

Errata for TCG Platform Certificate Profile
Version 1.1 Revision 19

Errata Version 2.0
December 9, 2021

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

DISCLAIMERS, NOTICES, AND LICENSE TERMS	1
CONTENTS.....	2
1 Introduction	3
2 Clarifications	4
2.1 Clarification 1	4
2.2 Clarification 2	4
2.3 Clarification 3	4
2.4 Clarification 4	4
2.5 Clarification 5	5
2.6 Clarification 6	5
3 Errata	6
3.1 Errata 1	6
3.2 Errata 2	6
3.3 Errata 3	6
3.4 Errata 4	6
3.5 Errata 5	7
3.6 Errata 6	7
3.7 Errata 7	7

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.

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 `componentIdentifer` 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”.