaluationAssuranceLevel ::= ENUMERATED {
            level1 (1),
            level2 (2),
            level3 (3),
            level4 (4),
            level5 (5),
            level6 (6),
            level7 (7) }

        StrengthOfFunction ::= ENUMERATED {
            basic (0),
            medium (1),
            high (2) }

        URIReference ::= SEQUENCE {
            uniformResourceIdentifier IA5String (SIZE (1..URIMAX)),
            hashAlgorithm AlgorithmIdentifier OPTIONAL,
            hashValue BIT STRING OPTIONAL }


        EvaluationStatus ::= ENUMERATED {
            designedToMeet (0),
            evaluationInProgress (1),
            evaluationCompleted (2) }


        -- fips evaluation

        FIPSLevel ::= SEQUENCE {
            version IA5STRING (SIZE (1..STRMAX)), -- "140-1" or "140-2"
            level SecurityLevel,
            plus BOOLEAN DEFAULT FALSE }


        SecurityLevel ::= ENUMERATED {
            level1 (1),
            level2 (2),
            level3 (3),
            level4 (4) }


        -- aik certificate label from tpm owner


        TPMIdLabel OTHER-NAME ::= {UTF8String IDENTIFIED BY {tcg-at-tpmIdLabel} }


        -- the following are deprecated but may be present for compatibility with TCPA

        TPMProtectionProfile ATTRIBUTE ::= {
            WITH SYNTAX ProtectionProfile
            ID tcg-at-tpmProtectionProfile }


        TPMSecurityTarget ATTRIBUTE ::= {
            WITH SYNTAX SecurityTarget
            ID tcg-at-tpmSecurityTarget }


        TBBProtectionProfile ATTRIBUTE ::= {
            WITH SYNTAX ProtectionProfile
```

```
    ID tcg-at-tbbProtectionProfile }


TBBSecurityTarget ATTRIBUTE ::= {
    WITH SYNTAX SecurityTarget
    ID tcg-at-tbbSecurityTarget }


ProtectionProfile ::= OBJECT IDENTIFIER

SecurityTarget ::= OBJECT IDENTIFIER


-- V1.1 addition for enabling references to other credentials or
-- XML-based Reference Manifests.  These data objects are included
-- in X.509 extensions using the new tcg-ce-[relevantCredentials,
-- relevantManifests] OIDs.

HashAlgAndValue ::= SEQUENCE {
   hashAlg         AlgorithmIdentifier,
   hashValue       OCTET STRING }


HashedSubjectInfoURI  ::=  SEQUENCE {
   documentURI IA5String (SIZE (1..URIMAX)),
   documentAccessInfo OBJECT IDENTIFIER OPTIONAL,
   documentHashInfo HashAlgAndValue OPTIONAL }

SubjectInfoURIList  ::=
   SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI


TCGRelevantCredentials::=

   SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI

TCGRelevantManifests::=

   SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI


-- V1.2 addition of virtualization oriented credential extensions.  This extension
indicates how a remote challenger can contact the (deep) attestation service below
the current credential holder in order to attest the layer below.  Using this model
allows the credential of each virtualization layer to reference the attestation
service for the layer below it.    A remote challenger could traverse the layer
hierarchy using this extension until reaching the physical trusted platform rooted
attestation.    The following URI is optionally included in a certificate for a
virtual machine associated with the tcg-ce-virtualPlatformAttestationService
extension OID.          These URI are associated with the tcg-ce-
[virtualPlatformAttestationService,          migrationControllerAttestationService,
migrationControllerRegistrationService,     virtualPlatformBackupService]     OIDs
respectively:

VirtualPlatformAttestationServiceURI ::= IA5String (SIZE (1..URIMAX)

MigrationControllerAttestationServiceURI ::= IA5String (SIZE (1..URIMAX)

MigrationControllerRegistrationServiceURI ::= IA5String (SIZE (1..URIMAX)

VirtualPlatformBackupServiceURI ::= SEQUENCE {
   restoreAllowed BOOLEAN DEFAULT FALSE,
   backupServiceURI    IA5String }
```

6 References

[1] TCG Specification Architecture Overview, Specification Version 1.2, http://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14

[2] TCG Infrastructure Working Group Reference Architecture for Interoperability (Part 1), Specification Version 1.0, http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_reference_architecture_for_interoperability_specification_part_1_version_10

[3] TCG Main Specification Version 1.2, level 2, revision 85, dated 13 February 2005, http://www.trustedcomputinggroup.org/resources/tpm_main_specification

[4] TCG Infrastructure Working Group Subject Key Attestation Evidence Extension, Specification Version 1.0, http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_subject_key_attestation_evidence_extension_version_10

[5] TCPA Main Specification Version 1.1b, dated 22 February 2002, https://www.trustedcomputinggroup.org/specs/TPM/TCPA_Main_TCG_Architecture_v1_1b.pdf

[6] TCG PC Client Specific Implementation Specification for Conventional BIOS Version 1.2, http://www.trustedcomputinggroup.org/resources/pc_client_work_group_specific_implementation_specification_for_conventional_bios_specification_version_12

[7] Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, www.ietf.org/rfc/rfc2119.txt

[8] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3279, www.ietf.org/rfc/rfc3279.txt

[9] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, www.ietf.org/rfc/rfc3280.txt

[10] An Internet Attribute Certificate Profile for Authorization, RFC 3281, www.ietf.org/rfc/rfc3281.txt

[11] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, www.ietf.org/rfc/rfc3447.txt

[12] TCG Credentials Profile Version 1.0, https://www.trustedcomputinggroup.org/specs/IWG/Credential_Profiles_V1_rev981.pdf

[13] Hypertext Markup Language – 2.0, RFC 1866, http://www.ietf.org/rfc/rfc1866.txt