

TCG Platform Certificate Profile

Specification Version 1.1

Revision 19

10 April 2020

Published

Contact: admin@trustedcomputinggroup.org

TCG PUBLISHED

Copyright © TCG 2020

TCG

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.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

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

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

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
Wyllis 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

1.	Introduction	1
1.1	Purpose	1
1.2	Document Scope	1
1.3	Relationship to Other TCG Specifications	1
1.4	Keywords.....	2
1.5	Intended Audiences	2
1.6	Definition of Terms	2
2.	Certificate Overview.....	3
2.1	Platform Certificate.....	3
2.1.1	Who Uses a Platform Certificate?.....	3
2.1.2	Who Issues a Platform Certificate?.....	3
2.1.3	Revocation of a Platform Certificate	4
2.1.4	Validity Period of a Platform Certificate	4
2.1.5	Assertions Made by a Platform Certificate.....	4
2.1.5.1	Certificate Type Label	5
2.1.5.2	EK Certificates	5
2.1.5.3	Platform Manufacturer String	5
2.1.5.4	Platform Manufacturer Identifier.....	5
2.1.5.5	Platform Model	6
2.1.5.6	Platform Version.....	6
2.1.5.7	Issuer	6
2.1.5.8	Platform Specification	6
2.1.5.9	Certificate Specification	6
2.1.5.10	Validity Period	6
2.1.5.11	Signature Value.....	6
2.1.5.12	Platform Serial Number.....	6
2.1.5.13	Platform Assertions	6
2.1.5.14	Platform Configuration	7
2.1.5.15	Platform Configuration Uri.....	7
2.1.5.16	Policy Reference	7
2.1.5.17	Revocation Locator	7
2.2	Delta Platform Certificate	7
2.2.1	Who Uses a Delta Platform Certificate?	8
2.2.2	Who Issues a Delta Platform Certificate?	8
2.2.3	Conditions for Issuing a Delta Platform Certificate	8

2.2.4	Requirements for Issuing a Delta Platform Certificate	8
2.2.5	Revocation of a Delta Platform Certificate	9
2.2.6	Assertions Made by a Delta Platform Certificate	9
2.2.6.1	Certificate Type Label	10
2.2.6.2	EK Certificates	10
2.2.6.3	Base Platform Certificate	10
2.2.6.4	Platform Manufacturer String	10
2.2.6.5	Platform Manufacturer Identifier.....	11
2.2.6.6	Platform Model.....	11
2.2.6.7	Platform Version.....	11
2.2.6.8	Issuer	11
2.2.6.9	Certificate Specification	11
2.2.6.10	Validity Period	11
2.2.6.11	Signature Value.....	11
2.2.6.12	Platform Serial Number.....	11
2.2.6.13	Platform Configuration	12
2.2.6.14	Platform Configuration Uri.....	12
2.2.6.15	Policy Reference	12
2.2.6.16	Revocation Locator	12
3.	X.509 ASN.1 Definitions	13
3.1	TCG Attributes.....	13
3.1.1	TPM and Platform Assertions	13
3.1.2	Name Attributes	15
3.1.3	TCG Specification Attributes.....	15
3.1.4	TCG Certificate Type Attributes	16
3.1.5	TCG Certificate Specification Attributes	16
3.1.6	Platform Configuration Attributes	16
3.1.7	Platform Configuration Uri Attribute	19
3.2	Platform Certificate.....	19
3.2.1	Version	21
3.2.2	Serial Number	22
3.2.3	Signature Algorithm	22
3.2.4	Holder.....	22
3.2.5	Issuer	22
3.2.6	Validity.....	22
3.2.7	Certificate Policies.....	22
3.2.8	Subject Alternative Names.....	23

3.2.9	Targeting Information	23
3.2.10	Attributes	23
3.2.11	Authority Key Identifier	24
3.2.12	Authority Info Access	24
3.2.13	CRL Distribution	24
3.2.14	Issuer Unique Id	24
3.3	Delta Platform Certificate	24
3.3.1	Version	26
3.3.2	Serial Number	26
3.3.3	Signature Algorithm	26
3.3.4	Holder	26
3.3.5	Issuer	27
3.3.6	Validity	27
3.3.7	Certificate Policies	27
3.3.8	Subject Alternative Names	27
3.3.9	Targeting Information	27
3.3.10	Attributes	27
3.3.11	Authority Key Identifier	28
3.3.12	Authority Info Access	28
3.3.13	CRL Distribution	28
3.3.14	Issuer Unique Id	28
4.	X.509 ASN.1 Structures and OIDs	29
5.	References	34
A.	Certificate Examples	36
A.1	Example 1 (Platform Certificate in Attribute Certificate Format)	36
A.1.1	PEM Format	36
A.1.2	DER Format	37
A.2	Example 2 (Delta Platform Certificate in Attribute Certificate Format)	43
A.2.1	PEM Format	43
A.2.2	DER Format	45

Table of Tables

Table 1: Platform Certificate Fields	5
Table 2: Delta Platform Certificate Fields.....	10
Table 3: Attribute Certificate Format Fields.....	21
Table 4: Delta Attribute Certificate Format Fields	26

Change Log

Date	Version	Comment
2018-01-11	1.0	Initial Release
2020-04-03	1.1	<p>Addition of Delta Platform Certificate and tree hierarchy.</p> <p>Section “Revocation of a Platform Certificate” has been modified to include multiple causes of revocation.</p> <p>Section “EK Certificates” clarifies which EK Certificates must be included as reference.</p> <p>Section “Holder” clarifies use of the TargettingInformation extension to reference additional EK Certificates.</p> <p>Section “X.509 ASN.1 Structures and OIDs” includes the correct CertificateIdentifier sequence.</p> <p>Section “Assertions Made by a Platform Certificate” includes additional assertions.</p> <p>Section “Platform Configuration Attributes” was updated to include additional attributes.</p> <p>Section “Targeting Information” was added.</p> <p>Sample certificates were added to Appendix.</p> <p>The following sections were removed:</p> <ul style="list-style-type: none"> • Platform Attribute Credential Privacy Protection Requirements • Security Qualities • Conformance Attributes

1 1. Introduction

2 1.1 Purpose

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

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

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

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

29 1.2 Document Scope

30 This document specifies a complete definition of the Platform Certificate for use with any TPM
31 Family version. This specification describes the abstract definition of the certificate and
32 specifically how it would appear as an X.509 certificate.

33 1.3 Relationship to Other TCG Specifications

34 This specification references the TCG Infrastructure Working Group Reference Architecture
35 for Interoperability [2], the TCG TPM Main Specification [3], the TCG Credential Profiles for
36 TPM Family 1.2 [6], the EK Credential Profile Specification [7], the PC Client Platform TPM
37 Profile Specification [10], the Generic Server Platform Specification [9], and the TCG Algorithm
38 Registry Specification [12]. This specification replaces the Platform Credential Specification
39 defined in the TCG Credential Profiles for TPM Family 1.2 [6].

40 1.4 **Keywords**

41 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”,
42 “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be
43 interpreted as described in RFC 2119 [4].

44 1.5 **Intended Audiences**

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

49 1.6 **Definition of Terms**

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

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

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

58

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

63 **2. Certificate Overview**

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

67 **2.1 Platform Certificate**

68 A Platform Certificate attests that a specific platform contains a unique TPM and Trusted
69 Building Block (TBB).

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

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

80 **2.1.1 Who Uses a Platform Certificate?**

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

85 Another consumer of the Platform Certificate is an Enterprise, which wishes to remotely
86 provision multiple devices that belong to it. Typically, in this case, the Enterprise knows the
87 serial number of the systems it owns, and the Platform Certificate is used to associate those
88 serial numbers with particular EK certificates [6][7]. This way, for example, a VPN can be
89 provisioned using the TPM to provide keys securely to clients of an Enterprise. In order to
90 support this use case, the optional Platform Serial Number attribute MUST be included in
91 the certificate. In addition, an Enterprise could use the Platform Certificate to assert non-
92 security related properties, such as platform components, included optionally by the platform
93 manufacturer in the certificate.

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

96 **2.1.2 Who Issues a Platform Certificate?**

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

103 **2.1.3 Revocation of a Platform Certificate**

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

109 **2.1.4 Validity Period of a Platform Certificate**

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

112 **2.1.5 Assertions Made by a Platform Certificate**

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

115

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

116

Table 1: Platform Certificate Fields117 **2.1.5.1 Certificate Type Label**

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

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

125 **2.1.5.2 EK Certificates**

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

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

135 **2.1.5.3 Platform Manufacturer String**

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

138 **2.1.5.4 Platform Manufacturer Identifier**

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

142 2.1.5.5 Platform Model

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

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

146 2.1.5.6 Platform Version

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

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

151 2.1.5.7 Issuer

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

153 2.1.5.8 Platform Specification

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

157 2.1.5.9 Certificate Specification

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

160 2.1.5.10 Validity Period

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

163 2.1.5.11 Signature Value

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

165 2.1.5.12 Platform Serial Number

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

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

172 2.1.5.13 Platform Assertions

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

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

177 **2.1.5.14 Platform Configuration**

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

181 **2.1.5.15 Platform Configuration Uri**

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

184 **2.1.5.16 Policy Reference**

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

187 **2.1.5.17 Revocation Locator**

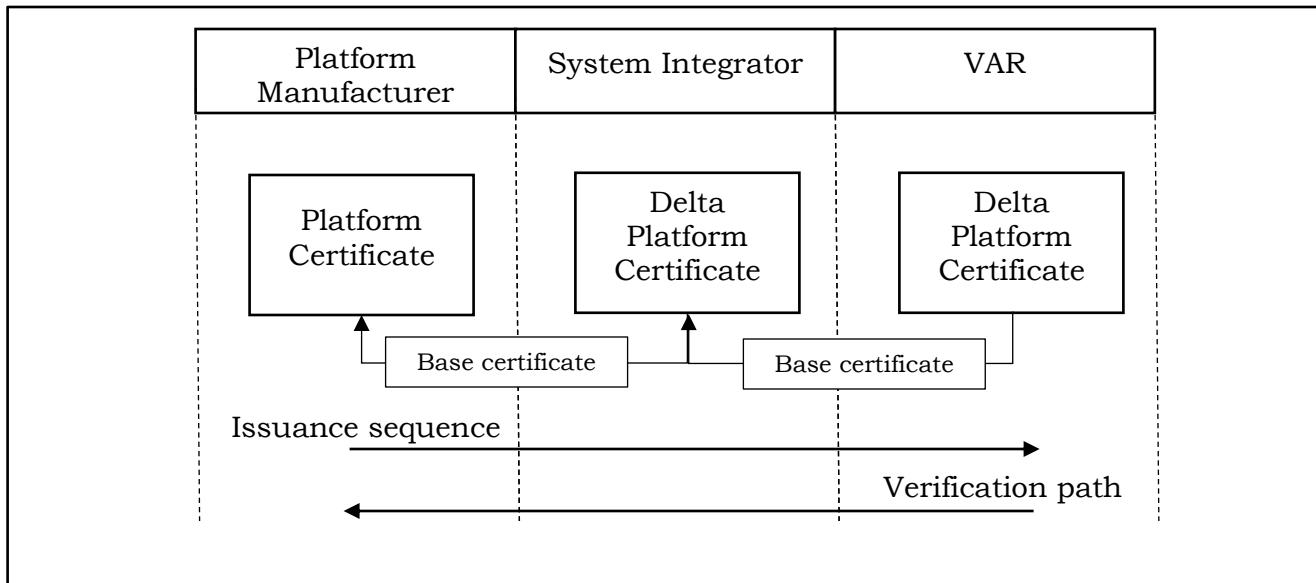
188 This assertion enables the certificate consumer to determine whether the Platform Certificate
189 has been revoked and should no longer be used as the basis for a trust decision.

190 **2.2 Delta Platform Certificate**

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

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

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



205

206

207

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.

249

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

250

Table 2: Delta Platform Certificate Fields251 **2.2.6.1 Certificate Type Label**252 For Platform Certificates, the value of this field MUST be the string, “TCG Trusted Platform
253 Endorsement”.254 **2.2.6.2 EK Certificates**255 This assertion is used to reference additional EK certificates issued by the Delta Platform
256 Certificate issuer.257 This SHALL be an unambiguous indication of the EK certificates of the TPM incorporated into
258 the platform.259 **2.2.6.3 Base Platform Certificate**260 This assertion is used by the verifier to bind the certificate to the previously issued Platform
261 Certificate or Delta Platform Certificate. The base certificate is the previously issued Platform
262 Certificate or Delta Platform Certificate amended by this certificate.

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

264 **2.2.6.4 Platform Manufacturer String**265 This assertion identifies the platform manufacturer using a Platform Manufacturer assigned
266 string. This field MUST equal that of the base Platform Certificate or base Delta Platform
267 Certificate.

268 **2.2.6.5 Platform Manufacturer Identifier**

269 This assertion identifies the platform manufacturer with a globally unique and verifiable
270 value. If included, the issuer SHALL use the manufacturer's Internet Assigned Numbers
271 Authority (IANA) Private Enterprise Number as the identifier [8]. This field MUST equal that
272 of the base Platform Certificate or base Delta Platform Certificate.

273 **2.2.6.6 Platform Model**

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

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

278 **2.2.6.7 Platform Version**

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

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

284 **2.2.6.8 Issuer**

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

286 **2.2.6.9 Certificate Specification**

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

290 **2.2.6.10 Validity Period**

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

292 **2.2.6.11 Signature Value**

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

294 **2.2.6.12 Platform Serial Number**

295 This assertion is a value that uniquely identifies the platform. This is used by the verifier to
296 correlate the certificate to a physical platform. The issuer SHALL use a customer visible serial
297 number as the identifier. This field MUST equal that of the base Platform Certificate or base
298 Delta Platform Certificate.

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

300 2.2.6.13 Platform Configuration

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

304 2.2.6.14 Platform Configuration Uri

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

308 2.2.6.15 Policy Reference

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

311 2.2.6.16 Revocation Locator

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

314 **3. X.509 ASN.1 Definitions**

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

318 **3.1 TCG Attributes**

319 **3.1.1 TPM and Platform Assertions**

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

321 Each attribute begins with a version number that identifies the version of the assertion
322 syntax. Future versions of this profile could add new assertions by appending new fields at
323 the end of the ASN.1 SEQUENCE and increasing the version number to identify which version
324 of the assertion syntax is encoded.

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

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

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

335
336 **URIMAX** is a constant used to provide an upper bound on the length of a URI included in the
337 certificate. This upper bound is helpful to consumers of the extension and also helps limit
338 the overall size of the certificate. In order to provide a reasonable upper bound for ASN.1
339 parsers, **URIMAX** SHOULD NOT exceed a value of 1024. This value was selected as it matches
340 the length limit for <A> anchors in HTML as specified by the SGML declaration (LITLEN) for
341 HTML[5].

342 **STRMAX** is a constant defining the upper bound on the length of a string type. Like the **URIMAX**
343 this is to aid ASN.1 parsers and help limit the upper bound on the length of the certificate.
344 Based on the expected sizes of the strings in the ASN.1 in this document an upper bound of
345 256 was selected. **STRMAX** SHOULD NOT exceed a value of 256.

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

347     tBBSecurityAssertions ATTRIBUTE ::= {
348         WITH SYNTAX TBBSecurityAssertions
349         ID tcg-at-tbbSecurityAssertions }

350

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

358

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

```

362 -- Virtual means the TPM is virtualized (possibly running in a VMM).
363 -- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
364 -- the capabilities of the platform.
365 MeasurementRootType ::= ENUMERATED {
366     static (0),
367     dynamic (1),
368     nonHost (2),
369     hybrid (3),
370     physical (4),
371     virtual (5) }
372
373
374 -- common criteria evaluation
375
376 CommonCriteriaMeasures ::= SEQUENCE {
377     version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined by CC
378     assuranceLevel EvaluationAssuranceLevel,
379     evaluationStatus EvaluationStatus,
380     plus BOOLEAN DEFAULT FALSE,
381     strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
382     profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
383     profileUri [2] IMPLICIT URIReference OPTIONAL,
384     targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
385     targetUri [4] IMPLICIT URIReference OPTIONAL }
386
387 EvaluationAssuranceLevel ::= ENUMERATED {
388     level1 (1),
389     level2 (2),
390     level3 (3),
391     level4 (4),
392     level5 (5),
393     level6 (6),
394     level7 (7) }
395
396 StrengthOfFunction ::= ENUMERATED {
397     basic (0),
398     medium (1),
399     high (2) }
400
401 -- Reference to external document containing information relevant to this subject.
402 -- The hashAlgorithm and hashValue MUST both exist in each reference if either
403 -- appear at all.
404 URIReference ::= SEQUENCE {
405     uniformResourceIdentifier IA5String (SIZE (1..URIMAX)),
406     hashAlgorithm AlgorithmIdentifier OPTIONAL,
407     hashValue BIT STRING OPTIONAL }
408
409 EvaluationStatus ::= ENUMERATED {
410     designedToMeet (0),
411     evaluationInProgress (1),
412     evaluationCompleted (2) }
413
414 -- fips evaluation
415
416 FIPSLevel ::= SEQUENCE {
417     version IA5STRING (SIZE (1..STRMAX)), -- "140-1", "140-2", or "140-3"
418     level SecurityLevel,
419     plus BOOLEAN DEFAULT FALSE }
420
421 SecurityLevel ::= ENUMERATED {
422     level1 (1),
423     level2 (2),
424     level3 (3),
425     level4 (4) }
426

```

427 **3.1.2 Name Attributes**

428 The following definitions define the syntax of the relative distinguished names (RDNs) used
429 in the subject alternative name extension to identify the type of the TPM and the platform.
430 The value of the **PlatformManufacturerStr** attribute is a UTF 8 string with the name of
431 platform manufacturing company.
432 The **PlatformModel** attribute is a UTF 8 string with the manufacturer-specific model.
433 The **PlatformVersion** attribute is a UTF 8 string with manufacturer-specific platform version
434 value.
435 The **PlatformSerial** optional attribute is a UTF 8 string with manufacturer-specific platform
436 serial number value.
437 The **PlatformManufacturerId** optional attribute is the OID of the IANA Private Enterprise
438 Number [8] assigned to the platform manufacturer.
439 These attributes MUST be included in the Delta Platform Certificate.
440

```
441
442     PlatformManufacturerStr ATTRIBUTE ::= {
443         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
444         ID tcg-at-platformManufacturerStr }
445
446     PlatformModel ATTRIBUTE ::= {
447         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
448         ID tcg-at-platformModel }
449
450     PlatformVersion ATTRIBUTE ::= {
451         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
452         ID tcg-at-platformVersion }
453
454     PlatformSerial ATTRIBUTE ::= {
455         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
456         ID tcg-at-platformSerial }
457
458     PlatformManufacturerId ATTRIBUTE ::= {
459         WITH SYNTAX ManufacturerId
460         ID tcg-at-platformManufacturerId
461     }
462
463     ManufacturerId ::= SEQUENCE {
464         manufacturerIdentifier    PrivateEnterpriseNumber
465     }
466
467     enterprise OBJECT IDENTIFIER ::= {
468         iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) }
469
470     PrivateEnterpriseNumber OBJECT IDENTIFIER ::= { enterprise private-enterprise-number }
```

471 All assigned private enterprise numbers are listed at the Internet Assigned Numbers
472 Authority (IANA) web site [8].
473

474 **3.1.3 TCG Specification Attributes**

475 The following definitions define the syntax of the TPM and platform-specific specification
476 attributes.
477 The **TCGPlatformSpecification** attribute identifies the platform class, version and revision
478 of the platform-specific specification with which a platform implementation is compliant. The
479 platform specification refers either to the PC Client Platform Specification [10] or the Server

480 Specification [9]. Standardized platform class values are defined in section 4 Platform Class
 481 of the Registry of Reserved TPM 2.0 Handles and Localities [22]. This attribute MUST NOT be
 482 included in the Delta Platform Certificate.

```
483
484   tCGPlatformSpecification ATTRIBUTE ::= {
485     WITH SYNTAX TCGPlatformSpecification
486     ID tcg-at-tcgPlatformSpecification }
487
488   TCGSpecificationVersion ::= SEQUENCE {
489     majorVersion INTEGER,
490     minorVersion INTEGER,
491     revision INTEGER }
492
493   TCGPlatformSpecification ::= SEQUENCE {
494     Version TCGSpecificationVersion,
495     platformClass OCTET STRING SIZE(4) }
```

496 3.1.4 TCG Certificate Type Attributes

497 The following defines the syntax of the certificate type attribute.

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

```
502
503   tCGCredentialType ATTRIBUTE ::= {
504     WITH SYNTAX TCGCredentialType
505     ID tcg-at-tcgCredentialType}
506
507   TCGCredentialType ::= SEQUENCE {
508     certificateType CredentialType }
509
510   CredentialType ::= OBJECT IDENTIFIER
511     (tcg-kp-PlatformAttributeCertificate | tcg-kp-
      DeltaPlatformAttributeCertificate )
```

512 3.1.5 TCG Certificate Specification Attributes

513 The following defines the syntax of the certificate specification attributes.

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

```
518
519   tCGCredentialSpecification ATTRIBUTE ::= {
520     WITH SYNTAX TCGSpecificationVersion
521     ID tcg-at-tcgCredentialSpecification }
522
523   TCGSpecificationVersion ::= SEQUENCE {
524     majorVersion INTEGER,
525     minorVersion INTEGER,
      revision INTEGER }
```

526 3.1.6 Platform Configuration Attributes

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

528 The **platformConfiguration** attribute contains optional lists of platform component
 529 identifiers, component identifier URI, platform properties, and platform property URI. The
 530 **componentIdentifier** field contains a list of individual components that constitute the

531 platform. The issuer MUST include the component class, manufacturer and model, and
532 optionally provide the component serial number, revision, and the component manufacturer's
533 IANA **PrivateEnterpriseNumber**. In addition, each component identifier MAY contain
534 information such as whether it is field replaceable, its network address, platform certificate,
535 and platform certificate URI.

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

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

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

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

556 The optional **platformProperties** field SHALL contain characteristics of the platform that
557 the issuer considers of interest to the consumer. Such properties are not prescribed by this
558 specification and the certificate issuer is free to choose which information to include in this
559 field. The manufacturer MAY use the **platformPropertiesUri** to publish information about
560 the Properties included in the **platformProperties** field. This MAY include the list of
561 **propertyName** and their semantics.

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

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

569

```
570     platformConfiguration ATTRIBUTE ::= {
571         WITH SYNTAX PlatformConfiguration
572         ID tcg-at-platformConfiguration-v2
573     }
574
575     PlatformConfiguration ::= SEQUENCE {
576         componentIdentifiers [0] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF ComponentIdentifier OPTIONAL,
577         componentIdentifiersUri [1] IMPLICIT URIReference OPTIONAL,
```

```

578     platformProperties [2] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF Property OPTIONAL,
579     platformPropertiesUri [3] IMPLICIT URIReference OPTIONAL
580   }
581
582   ComponentIdentifier ::= SEQUENCE {
583     componentClass ComponentClass,
584     componentManufacturer UTF8String (SIZE (1..STRMAX)),
585     componentModel UTF8String (SIZE (1..STRMAX)),
586     componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
587     componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
588     componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,
589     fieldReplaceable [3] IMPLICIT BOOLEAN OPTIONAL,
590     componentAddresses [4] IMPLICIT SEQUENCE(SIZE(1.. MAX)) OF ComponentAddress OPTIONAL
591     componentPlatformCert [5] IMPLICIT CertificateIdentifier OPTIONAL,
592     componentPlatformCertUri [6] IMPLICIT URIReference OPTIONAL,
593     status [7] IMPLICIT AttributeStatus OPTIONAL }
594
595   ComponentClass ::= SEQUENCE {
596     componentClassRegistry ComponentClassRegistry,
597     componentClassValue OCTET STRING SIZE(4) }
598
599   ComponentClassRegistry ::= OBJECT IDENTIFIER ( tcg-registry-componentClass-tcg | tcg-registry-
600   componentClass-ietf | tcg-registry-componentClass-dmtf )
601
602   ComponentAddress ::= SEQUENCE {
603     addressType AddressType,
604     addressValue UTF8String (SIZE (1..STRMAX)) }
605
606   AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
607   bluetoothmac)
608
609   Property ::= SEQUENCE {
610     propertyName UTF8String (SIZE (1..STRMAX)),
611     PropertyValue UTF8String (SIZE (1..STRMAX)),
612     status [0] IMPLICIT AttributeStatus OPTIONAL }
613
614   CertificateIdentifier ::= SEQUENCE {
615     attributeCertIdentifier [0] IMPLICIT AttributeCertificateIdentifier OPTIONAL,
616     genericCertIdentifier [1] IMPLICIT IssuerSerial OPTIONAL }
617
618   AttributeCertificateIdentifier ::= SEQUENCE {
619     hashAlgorithm AlgorithmIdentifier,
620     hashOverSignatureValue OCTET STRING
621   }
622
623   IssuerSerial ::= SEQUENCE {
624     issuer GeneralNames,
625     serial CertificateSerialNumber
626   }
627
628   AttributeStatus ::= ENUMERATED {
629     added (0),
630     modified (1),
631     removed (2) }
632
633 Three ComponentClassRegistry OIDs have been defined by the TCG. The tcg-registry-
634 componentClass-tcg is a placeholder that refers to a future TCG Component Class
635 Registry. The tcg-registry-componentClass-ietf refers to the IETF RFC8348 [19] IANA
636 Hardware Class. The tcg-registry-componentClass-dmtf is a placeholder to refer to a
637 future SMBIOS based registry.
638
639 The AttributeCertificateIdentifier sequence is comprised of the hashAlgorithm field
640 and the hashOverSignatureValue. The hashAlgorithm field is of type AlgorithmIdentifier as
641 defined in RFC5280 [13]. This field identifies the hashing algorithm used in
642 hashOverSignatureValue field. The hashOverSignatureValue is calculated over the Platform

```

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

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

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

650 Since the algorithms used are all hashing algorithms, the parameters field SHOULD not be
651 used. The issuer MAY utilize any of the hash algorithm OIDs found in RFC3279 [15], RFC4055
652 [16], SHA-3 Related Algorithms and Identifiers for PKIX [17], and GB/T 33560-2017 [18].

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

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

662 **3.1.7 Platform Configuration Uri Attribute**

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

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

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

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

674 **3.2 Platform Certificate**

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

677 The Platform Certificate makes the assertions listed in section 2.1.6. This certificate format
678 adheres to RFC 5755 [11] and all requirements and limitations from that specification apply
679 unless otherwise noted.

680 **NOTE:** some fields are assigned a value even though the certificate user performs no action
681 with that value. In such cases, the intention is to inhibit non-TCG implementations from
682 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	UniqueIdIdentifier	Unique value when using a shared issuer name	SHOULD NOT

683

Table 3: Attribute Certificate Format Fields

684

3.2.1 Version

685

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).

686

687

688 3.2.2 Serial Number

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

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

693 3.2.3 Signature Algorithm

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

697 3.2.4 Holder

698 This field contains a reference to one of the required X.509 TPM EK certificates. The
699 BaseCertificateID choice MUST be used. Additional required TPM EK certificates MUST be
700 referenced using the TargetingInformation extension. Optional EK certificates MAY be
701 referenced using the TargetingInformation extension.

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

704 3.2.5 Issuer

705 This field contains the distinguished name of the entity that issued this Platform Certificate.
706 This is the entity that asserts that the platform incorporates a TPM and RTM in a manner
707 that conforms to the relevant TCG Platform Specific specification.

708 3.2.6 Validity

709 This field contains the period during which the binding between the attributes and TPM EK
710 certificates is considered valid. It is represented by two date values named notBefore and
711 notAfter. Issuers SHOULD assign notBefore to the current time when the certificate is issued
712 and notAfter to the last date that the certificate will be considered valid. Both notBefore and
713 notAfter MUST use the appropriate time format as indicated by RFC 5755 [11], section 4.2.6
714 Validity Period.

715 3.2.7 Certificate Policies

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

717 Assign "critical" the value FALSE. Assign **policyIdentifier** at least one object identifier.
718 Assign the **cPSuri** policy qualifier the value of an HTTP URL at which a plain language version
719 of the platform endorsement entity's certificate policy could be obtained. Assign the explicit
720 text **userNotice** policy qualifier the value "TCG Trusted Platform Endorsement".

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

723 **3.2.8 Subject Alternative Names**

724 This extension contains the alternative name of the entity associated with this certificate.
725 Assign "critical" the value FALSE. Include the platform model, using the directory name-form
726 with RDNs for the platform manufacturer, model, version number, and optionally, the serial
727 number, and manufacturer ID. The "Platform Manufacturer Identifier" optional field uniquely
728 identifies the platform's manufacturer using the IANA Private Enterprise Number OID [8].
729 During certificate validation, the Privacy-CA MUST check that the platform manufacturer,
730 model, version, serial numbers, and manufacturer ID are acceptable.

731 **3.2.9 Targeting Information**

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

738 **3.2.10 Attributes**

739 The following attributes SHOULD be included:

- 740 • The "TCG Platform Specification" attribute references the platform class, version and
741 revision level of the TCG platform-specific specification to which the platform was
742 designed.
- 743 • The "TCG Certificate Type" attribute identifies the type of certificate and its format.
- 744 • The "TCG Certificate Specification" attribute references the version, level, and revision
745 of this specification.
- 746 • The platform "TBB Security Assertions" attribute describes various assertions about
747 the security properties of the TBB of the platform.

748 The following attributes MAY be included:

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

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

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

- 762 • If the RTM and the means by which the TPM and RTM have been incorporated into the
763 platform have been successfully evaluated against a Common Criteria protection
764 profile, then include the "TBB protection profile" identifier attribute.
765 • If the RTM and the means by which the TPM and RTM have been incorporated into the
766 platform have been successfully evaluated against a Common Criteria security target,
767 then include the "TBB security target" identifier attribute.
768 • Optionally, include the "security qualities" attribute with a text string reflecting the
769 security qualities of the platform.

770 **3.2.11 Authority Key Identifier**

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

774 **3.2.12 Authority Info Access**

775 This extension contains additional information about the issuer. Assign “critical” the value
776 FALSE. It MAY be omitted. If included, then the accessMethod OID SHOULD be set to id-ad-
777 ocsp (RFC 5755 [11]) and the accessLocation value SHOULD point to the access value of the
778 OCSP responder (HTTP URI).

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

783 **3.2.13 CRL Distribution**

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

788 **3.2.14 Issuer Unique Id**

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

791 **3.3 Delta Platform Certificate**

792 This section contains the format for a Delta Platform Certificate. The Delta Platform Certificate
793 makes the assertions listed in section 2.2.6. This certificate format adheres to RFC 5755 [11]
794 and all requirements and limitations from that specification apply unless otherwise noted.

795 **NOTE:** some fields are assigned a value even though the certificate user performs no action
796 with that value. In such cases, the intention is to inhibit non-TCG implementations from
797 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

798

Table 4: Delta Attribute Certificate Format Fields**799 3.3.1 Version**

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

802 3.3.2 Serial Number

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

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

807 3.3.3 Signature Algorithm

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

811 3.3.4 Holder

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

814 **3.3.5 Issuer**

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

819 **3.3.6 Validity**

820 This field contains the period during which the assertions made by the issuer about the
821 platform are considered valid. Issuers SHOULD assign notBefore to the current time when
822 the certificate is issued and notAfter to the last date that the certificate will be considered
823 valid. The notAfter date SHOULD not precede that of the base certificate. Both notBefore and
824 notAfter MUST use the appropriate time format as indicated by RFC 5755 [11], section 4.2.6
825 Validity Period.

826 **3.3.7 Certificate Policies**

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

828 Assign “critical” the value FALSE. Assign policyIdentifier at least one object identifier. Assign
829 the cPSuri policy qualifier the value of an HTTP URL at which a plain language version of the
830 platform endorsement entity’s certificate policy could be obtained. Assign the explicit text
831 userNotice policy qualifier the value “TCG Trusted Platform Endorsement”.

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

834 **3.3.8 Subject Alternative Names**

835 This extension contains the platform name attributes. This extension MUST equal that of the
836 base Platform or Delta Platform Certificate, the issuer MUST NOT introduce any changes.
837 Assign "critical" the value FALSE. Include the platform model, using the directory name-form
838 with RDNs for the platform manufacturer, model, version number, and optionally, the serial
839 number, and manufacturer ID. The “Platform Manufacturer Identifier” optional field uniquely
840 identifies the platform’s manufacturer using the IANA Private Enterprise Number OID [8].

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

843 **3.3.9 Targeting Information**

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

846 **3.3.10 Attributes**

847 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.

851 The following attributes MAY be included:

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

857 **3.3.11 Authority Key Identifier**

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

861 **3.3.12 Authority Info Access**

862 This extension contains additional information about the issuer. Assign “critical” the value
863 FALSE. This extension MAY be omitted. If included, then the accessMethod OID SHOULD be
864 set to id-ad-ocsp (RFC 5755 [11]) and the accessLocation value SHOULD point to the access
865 value of the OCSP responder (HTTP URI).

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

870 **3.3.13 CRL Distribution**

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

875 **3.3.14 Issuer Unique Id**

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

878 4. X.509 ASN.1 Structures and OIDs

879 TCG has registered an object identifier (OID) namespace as an “international body” in the ISO
880 registration hierarchy. This leads to shorter OIDs and gives TCG the ability to manage its own
881 namespace. The OID namespace is inherited from TCPA specifications. These definitions are
882 intended to be used within the context of an X.509 v3 certificate specifically leveraging the
883 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}
```

```

945      tcg-ce-relevantManifests OBJECT IDENTIFIER ::= {tcg-ce 3}
946      tcg-ce-virtualPlatformAttestationService OBJECT IDENTIFIER ::= {tcg-ce 4}
947      tcg-ce-migrationControllerAttestationService OBJECT IDENTIFIER ::= {tcg-ce 5}
948      tcg-ce-migrationControllerRegistrationService OBJECT IDENTIFIER ::= {tcg-ce 6}
949      tcg-ce-virtualPlatformBackupService OBJECT IDENTIFIER ::= {tcg-ce 7}
950
951      -- TCG Protocol OIDs
952      tcg-prt-tpmIdProtocol OBJECT IDENTIFIER ::= {tcg-protocol 1}
953
954      -- TCG Address OIDs
955      tcg-address-ethernetmac OBJECT IDENTIFIER ::= {tcg-address 1}
956      tcg-address-wlanniac OBJECT IDENTIFIER ::= {tcg-address 2}
957      tcg-address-bluetoothmac OBJECT IDENTIFIER ::= {tcg-address 3}
958
959      -- TCG Registry OIDs
960      tcg-registry-componentClass OBJECT IDENTIFIER ::= {tcg-registry 3}
961      tcg-registry-componentClass-tcg OBJECT IDENTIFIER ::= {tcg-registry-componentClass 1}
962      tcg-registry-componentClass-ietf OBJECT IDENTIFIER ::= {tcg-registry-componentClass 2}
963      tcg-registry-componentClass-dmtf OBJECT IDENTIFIER ::= {tcg-registry-componentClass 3}
964
965
966      -- tcg specification attributes for platform
967      tCGPlatformSpecification ATTRIBUTE ::= {
968          WITH SYNTAX TCGPlatformSpecification
969          ID tcg-at-tcgPlatformSpecification }
970
971      TCGSpecificationVersion ::= SEQUENCE {
972          majorVersion INTEGER,
973          minorVersion INTEGER,
974          revision INTEGER }
975
976      TCGPlatformSpecification ::= SEQUENCE {
977          Version TCGSpecificationVersion,
978          platformClass OCTET STRING SIZE(4) }
979
980      -- TCG Credential type attribute
981      tCGCredentialType ATTRIBUTE ::= {
982          WITH SYNTAX TCGCredentialType
983          ID tcg-at-tcgCredentialType}
984
985      TCGCredentialType ::= SEQUENCE {
986          certificateType CredentialType}
987
988      CredentialType ::= OBJECT IDENTIFIER (tcg-kp-PlatformAttributeCertificate | tcg-kp-
989          DeltaPlatformAttributeCertificate )
990
991      -- manufacturer implementation model and version attributes
992      PlatformManufacturerStr ATTRIBUTE ::= {
993          WITH SYNTAX UTF8String (SIZE (1..STRMAX))
994          ID tcg-at-platformManufacturerStr }
995
996      PlatformModel ATTRIBUTE ::= {
997          WITH SYNTAX UTF8String (SIZE (1..STRMAX))
998          ID tcg-at-platformModel }
999
1000     PlatformVersion ATTRIBUTE ::= {
1001         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1002         ID tcg-at-platformVersion }
1003
1004     PlatformSerial ATTRIBUTE ::= {
1005         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1006         ID tcg-at-platformSerial }
1007
1008     PlatformManufacturerId ATTRIBUTE ::= {
1009         WITH SYNTAX ManufacturerId
1010         ID tcg-at-platformManufacturerId
1011     }
1012
1013     ManufacturerId ::= SEQUENCE {
1014         manufacturerIdentifier PrivateEnterpriseNumber
1015     }

```

```

1016
1017 enterprise OBJECT IDENTIFIER ::= {
1018     iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)
1019
1020 PrivateEnterpriseNumber OBJECT IDENTIFIER ::= { enterprise private-enterprise-number }
1021
1022
1023 -- platform tbb security assertions
1024
1025 tBBSecurityAssertions ATTRIBUTE ::= {
1026     WITH SYNTAX TBBSecurityAssertions
1027     ID tcg-at-tbbSecurityAssertions }
1028
1029 TBBSecurityAssertions ::= SEQUENCE {
1030     version Version DEFAULT v1,
1031     ccInfo [0] IMPLICIT CommonCriteriaMeasures OPTIONAL,
1032     fipsLevel [1] IMPLICIT FIPSLevel OPTIONAL,
1033     rtmType [2] IMPLICIT MeasurementRootType OPTIONAL,
1034     iso9000Certified BOOLEAN DEFAULT FALSE,
1035     iso9000Uri IA5STRING (SIZE (1..URIMAX)) OPTIONAL }
1036
1037
1038 -- Hybrid means the measurement root is capable of static AND dynamic
1039 -- Physical means that the root is anchored by a physical TPM
1040 -- Virtual means the TPM is virtualized (possibly running in a VMM)
1041
1042 -- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
1043 -- the capabilities of the platform.
1044 MeasurementRootType ::= ENUMERATED {
1045     static (0),
1046     dynamic (1),
1047     nonHost (2),
1048     hybrid (3),
1049     physical (4),
1050     virtual (5) }
1051
1052
1053 -- common criteria evaluation
1054 CommonCriteriaMeasures ::= SEQUENCE {
1055     version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined by CC
1056     assurancelevel EvaluationAssuranceLevel,
1057     evaluationStatus EvaluationStatus,
1058     plus BOOLEAN DEFAULT FALSE,
1059     strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
1060     profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
1061     profileUri [2] IMPLICIT URIReference OPTIONAL,
1062     targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
1063     targetUri [4] IMPLICIT URIReference OPTIONAL }
1064
1065 EvaluationAssuranceLevel ::= ENUMERATED {
1066     level1 (1),
1067     level2 (2),
1068     level3 (3),
1069     level4 (4),
1070     level5 (5),
1071     level6 (6),
1072     level7 (7) }
1073
1074 StrengthOfFunction ::= ENUMERATED {
1075     basic (0),
1076     medium (1),
1077     high (2) }
1078
1079 URIReference ::= SEQUENCE {
1080     uniformResourceIdentifier IA5String (SIZE (1..URIMAX)),
1081     hashAlgorithm AlgorithmIdentifier OPTIONAL,
1082     hashValue BIT STRING OPTIONAL }
1083
1084 EvaluationStatus ::= ENUMERATED {
1085     designedToMeet (0),
1086     evaluationInProgress (1),

```

```

1087         evaluationCompleted (2) }

1088
1089 -- fips evaluation
1090 FIPSLevel ::= SEQUENCE {
1091     version IA5STRING (SIZE (1..STRMAX)), -- "140-1", "140-2", or "140-3"
1092     level SecurityLevel,
1093     plus BOOLEAN DEFAULT FALSE }

1094
1095 SecurityLevel ::= ENUMERATED {
1096     level1 (1),
1097     level2 (2),
1098     level3 (3),
1099     level4 (4) }

1100
1101
1102 -- platform configuration
1103 platformConfiguration ATTRIBUTE ::= {
1104     WITH SYNTAX PlatformConfiguration
1105     ID tcg-at-platformConfiguration-v2
1106 }
1107
1108 PlatformConfiguration ::= SEQUENCE {
1109     componentIdentifiers [0] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF ComponentIdentifier OPTIONAL,
1110     componentIdentifiersUri [1] IMPLICIT URIReference OPTIONAL,
1111     platformProperties [2] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF Properties OPTIONAL,
1112     platformPropertiesUri [3] IMPLICIT URIReference OPTIONAL
1113 }
1114
1115 ComponentIdentifier ::= SEQUENCE {
1116     componentClass ComponentClass,
1117     componentManufacturer UTF8String (SIZE (1..STRMAX)),
1118     componentModel UTF8String (SIZE (1..STRMAX)),
1119     componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
1120     componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
1121     componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,
1122     fieldReplaceable [3] IMPLICIT BOOLEAN OPTIONAL,
1123     componentAddresses [4] IMPLICIT SEQUENCE(SIZE(1.. MAX)) OF ComponentAddress OPTIONAL
1124     componentPlatformCert [5] IMPLICIT CertificateIdentifier OPTIONAL,
1125     componentPlatformCertUri [6] IMPLICIT URIReference OPTIONAL,
1126     status [7] IMPLICIT AttributeStatus OPTIONAL }

1127
1128 ComponentClass ::= SEQUENCE {
1129     componentClassRegistry ComponentClassRegistry,
1130     componentClassValue OCTET STRING SIZE(4) }

1131
1132 ComponentClassRegistry ::= OBJECT IDENTIFIER ( tcg-registry-componentClass-tcg | tcg-registry-
1133 componentClass-ietf | tcg-registry-componentClass-dmtf )
1134
1135 ComponentAddress ::= SEQUENCE {
1136     addressType AddressType,
1137     addressValue UTF8String (SIZE (1..STRMAX)) }

1138
1139 AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
1140 bluetoothmac)
1141
1142 Properties ::= SEQUENCE {
1143     propertyName UTF8String (SIZE (1..STRMAX)),
1144     propertyValue UTF8String (SIZE (1..STRMAX)),
1145     status [0] IMPLICIT AttributeStatus OPTIONAL }

1146
1147 CertificateIdentifier ::= SEQUENCE {
1148     attributeCertIdentifier [0] IMPLICIT AttributeCertificateIdentifier OPTIONAL,
1149     genericCertIdentifier [1] IMPLICIT IssuerSerial OPTIONAL }

1150
1151 AttributeCertificateIdentifier ::= SEQUENCE {
1152     hashAlgorithm AlgorithmIdentifier,
1153     hashOverSignatureValue OCTET STRING
1154 }
1155
1156 AttributeStatus ::= ENUMERATED {
1157     added (0),

```

```
1158     modified (1),
1159     removed (2) }
1160
1161 -- platform configuration Uri attribute
1162 PlatformConfigUri ATTRIBUTE ::= {
1163   WITH SYNTAX URIReference
1164   ID tcg-at-platformConfigUri  }
1165
1166
1167
1168
1169
1170
```

5. References

- 1171 [1] TCG Glossary, <https://trustedcomputinggroup.org/glossary>
- 1172 [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/>
- 1173 [3] TCPA Main Specification, Version 1.1b, <http://www.trustedcomputinggroup.org/tcpa-main-specification-version-1-1b/>
- 1174 [4] Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, www.ietf.org/rfc/rfc2119.txt
- 1175 [5] Hypertext Markup Language – 2.0, RFC 1866, www.ietf.org/rfc/rfc1866.txt
- 1176 [6] TCG Credential Profiles For TPM Family 1.2 Specification Version 1.2, <http://www.trustedcomputinggroup.org/infrastructure-work-group-tcg-credential-profiles-specification/>
- 1177 [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/>
- 1178 [8] IANA Private Enterprise Numbers, <http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>
- 1179 [9] Server Work Group Generic Server Specification, Version 1.0, <http://www.trustedcomputinggroup.org/server-work-group-generic-server-specification-version-1-0/>
- 1180 [10] PC Client Platform TPM Profile (PTP) Specification , <http://www.trustedcomputinggroup.org/pc-client-platform-tpm-profile-ptp-specification/>
- 1181 [11] An Internet Attribute Certificate Profile for Authorization, www.ietf.org/rfc/rfc5755.txt
- 1182 [12] TCG Algorithm Registry, <http://www.trustedcomputinggroup.org/tcg-algorithm-registry/>
- 1183 [13] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, <https://www.ietf.org/rfc/rfc5280.txt>
- 1184 [14] TCG Platform Attribute Credential Profile Version 1.0, <https://trustedcomputinggroup.org/tcg-platform-attribute-credential-profile/>
- 1185 [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>
- 1186 [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>
- 1187 [17] SHA-3 Related Algorithms and Identifiers for PKIX, <https://tools.ietf.org/html/draft-turner-lamps-adding-sha3-to-pkix-00>
- 1188 [18] GB/T 33560-2017. Information security technology—Cryptographic application identifier criterion specification. <http://www.spc.org.cn/gb168/online/GB%252FT%252033560-2017/>

- 1213 [19] A YANG Data Model for Hardware Management. <https://tools.ietf.org/html/rfc8348>
1214 [20] ITU-T X.520 Information Technology – Open Systems Interconnection – The
1215 Directory: Selected Attributed Types. <https://www.itu.int/rec/T-REC-X.520-201610-I>
1216 [21] TCG PC Client Platform TPM Profile (PTP) Specification.
1217 https://trustedcomputinggroup.org/wp-content/uploads/TCG_Protocol_Specification_TPM_Profile_PTP_2.0_r1.03_v22.pdf
1218 [22] TCG Registry of Reserved TPM 2.0 Handles and Localities.
1219 <https://trustedcomputinggroup.org/resource/registry/>
1220
1221
1222

1223 A. Certificate Examples

1224 A.1 Example 1 (Platform Certificate in Attribute Certificate Format)

1225 The following section provides an example of a Platform Certificate in Attribute Certificate
1226 format (RFC 5755) [11]. The PEM encoded version of the certificate as well as the ASN.1
1227 certificate text are included for convenience. The values used in this example are for
1228 illustrative purposes and must be replaced with manufacturer-specific data.

1229 A.1.1 PEM Format

```
1230 -----BEGIN ATTRIBUTE CERTIFICATE-----  
1231 MIIJmDCCCIACAQEWgZaggZMwgYqkgYcwgYQxCzAJBgNVBAYTA1VTMQswCQYDVQQI  
1232 DAJDQTEUMBIGA1UEBwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVsIENvcnBv  
1233 cmF0aW9uMR4wHAYDVQQLDVBVFSyBDZXJ0aWZpY2F0ZSBjc3N1ZXIxFjAUBgNVBAMM  
1234 DXd3dy5pbnR1bC5jb20CBDdAg3SggZ0wgZqkgZcwgZQxCzAJBgNVBAYTA1VTMQsw  
1235 CQYDVQQIDAJDQTEUMBIGA1UEBwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVs  
1236 IENvcnBvcmF0aW9uMS4wLAYDVQQLDVCQbGF0Zm9ybSBBdHRyaWJ1dGUgQ2VydGlm  
1237 aWNhdGUgSXNzdWVYmRYwFAYDVQQDDA13d3cuaW50ZWwuY29tMA0GCSqGSIb3DQE  
1238 CwUAhRgKWFqeST97mzBULkeg3d9H0J5mTAiGA8yMDE3MDgyMDIxMDc0OFoYDzIw  
1239 MjAwODIwMjEwNzQ4WjCCBK4wHAYFZ4EFAhExEZARMAkCAQICAQACASsEBAAAAAEw  
1240 EgYFZ4EFAhkxCTAHbgVngQUIAjAUBgVngQUCFzELMAkCAQECQAQswgccGBWeB  
1241 BQITMYG9MIG6AgEAoHQWazMuMQuBBwoBAGEBAlABAYEFKgMEBQaiLRYraHR0cHM6  
1242 Ly93d3cuaW50ZWwuY29tL3Byb3R1Y3Rp25wcm9maWx1LnBkZoMFUwQFBgekJBYi  
1243 aHR0cHM6Ly93d3cuaW50ZWwuY29tL2NjdGFyZ2V0LnBkZqENFgUxNDAtMgoBBAEB  
1244 AIIBAwEBABYqaHR0cHM6Ly93d3cuaW50ZWwuY29tL2lzb2N1cnRpZmljYXRpb24u  
1245 cGRmMIIdagYHZ4EFBQEHAjGCA10wggNZoIIC1zCCAXYwDgYGZ4EFegMBBAQAAA  
1246 DAdBQkMgT0VNDAxXUjA2WDc4NzFGVEyACUE1NTU1LTk5OYEDMS4xggcrBge  
1247 gwh/pDIwFwYFZ4EFEQEMDkFGOjNBojk0OjEwOkE1MBcGBWeBBRECDAs5BRj0zNzox  
1248 MDpEMjpBOKWBz6AxMA0GCysGAQQBgbAaAQIBBCBga6M0Mv2RS2ADozQy/ZFIYAOj  
1249 NDL9kUtgA6M0Mv2RS6GBmTCBj6SBjDCBiTELMAkGA1UEBhMCVVMxCzAJBgNVB  
1250 AgM AkZMMRcwFQYDVQQHDA5GdC4gTGF1ZGVyZGFsZTEYMBYGA1UECgwPQUJDIE  
1251 NvcnBv cmF0aW9uMSQwIgYDVQQLDtQbGF0Zm9ybSBDZXJ0aWZpY2F0ZSBjc3N1ZXIx  
1252 FDAS BgNVBAMM3d3dy5hYmMuY29tAgUKNUzN26YrFilodHRwczovL3d3dy5hYmMuY29t  
1253 L2N1cnRzLzQzODQzODk40DQzLmN1cjCCAVkwDgYGZ4EFegMBBAQAAA  
1254 AvDAdYVWog T0VNDA5MTUJUMzkwNERXMVQxR4AJQzU1NTU1gQMzLjGCBysGAQQB  
1255 giyDAQCK MjAXBgVngQURAQwO0DI6ODk6RkE6RDM6NjEwFwYFZ4EFEQIMDkQ00jgz  
1256 OkI00kYy Ojc4pYG1oCUwDQYLKwYBBAGBsBoBAGEEFDQy4UFLYJc0NDI0MuFBS2CX  
1257 NDQyoYGL MIGDpIGAMH4xCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJBWjEQMA4GA1UE  
1258 BwwHUGHv ZW5peDEUMBIGA1UECgwLWF1DIENvbXBhbnkxJDAiB  
1259 gNVBAsMG1BsYXRmb3JtIEN1 cnRpZmljYXR1IElzc3VlcjeUMBIGA1UEA  
1260 AwLd3d3Lnh5ei5jb20CAw5TsKYmFiRo dHRwczovL3d3dy54eXouY29tL2N1cnRzL  
1261 kzODkyOC5jZXKhLxYtaHR0cHM6Ly93
```

```

1262 d3cuaW50ZWwuY29tL3BsYXRmb3JtaWRlbnRpZmllcnMueG1sohswDAwEd1BybwwE
1263 dHJ1ZTALDANBTVQMBHRydWWjLhYsaHR0cHM6Ly93d3cuaW50ZWwuY29tL3BsYXRm
1264 b3JtcHJvcGVydG1lc54bWwwLAYGZ4EFBQEDMSIwIBYeaHR0cHM6Ly93d3cuaW50
1265 ZWwuY29tL1BDUnMueG1sMIICRTB8BgNVHSAEdTBzMHEGCiqGSIB4TQEFAgQwYzAx
1266 BggrBgEFBQcCARYlaHR0cHM6Ly93d3cuaW50ZWwuY29tL3BsYXRjZXJ0Y3BzLnBk
1267 ZjAuBggxBgEFBQcCAjAiDCBUQ0cgVHJ1c3R1ZCBQbGF0Zm9ybSBFbmRvcnNlbWVu
1268 dDB+BgNVHREEdzB1pHMwCTERMA8GBmeBBQUBAQwFSW50ZWwxFTATBgZngQUFAQIw
1269 CQYHKwYBBAGCVzETMBEGBmeBBQUBBAwHUzI2MDBLUDEWMQBGBmeBBQUBBQwKSDc2
1270 OTYyLTM1MDEYMBYGBmeBBQUBBQwMq1FLUDk5OTQwNjQzMIGyBgnVHTcBAf8Egacw
1271 gaQwgaGggZ6kgZswgZgxCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJDQTEUMBIGA1UE
1272 BwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVsIENvcnBvcmF0aW9uMR4wHAYD
1273 VQQLDBVFSyBDZXJ0aWZpY2F0ZSBjC3N1ZXIxFjAUBgNVBAMMDXd3dy5pbnR1bC5j
1274 b20xEjAQBgNVBAUTCTEyODk0Mzc4NzAfBgNVHSMEGDAwgbTUaZAmAoHVXoNLA5du
1275 q4qfj4TJgzA2BggxBgEFBQcBAQQqMCgwJgYIKwYBBQUHMGGGmh0dBzOi8vd3d3
1276 LmludGVsLmNvbS9vY3NwMDcGA1UdHwQwMC4wLKAqoCiGJmh0dBzOi8vd3d3Lmlu
1277 dGVsLmNvbS9wbGF0Zm9ybWNlcnQuY3JsMA0GCSqGSIB3DQEBCwUAA4IBAQCq6w/S
1278 /cuB8mUjI1V1i2JPfkbs+v2TmBf0sIUPdPfU/aH16NPctavfiEvpP11uWGty7/oY
1279 8sAq5ChEU3/KbI0zaY7X0Yjpcp5YfYqZZFqgrDmye+o5T5+sAnJOjNrHdIEUGyYH
1280 G47Isogmjj7i11RcF7JVCJTUOGQpWqVMKF3/VffWJ84XKE+nbTYCYufyYHRxUQ1T
1281 rSx5sQn0dAnW8Bdljc+zpaNJBxDxlCdhKefZSwf3Yc550d3QDqMekH/3++9MJhJO
1282 79BiL0CkXi5gAYLi5NU14X9S/Jv+hcaDWi/gEtB5s7c3rtEyoYByj//QycQhxMIb
1283 L2ciOd1FDte7CSyC
1284 -----END ATTRIBUTE CERTIFICATE-----
1285

```

1286 A.1.2 DER Format

1287

```

1288 SEQUENCE :
1289   SEQUENCE :
1290     INTEGER : 1
1291   SEQUENCE :
1292     CONTEXT SPECIFIC (0) :
1293       SEQUENCE :
1294         CONTEXT SPECIFIC (4) :
1295           SEQUENCE :
1296             SET :
1297               SEQUENCE :
1298                 OBJECT IDENTIFIER : countryName [2.5.4.6]
1299                 PRINTABLE STRING : 'US'
1300             SET :
1301               SEQUENCE :
1302                 OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
1303                 UTF8 STRING : 'CA'
1304             SET :
1305               SEQUENCE :
1306                 OBJECT IDENTIFIER : localityName [2.5.4.7]
1307                 UTF8 STRING : 'Santa Clara'
1308             SET :

```

```
1309          SEQUENCE :  
1310              OBJECT IDENTIFIER : organizationName [2.5.4.10]  
1311                  UTF8 STRING : 'Intel Corporation'  
1312          SET :  
1313              SEQUENCE :  
1314                  OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]  
1315                      UTF8 STRING : 'EK Certificate Issuer'  
1316          SET :  
1317              SEQUENCE :  
1318                  OBJECT IDENTIFIER : commonName [2.5.4.3]  
1319                      UTF8 STRING : 'www.intel.com'  
1320          INTEGER : 926974836  
1321      CONTEXT SPECIFIC (0) :  
1322          SEQUENCE :  
1323              CONTEXT SPECIFIC (4) :  
1324                  SEQUENCE :  
1325                      SET :  
1326                          SEQUENCE :  
1327                              OBJECT IDENTIFIER : countryName [2.5.4.6]  
1328                              PRINTABLE STRING : 'US'  
1329          SET :  
1330              SEQUENCE :  
1331                  OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]  
1332                      UTF8 STRING : 'CA'  
1333          SET :  
1334              SEQUENCE :  
1335                  OBJECT IDENTIFIER : localityName [2.5.4.7]  
1336                      UTF8 STRING : 'Santa Clara'  
1337          SET :  
1338              SEQUENCE :  
1339                  OBJECT IDENTIFIER : organizationName [2.5.4.10]  
1340                      UTF8 STRING : 'Intel Corporation'  
1341          SET :  
1342              SEQUENCE :  
1343                  OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]  
1344                      UTF8 STRING : 'Platform Attribute Certificate Issuer'  
1345          SET :  
1346              SEQUENCE :  
1347                  OBJECT IDENTIFIER : commonName [2.5.4.3]  
1348                      UTF8 STRING : 'www.intel.com'  
1349      SEQUENCE :  
1350          OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]  
1351          NULL :  
1352      INTEGER : 602967EA7924FDEE6CC150B91E83777D1F427999  
1353      SEQUENCE :  
1354          GENERALIZED TIME : '20170820210748Z'  
1355          GENERALIZED TIME : '20200820210748Z'  
1356      SEQUENCE :  
1357          SEQUENCE :  
1358              OBJECT IDENTIFIER : [2.23.133.2.17]  
1359              SET :  
1360                  SEQUENCE :  
1361                      SEQUENCE :  
1362                          INTEGER : 2  
1363                          INTEGER : 0  
1364                          INTEGER : 43  
1365                          OCTET STRING : 00000001  
1366      SEQUENCE :  
1367          OBJECT IDENTIFIER : [2.23.133.2.25]  
1368          SET :  
1369              SEQUENCE :  
1370                  OBJECT IDENTIFIER : [2.23.133.8.2]  
1371      SEQUENCE :
```

```
1372 OBJECT IDENTIFIER : [2.23.133.2.23]
1373 SET :
1374     SEQUENCE :
1375         INTEGER : 1
1376         INTEGER : 1
1377         INTEGER : 11
1378 SEQUENCE :
1379     OBJECT IDENTIFIER : [2.23.133.2.19]
1380     SET :
1381         SEQUENCE :
1382             INTEGER : 0
1383             CONTEXT SPECIFIC (0) :
1384                 IA5 STRING : '3.1'
1385                 ENUMERATED : '07'
1386                 ENUMERATED : '02'
1387                 BOOLEAN : '00'
1388                 CONTEXT SPECIFIC (0) : 01
1389                 CONTEXT SPECIFIC (1) : 2A03040506
1390                 CONTEXT SPECIFIC (2) :
1391                     IA5 STRING : 'https://www.intel.com/protectionprofile.pdf'
1392                     CONTEXT SPECIFIC (3) : 5304050607
1393                     CONTEXT SPECIFIC (4) :
1394                         IA5 STRING : 'https://www.intel.com/cctarget.pdf'
1395                     CONTEXT SPECIFIC (1) :
1396                         IA5 STRING : '140-2'
1397                         ENUMERATED : '04'
1398                         BOOLEAN : '00'
1399                         CONTEXT SPECIFIC (2) : 03
1400                         BOOLEAN : '00'
1401                         IA5 STRING : 'https://www.intel.com/isocertification.pdf'
1402 SEQUENCE :
1403     OBJECT IDENTIFIER : [2.23.133.5.1.7.2]
1404     SET :
1405         SEQUENCE :
1406             CONTEXT SPECIFIC (0) :
1407                 SEQUENCE :
1408                     SEQUENCE :
1409                         OBJECT IDENTIFIER : [2.23.133.18.3.1]
1410                         OCTET STRING : 0000000A
1411                         UTF8 STRING : 'ABC OEM'
1412                         UTF8 STRING : 'WR06X7871FTL'
1413                         CONTEXT SPECIFIC (0) : 41353535352D393939
1414                         CONTEXT SPECIFIC (1) : 312E31
1415                         CONTEXT SPECIFIC (2) : 2B06010401822C
1416                         CONTEXT SPECIFIC (3) : FF
1417                         CONTEXT SPECIFIC (4) :
1418                             SEQUENCE :
1419                                 OBJECT IDENTIFIER : [2.23.133.17.1]
1420                                 UTF8 STRING : 'AF:3A:94:10:A5'
1421 SEQUENCE :
1422     OBJECT IDENTIFIER : [2.23.133.17.2]
1423     UTF8 STRING : 'AF:37:10:D2:A8'
1424     CONTEXT SPECIFIC (5) :
1425         CONTEXT SPECIFIC (0) :
1426             SEQUENCE :
1427                 OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
1428                 OCTET STRING :
1429                 6003A33432FD914B6003A33432FD914B6003A33432FD914B
1430                 CONTEXT SPECIFIC (1) :
1431                     SEQUENCE :
1432                         CONTEXT SPECIFIC (4) :
1433                         SEQUENCE :
1434                             SET :
```

```

1435           SEQUENCE :
1436             OBJECT IDENTIFIER : countryName [2.5.4.6]
1437               PRINTABLE STRING : 'US'
1438           SET :
1439             SEQUENCE :
1440               OBJECT IDENTIFIER : stateOrProvinceName
1441           [2.5.4.8]           UTF8 STRING : 'FL'
1442           SET :
1443             SEQUENCE :
1444               OBJECT IDENTIFIER : localityName [2.5.4.7]
1445                 UTF8 STRING : 'Ft. Lauderdale'
1446           SET :
1447             SEQUENCE :
1448               OBJECT IDENTIFIER : organizationName
1449           [2.5.4.10]           UTF8 STRING : 'ABC Corporation'
1450           SET :
1451             SEQUENCE :
1452               OBJECT IDENTIFIER : organizationalUnitName
1453           [2.5.4.11]           UTF8 STRING : 'Platform Certificate Issuer'
1454           SET :
1455             SEQUENCE :
1456               OBJECT IDENTIFIER : commonName [2.5.4.3]
1457                 UTF8 STRING : 'www.abc.com'
1458                 INTEGER : 43843898843
1459           CONTEXT SPECIFIC (6) :
1460             IA5 STRING : 'https://www.abc.com/certs/43843898843.cer'
1461           SEQUENCE :
1462             SEQUENCE :
1463               OBJECT IDENTIFIER : [2.23.133.18.3.1]
1464                 OCTET STRING : 0000002F
1465                 UTF8 STRING : 'XYZ OEM'
1466                 UTF8 STRING : 'LMBT3904DW1T1G'
1467           CONTEXT SPECIFIC (0) : 43353535352D353535
1468           CONTEXT SPECIFIC (1) : 332E31
1469           CONTEXT SPECIFIC (2) : 2B06010401822C
1470           CONTEXT SPECIFIC (3) : 00
1471           CONTEXT SPECIFIC (4) :
1472             SEQUENCE :
1473               OBJECT IDENTIFIER : [2.23.133.17.1]
1474                 UTF8 STRING : '82:89:FA:D3:61'
1475             SEQUENCE :
1476               OBJECT IDENTIFIER : [2.23.133.17.2]
1477                 UTF8 STRING : 'D4:83:B4:F2:78'
1478           CONTEXT SPECIFIC (5) :
1479             CONTEXT SPECIFIC (0) :
1480               SEQUENCE :
1481                 OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
1482                   OCTET STRING : 3432E1414B60973434323432E1414B6097343432
1483             CONTEXT SPECIFIC (1) :
1484               SEQUENCE :
1485                 CONTEXT SPECIFIC (4) :
1486                   SEQUENCE :
1487                     SET :
1488                       SEQUENCE :
1489                         OBJECT IDENTIFIER : countryName [2.5.4.6]
1490                           PRINTABLE STRING : 'US'
1491                         SET :
1492                           SEQUENCE :
1493                             OBJECT IDENTIFIER : stateOrProvinceName
1494           [2.5.4.8]
1495
1496
1497

```

```
1498          UTF8 STRING : 'AZ'
1499
1500
1501      SET :
1502          SEQUENCE :
1503              OBJECT IDENTIFIER : localityName [2.5.4.7]
1504                  UTF8 STRING : 'Phoenix'
1505
1506      SET :
1507          SEQUENCE :
1508              OBJECT IDENTIFIER : organizationName
1509
1510      [2.5.4.10]          UTF8 STRING : 'XYC Company'
1511
1512      SET :
1513          SEQUENCE :
1514              OBJECT IDENTIFIER : organizationalUnitName
1515
1516      [2.5.4.11]          UTF8 STRING : 'Platform Certificate Issuer'
1517
1518      SET :
1519          CONTEXT SPECIFIC (6) :
1520              IA5 STRING : 'https://www.xyz.com/certs/938928.cer'
1521
1522      CONTEXT SPECIFIC (1) :
1523          IA5 STRING : 'https://www.intel.com/platformidentifiers.xml'
1524
1525      CONTEXT SPECIFIC (2) :
1526          SEQUENCE :
1527              UTF8 STRING : 'vPro'
1528              UTF8 STRING : 'true'
1529
1530      CONTEXT SPECIFIC (3) :
1531          IA5 STRING : 'https://www.intel.com/platformproperties.xml'
1532
1533      SEQUENCE :
1534          OBJECT IDENTIFIER : [2.23.133.5.1.3]
1535
1536      SET :
1537          SEQUENCE :
1538              IA5 STRING : 'https://www.intel.com/PCRs.xml'
1539
1540      SEQUENCE :
1541          SEQUENCE :
1542              OBJECT IDENTIFIER : certificatePolicies [2.5.29.32]
1543
1544      OCTET STRING :
1545
1546      SEQUENCE :
1547          SEQUENCE :
1548              OBJECT IDENTIFIER : [1.2.840.113741.1.5.2.4]
1549
1550      SEQUENCE :
1551          SEQUENCE :
1552              OBJECT IDENTIFIER : cps [1.3.6.1.5.5.7.2.1]
1553              IA5 STRING : 'https://www.intel.com/platcertcps.pdf'
1554
1555      SEQUENCE :
1556          SEQUENCE :
1557              OBJECT IDENTIFIER : unotice [1.3.6.1.5.5.7.2.2]
1558
1559      SEQUENCE :
1560          UTF8 STRING : 'TCG Trusted Platform Endorsement'
```

```

1561      SET :
1562          SEQUENCE :
1563              OBJECT IDENTIFIER : [2.23.133.5.1.2]
1564              SEQUENCE : OBJECT IDENTIFIER : [1.3.6.1.4.1.343]
1565      SET :
1566          SEQUENCE :
1567              OBJECT IDENTIFIER : [2.23.133.5.1.4]
1568              UTF8 STRING : 'S2600KP'
1569      SET :
1570          SEQUENCE :
1571              OBJECT IDENTIFIER : [2.23.133.5.1.5]
1572              UTF8 STRING : 'H76962-350'
1573      SET :
1574          SEQUENCE :
1575              OBJECT IDENTIFIER : [2.23.133.5.1.6]
1576              UTF8 STRING : 'BQKP99940643'
1577      SEQUENCE :
1578          OBJECT IDENTIFIER : [2.5.29.55]
1579          BOOLEAN : 'FF'
1580          OCTET STRING :
1581              SEQUENCE :
1582                  SEQUENCE :
1583                      CONTEXT SPECIFIC (0) :
1584                          CONTEXT SPECIFIC (4) :
1585                              SEQUENCE :
1586                                  SET :
1587                                      SEQUENCE :
1588                                          OBJECT IDENTIFIER : countryName [2.5.4.6]
1589                                          PRINTABLE STRING : 'US'
1590      SET :
1591          SEQUENCE :
1592              OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
1593              UTF8 STRING : 'CA'
1594      SET :
1595          SEQUENCE :
1596              OBJECT IDENTIFIER : localityName [2.5.4.7]
1597              UTF8 STRING : 'Santa Clara'
1598      SET :
1599          SEQUENCE :
1600              OBJECT IDENTIFIER : organizationName [2.5.4.10]
1601              UTF8 STRING : 'Intel Corporation'
1602      SET :
1603          SEQUENCE :
1604              OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
1605              UTF8 STRING : 'EK Certificate Issuer'
1606      SET :
1607          SEQUENCE :
1608              OBJECT IDENTIFIER : commonName [2.5.4.3]
1609              UTF8 STRING : 'www.intel.com'
1610      SET :
1611          SEQUENCE :
1612              OBJECT IDENTIFIER : serialNumber [2.5.4.5]
1613              PRINTABLE STRING : '128943787'
1614      SEQUENCE :
1615          OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
1616          OCTET STRING :
1617              SEQUENCE :
1618                  CONTEXT SPECIFIC (0) : D46990260281D55E834B03976EAB8A9F8F84C983
1619      SEQUENCE :
1620          OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
1621          OCTET STRING :
1622              SEQUENCE :
1623                  SEQUENCE :

```

```

1624          OBJECT IDENTIFIER : ocsp [1.3.6.1.5.5.7.48.1]
1625          CONTEXT SPECIFIC (6) : 'https://www.intel.com/ocsp'
1626      SEQUENCE :
1627          OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
1628          OCTET STRING :
1629              SEQUENCE :
1630                  SEQUENCE :
1631                      CONTEXT SPECIFIC (0) :
1632                          CONTEXT SPECIFIC (0) :
1633                              CONTEXT SPECIFIC (6) : 'https://www.intel.com/platformcert.crl'
1634      SEQUENCE :
1635          OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]
1636          NULL :
1637      BIT STRING UnusedBits:0 :
1638          AAEB0FD2FDDB81F265232255658B624F7E46D2FAFD939817F4B085
1639          0F74F7D4FDA1F5E8D3DCB5ABDF884BE93E5D6E586B72EFA18F2C0
1640          2AE42844537FCA6C8D33698ED7D188E9729E587D8A99645AA0AC39
1641          B27BEA394F9FAC02724E8CDAC77481141B26071B8EC8B28826263E
1642          E2D6545C17B2550894D43864295AA54C285DFF55F7D627CE17284F
1643          A76D360262E7F2607471510D53AD2C79B109F47409D6F017658DCF
1644          B3A5A349043C5D94276129E7D94B07F761CE79D1DDD00EA31E907F
1645          F7FBFEC4C26124EEFD0622F40A45E2E600182E2E4D525E17F52FC9B
1646          FE85C6835A2FE012D079B3B737AED132A180728FFD0C9C421C4C2
1647          1B2F672239DD450ED7BB092C82
1648
1649

```

1650 **A.2 Example 2 (Delta Platform Certificate in Attribute Certificate 1651 Format)**

1652 The following section provides an example of a Delta Platform Certificate in Attribute
1653 Certificate format (RFC 5755) [11]. The PEM encoded version of the certificate as well as the
1654 ASN.1 certificate text are included for convenience. The values used in this example are for
1655 illustrative purposes and must be replaced with manufacturer-specific data.

1656 **A.2.1 PEM Format**

```

1657 -----BEGIN ATTRIBUTE CERTIFICATE-----
1658 MIIKkzCCCXsCAQEwgbaggbMwgZqkgZcwgZQxCzAJBgNVBAYTA1VTMQswCQYDVQQI
1659 DAJDQTEUMBIGA1UEBwwLU2FudGEgQ2xhcmExGjAYBgNVBAoMEUludGVsIENvcnBv
1660 cmF0aW9uMS4wLAYDVQQLDCVQbGF0Zm9ybSBBdHRyaWJ1dGUgQ2VydGlmaWNhdGUg
1661 SXNzdWVyMRYwFAYDVQQDDA13d3cuaW50ZWwuY29tAhRgKWFqeST97mzBULkeg3d9
1662 H0J5maCBpDCBoaSBnjCBmzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMA1RYMQ8wDQYD
1663 VQQHDAZBdXN0aW4xFzAVBgvNVBAoMDlhZWiBJbnRlZ3JhdG9yMTQwMgYDVQQLDctE
1664 ZWx0YSBQbGF0Zm9ybSBBdHRyaWJ1dGUgQ2VydGlmaWNhdGUgSXNzdWVyMR8wHQYD
1665 VQQDBBZ3d3cueH16aW50ZWdyYXRvcnMuY29tMA0GCSqGSIb3DQEBCwUAAgQCFPcE
1666 MCIYDzIwMTgxMDE1MjEwODExWhgPMjAyMDA4MjAyMTA4MTFaMIIFeDASBgVngQUC
1667 GTEJMacGBWeBBQgFMBQGBWeBBQIXMQswCQIBAQIBAQIBDTCCBRAGB2eBBQUBBwIx
1668 ggUDMIIE/6CCBF0wggF5MA4GBmeBFRIDAQQEAAAACgwHQUJDIE9FTQwMV1IwNlg3
1669 ODCxR1RMgA1BNUTU1NS050TmBAzEuMYIHkwYBAGCLIMB/6QyMBcGBWeBBREBDA5B
1670 RjozQTo5NDoxMDpBNTAXBgvngQURAgwOQUY6Mzc6MTA6RDI6QTilgc+gMTANBgsr
1671 BgEEAYGwGgECAQQgYAOjNDL9kUtgA6M0Mv2RS2ADozQy/ZFLYAOjNDL9kUuhgZkw
1672

```

1673 gY+kgYwwgYkxCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJGTDEXMBUGA1UEBwwORnQu
1674 IEhdWRlcmRhbGUxGDAwBgNVBAoMD0FCQyBDB3Jwb3JhdGlvbjEkMCIGA1UECwwb
1675 UGxhdGZvcm0gQ2VydGlmaWNhdGUGSXNzdWVyMRQwEgYDVQQDDAt3d3cuYWJjLmNv
1676 bQIFCjVMzdumKxYpaHR0cHM6Ly93d3cuYWJjLmNvbS9jZXJ0cy80Mzg0Mzg5ODg0
1677 My5jZXKHAQIwgxF8MA4GBmeBFRIDAQQEAAAQQwOQ29tcG9uZW50IEvncnAMCVhU
1678 OTgyODdMTIAHRjk4MS0wMYEDMi4xggcrBgEEAYNIgwH/pDIwFwYFZ4EFEQIMDjcz
1679 Oj1CojkyOjQwOkZBMBcGBWeBBREDDA4xMzozRjo5ODpDNT01oAWBzaAxMA0GCysG
1680 AQQBgbaAQIBCCYqtWRg/qrkZiq1ZGD+quRmKrVkp6q5GYqtWRg/qrkaGB1zCB
1681 jqSBizCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMRewDwYDVQQHDAhTYW4g
1682 Sm9zZTEXMBUGA1UECgwOQ29tcG9uZW50IEvncnAxJDAiBgNVBAsMG1BsYXRmb3Jt
1683 IENlcnPzmljYXR1IE1zc3V1cjEaMBgGA1UEAwRD3d3LmNvbXBvbmVudC5jb20C
1684 BAXek66mLhYsaHR0cHM6Ly93d3cuY29tcG9uZW50LmNvbS9jZXJ0cy85ODQ3Mjg3
1685 OC5jZXKHAQAwggFcMA4GBmeBFRIDAQQEAAAALwwHWFlaIE9FTQwOTE1CVDM5MDRE
1686 VzFUMUeACUM1NTU1LTU1NYEDNC4wggcrBgEEAYIsgrwEApDIwFwYFZ4EFEQEMDjgy
1687 Ojg50kZBokQzOjYxMbcGBWeBBRECDAs5ENDo4MzpCNDpGMjo3OKWBtaAlMA0GCysG
1688 AQQBgbaAQIBBBQ0MuFBS2CXNDQyNDLhQUtg1zQ0MqGBizCBg6SBgDB+MQswCQYD
1689 VQQGEwJVUzELMAkGA1UECAwCQVoxEDAObgNVBAcMB1Bob2VuaxgxFDASBgNVBAoM
1690 C1hZQyBDb21wYW55MSQwIgYDVQQLDbtQbGF0Zm9ybSBDZXJ0aWZpY2F0ZSBJc3N1
1691 ZXIxFDASBgNVBAMMC3d3dy54eXouY29tAgMOU7CmJhYkaHR0cHM6Ly93d3cueH16
1692 LmNvbS9jZXJ0cy85Mzg5MjguY2VyhEB0TgWNmh0dHBz0i8vd3d3Lnh5emludGVn
1693 cmF0b3JzLmNvbS9wbGF0Zm9ybW1kZW50aWZpZXJzLnhtbKIpMBYMC1RTQyBFbmFi
1694 bGVkdAR0cnVlgAEAMA8MA0FNVAwFZmFsc2WAAQGjNxY1aHR0cHM6Ly93d3cueH16
1695 aW50ZWdyYXRvcnMuY29tL3BsYXRmb3JtchJvcGVydG11cy54bWwwOAYGZ4EFBQED
1696 MS4wLBYqaHR0cHM6Ly93d3cueH16aW50ZWdyYXRvcnMuY29tL1BDUnNfVjIueG1s
1697 MIICXzCBgwYDVR0gBHwejB4BggqhkjXjwMBAjBsMD0GCCsGAQUFBwIBFi5odHRw
1698 czovL3d3dy54eXppbnR1Z3JhdG9ycy5jb20vcGxhdGN1cnRjchMucGRmMC4GCCsG
1699 AQUFBwICMCIMIFDRDyBUcnVzdGVkIFBsYXRmb3JtIEVuZG9yc2VtZW50MH4GA1Ud
1700 EQR3MHWkcxBxMREwDwYGZ4EFBQEADAdTMjYwMEtQMRywFAYGZ4EFBQEFDApINzY5NjItMzUw
1701 AYJXMRMwEQYLGZ4EFBQEEDAdTMjYwMEtQMRywFAYGZ4EFBQEFDApINzY5NjItMzUw
1702 MRgwFgYGZ4EFBQEADAxCUtQOTk5NDA2NDMwgbIGA1UdNwEB/wSBpzCBpDCBoaCB
1703 nqSBmzCBmDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMA1RYMQ8wDQYDVQQHDAZBdxN0
1704 aW4xFzAVBgnNVBAoMD1hZW1BjbnR1Z3JhdG9yMR4whAYDVQQLDVFSyBDZXJ0aWZp
1705 Y2F0ZSBJc3N1ZXIxHzAdBgnNVBAMFnd3dy54eXppbnR1Z3JhdG9ycy5jb20xETAP
1706 BgNVBAUTCDMyODczODcyMB8GA1UdIwQYMBaAFNRpkCYCgdVeg0sD126rip+PhMmD
1707 MD8GCCsGAQUFBwEBBDMwMTAvBgggrBgfFBQcwAYYjaHR0cHM6Ly93d3cueH16aW50
1708 ZWdyYXRvcnMuY29tL29jc3AwQAYDVR0fBDkwNzA1oDOgMYYvaHR0cHM6Ly93d3cu
1709 eH16aW50ZWdyYXRvcnMuY29tL3BsYXRmb3JtY2VydC5jcmwwDQYJKoZIhvCNQEL
1710 BQADggEBAGx3K17RCixE32TPB4u52TeoQxla9zROywTOAVDLa0Na4mfqmt3mTYuE
1711 hkCbYnYX9sqa0KCYmBTTjj07LndOO7UisQsx8vKTDDVQ6E3etxeeqdiY8g4Rv+t1
1712 nC8Hna+UZ+Lv+rUze/FaOixH4rn6kxK7jsGe21VIC7qvIzWnjcF5kgxOQ3SqFmWJ

1713 VFXj2FUqauP4WbDQE/H+Fgr8QU5Qq/k6nPZXs1CG3cKZfcSQerF7nW0gCdC1bQ
1714 pmfS+PWz10RWbvx6s9+EI+3Ky0GXQrfq3kmbM6Owmfgr9WMkoHJTiBRx8kK+bObd
1715 7GjNOTGvbrHYTs1WFF5aDB78md+jJ8A=

1716 -----END ATTRIBUTE CERTIFICATE-----

1717 A.2.2 DER Format

1718
1719 SEQUENCE :
1720 SEQUENCE :
1721 INTEGER : 1
1722 SEQUENCE :
1723 CONTEXT SPECIFIC (0) :
1724 SEQUENCE :
1725 CONTEXT SPECIFIC (4) :
1726 SEQUENCE :
1727 SET :
1728 SEQUENCE :
1729 OBJECT IDENTIFIER : countryName [2.5.4.6]
1730 PRINTABLE STRING : 'US'
1731 SET :
1732 SEQUENCE :
1733 OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
1734 UTF8 STRING : 'CA'
1735 SET :
1736 SEQUENCE :
1737 OBJECT IDENTIFIER : localityName [2.5.4.7]
1738 UTF8 STRING : 'Santa Clara'
1739 SET :
1740 SEQUENCE :
1741 OBJECT IDENTIFIER : organizationName [2.5.4.10]
1742 UTF8 STRING : 'Intel Corporation'
1743 SET :
1744 SEQUENCE :
1745 OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
1746 UTF8 STRING : 'Platform Attribute Certificate Issuer'
1747 SET :
1748 SEQUENCE :
1749 OBJECT IDENTIFIER : commonName [2.5.4.3]
1750 UTF8 STRING : 'www.intel.com'
1751 INTEGER : 602967EA7924FDEE6CC150B91E83777D1F427999
1752 CONTEXT SPECIFIC (0) :
1753 SEQUENCE :
1754 CONTEXT SPECIFIC (4) :
1755 SEQUENCE :
1756 SET :
1757 SEQUENCE :
1758 OBJECT IDENTIFIER : countryName [2.5.4.6]
1759 PRINTABLE STRING : 'US'
1760 SET :
1761 SEQUENCE :
1762 OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
1763 UTF8 STRING : 'TX'
1764 SET :
1765 SEQUENCE :
1766 OBJECT IDENTIFIER : localityName [2.5.4.7]
1767 UTF8 STRING : 'Austin'
1768 SET :
1769 SEQUENCE :
1770 OBJECT IDENTIFIER : organizationName [2.5.4.10]
1771 UTF8 STRING : 'XYZ Integrator'

```
1772      SET :  
1773          SEQUENCE :  
1774              OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]  
1775              UTF8 STRING : 'Delta Platform Attribute Certificate Issuer'  
1776      SET :  
1777          SEQUENCE :  
1778              OBJECT IDENTIFIER : commonName [2.5.4.3]  
1779              UTF8 STRING : 'www.xyzintegrators.com'  
1780      SEQUENCE :  
1781          OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]  
1782          NULL :  
1783          INTEGER : 34928388  
1784      SEQUENCE :  
1785          GENERALIZED TIME : '20181015210811Z'  
1786          GENERALIZED TIME : '20200820210811Z'  
1787      SEQUENCE :  
1788          SEQUENCE :  
1789              OBJECT IDENTIFIER : [2.23.133.2.25]  
1790          SET :  
1791              SEQUENCE :  
1792                  OBJECT IDENTIFIER : [2.23.133.8.5]  
1793      SEQUENCE :  
1794          OBJECT IDENTIFIER : [2.23.133.2.23]  
1795          SET :  
1796              SEQUENCE :  
1797                  INTEGER : 1  
1798                  INTEGER : 1  
1799                  INTEGER : 13  
1800      SEQUENCE :  
1801          OBJECT IDENTIFIER : [2.23.133.5.1.7.2]  
1802          SET :  
1803              SEQUENCE :  
1804                  CONTEXT SPECIFIC (0) :  
1805                      SEQUENCE :  
1806                          SEQUENCE :  
1807                              OBJECT IDENTIFIER : [2.23.133.18.3.1]  
1808                              OCTET STRING : 0000000A  
1809                              UTF8 STRING : 'ABC OEM'  
1810                              UTF8 STRING : 'WR06X7871FTL'  
1811                              CONTEXT SPECIFIC (0) : 41353535352D393939  
1812                              CONTEXT SPECIFIC (1) : 312E31  
1813                              CONTEXT SPECIFIC (2) : 2B06010401822C  
1814                              CONTEXT SPECIFIC (3) : FF  
1815                              CONTEXT SPECIFIC (4) :  
1816                                  SEQUENCE :  
1817                                      OBJECT IDENTIFIER : [2.23.133.17.1]  
1818                                      UTF8 STRING : 'AF:3A:94:10:A5'  
1819                                  SEQUENCE :  
1820                                      OBJECT IDENTIFIER : [2.23.133.17.2]  
1821                                      UTF8 STRING : 'AF:37:10:D2:A8'  
1822          CONTEXT SPECIFIC (5) :  
1823              CONTEXT SPECIFIC (0) :  
1824                  SEQUENCE :  
1825                      OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]  
1826                      OCTET STRING :  
1827          6003A33432FD914B6003A33432FD914B6003A33432FD914B :  
1828              CONTEXT SPECIFIC (1) :  
1829                  SEQUENCE :  
1830                      CONTEXT SPECIFIC (4) :  
1831                      SEQUENCE :  
1832                          SET :  
1833                          SEQUENCE :  
1834                              OBJECT IDENTIFIER : countryName [2.5.4.6]
```

1835 PRINTABLE STRING : 'US'
1836 SET :
1837 SEQUENCE :
1838 OBJECT IDENTIFIER : stateOrProvinceName
1839 [2.5.4.8]
1840 UTF8 STRING : 'FL'
1841 SET :
1842 SEQUENCE :
1843 OBJECT IDENTIFIER : localityName [2.5.4.7]
1844 UTF8 STRING : 'Ft. Lauderdale'
1845 SET :
1846 SEQUENCE :
1847 OBJECT IDENTIFIER : organizationName [2.5.4.10]
1848 UTF8 STRING : 'ABC Corporation'
1849 SET :
1850 SEQUENCE :
1851 OBJECT IDENTIFIER : organizationalUnitName
1852 [2.5.4.11]
1853 UTF8 STRING : 'Platform Certificate Issuer'
1854 SET :
1855 SEQUENCE :
1856 OBJECT IDENTIFIER : commonName [2.5.4.3]
1857 UTF8 STRING : 'www.abc.com'
1858 INTEGER : 43843898843
1859 CONTEXT SPECIFIC (6) :
1860 IA5 STRING : 'https://www.abc.com/certs/43843898843.cer'
1861 CONTEXT SPECIFIC (7) : 02
1862 SEQUENCE :
1863 SEQUENCE :
1864 OBJECT IDENTIFIER : [2.23.133.18.3.1]
1865 OCTET STRING : 00000041
1866 UTF8 STRING : 'Component Corp'
1867 UTF8 STRING : 'XT98287LL'
1868 CONTEXT SPECIFIC (0) : 463938312D3031
1869 CONTEXT SPECIFIC (1) : 322E31
1870 CONTEXT SPECIFIC (2) : 2B060104018348
1871 CONTEXT SPECIFIC (3) : FF
1872 CONTEXT SPECIFIC (4) :
1873 SEQUENCE :
1874 OBJECT IDENTIFIER : [2.23.133.17.2]
1875 UTF8 STRING : '73:9B:92:40:FA'
1876 SEQUENCE :
1877 OBJECT IDENTIFIER : [2.23.133.17.3]
1878 UTF8 STRING : '13:3F:98:C5:59'
1879 CONTEXT SPECIFIC (5) :
1880 CONTEXT SPECIFIC (0) :
1881 SEQUENCE :
1882 OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
1883 OCTET STRING :
1884 98AAD59183FAAB9198AAD59183FAAB9198AAD59183FAAB91 :
1885 CONTEXT SPECIFIC (1) :
1886 SEQUENCE :
1887 CONTEXT SPECIFIC (4) :
1888 SEQUENCE :
1889 SET :
1890 SEQUENCE :
1891 OBJECT IDENTIFIER : countryName [2.5.4.6]
1892 PRINTABLE STRING : 'US'
1893 SET :
1894 SEQUENCE :
1895 OBJECT IDENTIFIER : stateOrProvinceName
1896 [2.5.4.8]
1897 UTF8 STRING : 'CA'

```

1898      SET :
1899          SEQUENCE :
1900              OBJECT IDENTIFIER : localityName [2.5.4.7]
1901                  UTF8 STRING : 'San Jose'
1902      SET :
1903          SEQUENCE :
1904              OBJECT IDENTIFIER : organizationName [2.5.4.10]
1905                  UTF8 STRING : 'Component Corp'
1906      SET :
1907          SEQUENCE :
1908              OBJECT IDENTIFIER : organizationalUnitName
1909                  [2.5.4.11]           UTF8 STRING : 'Platform Certificate Issuer'
1910
1911      SET :
1912          SEQUENCE :
1913              OBJECT IDENTIFIER : commonName [2.5.4.3]
1914                  UTF8 STRING : 'www.component.com'
1915                  INTEGER : 98472878
1916      CONTEXT SPECIFIC (6) :
1917          IA5 STRING : 'https://www.component.com/certs/98472878.cer'
1918      CONTEXT SPECIFIC (7) : 00
1919      SEQUENCE :
1920          SEQUENCE :
1921              OBJECT IDENTIFIER : [2.23.133.18.3.1]
1922                  OCTET STRING : 0000002F
1923                  UTF8 STRING : 'XYZ OEM'
1924                  UTF8 STRING : 'LMBT3904DW1T1G'
1925                  CONTEXT SPECIFIC (0) : 43353535352D353535
1926                  CONTEXT SPECIFIC (1) : 342E30
1927                  CONTEXT SPECIFIC (2) : 2B06010401822C
1928                  CONTEXT SPECIFIC (3) : 00
1929                  CONTEXT SPECIFIC (4) :
1930                      SEQUENCE :
1931                          OBJECT IDENTIFIER : [2.23.133.17.1]
1932                          UTF8 STRING : '82:89:FA:D3:61'
1933                      SEQUENCE :
1934                          OBJECT IDENTIFIER : [2.23.133.17.2]
1935                          UTF8 STRING : 'D4:83:B4:F2:78'
1936      CONTEXT SPECIFIC (5) :
1937          CONTEXT SPECIFIC (0) :
1938              SEQUENCE :
1939                  OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
1940                  OCTET STRING : 3432E1414B60973434323432E1414B6097343432
1941      CONTEXT SPECIFIC (1) :
1942          SEQUENCE :
1943              CONTEXT SPECIFIC (4) :
1944                  SEQUENCE :
1945                      SET :
1946                          SEQUENCE :
1947                              OBJECT IDENTIFIER : countryName [2.5.4.6]
1948                              PRINTABLE STRING : 'US'
1949      SET :
1950          SEQUENCE :
1951              OBJECT IDENTIFIER : stateOrProvinceName
1952                  [2.5.4.8]           UTF8 STRING : 'AZ'
1953
1954      SET :
1955          SEQUENCE :
1956              OBJECT IDENTIFIER : localityName [2.5.4.7]
1957                  UTF8 STRING : 'Phoenix'
1958      SET :
1959          SEQUENCE :
1960              OBJECT IDENTIFIER : organizationName [2.5.4.10]

```



```

2024          SEQUENCE :
2025            OBJECT IDENTIFIER : [2.23.133.5.1.4]
2026            UTF8 STRING : 'S2600KP'
2027          SET :
2028            SEQUENCE :
2029              OBJECT IDENTIFIER : [2.23.133.5.1.5]
2030              UTF8 STRING : 'H76962-350'
2031          SET :
2032            SEQUENCE :
2033              OBJECT IDENTIFIER : [2.23.133.5.1.6]
2034              UTF8 STRING : 'BQKP99940643'
2035          SEQUENCE :
2036            OBJECT IDENTIFIER : [2.5.29.55]
2037            BOOLEAN : 'FF'
2038            OCTET STRING :
2039              SEQUENCE :
2040                SEQUENCE :
2041                  CONTEXT SPECIFIC (0) :
2042                    CONTEXT SPECIFIC (4) :
2043                      SEQUENCE :
2044                        SET :
2045                          SEQUENCE :
2046                            OBJECT IDENTIFIER : countryName [2.5.4.6]
2047                            PRINTABLE STRING : 'US'
2048                        SET :
2049                          SEQUENCE :
2050                            OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
2051                            UTF8 STRING : 'TX'
2052                        SET :
2053                          SEQUENCE :
2054                            OBJECT IDENTIFIER : localityName [2.5.4.7]
2055                            UTF8 STRING : 'Austin'
2056                        SET :
2057                          SEQUENCE :
2058                            OBJECT IDENTIFIER : organizationName [2.5.4.10]
2059                            UTF8 STRING : 'XYZ Integrator'
2060                        SET :
2061                          SEQUENCE :
2062                            OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
2063                            UTF8 STRING : 'EK Certificate Issuer'
2064                        SET :
2065                          SEQUENCE :
2066                            OBJECT IDENTIFIER : commonName [2.5.4.3]
2067                            UTF8 STRING : 'www.xyzintegrators.com'
2068                        SET :
2069                          SEQUENCE :
2070                            OBJECT IDENTIFIER : serialNumber [2.5.4.5]
2071                            PRINTABLE STRING : '32873872'
2072          SEQUENCE :
2073            OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
2074            OCTET STRING :
2075              SEQUENCE :
2076                CONTEXT SPECIFIC (0) : D46990260281D55E834B03976EAB8A9F8F84C983
2077          SEQUENCE :
2078            OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
2079            OCTET STRING :
2080              SEQUENCE :
2081                SEQUENCE :
2082                  OBJECT IDENTIFIER : ocsp [1.3.6.1.5.5.7.48.1]
2083                  CONTEXT SPECIFIC (6) : 'https://www.xyzintegrators.com/ocsp'
2084          SEQUENCE :
2085            OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
2086            OCTET STRING :

```

```
2087      SEQUENCE :  
2088          SEQUENCE :  
2089              CONTEXT SPECIFIC (0) :  
2090                  CONTEXT SPECIFIC (0) :  
2091                      CONTEXT           SPECIFIC      (6)  
2092 'https://www.xyzintegrators.com/platformcert.crl'  
2093     SEQUENCE :  
2094         OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]  
2095         NULL :  
2096     BIT STRING UnusedBits:0 :  
2097       6C772B5ED10A2C44DF64CF078BB9D937A843195AF7344ECB04CE01  
2098       50CB6B435AE267EA9ADDE64D8B8486409B627617F6CA9AD0A09898  
2099       14D38E33BB2E774E3BB522B10B31F2F2930C3550E84DDEB7179EA9  
2100       D898F20E11BFEB759C2F079DAF9467E2EFFAB5337BF15A3A25C7E2  
2101       B9FA9312BB8EC19EDA55480BBAAF2335A78DC179920C4E4374AA16  
2102       65895455E3D8552A6AE3F859B0D0107FC7F8582BF1053942AFE4EA  
2103       73D95ECD421B770A65F7123907AB17B9D63A009D0A56D0A667D2F8  
2104       F5B3D744566EFC7AB3DF8423EDCACB419742B7EADE499B33A3B099  
2105       F82BF56324A07253881471F242BE6CE6DDEC68CD3931AF6EB1D84E  
2106       C956145E5A0C1EFC99DFA327C0  
2107
```