TCG Platform Certificate Profile

Specification Version 1.1
Revision 19
10 April 2020
Published

Contact: admin@trustedcomputinggroup.org

TCG PUBLISHED

Disclaimers, Notices, and License Terms

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.

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

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 Baumgartner (IWG co-chair)	Carolin Baumgartner
Dean Liberty	AMD
Randy Mummert	Atmel
Malcolm Duncan	CESG
Bill Jacobs	Cisco
Max Pritikin	Cisco
Amy Nelson	Dell
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
Ken Goldman	IBM
Markus Gueller	Infineon
Johann Schoetz	Infineon
Arkadiusz Berent	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
Andrew Medak	United States Government
Lawrence Reinert	United States Government
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
2020-04-03	1.1	Addition of Delta Platform Certificate and tree hierarchy. Section "Revocation of a Platform Certificate" has been modified to include multiple causes of revocation. Section "EK Certificates" clarifies which EK Certificates must be included as reference. Section "Holder" clarifies use of the TargettingInformation extension to reference additional EK Certificates. Section "X.509 ASN.1 Structures and OIDs" includes the correct CertificateIdentifier sequence. Section "Assertions Made by a Platform Certificate" includes additional assertions. Section "Platform Configuration Attributes" was updated to include additional attributes. Section "Targeting Information" was added. Sample certificates were added to Appendix. The following sections were removed: • Platform Attribute Credential Privacy Protection Requirements • Security Qualities • Conformance Attributes

1. Introduction

1.1 Purpose

The purpose of this document is to define the Platform Certificate profile. This specification contains the description of the certificate and sample X.509 instances of the certificate which vendors and customers could use with their products. This specification defines the Platform Certificate for use with any TPM Family 1.2 and 2.0 version. This specification defines the abstract definition of the certificate and specifically how it would appear as an X.509 certificate.

This specification builds upon the Platform Attribute Credential Profile version 1.0 [14] by incorporating the following changes:

- Fixed errors identified in the Platform Attribute Certificate specification version 1.0 errata document [14].
- Modified the ComponentIdentifier field of the Platform Configuration attribute to include a reference to the component's Platform Certificate. This change enables the issuer to construct a certificate tree of platform components and subcomponents.
- Added the field componentClass to the ComponentIdentifier element to unambiguously identify the type of component being referenced.
- Introduced the definition for the Delta Platform Certificate, modified the TCG Attributes definitions to identify applicability to the Delta Platform Certificate.
- Removed the Platform Certificate public key certificate format since it was considered redundant.
- Added support for multiple TPM EK Certificates by allowing the issuer to include multiple references using the TargetingInformation extension.
- Incorporated ComponentClass registry OID and value in the ComponentIdentifier field.

This specification replaces the existing Platform Credential Specification version 1.2 [6]. This certificate attests that a specific manufactured platform, identified by the platform serial number and TPM EK certificates, contains a unique TPM and Trusted Building Block (TBB). TBB is defined in the TCG Generic Server Specification [9].

1.2 Document Scope

This document specifies a complete definition of the Platform Certificate for use with any TPM Family version. This specification describes the abstract definition of the certificate 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 [2], 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], the Generic Server Platform Specification [9], and the TCG Algorithm Registry Specification [12]. This specification replaces the Platform Credential Specification defined in the TCG Credential Profiles for TPM Family 1.2 [6].

1.4 Keywords

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

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 – An artifact that cryptographically binds a subject’s identity to its public key or attributes using the industry-standard certificate structure from ISO/IEC/ITU-T X.509 version 3. Certificate generation consists of (a) assembling values for the certificate fields and (b) signing over the assembled fields.

NOTE: The term “Credential” has been replaced with “Certificate” throughout the document. Certificate is a more precise term to describe this artifact. Any uses of the word “Credential” in this document refer to titles of previously published specifications, attributes, or extensions.

2. Certificate Overview

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

2.1 Platform Certificate

A Platform Certificate 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.

Platform Certificates contain assertions about trust made by a platform manufacturer. The certificate asserts the platform's security properties and configuration as shipped. Delta Platform Certificates are used to reflect platform changes made by system integrators, resellers, and other entities after the platform has left the manufacturer's facility.

2.1.1 Who Uses a Platform Certificate?

A consumer of a Platform Certificate is a Privacy-CA. A Platform Certificate contains information that the Privacy-CA can use in attesting to the integrity characteristics of a platform. The Privacy-CA can copy field entries from the Platform Certificate to a new AK Certificate that the Privacy-CA creates for a trusted platform.

Another consumer of the Platform Certificate 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 Certificate 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. In order to support this use case, the optional Platform Serial Number attribute MUST be included in the certificate. In addition, an Enterprise could use the Platform Certificate to assert non-security related properties, such as platform components, included optionally by the platform manufacturer in the certificate.

For other users of the Platform Certificate, refer to section 6.2 Platform Endorsement Credential of Reference Architecture for Interoperability Specification [2].

2.1.2 Who Issues a Platform Certificate?

In general, the issuer of a Platform Certificate is the platform manufacturer (for example, an OEM). An entity should not generate a Platform Certificate unless the entity is satisfied that the platform contains the TPM referenced inside the certificate. Other types of entities in the platform manufacturing supply chain could issue a Platform Certificate. For more information, refer to section 3 The Trusted Platform Lifecycle of Reference Architecture for Interoperability Specification [2].

2.1.3 Revocation of a Platform Certificate

A Platform Certificate could be revoked by the platform manufacturer if there is evidence of CA compromise. Other reasons for revocation include replacement of a platform's TPM, replacement of the Endorsement Key, or reissuance of the EK certificate. Platform configuration changes made after the platform is shipped can be addressed by the issuance of a Delta Platform Certificate.

2.1.4 Validity Period of a Platform Certificate

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

2.1.5 Assertions Made by a Platform Certificate

The following table lists all the fields that are central to the use of this certificate and which MUST or MAY be in a Platform Certificate.

Field Name	**Description**	**Field Status**
Certificate Type Label	Distinguish certificate types issued under a shared key	MUST
EK Certificates	Identifies the associated EK Certificates	MUST
Platform Manufacturer String	Name of platform manufacturer as a string	MUST
Platform Model	Manufacturer-specific identifier	MUST
Platform Version	Manufacturer-specific identifier	MUST
Issuer	Identifies the issuer of the certificate	MUST
Platform Specification	Platform Specification to which this platform is built	MUST
Certificate Specification	Platform Certificate Specification Version, Level, and Revision	MUST
Validity Period	Time period when certificate 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
Platform Manufacturer Identifier	Platform manufacturer unique identifier as an IANA identifier	MAY
Platform Configuration Uri	URI where PCR information can be obtained	MAY
Policy Reference	Certificate policy reference	MAY
Revocation Locator	Identifies source of revocation status information	MAY

Table 1: Platform Certificate Fields

2.1.5.1 Certificate Type Label

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

For Platform Certificates, the value of this field MUST be the string, “TCG Trusted Platform Endorsement”.

2.1.5.2 EK Certificates

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

This SHALL be an unambiguous indication of the EK Certificates of the TPM incorporated into the platform. The Platform Certificate SHALL contain references to all TCG required Endorsement Key (EK) Certificates. The “TCG Infrastructure Working Group Reference Architecture for Interoperability (Part I)” [2] requires the TPM Manufacturer to issue an EK Certificate for each TPM Endorsement Key. The Platform Certificate MAY also contain references to optional EK Certificates, such as those issued by the Platform OEM or Platform Owner.

2.1.5.3 Platform Manufacturer String

This assertion identifies the platform manufacturer using a Platform Manufacturer assigned string.

2.1.5.4 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].

2.1.5.5 Platform Model

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

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

2.1.5.6 Platform Version

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

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

2.1.5.7 Issuer

This assertion identifies the entity that signed and issued the Platform Certificate.

2.1.5.8 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.

2.1.5.9 Certificate Specification

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

2.1.5.10 Validity Period

This assertion enables the certificate user to determine whether the Platform Certificate has begun to be valid or has expired.

2.1.5.11 Signature Value

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

2.1.5.12 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.

2.1.5.13 Platform Assertions

This field contains assertions about the general security properties of the platform. This could be used by the certificate user to verify that the platform implements acceptable security policies.

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

2.1.5.14 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.

2.1.5.15 Platform Configuration Uri

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

2.1.5.16 Policy Reference

This assertion enables the certificate user to identify the certificate issuance policy of the Platform Certificate issuer.

2.1.5.17 Revocation Locator

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

2.2 Delta Platform Certificate

A Delta Platform Certificate attests to specific changes made to the platform that are not reflected in the original Platform Certificate. A system integrator or value added retailer (VAR) can make modifications to a platform resulting in the Platform Certificate inaccurately reflecting its current configuration.

The entity making platform modifications could issue a Delta Platform Certificate to reflect those changes. A chain consisting of a Platform Certificate followed by multiple Delta Platform Certificates is supported in cases where multiple entities make valid modifications to a platform. A Delta Platform Certificate MUST only include additions, modifications and deletions of certain platform attributes. The issuer of the Delta Platform Certificate MUST verify that the changes made to the platform are adequately represented by the Delta Platform Certificate and that the Delta Platform Certificate references the appropriate base Platform or Delta Certificate.

Figure 1 illustrates how a chain of Platform and Delta Platform certificates can be constructed by linking the certificates using a base certificate reference.

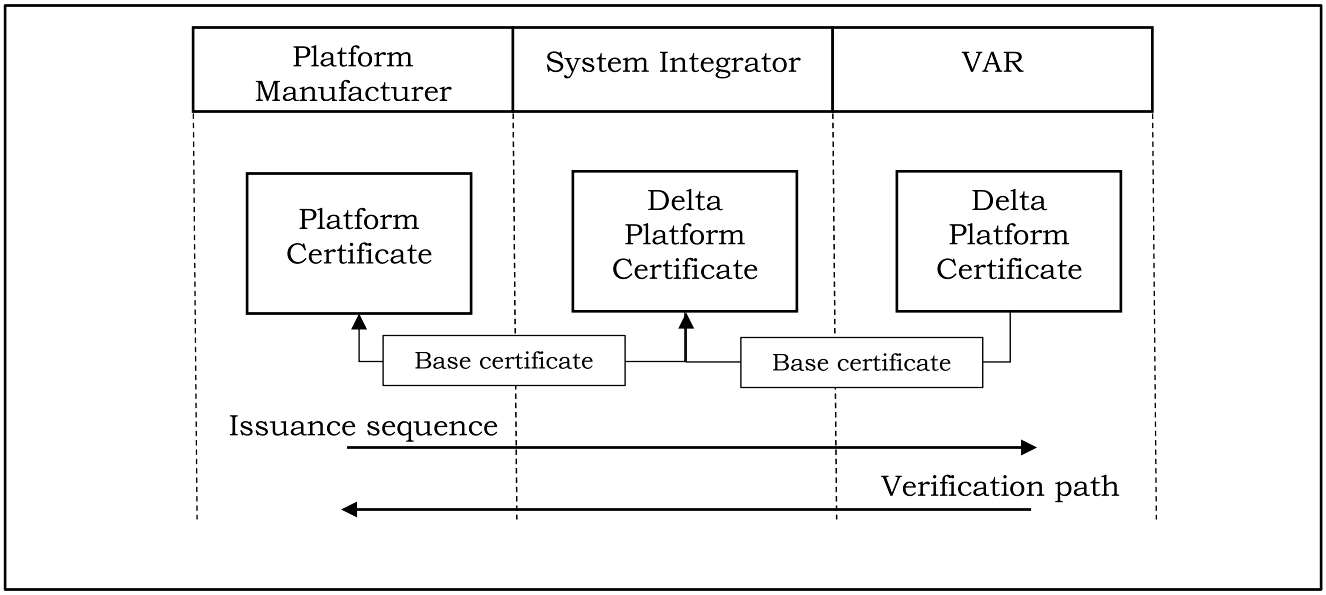

Figure 1: Delta Platform Certificate chain

2.2.1 Who Uses a Delta Platform Certificate?

A Delta Platform Certificate will be used by Privacy-CAs and Enterprises wanting to verify changes in platform attributes. This certificate allows a verifier to attest changes made to the platform as it progresses through the supply chain.

2.2.2 Who Issues a Delta Platform Certificate?

In addition to the entities that traditionally issue Platform Certificates, a system integrator or value added reseller could issue a Delta Platform Certificate to reflect platform attribute changes.

2.2.3 Conditions for Issuing a Delta Platform Certificate

Any authorized entity, typically a system integrator or value added retailer, modifying a platform's configuration can issue a Delta Platform Certificate. This certificate MAY be issued as long as the following conditions are maintained:

- Changes made to the platform do not invalidate the TBB security claims made by the original platform manufacturer.
- Changes made to the platform do not invalidate the TCG Platform Specification compliance claims made by the platform manufacturer.
- The platform TPM is not altered or replaced (including replacement of EK keys or EK certificates).

2.2.4 Requirements for Issuing a Delta Platform Certificate

An entity wanting to issue a Delta Platform Certificate MUST adhere to the following set of requirements:

- The Delta Platform Certificate issuer MUST NOT invalidate platform security assertions made by the base Platform Certificate.
- Platform changes made by the issuer MUST NOT introduce non-compliances to the TCG Platform Specification identified in the TCG Specification Attribute (Section 3.1.3).
- The issuing entity MUST NOT modify the TPM embedded in the platform, including invalidating the EK keys or EK certificates. For example, the issuer may not call ChangeEPS on the TPM. Doing so would break the binding between the base Platform Certificate and the TPM.
- The issuing entity MAY issue new EK keys and certificates, and include references to these certificates in the Delta Platform Certificate.

2.2.5 Revocation of a Delta Platform Certificate

If the platform is modified such that the chain of the Platform Certificate and the sequence of Delta Platform Certificates no longer reflects the configuration of the platform, a new Delta Platform Certificate can be issued. The current Delta Platform Certificate becomes the new base certificate.

A Delta Certificate could be revoked if there is evidence of CA compromise, or in cases where the base Platform Certificate or base Delta Platform Certificate are revoked.

2.2.6 Assertions Made by a Delta Platform Certificate

The following table lists all the fields that are central to the use of this certificate type and which MUST or MAY be in a Delta Platform Certificate.

Field Name	**Description**	**Field Status**
Certificate Type Label	Distinguishes certificate types issued under a shared key	MUST
Base Platform Certificate	Identifies the base Platform or Delta Platform certificate	MUST
Platform Manufacturer String	Name of platform manufacturer as a string	MUST
Platform Model	Manufacturer-specific identifier	MUST
Platform Version	Manufacturer-specific identifier	MUST
Issuer	Identifies the issuer of certificate	MUST
Certificate Specification	Platform Certificate Specification Version, Level, and Revision	MUST
Validity Period	Time period when the certificate is valid	MUST

Signature Value	Signature of the issuer over the other fields	MUST
Platform Serial Number	Platform's unique serial number	MAY
Platform Configuration	Non-security related platform properties	MAY
Platform Manufacturer Identifier	Platform manufacturer unique identifier as an IANA identifier	MAY
Platform Configuration Uri	URI where PCR information can be obtained	MAY
Policy Reference	Certificate policy reference	MAY
Revocation Locator	Identifies source of revocation status information	MAY
EK Certificates	Identifies newly issued EK Certificates	MAY

Table 2: Delta Platform Certificate Fields

2.2.6.1 Certificate Type Label

For Platform Certificates, the value of this field MUST be the string, "TCG Trusted Platform Endorsement".

2.2.6.2 EK Certificates

This assertion is used to reference additional EK certificates issued by the Delta Platform Certificate issuer.

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

2.2.6.3 Base Platform Certificate

This assertion is used by the verifier to bind the certificate to the previously issued Platform Certificate or Delta Platform Certificate. The base certificate is the previously issued Platform Certificate or Delta Platform Certificate amended by this certificate.

This SHALL be an unambiguous indication of the base Platform Certificate.

2.2.6.4 Platform Manufacturer String

This assertion identifies the platform manufacturer using a Platform Manufacturer assigned string. This field MUST equal that of the base Platform Certificate or base Delta Platform Certificate.

2.2.6.5 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]. This field MUST equal that of the base Platform Certificate or base Delta Platform Certificate.

2.2.6.6 Platform Model

This assertion identifies the specific platform model implementation. This is used by a Privacy-CA to verify that the platform contains a specific root of trust implementation. This field MUST equal that of the base Platform Certificate or base Delta Platform Certificate.

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

2.2.6.7 Platform Version

This assertion identifies the specific version of the platform. This is used by a Privacy-CA to verify that the platform contains a specific root of trust implementation. This field MUST equal that of the base Platform Certificate or base Delta Platform Certificate.

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

2.2.6.8 Issuer

This assertion identifies the entity that signed and issued the Delta Platform Certificate.

2.2.6.9 Certificate Specification

This assertion identifies the Platform Certificate Profile Specification version. This assertion includes the Platform Certificate Profile specification's Version, Level, and Revision. Included only if the delta certificate is issued under an updated version of this specification.

2.2.6.10 Validity Period

The validity period's "Not After" date MUST match that of the base certificate.

2.2.6.11 Signature Value

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

2.2.6.12 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 issuer SHALL use a customer visible serial number as the identifier. This field MUST equal that of the base Platform Certificate or base Delta Platform Certificate.

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

2.2.6.13 Platform Configuration

This field contains assertions of properties that are not security related. The Delta Platform Certificate MUST only include platform properties that have changed (added, modified, or deleted) with respect to the base certificate.

2.2.6.14 Platform Configuration Uri

This assertion provides an optional Uniform Resource Identifier where valid PCR and platform configuration information can be obtained. This field MAY be included only if the Platform Configuration Uri has changed.

2.2.6.15 Policy Reference

This assertion enables the certificate user to identify the certificate issuance policy of the Delta Platform Certificate issuer.

2.2.6.16 Revocation Locator

This assertion enables the certificate consumer to determine whether the Delta Platform Certificate 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 Certificate 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 TPM and Platform Assertions

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

Each attribute begins with a version number that identifies the version of the assertion syntax. Future versions of this profile could 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 an **URIReference** which describes the URI to the document and a cryptographic hash value which identifies a specific version of the document.

The **tBBSecurityAssertions** attribute MUST NOT be included in the Delta Platform Certificate.

URIMAX is a constant used to provide an upper bound on the length of a URI included in the certificate. This upper bound is 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 }

-- Hybrid means the measurement root is capable of static AND dynamic
-- Physical means that the root is anchored by a physical TPM
```

```
        -- Virtual means the TPM is virtualized (possibly running in a VMM).
        -- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
        -- the capabilities of the platform.
        MeasurementRootType ::= ENUMERATED {
            static (0),
            dynamic (1),
            nonHost (2),
            hybrid (3),
            physical (4),
            virtual (5) }


        -- common criteria evaluation

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

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

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

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

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

        -- fips evaluation

        FIPSLevel ::= SEQUENCE {
            version IA5STRING (SIZE (1..STRMAX)), -- “140-1”, “140-2”, or “140-3”
            level SecurityLevel,
            plus BOOLEAN DEFAULT FALSE }

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

3.1.2 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 **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.

These attributes MUST be included in the Delta Platform Certificate.

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

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].

3.1.3 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 platform class values are defined in section 4 Platform Class of the Registry of Reserved TPM 2.0 Handles and Localities [22]. This attribute MUST NOT be included in the Delta Platform Certificate.

```
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) }
```

3.1.4 TCG Certificate Type Attributes

The following defines the syntax of the certificate type attribute.

The **TCGCredentialType** attribute identifies the type of Platform Certificate. Values supported are Platform Certificate and Delta Platform Certificate in both attribute and public key formats. Values are encoded as TCG registered OIDs. This attribute MUST be included in the Delta Platform Certificate to differentiate from a Platform Certificate.

```
tCGCredentialType ATTRIBUTE ::= {
    WITH SYNTAX TCGCredentialType
    ID tcg-at-tcgCredentialType}

TCGCredentialType::= SEQUENCE {
    certificateType CredentialType}

CredentialType ::= OBJECT IDENTIFIER (tcg-kp-PlatformAttributeCertificate | tcg-kp-
    DeltaPlatformAttributeCertificate )
```

3.1.5 TCG Certificate Specification Attributes

The following defines the syntax of the certificate specification attributes.

The **TCGCredentialSpecification** attribute identifies the major version, minor version, and revision of the certificate specification with which a certificate is compliant. Values are encoded as three integers in this attribute. This attribute MAY be included in the Delta Platform Certificate if issued under a different specification version than the base certificate.

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

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

3.1.6 Platform Configuration Attributes

The following defines the syntax of the platform configuration attribute.

The **platformConfiguration** attribute contains optional lists of platform component identifiers, component identifier URI, platform properties, and platform property URI. The **componentIndentifer** field contains a list of individual components that constitute the platform. The issuer MUST include the component class, manufacturer and model, and optionally provide the component serial number, revision, and the component manufacturer's IANA **PrivateEnterpriseNumber**. In addition, each component identifier MAY contain information such as whether it is field replaceable, its network address, platform certificate, and platform certificate URI.

The **componentClass** sequence is used to identify the type of component. The **componentClass** field consists of a **componentClassRegistry** OID and the **componentClassValue**. The **componentClassRegistry** OID allows the issuer to convey which component class registry is used to identify the component. The **componentClassValue** is the specific registry value for the component.

The **componentPlatformCert** field contains information about the component's Platform Certificate. This field allows the issuer to create a hierarchy of platforms by constructing a general tree of Platform Certificates. The issuer MUST include attributeCertificateIdentifier or **genericCertIdentifier** to provide a reference to the component's Platform Certificate. The verifier can use the **componentPlatformCert** attribute to cryptographically verify the constituent components and subcomponents of a platform. In order to verify the certificate hierarchy, the verifier can use the **attributeCertIdentifier** or **genericCertIdentifier** fields to identify the component Platform Certificate. This operation would have to be repeated for any component of the platform, and subsequently down the hierarchical tree. The verifier can use this information to effectively confirm a platform's components remain unchanged from the as-built configuration.

The platform manufacturer can use the **componentPlatformCertificateUri** to identify the public distribution point of the component platform certificate.

The **status** field contained within the **componentIdentifier** field MUST be used only in Delta Platform Certificates.

The optional **platformProperties** field SHALL contain characteristics of the platform that the issuer considers 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.

The **status** field contained within the **Properties** field MUST be used only in Delta Platform Certificates.

The **platformConfiguration** attribute MAY be included in the Delta Platform Certificate to reflect changes made to the **componentIdentifiers**, **componentIdentifiersUri,** **platformProperties**, and **platformPropertiesUri** fields. In this case, the **status** enumerator MUST be included to indicate whether the field was added, modified, or removed from the base certificate.

```
platformConfiguration ATTRIBUTE ::= {
    WITH SYNTAX PlatformConfiguration
    ID tcg-at-platformConfiguration-v2
}

PlatformConfiguration ::= SEQUENCE {
   componentIdentifiers [0] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF ComponentIdentifier OPTIONAL,
   componentIdentifiersUri [1] IMPLICIT URIReference OPTIONAL,
    platformProperties [2] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF Property OPTIONAL,
    platformPropertiesUri [3] IMPLICIT URIReference OPTIONAL
}

ComponentIdentifier ::= SEQUENCE {
    componentClass ComponentClass,
    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,
    componentAddresses  [4]  IMPLICIT  SEQUENCE(SIZE(1..  MAX))  OF  ComponentAddress  OPTIONAL
    componentPlatformCert [5] IMPLICIT CertificateIdentifier OPTIONAL,
    componentPlatformCertUri [6] IMPLICIT URIReference OPTIONAL,
    status [7] IMPLICIT AttributeStatus OPTIONAL  }

ComponentClass ::= SEQUENCE {
    componentClassRegistry ComponentClassRegistry,
    componentClassValue OCTET STRING SIZE(4) }

ComponentClassRegistry ::= OBJECT IDENTIFIER ( tcg-registry-componentClass-tcg | tcg-registry-
componentClass-ietf | tcg-registry-componentClass-dmtf )

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

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

Property ::= SEQUENCE {
    propertyName UTF8String (SIZE (1..STRMAX)),
    propertyValue UTF8String (SIZE (1..STRMAX)),
    status [0] IMPLICIT AttributeStatus OPTIONAL  }

CertificateIdentifier::= SEQUENCE {
    attributeCertIdentifier   [0] IMPLICIT AttributeCertificateIdentifier  OPTIONAL,
    genericCertIdentifier     [1] IMPLICIT IssuerSerial     OPTIONAL }

AttributeCertificateIdentifier ::= SEQUENCE {
    hashAlgorithm             AlgorithmIdentifier,
    hashOverSignatureValue    OCTET STRING
}

IssuerSerial ::= SEQUENCE {
    issuer     GeneralNames,
    serial     CertificateSerialNumber
 }

AttributeStatus ::= ENUMERATED {
    added (0),
    modified (1),
    removed (2) }
```

Three **ComponentClassRegistry** OIDs have been defined by the TCG. The **tcg-registry-componentClass-tcg** is a placeholder that refers to a future TCG Component Class Registry. The **tcg-registry-componentClass-ietf** refers to the IETF RFC8348 [19] IANA Hardware Class. The **tcg-registry-componentClass-dmtf** is a placeholder to refer to a future SMBIOS based registry.

The **AttributeCertificateIdentifier** sequence is comprised of the hashAlgorithm field and the hashOverSignatureValue. The hashAlgorithm field is of type AlgorithmIdentifier as defined in RFC5280 [13]. This field identifies the hashing algorithm used in hashOverSignatureValue field. The hashOverSignatureValue is calculated over the Platform

Certificate's BIT STRING signatureValue (excluding the tag, length, and number of unused bits).

The definition of AlgorithmIdentifier from RFC5280 [13] is provided here for convenience:

```
AlgorithmIdentifier ::= SEQUENCE {
        algorithm OBJECT IDENTIFIER,
        parameters ANY DEFINED BY algorithm OPTIONAL }
```

Since the algorithms used are all hashing algorithms, the parameters field SHOULD not be used. The issuer MAY utilize any of the hash algorithm OIDs found in RFC3279 [15], RFC4055 [16], SHA-3 Related Algorithms and Identifiers for PKIX [17], and GB/T 33560-2017 [18].

MAX is to be interpreted, as described in RFC 5280[13], to mean the upper bound is unspecified.

NOTE: Parsers and verifiers should be version aware, and make the necessary adjustments to support current and prior versions of the **platformConfiguration** attribute. Future versions of this specification could introduce modifications to the **platformConfiguration** attribute. If such changes impact the structure and semantics of existing fields (componentIdentifiers, componentIdentifiersURI, platformProperties, and platformPropertiesURI) the attribute's OID will be updated to the next version (**tcg-at-platformConfiguration-*v3***).

3.1.7 Platform Configuration Uri Attribute

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

The **PlatformConfigUri** attribute contains the URI where the reference integrity measurements could be obtained by the verifier. The format used to convey the reference measurement values is vendor specific and not defined by the TCG. This field uses an **URIReference** sequence.

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

The **PlatformConfigUri** attribute MAY be included in the Delta Platform Certificate to assert changes to the URI where PCR values are published.

3.2 Platform Certificate

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

The Platform Certificate 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. Additional EK Certificates can be referenced using the TargetingInformation extension.	Standard
Issuer	Name	Distinguished name of the platform certificate issuer	Standard
Validity	notBefore notAfter	Beginning and end of validity period	Standard
Attributes			Standard
TBB Security Assertions	version ccInfo fipsLevel rtmType iso9000Certified iso9000Uri	Describes security-related assertions about the platform TBB	SHOULD
TCG Platform Specification	majorVersion minorVersion revision platformClass	Identifies platform class, version, and revision pf the platform-specific specification	SHOULD
TCG Certificate Type	credentialType	Identifies the Platform Certificate in attribute certificate format	SHOULD
TCG Certificate Specification	majorVersion minorVersion revision	Major, minor, and revision of the Platform Certificate spec under which the Platform Certificate was issued	SHOULD

Field Name	**RFC 5755 Type**	**Value**	**Field Status**
Platform Configuration	componentIdentifier platformProperties platformPropertiesUri	Platform components and properties MAY be reflected by this attribute	MAY
Platform Configuration URI	URIReference	Points to the PCR list	MAY
Extensions			
Certificate Policies	CertificatePolicies	CertPolicyId CPSuri UserNotice	MUST Non-critical
Subject Alternative Names	GeneralName directoryName	PlatformManufacturerStr PlatformModel PlatformVersion PlatformSerial (optional) PlatformManufacturerId (optional)	MUST non-critical
Targeting Information	TargetingInformation	Additional TPM EK Certificates not included in Holder. Use targetName option.	MAY 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 3: Attribute Certificate Format Fields

3.2.1 Version

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

3.2.2 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 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 one of the required X.509 TPM EK certificates. The BaseCertificateID choice MUST be used. Additional required TPM EK certificates MUST be referenced using the TargetingInformation extension. Optional EK certificates MAY be referenced using the TargetingInformation extension.

NOTE: This specification does not stipulate the order in which the EK certificate references must appear in the Platform Certificate. Certificates will appear in any order.

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 relevant TCG Platform Specific specification.

3.2.6 Validity

This field contains the period during which the binding between the attributes and TPM EK certificates 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 [11], section 4.2.6 Validity Period.

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 could 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 Targeting Information

This extension contains references to additional EK certificates not included in the Holder field. This extension is implemented using AC Targeting extension defined in RFC5755 [11]. This extension is OPTIONAL, but if included, assign “critical” the value of TRUE. Use the targetName option. The EK certificate serial number MUST be included by adding the RDN attribute serialNumber to the GeneralName. Attribute serialNumber is defined in ITU-T X.520 specification [19].

3.2.10 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 Certificate Type” attribute identifies the type of certificate and its format.
- The “TCG Certificate 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 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.

3.2.11 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.

3.2.12 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 CRL Distribution Point (CDP) and OCSP AIA extension are present in the certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

3.2.13 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.

3.2.14 Issuer Unique Id

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

3.3 Delta Platform Certificate

This section contains the format for a Delta Platform Certificate. The Delta Platform Certificate makes the assertions listed in section 2.2.6. 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 base Platform/Delta Platform Certificate, use BaseCertificateID.	Standard
Issuer	Name	Distinguished name of the delta platform certificate issuer	Standard
Validity	notBefore notAfter	Beginning and end of validity period	Standard
Attributes			Standard
TCG Certificate Type	credentialType	Identifies the Delta Platform Certificate	MUST
TCG Certificate Specification	majorVersion minorVersion revision	Major, minor, and revision of the Platform Certificate spec under which this certificate was issued	MAY (If different from base Platform Certificate)
Platform Configuration	componentIdentifier platformProperties platformPropertiesUri	Changes to platform components and properties MAY be reflected by this attribute	MAY (If different from base Platform Certificate)
Platform Configuration URI	URIReference	Points to the PCR list	MAY (If different from base Platform Certificate)
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 (Must not differ from base Platform Certificate)
Targeting Information	TargetingInformation	TPM EK Certificates issued and not included in base certificate. Use targetName option.	MAY 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

Table 4: Delta Attribute Certificate Format Fields

3.3.1 Version

This field contains the version of the certificate syntax. The Delta Platform Certificate version number MUST be set to 2 (which is encoded as the value 1 in ASN.1).

3.3.2 Serial Number

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

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

3.3.3 Signature Algorithm

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

3.3.4 Holder

This field contains a reference to the base Platform Certificate or base Delta Platform Certificate. The BaseCertificateID choice MUST be used.

3.3.5 Issuer

This field contains the distinguished name of the entity that issued this Delta Platform Certificate. This is the entity that asserts that the changes made to the platform are correctly reflected in this certificate, and that it references the appropriate base Platform or Delta Certificate.

3.3.6 Validity

This field contains the period during which the assertions made by the issuer about the platform are considered valid. 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. The notAfter date SHOULD not precede that of the base certificate. Both notBefore and notAfter MUST use the appropriate time format as indicated by RFC 5755 [11], section 4.2.6 Validity Period.

3.3.7 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 could 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.

3.3.8 Subject Alternative Names

This extension contains the platform name attributes. This extension MUST equal that of the base Platform or Delta Platform Certificate, the issuer MUST NOT introduce any changes. 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.

3.3.9 Targeting Information

This extension contains references to additional EK certificates issued by the Delta Platform Certificate issuer. Refer to section 3.2.9 for details on how to implement this extension.

3.3.10 Attributes

The following attributes SHOULD be included:

- The “TCG Certificate Type” attribute identifies the type of certificate and its format.
- The “TCG Certificate Specification” attribute references the version, level, and revision of this specification.

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, and network adapter MAC addresses.
- The “Platform Configuration Uri” attribute which provides the URI to the manufacturer published list of valid PCR values.

3.3.11 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.

3.3.12 Authority Info Access

This extension contains additional information about the issuer. Assign “critical” the value FALSE. This extension 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 CRL Distribution Point (CDP) and OCSP AIA extension are present in the certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

3.3.13 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.

3.3.14 Issuer Unique Id

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

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-registry OBJECT IDENTIFIER ::= {tcg 18}

-- 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-at-tcgCredentialType OBJECT IDENTIFIER ::= {tcg-attribute 25}

-- 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-at-platformConfiguration-v2 OBJECT IDENTIFIER ::= {tcg-at-platformConfiguration 2}


-- 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-PlatformAttributeCertificate OBJECT IDENTIFIER ::= {tcg-kp 2}
tcg-kp-AIKCertificate OBJECT IDENTIFIER ::= {tcg-kp 3}
tcg-kp-PlatformKeyCertificate OBJECT IDENTIFIER ::= {tcg-kp 4}
tcg-kp-DeltaPlatformAttributeCertificate OBJECT IDENTIFIER ::= {tcg-kp 5}


-- 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 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}

-- TCG Registry OIDs
tcg-registry-componentClass OBJECT IDENTIFIER ::= {tcg-registry 3}
tcg-registry-componentClass-tcg OBJECT IDENTIFIER ::= {tcg-registry-componentClass 1}
tcg-registry-componentClass-ietf OBJECT IDENTIFIER ::= {tcg-registry-componentClass 2}
tcg-registry-componentClass-dmtf OBJECT IDENTIFIER ::= {tcg-registry-componentClass 3}


-- tcg specification attributes for platform
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 Credential type attribute
tCGCredentialType ATTRIBUTE ::= {
    WITH SYNTAX TCGCredentialType
    ID tcg-at-tcgCredentialType}

TCGCredentialType::= SEQUENCE {
    certificateType CredentialType}

CredentialType   ::=   OBJECT   IDENTIFIER   (tcg-kp-PlatformAttributeCertificate   |   tcg-kp-
    DeltaPlatformAttributeCertificate )

-- manufacturer implementation model and version attributes
PlatformManufacturerStr ATTRIBUTE ::= {
    WITH SYNTAX UTF8String (SIZE (1..STRMAX))
    ID tcg-at-platformManufacturerStr }

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 }


-- platform tbb security assertions

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 }


-- Hybrid means the measurement root is capable of static AND dynamic
-- Physical means that the root is anchored by a physical TPM
-- Virtual means the TPM is virtualized (possibly running in a VMM)

-- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
-- the capabilities of the platform.
MeasurementRootType ::= ENUMERATED {
    static (0),
    dynamic (1),
    nonHost (2),
    hybrid (3),
    physical (4),
    virtual (5) }


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

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

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

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

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

-- fips evaluation
FIPSLevel ::= SEQUENCE {
    version IA5STRING (SIZE (1..STRMAX)), -- “140-1”, “140-2”, or “140-3”
    level SecurityLevel,
    plus BOOLEAN DEFAULT FALSE }

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


-- platform configuration
platformConfiguration ATTRIBUTE ::= {
    WITH SYNTAX PlatformConfiguration
    ID tcg-at-platformConfiguration-v2
}

PlatformConfiguration ::= SEQUENCE {
    componentIdentifiers [0] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF ComponentIdentifier OPTIONAL,
    componentIdentifiersUri [1] IMPLICIT URIReference OPTIONAL,
    platformProperties [2] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF Properties OPTIONAL,
    platformPropertiesUri [3] IMPLICIT URIReference OPTIONAL
}

ComponentIdentifier ::= SEQUENCE {
    componentClass ComponentClass,
    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,
    componentAddresses  [4]  IMPLICIT  SEQUENCE(SIZE(1..  MAX))  OF  ComponentAddress  OPTIONAL
    componentPlatformCert [5] IMPLICIT CertificateIdentifier OPTIONAL,
    componentPlatformCertUri [6] IMPLICIT URIReference OPTIONAL,
    status [7] IMPLICIT AttributeStatus OPTIONAL  }

ComponentClass ::= SEQUENCE {
    componentClassRegistry ComponentClassRegistry,
    componentClassValue OCTET STRING SIZE(4) }

ComponentClassRegistry ::= OBJECT IDENTIFIER ( tcg-registry-componentClass-tcg | tcg-registry-
componentClass-ietf | tcg-registry-componentClass-dmtf )

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)),
    status [0] IMPLICIT AttributeStatus OPTIONAL  }

CertificateIdentifier::= SEQUENCE {
    attributeCertIdentifier   [0] IMPLICIT AttributeCertificateIdentifier  OPTIONAL,
    genericCertIdentifier     [1] IMPLICIT IssuerSerial     OPTIONAL }

AttributeCertificateIdentifier ::= SEQUENCE {
    hashAlgorithm             AlgorithmIdentifier,
    hashOverSignatureValue    OCTET STRING
}

AttributeStatus ::= ENUMERATED {
    added (0),
    modified (1),
    removed (2) }

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

5. References

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

[2] TCG Infrastructure Working Group Reference Architecture for Interoperability (Part 1), Specification Version 1.0, https://trustedcomputinggroup.org/resource/infrastructure-work-group-reference-architecture-for-interoperability-specification-part-1-version-1-0/

[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

[14] TCG Platform Attribute Credential Profile Version 1.0, https://trustedcomputinggroup.org/tcg-platform-attribute-credential-profile/

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

[16] Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://www.ietf.org/rfc/rfc4055.txt

[17] SHA-3 Related Algorithms and Identifiers for PKIX, https://tools.ietf.org/html/draft-turner-lamps-adding-sha3-to-pkix-00

[18] GB/T 33560-2017. Information security technology—Cryptographic application identifier criterion specification. http://www.spc.org.cn/gb168/online/GB%252FT%252033560-2017/

[19] A YANG Data Model for Hardware Management. https://tools.ietf.org/html/rfc8348

[20] ITU-T X.520 Information Technology – Open Systems Interconnection – The Directory: Selected Attributed Types. https://www.itu.int/rec/T-REC-X.520-201610-I

[21] TCG PC Client Platform TPM Profile (PTP) Specification. https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_Platform_TPM_Profile_PTP_2.0_r1.03_v22.pdf

[22] TCG Registry of Reserved TPM 2.0 Handles and Localities. https://trustedcomputinggroup.org/resource/registry/

A. Certificate Examples

A.1 Example 1 (Platform Certificate in Attribute Certificate Format)

The following section provides an example of a Platform Certificate in Attribute Certificate format (RFC 5755) [11]. The PEM encoded version of the certificate as well as the ASN.1 certificate text are included for convenience. The values used in this example are for illustrative purposes and must be replaced with manufacturer-specific data.

A.1.1 PEM Format

```
-----BEGIN ATTRIBUTE CERTIFICATE-----
MIIJmDCCCIACAQEwgZaggZMwgYqkgYcwgYQxCzAJBgNVBAYTAlVTMQswCQYDVQQI
DAJDQTEUMBIGA1UEBwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVsIENvcnBv
cmF0aW9uMR4wHAYDVQQLDBVFSyBDZXJ0aWZpY2F0ZSBJc3N1ZXIxFjAUBgNVBAMM
DXd3dy5pbnRlbC5jb20CBDdAg3SggZ0wgZqkgZcwgZQxCzAJBgNVBAYTAlVTMQsw
CQYDVQQIDAJDQTEUMBIGA1UEBwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVs
IENvcnBvcmF0aW9uMS4wLAYDVQQLDCVQbGF0Zm9ybSBBdHRyaWJ1dGUgQ2VydGlm
aWNhdGUgSXNzdWVyMRYwFAYDVQQDDA13d3cuaW50ZWwuY29tMA0GCSqGSIb3DQEB
CwUAAhRgKWfqeST97mzBULkeg3d9H0J5mTAiGA8yMDE3MDgyMDIxMDc0OFoYDzIw
MjAwODIwMjEwNzQ4WjCCBK4wHAYFZ4EFAhExEzARMAkCAQICAQACASsEBAAAAAEw
EgYFZ4EFAhkxCTAHBgVngQUIAjAUBgVngQUCFzELMAkCAQECAQECAQswgccGBWeB
BQITMYG9MIG6AgEAoHQWAzMuMQoBBwoBAgEBAIABAYEFKgMEBQaiLRYraHR0cHM6
Ly93d3cuaW50ZWwuY29tL3Byb3RlY3Rpb25wcm9maWxlLnBkZoMFUwQFBgekJBYi
aHR0cHM6Ly93d3cuaW50ZWwuY29tL2NjdGFyZ2V0LnBkZqENFgUxNDAtMgoBBAEB
AIIBAwEBABYqaHR0cHM6Ly93d3cuaW50ZWwuY29tL2lzb2NlcnRpZmljYXRpb24u
cGRmMIIDagYHZ4EFBQEHAjGCA10wggNZoIIC1zCCAXYwDgYGZ4EFEgMBBAQAAAAK
DAdBQkMgT0VNDAxXUjA2WDc4NzFGVEyACUE1NTU1LTk5OYEDMS4xggcrBgEEEAYIs
gwH/pDIwFwYFZ4EFEQEMDkFGOjNBOjk0OjEwOkE1MBcGBWeBBRECDA5BRjozNzox
MDpEMjpBOKWBz6AxMA0GCysGAQQBgbAaAQIBBCBgA6M0Mv2RS2ADozQy/ZFLYAOj
NDL9kUtgA6M0Mv2RS6GBmTCBj6SBjDCBiTELMAkGA1UEBhMCVVMxCzAJBgNVBAgM
AkZMMRcwFQYDVQQHDA5GdC4gTGF1ZGVyZGFsZTEYMBYGA1UECgwPQUJDIENvcnBv
cmF0aW9uMSQwIgYDVQQLDBtQbGF0Zm9ybSBDZXJ0aWZpY2F0ZSBJc3N1ZXIxFDAS
BgNVBAMMC3d3dy5hYmMuY29tAgUKNUzN26YrFilodHRwczovL3d3dy5hYmMuY29t
L2NlcnRzLzQzODQzODk4ODQzLmNlcjCCAVkwDgYGZ4EFEgMBBAQAAAAvDAdYWVog
T0VNDA5MTUJUMzkwNERXMVQxR4AJQzU1NTUtNTU1gQMzLjGCBysGAQQBgiyDAQCk
MjAXBgVngQURAQwOODI6ODk6RkE6RDM6NjEwFwYFZ4EFEQIMDkQ0OjgzOkI0OkYy
Ojc4pYG1oCUwDQYLKwYBBAGBsBoBAgEEFDQy4UFLYJc0NDI0MuFBS2CXNDQyoYGL
MIGDpIGAMH4xCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJBWjEQMA4GA1UEBwwHUGhv
ZW5peDEUMBIGA1UECgwLWFlDIENvbXBhbnkxJDAiBgNVBAsMG1BsYXRmb3JtIENl
cnRpZmljYXRlIElzc3VlcjEUMBIGA1UEAwwLd3d3Lnh5ei5jb20CAw5TsKYmFiRo
dHRwczovL3d3dy54eXouY29tL2NlcnRzLzkzODkyOC5jZXKhLxYtaHR0cHM6Ly93
```

```
d3cuaW50ZWwuY29tL3BsYXRmb3JtaWRlbnRpZmllcnMueG1sohswDAwEdlBybwwE
dHJ1ZTALDANBTVQMBHRydWWjLhYsaHR0cHM6Ly93d3cuaW50ZWwuY29tL3BsYXRm
b3JtcHJvcGVydGllcy54bWwwLAYGZ4EFBQEDMSIwIBYeaHR0cHM6Ly93d3cuaW50
ZWwuY29tL1BDUnMueG1sMIICRTB8BgNVHSAEdTBzMHEGCiqGSIb4TQEFAgQwYzAx
BggrBgEFBQcCARYlaHR0cHM6Ly93d3cuaW50ZWwuY29tL3BsYXRjZXJ0Y3BzLnBk
ZjAuBggrBgEFBQcCAjAiDCBUQ0cgVHJ1c3RlZCBQbGF0Zm9ybSBFbmRvcnNlbWVu
dDB+BgNVHREEdzB1pHMwcTERMA8GBmeBBQUBAQwFSW50ZWwxFTATBgZngQUFAQIw
CQYHKwYBBAGCVzETMBEGBmeBBQUBBAwHUzI2MDBLUDEWMBQGBmeBBQUBBQwKSDc2
OTYyLTM1MDEYMBYGBmeBBQUBBgwMQlFLUDk5OTQwNjQzMIGyBgNVHTcBAf8Egacw
gaQwgaGggZ6kgZswgZgxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTEUMBIGA1UE
BwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVsIENvcnBvcmF0aW9uMR4wHAYD
VQQLDBVFSyBDZXJ0aWZpY2F0ZSBJc3N1ZXIxFjAUBgNVBAMMDXd3dy5pbnRlbC5j
b20xEjAQBgNVBAUTCTEyODk0Mzc4NzAfBgNVHSMEGDAWgBTUaZAmAoHVXoNLA5du
q4qfj4TJgzA2BggrBgEFBQcBAQQqMCgwJgYIKwYBBQUHMAGGGmh0dHBzOi8vd3d3
LmludGVsLmNvbS9vY3NwMDcGA1UdHwQwMC4wLKAqoCiGJmh0dHBzOi8vd3d3Lmlu
dGVsLmNvbS9wbGF0Zm9ybWNlcnQuY3JsMA0GCSqGSIb3DQEBCwUAA4IBAQCq6w/S
/cuB8mUjIlVli2JPfkbS+v2TmBf0sIUPdPfU/aH16NPctavfiEvpPl1uWGty7/oY
8sAq5ChEU3/KbI0zaY7X0Yjpcp5YfYqZZFqgrDmye+o5T5+sAnJOjNrHdIEUGyYH
G47IsogmJj7i1lRcF7JVCJTUOGQpWqVMKF3/VffWJ84XKE+nbTYCYufyYHRxUQ1T
rSx5sQn0dAnW8Bdljc+zpaNJBDxdlCdhKefZSwf3Yc550d3QDqMekH/3++9MJhJO
79BiL0CkXi5gAYLi5NUl4X9S/Jv+hcaDWi/gEtB5s7c3rtEyoYByj//QycQhxMIb
L2ciOd1FDte7CSyC
-----END ATTRIBUTE CERTIFICATE-----
```

A.1.2 DER Format

```
SEQUENCE :
   SEQUENCE :
      INTEGER : 1
      SEQUENCE :
         CONTEXT SPECIFIC (0) :
            SEQUENCE :
               CONTEXT SPECIFIC (4) :
                  SEQUENCE :
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : countryName [2.5.4.6]
                           PRINTABLE STRING : 'US'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
                           UTF8 STRING : 'CA'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : localityName [2.5.4.7]
                           UTF8 STRING : 'Santa Clara'
                     SET :
```

```
                  SEQUENCE :
                     OBJECT IDENTIFIER : organizationName [2.5.4.10]
                     UTF8 STRING : 'Intel Corporation'
               SET :
                  SEQUENCE :
                     OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                     UTF8 STRING : 'EK Certificate Issuer'
               SET :
                  SEQUENCE :
                     OBJECT IDENTIFIER : commonName [2.5.4.3]
                     UTF8 STRING : 'www.intel.com'
      INTEGER : 926974836
CONTEXT SPECIFIC (0) :
   SEQUENCE :
      CONTEXT SPECIFIC (4) :
         SEQUENCE :
            SET :
               SEQUENCE :
                  OBJECT IDENTIFIER : countryName [2.5.4.6]
                  PRINTABLE STRING : 'US'
            SET :
               SEQUENCE :
                  OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
                  UTF8 STRING : 'CA'
            SET :
               SEQUENCE :
                  OBJECT IDENTIFIER : localityName [2.5.4.7]
                  UTF8 STRING : 'Santa Clara'
            SET :
               SEQUENCE :
                  OBJECT IDENTIFIER : organizationName [2.5.4.10]
                  UTF8 STRING : 'Intel Corporation'
            SET :
               SEQUENCE :
                  OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                  UTF8 STRING : 'Platform Attribute Certificate Issuer'
            SET :
               SEQUENCE :
                  OBJECT IDENTIFIER : commonName [2.5.4.3]
                  UTF8 STRING : 'www.intel.com'
SEQUENCE :
   OBJECT IDENTIFIER :  [1.2.840.113549.1.1.11]
   NULL :
INTEGER : 602967EA7924FDEE6CC150B91E83777D1F427999
SEQUENCE :
   GENERALIZED TIME : '20170820210748Z'
   GENERALIZED TIME : '20200820210748Z'
SEQUENCE :
   SEQUENCE :
      OBJECT IDENTIFIER :  [2.23.133.2.17]
      SET :
         SEQUENCE :
            SEQUENCE :
               INTEGER : 2
               INTEGER : 0
               INTEGER : 43
            OCTET STRING : 00000001
   SEQUENCE :
      OBJECT IDENTIFIER :  [2.23.133.2.25]
      SET :
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.8.2]
   SEQUENCE :
```

```
            OBJECT IDENTIFIER :  [2.23.133.2.23]
            SET :
               SEQUENCE :
                  INTEGER : 1
                  INTEGER : 1
                  INTEGER : 11
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.2.19]
            SET :
               SEQUENCE :
                  INTEGER : 0
                  CONTEXT SPECIFIC (0) :
                     IA5 STRING : '3.1'
                     ENUMERATED : '07'
                     ENUMERATED : '02'
                     BOOLEAN : '00'
                     CONTEXT SPECIFIC (0) : 01
                     CONTEXT SPECIFIC (1) : 2A03040506
                     CONTEXT SPECIFIC (2) :
                        IA5 STRING : 'https://www.intel.com/protectionprofile.pdf'
                     CONTEXT SPECIFIC (3) : 5304050607
                     CONTEXT SPECIFIC (4) :
                        IA5 STRING : 'https://www.intel.com/cctarget.pdf'
                  CONTEXT SPECIFIC (1) :
                     IA5 STRING : '140-2'
                     ENUMERATED : '04'
                     BOOLEAN : '00'
                  CONTEXT SPECIFIC (2) : 03
                  BOOLEAN : '00'
                  IA5 STRING : 'https://www.intel.com/isocertification.pdf'
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.5.1.7.2]
            SET :
               SEQUENCE :
                  CONTEXT SPECIFIC (0) :
                     SEQUENCE :
                        SEQUENCE :
                           OBJECT IDENTIFIER :  [2.23.133.18.3.1]
                           OCTET STRING : 0000000A
                        UTF8 STRING : 'ABC OEM'
                        UTF8 STRING : 'WR06X7871FTL'
                        CONTEXT SPECIFIC (0) : 41353535352D393939
                        CONTEXT SPECIFIC (1) : 312E31
                        CONTEXT SPECIFIC (2) : 2B06010401822C
                        CONTEXT SPECIFIC (3) : FF
                        CONTEXT SPECIFIC (4) :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.1]
                              UTF8 STRING : 'AF:3A:94:10:A5'
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.2]
                              UTF8 STRING : 'AF:37:10:D2:A8'
                        CONTEXT SPECIFIC (5) :
                           CONTEXT SPECIFIC (0) :
                              SEQUENCE :
                                 OBJECT IDENTIFIER :  [1.3.6.1.4.1.22554.1.2.1]
                              OCTET STRING :
6003A33432FD914B6003A33432FD914B6003A33432FD914B6003A33432FD914B
                           CONTEXT SPECIFIC (1) :
                              SEQUENCE :
                                 CONTEXT SPECIFIC (4) :
                                    SEQUENCE :
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : countryName [2.5.4.6]
                                             PRINTABLE STRING : 'US'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : stateOrProvinceName
[2.5.4.8]
                                             UTF8 STRING : 'FL'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : localityName [2.5.4.7]
                                             UTF8 STRING : 'Ft. Lauderdale'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : organizationName
[2.5.4.10]
                                             UTF8 STRING : 'ABC Corporation'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : organizationalUnitName
[2.5.4.11]
                                             UTF8 STRING : 'Platform Certificate Issuer'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : commonName [2.5.4.3]
                                             UTF8 STRING : 'www.abc.com'
                              INTEGER : 43843898843
                        CONTEXT SPECIFIC (6) :
                           IA5 STRING : 'https://www.abc.com/certs/43843898843.cer'
                     SEQUENCE :
                        SEQUENCE :
                           OBJECT IDENTIFIER :  [2.23.133.18.3.1]
                           OCTET STRING : 0000002F
                        UTF8 STRING : 'XYZ OEM'
                        UTF8 STRING : 'LMBT3904DW1T1G'
                        CONTEXT SPECIFIC (0) : 43353535352D353535
                        CONTEXT SPECIFIC (1) : 332E31
                        CONTEXT SPECIFIC (2) : 2B06010401822C
                        CONTEXT SPECIFIC (3) : 00
                        CONTEXT SPECIFIC (4) :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.1]
                              UTF8 STRING : '82:89:FA:D3:61'
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.2]
                              UTF8 STRING : 'D4:83:B4:F2:78'
                        CONTEXT SPECIFIC (5) :
                           CONTEXT SPECIFIC (0) :
                              SEQUENCE :
                                 OBJECT IDENTIFIER :  [1.3.6.1.4.1.22554.1.2.1]
                              OCTET STRING : 3432E1414B60973434323432E1414B6097343432
                           CONTEXT SPECIFIC (1) :
                              SEQUENCE :
                                 CONTEXT SPECIFIC (4) :
                                    SEQUENCE :
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : countryName [2.5.4.6]
                                             PRINTABLE STRING : 'US'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : stateOrProvinceName
[2.5.4.8]
```

```
                                             UTF8 STRING : 'AZ'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : localityName [2.5.4.7]
                                             UTF8 STRING : 'Phoenix'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : organizationName 
[2.5.4.10]
                                             UTF8 STRING : 'XYC Company'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : organizationalUnitName 
[2.5.4.11]
                                             UTF8 STRING : 'Platform Certificate Issuer'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : commonName [2.5.4.3]
                                             UTF8 STRING : 'www.xyz.com'
                              INTEGER : 938928
                        CONTEXT SPECIFIC (6) :
                           IA5 STRING : 'https://www.xyz.com/certs/938928.cer'
                  CONTEXT SPECIFIC (1) :
                     IA5 STRING : 'https://www.intel.com/platformidentifiers.xml'
                  CONTEXT SPECIFIC (2) :
                     SEQUENCE :
                        UTF8 STRING : 'vPro'
                        UTF8 STRING : 'true'
                     SEQUENCE :
                        UTF8 STRING : 'AMT'
                        UTF8 STRING : 'true'
                  CONTEXT SPECIFIC (3) :
                     IA5 STRING : 'https://www.intel.com/platformproperties.xml'
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.5.1.3]
            SET :
               SEQUENCE :
                  IA5 STRING : 'https://www.intel.com/PCRs.xml'
      SEQUENCE :
         SEQUENCE :
            OBJECT IDENTIFIER : certificatePolicies [2.5.29.32]
            OCTET STRING :
               SEQUENCE :
                  SEQUENCE :
                     OBJECT IDENTIFIER :  [1.2.840.113741.1.5.2.4]
                     SEQUENCE :
                        SEQUENCE :
                           OBJECT IDENTIFIER : cps [1.3.6.1.5.5.7.2.1]
                           IA5 STRING : 'https://www.intel.com/platcertcps.pdf'
                        SEQUENCE :
                           OBJECT IDENTIFIER : unotice [1.3.6.1.5.5.7.2.2]
                           SEQUENCE :
                              UTF8 STRING : 'TCG Trusted Platform Endorsement'
         SEQUENCE :
            OBJECT IDENTIFIER : subjectAltName [2.5.29.17]
            OCTET STRING :
               SEQUENCE :
                  CONTEXT SPECIFIC (4) :
                     SEQUENCE :
                        SET :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.5.1.1]
                              UTF8 STRING : 'Intel'
                        SET :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.5.1.2]
                              SEQUENCE : OBJECT IDENTIFIER :  [1.3.6.1.4.1.343]
                        SET :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.5.1.4]
                              UTF8 STRING : 'S2600KP'
                        SET :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.5.1.5]
                              UTF8 STRING : 'H76962-350'
                        SET :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.5.1.6]
                              UTF8 STRING : 'BQKP99940643'
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.5.29.55]
            BOOLEAN : 'FF'
            OCTET STRING :
               SEQUENCE :
                  SEQUENCE :
                     CONTEXT SPECIFIC (0) :
                        CONTEXT SPECIFIC (4) :
                           SEQUENCE :
                              SET :
                                 SEQUENCE :
                                    OBJECT IDENTIFIER : countryName [2.5.4.6]
                                    PRINTABLE STRING : 'US'
                              SET :
                                 SEQUENCE :
                                    OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
                                    UTF8 STRING : 'CA'
                              SET :
                                 SEQUENCE :
                                    OBJECT IDENTIFIER : localityName [2.5.4.7]
                                    UTF8 STRING : 'Santa Clara'
                              SET :
                                 SEQUENCE :
                                    OBJECT IDENTIFIER : organizationName [2.5.4.10]
                                    UTF8 STRING : 'Intel Corporation'
                              SET :
                                 SEQUENCE :
                                    OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                                    UTF8 STRING : 'EK Certificate Issuer'
                              SET :
                                 SEQUENCE :
                                    OBJECT IDENTIFIER : commonName [2.5.4.3]
                                    UTF8 STRING : 'www.intel.com'
                              SET :
                                 SEQUENCE :
                                    OBJECT IDENTIFIER : serialNumber [2.5.4.5]
                                    PRINTABLE STRING : '128943787'
         SEQUENCE :
            OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
            OCTET STRING :
               SEQUENCE :
                  CONTEXT SPECIFIC (0) : D46990260281D55E834B03976EAB8A9F8F84C983
         SEQUENCE :
            OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
            OCTET STRING :
               SEQUENCE :
                  SEQUENCE :
```

```
                  OBJECT IDENTIFIER : ocsp [1.3.6.1.5.5.7.48.1]
                  CONTEXT SPECIFIC (6) : 'https://www.intel.com/ocsp'
      SEQUENCE :
         OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
         OCTET STRING :
            SEQUENCE :
               SEQUENCE :
                  CONTEXT SPECIFIC (0) :
                     CONTEXT SPECIFIC (0) :
                        CONTEXT SPECIFIC (6) : 'https://www.intel.com/platformcert.crl'
SEQUENCE :
   OBJECT IDENTIFIER :  [1.2.840.113549.1.1.11]
   NULL :
BIT STRING UnusedBits:0 :
   AAEB0FD2FDCB81F265232255658B624F7E46D2FAFD939817F4B085
   0F74F7D4FDA1F5E8D3DCB5ABDF884BE93E5D6E586B72EFFA18F2C0
   2AE42844537FCA6C8D33698ED7D188E9729E587D8A99645AA0AC39
   B27BEA394F9FAC02724E8CDAC77481141B26071B8EC8B28826263E
   E2D6545C17B2550894D43864295AA54C285DFF55F7D627CE17284F
   A76D360262E7F2607471510D53AD2C79B109F47409D6F017658DCF
   B3A5A349043C5D94276129E7D94B07F761CE79D1DDD00EA31E907F
   F7FBEF4C26124EEFD0622F40A45E2E600182E2E4D525E17F52FC9B
   FE85C6835A2FE012D079B3B737AED132A180728FFFD0C9C421C4C2
   1B2F672239DD450ED7BB092C82
```

A.2 Example 2 (Delta Platform Certificate in Attribute Certificate Format)

The following section provides an example of a Delta Platform Certificate in Attribute Certificate format (RFC 5755) [11]. The PEM encoded version of the certificate as well as the ASN.1 certificate text are included for convenience. The values used in this example are for illustrative purposes and must be replaced with manufacturer-specific data.

A.2.1 PEM Format

```
-----BEGIN ATTRIBUTE CERTIFICATE-----
MIIKkzCCCXsCAQEwgbaggbMwgZqkgZcwgZQxCzAJBgNVBAYTAlVTMQswCQYDVQQI
DAJDQTEUMBIGA1UEBwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVsIENvcnBv
cmF0aW9uMS4wLAYDVQQLDCVQbGF0Zm9ybSBBdHRyaWJ1dGUgQ2VydGlmaWNhdGUg
SXNzdWVyMRYwFAYDVQQDDA13d3cuaW50ZWwuY29tAhRgKWfqeST97mzBULkeg3d9
H0J5maCBpDCBoaSBnjCBmzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMQ8wDQYD
VQQHDAZBdXN0aW4xFzAVBgNVBAoMDlhZWiBJbnRlZ3JhdG9yMTQwMgYDVQQLDCtE
ZWx0YSBQbGF0Zm9ybSBBdHRyaWJ1dGUgQ2VydGlmaWNhdGUgSXNzdWVyMR8wHQYD
VQQDDBZ3d3cueHl6aW50ZWdyYXRvcnMuY29tMA0GCSqGSIb3DQEBCwUAAgQCFPcE
MCIYDzIwMTgxMDE1MjEwODExWhgPMjAyMDA4MjAyMTA4MTFaMIIFeDASBgVngQUC
GTEJMAcGBWeBBQgFMBQGBWeBBQIXMQswCQIBAQIBAQIBDTCCBRAGB2eBBQUBBwIx
ggUDMIIE/6CCBF0wggF5MA4GBmeBBRIDAQQEAAAACgwHQUJDIE9FTQwMV1IwNlg3
ODcxRlRMgAlBNTU1NS05OTmBAzEuMYIHKwYBBAGCLIMB/6QyMBcGBWeBBREBDA5B
RjozQTo5NDoxMDpBNTAXBgVngQURAgwOQUY6Mzc6MTA6RDI6QTilgc+gMTANBgsr
BgEEAYGwGgECAQQgYAOjNDL9kUtgA6M0Mv2RS2ADozQy/ZFLYAOjNDL9kUuhgZkw
```

```
gY+kgYwwgYkxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJGTDEXMBUGA1UEBwwORnQu
IExhdWRlcmRhbGUxGDAWBgNVBAoMD0FCQyBDb3Jwb3JhdGlvbjEkMCIGA1UECwwb
UGxhdGZvcm0gQ2VydGlmaWNhdGUgSXNzdWVyMRQwEgYDVQQDDAt3d3cuYWJjLmNv
bQIFCjVMzdumKxYpaHR0cHM6Ly93d3cuYWJjLmNvbS9jZXJ0cy80Mzg0Mzg5ODg0
My5jZXKHAQIwggF8MA4GBmeBBRIDAQQEAAAAQQwOQ29tcG9uZW50IENvcnAMCVhU
OTgyODdMTIAHRjk4MS0wMYEDMi4xggcrBgEEAYNIgwH/pDIwFwYFZ4EFEQIMDjcz
OjlCOjkyOjQwOkZBMBcGBWeBBREDDA4xMzozRjo5ODpDNTo1OaWBzaAxMA0GCysG
AQQBgbAaAQIBBCCYqtWRg/qrkZiq1ZGD+quRmKrVkYP6q5GYqtWRg/qrkaGBlzCB
jqSBizCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMREwDwYDVQQHDAhTYW4g
Sm9zZTEXMBUGA1UECgwOQ29tcG9uZW50IENvcnAxJDAiBgNVBAsMG1BsYXRmb3Jt
IENlcnRpZmljYXRlIElzc3VlcjEaMBgGA1UEAwwRd3d3LmNvbXBvbmVudC5jb20C
BAXek66mLhYsaHR0cHM6Ly93d3cuY29tcG9uZW50LmNvbS9jZXJ0cy85ODQ3Mjg3
OC5jZXKHAQAwggFcMA4GBmeBBRIDAQQEAAAALwwHWFlaIE9FTQwOTE1CVDM5MDRE
VzFUMUeACUM1NTU1LTU1NYEDNC4wggcrBgEEAYIsgwEApDIwFwYFZ4EFEQEMDjgy
Ojg5OkZBOkQzOjYxMBcGBWeBBRECDA5ENDo4MzpCNDpGMjo3OKWBtaAlMA0GCysG
AQQBgbAaAQIBBBQ0MuFBS2CXNDQyNDLhQUtglzQ0MqGBizCBg6SBgDB+MQswCQYD
VQQGEwJVUzELMAkGA1UECAwCQVoxEDAOBgNVBAcMB1Bob2VuaXgxFDASBgNVBAoM
C1hZQyBDb21wYW55MSQwIgYDVQQLDBtQbGF0Zm9ybSBDZXJ0aWZpY2F0ZSBJc3N1
ZXIxFDASBgNVBAMMC3d3dy54eXouY29tAgMOU7CmJhYkaHR0cHM6Ly93d3cueHl6
LmNvbS9jZXJ0cy85Mzg5MjguY2VyhwEBoTgWNmh0dHBzOi8vd3d3Lnh5emludGVn
cmF0b3JzLmNvbS9wbGF0Zm9ybWlkZW50aWZpZXJzLnhtbKIpMBYMC1RTQyBFbmFi
bGVkDAR0cnVlgAEAMA8MA0FNVAwFZmFsc2WAAQGjNxY1aHR0cHM6Ly93d3cueHl6
aW50ZWdyYXRvcnMuY29tL3BsYXRmb3JtcHJvcGVydGllcy54bWwwOAYGZ4EFBQED
MS4wLBYqaHR0cHM6Ly93d3cueHl6aW50ZWdyYXRvcnMuY29tL1BDUnNfVjIueG1s
MIICXzCBgwYDVR0gBHwwejB4BggqhkiXJwMBAjBsMDoGCCsGAQUFBwIBFi5odHRw
czovL3d3dy54eXppbnRlZ3JhdG9ycy5jb20vcGxhdGNlcnRjcHMucGRmMC4GCCsG
AQUFBwICMCIMIFRDRyBUcnVzdGVkIFBsYXRmb3JtIEVuZG9yc2VtZW50MH4GA1Ud
EQR3MHWkczBxMREwDwYGZ4EFBQEBDAVJbnRlbDEVMBMGBmeBBQUBAjAJBgcrBgEE
AYJXMRMwEQYGZ4EFBQEEDAdTMjYwMEtQMRYwFAYGZ4EFBQEFDApINzY5NjItMzUw
MRgwFgYGZ4EFBQEGDAxCUUtQOTk5NDA2NDMwgbIGA1UdNwEB/wSBpzCBpDCBoaCB
nqSBmzCBmDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAlRYMQ8wDQYDVQQHDAZBdXN0
aW4xFzAVBgNVBAoMDlhZWiBJbnRlZ3JhdG9yMR4wHAYDVQQLDBVFSyBDZXJ0aWZp
Y2F0ZSBJc3N1ZXIxHzAdBgNVBAMMFnd3dy54eXppbnRlZ3JhdG9ycy5jb20xETAP
BgNVBAUTCDMyODczODcyMB8GA1UdIwQYMBaAFNRpkCYCgdVeg0sDl26rip+PhMmD
MD8GCCsGAQUFBwEBBDMwMTAvBggrBgEFBQcwAYYjaHR0cHM6Ly93d3cueHl6aW50
ZWdyYXRvcnMuY29tL29jc3AwQAYDVR0fBDkwNzA1oDOgMYYvaHR0cHM6Ly93d3cu
eHl6aW50ZWdyYXRvcnMuY29tL3BsYXRmb3JtY2VydC5jcmwwDQYJKoZIhvcNAQEL
BQADggEBAGx3K17RCixE32TPB4u52TeoQxla9zROywTOAVDLa0Na4mfqmt3mTYuE
hkCbYnYX9sqa0KCYmBTTjjO7LndOO7UisQsx8vKTDDVQ6E3etxeeqdiY8g4Rv+t1
nC8Hna+UZ+Lv+rUze/FaOiXH4rn6kxK7jsGe2lVIC7qvIzWnjcF5kgxOQ3SqFmWJ
```

VFXj2FUqauP4WbDQEH/H+Fgr8QU5Qq/k6nPZXs1CG3cKZfcSOQerF7nWOgCdClbQ
pmfS+PWz10RWbvx6s9+EI+3Ky0GXQrfq3kmbM6Owmfgr9WMkoHJTiBRx8kK+bObd
7GjNOTGvbrHYTslWFF5aDB78md+jJ8A=
-----END ATTRIBUTE CERTIFICATE-----

A.2.2 DER Format

```
SEQUENCE :
   SEQUENCE :
      INTEGER : 1
      SEQUENCE :
         CONTEXT SPECIFIC (0) :
            SEQUENCE :
               CONTEXT SPECIFIC (4) :
                  SEQUENCE :
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : countryName [2.5.4.6]
                           PRINTABLE STRING : 'US'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
                           UTF8 STRING : 'CA'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : localityName [2.5.4.7]
                           UTF8 STRING : 'Santa Clara'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : organizationName [2.5.4.10]
                           UTF8 STRING : 'Intel Corporation'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                           UTF8 STRING : 'Platform Attribute Certificate Issuer'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : commonName [2.5.4.3]
                           UTF8 STRING : 'www.intel.com'
            INTEGER : 602967EA7924FDEE6CC150B91E83777D1F427999
      CONTEXT SPECIFIC (0) :
         SEQUENCE :
            CONTEXT SPECIFIC (4) :
               SEQUENCE :
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : countryName [2.5.4.6]
                        PRINTABLE STRING : 'US'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
                        UTF8 STRING : 'TX'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : localityName [2.5.4.7]
                        UTF8 STRING : 'Austin'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : organizationName [2.5.4.10]
                        UTF8 STRING : 'XYZ Integrator'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                        UTF8 STRING : 'Delta Platform Attribute Certificate Issuer'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : commonName [2.5.4.3]
                        UTF8 STRING : 'www.xyzintegrators.com'
      SEQUENCE :
         OBJECT IDENTIFIER :  [1.2.840.113549.1.1.11]
         NULL :
      INTEGER : 34928388
      SEQUENCE :
         GENERALIZED TIME : '20181015210811Z'
         GENERALIZED TIME : '20200820210811Z'
      SEQUENCE :
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.2.25]
            SET :
               SEQUENCE :
                  OBJECT IDENTIFIER :  [2.23.133.8.5]
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.2.23]
            SET :
               SEQUENCE :
                  INTEGER : 1
                  INTEGER : 1
                  INTEGER : 13
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.5.1.7.2]
            SET :
               SEQUENCE :
                  CONTEXT SPECIFIC (0) :
                     SEQUENCE :
                        SEQUENCE :
                           OBJECT IDENTIFIER :  [2.23.133.18.3.1]
                           OCTET STRING : 0000000A
                        UTF8 STRING : 'ABC OEM'
                        UTF8 STRING : 'WR06X7871FTL'
                        CONTEXT SPECIFIC (0) : 41353535352D393939
                        CONTEXT SPECIFIC (1) : 312E31
                        CONTEXT SPECIFIC (2) : 2B06010401822C
                        CONTEXT SPECIFIC (3) : FF
                        CONTEXT SPECIFIC (4) :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.1]
                              UTF8 STRING : 'AF:3A:94:10:A5'
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.2]
                              UTF8 STRING : 'AF:37:10:D2:A8'
                        CONTEXT SPECIFIC (5) :
                           CONTEXT SPECIFIC (0) :
                              SEQUENCE :
                                 OBJECT IDENTIFIER :  [1.3.6.1.4.1.22554.1.2.1]
                              OCTET                          STRING                               :
6003A33432FD914B6003A33432FD914B6003A33432FD914B6003A33432FD914B
                           CONTEXT SPECIFIC (1) :
                              SEQUENCE :
                                 CONTEXT SPECIFIC (4) :
                                    SEQUENCE :
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : countryName [2.5.4.6]
                                             PRINTABLE STRING : 'US'
                                       SET :
                                          SEQUENCE :
                                             OBJECT   IDENTIFIER   :   stateOrProvinceName
[2.5.4.8]
                                             UTF8 STRING : 'FL'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : localityName [2.5.4.7]
                                             UTF8 STRING : 'Ft. Lauderdale'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : organizationName [2.5.4.10]
                                             UTF8 STRING : 'ABC Corporation'
                                       SET :
                                          SEQUENCE :
                                             OBJECT   IDENTIFIER   :   organizationalUnitName
[2.5.4.11]
                                             UTF8 STRING : 'Platform Certificate Issuer'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : commonName [2.5.4.3]
                                             UTF8 STRING : 'www.abc.com'
                              INTEGER : 43843898843
                        CONTEXT SPECIFIC (6) :
                           IA5 STRING : 'https://www.abc.com/certs/43843898843.cer'
                        CONTEXT SPECIFIC (7) : 02
                     SEQUENCE :
                        SEQUENCE :
                           OBJECT IDENTIFIER :  [2.23.133.18.3.1]
                           OCTET STRING : 00000041
                        UTF8 STRING : 'Component Corp'
                        UTF8 STRING : 'XT98287LL'
                        CONTEXT SPECIFIC (0) : 463938312D3031
                        CONTEXT SPECIFIC (1) : 322E31
                        CONTEXT SPECIFIC (2) : 2B060104018348
                        CONTEXT SPECIFIC (3) : FF
                        CONTEXT SPECIFIC (4) :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.2]
                              UTF8 STRING : '73:9B:92:40:FA'
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.17.3]
                              UTF8 STRING : '13:3F:98:C5:59'
                        CONTEXT SPECIFIC (5) :
                           CONTEXT SPECIFIC (0) :
                              SEQUENCE :
                                 OBJECT IDENTIFIER :  [1.3.6.1.4.1.22554.1.2.1]
                              OCTET                         STRING                         :
98AAD59183FAAB9198AAD59183FAAB9198AAD59183FAAB9198AAD59183FAAB91
                           CONTEXT SPECIFIC (1) :
                              SEQUENCE :
                                 CONTEXT SPECIFIC (4) :
                                    SEQUENCE :
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : countryName [2.5.4.6]
                                             PRINTABLE STRING : 'US'
                                       SET :
                                          SEQUENCE :
                                             OBJECT   IDENTIFIER   :   stateOrProvinceName
[2.5.4.8]
                                             UTF8 STRING : 'CA'
```

```
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : localityName [2.5.4.7]
                        UTF8 STRING : 'San Jose'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : organizationName [2.5.4.10]
                        UTF8 STRING : 'Component Corp'
                  SET :
                     SEQUENCE :
                        OBJECT   IDENTIFIER   :   organizationalUnitName [2.5.4.11]
                        UTF8 STRING : 'Platform Certificate Issuer'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : commonName [2.5.4.3]
                        UTF8 STRING : 'www.component.com'
         INTEGER : 98472878
   CONTEXT SPECIFIC (6) :
      IA5 STRING : 'https://www.component.com/certs/98472878.cer'
   CONTEXT SPECIFIC (7) : 00
SEQUENCE :
   SEQUENCE :
      OBJECT IDENTIFIER :  [2.23.133.18.3.1]
      OCTET STRING : 0000002F
   UTF8 STRING : 'XYZ OEM'
   UTF8 STRING : 'LMBT3904DW1T1G'
   CONTEXT SPECIFIC (0) : 43353535352D353535
   CONTEXT SPECIFIC (1) : 342E30
   CONTEXT SPECIFIC (2) : 2B06010401822C
   CONTEXT SPECIFIC (3) : 00
   CONTEXT SPECIFIC (4) :
      SEQUENCE :
         OBJECT IDENTIFIER :  [2.23.133.17.1]
         UTF8 STRING : '82:89:FA:D3:61'
      SEQUENCE :
         OBJECT IDENTIFIER :  [2.23.133.17.2]
         UTF8 STRING : 'D4:83:B4:F2:78'
   CONTEXT SPECIFIC (5) :
      CONTEXT SPECIFIC (0) :
         SEQUENCE :
            OBJECT IDENTIFIER :  [1.3.6.1.4.1.22554.1.2.1]
         OCTET STRING : 3432E1414B60973434323432E1414B6097343432
      CONTEXT SPECIFIC (1) :
         SEQUENCE :
            CONTEXT SPECIFIC (4) :
               SEQUENCE :
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : countryName [2.5.4.6]
                        PRINTABLE STRING : 'US'
                  SET :
                     SEQUENCE :
                        OBJECT    IDENTIFIER    :    stateOrProvinceName [2.5.4.8]
                        UTF8 STRING : 'AZ'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : localityName [2.5.4.7]
                        UTF8 STRING : 'Phoenix'
                  SET :
                     SEQUENCE :
                        OBJECT IDENTIFIER : organizationName [2.5.4.10]
```

```
                                             UTF8 STRING : 'XYC Company'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                                             UTF8 STRING : 'Platform Certificate Issuer'
                                       SET :
                                          SEQUENCE :
                                             OBJECT IDENTIFIER : commonName [2.5.4.3]
                                             UTF8 STRING : 'www.xyz.com'
                              INTEGER : 938928
                        CONTEXT SPECIFIC (6) :
                           IA5 STRING : 'https://www.xyz.com/certs/938928.cer'
                        CONTEXT SPECIFIC (7) : 01
                  CONTEXT SPECIFIC (1) :
                     IA5 STRING : 'https://www.xyzintegrators.com/platformidentifiers.xml'
                  CONTEXT SPECIFIC (2) :
                     SEQUENCE :
                        UTF8 STRING : 'TSC Enabled'
                        UTF8 STRING : 'true'
                        CONTEXT SPECIFIC (0) : 00
                     SEQUENCE :
                        UTF8 STRING : 'AMT'
                        UTF8 STRING : 'false'
                        CONTEXT SPECIFIC (0) : 01
                  CONTEXT SPECIFIC (3) :
                     IA5 STRING : 'https://www.xyzintegrators.com/platformproperties.xml'
         SEQUENCE :
            OBJECT IDENTIFIER :  [2.23.133.5.1.3]
            SET :
               SEQUENCE :
                  IA5 STRING : 'https://www.xyzintegrators.com/PCRs_V2.xml'
      SEQUENCE :
         SEQUENCE :
            OBJECT IDENTIFIER : certificatePolicies [2.5.29.32]
            OCTET STRING :
               SEQUENCE :
                  SEQUENCE :
                     OBJECT IDENTIFIER :  [1.2.840.2983.3.1.2]
                     SEQUENCE :
                        SEQUENCE :
                           OBJECT IDENTIFIER : cps [1.3.6.1.5.5.7.2.1]
                           IA5 STRING : 'https://www.xyzintegrators.com/platcertcps.pdf'
                        SEQUENCE :
                           OBJECT IDENTIFIER : unotice [1.3.6.1.5.5.7.2.2]
                           SEQUENCE :
                              UTF8 STRING : 'TCG Trusted Platform Endorsement'
         SEQUENCE :
            OBJECT IDENTIFIER : subjectAltName [2.5.29.17]
            OCTET STRING :
               SEQUENCE :
                  CONTEXT SPECIFIC (4) :
                     SEQUENCE :
                        SET :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.5.1.1]
                              UTF8 STRING : 'Intel'
                        SET :
                           SEQUENCE :
                              OBJECT IDENTIFIER :  [2.23.133.5.1.2]
                              SEQUENCE :
                                 OBJECT IDENTIFIER :  [1.3.6.1.4.1.343]
                        SET :
```

```
                  SEQUENCE :
                     OBJECT IDENTIFIER :  [2.23.133.5.1.4]
                     UTF8 STRING : 'S2600KP'
               SET :
                  SEQUENCE :
                     OBJECT IDENTIFIER :  [2.23.133.5.1.5]
                     UTF8 STRING : 'H76962-350'
               SET :
                  SEQUENCE :
                     OBJECT IDENTIFIER :  [2.23.133.5.1.6]
                     UTF8 STRING : 'BQKP99940643'
SEQUENCE :
   OBJECT IDENTIFIER :  [2.5.29.55]
   BOOLEAN : 'FF'
   OCTET STRING :
      SEQUENCE :
         SEQUENCE :
            CONTEXT SPECIFIC (0) :
               CONTEXT SPECIFIC (4) :
                  SEQUENCE :
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : countryName [2.5.4.6]
                           PRINTABLE STRING : 'US'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
                           UTF8 STRING : 'TX'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : localityName [2.5.4.7]
                           UTF8 STRING : 'Austin'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : organizationName [2.5.4.10]
                           UTF8 STRING : 'XYZ Integrator'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
                           UTF8 STRING : 'EK Certificate Issuer'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : commonName [2.5.4.3]
                           UTF8 STRING : 'www.xyzintegrators.com'
                     SET :
                        SEQUENCE :
                           OBJECT IDENTIFIER : serialNumber [2.5.4.5]
                           PRINTABLE STRING : '32873872'
SEQUENCE :
   OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
   OCTET STRING :
      SEQUENCE :
         CONTEXT SPECIFIC (0) : D46990260281D55E834B03976EAB8A9F8F84C983
SEQUENCE :
   OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
   OCTET STRING :
      SEQUENCE :
         SEQUENCE :
            OBJECT IDENTIFIER : ocsp [1.3.6.1.5.5.7.48.1]
            CONTEXT SPECIFIC (6) : 'https://www.xyzintegrators.com/ocsp'
SEQUENCE :
   OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
   OCTET STRING :
```

```
               SEQUENCE :
                  SEQUENCE :
                     CONTEXT SPECIFIC (0) :
                        CONTEXT SPECIFIC (0) :
                           CONTEXT SPECIFIC (6) :
'https://www.xyzintegrators.com/platformcert.crl'
   SEQUENCE :
      OBJECT IDENTIFIER :  [1.2.840.113549.1.1.11]
      NULL :
   BIT STRING UnusedBits:0 :
      6C772B5ED10A2C44DF64CF078BB9D937A843195AF7344ECB04CE01
      50CB6B435AE267EA9ADDE64D8B8486409B627617F6CA9AD0A09898
      14D38E33BB2E774E3BB522B10B31F2F2930C3550E84DDEB7179EA9
      D898F20E11BFEB759C2F079DAF9467E2EFFAB5337BF15A3A25C7E2
      B9FA9312BB8EC19EDA55480BBAAF2335A78DC179920C4E4374AA16
      65895455E3D8552A6AE3F859B0D0107FC7F8582BF1053942AFE4EA
      73D95ECD421B770A65F7123907AB17B9D63A009D0A56D0A667D2F8
      F5B3D744566EFC7AB3DF8423EDCACB419742B7EADE499B33A3B099
      F82BF56324A07253881471F242BE6CE6DDEC68CD3931AF6EB1D84E
      C956145E5A0C1EFC99DFA327C0
```