

TCG Credential Profiles

Specification Version 1.0
Revision 0.981
18 January 2006
For TPM Family 1.2; Level 2

TCG

TCG PUBLISHED

Copyright © Trusted Computing Group 2006

Copyright © 2006 Trusted Computing Group, Incorporated.

Disclaimer

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

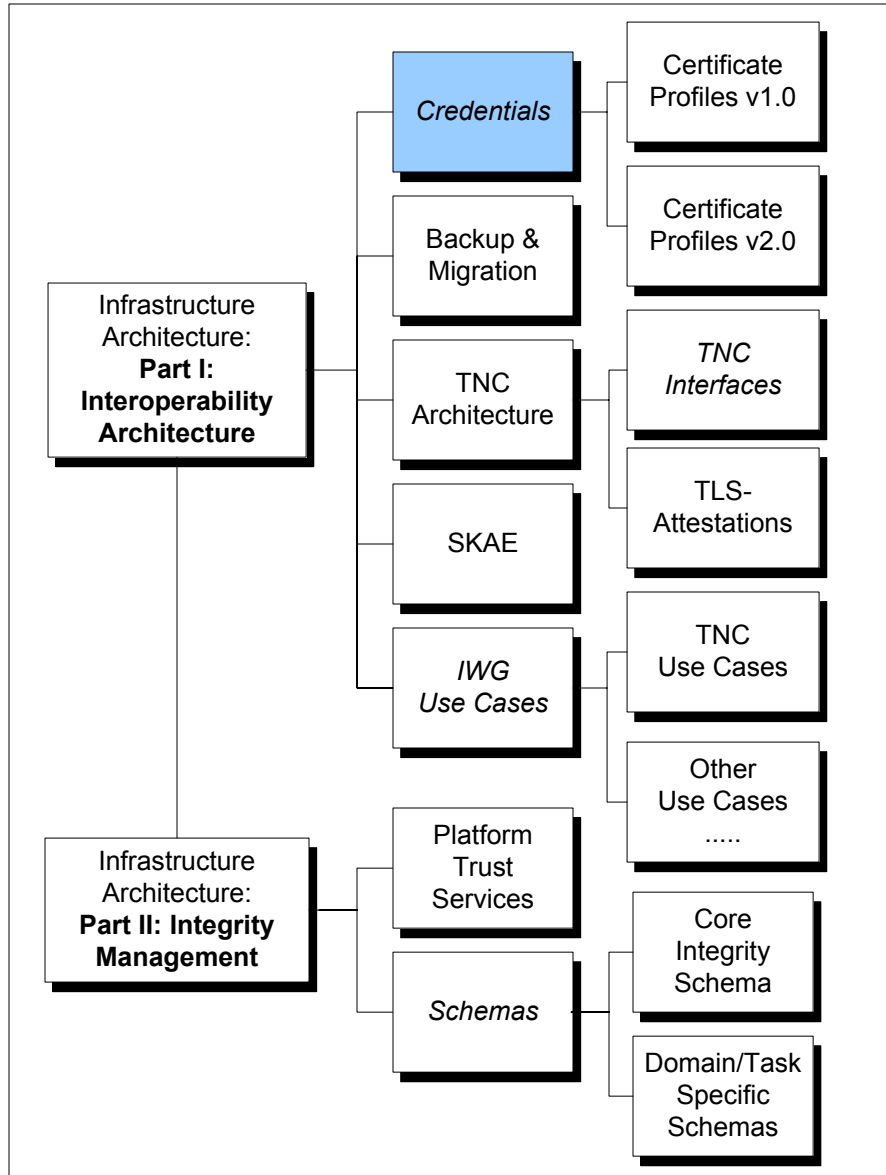
No license, express or implied, by estoppel or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

Except that a license is hereby granted by TCG to copy and reproduce this specification for internal use only.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owner

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:

Geoffrey Strongin	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	Infinion
Johann Schoetz	Infinion
David Grawrock	Intel
Ned Smith (IWG co-chair)	Intel
Monty Wiseman	Intel
Daniel Wong	Microsoft
Mark Williams	Microsoft
Mark Redman	Motorola
Laszlo Elteto	SafeNet
Manuel Offenberg	Seagate Technology
Brad Andersen	SignaCert
Nicholas Szeto	Sony
Jeff Nisewanger (editor)	Sun Microsystems
Paul Sangster	Sun Microsystems
Thomas Hardjono (IWG co-chair)	Verisign
Greg Kazmierczak	Wave Systems
Len Veil	Wave Systems
Mihran Dars	Wave Systems

Table of Contents

1	Introduction	8
1.1	Purpose	8
1.2	Scope and Document Time-Line	8
1.3	Relationship to Other TCG Specifications	8
1.4	Intended Audiences	8
1.5	Specification Design Goals	8
1.6	References to Other Documents	9
1.7	Definition of Terms	9
2	TCG 1.0 Credential Overview	10
2.1	Relationships Between the TCG Credentials	10
2.2	Fields Common to All Three TCG Credential Types	11
2.3	Endorsement Key (EK) Credential	12
2.3.1	Who Uses an EK Credential?	12
2.3.2	Who Issues an EK credential?	12
2.3.3	EK Credential Privacy Protection Requirements	12
2.3.4	EK Credential Creation Requirements	12
2.3.5	Revocation of an EK Credential	12
2.3.6	Validity Period of an EK Credential	13
2.3.7	Assertions Made By an EK Credential	13
2.3.7.1	Credential Type Label	14
2.3.7.2	Public EK	14
2.3.7.3	TPM Model	14
2.3.7.4	Issuer	14
2.3.7.5	TPM Specification	14
2.3.7.6	Signature Value	14
2.3.7.7	TPM Assertions	14
2.3.7.8	Validity Period	15
2.3.7.9	Policy Reference	15
2.3.7.10	Revocation Locator	15
2.4	Platform Credential	15
2.4.1	Who Uses a Platform Credential?	15
2.4.2	Who Issues a Platform Credential?	15
2.4.3	Platform Credential Privacy Protection Requirements	15
2.4.4	Revocation of a Platform Credential	16
2.4.5	Validity Period of a Platform Credential	16
2.4.6	Assertions Made by a Platform Credential	16
2.4.6.1	Credential Type Label	16
2.4.6.2	EK Credential	17
2.4.6.3	Platform Model	17
2.4.6.4	Issuer	17
2.4.6.5	Platform Specification	17
2.4.6.6	Signature Value	17
2.4.6.7	Platform Assertions	17
2.4.6.8	Validity Period	17
2.4.6.9	Policy Reference	17
2.4.6.10	Revocation Locator	17
2.5	Attestation Identity Key (AIK) Credential	18
2.5.1	Who Uses an AIK Credential?	18
2.5.2	Who Issues an AIK Credential?	18
2.5.3	Revocation of an AIK Credential	18
2.5.4	Validity Period of an AIK Credential	18
2.5.5	Assertions Made By an AIK Credential	19
2.5.5.1	Credential Type Label	20
2.5.5.2	Public AIK	20
2.5.5.3	TPM Model	20
2.5.5.4	Platform Model	20

2.5.5.5	Issuer	20
2.5.5.6	TPM Specification	20
2.5.5.7	Platform Specification	21
2.5.5.8	Signature Value	21
2.5.5.9	Identity Label	21
2.5.5.10	TPM Assertions	21
2.5.5.11	Platform Assertions	21
2.5.5.12	Validity Period	21
2.5.5.13	Policy Reference	21
2.5.5.14	Revocation Locator	21
3	X.509 ASN.1 Definitions	22
3.1	TCG Attributes	22
3.1.1	Security Qualities	22
3.1.2	TPM and Platform Assertions	22
3.1.3	Conformance Attributes	24
3.1.4	Name Attributes	25
3.1.5	TCG Specification Attributes	25
3.2	EK Certificate	26
3.2.1	Version	27
3.2.2	Serial Number	28
3.2.3	Signature Algorithm	28
3.2.4	Issuer	28
3.2.5	Validity	28
3.2.6	Subject	28
3.2.7	Public Key Info	28
3.2.8	Certificate Policies	28
3.2.9	Alternative Names	29
3.2.10	Basic Constraints	29
3.2.11	Subject Directory Attributes	29
3.2.12	Authority Key Id	29
3.2.13	Authority Info Access	30
3.2.14	CRL Distribution	30
3.2.15	Key Usage	30
3.2.16	Extended Key Usage	30
3.2.17	Subject Key Id	30
3.2.18	Subject and Issuer Unique Ids	30
3.3	Platform Certificate	30
3.3.1	Version	31
3.3.2	Serial Number	31
3.3.3	Signature Algorithm	31
3.3.4	Holder	32
3.3.5	Issuer	32
3.3.6	Validity	32
3.3.7	Certificate Policies	32
3.3.8	Alternative Names	32
3.3.9	Attributes	32
3.3.10	Authority Key Identifier	33
3.3.11	Authority Info Access	33
3.3.12	CRL Distribution	33
3.3.13	Subject and Issuer Unique Ids	33
3.4	AIK Certificate	33
3.4.1	Version	34
3.4.2	Serial Number	35
3.4.3	Signature Algorithm	35
3.4.4	Issuer	35
3.4.5	Validity	35
3.4.6	Subject	35

3.4.7	Public Key Info	35
3.4.8	Certificate Policies	35
3.4.9	Alternative Names.....	36
3.4.10	Basic Constraints	36
3.4.11	Subject Directory Attributes	36
3.4.12	Authority Key Id.....	37
3.4.13	Authority Info Access	37
3.4.14	CRL Distribution	37
3.4.15	Key Usage.....	37
3.4.16	Extended Key Usage	37
3.4.17	Subject Key Id	37
3.4.18	Subject and Issuer Unique Ids.....	38
4	Changes Since TCPA 1.1b	39
5	X.509 ASN.1 Structures and OIDs	40

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 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 establishes the use of these three 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.

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 how it maps to an X.509 certificate. Other documents may describe the mapping of these credentials to other formats such as those based on XML.

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 Intended Audiences

The intended audience for this document is people who work for the entities, such as Privacy-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.

1.5 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

1.6 References to Other Documents

- [1] TCG Specification Architecture Overview, Specification Version 1.2, at www.trustedcomputinggroup.org
- [2] TCG Infrastructure Working Group Reference Architecture for Interoperability (Part 1), Specification Version 1.0, at www.trustedcomputinggroup.org
- [3] TCG Main Specification Version 1.2, level 2, revision 85, dated 13 February 2005, at www.trustedcomputinggroup.org
- [4] TCG Infrastructure Working Group Subject Key Attestation Evidence Extension, Specification Version 1.0, at www.trustedcomputinggroup.org
- [5] TCPA Main Specification Version 1.1b, dated 22 February 2002, at www.trustedcomputinggroup.org
- [6] TCG PC Client Specific Implementation Specification for Conventional BIOS Version 1.2, available at www.trustedcomputinggroup.org
- [7] RFC 2119 – Key words for use in RFCs to Indicate Requirement Levels, at www.ietf.org/rfc/rfc2119.txt
- [8] RFC 3279 – Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, available at www.ietf.org/rfc/rfc3279.txt
- [9] RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, available at www.ietf.org/rfc/rfc3280.txt
- [10] RFC 3281 – An Internet Attribute Certificate Profile for Authorization, available at www.ietf.org/rfc/rfc3281.txt
- [11] RFC 3447 – Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, available at www.ietf.org/rfc/rfc3447.txt

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 an industry-standard certificate structure such as X.509 version 3. Certificate generation consists of (a) assembling values for the credential fields and, if necessary converting those values into x.509v3, XML, or other interoperability standards format 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..

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.

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 TCG Credentials

Figure 1 shows the relationship between the TCG credential types. 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.
- The AIK Credential references 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 reference to 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 contains a reference to the platform root of trust manufacturer, model, and version in the Platform Credential, shown as “B” in the diagram. Note that this reference is not to the Platform Credential itself; instead, it is a reference to the information contained within the Platform Credential that is not privacy-sensitive.

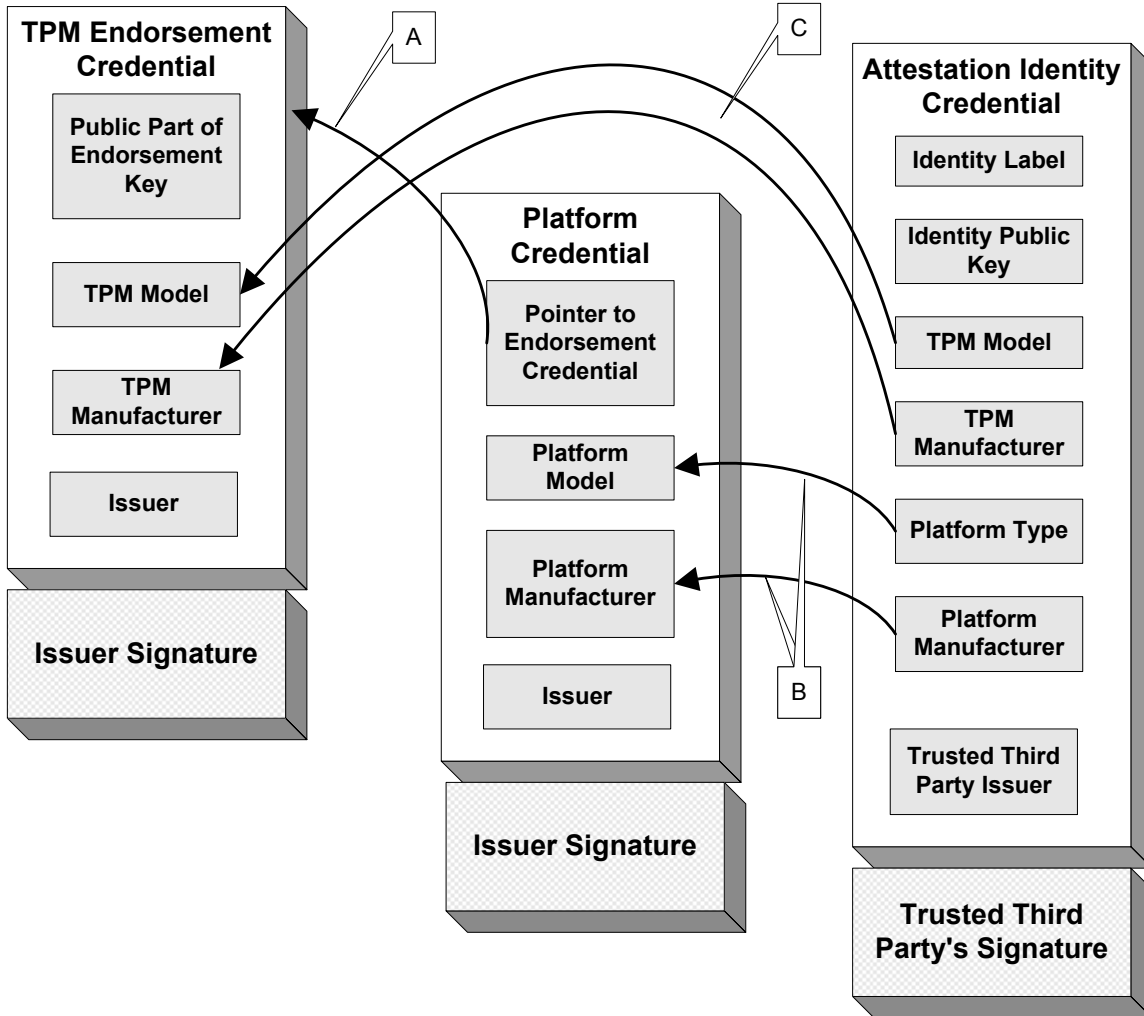


Figure 1: Credential Relationship Diagram

2.2 Fields Common to All Three TCG Credential Types

The following four fields **MUST** be included in all three 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 three TCG credential types are summarized in this section below.

2.3 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, is privacy-sensitive due to the fact that it uniquely identifies the TPM and by extension the platform.

2.3.1 Who Uses an EK Credential?

A Privacy-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.

2.3.2 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].

2.3.3 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.

2.3.4 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.

2.3.5 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.

2.3.6 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.

2.3.7 Assertions Made By an EK Credential

In general, a 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, a 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)

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	MUST
Issuer	Identifies the issuer of the credential	MUST
TPM Specification	Identifies the specification this TPM conforms to	MUST
Signature Value	Signature of the issuer over the other fields	MUST
TPM Assertions	Security-related assertions about the TPM	MAY
Validity Period	Time period when credential is valid	MAY
Policy Reference	Credential policy reference	MAY

Field Name	Description	Field Status
Revocation Locator	Identifies source of revocation status information	MAY

Table 1: EK Credential Fields

2.3.7.1 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. TCGA 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, "TCGA Trusted Platform Module Endorsement".

2.3.7.2 Public EK

The TPM public Endorsement Key value.

2.3.7.3 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].

2.3.7.4 Issuer

Identifies the entity that signed and issued the EK credential.

2.3.7.5 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.

2.3.7.6 Signature Value

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

2.3.7.7 TPM Assertions

This field may contain assertions about the security properties of the issuance process, such as, but not limited to, a description of EK creation process, whether the EK was created early or late, and/or whether the EK Credential issuance was early or late. It may also describe the conformance evaluation process for the design and implementation of the TPM.

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

2.3.7.8 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.

2.3.7.9 Policy Reference

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

2.3.7.10 Revocation Locator

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

2.4 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.

2.4.1 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].

2.4.2 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].

2.4.3 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.

2.4.4 Revocation of a Platform Credential

If the platform has the ability to be patched, the existing Platform Credential SHOULD be invalidated and MAY be revoked and 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.

2.4.5 Validity Period of a Platform Credential

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

2.4.6 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.

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
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

2.4.6.1 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. TCGA 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, “TCGA Trusted Platform Endorsement”.

2.4.6.2 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.

2.4.6.3 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.

2.4.6.4 Issuer

Identifies the entity that signed and issued the Platform Credential.

2.4.6.5 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.

2.4.6.6 Signature Value

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

2.4.6.7 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].

2.4.6.8 Validity Period

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

2.4.6.9 Policy Reference

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

2.4.6.10 Revocation Locator

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

2.5 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 and 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].

2.5.1 Who Uses an AIK Credential?

An AIK Credential is used in a Requestor-Verifier-Relying party protocol.

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.

2.5.2 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].

2.5.3 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.

2.5.4 Validity Period of an AIK Credential

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

2.5.5 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 binding / physical binding of the Root of Trust for Measurement (RTM), Root of Trust for Storage (RTS), Root of Trust for Reporting (RTR), 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.

To summarize the contents of the table, in order to meet the assertions requirements an AIK Credential **MUST** contain the following information fields, in addition to the mandatory fields that are common to all TCG credential types:

- Identity (AIK) public key
- TPM model/manufacturer/version
- Platform model/manufacturer/type

Otherwise, an AIK Credential can contain as much or as little information as dictated by requester and issuer policy. Some example optional elements that may be used in an AIK credential are listed here; to see the full list, refer to the table.

- Identity label
- Validity period (not valid before this time; not valid after this time)

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

Field Name	Description	Field Status
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

2.5.5.1 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. TCGA 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, "TCGA Trusted Platform Identity".

2.5.5.2 Public AIK

The public Attestation Identity Key.

2.5.5.3 TPM Model

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

This may be a copy of the TPM model information from the EK 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.

2.5.5.4 Platform Model

This is a copy of the platform model information from the platform credential.

2.5.5.5 Issuer

Identifies the entity that signed and issued the AIK credential.

2.5.5.6 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.

2.5.5.7 Platform Specification

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

2.5.5.8 Signature Value

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

2.5.5.9 Identity Label

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

2.5.5.10 TPM Assertions

This field may contain assertions about the security properties of the issuance process, such as, but not limited to, a description of the EK creation process, whether the EK was created early or late, and/or whether the EK certificate issuance was early or late. It may also describe the conformance evaluation process for the design and implementation of the TPM.

2.5.5.11 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..

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

2.5.5.12 Validity Period

Enables the Credential user to determine whether the AIK credential has begun to be valid and/or has expired.

2.5.5.13 Policy Reference

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

2.5.5.14 Revocation Locator

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

3 X.509 ASN.1 Definitions

This section contains the X.509 ASN.1 definitions for all the common and information fields in all three TCG credential types defined in this specification.

Instantiations of TCG credentials can be realized using ASN.1 (DER) formatting conventions. ASN.1 has been and continues to be widely used to encode a variety of data structures for a variety of purposes.

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 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 a **URIReference** which describes the URI to the document and a cryptographic hash value which identifies a specific version of the document.

```

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 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 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) }

MeasurementRootType ::= BIT STRING {
    static (0),
    dynamic (1),
    nonHost (2) }

```

```

-- common criteria evaluation

CommonCriteriaMeasures ::= SEQUENCE {
    version IA5STRING, -- "2.2" or "3.0"; future syntax defined by CC
    assuranceLevel EvaluationAssuranceLevel,
    evaluationStatus EvaluationStatus,
    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,
    hashAlgorithm AlgorithmIdentifier,
    hashValue BIT STRING }

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

-- fips evaluation

FIPSLLevel ::= SEQUENCE {
    version IA5STRING, -- "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 TCGA.

```

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  
  ID tcg-at-tpmManufacturer }  
  
TPMModel ATTRIBUTE ::= {  
  WITH SYNTAX UTF8String  
  ID tcg-at-tpmModel }  
  
TPMVersion ATTRIBUTE ::= {  
  WITH SYNTAX UTF8String  
  ID tcg-at-tpmVersion }  
  
PlatformManufacturer ATTRIBUTE ::= {  
  WITH SYNTAX UTF8String  
  ID tcg-at-platformManufacturer }  
  
PlatformModel ATTRIBUTE ::= {  
  WITH SYNTAX UTF8String  
  ID tcg-at-platformModel }  
  
PlatformVersion ATTRIBUTE ::= {  
  WITH SYNTAX UTF8String  
  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 TCG 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,  
  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) }
```

3.2 EK Certificate

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 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
Certificate Policies	Policy terms under which the certificate was issued	MUST
Alternative Names	Name forms other than directory distinguished names	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
Subject Key Id	Identifies the subject public key of the certificate	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

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).

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

3.2.2 Serial Number

The serial number MUST be a positive integer which is uniquely assigned to each EK certificate by the issuer.

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.

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

3.2.4 Issuer

The distinguished name of the TPM endorsement entity which is the entity that asserts that the subject TPM conforms with 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

This 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.

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 Alternative Names

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

Assign "critical" the value TRUE. Assign "CA" the value FALSE.

3.2.11 Subject Directory Attributes

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

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

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 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.

3.3 Platform Certificate

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
------------	-------------	--------------

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
Certificate Policies	Policy terms under which the certificate was issued	MUST
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
Subject Unique Id	Unique value when using a shared subject name	SHOULD NOT
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).

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

3.3.2 Serial Number

The serial number MUST be a positive integer which is uniquely assigned to each certificate by the issuer.

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.

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

3.3.4 Holder

BaseCertificateID referencing the corresponding TPM EK certificate.

3.3.5 Issuer

The distinguished name of the entity that is issuing 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 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.

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 Alternative Names

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

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

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 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 AIK Certificate

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 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
Certificate Policies	Policy terms under which the certificate was issued	MUST
Alternative Names	Name forms other than directory distinguished names.	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
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
Issuer Unique Id	Unique value when using a shared issuer name	SHOULD NOT

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).

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

3.4.2 Serial Number

The serial number MUST be a positive integer which is uniquely assigned to each AIK certificate by the issuer.

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.

```
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 with the TCG specification.

3.4.5 Validity

This 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.

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 Alternative Names

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

Assign “critical” the value TRUE. Assign “CA” the value FALSE.

3.4.11 Subject Directory Attributes

The extension 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

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

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 Subject Key Id

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

3.4.18 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.

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.

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 TCGA.

```
-- 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-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-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,
    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) }

-- tcg 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
    ID tcg-at-tpmManufacturer }

TPMModel ATTRIBUTE ::= {
    WITH SYNTAX UTF8String
    ID tcg-at-tpmModel }

TPMVersion ATTRIBUTE ::= {
    WITH SYNTAX UTF8String
    ID tcg-at-tpmVersion }

PlatformManufacturer ATTRIBUTE ::= {
    WITH SYNTAX UTF8String
    ID tcg-at-platformManufacturer }

PlatformModel ATTRIBUTE ::= {
    WITH SYNTAX UTF8String
    ID tcg-at-platformModel }

PlatformVersion ATTRIBUTE ::= {
    WITH SYNTAX UTF8String
    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 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 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) }

MeasurementRootType ::= ENUMERATED {
    static (0),
    dynamic (1),
    nonHost (2) }

-- common criteria evaluation

CommonCriteriaMeasures ::= SEQUENCE {
    version IA5STRING, -- "2.2" or "3.0"; future syntax defined by CC
    assuranceLevel EvaluationAssuranceLevel,
    evaluationStatus EvaluationStatus,
    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,
    hashAlgorithm AlgorithmIdentifier,
    hashValue BIT STRING }

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

-- fips evaluation

FIPSLevel ::= SEQUENCE {
    version IA5STRING, -- "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
```