

TCG Platform Certificate Profile

Specification Version 1.1
Revision 15
13 Feb 2019
Draft

Contact: admin@trustedcomputinggroup.org

Work in Progress

This document is an intermediate draft for comment only and is subject to change without notice. Readers should not design products based on this document.

TCG PUBLIC REVIEW

Copyright © TCG 2019

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 Latze (IWG co-chair)	Carolin Latze
Dean Liberty	AMD
Randy Mummert	Atmel
Malcolm Duncan	CESG
Bill Jacobs	Cisco
Max Pritikin	Cisco
Kazuaki Nimura	Fujitsu
Monty Wiseman (IWG co-chair)	GE
Graeme Proudler	Graeme Proudler
Takeuchi Keisuke	Hitachi
Hisanori Mishima	Hitachi
Tom Laffey	HPE
Diana Arroyo	IBM
Lee Terrell	IBM
Roger Zimmermann	IBM
Markus Gueller	Infineon
Johann Schoetz	Infineon
Arkadiusz Berent	Intel
David Grawrock	Intel
Eduardo Cabre	Intel
Geoffrey Strongin	Intel
Ned Smith	Intel
David Challener	John Hopkins University
Daniel Wong	Microsoft
Mark Williams	Microsoft
Mark Redman	Motorola
Sue Roddy	NSA
Laszlo Elteto	SafeNet
Manuel Offenber	Seagate Technology
Brad Andersen	SignaCert
Nicholas Szeto	Sony
Wyllys Ingersoll	Sun Microsystems
Jeff Nisewanger	Sun Microsystems
Paul Sangster	Symantec Corporation
Thomas Hardjono	Wave Systems
Greg Kazmierczak	Wave Systems
Len Veil	Wave Systems
Mihran Dars	Wave Systems

Table of Contents

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	Platform Certificate Privacy Protection Requirements.....	4
2.1.4	Revocation 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.....	6
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.....	7
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	Delta Platform Certificate Privacy Protection Requirements	9
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	10
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	11
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	Security Qualities	13
3.1.2	TPM and Platform Assertions	13
3.1.3	Conformance Attributes	15
3.1.4	Name Attributes	15
3.1.5	TCG Specification Attributes	16
3.1.6	TCG Certificate Type Attributes	16
3.1.7	TCG Certificate Specification Attributes	17
3.1.8	Platform Configuration Attributes	17
3.1.9	Platform Configuration Uri Attribute	20
3.2	Platform Certificate	20
3.2.1	Version	22
3.2.2	Serial Number	22
3.2.3	Signature Algorithm	22
3.2.4	Holder	23
3.2.5	Issuer	23
3.2.6	Validity	23

3.2.7	Certificate Policies	23
3.2.8	Subject Alternative Names.....	23
3.2.9	Targeting Information.....	23
3.2.10	Attributes.....	24
3.2.11	Authority Key Identifier.....	24
3.2.12	Authority Info Access	24
3.2.13	CRL Distribution.....	25
3.2.14	Issuer Unique Id.....	25
3.3	Delta Platform Certificate	25
3.3.1	Version.....	27
3.3.2	Serial Number.....	27
3.3.3	Signature Algorithm	27
3.3.4	Holder.....	27
3.3.5	Issuer	27
3.3.6	Validity.....	27
3.3.7	Certificate Policies	27
3.3.8	Subject Alternative Names.....	28
3.3.9	Targeting Information.....	28
3.3.10	Attributes.....	28
3.3.11	Authority Key Identifier.....	28
3.3.12	Authority Info Access	28
3.3.13	CRL Distribution.....	29
3.3.14	Issuer Unique Id.....	29
4.	X.509 ASN.1 Structures and OIDs	30
5.	References.....	36
A.	Certificate Examples.....	38
A.1	Example 1 (Platform Certificate in Attribute Certificate Format).....	38
A.1.1	PEM Format.....	38
A.1.2	DER Format	39
A.2	Example 2 (Delta Platform Certificate in Attribute Certificate Format).....	45
A.2.1	PEM Format.....	45
A.2.2	DER Format	47

Table of Tables

Table 1: Platform Certificate Fields	5
Table 2: Delta Platform Certificate Fields.....	10
Table 3: Attribute Certificate Format Fields.....	22
Table 4: Delta Attribute Certificate Format Fields	27

DRAFT

Change Log

Date	Version	Comment
2018-01-11	1.0	Initial Release
2018-05-02	1.1	Addition of Delta Platform Certificate and tree hierarchy.

DRAFT

1. Introduction

1.1 Purpose

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

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

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

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

1.2 Document Scope

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

1.3 Relationship to Other TCG Specifications

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

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 This document specifies one aspect of the architectural framework described in sections 3, 4,
50 5, and 6 of the document entitled “TCG Infrastructure Working Group Reference Architecture
51 for Interoperability” [2].

52 **1.6 Definition of Terms**

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

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

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

61

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

66 **2. Certificate Overview**

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

70 **2.1 Platform Certificate**

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

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

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

83 **2.1.1 Who Uses a Platform Certificate?**

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

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

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

99 **2.1.2 Who Issues a Platform Certificate?**

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

105 **2.1.3 Platform Certificate Privacy Protection Requirements**

106 If the Platform Certificate is stored on a platform after an Owner has taken ownership of that
107 platform, it SHALL exist only in storage to which access is controlled and is available to
108 authorized entities; this is to protect the privacy of the platform owner and the privacy of
109 users of the platform. Access to the Platform Certificate must be restricted to entities that
110 have a “need to know.” This is for reasons of privacy protection.

111 **2.1.4 Revocation of a Platform Certificate**

112 A Platform Certificate MAY only be revoked if there is evidence of CA compromise. Otherwise,
113 platform configuration changes made after the platform is shipped can be addressed by the
114 issuance of a Delta Platform Certificate.

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

117 **2.1.5 Assertions Made by a Platform Certificate**

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

120

Field Name	Description	Field Status
Certificate Type Label	Distinguish certificate types issued under a shared key	MUST
EK Certificates	Identifies the associated EK Certificates	MUST
Platform Manufacturer String	Name of platform manufacturer as a string	MUST
Platform Model	Manufacturer-specific identifier	MUST
Platform Version	Manufacturer-specific identifier	MUST
Issuer	Identifies the issuer of the certificate	MUST
Platform Specification	Platform Specification to which this platform is built	MUST
Certificate Specification	Platform Certificate Specification Version, Level, and Revision	MUST
Validity Period	Time period when certificate is valid	MUST
Signature Value	Signature of the issuer over the other fields	MUST

Platform Serial Number	Platform's unique serial number	MAY
Platform Assertions	Security assertions about the platform	MAY
Platform Configuration	Non-security related platform properties	MAY
Platform Manufacturer Identifier	Platform manufacturer unique identifier as an IANA identifier	MAY
Platform Configuration Uri	URI where PCR information can be obtained	MAY
Policy Reference	Certificate policy reference	MAY
Revocation Locator	Identifies source of revocation status information	MAY

Table 1: Platform Certificate Fields

121

122 **2.1.5.1 Certificate Type Label**

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

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

130 **2.1.5.2 EK Certificates**

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

133 This SHALL be an unambiguous indication of the EK Certificates of the TPM incorporated
134 into the platform. The Platform Certificate SHALL contain a reference to all mandatory (those
135 with MUST or SHALL) Endorsement Key (EK) Certificates. The requirements for the
136 Endorsement Key Certificates is typically stated in the Platform TPM Profile for that platform
137 class. For example, the Endorsement Key and Endorsement Key Certificate requirements for
138 the PC Client platform class is stated in the "TCG PC Client Platform TPM Profile (PTP)
139 Specification" [21] and described in Section 3.6.1 NV Storage Size. The Platform Certificate
140 MAY also contain references to non-mandatory EK Certificates if they exist for the TPM.

141 **2.1.5.3 Platform Manufacturer String**

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

144 **2.1.5.4 Platform Manufacturer Identifier**

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

148 **2.1.5.5 Platform Model**

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

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

152 **2.1.5.6 Platform Version**

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

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

157 **2.1.5.7 Issuer**

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

159 **2.1.5.8 Platform Specification**

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

163 **2.1.5.9 Certificate Specification**

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

166 **2.1.5.10 Validity Period**

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

169 **2.1.5.11 Signature Value**

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

171 **2.1.5.12 Platform Serial Number**

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

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

178 **2.1.5.13 Platform Assertions**

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

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

183 **2.1.5.14 Platform Configuration**

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

187 **2.1.5.15 Platform Configuration Uri**

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

190 **2.1.5.16 Policy Reference**

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

193 **2.1.5.17 Revocation Locator**

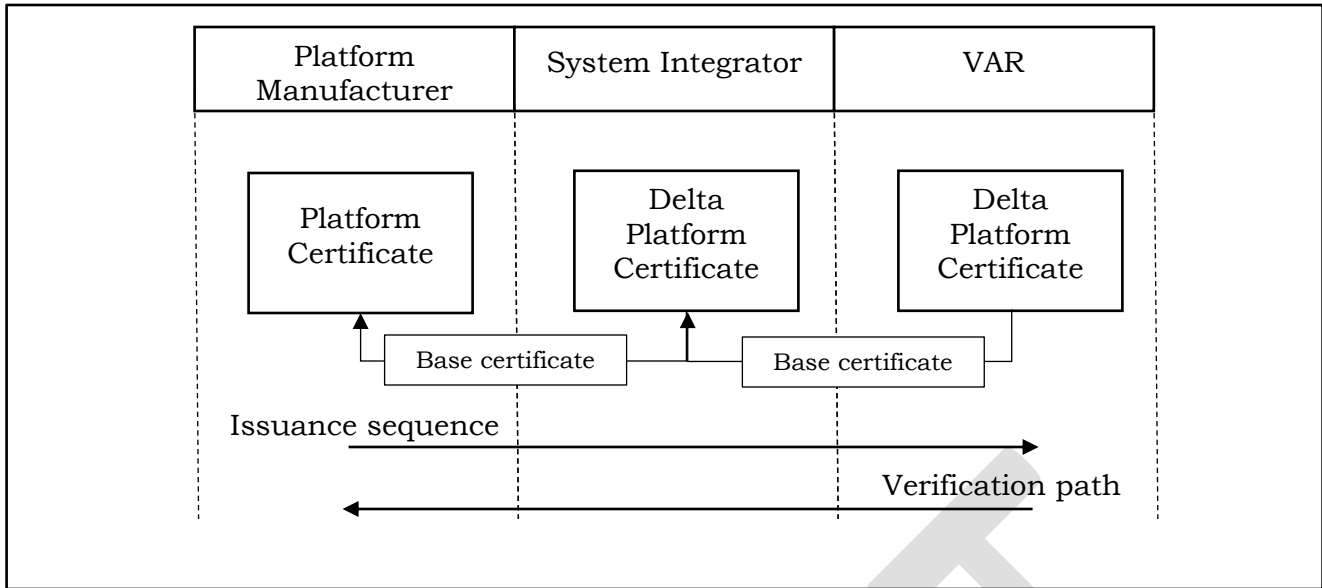
194 This assertion enables the certificate consumer to determine whether the Platform Certificate
195 has been revoked and should no longer be used as the basis for a trust decision.

196 **2.2 Delta Platform Certificate**

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

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

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



210
211 **Figure 1: Delta Platform Certificate chain**
212

213 **2.2.1 Who Uses a Delta Platform Certificate?**

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

217 **2.2.2 Who Issues a Delta Platform Certificate?**

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

221 **2.2.3 Conditions for Issuing a Delta Platform Certificate**

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

225 Changes made to the platform do not invalidate the TBB security claims made by the original
226 platform manufacturer. The Delta Platform Certificate issuer MUST NOT invalidate platform
227 security assertions made by the base Platform Certificate.

228 Changes made to the platform do not invalidate the TCG Platform Specification compliance
229 claims made by the platform manufacturer. Changes to the platform MAY NOT introduce
230 non-compliances to the TCG specification.

231 The issuing entity MUST NOT modify the TPM embedded in the platform (replace or modify
232 the TPM including replacing the EK keys or EK certificates). The issuing entity MAY issue
233 new EK keys and certificates.

234 **2.2.4 Delta Platform Certificate Privacy Protection Requirements**

235 The Delta Platform Certificate SHALL adhere to the same private protection requirements as
236 the Platform Certificate.

237 **2.2.5 Revocation of a Delta Platform Certificate**

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

242 A Delta Certificate MAY only be revoked if there is evidence of CA compromise.

243 **2.2.6 Assertions Made by a Delta Platform Certificate**

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

246

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 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

247 **Table 2: Delta Platform Certificate Fields**

248 **2.2.6.1 Certificate Type Label**

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

251 **2.2.6.2 EK Certificates**

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

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

256 **2.2.6.3 Base Platform Certificate**

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

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

261 **2.2.6.4 Platform Manufacturer String**

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

265 **2.2.6.5 Platform Manufacturer Identifier**

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

270 **2.2.6.6 Platform Model**

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

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

275 **2.2.6.7 Platform Version**

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

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

281 **2.2.6.8 Issuer**

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

283 **2.2.6.9 Certificate Specification**

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

287 **2.2.6.10 Validity Period**

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

289 **2.2.6.11 Signature Value**

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

291 **2.2.6.12 Platform Serial Number**

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

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

297 **2.2.6.13 Platform Configuration**

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

301 **2.2.6.14 Platform Configuration Uri**

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

305 **2.2.6.15 Policy Reference**

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

308 **2.2.6.16 Revocation Locator**

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

DRAFT

311 3. X.509 ASN.1 Definitions

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

315 3.1 TCG Attributes

316 3.1.1 Security Qualities

317 This attribute describes the platform security qualities in the Platform Certificate.

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

```
322 securityQualities ATTRIBUTE ::= {  
323     WITH SYNTAX SecurityQualities  
324     ID tcg-at-securityQualities }  
325  
326 SecurityQualities ::= SEQUENCE {  
327     version INTEGER,  
328     -- version 0 defined by TCPA 1.1b  
329     statement UTF8String }  
330
```

331 This attribute MUST NOT be included in Delta Platform Certificates.

332 3.1.2 TPM and Platform Assertions

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

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

336 Each attribute begins with a version number that identifies the version of the assertion
337 syntax. Future versions of this profile may add new assertions by appending new fields at the
338 end of the ASN.1 SEQUENCE and increasing the version number to identify which version of
339 the assertion syntax is encoded.

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

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

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

350

351 **URIMAX** is a constant used to provide an upper bound on the length of a URI included in the
352 certificate. This upper bound may be helpful to consumers of the extension and also helps
353 limit the overall size of the certificate. In order to provide a reasonable upper bound for ASN.1

354 parsers, **URIMAX** SHOULD NOT exceed a value of 1024. This value was selected as it matches
355 the length limit for <A> anchors in HTML as specified by the SGML declaration (LITLEN) for
356 HTML[5].

357 **STRMAX** is a constant defining the upper bound on the length of a string type. Like the **URIMAX**
358 this is to aid ASN.1 parsers and help limit the upper bound on the length of the certificate.
359 Based on the expected sizes of the strings in the ASN.1 in this document an upper bound of
360 256 was selected. **STRMAX** SHOULD NOT exceed a value of 256.

```
361     Version ::= INTEGER { v1(0) }
362
363     tbbSecurityAssertions ATTRIBUTE ::= {
364         WITH SYNTAX TbbSecurityAssertions
365         ID tcg-at-tbbSecurityAssertions }
366
367     TbbSecurityAssertions ::= SEQUENCE {
368         version Version DEFAULT v1,
369         ccInfo [0] IMPLICIT CommonCriteriaMeasures OPTIONAL,
370         fipsLevel [1] IMPLICIT FIPSLevel OPTIONAL,
371         rtmType [2] IMPLICIT MeasurementRootType OPTIONAL,
372         iso9000Certified BOOLEAN DEFAULT FALSE,
373         iso9000Uri IA5STRING (SIZE (1..URIMAX) OPTIONAL )
374
375         -- Hybrid means the measurement root is capable of static AND dynamic
376         -- Physical means that the root is anchored by a physical TPM
377         -- Virtual means the TPM is virtualized (possibly running in a VMM).
378         -- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
379         -- the capabilities of the platform.
380     MeasurementRootType ::= ENUMERATED {
381         static (0),
382         dynamic (1),
383         nonHost (2),
384         hybrid (3),
385         physical (4),
386         virtual (5) }
387
388
389     -- common criteria evaluation
390
391     CommonCriteriaMeasures ::= SEQUENCE {
392         version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined by CC
393         assuranceLevel EvaluationAssuranceLevel,
394         evaluationStatus EvaluationStatus,
395         plus BOOLEAN DEFAULT FALSE,
396         strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
397         profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
398         profileUri [2] IMPLICIT URIReference OPTIONAL,
399         targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
400         targetUri [4] IMPLICIT URIReference OPTIONAL }
401
402     EvaluationAssuranceLevel ::= ENUMERATED {
403         level1 (1),
404         level2 (2),
405         level3 (3),
406         level4 (4),
407         level5 (5),
408         level6 (6),
409         level7 (7) }
410
411     StrengthOfFunction ::= ENUMERATED {
412         basic (0),
413         medium (1),
414         high (2) }
415
416     -- Reference to external document containing information relevant to this subject.
417     -- The hashAlgorithm and hashValue MUST both exist in each reference if either
418     -- appear at all.
419     URIReference ::= SEQUENCE {
```

```

420     uniformResourceIdentifier IA5String (SIZE (1..URIMAX)),
421     hashAlgorithm AlgorithmIdentifier OPTIONAL,
422     hashValue BIT STRING OPTIONAL }
423
424 EvaluationStatus ::= ENUMERATED {
425     designedToMeet (0),
426     evaluationInProgress (1),
427     evaluationCompleted (2) }
428
429 -- fips evaluation
430
431 FIPSLevel ::= SEQUENCE {
432     version IA5STRING (SIZE (1..STRMAX)), -- "140-1" or "140-2"
433     level SecurityLevel,
434     plus BOOLEAN DEFAULT FALSE }
435
436 SecurityLevel ::= ENUMERATED {
437     level1 (1),
438     level2 (2),
439     level3 (3),
440     level4 (4) }
441

```

442 3.1.3 Conformance Attributes

443 Conformance Attributes are the syntax of the protection profile and security target attributes.
444 These attributes are deprecated and replaced with the TPM and Platform Assertion attributes.
445 They MAY be present for compatibility with previously published TCG and TCPA
446 specifications.

```

447 ProtectionProfile ::= OBJECT IDENTIFIER
448 SecurityTarget ::= OBJECT IDENTIFIER
449
450 TBBProtectionProfile ATTRIBUTE ::= {
451     WITH SYNTAX ProtectionProfile
452     ID tcg-at-tbbProtectionProfile }
453
454 TBBSecurityTarget ATTRIBUTE ::= {
455     WITH SYNTAX SecurityTarget
456     ID tcg-at-tbbSecurityTarget }

```

457 3.1.4 Name Attributes

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

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

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

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

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

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

469 These attributes MUST be included in the Delta Platform Certificate.

470

```

471 PlatformManufacturerStr ATTRIBUTE ::= {
472

```

```

473     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
474     ID tcg-at-platformManufacturerStr }
475
476 PlatformModel ATTRIBUTE ::= {
477     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
478     ID tcg-at-platformModel }
479
480 PlatformVersion ATTRIBUTE ::= {
481     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
482     ID tcg-at-platformVersion }
483
484 PlatformSerial ATTRIBUTE ::= {
485     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
486     ID tcg-at-platformSerial }
487
488 PlatformManufacturerId ATTRIBUTE ::= {
489     WITH SYNTAX ManufacturerId
490     ID tcg-at-platformManufacturerId
491 }
492
493 ManufacturerId ::= SEQUENCE {
494     manufacturerIdentifier PrivateEnterpriseNumber
495 }
496
497 enterprise OBJECT IDENTIFIER ::= {
498     iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)}
499
500 PrivateEnterpriseNumber OBJECT IDENTIFIER ::= { enterprise private-enterprise-number }
501
502 All assigned private enterprise numbers are listed at the Internet Assigned Numbers
503 Authority (IANA) web site [8].

```

504 3.1.5 TCG Specification Attributes

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

507 The **TCGPlatformSpecification** attribute identifies the platform class, version and revision
508 of the platform-specific specification with which a platform implementation is compliant. The
509 platform specification refers either to the PC Client Platform Specification [10] or the Server
510 Specification [9]. Standardized platform class values are defined in Section 5 of the Registry
511 of Reserved TPM 2.0 Handles and Localities [22]. This attribute MUST NOT be included in the
512 Delta Platform Certificate.

```

513
514 tCGPlatformSpecification ATTRIBUTE ::= {
515     WITH SYNTAX TCGPlatformSpecification
516     ID tcg-at-tcgPlatformSpecification }
517
518 TCGSpecificationVersion ::= SEQUENCE {
519     majorVersion INTEGER,
520     minorVersion INTEGER,
521     revision INTEGER }
522
523 TCGPlatformSpecification ::= SEQUENCE {
524     Version TCGSpecificationVersion,
525     platformClass OCTET STRING SIZE(4) }

```

526 3.1.6 TCG Certificate Type Attributes

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

528 The **TCGCredentialType** attribute identifies the type of Platform Certificate. Values
529 supported are Platform Certificate and Delta Platform Certificate in both attribute and public

530 key formats. Values are encoded as TCG registered OIDs. This attribute MUST be included
531 in the Delta Platform Certificate to differentiate from a Platform Certificate.

```
532     tcgCredentialType ATTRIBUTE ::= {  
533         WITH SYNTAX TCGCredentialType  
534         ID tcg-at-tcgCredentialType  
535     }  
536     TCGCredentialType ::= SEQUENCE {  
537         certificateType CredentialType  
538     }  
539     CredentialType ::= OBJECT IDENTIFIER (tcg-kp-PlatformAttributeCertificate | tcg-kp-  
540         DeltaPlatformAttributeCertificate )  
541
```

542 3.1.7 TCG Certificate Specification Attributes

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

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

```
548     tcgCredentialSpecification ATTRIBUTE ::= {  
549         WITH SYNTAX TCGSpecificationVersion  
550         ID tcg-at-tcgCredentialSpecification }  
551     TCGSpecificationVersion ::= SEQUENCE {  
552         majorVersion INTEGER,  
553         minorVersion INTEGER,  
554         revision INTEGER }  
555
```

556 3.1.8 Platform Configuration Attributes

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

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

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

571 The **componentPlatformCert** field contains information about the component's Platform
572 Certificate. This field allows the issuer to create a hierarchy of platforms by constructing a
573 general tree of Platform Certificates. The issuer MUST include **attributeCertificateIdentifier** or
574 **genericCertIdentifier** to provide a reference to the component's Platform Certificate. The
575 verifier can use the **componentPlatformCert** attribute to cryptographically verify the
576 constituent components and subcomponents of a platform. In order to verify the certificate
577 hierarchy, the verifier can use the **attributeCertIdentifier** or **genericCertIdentifier**

578 fields to identify the component Platform Certificate. This operation would have to be repeated
579 for any component of the platform, and subsequently down the hierarchical tree. The verifier
580 can use this information to effectively confirm a platform's components remain unchanged
581 from the as-built configuration.

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

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

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

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

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

599

```
600 platformConfiguration ATTRIBUTE ::= {  
601   WITH SYNTAX PlatformConfiguration  
602   ID tcg-at-platformConfiguration-v2  
603 }  
604  
605 PlatformConfiguration ::= SEQUENCE {  
606   componentIdentifiers [0] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF ComponentIdentifier OPTIONAL,  
607   componentIdentifiersUri [1] IMPLICIT URIReference OPTIONAL,  
608   platformProperties [2] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF Property OPTIONAL,  
609   platformPropertiesUri [3] IMPLICIT URIReference OPTIONAL  
610 }  
611  
612 ComponentIdentifier ::= SEQUENCE {  
613   componentClass ComponentClass,  
614   componentManufacturer UTF8String (SIZE (1..STRMAX)),  
615   componentModel UTF8String (SIZE (1..STRMAX)),  
616   componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,  
617   componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,  
618   componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,  
619   fieldReplaceable [3] IMPLICIT BOOLEAN OPTIONAL,  
620   componentAddresses [4] IMPLICIT SEQUENCE(SIZE(1.. MAX)) OF ComponentAddress OPTIONAL  
621   componentPlatformCert [5] IMPLICIT CertificateIdentifier OPTIONAL,  
622   componentPlatformCertUri [6] IMPLICIT URIReference OPTIONAL,  
623   status [7] IMPLICIT AttributeStatus OPTIONAL }  
624  
625 ComponentClass ::= SEQUENCE {  
626   componentClassRegistry ComponentClassRegistry,  
627   componentClassValue OCTET STRING SIZE(4) }  
628  
629 ComponentClassRegistry ::= OBJECT IDENTIFIER ( tcg-registry-componentClass-tcg | tcg-registry-  
630 componentClass-ietf | tcg-registry-componentClass-dmtf )  
631  
632 ComponentAddress ::= SEQUENCE {  
633   addressType AddressType,
```

```

634         addressValue UTF8String (SIZE (1..STRMAX)) }
635
636 AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
637         bluetoothmac)
638
639 Property ::= SEQUENCE {
640     propertyName UTF8String (SIZE (1..STRMAX)),
641     propertyValue UTF8String (SIZE (1..STRMAX)),
642     status [0] IMPLICIT AttributeStatus OPTIONAL }
643
644 CertificateIdentifier ::= SEQUENCE {
645     attributeCertIdentifier [0] IMPLICIT AttributeCertificateIdentifier OPTIONAL,
646     genericCertIdentifier [1] IMPLICIT IssuerSerial OPTIONAL }
647
648 AttributeCertificateIdentifier ::= SEQUENCE {
649     hashAlgorithm AlgorithmIdentifier,
650     hashOverSignatureValue OCTET STRING
651 }
652
653 IssuerSerial ::= SEQUENCE {
654     issuer GeneralNames,
655     serial CertificateSerialNumber
656 }
657
658 AttributeStatus ::= ENUMERATED {
659     added (0),
660     modified (1),
661     removed (2) }
662

```

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

668
669 The **AttributeCertificateIdentifier** sequence is comprised of the hashAlgorithm field
670 and the hashOverSignatureValue. The hashAlgorithm field is of type AlgorithmIdentifier as
671 defined in RFC5280 [13]. This field identifies the hashing algorithm used in
672 hashOverSignatureValue field. The hashOverSignatureValue is calculated over the Platform
673 Certificate's BIT STRING signatureValue (excluding the tag, length, and number of unused
674 bits).

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

```

676     AlgorithmIdentifier ::= SEQUENCE {
677         algorithm OBJECT IDENTIFIER,
678         parameters ANY DEFINED BY algorithm OPTIONAL }
679

```

680 Since the algorithms used are all hashing algorithms, the parameters field SHOULD not be
681 used. The issuer MAY utilize any of the hash algorithm OIDs found in RFC3279 [15], RFC4055
682 [16], SHA-3 Related Algorithms and Identifiers for PKIX [17], and GB/T 33560-2017 [18].

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

685 **NOTE:** Future versions of this specification could introduce modifications to the
686 **platformConfiguration** attribute. If such changes impact the structure and semantics of
687 existing fields (componentIdentifiers, componentIdentifiersURI, platformProperties, and
688 platformPropertiesURI) the attribute's OID will be updated to the next version (**tcg-at-**

689 **platformConfiguration-v3**). Parsers and verifiers should be version aware, and make the
690 necessary adjustments to support current and prior versions of the attribute.

691 3.1.9 Platform Configuration Uri Attribute

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

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

```
697 PlatformConfigUri ATTRIBUTE ::= {  
698 WITH SYNTAX URIReference  
699 ID tcg-at-platformConfigUri }  
700
```

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

703 3.2 Platform Certificate

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

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

709 Note: some fields are assigned a value even though the certificate user performs no action
710 with that value. In such cases, the intention is to inhibit non-TCG implementations from
711 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

Field Name	RFC 5755 Type	Value	Field Status
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 of 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
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

Field Name	RFC 5755 Type	Value	Field Status
Subject Alternative Names	GeneralName directoryName	PlatformManufacturerStr PlatformModel PlatformVersion PlatformSerial (optional) PlatformManufacturerId (optional)	MUST non-critical
Targeting Information	TargetingInformation	Additional TPM EK Certificates not included in Holder. Use targetName option.	MAY critical
Authority Key Id	AuthorityKeyIdentifier	Key identifier Issuer name and serial number (optional)	MUST non-critical
Authority Info Access	AuthorityInfoAccessSyntax	id-ad-caIssuers URI to issuing CA id-ad-ocsp (optional) URI to OCSP responder	SHOULD non-critical
CRL Distribution	CRLDistributionPoints	URI to CRL	MAY non-critical
Issuer Unique Id	UniqueIdentifier	Unique value when using a shared issuer name	SHOULD NOT

Table 3: Attribute Certificate Format Fields

712

713 3.2.1 Version

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

717 3.2.2 Serial Number

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

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

722 3.2.3 Signature Algorithm

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

726 3.2.4 Holder

727 This field contains a reference to the X.509 certificate of the TPM EK certificate. The
728 BaseCertificateID choice MUST be used. Additional TPM EK certificates MAY be referenced
729 using the TargetingInformation extension.

730 3.2.5 Issuer

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

734 3.2.6 Validity

735 This field contains the period during which the binding between the attributes and TPM EK
736 certificates is considered valid. It is represented by two date values named notBefore and
737 notAfter. Issuers SHOULD assign notBefore to the current time when the certificate is issued
738 and notAfter to the last date that the certificate will be considered valid. Both notBefore and
739 notAfter MUST use the appropriate time format as indicated by RFC 5755, section 4.2.6.

740 3.2.7 Certificate Policies

741 This extension indicates policy terms under which the certificate was issued.
742 Assign "critical" the value FALSE. Assign **policyIdentifier** at least one object identifier.
743 Assign the **cPSuri** policy qualifier the value of an HTTP URL at which a plain language version
744 of the platform endorsement entity's certificate policy may be obtained. Assign the explicit
745 text **userNotice** policy qualifier the value "TCG Trusted Platform Endorsement".
746 During certificate path validation, check that at least one acceptable **policyIdentifier**
747 value is present.

748 3.2.8 Subject Alternative Names

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

756 3.2.9 Targeting Information

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

763 **3.2.10 Attributes**

764 The following attributes SHOULD be included:

- 765 • The “TCG Platform Specification” attribute references the platform class, version and
766 revision level of the TCG platform-specific specification to which the platform was
767 designed.
- 768 • The “TCG Certificate Type” attribute identifies the type of certificate and its format.
- 769 • The “TCG Certificate Specification” attribute references the version, level, and revision
770 of this specification.
- 771 • The platform “TBB Security Assertions” attribute describes various assertions about
772 the security properties of the TBB of the platform.

773 The following attributes MAY be included:

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

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

- 781 • The "TCPA Specification Version" attribute, with field values correctly reflecting the
782 highest version of the TCG specification with which the TPM implementation conforms.
- 783 • If the TPM has been successfully evaluated against a Common Criteria protection
784 profile, then include the TPM protection profile identifier attribute.
- 785 • If the TPM has been successfully evaluated against a Common Criteria security target,
786 then include the TPM security target identifier attribute.
- 787 • If the RTM and the means by which the TPM and RTM have been incorporated into the
788 platform have been successfully evaluated against a Common Criteria protection
789 profile, then include the "TBB protection profile" identifier attribute.
- 790 • If the RTM and the means by which the TPM and RTM have been incorporated into the
791 platform have been successfully evaluated against a Common Criteria security target,
792 then include the "TBB security target" identifier attribute.
- 793 • Optionally, include the "security qualities" attribute with a text string reflecting the
794 security qualities of the platform.

795 **3.2.11 Authority Key Identifier**

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

799 **3.2.12 Authority Info Access**

800 This extension contains additional information about the issuer. Assign “critical” the value
801 FALSE. It MAY be omitted. If included, then the accessMethod OID SHOULD be set to id-ad-

802 ocs (RFC 5755 [11]) and the accessLocation value SHOULD point to the access value of the
803 OCS responder (HTTP URI).

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

808 3.2.13 CRL Distribution

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

813 3.2.14 Issuer Unique Id

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

816 3.3 Delta Platform Certificate

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

820 Note: some fields are assigned a value even though the certificate user performs no action
821 with that value. In such cases, the intention is to inhibit non-TCG implementations from
822 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

Field Name	RFC 5755 Type	Value	Field Status
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
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

Field Name	RFC 5755 Type	Value	Field Status
CRL Distribution	CRLDistributionPoints	URI to CRL	MAY non-critical

Table 4: Delta Attribute Certificate Format Fields

823

824 **3.3.1 Version**

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

827 **3.3.2 Serial Number**

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

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

832 **3.3.3 Signature Algorithm**

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

836 **3.3.4 Holder**

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

839 **3.3.5 Issuer**

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

844 **3.3.6 Validity**

845 This field contains the period during which the assertions made by the issuer about the
846 platform are considered valid. Issuers SHOULD assign notBefore to the current time when
847 the certificate is issued and notAfter to the last date that the certificate will be considered
848 valid. The notAfter date SHOULD not precede that of the base certificate. Both notBefore and
849 notAfter MUST use the appropriate time format as indicated by RFC 5755, section 4.2.6.

850 **3.3.7 Certificate Policies**

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

852 Assign "critical" the value FALSE. Assign policyIdentifier at least one object identifier. Assign
853 the cPSuri policy qualifier the value of an HTTP URL at which a plain language version of the

854 platform endorsement entity's certificate policy may be obtained. Assign the explicit text
855 userNotice policy qualifier the value "TCG Trusted Platform Endorsement".

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

858 **3.3.8 Subject Alternative Names**

859 This extension contains the platform name attributes. This extension MUST equal that of the
860 base Platform or Delta Platform Certificate, the issuer MUST NOT introduce any changes.
861 Assign "critical" the value FALSE. Include the platform model, using the directory name-form
862 with RDNs for the platform manufacturer, model, version number, and optionally, the serial
863 number, and manufacturer ID. The "Platform Manufacturer Identifier" optional field uniquely
864 identifies the platform's manufacturer using the IANA Private Enterprise Number OID [8].

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

867 **3.3.9 Targeting Information**

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

870 **3.3.10 Attributes**

871 The following attributes SHOULD be included:

- 872 • The "TCG Certificate Type" attribute identifies the type of certificate and its format.
- 873 • The "TCG Certificate Specification" attribute references the version, level, and revision
874 of this specification.

875 The following attributes MAY be included:

- 876 • The "Platform Configuration" attribute describes various assertions of platform
877 properties that are not security related, including CPU and motherboard serial
878 numbers, and network adapter MAC addresses.
- 879 • The "Platform Configuration Uri" attribute which provides the URI to the manufacturer
880 published list of valid PCR values.

881 **3.3.11 Authority Key Identifier**

882 This extension identifies the subject public key of the certificate issuer. Assign "critical" the
883 value FALSE. Assign the value of "subject key identifier" from the issuer's public-key
884 certificate, if available, else omit.

885 **3.3.12 Authority Info Access**

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

890 The relying party can access the certificate status for this certificate by sending a properly
891 formatted OCSPRequest to the URI. If both a CRL Distribution Point (CDP) and OCSP AIA

892 extension are present in the certificate, then the relying parties SHOULD use OCSP as the
893 primary validation mechanism.

894 **3.3.13 CRL Distribution**

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

899 **3.3.14 Issuer Unique Id**

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

DRAFT

902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968

4. X.509 ASN.1 Structures and OIDs

TCG has registered an object identifier (OID) namespace as an “international body” in the ISO registration hierarchy. This leads to shorter OIDs and gives TCG the ability to manage its own namespace. The OID namespace is inherited from TCPA specifications. These definitions are intended to be used within the context of an X.509 v3 certificate specifically leveraging the profile described in RFC 5755.

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

tcg-tcpaSpecVersion OBJECT IDENTIFIER ::= {tcg 1}
tcg-attribute OBJECT IDENTIFIER ::= {tcg 2}
tcg-protocol OBJECT IDENTIFIER ::= {tcg 3}
tcg-algorithm OBJECT IDENTIFIER ::= {tcg 4}
tcg-platformClass OBJECT IDENTIFIER ::= {tcg 5}
tcg-ce OBJECT IDENTIFIER ::= {tcg 6}
tcg-kp OBJECT IDENTIFIER ::= {tcg 8}
tcg-address OBJECT IDENTIFIER ::= {tcg 17}
tcg-registry OBJECT IDENTIFIER ::= {tcg 18}

-- TCG Attribute OIDs
tcg-at-tpmManufacturer OBJECT IDENTIFIER ::= {tcg-attribute 1}
tcg-at-tpmModel OBJECT IDENTIFIER ::= {tcg-attribute 2}
tcg-at-tpmVersion OBJECT IDENTIFIER ::= {tcg-attribute 3}
tcg-at-securityQualities OBJECT IDENTIFIER ::= {tcg-attribute 10}
tcg-at-tpmProtectionProfile OBJECT IDENTIFIER ::= {tcg-attribute 11}
tcg-at-tpmSecurityTarget OBJECT IDENTIFIER ::= {tcg-attribute 12}
tcg-at-tbbProtectionProfile OBJECT IDENTIFIER ::= {tcg-attribute 13}
tcg-at-tbbSecurityTarget OBJECT IDENTIFIER ::= {tcg-attribute 14}
tcg-at-tpmIdLabel OBJECT IDENTIFIER ::= {tcg-attribute 15}
tcg-at-tpmSpecification OBJECT IDENTIFIER ::= {tcg-attribute 16}
tcg-at-tcgPlatformSpecification OBJECT IDENTIFIER ::= {tcg-attribute 17}
tcg-at-tpmSecurityAssertions OBJECT IDENTIFIER ::= {tcg-attribute 18}
tcg-at-tbbSecurityAssertions OBJECT IDENTIFIER ::= {tcg-attribute 19}
tcg-at-tcgCredentialSpecification OBJECT IDENTIFIER ::= {tcg-attribute 23}
tcg-at-tcgCredentialType OBJECT IDENTIFIER ::= {tcg-attribute 25}

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

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

-- TCG Platform Configuration OIDs
tcg-at-platformConfiguration-v1 OBJECT IDENTIFIER ::= {tcg-at-platformConfiguration 1}
tcg-at-platformConfiguration-v2 OBJECT IDENTIFIER ::= {tcg-at-platformConfiguration 2}

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

-- TCG Key Purposes OIDs
tcg-kp-EKCertificate OBJECT IDENTIFIER ::= {tcg-kp 1}
tcg-kp-PlatformAttributeCertificate OBJECT IDENTIFIER ::= {tcg-kp 2}
tcg-kp-AIKCertificate OBJECT IDENTIFIER ::= {tcg-kp 3}
tcg-kp-PlatformKeyCertificate OBJECT IDENTIFIER ::= {tcg-kp 4}
tcg-kp-DeltaPlatformAttributeCertificate OBJECT IDENTIFIER ::= {tcg-kp 5}

-- TCG Certificate Extensions
tcg-ce-relevantCredentials OBJECT IDENTIFIER ::= {tcg-ce 2}
```

```

969 tcg-ce-relevantManifests OBJECT IDENTIFIER ::= {tcg-ce 3}
970 tcg-ce-virtualPlatformAttestationService OBJECT IDENTIFIER ::= {tcg-ce 4}
971 tcg-ce-migrationControllerAttestationService OBJECT IDENTIFIER ::= {tcg-ce 5}
972 tcg-ce-migrationControllerRegistrationService OBJECT IDENTIFIER ::= {tcg-ce 6}
973 tcg-ce-virtualPlatformBackupService OBJECT IDENTIFIER ::= {tcg-ce 7}
974
975 -- TCG Protocol OIDs
976 tcg-prt-tpmIdProtocol OBJECT IDENTIFIER ::= {tcg-protocol 1}
977
978 -- TCG Address OIDs
979 tcg-address-ethernetmac OBJECT IDENTIFIER ::= {tcg-address 1}
980 tcg-address-wlanmac OBJECT IDENTIFIER ::= {tcg-address 2}
981 tcg-address-bluetoothmac OBJECT IDENTIFIER ::= {tcg-address 3}
982
983 -- TCG Registry OIDs
984 tcg-registry-componentClass OBJECT IDENTIFIER ::= {tcg-registry 3}
985 tcg-registry-componentClass-tcg OBJECT IDENTIFIER ::= {tcg-registry-componentClass 1}
986 tcg-registry-componentClass-ietf OBJECT IDENTIFIER ::= {tcg-registry-componentClass 2}
987 tcg-registry-componentClass-dmtf OBJECT IDENTIFIER ::= {tcg-registry-componentClass 3}
988
989
990 -- tcg specification attributes for tpm and platform
991 tPMSpecification ATTRIBUTE ::= {
992     WITH SYNTAX TPMSpecification
993     ID tcg-at-tpmSpecification }
994
995 TPMSpecification ::= SEQUENCE {
996     family UTF8String (SIZE (1..STRMAX)),
997     level INTEGER,
998     revision INTEGER }
999
1000 tCGPlatformSpecification ATTRIBUTE ::= {
1001     WITH SYNTAX TCGPlatformSpecification
1002     ID tcg-at-tcgPlatformSpecification }
1003
1004 TCGSpecificationVersion ::= SEQUENCE {
1005     majorVersion INTEGER,
1006     minorVersion INTEGER,
1007     revision INTEGER }
1008
1009 TCGPlatformSpecification ::= SEQUENCE {
1010     Version TCGSpecificationVersion,
1011     platformClass OCTET STRING SIZE(4) }
1012
1013 -- TCG Credential type attribute
1014 tCGCredentialType ATTRIBUTE ::= {
1015     WITH SYNTAX TCGCredentialType
1016     ID tcg-at-tcgCredentialType}
1017
1018 TCGCredentialType ::= SEQUENCE {
1019     certificateType CredentialType}
1020
1021 CredentialType ::= OBJECT IDENTIFIER (tcg-kp-PlatformAttributeCertificate | tcg-kp-
1022     DeltaPlatformAttributeCertificate )
1023
1024 -- manufacturer implementation model and version attributes
1025 TPMManufacturer ATTRIBUTE ::= {
1026     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1027     ID tcg-at-tpmManufacturer }
1028
1029 TPMModel ATTRIBUTE ::= {
1030     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1031     ID tcg-at-tpmModel }
1032
1033 TPMVersion ATTRIBUTE ::= {
1034     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1035     ID tcg-at-tpmVersion }
1036
1037 PlatformManufacturerStr ATTRIBUTE ::= {
1038     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1039     ID tcg-at-platformManufacturerStr }

```

```

1040
1041 PlatformModel ATTRIBUTE ::= {
1042     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1043     ID tcg-at-platformModel }
1044
1045 PlatformVersion ATTRIBUTE ::= {
1046     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1047     ID tcg-at-platformVersion }
1048
1049 PlatformSerial ATTRIBUTE ::= {
1050     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
1051     ID tcg-at-platformSerial }
1052
1053 PlatformManufacturerId ATTRIBUTE ::= {
1054     WITH SYNTAX ManufacturerId
1055     ID tcg-at-platformManufacturerId
1056 }
1057
1058 ManufacturerId ::= SEQUENCE {
1059     manufacturerIdentifier PrivateEnterpriseNumber
1060 }
1061
1062 enterprise OBJECT IDENTIFIER ::= {
1063     iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) }
1064
1065 PrivateEnterpriseNumber OBJECT IDENTIFIER ::= { enterprise private-enterprise-number }
1066
1067
1068 -- tpm and platform tbb security assertions
1069 Version ::= INTEGER { v1(0) }
1070 TPMSecurityAssertions ATTRIBUTE ::= {
1071     WITH SYNTAX TPMSecurityAssertions
1072     ID tcg-at-tpmSecurityAssertions
1073 }
1074
1075 TPMSecurityAssertions ::= SEQUENCE {
1076     version Version DEFAULT v1,
1077     fieldUpgradable BOOLEAN DEFAULT FALSE,
1078     ekGenerationType [0] IMPLICIT EKGenerationType OPTIONAL,
1079     ekGenerationLocation [1] IMPLICIT EKGenerationLocation OPTIONAL,
1080     ekCertificateGenerationLocation [2] IMPLICIT EKCertificateGenerationLocation OPTIONAL,
1081     ccInfo [3] IMPLICIT CommonCriteriaMeasures OPTIONAL,
1082     fipsLevel [4] IMPLICIT FIPSLevel OPTIONAL,
1083     iso9000Certified [5] IMPLICIT BOOLEAN DEFAULT FALSE,
1084     iso9000Uri IA5STRING (SIZE (1..URIMAX)) OPTIONAL }
1085
1086 TBBSecurityAssertions ATTRIBUTE ::= {
1087     WITH SYNTAX TBBSecurityAssertions
1088     ID tcg-at-tbbSecurityAssertions }
1089
1090 TBBSecurityAssertions ::= SEQUENCE {
1091     version Vers1 DEFAULT v1,
1092     ccInfo [0] IMPLICIT CommonCriteriaMeasures OPTIONAL,
1093     fipsLevel [1] IMPLICIT FIPSLevel OPTIONAL,
1094     rtmType [2] IMPLICIT MeasurementRootType OPTIONAL,
1095     iso9000Certified BOOLEAN DEFAULT FALSE,
1096     iso9000Uri IA5STRING (SIZE (1..URIMAX)) OPTIONAL }
1097
1098 EKGenerationType ::= ENUMERATED {
1099     internal (0),
1100     injected (1),
1101     internalRevocable(2),
1102     injectedRevocable(3) }
1103
1104 EKGenerationLocation ::= ENUMERATED {
1105     tpmManufacturer (0),
1106     platformManufacturer (1),
1107     ekCertSigner (2) }
1108
1109 EKCertificateGenerationLocation ::= ENUMERATED {
1110     tpmManufacturer (0),

```



```

1111     platformManufacturer (1),
1112     ekCertSigner (2) }
1113
1114 -- Hybrid means the measurement root is capable of static AND dynamic
1115 -- Physical means that the root is anchored by a physical TPM
1116 -- Virtual means the TPM is virtualized (possibly running in a VMM)
1117
1118 -- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
1119 -- the capabilities of the platform.
1120 MeasurementRootType ::= ENUMERATED {
1121     static (0),
1122     dynamic (1),
1123     nonHost (2),
1124     hybrid (3),
1125     physical (4),
1126     virtual (5) }
1127
1128
1129 -- common criteria evaluation
1130 CommonCriteriaMeasures ::= SEQUENCE {
1131     version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined by CC
1132     assuranceLevel EvaluationAssuranceLevel,
1133     evaluationStatus EvaluationStatus,
1134     plus BOOLEAN DEFAULT FALSE,
1135     strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
1136     profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
1137     profileUri [2] IMPLICIT URIReference OPTIONAL,
1138     targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
1139     targetUri [4] IMPLICIT URIReference OPTIONAL }
1140
1141 EvaluationAssuranceLevel ::= ENUMERATED {
1142     level1 (1),
1143     level2 (2),
1144     level3 (3),
1145     level4 (4),
1146     level5 (5),
1147     level6 (6),
1148     level7 (7) }
1149
1150 StrengthOfFunction ::= ENUMERATED {
1151     basic (0),
1152     medium (1),
1153     high (2) }
1154
1155 URIReference ::= SEQUENCE {
1156     uniformResourceIdentifier IA5String (SIZE (1..URIMAX)),
1157     hashAlgorithm AlgorithmIdentifier OPTIONAL,
1158     hashValue BIT STRING OPTIONAL }
1159
1160 EvaluationStatus ::= ENUMERATED {
1161     designedToMeet (0),
1162     evaluationInProgress (1),
1163     evaluationCompleted (2) }
1164
1165 -- fips evaluation
1166 FIPSLevel ::= SEQUENCE {
1167     version IA5STRING (SIZE (1..STRMAX)), -- "140-1" or "140-2"
1168     level SecurityLevel,
1169     plus BOOLEAN DEFAULT FALSE }
1170
1171 SecurityLevel ::= ENUMERATED {
1172     level1 (1),
1173     level2 (2),
1174     level3 (3),
1175     level4 (4) }
1176
1177 -- aik certificate label from tpm owner
1178
1179 TPMIdLabel OTHER-NAME ::= {UTF8String IDENTIFIED BY {tcg-at-tpmIdLabel} }
1180
1181 -- platform configuration

```

```

1182 platformConfiguration ATTRIBUTE ::= {
1183     WITH SYNTAX PlatformConfiguration
1184     ID tcg-at-platformConfiguration-v2
1185 }
1186
1187 PlatformConfiguration ::= SEQUENCE {
1188     componentIdentifiers [0] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF ComponentIdentifier OPTIONAL,
1189     componentIdentifiersUri [1] IMPLICIT URIReference OPTIONAL,
1190     platformProperties [2] IMPLICIT SEQUENCE(SIZE(1..MAX)) OF Properties OPTIONAL,
1191     platformPropertiesUri [3] IMPLICIT URIReference OPTIONAL
1192 }
1193
1194 ComponentIdentifier ::= SEQUENCE {
1195     componentClass ComponentClass,
1196     componentManufacturer UTF8String (SIZE (1..STRMAX)),
1197     componentModel UTF8String (SIZE (1..STRMAX)),
1198     componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
1199     componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
1200     componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,
1201     fieldReplaceable [3] IMPLICIT BOOLEAN OPTIONAL,
1202     componentAddresses [4] IMPLICIT SEQUENCE(SIZE(1.. MAX)) OF ComponentAddress OPTIONAL
1203     componentPlatformCert [5] IMPLICIT CertificateIdentifier OPTIONAL,
1204     componentPlatformCertUri [6] IMPLICIT URIReference OPTIONAL,
1205     status [7] IMPLICIT AttributeStatus OPTIONAL }
1206
1207 ComponentClass ::= SEQUENCE {
1208     componentClassRegistry ComponentClassRegistry,
1209     componentClassValue OCTET STRING SIZE(4) }
1210
1211 ComponentClassRegistry ::= OBJECT IDENTIFIER ( tcg-registry-componentClass-tcg | tcg-registry-
1212 componentClass-ietf | tcg-registry-componentClass-dmtf )
1213
1214 ComponentAddress ::= SEQUENCE {
1215     addressType AddressType,
1216     addressValue UTF8String (SIZE (1..STRMAX)) }
1217
1218 AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
1219 bluetoothmac)
1220
1221 Properties ::= SEQUENCE {
1222     propertyName UTF8String (SIZE (1..STRMAX)),
1223     propertyValue UTF8String (SIZE (1..STRMAX)),
1224     status [0] IMPLICIT AttributeStatus OPTIONAL }
1225
1226 CertificateIdentifier ::= SEQUENCE {
1227     attributeCertIdentifier [0] AttributeCertificateIdentifier OPTIONAL,
1228     certificateIssuer [1] GeneralNames OPTIONAL,
1229     certificateSerialNumber [2] CertificateSerialNumber OPTIONAL }
1230
1231 AttributeCertificateIdentifier ::= SEQUENCE {
1232     hashAlgorithm AlgorithmIdentifier,
1233     hashOverSignatureValue OCTET STRING
1234 }
1235
1236 AttributeStatus ::= ENUMERATED {
1237     added (0),
1238     modified (1),
1239     removed (2) }
1240
1241 -- platform configuration Uri attribute
1242 PlatformConfigUri ATTRIBUTE ::= {
1243     WITH SYNTAX URIReference
1244     ID tcg-at-platformConfigUri }
1245
1246 -- the following are deprecated but may be present for compatibility with TCG
1247 TPMProtectionProfile ATTRIBUTE ::= {
1248     WITH SYNTAX ProtectionProfile
1249     ID tcg-at-tpmProtectionProfile }
1250
1251 TPMSecurityTarget ATTRIBUTE ::= {
1252     WITH SYNTAX SecurityTarget

```

```

1253         ID tcg-at-tpmSecurityTarget }
1254
1255 TBBProtectionProfile ATTRIBUTE ::= {
1256     WITH SYNTAX ProtectionProfile
1257     ID tcg-at-tbbProtectionProfile }
1258
1259 TBBSecurityTarget ATTRIBUTE ::= {
1260     WITH SYNTAX SecurityTarget
1261     ID tcg-at-tbbSecurityTarget }
1262
1263 ProtectionProfile ::= OBJECT IDENTIFIER
1264 SecurityTarget ::= OBJECT IDENTIFIER
1265
1266 -- These data objects are included
1267 -- in X.509 extensions using the new tcg-ce-[relevantCredentials,
1268 -- relevantManifests] OIDs.
1269
1270 HashAlgAndValue ::= SEQUENCE {
1271     hashAlg      AlgorithmIdentifier,
1272     hashValue    OCTET STRING }
1273
1274 HashedSubjectInfoURI ::= SEQUENCE {
1275     documentURI IA5String (SIZE (1..URIMAX)),
1276     documentAccessInfo OBJECT IDENTIFIER OPTIONAL,
1277     documentHashInfo HashAlgAndValue OPTIONAL }
1278
1279 SubjectInfoURIList ::=
1280     SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI
1281
1282 TCGRelevantCredentials ::=
1283     SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI
1284 TCGRelevantManifests ::=
1285     SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI
1286
1287 -- tcpa tpm specification attribute (deprecated)
1288 tcPASpecVersion ATTRIBUTE ::= {
1289     WITH SYNTAX TCPASpecVersion
1290     ID tcg-tcpaSpecVersion }
1291
1292 TCPASpecVersion ::= SEQUENCE {
1293     major INTEGER,
1294     minor INTEGER }
1295
1296 -- This extension indicates how a remote challenger can contact the (deep) attestation service
1297 -- below the current certificate holder in order to attest the layer below. Using this model allows
1298 -- the certificate of each virtualization layer to reference the attestation service for the layer
1299 -- below it. A remote challenger could traverse the layer hierarchy using this extension until
1300 -- reaching the physical trusted platform rooted attestation. The following URI is optionally
1301 -- included in a certificate for a virtual machine associated with the tcg-ce-
1302 -- virtualPlatformAttestationService extension OID. These URI are associated with the tcg-ce-
1303 -- [virtualPlatformAttestationService, migrationControllerAttestationService,
1304 -- migrationControllerRegistrationService, virtualPlatformBackupService] OIDs respectively:
1305 VirtualPlatformAttestationServiceURI ::= IA5String (SIZE (1..URIMAX))
1306 MigrationControllerAttestationServiceURI ::= IA5String (SIZE (1..URIMAX))
1307 MigrationControllerRegistrationServiceURI ::= IA5String (SIZE (1..URIMAX))
1308 VirtualPlatformBackupServiceURI ::= SEQUENCE {
1309     restoreAllowed BOOLEAN DEFAULT FALSE,
1310     backupServiceURI IA5String }
1311
1312

```

1313 5. References

- 1314 [1] TCG Glossary, <https://trustedcomputinggroup.org/glossary>
- 1315 [2] TCG Infrastructure Working Group Reference Architecture for Interoperability (Part
1316 1), Specification Version 1.0,
1317 [http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_refer-
ence_architecture_for_interoperability_specification_part_1_version_10](http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_refer-
1318 ence_architecture_for_interoperability_specification_part_1_version_10)
- 1319 [3] TCPA Main Specification, Version 1.1b,
1320 <http://www.trustedcomputinggroup.org/tcpa-main-specification-version-1-1b/>
- 1321 [4] Key words for use in RFCs to Indicate Requirement Levels, RFC 2119,
1322 www.ietf.org/rfc/rfc2119.txt
- 1323 [5] Hypertext Markup Language – 2.0, RFC 1866, www.ietf.org/rfc/rfc1866.txt
- 1324 [6] TCG Credential Profiles For TPM Family 1.2 Specification Version 1.2,
1325 [http://www.trustedcomputinggroup.org/infrastructure-work-group-tcg-credential-
profiles-specification/](http://www.trustedcomputinggroup.org/infrastructure-work-group-tcg-credential-
1326 profiles-specification/)
- 1327 [7] TCG EK Credential Profile for TPM Family 2.0, Specification Version 2.0,
1328 <http://www.trustedcomputinggroup.org/tcg-ek-credential-profile-tpm-family-2-0/>
- 1329 [8] IANA Private Enterprise Numbers, [http://www.iana.org/assignments/enterprise-
numbers/enterprise-numbers](http://www.iana.org/assignments/enterprise-
1330 numbers/enterprise-numbers)
- 1331 [9] Server Work Group Generic Server Specification, Version 1.0,
1332 [http://www.trustedcomputinggroup.org/server-work-group-generic-server-
specification-version-1-0/](http://www.trustedcomputinggroup.org/server-work-group-generic-server-
1333 specification-version-1-0/)
- 1334 [10] PC Client Platform TPM Profile (PTP) Specification ,
1335 [http://www.trustedcomputinggroup.org/pc-client-platform-tpm-profile-tp-
specification/](http://www.trustedcomputinggroup.org/pc-client-platform-tpm-profile-tp-
1336 specification/)
- 1337 [11] An Internet Attribute Certificate Profile for Authorization,
1338 www.ietf.org/rfc/rfc5755.txt
- 1339 [12] TCG Algorithm Registry, [http://www.trustedcomputinggroup.org/tcg-algorithm-
registry/](http://www.trustedcomputinggroup.org/tcg-algorithm-
1340 registry/)
- 1341 [13] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List
1342 (CRL) Profile, <https://www.ietf.org/rfc/rfc5280.txt>
- 1343 [14] TCG Platform Attribute Credential Profile Version 1.0,
1344 <https://trustedcomputinggroup.org/tcg-platform-attribute-credential-profile/>
- 1345 [15] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate
1346 and Certificate Revocation List (CRL) Profile, <https://www.ietf.org/rfc/rfc3279.txt>
- 1347 [16] Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet
1348 X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
1349 Profile, <https://www.ietf.org/rfc/rfc4055.txt>
- 1350 [17] SHA-3 Related Algorithms and Identifiers for PKIX, [https://tools.ietf.org/html/draft-
turner-lamps-adding-sha3-to-pkix-00](https://tools.ietf.org/html/draft-
1351 turner-lamps-adding-sha3-to-pkix-00)
- 1352 [18] GB/T 33560-2017. Information security technology—Cryptographic application
1353 identifier criterion specification.
1354 <http://www.spc.org.cn/gb168/online/GB%252FT%252033560-2017/>

- 1355 [19] A YANG Data Model for Hardware Management. <https://tools.ietf.org/html/rfc8348>
- 1356 [20] ITU-T X.520 Information Technology – Open Systems Interconnection – The
- 1357 Directory: Selected Attributed Types. [https://www.itu.int/rec/T-REC-X.520-201610-](https://www.itu.int/rec/T-REC-X.520-201610-1)
- 1358 [1](https://www.itu.int/rec/T-REC-X.520-201610-1)
- 1359 [21] TCG PC Client Platform TPM Profile (PTP) Specification.
- 1360 [https://trustedcomputinggroup.org/wp-](https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_Platform_TPM_Profile_PTP_2.0_r1.03_v22.pdf)
- 1361 [content/uploads/TCG_PC_Client_Platform_TPM_Profile_PTP_2.0_r1.03_v22.pdf](https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client_Platform_TPM_Profile_PTP_2.0_r1.03_v22.pdf)
- 1362 [22] TCG Registry of Reserved TPM 2.0 Handles and Localities.
- 1363 <https://trustedcomputinggroup.org/resource/registry/>
- 1364

DRAFT

1365

A. Certificate Examples

1366

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

1367

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

1368

1369

1370

1371

A.1.1 PEM Format

1372

1373

-----BEGIN ATTRIBUTE CERTIFICATE-----

1374

MIIJmDCCCIACAQEwgZaggZMwgYqkgYcwgYQxCzAJBgNVBAYTA1VTMQswCQYDVQQI

1375

DAJDQTEUMBIGAlUEBwwLU2FudGEGeQ2xhcmExGjAYBgNVBAoMEU1udGVsIENvcnBv

1376

cmF0aW9uMR4wHAYDVQQQLDBVFSyBDZXJ0aWZpY2F0ZSBJc3N1ZXIxXjFjAUBgNVBAMM

1377

DXd3dy5pbnRlbC5jb20CBDDAg3SggZ0wgZqkgZcwgZQxCzAJBgNVBAYTA1VTMQsw

1378

CQYDVQQIDAJDQTEUMBIGAlUEBwwLU2FudGEGeQ2xhcmExGjAYBgNVBAoMEU1udGVs

1379

IENvcnBvcnF0aW9uMS4wLAYDVQQQLDVCVQbGF0Zm9ybSBDbHRyaWJ1dGUgQ2VydGlm

1380

aWNhdGUgSXNzdWVYMRyWFAyDVQQDDA13d3cuaW50ZWwuY29tMA0GCSqGSIb3DQEB

1381

CwUAAhRgKWFqeST97mzBULkeg3d9H0J5mTAiGA8yMDE3MDgyMDIxMDc00FoYDzIw

1382

MjAwODIwMjEwNzQ4WjCCBK4wHAYFZ4EFAhExEzARMAkCAQICAQACASsEBAAAAAEw

1383

EgYFZ4EFAhKxCTAHBgVngQUIAjAUBgVngQUcFzELMAkCAQECAQswGccGBWeB

1384

BQITMYG9MIG6AgEAoHQWazMuMQoBBwoBAGEBAlABAYEFKgmEBQailRYraHR0cHM6

1385

Ly93d3cuaW50ZWwuY29tL3Byb3RlY3Rpb25wcm9maWxlLnBkZ0MFUwQFBgekjBYi

1386

aHR0cHM6Ly93d3cuaW50ZWwuY29tL2NjdGFyZ2V0LnBkZqENFgUxNDAtMgoBBAEB

1387

AIIBAwEBABYqaHR0cHM6Ly93d3cuaW50ZWwuY29tL2lzb2N1cnRpb24u

1388

cGRmMIIDagYHZ4EFBQEHAjGCA10wgGZ0IIC1zCCAXYwDgYGGZ4EFEgMBBAQAAAAK

1389

DAdBQkMgT0VNDAxXUjA2Wdc4NzFGVEyACUE1NTU1LTk50YEDMS4xggcrBgEEAYIs

1390

gWwH/pDIwFwYFZ4EFEQEMDKFG0jNBOjk00jEwOke1MBcGBWeBBRECD5BRj0zNzox

1391

MDpEMjpbBOKWBz6AxMA0GCysGAQQBgbAaAQIBBCBgA6M0Mv2RS2ADozQy/ZFLYAOj

1392

NDL9kUtga6M0Mv2RS6GBmTCBj6SBjDCBiTElMAkGA1UEBhMCMVVMxXjFjAUBgNVBAGM

1393

AkZMMRcwfQYDVQQHDA5GdC4gTGF1ZGVyZGFsZTEYMBYGA1UECgwPQUJDIENvcnBv

1394

cmF0aW9uMSQwIgwYDVQQQLDBtQbGF0Zm9ybSBDbDZXJ0aWZpY2F0ZSBJc3N1ZXIxXjFj

1395

BgNVBAMMC3d3dy5hYmMuY29tAgUKNUzN26YrFilodHRwczovL3d3dy5hYmMuY29t

1396

L2N1cnRzLzQzODQzODk4ODQzLmN1cjcCAVkwDgYGGZ4EFEgMBBAQAAAAvDAdYWog

1397

T0VNDA5MTUJUMzkwNERXMQXR4AJQzU1NTU1NTU1gQMzLjGCBysGAQQBgiyDAQck

1398

MjAXBgVngQURAQWOOODI6ODk6Rke6RDM6NjEwFwYFZ4EFEQIMDKQ00jgzOkI0OkYy

1399

OjC4pYg1oCuwDQYLKwYBBAGBsBoBAGEEFDQy4UFLYJc0NDI0MuFBS2CXNDQyoYGL

1400

MIGDpIGAMH4xCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJBWjEQA4GA1UEBwwHUGhv

1401

ZW5peDEUMBIGAlUECgwLWFlDIENvbXBhbnkxJDAiBgNVBAsMG1BsYXRmb3JtIEN1

1402

cnRpb24uYXR1IElzc3VlcjEUMBIGAlUEAwLd3d3Lnh5ei5jb20CAw5TSkYmFiRo

1403

dHRwczovL3d3dy54eXouY29tL2N1cnRzLzQzODQzODk5jZXXkLxYtaHR0cHM6Ly93

1404 d3cuaW50ZWwuY29tL3BsYXRmb3JtaWRlbnRpZml1cnMueG1sohswDAwEdlBybwwE
1405 dHJ1ZTALDANBTvQMBHRydWWjLhYsaHR0cHM6Ly93d3cuaW50ZWwuY29tL3BsYXRm
1406 b3JtcHJvcGVydGllcy54bWwwLAYGZ4EFBQEDMSIwIBYeaHR0cHM6Ly93d3cuaW50
1407 ZWwuY29tL1BDUnMueG1sMIICRTB8BgNVHSAEdTBzMHEGCIqGSib4TQEFAGQwYzAx
1408 BggrBgEFBQcCARYlaHR0cHM6Ly93d3cuaW50ZWwuY29tL3BsYXRjZXJ0Y3BzLnBk
1409 ZjAuBggrBgEFBQcCAjAidCBUQ0cgVHJ1c3RlZCBQbGF0Zm9ybSBFbRvcnNlbWVu
1410 dDB+BgNVHREEdzB1pHMwcTERMA8GBmeBBQUBAQwFSW50ZWwxFTATBgZngQUFAQIw
1411 CQYHKwYBBAGCVzETMBEGBmeBBQUBBAwHUzI2MDBLUDEWMBQGBmeBBQUBBQwKSDc2
1412 OTYyLTM1MDEYMBYGBmeBBQUBBgmQ1FLUDk5OTQwNjQzMIGyBgNVHTcBAf8Egacw
1413 gaQwgaGggZ6kgZswgZgxZcZAJBgNVBAYTAlVTMQswCQYDVQQUIDAJDQTEUMBIGAlUE
1414 BwwLU2FudGEGQ2xhcmeXGjAYBgNVBAoMEUluDGVsIENvcnBvcnF0aW9uMR4wHAYD
1415 VQQLDBVFSyBDZXJ0aWZpY2F0ZSBjZ3N1ZlZlIjAUBG9NVBAMMDXd3dy5pbmR1bC5j
1416 b20xEjAQBgNVBAUTCTEYODk0Mzc4NzAfbG9NVHSMEGDAWgBTUaZAmAoHVXoNLA5du
1417 q4qfj4TJgzA2BggrBgEFBQcBAQQqMCgwJgYIKwYBBQUHMAGGGmh0dHBzOi8vd3d3
1418 LmludGVsLmNvbS9vY3NwMdcGA1UdHwQwMC4wLKAQoCiGJmh0dHBzOi8vd3d3Lmlu
1419 dGVsLmNvbS9wbGF0Zm9ybWN1cnQuY3JsMA0GCSqGSib3DQEBcWUAA4IBAQCq6w/S
1420 /cuB8mUjI1Vli2JPfkbS+v2Tmbf0sIUPdPfu/aH16NPctavfiEvpF11uWGty7/oY
1421 8sAq5ChEU3/KbI0zaY7X0Yjpcp5YfyZzFqgrDmye+o5T5+sAnJOjNrHdIEUGyYH
1422 G47IsogmJj7i1lRcF7JVCJTUOGQpWqVMKF3/VffWJ84XKE+nbTYCyufyYHRxUQ1T
1423 rSx5sQn0dAnW8BdljczpANJBdxdlCdhKefZSwf3Yc550d3QDqMekH/3++9MJhJO
1424 79BiL0CkXi5gAYLi5NU14X9S/Jv+hcaDwi/gEtB5s7c3rtEyoYByj//QycQhxMIb
1425 L2ciOd1FDte7CSyC
1426 -----END ATTRIBUTE CERTIFICATE-----
1427

A.1.2 DER Format

1428
1429
1430 SEQUENCE :
1431 SEQUENCE :
1432 INTEGER : 1
1433 SEQUENCE :
1434 CONTEXT SPECIFIC (0) :
1435 SEQUENCE :
1436 CONTEXT SPECIFIC (4) :
1437 SEQUENCE :
1438 SET :
1439 SEQUENCE :
1440 OBJECT IDENTIFIER : countryName [2.5.4.6]
1441 PRINTABLE STRING : 'US'
1442 SET :
1443 SEQUENCE :
1444 OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
1445 UTF8 STRING : 'CA'
1446 SET :
1447 SEQUENCE :
1448 OBJECT IDENTIFIER : localityName [2.5.4.7]
1449 UTF8 STRING : 'Santa Clara'
1450 SET :

```

1451         SEQUENCE :
1452             OBJECT IDENTIFIER : organizationName [2.5.4.10]
1453             UTF8 STRING : 'Intel Corporation'
1454     SET :
1455         SEQUENCE :
1456             OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
1457             UTF8 STRING : 'EK Certificate Issuer'
1458     SET :
1459         SEQUENCE :
1460             OBJECT IDENTIFIER : commonName [2.5.4.3]
1461             UTF8 STRING : 'www.intel.com'
1462     INTEGER : 926974836
1463     CONTEXT SPECIFIC (0) :
1464     SEQUENCE :
1465         CONTEXT SPECIFIC (4) :
1466         SEQUENCE :
1467             SET :
1468                 SEQUENCE :
1469                     OBJECT IDENTIFIER : countryName [2.5.4.6]
1470                     PRINTABLE STRING : 'US'
1471             SET :
1472                 SEQUENCE :
1473                     OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
1474                     UTF8 STRING : 'CA'
1475             SET :
1476                 SEQUENCE :
1477                     OBJECT IDENTIFIER : localityName [2.5.4.7]
1478                     UTF8 STRING : 'Santa Clara'
1479             SET :
1480                 SEQUENCE :
1481                     OBJECT IDENTIFIER : organizationName [2.5.4.10]
1482                     UTF8 STRING : 'Intel Corporation'
1483             SET :
1484                 SEQUENCE :
1485                     OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
1486                     UTF8 STRING : 'Platform Attribute Certificate Issuer'
1487             SET :
1488                 SEQUENCE :
1489                     OBJECT IDENTIFIER : commonName [2.5.4.3]
1490                     UTF8 STRING : 'www.intel.com'
1491     SEQUENCE :
1492         OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]
1493     NULL :
1494     INTEGER : 602967EA7924FDEE6CC150B91E83777D1F427999
1495     SEQUENCE :
1496         GENERALIZED TIME : '20170820210748Z'
1497         GENERALIZED TIME : '20200820210748Z'
1498     SEQUENCE :
1499         SEQUENCE :
1500             OBJECT IDENTIFIER : [2.23.133.2.17]
1501         SET :
1502             SEQUENCE :
1503                 SEQUENCE :
1504                     INTEGER : 2
1505                     INTEGER : 0
1506                     INTEGER : 43
1507                 OCTET STRING : 00000001
1508         SEQUENCE :
1509             OBJECT IDENTIFIER : [2.23.133.2.25]
1510         SET :
1511             SEQUENCE :
1512                 OBJECT IDENTIFIER : [2.23.133.8.2]
1513     SEQUENCE :

```



```
1514 OBJECT IDENTIFIER : [2.23.133.2.23]
1515 SET :
1516 SEQUENCE :
1517 INTEGER : 1
1518 INTEGER : 1
1519 INTEGER : 11
1520 SEQUENCE :
1521 OBJECT IDENTIFIER : [2.23.133.2.19]
1522 SET :
1523 SEQUENCE :
1524 INTEGER : 0
1525 CONTEXT SPECIFIC (0) :
1526 IA5 STRING : '3.1'
1527 ENUMERATED : '07'
1528 ENUMERATED : '02'
1529 BOOLEAN : '00'
1530 CONTEXT SPECIFIC (0) : 01
1531 CONTEXT SPECIFIC (1) : 2A03040506
1532 CONTEXT SPECIFIC (2) :
1533 IA5 STRING : 'https://www.intel.com/protectionprofile.pdf'
1534 CONTEXT SPECIFIC (3) : 5304050607
1535 CONTEXT SPECIFIC (4) :
1536 IA5 STRING : 'https://www.intel.com/cctarget.pdf'
1537 CONTEXT SPECIFIC (1) :
1538 IA5 STRING : '140-2'
1539 ENUMERATED : '04'
1540 BOOLEAN : '00'
1541 CONTEXT SPECIFIC (2) : 03
1542 BOOLEAN : '00'
1543 IA5 STRING : 'https://www.intel.com/isocertification.pdf'
1544 SEQUENCE :
1545 OBJECT IDENTIFIER : [2.23.133.5.1.7.2]
1546 SET :
1547 SEQUENCE :
1548 CONTEXT SPECIFIC (0) :
1549 SEQUENCE :
1550 SEQUENCE :
1551 OBJECT IDENTIFIER : [2.23.133.18.3.1]
1552 OCTET STRING : 0000000A
1553 UTF8 STRING : 'ABC OEM'
1554 UTF8 STRING : 'WR06X7871FTL'
1555 CONTEXT SPECIFIC (0) : 41353535352D393939
1556 CONTEXT SPECIFIC (1) : 312E31
1557 CONTEXT SPECIFIC (2) : 2B06010401822C
1558 CONTEXT SPECIFIC (3) : FF
1559 CONTEXT SPECIFIC (4) :
1560 SEQUENCE :
1561 OBJECT IDENTIFIER : [2.23.133.17.1]
1562 UTF8 STRING : 'AF:3A:94:10:A5'
1563 SEQUENCE :
1564 OBJECT IDENTIFIER : [2.23.133.17.2]
1565 UTF8 STRING : 'AF:37:10:D2:A8'
1566 CONTEXT SPECIFIC (5) :
1567 CONTEXT SPECIFIC (0) :
1568 SEQUENCE :
1569 OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
1570 OCTET STRING :
1571 6003A33432FD914B6003A33432FD914B6003A33432FD914B6003A33432FD914B
1572 CONTEXT SPECIFIC (1) :
1573 SEQUENCE :
1574 CONTEXT SPECIFIC (4) :
1575 SEQUENCE :
1576 SET :
```

```

1577 SEQUENCE :
1578     OBJECT IDENTIFIER : countryName [2.5.4.6]
1579     PRINTABLE STRING : 'US'
1580 SET :
1581     SEQUENCE :
1582     OBJECT IDENTIFIER : stateOrProvinceName
1583 [2.5.4.8]
1584     UTF8 STRING : 'FL'
1585 SET :
1586     SEQUENCE :
1587     OBJECT IDENTIFIER : localityName [2.5.4.7]
1588     UTF8 STRING : 'Ft. Lauderdale'
1589 SET :
1590     SEQUENCE :
1591     OBJECT IDENTIFIER : organizationName
1592 [2.5.4.10]
1593     UTF8 STRING : 'ABC Corporation'
1594 SET :
1595     SEQUENCE :
1596     OBJECT IDENTIFIER : organizationalUnitName
1597 [2.5.4.11]
1598     UTF8 STRING : 'Platform Certificate Issuer'
1599 SET :
1600     SEQUENCE :
1601     OBJECT IDENTIFIER : commonName [2.5.4.3]
1602     UTF8 STRING : 'www.abc.com'
1603     INTEGER : 43843898843
1604     CONTEXT SPECIFIC (6) :
1605     IA5 STRING : 'https://www.abc.com/certs/43843898843.cer'
1606 SEQUENCE :
1607     SEQUENCE :
1608     OBJECT IDENTIFIER : [2.23.133.18.3.1]
1609     OCTET STRING : 000002F
1610     UTF8 STRING : 'XYZ OEM'
1611     UTF8 STRING : 'LMBT3904DWT1G'
1612     CONTEXT SPECIFIC (0) : 43353535352D353535
1613     CONTEXT SPECIFIC (1) : 332E31
1614     CONTEXT SPECIFIC (2) : 2B06010401822C
1615     CONTEXT SPECIFIC (3) : 00
1616     CONTEXT SPECIFIC (4) :
1617     SEQUENCE :
1618     OBJECT IDENTIFIER : [2.23.133.17.1]
1619     UTF8 STRING : '82:89:FA:D3:61'
1620     SEQUENCE :
1621     OBJECT IDENTIFIER : [2.23.133.17.2]
1622     UTF8 STRING : 'D4:83:B4:F2:78'
1623     CONTEXT SPECIFIC (5) :
1624     CONTEXT SPECIFIC (0) :
1625     SEQUENCE :
1626     OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
1627     OCTET STRING : 3432E1414B60973434323432E1414B6097343432
1628     CONTEXT SPECIFIC (1) :
1629     SEQUENCE :
1630     CONTEXT SPECIFIC (4) :
1631     SEQUENCE :
1632     SET :
1633     SEQUENCE :
1634     OBJECT IDENTIFIER : countryName [2.5.4.6]
1635     PRINTABLE STRING : 'US'
1636     SET :
1637     SEQUENCE :
1638     OBJECT IDENTIFIER : stateOrProvinceName
1639 [2.5.4.8]

```



```

1703     SET :
1704         SEQUENCE :
1705             OBJECT IDENTIFIER : [2.23.133.5.1.2]
1706             SEQUENCE : OBJECT IDENTIFIER : [1.3.6.1.4.1.343]
1707     SET :
1708         SEQUENCE :
1709             OBJECT IDENTIFIER : [2.23.133.5.1.4]
1710             UTF8 STRING : 'S2600KP'
1711     SET :
1712         SEQUENCE :
1713             OBJECT IDENTIFIER : [2.23.133.5.1.5]
1714             UTF8 STRING : 'H76962-350'
1715     SET :
1716         SEQUENCE :
1717             OBJECT IDENTIFIER : [2.23.133.5.1.6]
1718             UTF8 STRING : 'BQKP99940643'
1719 SEQUENCE :
1720     OBJECT IDENTIFIER : [2.5.29.55]
1721     BOOLEAN : 'FF'
1722     OCTET STRING :
1723         SEQUENCE :
1724             SEQUENCE :
1725                 CONTEXT SPECIFIC (0) :
1726                 CONTEXT SPECIFIC (4) :
1727                     SEQUENCE :
1728                         SET :
1729                             SEQUENCE :
1730                                 OBJECT IDENTIFIER : countryName [2.5.4.6]
1731                                 PRINTABLE STRING : 'US'
1732                         SET :
1733                             SEQUENCE :
1734                                 OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
1735                                 UTF8 STRING : 'CA'
1736                         SET :
1737                             SEQUENCE :
1738                                 OBJECT IDENTIFIER : localityName [2.5.4.7]
1739                                 UTF8 STRING : 'Santa Clara'
1740                         SET :
1741                             SEQUENCE :
1742                                 OBJECT IDENTIFIER : organizationName [2.5.4.10]
1743                                 UTF8 STRING : 'Intel Corporation'
1744                         SET :
1745                             SEQUENCE :
1746                                 OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
1747                                 UTF8 STRING : 'EK Certificate Issuer'
1748                         SET :
1749                             SEQUENCE :
1750                                 OBJECT IDENTIFIER : commonName [2.5.4.3]
1751                                 UTF8 STRING : 'www.intel.com'
1752                         SET :
1753                             SEQUENCE :
1754                                 OBJECT IDENTIFIER : serialNumber [2.5.4.5]
1755                                 PRINTABLE STRING : '128943787'
1756 SEQUENCE :
1757     OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
1758     OCTET STRING :
1759         SEQUENCE :
1760             CONTEXT SPECIFIC (0) : D46990260281D55E834B03976EAB8A9F8F84C983
1761 SEQUENCE :
1762     OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
1763     OCTET STRING :
1764         SEQUENCE :
1765             SEQUENCE :

```

```

1766         OBJECT IDENTIFIER : omsp [1.3.6.1.5.5.7.48.1]
1767         CONTEXT SPECIFIC (6) : 'https://www.intel.com/ocsp'
1768     SEQUENCE :
1769         OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
1770         OCTET STRING :
1771             SEQUENCE :
1772                 SEQUENCE :
1773                     CONTEXT SPECIFIC (0) :
1774                     CONTEXT SPECIFIC (0) :
1775                     CONTEXT SPECIFIC (6) : 'https://www.intel.com/platformcert.crl'
1776     SEQUENCE :
1777         OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]
1778     NULL :
1779     BIT STRING UnusedBits:0 :
1780     AAEB0FD2FDCB81F265232255658B624F7E46D2FAFD939817F4B085
1781     0F74F7D4FDA1F5E8D3DCB5ABDF884BE93E5D6E586B72E9FA18F2C0
1782     2AE42844537FCA6C8D33698ED7D188E9729E587D8A99645AA0AC39
1783     B27BEA394F9FAC02724E8CDAC77481141B26071B8EC8B28826263E
1784     E2D6545C17B2550894D43864295AA54C285DFF55F7D627CE17284F
1785     A76D360262E7F2607471510D53AD2C79B109F47409D6F017658DCF
1786     B3A5A349043C5D94276129E7D94B07F761CE79D1DDD00EA31E907F
1787     F7FBEF4C26124EEFD0622F40A45E2E600182E2E4D525E17F52FC9B
1788     FE85C6835A2FE012D079B3B737AED132A180728FFFD0C9C421C4C2
1789     1B2F672239DD450ED7BB092C82
1790
1791

```

1792 A.2 Example 2 (Delta Platform Certificate in Attribute Certificate 1793 Format)

1794 The following section provides an example of a Delta Platform Certificate in Attribute
1795 Certificate format (RFC 5755) [11]. The PEM encoded version of the certificate as well as the
1796 ASN.1 certificate text are included for convenience. The values used in this example are for
1797 illustrative purposes and must be replaced with manufacturer-specific data.

1798 A.2.1 PEM Format

```

1799 -----BEGIN ATTRIBUTE CERTIFICATE-----
1800
1801 MIIKkzCCCXsCAQEwgbaggbMwgZqkgZcwqZQxCzAJBgNVBAYTAlVTMQswCQYDVQQLI
1802 DAJDQTEUMBIGAlUEBwwLU2FudGEGeQ2xhcmExGjAYBgNVBAoMEU1udGVsIENvcnBv
1803 cmF0aW9uMS4wLAYDVQQQLDCVQbGF0Zm9ybSBBdHRyaWJ1dGUGQ2VydG1maWNhdGUG
1804 SXNzdWVYMRywFAYDVQQDDA13d3cuaW50ZWwuY29tAhRgKWfqeST97mzBULkeg3d9
1805 H0J5maCBpDCBoaSBnjCBmzELMAkGAlUEBhMVCVVMxCzAJBgNVBAGMAlRYMQ8wDQYD
1806 VQQHDAZBdXN0aW4xZm9ybSBBdHRyaWJ1dGUGQ2VydG1maWNhdGUGSXNzdWVYMR8wHQYD
1807 ZWx0YSBQbGF0Zm9ybSBBdHRyaWJ1dGUGQ2VydG1maWNhdGUGSXNzdWVYMR8wHQYD
1808 VQQDBBZ3d3cueH16aW50ZWdyYXRvcnMuY29tMA0GCSqGSIb3DQEBCwUAAgQCFFpCE
1809 MCIYdZiWMTgxMDE1MjEwODEwXWhgPMjAyMDA4MjAyMTA4MTFfAmIIFeDASBgVngQUC
1810 GTEJMAcGBWeBBQgFMBQGBWeBBQIXMQswCQIBAQIBAQIBDTCCBRAGB2eBBQUUBwIx
1811 ggUDMIIIE/6CCBF0wggF5MA4GBmeBBRIDAQQEAAAACgwHQUJDIE9FTQwMV1IwNlg3
1812 ODcxRlRmGAlBNTU1NS050TmBAZeuMYIHKwYBBAGCLIMB/6QyMbcGBWeBBREBDA5B
1813 RjjozQTo5ND0xMDpBNTAXBgVngQURAgwOQUY6Mzc6MTA6RDI6QTilgc+gMTANBgSr
1814 BgEEAYGwGgECAQQgYAOjNDL9kUtG6M0Mv2RS2ADozQy/ZFLYAOjNDL9kUuhgZkw

```

1815 gY+kgYwWgYkxCzAJBgNVBAYTA1VMTQswCQYDVQQLIDAJGTDEXMBUGA1UEBwwORnQu
1816 IExhdWRlcmRhbGUxGDAWBgNVBAoMD0FCQyBDb3Jwb3JhdGlvbGJkMCIGA1UECwwb
1817 UGxhdGZvcmlkZWVudG1maWNhdGUgSXNzdWVYMRQwEgYDVQDDAt3d3cuYwJjLmNv
1818 bQIFCjVzZm93d3cuYwJjLmNvbS9jZXJ0cy80Mzg0Mzg5ODg0
1819 My5jZXXKHAQIwggF8MA4GBmeBBRIDAQQEAAAAQW0Q29tcG9uZW50IENvcnAMCVhU
1820 OTgyODdMTIAHRjk4MS0wMYEDMI4xggcrBgEEAYNIgWH/pDIwFwYFZ4EFEQIMDjcz
1821 Oj1COjkyOjQwOkZBMBcGBWeBBREDDA4xMzozRj05ODpDNT010aWBzaAxMA0GCysG
1822 AQQBgbAaAQIBBCCYqtWRg/qrkZiq1ZGD+quRmKrVkyP6q5GYqtWRg/qrkaGBlzCB
1823 jqsBzCBiDELMAkGA1UEBhmCVVMxZCZAJBgNVBAGMAkNBMRwDwYDVQHQDAhTYW4g
1824 Sm9zZTEXMBUGA1UECgwOQ29tcG9uZW50IENvcnAxJDAiBgNVBAsMG1BsYXRmb3Jt
1825 IENlcnpZmljYXRlIElzc3VlcjEaMBGGA1UEAwRd3d3LmNvbXBvbmVudC5jb20C
1826 BAXek66mLhYsaHR0cHM6Ly93d3cuY29tcG9uZW50LmNvbS9jZXJ0cy85ODQ3Mjg3
1827 OC5jZXXKHAQAwggF8MA4GBmeBBRIDAQQEAAAALwHWF1aIE9FTQwOTE1CVDM5MDRE
1828 VzFUMUeACUM1NTU1LTU1NYEDNC4wggcrBgEEAYIsgeApDIwFwYFZ4EFEQEMDjgy
1829 Ojg5OkZBOKzOjYxMBCGBWeBBRECD5END04MzpcNDpGMjo3OKWBtaAlMA0GCysG
1830 AQQBgbAaAQIBBBQ0MuFBS2CXNDQyNDLhQUtglzQ0MqGBizCBg6SBgDB+MQswCQYD
1831 VQQGEwJVUzELMAkGA1UECAwCQVoxEDAObgNVBAcMB1Bob2VuaXgxZDASBgNVBAoM
1832 ClhZQyBDb21wYW55MSQwIgyYDVQQLDBtQbGF0Zm9ybSBBDXJ0aWZpY2F0ZSBJc3N1
1833 ZXIxZDASBgNVBAMMC3d3dy54eXouY29tcG9uZW50LmNvbS9jZXJ0cy85ODQ3Mjg3
1834 LmNvbS9jZXJ0cy85Mzg5MjguY2VyhWBoTgWNmh0dHBzOi8vd3d3Lnh5emludGVn
1835 cmF0b3JzLmNvbS9wbGF0Zm9ybWlkZW50aWZpZXJzLnhtbKIipMBYMC1RTQyBFbFi
1836 bGVkDAR0cnVlgAEAMA8MA0FNVAwFzZmFsc2WAAQgjNxY1aHR0cHM6Ly93d3cuY29tcG9uZW50ZwdyYXRvcnMuY29tL3BsYXRmb3JtcHJvcGVydGllcy54bWwvOAYGZ4EFBQED
1837 aW50ZWdyYXRvcnMuY29tL3BsYXRmb3JtcHJvcGVydGllcy54bWwvOAYGZ4EFBQED
1838 MS4wLBYqaHR0cHM6Ly93d3cuY29tcG9uZW50ZwdyYXRvcnMuY29tL1BDUnNfVjIueG1s
1839 MIICXzCBgwYDVR0gBHwwejB4BggqhkiXJwMBAjBsmDoGCCsGAQUFBwIBFi5odHRw
1840 czovL3d3dy54eXppbnRlZ3JhdG9y5j5jb20vcGxhdGNlcjRjchMucGRmMC4GCCsG
1841 AQUFBwICMCIIFRDRyBUcnVzdGVkIFBsYXRmb3JtIEVuZG9yc2VtZW50MH4GA1Ud
1842 EQR3MHWkczBxMREwDwYGZ4EFBQEEDAVJbnRlbDEVMBMGbmeBBQUBAjAJBgcrBgEE
1843 AYJXMRMwEYQZ4EFBQEEDAdTMjYwMETQMRyWfAYGZ4EFBQEFDAPINzY5NjItMzUw
1844 MRgwFgYGZ4EFBQEGDAXCUUtQOTk5NDA2NDMwgbIGA1UdNwEB/wSBpzCBpDCBoaCB
1845 nqSBmzCBmDELMAkGA1UEBhmCVVMxZCZAJBgNVBAGMA1RYMQ8wDQYDVQHQDAZBdXN0
1846 aW4xZfzAVBgNVBAoMDlhZW1BjbnRlZ3JhdG9yMR4wHAYDVQQLDBVFSyBDZXJ0aWZp
1847 Y2F0ZSBJc3N1ZXIxHzaDgNVBAMMFnd3dy54eXppbnRlZ3JhdG9y5j5jb20xETAP
1848 BgNVBAUTCdMyODczODcyMB8GA1UdIwQYMBaAFNRpkCYCgdVeg0sDl26rip+PhMmD
1849 MD8GCCsGAQUFBwEBBDMwMTAvBggrBgEFBQcwAYYjaHR0cHM6Ly93d3cuY29tcG9uZW50ZwdyYXRvcnMuY29tL29jc3AQAQYDVROfBDkwnZa1oD0gMYyvaHR0cHM6Ly93d3cu
1850 ZWdyYXRvcnMuY29tL29jc3AQAQYDVROfBDkwnZa1oD0gMYyvaHR0cHM6Ly93d3cu
1851 eHl6aW50ZWdyYXRvcnMuY29tL3BsYXRmb3JtY2VydC5jcmwwDQYJKoZIhvcNAQEL
1852 BQADggEBAGx3K17RCixE32TPB4u52TeoQxla9zROywtOAVDLa0Na4mfqmt3mTYuE
1853 hkCbYnYX9sqa0KCYmBTTj07Lnd007UisQsx8vKTDDVQ6E3etxeeqdiY8g4Rv+t1
1854 nC8Hna+UZ+Lv+rUze/FaOiXH4rn6kxK7jsGe21VIC7qvIzWnjcF5kgxOQ3SqFmWJ


```

1914         SET :
1915             SEQUENCE :
1916                 OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
1917                 UTF8 STRING : 'Delta Platform Attribute Certificate Issuer'
1918         SET :
1919             SEQUENCE :
1920                 OBJECT IDENTIFIER : commonName [2.5.4.3]
1921                 UTF8 STRING : 'www.xyzintegrators.com'
1922 SEQUENCE :
1923     OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]
1924     NULL :
1925     INTEGER : 34928388
1926 SEQUENCE :
1927     GENERALIZED TIME : '20181015210811Z'
1928     GENERALIZED TIME : '20200820210811Z'
1929 SEQUENCE :
1930     SEQUENCE :
1931         OBJECT IDENTIFIER : [2.23.133.2.25]
1932     SET :
1933         SEQUENCE :
1934             OBJECT IDENTIFIER : [2.23.133.8.5]
1935 SEQUENCE :
1936     OBJECT IDENTIFIER : [2.23.133.2.23]
1937     SET :
1938         SEQUENCE :
1939             INTEGER : 1
1940             INTEGER : 1
1941             INTEGER : 13
1942 SEQUENCE :
1943     OBJECT IDENTIFIER : [2.23.133.5.1.7.2]
1944     SET :
1945         SEQUENCE :
1946             CONTEXT SPECIFIC (0) :
1947                 SEQUENCE :
1948                     SEQUENCE :
1949                         OBJECT IDENTIFIER : [2.23.133.18.3.1]
1950                         OCTET STRING : 0000000A
1951                         UTF8 STRING : 'ABC OEM'
1952                         UTF8 STRING : 'WR06X7871FTL'
1953                         CONTEXT SPECIFIC (0) : 41353535352D393939
1954                         CONTEXT SPECIFIC (1) : 312E31
1955                         CONTEXT SPECIFIC (2) : 2B06010401822C
1956                         CONTEXT SPECIFIC (3) : FF
1957                         CONTEXT SPECIFIC (4) :
1958                     SEQUENCE :
1959                         OBJECT IDENTIFIER : [2.23.133.17.1]
1960                         UTF8 STRING : 'AF:3A:94:10:A5'
1961                     SEQUENCE :
1962                         OBJECT IDENTIFIER : [2.23.133.17.2]
1963                         UTF8 STRING : 'AF:37:10:D2:A8'
1964                     CONTEXT SPECIFIC (5) :
1965                     CONTEXT SPECIFIC (0) :
1966                     SEQUENCE :
1967                         OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
1968                     OCTET STRING :
1969 6003A33432FD914B6003A33432FD914B6003A33432FD914B6003A33432FD914B :
1970                     CONTEXT SPECIFIC (1) :
1971                     SEQUENCE :
1972                         CONTEXT SPECIFIC (4) :
1973                         SEQUENCE :
1974                         SET :
1975                         SEQUENCE :
1976                             OBJECT IDENTIFIER : countryName [2.5.4.6]

```



```

1977          PRINTABLE STRING : 'US'
1978
1979          SET :
1980              SEQUENCE :
1981                  OBJECT IDENTIFIER : stateOrProvinceName
1982 [2.5.4.8]
1983                  UTF8 STRING : 'FL'
1984          SET :
1985              SEQUENCE :
1986                  OBJECT IDENTIFIER : localityName [2.5.4.7]
1987                  UTF8 STRING : 'Ft. Lauderdale'
1988          SET :
1989              SEQUENCE :
1990                  OBJECT IDENTIFIER : organizationName [2.5.4.10]
1991                  UTF8 STRING : 'ABC Corporation'
1992          SET :
1993              SEQUENCE :
1994                  OBJECT IDENTIFIER : organizationalUnitName
1995 [2.5.4.11]
1996                  UTF8 STRING : 'Platform Certificate Issuer'
1997          SET :
1998              SEQUENCE :
1999                  OBJECT IDENTIFIER : commonName [2.5.4.3]
2000                  UTF8 STRING : 'www.abc.com'
2001          INTEGER : 43843898843
2002          CONTEXT SPECIFIC (6) :
2003              IA5 STRING : 'https://www.abc.com/certs/43843898843.cer'
2004          CONTEXT SPECIFIC (7) : 02
2005          SEQUENCE :
2006              SEQUENCE :
2007                  OBJECT IDENTIFIER : [2.23.133.18.3.1]
2008                  OCTET STRING : 00000041
2009                  UTF8 STRING : 'Component Corp'
2010                  UTF8 STRING : 'XT98287LL'
2011          CONTEXT SPECIFIC (0) : 463938312D3031
2012          CONTEXT SPECIFIC (1) : 322E31
2013          CONTEXT SPECIFIC (2) : 2B060104018348
2014          CONTEXT SPECIFIC (3) : FF
2015          CONTEXT SPECIFIC (4) :
2016              SEQUENCE :
2017                  OBJECT IDENTIFIER : [2.23.133.17.2]
2018                  UTF8 STRING : '73:9B:92:40:FA'
2019              SEQUENCE :
2020                  OBJECT IDENTIFIER : [2.23.133.17.3]
2021                  UTF8 STRING : '13:3F:98:C5:59'
2022          CONTEXT SPECIFIC (5) :
2023          CONTEXT SPECIFIC (0) :
2024              SEQUENCE :
2025                  OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
2026                  OCTET STRING :
2027          98AAD59183FAAB9198AAD59183FAAB9198AAD59183FAAB9198AAD59183FAAB91
2028          CONTEXT SPECIFIC (1) :
2029              SEQUENCE :
2030                  CONTEXT SPECIFIC (4) :
2031              SEQUENCE :
2032          SET :
2033              SEQUENCE :
2034                  OBJECT IDENTIFIER : countryName [2.5.4.6]
2035                  PRINTABLE STRING : 'US'
2036          SET :
2037              SEQUENCE :
2038                  OBJECT IDENTIFIER : stateOrProvinceName
2039 [2.5.4.8]
                UTF8 STRING : 'CA'

```

```

2040 SET :
2041 SEQUENCE :
2042 OBJECT IDENTIFIER : localityName [2.5.4.7]
2043 UTF8 STRING : 'San Jose'
2044 SET :
2045 SEQUENCE :
2046 OBJECT IDENTIFIER : organizationName [2.5.4.10]
2047 UTF8 STRING : 'Component Corp'
2048 SET :
2049 SEQUENCE :
2050 OBJECT IDENTIFIER : organizationalUnitName
2051 [2.5.4.11] UTF8 STRING : 'Platform Certificate Issuer'
2052 SET :
2053 SEQUENCE :
2054 OBJECT IDENTIFIER : commonName [2.5.4.3]
2055 UTF8 STRING : 'www.component.com'
2056 INTEGER : 98472878
2057 CONTEXT SPECIFIC (6) :
2058 IA5 STRING : 'https://www.component.com/certs/98472878.cer'
2059 CONTEXT SPECIFIC (7) : 00
2060 SEQUENCE :
2061 SEQUENCE :
2062 OBJECT IDENTIFIER : [2.23.133.18.3.1]
2063 OCTET STRING : 0000002F
2064 UTF8 STRING : 'XYZ OEM'
2065 UTF8 STRING : 'LMBT3904DW1T1G'
2066 CONTEXT SPECIFIC (0) : 43353535352D353535
2067 CONTEXT SPECIFIC (1) : 342E30
2068 CONTEXT SPECIFIC (2) : 2B06010401822C
2069 CONTEXT SPECIFIC (3) : 00
2070 CONTEXT SPECIFIC (4) :
2071 SEQUENCE :
2072 OBJECT IDENTIFIER : [2.23.133.17.1]
2073 UTF8 STRING : '82:89:FA:D3:61'
2074 SEQUENCE :
2075 OBJECT IDENTIFIER : [2.23.133.17.2]
2076 UTF8 STRING : 'D4:83:B4:F2:78'
2077 CONTEXT SPECIFIC (5) :
2078 CONTEXT SPECIFIC (0) :
2079 SEQUENCE :
2080 OBJECT IDENTIFIER : [1.3.6.1.4.1.22554.1.2.1]
2081 OCTET STRING : 3432E1414B60973434323432E1414B6097343432
2082 CONTEXT SPECIFIC (1) :
2083 SEQUENCE :
2084 CONTEXT SPECIFIC (4) :
2085 SEQUENCE :
2086 SET :
2087 SEQUENCE :
2088 OBJECT IDENTIFIER : countryName [2.5.4.6]
2089 PRINTABLE STRING : 'US'
2090 SET :
2091 SEQUENCE :
2092 OBJECT IDENTIFIER : stateOrProvinceName
2093 [2.5.4.8] UTF8 STRING : 'AZ'
2094 SET :
2095 SEQUENCE :
2096 OBJECT IDENTIFIER : localityName [2.5.4.7]
2097 UTF8 STRING : 'Phoenix'
2098 SET :
2099 SEQUENCE :
2100 OBJECT IDENTIFIER : organizationName [2.5.4.10]
2101
2102

```

```
2103 UTF8 STRING : 'XYC Company'
2104 SET :
2105 SEQUENCE :
2106 OBJECT IDENTIFIER : organizationalUnitName
2107 [2.5.4.11]
2108 UTF8 STRING : 'Platform Certificate Issuer'
2109 SET :
2110 SEQUENCE :
2111 OBJECT IDENTIFIER : commonName [2.5.4.3]
2112 UTF8 STRING : 'www.xyz.com'
2113 INTEGER : 938928
2114 CONTEXT SPECIFIC (6) :
2115 IA5 STRING : 'https://www.xyz.com/certs/938928.cer'
2116 CONTEXT SPECIFIC (7) : 01
2117 CONTEXT SPECIFIC (1) :
2118 IA5 STRING : 'https://www.xyzintegrators.com/platformidentifiers.xml'
2119 CONTEXT SPECIFIC (2) :
2120 SEQUENCE :
2121 UTF8 STRING : 'TSC Enabled'
2122 UTF8 STRING : 'true'
2123 CONTEXT SPECIFIC (0) : 00
2124 SEQUENCE :
2125 UTF8 STRING : 'AMT'
2126 UTF8 STRING : 'false'
2127 CONTEXT SPECIFIC (0) : 01
2128 CONTEXT SPECIFIC (3) :
2129 IA5 STRING : 'https://www.xyzintegrators.com/platformproperties.xml'
2130 SEQUENCE :
2131 OBJECT IDENTIFIER : [2.23.133.5.1.3]
2132 SET :
2133 SEQUENCE :
2134 IA5 STRING : 'https://www.xyzintegrators.com/PCRs_V2.xml'
2135 SEQUENCE :
2136 SEQUENCE :
2137 OBJECT IDENTIFIER : certificatePolicies [2.5.29.32]
2138 OCTET STRING :
2139 SEQUENCE :
2140 SEQUENCE :
2141 OBJECT IDENTIFIER : [1.2.840.2983.3.1.2]
2142 SEQUENCE :
2143 SEQUENCE :
2144 OBJECT IDENTIFIER : cps [1.3.6.1.5.5.7.2.1]
2145 IA5 STRING : 'https://www.xyzintegrators.com/platcertcps.pdf'
2146 SEQUENCE :
2147 OBJECT IDENTIFIER : unotice [1.3.6.1.5.5.7.2.2]
2148 SEQUENCE :
2149 UTF8 STRING : 'TCG Trusted Platform Endorsement'
2150 SEQUENCE :
2151 OBJECT IDENTIFIER : subjectAltName [2.5.29.17]
2152 OCTET STRING :
2153 SEQUENCE :
2154 CONTEXT SPECIFIC (4) :
2155 SEQUENCE :
2156 SET :
2157 SEQUENCE :
2158 OBJECT IDENTIFIER : [2.23.133.5.1.1]
2159 UTF8 STRING : 'Intel'
2160 SET :
2161 SEQUENCE :
2162 OBJECT IDENTIFIER : [2.23.133.5.1.2]
2163 SEQUENCE :
2164 OBJECT IDENTIFIER : [1.3.6.1.4.1.343]
2165 SET :
```

```

2166         SEQUENCE :
2167             OBJECT IDENTIFIER : [2.23.133.5.1.4]
2168             UTF8 STRING : 'S2600KP'
2169     SET :
2170         SEQUENCE :
2171             OBJECT IDENTIFIER : [2.23.133.5.1.5]
2172             UTF8 STRING : 'H76962-350'
2173     SET :
2174         SEQUENCE :
2175             OBJECT IDENTIFIER : [2.23.133.5.1.6]
2176             UTF8 STRING : 'BQKP99940643'
2177 SEQUENCE :
2178     OBJECT IDENTIFIER : [2.5.29.55]
2179     BOOLEAN : 'FF'
2180     OCTET STRING :
2181     SEQUENCE :
2182     SEQUENCE :
2183         CONTEXT SPECIFIC (0) :
2184         CONTEXT SPECIFIC (4) :
2185             SEQUENCE :
2186             SET :
2187                 SEQUENCE :
2188                     OBJECT IDENTIFIER : countryName [2.5.4.6]
2189                     PRINTABLE STRING : 'US'
2190             SET :
2191                 SEQUENCE :
2192                     OBJECT IDENTIFIER : stateOrProvinceName [2.5.4.8]
2193                     UTF8 STRING : 'TX'
2194             SET :
2195                 SEQUENCE :
2196                     OBJECT IDENTIFIER : localityName [2.5.4.7]
2197                     UTF8 STRING : 'Austin'
2198             SET :
2199                 SEQUENCE :
2200                     OBJECT IDENTIFIER : organizationName [2.5.4.10]
2201                     UTF8 STRING : 'XYZ Integrator'
2202             SET :
2203                 SEQUENCE :
2204                     OBJECT IDENTIFIER : organizationalUnitName [2.5.4.11]
2205                     UTF8 STRING : 'EK Certificate Issuer'
2206             SET :
2207                 SEQUENCE :
2208                     OBJECT IDENTIFIER : commonName [2.5.4.3]
2209                     UTF8 STRING : 'www.xyzintegrators.com'
2210             SET :
2211                 SEQUENCE :
2212                     OBJECT IDENTIFIER : serialNumber [2.5.4.5]
2213                     PRINTABLE STRING : '32873872'
2214 SEQUENCE :
2215     OBJECT IDENTIFIER : authorityKeyIdentifier [2.5.29.35]
2216     OCTET STRING :
2217     SEQUENCE :
2218         CONTEXT SPECIFIC (0) : D46990260281D55E834B03976EAB8A9F8F84C983
2219 SEQUENCE :
2220     OBJECT IDENTIFIER : authorityInfoAccess [1.3.6.1.5.5.7.1.1]
2221     OCTET STRING :
2222     SEQUENCE :
2223     SEQUENCE :
2224         OBJECT IDENTIFIER : ocsp [1.3.6.1.5.5.7.48.1]
2225         CONTEXT SPECIFIC (6) : 'https://www.xyzintegrators.com/ocsp'
2226 SEQUENCE :
2227     OBJECT IDENTIFIER : cRLDistributionPoints [2.5.29.31]
2228     OCTET STRING :

```

2229 SEQUENCE :
2230 SEQUENCE :
2231 CONTEXT SPECIFIC (0) :
2232 CONTEXT SPECIFIC (0) :
2233 CONTEXT SPECIFIC (6) :
2234 'https://www.xyzintegrators.com/platformcert.crl'
2235 SEQUENCE :
2236 OBJECT IDENTIFIER : [1.2.840.113549.1.1.11]
2237 NULL :
2238 BIT STRING UnusedBits:0 :
2239 6C772B5ED10A2C44DF64CF078BB9D937A843195AF7344ECB04CE01
2240 50CB6B435AE267EA9ADDE64D8B8486409B627617F6CA9AD0A09898
2241 14D38E33BB2E774E3BB522B10B31F2F2930C3550E84DDEB7179EA9
2242 D898F20E11BFEB759C2F079DAF9467E2EFFAB5337BF15A3A25C7E2
2243 B9FA9312BB8EC19EDA55480BBAAF2335A78DC179920C4E4374AA16
2244 65895455E3D8552A6AE3F859B0D0107FC7F8582BF1053942AFE4EA
2245 73D95ECD421B770A65F7123907AB17B9D63A009D0A56D0A667D2F8
2246 F5B3D744566EFC7AB3DF8423EDCACB419742B7EADE499B33A3B099
2247 F82BF56324A07253881471F242BE6CE6DDEC68CD3931AF6EB1D84E
2248 C956145E5A0C1EFC99DFA327C0
2249
2250

DRAFT