

TCG Platform Attribute Credential Profile

Specification Version 1.0
Revision 16
16 January 2018
Published

Contact: admin@trustedcomputinggroup.org

TCG Published

Copyright © TCG 2018

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
Carolyn Latze (IWG co-chair)	Carolyn 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 Challenger	John Hopkins University
Daniel Wong	Microsoft
Mark Williams	Microsoft
Mark Redman	Motorola
Sue Roddy	NSA
Laszlo Elteto	SafeNet
Manuel Offenbergl	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.	Credential Overview.....	3
2.1	Platform Attribute Credential	3
2.1.1	Who Uses a Platform Attribute Credential?	3
2.1.2	Who Issues a Platform Attribute Credential?.....	3
2.1.3	Platform Attribute Credential Privacy Protection Requirements.....	4
2.1.4	Revocation of a Platform Attribute Credential	4
2.1.5	Validity Period of a Platform Attribute Credential.....	4
2.1.6	Assertions Made by a Platform Attribute Credential	4
2.1.6.1	Credential Type Label	5
2.1.6.2	EK Credential.....	5
2.1.6.3	Platform Model	5
2.1.6.4	Platform Manufacturer Identifier	6
2.1.6.5	Issuer	6
2.1.6.6	Platform Specification.....	6
2.1.6.7	Credential Specification	6
2.1.6.8	Validity Period	6
2.1.6.9	Signature Value	6
2.1.6.10	Platform Serial Number.....	6
2.1.6.11	Platform Assertions	6
2.1.6.12	Platform Configuration.....	7
2.1.6.13	Platform Configuration Uri.....	7
2.1.6.14	Policy Reference	7
2.1.6.15	Revocation Locator.....	7
3.	X.509 ASN.1 Definitions	8
3.1	TCG Attributes	8
3.1.1	Security Qualities	8
3.1.2	TPM and Platform Assertions	8
3.1.3	Conformance Attributes.....	10

3.1.4	Name Attributes	10
3.1.5	TCG Specification Attributes	11
3.1.5.1	TCG Credential Specification Attributes	11
3.1.5.2	Platform Configuration.....	12
3.1.5.3	Platform Configuration Uri Attribute	12
3.2	Attribute Certificate Format	13
3.2.1	Version.....	14
3.2.2	Serial Number	14
3.2.3	Signature Algorithm	14
3.2.4	Holder	14
3.2.5	Issuer	15
3.2.6	Validity.....	15
3.2.7	Certificate Policies.....	15
3.2.8	Subject Alternative Names	15
3.2.9	Attributes.....	15
3.2.10	Authority Key Identifier	16
3.2.11	Authority Info Access	16
3.2.12	CRL Distribution	16
3.2.13	Issuer Unique Id.....	17
3.3	Public Key Certificate Format.....	17
3.3.1	Version	19
3.3.2	Serial Number	19
3.3.3	Signature Algorithm	19
3.3.4	Issuer	19
3.3.5	Validity.....	19
3.3.6	Subject.....	19
3.3.7	Subject Public Key Info	19
3.3.8	Certificate Policies.....	19
3.3.9	Subject Alternative Name.....	20
3.3.10	Basic Constraints.....	20
3.3.11	Subject Directory Attributes.....	20
3.3.12	Authority Key Identifier	21
3.3.13	Authority Info Access	21
3.3.14	CRL Distribution	21
3.3.15	Key Usage.....	21
3.3.16	Extended Key Usage	21
3.3.17	Subject Key Identifier.....	22

4. X.509 ASN.1 Structures and OIDs..... 23

5. References.....29

Table of Tables

Table 1: Platform Attribute Credential Fields	5
Table 2: Attribute Certificate Format Fields	14
Table 3: Public Key Certificate Format Fields	18

Change Log

Date	Version	Comment
2018-01-11	1.0	Initial Release

1. Introduction

1.1 Purpose

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

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

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

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

1.2 Document Scope

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

1.3 Relationship to Other TCG Specifications

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

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

44 **1.4 Keywords**

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

48 **1.5 Intended Audiences**

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

53 This document specifies one aspect of the architectural framework described in the document
54 entitled “TCG Infrastructure Working Group Reference Architecture for Interoperability” [1]
55 In particular, see sections 3, 4, 5, and 6.

56 **1.6 Definition of Terms**

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

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

61 **Certificate** – A certificate is an instantiation of a credential using the industry-standard
62 certificate structure from ISO/IEC/ITU-T X.509 version 3. Certificate generation consists of
63 (a) assembling values for the credential fields and (b) signing over the assembled fields.

64 **Credential** – A credential is an abstract proof that must be instantiated as a certificate before
65 it can be exchanged between entities.

66 **2. Credential Overview**

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

70 **2.1 Platform Attribute Credential**

71 A Platform Attribute Credential attests that a specific platform contains a unique TPM and
72 Trusted 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 In general, the issuer of a Platform Attribute Credential is the platform manufacturer (for
80 example, an OEM). An entity should not generate a Platform Attribute Credential unless the
81 entity is satisfied that the platform contains the TPM referenced inside the credential.
82 Platform Attribute Credentials contain assertions about trust made by a platform
83 manufacturer.

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

88 Another consumer of the Platform Credential 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 Credential 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.

93 **2.1.1 Who Uses a Platform Attribute Credential?**

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

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

102 **2.1.2 Who Issues a Platform Attribute Credential?**

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

106 2.1.3 Platform Attribute Credential Privacy Protection Requirements

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

112 2.1.4 Revocation of a Platform Attribute Credential

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

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

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

119 2.1.5 Validity Period of a Platform Attribute Credential

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

122 2.1.6 Assertions Made by a Platform Attribute Credential

123 The following table lists all the fields that are central to the use of this credential type by TCG
124 and which MUST or MAY be in a Platform Attribute Credential.

125

Field Name	Description	Field Status
Credential Type Label	Distinguish credential types issued under a shared key	MUST
EK Credential	Identifies the associated EK Credential	MUST
Platform Manufacturer	Name of platform manufacturer	MUST
Platform Model	Manufacturer-specific identifier	MUST
Platform Version	Manufacturer-specific identifier	MUST
Issuer	Identifies the issuer of the credential	MUST
Platform Specification	Platform Specification to which this platform is built	MUST
Credential Specification	Platform Attribute Certificate Specification Version, Level, and Revision	MUST

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

Table 1: Platform Attribute Credential Fields

126

127 **2.1.6.1 Credential Type Label**

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

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

135 **2.1.6.2 EK Credential**

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

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

140 **2.1.6.3 Platform Model**

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

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

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

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

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

148 **2.1.6.4 Platform Manufacturer Identifier**

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

152 **2.1.6.5 Issuer**

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

154 **2.1.6.6 Platform Specification**

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

158 **2.1.6.7 Credential Specification**

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

161 **2.1.6.8 Validity Period**

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

164 **2.1.6.9 Signature Value**

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

166 **2.1.6.10 Platform Serial Number**

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

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

173 **2.1.6.11 Platform Assertions**

174 This field may contain assertions about the general security properties of the platform. This
175 may be used by the credential user to verify that the platform implements acceptable security
176 policies.

177 For more information, see Section 5, Entities, Assertions, and Signed Structures [1].

178 **2.1.6.12 Platform Configuration**

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

182 **2.1.6.13 Platform Configuration Uri**

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

185 **2.1.6.14 Policy Reference**

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

188 **2.1.6.15 Revocation Locator**

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

191 3. X.509 ASN.1 Definitions

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

195 3.1 TCG Attributes

196 3.1.1 Security Qualities

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

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

```
202     securityQualities ATTRIBUTE ::= {  
203         WITH SYNTAX SecurityQualities  
204         ID tcg-at-tpmSecurityQualities }  
205  
206     SecurityQualities ::= SEQUENCE {  
207         version INTEGER,  
208         -- version 0 defined by TCPA 1.1b  
209         statement UTF8String }
```

210 3.1.2 TPM and Platform Assertions

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

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

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

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

221 In the **CommonCriteriaMeasures**, the profile and target for the evaluation can be described
222 by either an OID, a URI to a document describing the value, or both. If both are present, they
223 must represent consistent values. The URI values are included in a **URIReference** which
224 describes the URI to the document and a cryptographic hash value which identifies a specific
225 version of the document.

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

232 **STRMAX** is a constant defining the upper bound on the length of a string type. Like the **URIMAX**
233 this is to aid ASN.1 parsers and help limit the upper bound on the length of the certificate.

234 Based on the expected sizes of the strings in the ASN.1 in this document an upper bound of
235 256 was selected. **STRMAX SHOULD NOT** exceed a value of 256.

```
236     Version ::= INTEGER { v1(0) }
237
238     tbbSecurityAssertions ATTRIBUTE ::= {
239         WITH SYNTAX TbbSecurityAssertions
240         ID tcg-at-tbbSecurityAssertions }
241
242     TbbSecurityAssertions ::= SEQUENCE {
243         version Version DEFAULT v1,
244         ccInfo [0] IMPLICIT CommonCriteriaMeasures OPTIONAL,
245         fipsLevel [1] IMPLICIT FIPSLevel OPTIONAL,
246         rtmType [2] IMPLICIT MeasurementRootType OPTIONAL,
247         iso9000Certified BOOLEAN DEFAULT FALSE,
248         iso9000Uri IA5STRING (SIZE (1..URIMAX) OPTIONAL }
249
250     -- V1.1 of this specification adds hybrid and physical.
251     -- Hybrid means the measurement root is capable of static AND dynamic
252     -- Physical means that the root is anchored by a physical TPM
253     -- Virtual means the TPM is virtualized (possibly running in a VMM).
254     -- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
255     -- the capabilities of the platform.
256     MeasurementRootType ::= ENUMERATED {
257         static (0),
258         dynamic (1),
259         nonHost (2),
260         hybrid (3),
261         physical (4),
262         virtual (5) }
263
264
265     -- common criteria evaluation
266
267     CommonCriteriaMeasures ::= SEQUENCE {
268         version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined by CC
269         assuranceLevel EvaluationAssuranceLevel,
270         evaluationStatus EvaluationStatus,
271         plus BOOLEAN DEFAULT FALSE,
272         strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
273         profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
274         profileUri [2] IMPLICIT URIReference OPTIONAL,
275         targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
276         targetUri [4] IMPLICIT URIReference OPTIONAL }
277
278     EvaluationAssuranceLevel ::= ENUMERATED {
279         level1 (1),
280         level2 (2),
281         level3 (3),
282         level4 (4),
283         level5 (5),
284         level6 (6),
285         level7 (7) }
286
287     StrengthOfFunction ::= ENUMERATED {
288         basic (0),
289         medium (1),
290         high (2) }
291
292     -- Reference to external document containing information relevant to this subject.
293     -- The hashAlgorithm and hashValue MUST both exist in each reference if either
294     -- appear at all.
295     URIReference ::= SEQUENCE {
296         uniformResourceIdentifier IA5String (SIZE (1..URIMAX),
297         hashAlgorithm AlgorithmIdentifier OPTIONAL,
298         hashValue BIT STRING OPTIONAL }
299
300     EvaluationStatus ::= ENUMERATED {
301         designedToMeet (0),
302         evaluationInProgress (1),
```

```

303         evaluationCompleted (2) }
304
305     -- fips evaluation
306
307     FIPSLevel ::= SEQUENCE {
308         version IA5STRING (SIZE (1..STRMAX)), -- "140-1" or "140-2"
309         level SecurityLevel,
310         plus BOOLEAN DEFAULT FALSE }
311
312     SecurityLevel ::= ENUMERATED {
313         level1 (1),
314         level2 (2),
315         level3 (3),
316         level4 (4) }

```

317 3.1.3 Conformance Attributes

318 Conformance Attributes are the syntax of the protection profile and security target attributes.
319 These attributes are deprecated and replaced with the TPM and Platform Assertion attributes.
320 They MAY be present for compatibility with previously published TCG and TCPA
321 specifications.

```

322     ProtectionProfile ::= OBJECT IDENTIFIER
323     SecurityTarget ::= OBJECT IDENTIFIER
324
325     TBBProtectionProfile ATTRIBUTE ::= {
326         WITH SYNTAX ProtectionProfile
327         ID tcg-at-tbbProtectionProfile }
328
329     TBBSecurityTarget ATTRIBUTE ::= {
330         WITH SYNTAX SecurityTarget
331         ID tcg-at-tbbSecurityTarget }

```

332 3.1.4 Name Attributes

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

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

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

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

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

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

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

```

345
346     PlatformManufacturerStr ATTRIBUTE ::= {
347         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
348         ID tcg-at-platformManufacturer }
349
350     PlatformModel ATTRIBUTE ::= {
351         WITH SYNTAX UTF8String (SIZE (1..STRMAX))
352         ID tcg-at-platformModel }
353
354     PlatformVersion ATTRIBUTE ::= {
355         WITH SYNTAX UTF8String (SIZE (1..STRMAX))

```

```

356         ID tcg-at-platformVersion }
357
358 PlatformSerial ATTRIBUTE ::= {
359     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
360     ID tcg-at-platformSerial }
361
362 PlatformManufacturerId ATTRIBUTE ::= {
363     WITH SYNTAX ManufacturerId
364     ID tcg-at-platformManufacturerId
365 }
366
367 ManufacturerId ::= SEQUENCE {
368     manufacturerIdentifier PrivateEnterpriseNumber
369 }
370
371 enterprise OBJECT IDENTIFIER ::= {
372     iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)}
373
374 PrivateEnterpriseNumber OBJECT IDENTIFIER ::= { enterprise private-enterprise-number }
375
376 All assigned private enterprise numbers are listed at the Internet Assigned Numbers
377 Authority (IANA) web site [8].

```

378 3.1.5 TCG Specification Attributes

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

381 The **TCGPlatformSpecification** attribute identifies the platform class, version and revision
382 of the platform-specific specification with which a platform implementation is compliant. The
383 platform specification refers either to the PC Client Platform Specification [10] or the Server
384 Specification [9]. Standardized four byte platform class values are defined in each platform-
385 specific specification document.

```

386 tCGPlatformSpecification ATTRIBUTE ::= {
387     WITH SYNTAX TCGPlatformSpecification
388     ID tcg-at-tcgPlatformSpecification }
389
390 TCGSpecificationVersion ::= SEQUENCE {
391     majorVersion INTEGER,
392     minorVersion INTEGER,
393     revision INTEGER }
394
395 TCGPlatformSpecification ::= SEQUENCE {
396     Version TCGSpecificationVersion,
397     platformClass OCTET STRING SIZE(4) }
398

```

399 3.1.5.1 TCG Credential Specification Attributes

400 The following defines the syntax of the credential specification attributes.

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

```

404 tCGCredentialsSpecification ATTRIBUTE ::= {
405     WITH SYNTAX TCGSpecificationVersion
406     ID tcg-at-tcgCredentialsSpecification }
407
408 TCGSpecificationVersion ::= SEQUENCE {
409     majorVersion INTEGER,
410     minorVersion INTEGER,
411     revision INTEGER }

```

412 3.1.5.2 Platform Configuration

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

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

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

```

427 platformConfiguration ATTRIBUTE ::= {
428     WITH SYNTAX PlatformConfiguration
429     ID tcg-at-platformConfiguration-v1
430 }
431
432 PlatformConfiguration ::= SEQUENCE {
433     componentIdentifier [0] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF ComponentIdentifier
434     OPTIONAL,
435     platformProperties [1] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF Properties OPTIONAL,
436     platformPropertiesUri [2] IMPLICIT URIReference OPTIONAL
437 }
438
439 ComponentIdentifier ::= SEQUENCE {
440     componentManufacturer UTF8String (SIZE (1..STRMAX)),
441     componentModel UTF8String (SIZE (1..STRMAX)),
442     componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
443     componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
444     componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,
445     fieldReplaceable [3] IMPLICIT BOOLEAN OPTIONAL,
446     componentAddress [4] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF ComponentAddress OPTIONAL }
447
448 ComponentAddress ::= SEQUENCE {
449     addressType AddressType,
450     addressValue UTF8String (SIZE (1..STRMAX)) }
451
452 AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
453     bluetoothmac)
454
455 Properties ::= SEQUENCE {
456     propertyName UTF8String (SIZE (1..STRMAX)),
457     propertyValue UTF8String (SIZE (1..STRMAX)) }
458

```

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

462 3.1.5.3 Platform Configuration Uri Attribute

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

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

```
467 PlatformConfigUri ATTRIBUTE ::= {
468 WITH SYNTAX URIReference
469 ID tcg-at-platformConfigUri }
470
```

471 3.2 Attribute Certificate Format

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

474 The Platform Attribute Credential makes the assertions listed in section 2.1.6. This certificate
 475 format adheres to RFC 5755 [11] and all requirements and limitations from that specification
 476 apply unless otherwise noted.

477 Note: some fields are assigned a value even though the certificate user performs no action
 478 with that value. In such cases, the intention is to inhibit non-TCG implementations from
 479 making inappropriate use of the certificate.

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

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

480 **Table 2: Attribute Certificate Format Fields**

481 **3.2.1 Version**

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

485 **3.2.2 Serial Number**

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

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

490 **3.2.3 Signature Algorithm**

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

494 **3.2.4 Holder**

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

497 **3.2.5 Issuer**

498 This field contains the distinguished name of the entity that issued this platform certificate.
499 This is the entity that asserts that the platform incorporates a TPM and RTM in a manner
500 that conforms to the TCG specification.

501 **3.2.6 Validity**

502 This field contains the period during which the binding between the attributes and TPM EK
503 certificate is considered valid. It is represented by two date values named notBefore and
504 notAfter. Issuers should assign notBefore to the current time when the certificate is issued
505 and notAfter to the last date that the certificate will be considered valid. Both notBefore and
506 notAfter MUST use the appropriate time format as indicated by RFC 5755, section 4.2.6.

507 **3.2.7 Certificate Policies**

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

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

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

515 **3.2.8 Subject Alternative Names**

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

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

523 **3.2.9 Attributes**

524 The following attributes SHOULD be included:

- 525 • The “TCG Platform Specification” attribute references the platform class, version and
526 revision level of the TCG platform-specific specification to which the platform was
527 designed.
- 528 • The “TCG Credential Specification” attribute references the version, level, and revision
529 of this specification.
- 530 • The platform “TBB Security Assertions” attribute describes various assertions about
531 the security properties of the TBB of the platform.

532 The following attributes MAY be included:

533 • The “Platform Configuration” attribute describes various assertions of platform
534 properties that are not security related. Including CPU and motherboard serial
535 numbers, network adapter MAC addresses.

536 • The “Platform Configuration Uri” attribute which provides the URI to the manufacturer
537 published list of valid PCR values.

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

540 • The "TCPA Specification Version" attribute, with field values correctly reflecting the
541 highest version of the TCG specification with which the TPM implementation conforms.

542 • If the TPM has been successfully evaluated against a Common Criteria protection
543 profile, then include the TPM protection profile identifier attribute.

544 • If the TPM has been successfully evaluated against a Common Criteria security target,
545 then include the TPM security target identifier attribute.

546 • If the RTM and the means by which the TPM and RTM have been incorporated into the
547 platform have been successfully evaluated against a Common Criteria protection
548 profile, then include the "TBB protection profile" identifier attribute.

549 • If the RTM and the means by which the TPM and RTM have been incorporated into the
550 platform have been successfully evaluated against a Common Criteria security target,
551 then include the "TBB security target" identifier attribute.

552 • Optionally, include the "security qualities" attribute with a text string reflecting the
553 security qualities of the platform.

554 **3.2.10 Authority Key Identifier**

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

558 **3.2.11 Authority Info Access**

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

563 The relying party can access the certificate status for this certificate by sending a properly
564 formatted OCSPRequest to the URI. If both a CDP and OCSP AIA extension are present in the
565 certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

566 **3.2.12 CRL Distribution**

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

571 **3.2.13 Issuer Unique Id**

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

574 **3.3 Public Key Certificate Format**

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

577 The Platform Public Key Certificate makes the assertions listed in section 2.1.6. The platform
578 certificate supports a public key certificate profile of RFC 5280 [13] and all requirements and
579 limitations from that specification apply unless otherwise noted.

580 Note: some fields are assigned a value even though the certificate user performs no action
581 with that value. In such cases, the intention is to inhibit non-TCG implementations from
582 making inappropriate use of the certificate.

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

Field Name	RFC 5280 Type	Value	Field Status
Subject Alternative Name	GeneralName directoryName	PlatformManufacturerStr PlatformModel PlatformVersion PlatformSerial (optional) PlatformManufacturerId (optional)	MUST critical/ non- critical (depending on subject)
Basic Constraints	BasicConstraints	CA=FALSE	MUST critical
Subject Directory Attributes	SubjectDirectoryAt tributes	TCGPlatformSpecification TCGCertificateSpecification TBBSecurityAssertions PlatformConfiguration (optional) PlatformConfigurationUri (optional)	MUST non-critical
Authority Key Id	AuthorityKeyIdenti fier	Key identifier Issuer name and serial number (optional)	MUST non-critical
Authority Info Access	AuthorityInfoAcces sSyntax	id-ad-caIssuers URI to issuing CA id-ad-ocsp (optional) URI to OCSP responder	SHOULD non-critical
CRL Distribution	CRLDistributionPo ints	URI to CRL	MAY non-critical
Key Usage	KeyUsage	keyEncipherment or keyAgreement or digitalSignature	MUST critical
Extended Key Usage	ExtKeyUsageSynta x	tcg-kp- PlatformKeyCertificate	SHOULD non-critical
Subject Key Id	SubjectKeyId entifier	Key identifier	MAY

Table 3: Public Key Certificate Format Fields

584 **3.3.1 Version**

585 This field contains the version of the certificate syntax. Version number must be set to 3
586 (which is encoded as the value 2 in ASN.1).

587 **3.3.2 Serial Number**

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

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

592 **3.3.3 Signature Algorithm**

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

596 **3.3.4 Issuer**

597 This field contains the distinguished name of the entity that issued this platform certificate.
598 This is the entity that asserts that the platform incorporates a TPM and RTM in a manner
599 that conforms to the TCG specification.

600 **3.3.5 Validity**

601 This field contains the period during which the binding between the attributes and TPM EK
602 certificate is considered valid. It is represented by two date values named notBefore and
603 notAfter. Issuers should assign notBefore to the current time when the certificate is issued
604 and notAfter to the last date that the certificate will be considered valid. Both notBefore and
605 notAfter MUST use the appropriate time format as indicated by RFC 5280 [13].

606 **3.3.6 Subject**

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

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

611 **3.3.7 Subject Public Key Info**

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

617 **3.3.8 Certificate Policies**

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

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

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

625 **3.3.9 Subject Alternative Name**

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

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

634 **3.3.10 Basic Constraints**

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

637 **3.3.11 Subject Directory Attributes**

638 The extension includes miscellaneous properties and security assertions about the platform’s
639 manufacturer. This extension MUST be non-critical. The following attributes SHOULD be
640 included:

- 641 • The “TCG Platform Specification” attribute references the platform class, version and
642 revision level of the TCG platform-specific Specification to which the platform was
643 designed.
- 644 • The “TCG Credential Specification” attribute references the version, level, and revision
645 of this specification.
- 646 • The platform “TBB Security Assertions” attribute describes various assertions about
647 the security properties of the TBB of the platform.

648 The following attributes MAY be included:

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

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

- 656 • The "TCPA Specification Version" attribute, with field values correctly reflecting the
657 highest version of the TCG specification with which the TPM implementation conforms.

- 658 • If the TPM has been successfully evaluated against a Common Criteria protection
659 profile, then include the TPM protection profile identifier attribute.
- 660 • If the TPM has been successfully evaluated against a Common Criteria security target,
661 then include the TPM security target identifier attribute.
- 662 • If the RTM and the means by which the TPM and RTM have been incorporated into the
663 platform have been successfully evaluated against a Common Criteria protection
664 profile, then include the "TBB protection profile" identifier attribute.
- 665 • If the RTM and the means by which the TPM and RTM have been incorporated into the
666 platform have been successfully evaluated against a Common Criteria security target,
667 then include the "TBB security target" identifier attribute.
- 668 • Optionally, include the "security qualities" attribute with a text string reflecting the
669 security qualities of the platform.

670 **3.3.12 Authority Key Identifier**

671 This extension identifies the subject public key of the certificate issuer. Assign "critical" the
672 value FALSE. Assign the value of "subject key identifier" from the issuer's public-key
673 certificate, if available, else derive from the issuer's public key.

674 **3.3.13 Authority Info Access**

675 This extension contains additional information about the issuer. It MAY be included. If
676 included, then the accessMethod OID SHOULD be set to id-ad-ocsp (RFC 5755 [11]) and the
677 accessLocation value SHOULD point to the access value of the OCSP responder (HTTP URI).

678 The relying party can access the certificate status for this certificate by sending a properly
679 formatted OCSPRequest to the URI. If both a CDP and OCSP AIA extension are present in the
680 certificate, then the relying parties SHOULD use OCSP as the primary validation mechanism.

681 **3.3.14 CRL Distribution**

682 This extension provides the location of the subject's revocation information. The relying party
683 can access the CRL for this certificate from this URI. If both a CDP and OCSP AIA extension
684 are present in the certificate, then relying parties SHOULD use OCSP as the primary
685 validation mechanism.

686 **3.3.15 Key Usage**

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

691 This extension MUST be critical.

692 **3.3.16 Extended Key Usage**

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

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

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

702 **3.3.17 Subject Key Identifier**

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

705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771

4. X.509 ASN.1 Structures and OIDs

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

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

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

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

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

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

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

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

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

-- TCG Certificate Extensions
tcg-ce-relevantCredentials OBJECT IDENTIFIER ::= {tcg-ce 2}
tcg-ce-relevantManifests OBJECT IDENTIFIER ::= {tcg-ce 3}
tcg-ce-virtualPlatformAttestationService OBJECT IDENTIFIER ::= {tcg-ce 4}
tcg-ce-migrationControllerAttestationService OBJECT IDENTIFIER ::= (tcg-ce 5)
tcg-ce-migrationControllerRegistrationService OBJECT IDENTIFIER ::= (tcg-ce 6)
tcg-ce-virtualPlatformBackupService OBJECT IDENTIFIER ::= (tcg-ce 7)
```

```

772 -- TCG Protocol OIDs
773 tcg-prt-tpmIdProtocol OBJECT IDENTIFIER ::= {tcg-protocol 1}
774
775 -- tcg specification attributes for tpm and platform
776 tPMSpecification ATTRIBUTE ::= {
777     WITH SYNTAX TPMSpecification
778     ID tcg-at-tpmSpecification }
779
780 TPMSpecification ::= SEQUENCE {
781     family UTF8String (SIZE (1..STRMAX)),
782     level INTEGER,
783     revision INTEGER }
784
785 tCGPlatformSpecification ATTRIBUTE ::= {
786     WITH SYNTAX TCGPlatformSpecification
787     ID tcg-at-tcgPlatformSpecification }
788
789 TCGSpecificationVersion ::= SEQUENCE {
790     majorVersion INTEGER,
791     minorVersion INTEGER,
792     revision INTEGER }
793
794 TCGPlatformSpecification ::= SEQUENCE {
795     Version TCGSpecificationVersion,
796     platformClass OCTET STRING SIZE(4) }
797
798 -- tcpa tpm specification attribute (deprecated)
799 tCPASpecVersion ATTRIBUTE ::= {
800     WITH SYNTAX TCPASpecVersion
801     ID tcg-tcpaSpecVersion }
802
803 TCPASpecVersion ::= SEQUENCE {
804     major INTEGER,
805     minor INTEGER }
806
807 -- manufacturer implementation model and version attributes
808 TPMManufacturer ATTRIBUTE ::= {
809     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
810     ID tcg-at-tpmManufacturer }
811
812 TPMModel ATTRIBUTE ::= {
813     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
814     ID tcg-at-tpmModel }
815
816 TPMVersion ATTRIBUTE ::= {
817     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
818     ID tcg-at-tpmVersion }
819
820 PlatformManufacturer ATTRIBUTE ::= {
821     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
822     ID tcg-at-platformManufacturer }
823
824 PlatformModel ATTRIBUTE ::= {
825     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
826     ID tcg-at-platformModel }
827
828 PlatformVersion ATTRIBUTE ::= {
829     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
830     ID tcg-at-platformVersion }
831
832 PlatformSerial ATTRIBUTE ::= {
833     WITH SYNTAX UTF8String (SIZE (1..STRMAX))
834     ID tcg-at-platformSerial }
835
836 PlatformManufacturerId ATTRIBUTE ::= {
837     WITH SYNTAX ManufacturerId
838     ID tcg-at-platformManufacturerId
839 }
840
841 ManufacturerId ::= SEQUENCE {
842     manufacturerIdentifier PrivateEnterpriseNumber

```

```

843     }
844
845     enterprise OBJECT IDENTIFIER ::= {
846         iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)}
847
848     PrivateEnterpriseNumber OBJECT IDENTIFIER ::= { enterprise private-enterprise-number }
849
850
851     -- tpm and platform tbb security assertions
852     Version ::= INTEGER { v1(0) }
853     TPMSecurityAssertions ATTRIBUTE ::= {
854         WITH SYNTAX TPMSecurityAssertions
855         ID tcg-at-tpmSecurityAssertions
856     }
857
858     TPMSecurityAssertions ::= SEQUENCE {
859         version Version DEFAULT v1,
860         fieldUpgradable BOOLEAN DEFAULT FALSE,
861         ekGenerationType [0] IMPLICIT EKGenerationType OPTIONAL,
862         ekGenerationLocation [1] IMPLICIT EKGenerationLocation OPTIONAL,
863         ekCertificateGenerationLocation [2] IMPLICIT EKCertificateGenerationLocation OPTIONAL,
864         ccInfo [3] IMPLICIT CommonCriteriaMeasures OPTIONAL,
865         fipsLevel [4] IMPLICIT FIPSLevel OPTIONAL,
866         iso9000Certified [5] IMPLICIT BOOLEAN DEFAULT FALSE,
867         iso9000Uri IA5STRING (SIZE (1..URIMAX)) OPTIONAL }
868
869     TBBSecurityAssertions ATTRIBUTE ::= {
870         WITH SYNTAX TBBSecurityAssertions
871         ID tcg-at-tbbSecurityAssertions }
872
873     TBBSecurityAssertions ::= SEQUENCE {
874         version Version DEFAULT v1,
875         ccInfo [0] IMPLICIT CommonCriteriaMeasures OPTIONAL,
876         fipsLevel [1] IMPLICIT FIPSLevel OPTIONAL,
877         rtmType [2] IMPLICIT MeasurementRootType OPTIONAL,
878         iso9000Certified BOOLEAN DEFAULT FALSE,
879         iso9000Uri IA5STRING (SIZE (1..URIMAX)) OPTIONAL }
880
881     EKGenerationType ::= ENUMERATED {
882         internal (0),
883         injected (1),
884         internalRevocable(2),
885         injectedRevocable(3) }
886
887     EKGenerationLocation ::= ENUMERATED {
888         tpmManufacturer (0),
889         platformManufacturer (1),
890         ekCertSigner (2) }
891
892     EKCertificateGenerationLocation ::= ENUMERATED {
893         tpmManufacturer (0),
894         platformManufacturer (1),
895         ekCertSigner (2) }
896
897     -- V1.1 of this specification adds hybrid and physical.
898     -- Hybrid means the measurement root is capable of static AND dynamic
899     -- Physical means that the root is anchored by a physical TPM
900     -- Virtual means the TPM is virtualized (possibly running in a VMM)
901
902     -- TPMs or RTMs might leverage other lower layer RTMs to virtualize the
903     -- the capabilities of the platform.
904     MeasurementRootType ::= ENUMERATED {
905         static (0),
906         dynamic (1),
907         nonHost (2),
908         hybrid (3),
909         physical (4),
910         virtual (5) }
911
912
913     -- common criteria evaluation

```

```

914 CommonCriteriaMeasures ::= SEQUENCE {
915     version IA5STRING (SIZE (1..STRMAX)), -- "2.2" or "3.1"; future syntax defined by CC
916     assuranceLevel EvaluationAssuranceLevel,
917     evaluationStatus EvaluationStatus,
918     plus BOOLEAN DEFAULT FALSE,
919     strengthOfFunction [0] IMPLICIT StrengthOfFunction OPTIONAL,
920     profileOid [1] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
921     profileUri [2] IMPLICIT URIReference OPTIONAL,
922     targetOid [3] IMPLICIT OBJECT IDENTIFIER OPTIONAL,
923     targetUri [4] IMPLICIT URIReference OPTIONAL }
924
925 EvaluationAssuranceLevel ::= ENUMERATED {
926     level1 (1),
927     level2 (2),
928     level3 (3),
929     level4 (4),
930     level5 (5),
931     level6 (6),
932     level7 (7) }
933
934 StrengthOfFunction ::= ENUMERATED {
935     basic (0),
936     medium (1),
937     high (2) }
938
939 URIReference ::= SEQUENCE {
940     uniformResourceIdentifier IA5String (SIZE (1..URIMAX)),
941     hashAlgorithm AlgorithmIdentifier OPTIONAL,
942     hashValue BIT STRING OPTIONAL }
943
944 EvaluationStatus ::= ENUMERATED {
945     designedToMeet (0),
946     evaluationInProgress (1),
947     evaluationCompleted (2) }
948
949 -- fips evaluation
950 FIPSLevel ::= SEQUENCE {
951     version IA5STRING (SIZE (1..STRMAX)), -- "140-1" or "140-2"
952     level SecurityLevel,
953     plus BOOLEAN DEFAULT FALSE }
954
955 SecurityLevel ::= ENUMERATED {
956     level1 (1),
957     level2 (2),
958     level3 (3),
959     level4 (4) }
960
961 -- aik certificate label from tpm owner
962
963 TPMIdLabel OTHER-NAME ::= {UTF8String IDENTIFIED BY {tcg-at-tpmIdLabel} }
964
965 -- platform configuration
966 platformConfiguration ATTRIBUTE ::= {
967     WITH SYNTAX PlatformConfiguration
968     ID tcg-at-platformConfiguration-v1
969 }
970
971 PlatformConfiguration ::= SEQUENCE {
972     componentIdentifier [0] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF ComponentIdentifier
973     OPTIONAL,
974     platformProperties [1] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF Properties OPTIONAL
975 }
976
977 ComponentIdentifier ::= SEQUENCE {
978     componentManufacturer UTF8String (SIZE (1..STRMAX)),
979     componentModel UTF8String (SIZE (1..STRMAX)),
980     componentSerial[0] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
981     componentRevision [1] IMPLICIT UTF8String (SIZE (1..STRMAX)) OPTIONAL,
982     componentManufacturerId [2] IMPLICIT PrivateEnterpriseNumber OPTIONAL,
983     componentAddress [3] IMPLICIT SEQUENCE(SIZE(1..CONFIGMAX)) OF ComponentAddress OPTIONAL }
984

```



```

985 ComponentAddress ::= SEQUENCE {
986     addressType AddressType,
987     addressValue UTF8String (SIZE (1..STRMAX)) }
988
989 AddressType ::= OBJECT IDENTIFIER (tcg-address-ethernetmac | tcg-address-wlanmac | tcg-address-
990 bluetoothmac)
991
992 Properties ::= SEQUENCE {
993     propertyName UTF8String (SIZE (1..STRMAX)),
994     propertyValue UTF8String (SIZE (1..STRMAX)) }
995
996 -- platform configuration Uri attribute
997 PlatformConfigUri ATTRIBUTE ::= {
998     WITH SYNTAX URIReference
999     ID tcg-at-platformConfigUri }
1000
1001 -- the following are deprecated but may be present for compatibility with TCG
1002 TPMProtectionProfile ATTRIBUTE ::= {
1003     WITH SYNTAX ProtectionProfile
1004     ID tcg-at-tpmProtectionProfile }
1005
1006 TPMSecurityTarget ATTRIBUTE ::= {
1007     WITH SYNTAX SecurityTarget
1008     ID tcg-at-tpmSecurityTarget }
1009
1010 TBBProtectionProfile ATTRIBUTE ::= {
1011     WITH SYNTAX ProtectionProfile
1012     ID tcg-at-tbbProtectionProfile }
1013
1014 TBBSecurityTarget ATTRIBUTE ::= {
1015     WITH SYNTAX SecurityTarget
1016     ID tcg-at-tbbSecurityTarget }
1017
1018 ProtectionProfile ::= OBJECT IDENTIFIER
1019 SecurityTarget ::= OBJECT IDENTIFIER
1020
1021 -- V1.1 addition for enabling references to other credentials or
1022 -- XML-based Reference Manifests. These data objects are included
1023 -- in X.509 extensions using the new tcg-ce-[relevantCredentials,
1024 -- relevantManifests] OIDs.
1025
1026 HashAlgAndValue ::= SEQUENCE {
1027     hashAlg AlgorithmIdentifier,
1028     hashValue OCTET STRING }
1029
1030 HashedSubjectInfoURI ::= SEQUENCE {
1031     documentURI IA5String (SIZE (1..URIMAX)),
1032     documentAccessInfo OBJECT IDENTIFIER OPTIONAL,
1033     documentHashInfo HashAlgAndValue OPTIONAL }
1034
1035 SubjectInfoURIList ::=
1036     SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI
1037
1038 TCGRelevantCredentials ::=
1039     SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI
1040 TCGRelevantManifests ::=
1041     SEQUENCE SIZE (1..REFMAX) OF HashedSubjectInfoURI
1042
1043 -- V1.2 addition of virtualization oriented credential extensions. This extension indicates how
1044 -- a remote challenger can contact the (deep) attestation service below the current credential holder
1045 -- in order to attest the layer below. Using this model allows the credential of each virtualization
1046 -- layer to reference the attestation service for the layer below it. A remote challenger could
1047 -- traverse the layer hierarchy using this extension until reaching the physical trusted platform
1048 -- rooted attestation. The following URI is optionally included in a certificate for a virtual
1049 -- machine associated with the tcg-ce-virtualPlatformAttestationService extension OID. These URI are
1050 -- associated with the tcg-ce-[virtualPlatformAttestationService,
1051 -- migrationControllerAttestationService,
1052 -- virtualPlatformBackupService] OIDs respectively:
1053 VirtualPlatformAttestationServiceURI ::= IA5String (SIZE (1..URIMAX))
1054 MigrationControllerAttestationServiceURI ::= IA5String (SIZE (1..URIMAX))
1055 MigrationControllerRegistrationServiceURI ::= IA5String (SIZE (1..URIMAX))

```

```
1056 VirtualPlatformBackupServiceURI ::= SEQUENCE {
1057     restoreAllowed BOOLEAN DEFAULT FALSE,
1058     backupServiceURI IA5String }
1059
1060 -- TCG Address OIDs
1061 tcg-address-ethernetmac OBJECT IDENTIFIER ::= {tcg-address 1}
1062 tcg-address-wlanmac OBJECT IDENTIFIER ::= {tcg-address 2}
1063 tcg-address-bluetoothmac OBJECT IDENTIFIER ::= {tcg-address 3}
1064
```

5. References

- 1065
- 1066 [1] TCG Glossary, <https://trustedcomputinggroup.org/glossary>
- 1067 [2] TCG Infrastructure Working Group Reference Architecture for Interoperability (Part
1068 1), Specification Version 1.0,
1069 [http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_refer
1070 ence_architecture_for_interoperability_specification_part_1_version_10](http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_reference_architecture_for_interoperability_specification_part_1_version_10)
- 1071 [3] TCPA Main Specification, Version 1.1b,
1072 <http://www.trustedcomputinggroup.org/tcpa-main-specification-version-1-1b/>
- 1073 [4] Key words for use in RFCs to Indicate Requirement Levels, RFC 2119,
1074 www.ietf.org/rfc/rfc2119.txt
- 1075 [5] Hypertext Markup Language – 2.0, RFC 1866, www.ietf.org/rfc/rfc1866.txt
- 1076 [6] TCG Credential Profiles For TPM Family 1.2 Specification Version 1.2,
1077 [http://www.trustedcomputinggroup.org/infrastructure-work-group-tcg-credential-
1078 profiles-specification/](http://www.trustedcomputinggroup.org/infrastructure-work-group-tcg-credential-profiles-specification/)
- 1079 [7] TCG EK Credential Profile for TPM Family 2.0, Specification Version 2.0,
1080 <http://www.trustedcomputinggroup.org/tcg-ek-credential-profile-tpm-family-2-0/>
- 1081 [8] IANA Private Enterprise Numbers, [http://www.iana.org/assignments/enterprise-
1082 numbers/enterprise-numbers](http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers)
- 1083 [9] Server Work Group Generic Server Specification, Version 1.0,
1084 [http://www.trustedcomputinggroup.org/server-work-group-generic-server-
1085 specification-version-1-0/](http://www.trustedcomputinggroup.org/server-work-group-generic-server-specification-version-1-0/)
- 1086 [10] PC Client Platform TPM Profile (PTP) Specification ,
1087 [http://www.trustedcomputinggroup.org/pc-client-platform-tpm-profile-tp-
1088 specification/](http://www.trustedcomputinggroup.org/pc-client-platform-tpm-profile-ptp-specification/)
- 1089 [11] An Internet Attribute Certificate Profile for Authorization,
1090 www.ietf.org/rfc/rfc5755.txt
- 1091 [12] TCG Algorithm Registry, [http://www.trustedcomputinggroup.org/tcg-algorithm-
1092 registry/](http://www.trustedcomputinggroup.org/tcg-algorithm-registry/)
- 1093 [13] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List
1094 (CRL) Profile, <https://www.ietf.org/rfc/rfc5280.txt>