TCG Platform Attribute Credential Profile

Specification Version 1.0
Revision 16
16 January 2018
Published

Contact: admin@trustedcomputinggroup.org

TCG Published

TCG

Disclaimers, Notices, and License Terms

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 (IWG co-chair)	Carolin Latze
Dean Liberty	AMD
Randy Mummert	Atmel
Malcolm Duncan	CESG
Bill Jacobs	Cisco
Max Pritikin	Cisco
Kazuaki Nimura	Fujitsu
Monty Wiseman (IWG co-chair)	GE
Graeme Proudler	Graeme Proudler
Takeuchi Keisuke	Hitachi
Hisanori Mishima	Hitachi
Tom Laffey	HPE
Diana Arroyo	IBM
Lee Terrell	IBM
Roger Zimmermann	IBM
Markus Gueller	Infineon
Johann Schoetz	Infineon
Arkadiusz Berent	Intel
David Grawrock	Intel
Eduardo Cabre	Intel
Geoffrey Strongin	Intel
Ned Smith	Intel
David Challener	John Hopkins University
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	Sun Microsystems
Jeff Nisewanger	Sun Microsystems
Paul Sangster	Symantec Corporation
Thomas Hardjono	Wave Systems
Greg Kazmierczak	Wave Systems
Len Veil	Wave Systems
Mihran Dars	Wave Systems

Table of Contents

Table of Tables

Change Log

Date	Version	Comment
2018-01-11	1.0	Initial Release

1. Introduction

1.1 Purpose

The purpose of this document is to define the Platform Attribute Credential profile. This specification contains the description of the credential and a sample X.509 instance of the credential which vendors and customers could use with their products. This specification is based on the Platform Credential defined in the TPM 1.2 TCG Credential Profiles document, section 2.5 [6].

This specification builds upon the Platform Credential specification version 1.2 [6] by incorporating the following changes:

- Adds the Platform Serial Number attribute extension. The intent is to associate the certificate to the platform identity by incorporating the platform serial number in the certificate.
- Adds the Platform Manufacturer Identifier to the Subject Alternative Name extension. The manufacturer ID is based on the IANA Private Enterprise Number [8], allowing unambiguous manufacturer identification.
- Incorporates Platform Attribute Credential Profile Specification Version, Level, and Revision extension.
- Adds the Platform Configuration extension containing list of platform components, non-security properties, and platform property URI.
- Includes a Platform Configuration URI attribute where valid PCR values can be published by the manufacturer.
- Introduces Public Key certificate format for the Platform Credential. Manufacturer may choose between Attribute Certificate format RFC 5755 [11] or a Public Key Certificate format RFC 5280 [13] when creating Platform Certificates.
- Replaces SHA1 based signatures with any signature algorithm listed in the TCG Algorithm Registry [12].
- Exclusive RSA based signing is no longer required, instead, this specification will support all algorithms listed in the TCG Algorithm Registry [12].

This credential replaces the existing Platform Credential Specification version 1.2 [6]. This credential attests that a specific manufactured platform, identified by the platform serial number and TPM EK certificate, contains a unique TPM and Trusted Building Block (TBB).

1.2 Document Scope

This document specifies a full definition of the Platform Attribute Credential for use with any TPM Family version. This specification describes the abstract definition of the credential and specifically how it would appear as an X.509 certificate.

1.3 Relationship to Other TCG Specifications

This specification references the TCG Infrastructure Working Group Reference Architecture for Interoperability [1], the TCG TPM Main Specification [3], the TCG Credential Profiles for TPM Family 1.2 [6], the EK Credential Profile Specification [7], the PC Client Platform TPM

Profile Specification [10], and the Generic Server Platform Specification [9]. The Platform Attribute Credential Specification replaces the Platform Credential Specification defined in the TCG Credential Profiles for TPM Family 1.2 [6]. This specification also references the TCG Algorithm Registry Specification [12].

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 [4].

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 the architectural framework described in the document entitled “TCG Infrastructure Working Group Reference Architecture for Interoperability” [1] In particular, see sections 3, 4, 5, and 6.

1.6 Definition of Terms

The TCG Glossary [1] contains definitions that are fundamental to this specification. Rather than repeat those definitions, the reader is assumed to be familiar with the terms in the TCG glossary.

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. Credential Overview

This section describes the Platform Attribute Credential type. The Platform Attribute Credential provides the foundation for binding the identity of the platform to the TPM and the Trusted Building Block of the platform.

2.1 Platform Attribute Credential

A Platform Attribute 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 Attribute Credential is the platform manufacturer (for example, an OEM). An entity should not generate a Platform Attribute Credential unless the entity is satisfied that the platform contains the TPM referenced inside the credential. Platform Attribute Credentials contain assertions about trust made by a platform manufacturer.

The consumer of a Platform Attribute Credential is a Privacy-CA. A Platform Attribute 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 Attribute Credential to a new AK Credential that the Privacy-CA creates for a trusted platform.

Another consumer of the Platform Credential is an Enterprise, which wishes to remotely provision multiple devices that belong to it. Typically, in this case the Enterprise knows the serial number of the systems it owns, and the Platform Credential is used to associate those serial numbers with particular EK certificates [6][7]. This way, for example, a VPN can be provisioned using the TPM to provide keys securely to clients of an Enterprise.

2.1.1 Who Uses a Platform Attribute Credential?

A Privacy-CA is one of the users of a Platform Attribute Credential. For more information, refer to section 6.2 of Reference Architecture for Interoperability Specification [1].

An Enterprise may use a Platform Attribute Credential to correlate a list of platform serial numbers (used for physical property management) with EK Credentials (used for logical property management). In order to support this use case, the optional Platform Serial Number attribute MUST be included in the certificate. In addition, an Enterprise may use the Platform Attribute Credential to assert non-security related properties included optionally by the platform manufacturer in the certificate.

2.1.2 Who Issues a Platform Attribute Credential?

Several different types of entities in the platform manufacturing supply chain may sign a Platform Attribute Credential. For more information, refer to section 3 of Reference Architecture for Interoperability Specification [1].

2.1.3 Platform Attribute Credential Privacy Protection Requirements

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

2.1.4 Revocation of a Platform Attribute Credential

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

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

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

2.1.5 Validity Period of a Platform Attribute Credential

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

2.1.6 Assertions Made by a Platform Attribute 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 Attribute 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 Manufacturer	Name of platform manufacturer	MUST
Platform Model	Manufacturer-specific identifier	MUST
Platform Version	Manufacturer-specific identifier	MUST
Issuer	Identifies the issuer of the credential	MUST
Platform Specification	Platform Specification to which this platform is built	MUST
Credential Specification	Platform Attribute Certificate Specification Version, Level, and Revision	MUST

Validity Period	Time period when credential is valid	MUST
Signature Value	Signature of the issuer over the other fields	MUST
Platform Serial Number	Platform's unique serial number	MAY
Platform Assertions	Security assertions about the platform	MAY
Platform Configuration	Non-security related platform properties	MAY
Manufacturer Identifier	Platform manufacturer unique identifier	MAY
Platform Configuration Uri	URI where PCR information can be obtained	MAY
Policy Reference	Credential policy reference	MAY
Revocation Locator	Identifies source of revocation status information	MAY

126 **Table 1: Platform Attribute Credential Fields**

127 2.1.6.1 Credential Type Label

128 The label enables the issuer to sign the credential with a key that is not reserved exclusively
129 for signing a Platform Attribute Credential. It allows different types of credentials to be reliably
130 distinguished from each other by this label instead of based on which signer key was used.
131 TCG [3] reserved this flexible key re-purposing capability and the credential labels have been
132 retained for compatibility.

133 For Platform Attribute Credentials, the value of this field must be the string, "TCG Trusted
134 Platform Endorsement".

135 2.1.6.2 EK Credential

136 This assertion is used by the Privacy-CA to verify that the platform contains a unique TPM
137 referenced by this Platform Attribute Credential.

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

140 2.1.6.3 Platform Model

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

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

144 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.

2.1.6.4 Platform Manufacturer Identifier

This assertion identifies the platform manufacturer with a globally unique and verifiable value. If included, the issuer SHALL use the manufacturer's Internet Assigned Numbers Authority (IANA) Private Enterprise Number as the identifier [8].

2.1.6.5 Issuer

This assertion identifies the entity that signed and issued the Platform Attribute Credential.

2.1.6.6 Platform Specification

This assertion identifies the relevant TCG platform specific specification to which the platform was designed. This describes the platform class as well as the major and minor version number and the revision level.

2.1.6.7 Credential Specification

This assertions identifies the Platform Attribute Credential Specification version. Includes this specification's Version, Level, and Revision.

2.1.6.8 Validity Period

This assertion enables the credential user to determine whether the Platform Attribute Credential has begun to be valid or has expired.

2.1.6.9 Signature Value

This assertion is the signature of the issuer over the other fields in the credential.

2.1.6.10 Platform Serial Number

This assertion is a value that uniquely identifies the platform. This is used by the verifier to correlate the certificate to a physical platform. The manufacturer SHALL use a customer visible serial number as the identifier. Even though this attribute is optional, the field MUST be included when enabling Enterprise use cases such as remote provisioning using the platform TPM.

The Platform Serial Number is encoded as a string and is manufacturer specific.

2.1.6.11 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 [1].

2.1.6.12 Platform Configuration

This field contains assertions of properties that are not security related. These properties MAY include the platform's component serial numbers, network adapter MAC addresses, and motherboard serial number.

2.1.6.13 Platform Configuration Uri

This assertion provides an optional Uniform Resource Identifier where valid PCR and platform configuration information can be obtained.

2.1.6.14 Policy Reference

This assertion enables the credential user to identify the credential issuance policy of the Platform Attribute Credential issuer.

2.1.6.15 Revocation Locator

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

3. X.509 ASN.1 Definitions

This section contains the format for the Platform Attribute Credential instantiated as an X.509 certificate for all the common and information fields in this specification. All fields are defined in ASN.1 and encoded using DER.

3.1 TCG Attributes

3.1.1 Security Qualities

This attribute describes the platform security qualities in the platform attribute certificate.

The text string describing the qualities of the TPM is manufacturer-specific. This attribute is deprecated but is retained for compatibility with previously published TCG and TCPA specifications. If present, the security qualities attribute, which has manufacturer-specific syntax, should be consistent with any Platform Assertions 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 that 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 **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.

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[5].

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) }

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 }

-- 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 {
    levell (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

Conformance Attributes are 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 previously published TCG and TCPA specifications.

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

    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.

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

The value of the **PlatformManufacturerStr a**ttribute is a UTF 8 string with the name of platform manufacturing company.

The **PlatformModel** attribute is a UTF 8 string with the manufacturer-specific model.

The **PlatformVersion** attribute is a UTF 8 string with manufacturer-specific platform version value.

The **PlatformSerial** optional attribute is a UTF 8 string with manufacturer-specific platform serial number value.

The **PlaftformManufacturerId** optional attribute is the OID of the IANA Private Enterprise Number [8] assigned to the platform manufacturer.

```
    PlatformManufacturerStr 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 }

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

PlatformManufacturerId ATTRIBUTE ::= {
    WITH SYNTAX ManufacturerId
    ID tcg-at-platformManufacturerId
}

ManufacturerId ::= SEQUENCE {
   manufacturerIdentifier   PrivateEnterpriseNumber
}

enterprise OBJECT IDENTIFIER :: = {
    iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)}

PrivateEnterpriseNumber OBJECT IDENTIFIER :: = { enterprise private-enterprise-number }
```

All assigned private enterprise numbers are listed at the Internet Assigned Numbers Authority (IANA) web site [8].

3.1.5 TCG Specification Attributes

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

The **TCGPlatformSpecification** attribute identifies the platform class, version and revision of the platform-specific specification with which a platform implementation is compliant. The platform specification refers either to the PC Client Platform Specification [10] or the Server Specification [9]. 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) }
```

3.1.5.1 TCG Credential Specification Attributes

The following defines the syntax of the credential specification attributes.

The **TCGCredentialSpecification** attribute identifies the major version, minor version, and revision of the credential specification with which a certificate is compliant. Values are encoded as three integers in this attribute.

```
tCGCredentialSpecification ATTRIBUTE ::= {
    WITH SYNTAX TCGSpecificationVersion
    ID tcg-at-tcgCredentialSpecification }

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

3.1.5.2 Platform Configuration

The following defines the syntax of the platform configuration attribute.

The **platformConfiguration** attribute contains optional lists of platform components, platform properties, and platform property URI. The **componentIndentifer** field may contain a list of individual components that constitute the platform. The issuer must include the component manufacturer and model, and optionally provide the component serial number, revision, and the component manufacturer's IANA **PrivateEnterpriseNumber**. If known, the issuer must indicate whether the component is field replaceable (removable or pluggable), and may provide MAC addresses associated with the component.

The optional **platformProperties** field shall contain characteristics of the platform that the issuer may consider of interest to the consumer. Such properties are not prescribed by this specification and the certificate issuer is free to choose which information to include in this field. The manufacturer may use the **platformPropertiesUri** to publish information about the Properties included in the **platformProperties** field. This may include the list of **propertyName** and their semantics.

```
platformConfiguration ATTRIBUTE ::= {
    WITH SYNTAX PlatformConfiguration
    ID tcg-at-platformConfiguration-v1
}

PlatformConfiguration ::= SEQUENCE {
    componentIdentifier   [0]   IMPLICIT   SEQUENCE(SIZE(1..CONFIGMAX))   OF   ComponentIdentifier
        OPTIONAL,
    platformProperties [1] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF Properties OPTIONAL,
    platformPropertiesUri [2] IMPLICIT URIReference OPTIONAL
}

ComponentIdentifier ::= SEQUENCE {
    componentManufacturer UTF8String (SIZE (1..STRMAX)),
    componentModel UTF8String (SIZE (1..STRMAX)),
    componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
    componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
    componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,
    fieldReplaceable [3] IMPLICIT BOOLEAN OPTIONAL,
    componentAddress [4] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF ComponentAddress OPTIONAL }

ComponentAddress ::= SEQUENCE {
    addressType AddressType,
    addressValue UTF8String (SIZE (1..STRMAX)) }

AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
    bluetoothmac)

Properties ::= SEQUENCE {
    propertyName UTF8String (SIZE (1..STRMAX)),
    propertyValue UTF8String (SIZE (1..STRMAX)) }
```

CONFIGMAX is a constant used to provide an upper bound on the platform configuration lists. This upper bound is helpful to limit the overall size of the certificate, while providing sufficient space to convey the necessary information. CONFIGMAX SHOULD NOT exceed a value of 32.

3.1.5.3 Platform Configuration Uri Attribute

The following defines the syntax of the platform configuration Uri attribute.

The **PlatformConfigUri** attribute contains the URI where valid Platform Configuration Registers values can be obtained. The attesting party may obtain the platform's valid measurement hashes from this location. Value is encoded as an **URIReference** sequence.

```
PlatformConfigUri ATTRIBUTE ::= {
    WITH SYNTAX URIReference
    ID tcg-at-platformConfigUri  }
```

3.2 Attribute Certificate Format

This section contains the format for a Platform Attribute Credential conforming to version 1.0 of this specification.

The Platform Attribute Credential makes the assertions listed in section 2.1.6. This certificate format adheres to RFC 5755 [11] 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	**RFC 5755 Type**	**Value**	**Field Status**
Version	INTEGER	V2 (encoded as value 1)	Standard
Serial Number	INTEGER	Positive integer value unique relative to the issuer	Standard
Signature Algorithm	AlgorithmIdentifier	Algorithm used by the issuer to sign this certificate	Standard
Holder	Holder	Identity of the associated TPM EK Certificate, use BaseCertificateID.	Standard
Issuer	Name	Distinguished name of the platform certificate issuer	Standard
Validity	notBefore notAfter	Beginning and end of validity period	Standard
Attributes	Attributes	Information about the platform of this certificate	Standard
Extensions			
Certificate Policies	CertificatePolicies	CertPolicyId CPSuri UserNotice	MUST Non-critical

Field Name	**RFC 5755 Type**	**Value**	**Field Status**
Subject Alternative Names	GeneralName directoryName	PlatformManufacturerStr PlatformModel PlatformVersion PlatformSerial (optional) PlatformManufacturerId (optional)	MUST non-critical
Authority Key Id	AuthorityKeyIdentifier	Key identifier Issuer name and serial number (optional)	MUST non-critical
Authority Info Access	AuthorityInfoAccessSyntax	id-ad-caIssuers URI to issuing CA id-ad-ocsp (optional) URI to OCSP responder	SHOULD non-critical
CRL Distribution	CRLDistributionPoints	URI to CRL	MAY non-critical
Issuer Unique Id	UniqueIdentifier	Unique value when using a shared issuer name	SHOULD NOT

Table 2: Attribute Certificate Format Fields

3.2.1 Version

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

3.2.2 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".

3.2.3 Signature Algorithm

This OID identifies the algorithm used by the platform certificate issuer to sign the certificate. Platform Attribute Certificate verifiers MUST support certificates signed with algorithms available in the TCG Algorithm Registry [12].

3.2.4 Holder

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

3.2.5 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.

3.2.6 Validity

This field 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 5755, section 4.2.6.

3.2.7 Certificate Policies

This extension indicates policy terms under which the certificate was issued.

Assign “critical” the value FALSE. 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 “TCG Trusted Platform Endorsement”.

During certificate path validation, check that at least one acceptable policyIdentifier value is present.

3.2.8 Subject Alternative Names

This extension contains the alternative name of the entity associated with this certificate. Assign "critical" the value FALSE. Include the platform model, using the directory name-form with RDNs for the platform manufacturer, model, version number, and optionally, the serial number, and manufacturer ID. The “Platform Manufacturer Identifier” optional field uniquely identifies the platform’s manufacturer using the IANA Private Enterprise Number OID [8].

During certificate validation, the Privacy-CA MUST check that the platform manufacturer, model, version, serial numbers, and manufacturer ID are acceptable.

3.2.9 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 “TCG Credential Specification” attribute references the version, level, and revision of this specification.
- The platform “TBB Security Assertions” attribute describes various assertions about the security properties of the TBB of the platform.

The following attributes MAY be included:

- The “Platform Configuration” attribute describes various assertions of platform properties that are not security related. Including CPU and motherboard serial numbers, network adapter MAC addresses.
- The “Platform Configuration Uri” attribute which provides the URI to the manufacturer published list of valid PCR values.

The following attributes are documented for compatibility with previous published TCG or TCPA specifications but SHOULD NOT be included in Platform Attribute Certificates:

- 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.

3.2.10 Authority Key Identifier

This extension 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.

3.2.11 Authority Info Access

This extension contains additional information about the issuer. Assign “critical” the value FALSE. It MAY be omitted. If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 5755 [11]) 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.

3.2.12 CRL Distribution

This extension provides the location of the subject’s revocation information. Assign “critical” the value FALSE. 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.

3.2.13 Issuer Unique Id

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

3.3 Public Key Certificate Format

This section contains the format for a Platform Public Key Credential conforming to a standard X.509 public key certificate.

The Platform Public Key Certificate makes the assertions listed in section 2.1.6. The platform certificate supports a public key certificate profile of RFC 5280 [13] 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	**RFC 5280 Type**	**Value**	**Field Status**
Version	INTEGER	V3 (encoded as value 2)	Standard
Serial Number	INTEGER	Positive integer	Standard
Signature Algorithm	AlgorithmIdentifier	Algorithm used by the issuer to sign this certificate	Standard
Issuer	Name	Distinguished name of the platform certificate issuer	Standard
Validity	notBefore notAfter	Beginning and end of validity period	Standard
Subject	Name	Platform name assigned by the manufacturer or empty	Standard
Subject Public Key Info	SubjectPublicKeyInfo	The platform's TPM EK public key	Standard
Extensions			
Certificate Policies	CertificatePolicies	CertPolicyId CPSuri UserNotice	MUST non-critical

Field Name	**RFC 5280 Type**	**Value**	**Field Status**
Subject Alternative Name	GeneralName directoryName	PlatformManufacturerStr PlatformModel PlatformVersion PlatformSerial (optional) PlatformManufacturerId (optional)	MUST critical/ non-critical (depending on subject)
Basic Constraints	BasicConstraints	CA=FALSE	MUST critical
Subject Directory Attributes	SubjectDirectoryAttributes	TCGPlatformSpecification TCGCertificateSpecification TBBSecurityAssertions PlatformConfiguration (optional) PlatformConfigurationUri (optional)	MUST non-critical
Authority Key Id	AuthorityKeyIdentifier	Key identifier Issuer name and serial number (optional)	MUST non-critical
Authority Info Access	AuthorityInfoAccessSyntax	id-ad-caIssuers URI to issuing CA id-ad-ocsp (optional) URI to OCSP responder	SHOULD non-critical
CRL Distribution	CRLDistributionPoints	URI to CRL	MAY non-critical
Key Usage	KeyUsage	keyEncipherment or keyAgreement or digitalSignature	MUST critical
Extended Key Usage	ExtKeyUsageSyntax	tcg-kp-PlatformKeyCertificate	SHOULD non-critical
Subject Key Id	SubjectKeyIdentifier	Key identifier	MAY

583 **Table 3: Public Key Certificate Format Fields**

3.3.1 Version

This field contains the version of the certificate syntax. Version number must be set to 3 (which is encoded as the value 2 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 Attribute Certificate verifiers MUST support certificates signed with algorithms available in the TCG Algorithm Registry [12].

3.3.4 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.

3.3.5 Validity

This field 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 5280 [13].

3.3.6 Subject

This field MUST contain an X.500 distinguished name (DN) that uniquely identifies the platform or, if unique identification through the subject field is not required, MUST be empty.

If the subject name field is empty, the subject alternative name extension MUST be critical in accordance with RFC 5280[13], otherwise it SHOULD be non-critical.

3.3.7 Subject Public Key Info

This field describes the public Endorsement Key algorithm and key value obtained from the platform's TPM EK Certificate. This field must comply with the Subject Public Key Info requirement defined in the TCG EK Credential Profile Specification [7]. The Privacy-CA SHOULD transfer the SubjectPublicKeyInfo from the EK Certificate to the Platform Attribute Certificate.

3.3.8 Certificate Policies

This extension indicates policy terms under which the certificate was issued.

Assign “critical” the value FALSE. 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 “TCG Trusted Platform Endorsement”.

During certificate path validation, check that at least one acceptable policyIdentifier value is present.

3.3.9 Subject Alternative Name

This extension contains the alternative name of the entity associated with this certificate. Assign "critical" the value TRUE if Subject is empty, FALSE otherwise. Include the platform model, using the directory name-form with RDNs for the platform manufacturer, model, version number, and optionally, the serial number, and manufacturer ID. The “Platform Manufacturer Identifier” optional field uniquely identifies the platform’s manufacturer using the IANA Private Enterprise Number OID [8].

During certificate validation, the Privacy-CA MUST check that the platform manufacturer, model, version, serial numbers, and manufacturer ID are acceptable.

3.3.10 Basic Constraints

This extension indicates whether the subject is a CA. “CA” MUST be set to FALSE. This extension MUST be critical.

3.3.11 Subject Directory Attributes

The extension includes miscellaneous properties and security assertions about the platform’s manufacturer. This extension MUST be non-critical. 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 “TCG Credential Specification” attribute references the version, level, and revision of this specification.
- The platform “TBB Security Assertions” attribute describes various assertions about the security properties of the TBB of the platform.

The following attributes MAY be included:

- The “Platform Configuration” attribute describes various assertions of platform properties that are not security related including CPU and motherboard serial numbers, network adapter MAC addresses.
- The “Platform Configuration Uri” attribute that provides the URI to the manufacturer published list of valid PCR values.

The following attributes are documented for compatibility with previously published TCG or TCPA specifications but SHOULD NOT be included in Platform Attribute Certificates:

- 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.

3.3.12 Authority Key Identifier

This extension 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 derive from the issuer’s public key.

3.3.13 Authority Info Access

This extension contains additional information about the issuer. It MAY be included. If included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 5755 [11]) 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.

3.3.14 CRL Distribution

This extension 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.

3.3.15 Key Usage

This extension indicates the intended purpose of the subject public key as defined in the platform’s TPM EK Certificate. This field must comply with the Key Usage requirement defined in the TCG EK Credential Profile Specification [7]. The Privacy-CA SHOULD transfer the KeyUsage field from the EK Certificate to the Platform Attribute Certificate.

This extension MUST be critical.

3.3.16 Extended Key Usage

This extension indicates the intended purpose of the subject public key. Extended key usage SHOULD contain the OID tcg-kp-PlatformKeyCertificate defined in section 4 of this

document. The OID is used to unambiguously identify the certificate as a Platform Public Key Certificate. This extension MUST be non-critical.

NOTE: If the issuing CA is used exclusively to issue Platform certificates, it is recommended to include the OID tcg-kp-PlatformKeyCertificate in the issuing CA certificate. This ensures that the use of the CA is limited to that particular purpose. If the issuing CA issues certificates for multiple known purposes, then the set of relevant EKU OIDs could be included in the issuing CA certificate.

3.3.17 Subject Key Identifier

This extension identifies the public key of the certificate. This extension MAY be included in Platform certificates.

4. 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 specifications. These definitions are intended to be used within the context of an X.509 v3 certificate specifically leveraging the profile described in RFC 5755.

```
-- 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-platformClass OBJECT IDENTIFIER ::= {tcg 5}
tcg-ce OBJECT IDENTIFIER ::= {tcg 6}
tcg-kp OBJECT IDENTIFIER ::= {tcg 8}
tcg-address OBJECT IDENTIFIER ::= {tcg 17}

-- 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-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-at-tcgCredentialSpecification OBJECT IDENTIFIER ::= {tcg-attribute 23}

-- TCG Platform Class Common OIDs
tcg-common OBJECT IDENTIFIER ::= { tcg-platformClass 1}

-- TCG Common Attribute OIDs
tcg-at-platformManufacturerStr OBJECT IDENTIFIER ::= {tcg-common 1}
tcg-at-platformManufacturerId OBJECT IDENTIFIER ::= {tcg-common 2}
tcg-at-platformConfigUri OBJECT IDENTIFIER ::= {tcg-common 3}
tcg-at-platformModel OBJECT IDENTIFIER ::= {tcg-common 4}
tcg-at-platformVersion OBJECT IDENTIFIER ::= {tcg-common 5}
tcg-at-platformSerial OBJECT IDENTIFIER ::= { tcg-common 6}
tcg-at-platformConfiguration OBJECT IDENTIFIER ::= {tcg-common 7}

-- TCG Platform Configuration OIDs
tcg-at-platformConfiguration-v1 OBJECT IDENTIFIER ::= {tcg-at-platformConfiguration 1}

-- 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-kp-PlatformKeyCertificate OBJECT IDENTIFIER ::= {tcg-kp 4}

-- 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 }

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

PlatformManufacturerId ATTRIBUTE ::= {
    WITH SYNTAX ManufacturerId
    ID tcg-at-platformManufacturerId
}

ManufacturerId ::= SEQUENCE {
   manufacturerIdentifier   PrivateEnterpriseNumber
```

```
}

enterprise OBJECT IDENTIFIER :: = {
    iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)}

PrivateEnterpriseNumber OBJECT IDENTIFIER :: = { enterprise private-enterprise-number }


-- 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 {
    levell (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} }

-- platform configuration
platformConfiguration ATTRIBUTE ::= {
    WITH SYNTAX PlatformConfiguration
    ID tcg-at-platformConfiguration-v1
}

PlatformConfiguration ::= SEQUENCE {
    componentIdentifier   [0]   IMPLICIT   SEQUENCE(SIZE(1..CONFIGMAX))   OF   ComponentIdentifier
        OPTIONAL,
    platformProperties [1] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF Properties OPTIONAL
}

ComponentIdentifier ::= SEQUENCE {
    componentManufacturer UTF8String (SIZE (1..STRMAX)),
    componentModel UTF8String (SIZE (1..STRMAX)),
    componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
    componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
    componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,
    componentAddress [3] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF ComponentAddress OPTIONAL }
```

```
ComponentAddress ::= SEQUENCE {
    addressType AddressType,
    addressValue UTF8String (SIZE (1..STRMAX)) }

AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
bluetoothmac)

Properties ::= SEQUENCE {
    propertyName UTF8String (SIZE (1..STRMAX)),
    propertyValue UTF8String (SIZE (1..STRMAX)) }

-- platform configuration Uri attribute
PlatformConfigUri ATTRIBUTE ::= {
    WITH SYNTAX URIReference
    ID tcg-at-platformConfigUri  }

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

-- TCG Address OIDs
tcg-address-ethernetmac OBJECT IDENTIFIER ::= {tcg-address 1}
tcg-address-wlanmac OBJECT IDENTIFIER ::= {tcg-address 2}
tcg-address-bluetoothmac OBJECT IDENTIFIER ::= {tcg-address 3}
```

5. References

[1] TCG Glossary, https://trustedcomputinggroup.org/glossary

[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] TCPA Main Specification, Version 1.1b, http://www.trustedcomputinggroup.org/tcpa-main-specification-version-1-1b/

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

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

[6] TCG Credential Profiles For TPM Family 1.2 Specification Version 1.2, http://www.trustedcomputinggroup.org/infrastructure-work-group-tcg-credential-profiles-specification/

[7] TCG EK Credential Profile for TPM Family 2.0, Specification Version 2.0, http://www.trustedcomputinggroup.org/tcg-ek-credential-profile-tpm-family-2-0/

[8] IANA Private Enterprise Numbers, http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

[9] Server Work Group Generic Server Specification, Version 1.0, http://www.trustedcomputinggroup.org/server-work-group-generic-server-specification-version-1-0/

[10] PC Client Platform TPM Profile (PTP) Specification , http://www.trustedcomputinggroup.org/pc-client-platform-tpm-profile-ptp-specification/

[11] An Internet Attribute Certificate Profile for Authorization, www.ietf.org/rfc/rfc5755.txt

[12] TCG Algorithm Registry, http://www.trustedcomputinggroup.org/tcg-algorithm-registry/

[13] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://www.ietf.org/rfc/rfc5280.txt