TRUSTED® COMPUTING GROUP

ERRATA

Errata for TCG Platform Certificate Profile Version 1.1 Revision 19

Errata Version 3.0
March 3, 2022

Contact: admin@trustedcomputinggroup.org

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

THIS SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

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.

CONTENTS

1 Introduction

This document describes errata and clarifications for the TCG Platform Certificate Profile; Specification Version 1.1; Specification Revision 19 as published. The information in this document is likely – but not certain – to be incorporated into a future version of the specification. Suggested fixes proposed in this document may be modified before being published in a later TCG Specification. Therefore, the contents of this document are not normative and only become normative when included in an updated version of the published specification. Note that since the errata in this document are non-normative, the patent licensing rights granted by Section 16.4 of the Bylaws do not apply.

2 Clarifications

The following clarifications will help readers in understanding the specification.

2.1 Clarification 1

Table 3: Attribute Certificate Format Fields

Current:

Field Name	RFC 5755 Type	Value	Field Status
Holder	Holder	Identity of the associated TPM EK Certificate, use BaseCertificateID. Additional EK Certificates can be referenced using the TargetingInformation extension.	Standard

Clarification:

In order to encode the TPM EK Certificate information in the Platform Certificate's Holder field, the issuer must use the baseCertificateID option as defined in RFC5755. The TPM EK certificate's Issuer and Serial number must be included in the baseCertificateID.

2.2 Clarification 2

Section A. Certificate Examples

Clarification:

This section contains informative examples of Platform Certificates and Delta Platform Certificates. The values included in the certificate are for illustrative purposes only. Implementers should replace values such as dates, specification versions, and others with actual values.

2.3 Clarification 3

Section 3. X.509 ASN.1 Definitions

In this section, the specification is silent whether structures can be extended by the issuer. There is no intention to allow extensibility and in the future this specification may explicitly disallow the modification of existing sequences and attributes.

2.4 Clarification 4

Section 3.1.6 Platform Configuration Attributes

Clarification:

Verifiers need to support multiple MAC address formats in order to parse the **`addressValue`** field of the **`ComponentAddress`** sequence. The most common MAC address formats include:

1. Dash separated hexadecimal octets, ex: 00-A0-C9-14-C8-29

2. Colon separated hexadecimal octets, ex: 00:A0:C9:14:C8:29
3. Space separated hexadecimal octets, ex: 00 A0 C9 14 C8 29
4. Non-separated hexadecimal octets, ex: 00A0C914C829
5. Dash separated octet pairs, ex: 00A0-C914-C829
6. Period separated octet pairs, ex: 00A0.C914.C829

2.5 Clarification 5

Sections 2.1.5.1 Certificate Type Label, 3.1.4 TCG Certificate Type Attributes and 3.2.7 Certificate Policies

The last paragraph of section 2.1.5.1 states the following:

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

This text contradicts the ASN.1 structure defined in Section 3.1.4 that defines the attribute **`CredentialType`** as an Object Identifier. This attribute is not the same as the Certificate Type Label.

This Certificate Type Label string is used in the Certificate Policies **`userNotice`** field as defined in Section 3.2.7. The reader should interpret section 3.2.7 as defining the **`userNotice`** field to contain the string defined in the Certificate Type Label section.

2.6 Clarification 6

Sections 2.2.6.1 Certificate Type Label, 3.1.4 TCG Certificate Type Attributes and 3.2.7 Certificate Policies

Section 2.2.6.1 states the following:

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

This text contradicts the ASN.1 structure defined in Section 3.1.4 that defines **`CredentialType`** as an Object Identifier. This attribute is not the same as the Certificate Type Label.

This Certificate Type Label string is used in the Certificate Policies **`userNotice`** field as defined in Section 3.2.7. The Reader should interpret section 3.2.7 as defining the **`userNotice`** field to contain the string defined in the Certificate Type Label section.

2.7 Clarification 7

Section 3.2.8 Subject Alternative Names

In section 3.2.8, the specification is silent on the ordering of the RDN sequence's attribute. There is no order required by the specification.

3 Errata

The following are corrections to editing errors.

3.1 Errata 1

Section 3.1.6 Platform Configuration Attributes

Immediately after the sentence “The **`status`** field contained within the **`componentIdentifier`** field MUST be used only in Delta Platform Certificates”, add the following statement:

“This specification does not dictate the order in which a **`ComponentIdentifier`** entry may appear within the **`componentIdentifiers`** sequence. The order in which a **`ComponentIdentifier`** entry appears in the certificate may differ from platform information sources such as SMBIOS tables or DMIdecode.”

3.2 Errata 2

Section 3.1.6 Platform Configuration Attributes

In the second sentence of paragraph two, the field **`componentIdentifiers`** is incorrectly spelled.

Current:

“The **`componentIndentifer`** field contains a list of individual components that constitute the platform.”

Change to:

“The **`componentIdentifiers`** field contains a list of individual components that constitute the platform.”

3.3 Errata 3

Section 3.1.6 Platform Configuration Attributes

In paragraph five, the field **`componentPlatformCertUri`** is incorrectly spelled.

Current:

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

Change to:

“The platform manufacturer can use the **`componentPlatformCertUri`** to identify the public distribution point of the component platform certificate.”

3.4 Errata 4

Section 3.1.6 Platform Configuration Attributes

In paragraph four, the field **`attributeCertificateIdentifier`** is incorrectly formatted.

Current:

“The issuer MUST include attributeCertificateIdentifier or **`genericCertIdentifier`** to provide a reference to the component’s Platform Certificate.”

Change to:

"The issuer MUST include **attributeCertificateIdentifier** or **genericCertIdentifier** to provide a reference to the component's Platform Certificate."

3.5 Errata 5

Section 3.1.6 Platform Configuration Attributes

In the last paragraph, the fields **componentIdentifiers, componentIdentifiersURI, platformProperties,** and **platformPropertiesURI** are incorrectly formatted.

Current:

"If such changes impact the structure and semantics of existing fields (componentIdentifiers, componentIdentifiersURI, platformProperties, and platformPropertiesURI) the attribute's OID will be updated to the next version (**tcg-at-platformConfiguration-*v3***)."

Change to:

"If such changes impact the structure and semantics of existing fields (**componentIdentifiers**, **componentIdentifiersUri**, **platformProperties**, and **platformPropertiesUri**) the attribute's OID will be updated to the next version (**tcg-at-platformConfiguration-*v3***)."

3.6 Errata 6

Section 3.1.6 Platform Configuration Attributes

The OIDs **tcg-address-ethernetmac**, **tcg-address-wlanmac**, and **tcg-address-bluetoothmac** listed in this section only support 48-bit MAC addresses. Future OIDs may be defined to support 64-bit MAC addresses.

3.7 Errata 7

Section 2.2.6.1 Certificate Type Label

This section is intended to describe the requirement for Delta Platform Certificates, not Platform Certificates.

Current:

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

Change to:

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

3.8 Errata 8

Sections 3.1.2 Name Attributes, 3.1.3 TCG Specification Attributes, 3.1.7 Platform Configuration Uri Attribute and 4. X.509 ASN.1 Structures and OIDs

The following attribute objects or field have their first letter incorrectly capitalized.

Current:

"**PlatformManufacturerStr**"

Change to:

"**platformManufacturerStr**"

Current:

"**PlatformModel**"

Change to:

"**platformModel**"

Current:

"**PlatformVersion**"

Change to:

"**platformVersion**"

Current:

"**PlatformSerial**"

Change to:

"**platformSerial**"

Current:

"**PlatformManufacturerId**"

Change to:

"**platformManufacturerId**"

Current:

"**Version TCGSpecificationVersion**"

Change to:

"**version TCGSpecificationVersion**"

Current:

"**PlatformConfigUri**"

Change to:

"**platformConfigUri**"

3.9 Errata 9

Section 3.1.2 Name Attributes

Section 3.1.2 incorrectly defines the type **`PrivateEnterpriseNumber`**. The **`manufacturerIdentifier`** value, of type **`PrivateEnterpriseNumber`**, equals one of the IANA private enterprise numbers assigned to the manufacturer of the platform.

Current:

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

Change to:

"**`PrivateEnterpriseNumber ::= OBJECT IDENTIFIER`**"

3.10 Errata 10

Section 3.2 Platform Certificate

The Issuer Unique Id field is incorrectly listed under the **Extensions** section in Table 3. The Issuer Unique Id field actually belongs to the **Field Name** section of Table 3.

Current:

Field Name	**RFC 5755 Type**	**Value**	**Field Status**
Version	INTEGER	V2 (encoded as value 1)	Standard
Serial Number	INTEGER	Positive integer value unique relative to the issuer	Standard
Signature Algorithm	AlgorithmIdentifier	Algorithm used by the issuer to sign this certificate	Standard
Holder	Holder	Identity of the associated TPM EK Certificate, use BaseCertificateID. Additional EK Certificates can be referenced using the TargetingInformation extension.	Standard
Issuer	Name	Distinguished name of the platform certificate issuer	Standard
Validity	notBefore notAfter	Beginning and end of validity period	Standard
Attributes			Standard

TBB Security Assertions	version ccInfo fipsLevel rtmType iso9000Certified iso9000Uri	Describes security-related assertions about the platform TBB	SHOULD
TCG Platform Specification	majorVersion minorVersion revision platformClass	Identifies platform class, version, and revision pf the platform-specific specification	SHOULD
TCG Certificate Type	credentialType	Identifies the Platform Certificate in attribute certificate format	SHOULD
TCG Certificate Specification	majorVersion minorVersion revision	Major, minor, and revision of the Platform Certificate spec under which the Platform Certificate was issued	SHOULD
Platform Configuration	componentIdentifier platformProperties platformPropertiesUri	Platform components and properties MAY be reflected by this attribute	MAY
Platform Configuration URI	URIReference	Points to the PCR list	MAY
Extensions			
Certificate Policies	CertificatePolicies	CertPolicyId CPSuri UserNotice	MUST Non-critical
Subject Alternative Names	GeneralName directoryName	PlatformManufacturerStr PlatformModel PlatformVersion PlatformSerial (optional) PlatformManufacturerId (optional)	MUST non-critical
Targeting Information	TargetingInformation	Additional TPM EK Certificates not included in Holder. Use targetName option.	MAY critical
Authority Key Id	AuthorityKeyIdentifier	Key identifier Issuer name and serial number (optional)	MUST non-critical

Authority Info Access	AuthorityInfoAccessSyntax	id-ad-caIssuers URI to issuing CA id-ad-ocsp (optional) URI to OCSP responder	SHOULD non-critical
CRL Distribution	CRLDistributionPoints	URI to CRL	MAY non-critical
Issuer Unique Id	UniqueIdentifier	Unique value when using a shared issuer name	SHOULD NOT

Table 1: Attribute Certificate Format Fields

Change to:

Field Name	**RFC 5755 Type**	**Value**	**Field Status**
Version	INTEGER	V2 (encoded as value 1)	Standard
Serial Number	INTEGER	Positive integer value unique relative to the issuer	Standard
Signature Algorithm	AlgorithmIdentifier	Algorithm used by the issuer to sign this certificate	Standard
Holder	Holder	Identity of the associated TPM EK Certificate, use BaseCertificateID. Additional EK Certificates can be referenced using the TargetingInformation extension.	Standard
Issuer	Name	Distinguished name of the platform certificate issuer	Standard
Validity	notBefore notAfter	Beginning and end of validity period	Standard
Issuer Unique Id	UniqueIdentifier	Unique value when using a shared issuer name	SHOULD NOT
Attributes			Standard
TBB Security Assertions	version ccInfo fipsLevel rtmType iso9000Certified iso9000Uri	Describes security-related assertions about the platform TBB	SHOULD

TCG Platform Specification	majorVersion minorVersion revision platformClass	Identifies platform class, version, and revision pf the platform-specific specification	SHOULD
TCG Certificate Type	credentialType	Identifies the Platform Certificate in attribute certificate format	SHOULD
TCG Certificate Specification	majorVersion minorVersion revision	Major, minor, and revision of the Platform Certificate spec under which the Platform Certificate was issued	SHOULD
Platform Configuration	componentIdentifier platformProperties platformPropertiesUri	Platform components and properties MAY be reflected by this attribute	MAY
Platform Configuration URI	URIReference	Points to the PCR list	MAY
Extensions			
Certificate Policies	CertificatePolicies	CertPolicyId CPSuri UserNotice	MUST Non-critical
Subject Alternative Names	GeneralName directoryName	PlatformManufacturerStr PlatformModel PlatformVersion PlatformSerial (optional) PlatformManufacturerId (optional)	MUST non-critical
Targeting Information	TargetingInformation	Additional TPM EK Certificates not included in Holder. Use targetName option.	MAY critical
Authority Key Id	AuthorityKeyIdentifier	Key identifier Issuer name and serial number (optional)	MUST non-critical
Authority Info Access	AuthorityInfoAccessSyntax	id-ad-caIssuers URI to issuing CA id-ad-ocsp (optional) URI to OCSP responder	SHOULD non-critical
CRL Distribution	CRLDistributionPoints	URI to CRL	MAY non-critical

Table 2: Attribute Certificate Format Fields

3.11 Errata 11

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

The **tcg-ce-migrationControllerAttestationService**, **tcg-ce-migrationControllerRegistrationService** and **tcg-ce-virtualPlatformBackupService** OIDs are incorrectly specified. The "**(**" should be "**{**".

Current:

"**tcg-ce-migrationControllerAttestationService OBJECT IDENTIFIER ::= (tcg-ce 5}**"

Change to:

"**tcg-ce-migrationControllerAttestationService OBJECT IDENTIFIER ::= {tcg-ce 5}**"

Current:

"**tcg-ce-migrationControllerRegistrationService OBJECT IDENTIFIER ::= (tcg-ce 6}**"

Change to:

"**tcg-ce-migrationControllerRegistrationService OBJECT IDENTIFIER ::= {tcg-ce 6}**"

Current:

"**tcg-ce-virtualPlatformBackupService OBJECT IDENTIFIER ::= (tcg-ce 7}**"

Change to:

"**tcg-ce-virtualPlatformBackupService OBJECT IDENTIFIER ::= {tcg-ce 7}**"

3.12 Errata 12

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

The **platformClass** field is incorrectly specified.

Current:

"**TCGPlatformSpecification ::= SEQUENCE {**
Version TCGSpecificationVersion,
platformClass OCTET STRING SIZE(4) }"

Change to:

"**TCGPlatformSpecification ::= SEQUENCE {**
version TCGSpecificationVersion,
platformClass OCTET STRING (SIZE(4)) }"

3.13 Errata 13

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

Section 4 is missing the definition of the **`Version`** value.

Add:

"**`Version ::= INTEGER { v1(0) }`**"

Before:

"
```
tBBSecurityAssertions ATTRIBUTE ::= {
    WITH SYNTAX TBBSecurityAssertions
    ID tcg-at-tbbSecurityAssertions }
```
"

