TRUSTED COMPUTING GROUP

ERRATA

Errata for DICE Certificate Profiles

Version 1.0
Revision 0.01
July 23, 2020

Version 1.0
Revision 0.2
June 7, 2021

Contact: admin@trustedcomputinggroup.org

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

CONTENTS

1 REFERENCES

[1] Trusted Computing Group, "DICE Certificate Profiles," 2020. [Online]. Available: https://www.trustedcomputinggroup.org.

[2] Internet Engineering Task Force, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," 2008. [Online]. Available: https://tools.ietf.org/html/rfc5280.

[3] Trusted Computing Group, "DICE Attestaiton Architecture," 2021. [Online]. Available: https://trustedcomputinggroup.org.

[4] Trusted Computing Group, "Hardware Requirements for a Device Identifier Composition Engine," 2018. [Online]. Available: https://www.trustedcomputinggroup.org.

2 INTRODUCTION

This document describes errata for the TCG DICE Certification Profiles Version 1.0 Revision 0.01 as published [1]. 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.

3 CLARIFICATIONS

3.1 Subject Name

The section 5.1.3 heading text “Subject Name” should instead read “Subject and Subject Alternative Name” to clarify that the section deals with both fields. Further, a reference should be added to section 5.1.3 to note these relevant sections of RFC5280 [2]: Subject – section 4.1.2.6 and Subject Alternative Name – section 4.2.1.6 in RFC5280 [2].

In the second sentence in the first paragraph, the text “If the component identity (e.g., TCI_{Ln}) is a device identifier then the device vendor name may also be needed to make Subject unique” should be removed, as it may be confusing to the reader and is unnecessary.

3.2 Policy OIDs

The section 5.1.5 heading text “Policy OIDs” should be clarified to include the purpose that policy OIDs serve in this certificate profile. It should be expressed as “Policy OIDs for Key Usage” to clarify that usage of the policy OIDs within certificate policy extension is not required or anticipated.

4 ERRATA

4.1 Subject Name

There was an omission in section 5.1.3. The following paragraph should be included before the second paragraph of section 5.1.3:

"The subjectAltName extension can be present in certificates issued by an embedded CA, including intermediate certificates that supplement the subject name information in the subject field as specified in RFC5280. If an ECA certificate includes a subjectAltName, subjectAltName could include a HardwareModuleName (as specified in RFC 4108) that provides additional information about the device. See [6] section 8.6."

4.2 Policy OIDs

In the first sentence of the first paragraph, "The policy OID certificate extension may include the following policy OIDs", incorrectly implies the use of a policy OID certificate extension. It should instead read "The policy OIDs for key usage are used with the extended key usage extension (see section 4.2.1.12 in RFC5280 [2]) that may include the following OIDs". It is incorrect to imply the usage of policy OIDs within certificate policy extensions for this certificate profile.

4.3 Initial Device Identifier (IDevID) Certificates

In Table 1 in section 5.1.6.1, the "Policy OID" row in the table incorrectly suggests the usage of policy OIDs within certificate policy extensions. Instead, the content of this row should be moved to the "Extended Key Usage" row and the "Policy OID" row deleted. The table should appear as follows: (note that no other table contents are changed).

FIELD NAME	CONTENTS
Issuer	MUST identify or chain to the device manufacturer / supply chain entity that issues the certificate. If the Issuer is an embedded CA then the ECA issuer MUST chain to the manufacturer CA.
Subject	MUST identify the TCB owning the IDevID private key. The Subject name may be a class identifier implying there may be other device instances sharing the same name.
Subject Public Key Info	Contains the public key and algorithm identifier that is protected by an immutable TCB layer or a TCB layer that SHALL be modifiable only by the Issuer (as per [4]).
Key Usage	If Subject is an ECA then this field MUST contain keyCertSign and MUST NOT contain cRLSign. Otherwise, MUST NOT contain keyCertSign.
Extended Key Usage	This extension MAY contain any appropriate values for the usage model, e.g., id-kp-clientAuth for clients. This extension MUST contain id-tcg-kp-identityInit, and MAY contain id-tcg-kp-eca, or id-tcg-kp-attestInit.
Basic Constraints	If Subject is an ECA then this field MUST contain cA:TRUE and pathLengthConstraint as appropriate. Otherwise, the certificate SHOULD NOT contain BasicConstraints.
Attestation Extensions	A future TCG specification may address attestation extensions.

Table 1: IDevID certificate profile

Previous Table 1:

FIELD NAME	CONTENTS
Issuer	MUST identify or chain to the device manufacturer / supply chain entity that issues the certificate. If the Issuer is an embedded CA then the ECA issuer MUST chain to the manufacturer CA.
Subject	MUST identify the TCB owning the IDevID private key. The Subject name may be a class identifier implying there may be other device instances sharing the same name.
Subject Public Key Info	Contains the public key and algorithm identifier that is protected by an immutable TCB layer or a TCB layer that SHALL be modifiable only by the Issuer (as per [4]).
Key Usage	If Subject is an ECA then this field MUST contain keyCertSign and MUST NOT contain cRLSign. Otherwise, MUST NOT contain keyCertSign.
Extended Key Usage	This field may contain any appropriate values for the usage model, e.g., id-kp-clientAuth for clients.
Basic Constraints	If Subject is an ECA then this field MUST contain cA:TRUE and pathLengthConstraint as appropriate. Otherwise, the certificate SHOULD NOT contain BasicConstraints.
Policy OIDs	MUST contain id-tcg-kp-identityInit, MAY contain id-tcg-kp-eca, id-tcg-kp-attestInit.
Attestation Extensions	A future TCG specification may address attestation extensions.

Table 2: IDevID certificate profile

4.4 Local Device ID (LDevID) Certificates

In Table 2 in section 5.1.6.2, the “Policy OID” row in the table incorrectly suggests the usage of policy OIDs within certificate policy extensions. Instead, the content of this row should be part of the “Extended Key Usage” row.

Further, the references within this table to Table 1 in section 5.1.6.1 should be resolved as they may lead to incorrect assumptions on the part of the reader. The table should appear as follows: (note that no new requirements are added, this error is addressed via the resolution of textual references as they pertain to Local Device ID (LDevID) certificates and the statement of existing requirements provided in the DICE Attestation Architecture specification [3])

FIELD NAME	CONTENTS
Issuer	MUST identify or chain to the owner CA. If the Issuer is an embedded CA then the ECA issuer MUST chain to the owner CA.
Subject	MUST identify the TCB owning the LDevID private key. The Subject name MAY be a class identifier implying there could be other device instances sharing the same name.
Subject Public Key Info	Contains the public key and algorithm identifier that is protected by an immutable TCB layer or a TCB layer that SHALL be modifiable only by the Issuer.
Key Usage	If Subject is an ECA then this field MUST contain keyCertSign and MUST NOT contain cRLSign. Otherwise, MUST NOT contain keyCertSign.
Extended Key Usage	This extension MAY contain any appropriate values for the usage model, e.g., id-kp-clientAuth for clients. This extension MUST contain tcg-dice-kp-identityLoc, and MAY contain tcg-dice-kp-eca, tcg-dice-kp-attestLoc

Basic Constraints	If Subject is an ECA then this field MUST contain cA:TRUE and pathLengthConstraint as appropriate. Otherwise, the certificate SHOULD NOT contain BasicConstraints.
Attestation Extensions	A future TCG specification may address attestation extensions.

Table 3: LDevID certificate profile

Previous Table 2:

FIELD NAME	CONTENTS
Issuer	MUST identify or chain to the owner CA. If the Issuer is an embedded CA then the ECA issuer MUST chain to the owner CA.
Subject	See Section **Error! Reference source not found.** - Subject
Subject Public Key Info	See Section **Error! Reference source not found.** – Subject Public Key Info
Key Usage	See Section **Error! Reference source not found.** – Key Usage
Extended Key Usage	See Section **Error! Reference source not found.** – Extended Key Usage
Basic Constraints	See Section **Error! Reference source not found.** – Basic Constraints
Policy OIDs	MUST contain id-tcg-kp-identityLoc, may contain id-tcg-kp-eca, id-tcg-kp-attestLoc.
Assertions Extensions	See Section **Error! Reference source not found.** – *Attestation Extensions*

Table 4: LDevID certificate profile

4.5 ECA Certificates

In Table 3 in section 5.1.6.3, the “Policy OID” row in the table incorrectly suggests the usage of policy OIDs within certificate policy extensions. Instead, this row should be renamed “Extended Key Usage”. The table should appear as follows: (note that no other table contents are changed).

FIELD NAME	CONTENTS
Issuer	MUST identify the CA or embedded CA that issues the certificate. The Issuer MUST ensure that the private portion of the Subject Public Key is protected by a TCB. If Issuer is an embedded CA, then Issuer MUST identify the TCB instance that issues this certificate.
Subject	MUST identify the TCB containing ECA functionality.
Subject Public Key Info	MUST contain the current TCB Layer ECA public key and algorithm identifier.
Key Usage	MUST contain keyCertSign. MUST NOT contain cRLSign, may contain other KeyUsage attributes as appropriate
Extended Key Usage	This extension MUST contain id-tcg-kp-eca, and MAY contain id-tcg-kp-attestInit, id-tcg-kp-attestLoc, id-tcg-kp-identityInit, or id-tcg-kp-identityLoc
Basic Constraints	MUST contain cA:TRUE and pathLengthConstraint as appropriate
Attestation Extensions	A future TCG specification may address attestation extensions.
CRLDistributionPoints Extension	MUST be present.

Table 3: ECA certificate profile

Previous Table 3:

FIELD NAME	CONTENTS
Issuer	MUST identify the CA or embedded CA that issues the certificate. The Issuer MUST ensure that the private portion of the Subject Public Key is protected by a TCB. If Issuer is an embedded CA, then Issuer MUST identify the TCB instance that issues this certificate.
Subject	MUST identify the TCB containing ECA functionality.
Subject Public Key Info	MUST contain the current TCB Layer ECA public key and algorithm identifier.
Key Usage	MUST contain keyCertSign. MUST NOT contain cRLSign, may contain other KeyUsage attributes as appropriate
Basic Constraints	MUST contain cA:TRUE and pathLengthConstraint as appropriate
Policy OIDs	MUST contain tcg-dice-kp-eca, may contain tcg-dice-kp-attestInit, tcg-dice-kp-attestLoc, tcg-dice-kp-identityInit, and/or tcg-dice-kp-identityLoc
Attestation Extensions	See Section **Error! Reference source not found.** – *Attestation Extensions*
CRLDistributionPoints Extension	MUST be present.

Table 3: ECA certificate profile

4.6 Attestation Certificates

In Table 4 in section 5.1.6.4, the “Policy OID” row in the table incorrectly suggests the usage of the policy OID certificate extension. Instead, the content of this row should be moved to the “Extended Key Usage” row and the “Policy OID” row deleted. The table should appear as follows: (note that no other table contents are changed).

FIELD NAME	CONTENTS
Issuer	MUST contain the name of the embedded CA that issues the Subject Public Key certificate. The Issuer may be an ECA (i.e., the previous TCB layer) or an external CA. If the Issuer is an ECA, the Issuer MUST identify the TCB that issues this certificate.
Subject	MUST identify a TCB class or instance.
Subject Public Key Info	MUST contain a current TCB attestation public key and algorithm identifier.
Key Usage	If Subject is an ECA then this field MUST contain keyCertSign and MUST NOT contain cRLSign. Otherwise, MUST NOT contain keyCertSign.
Extended Key Usage	May contain any appropriate values for the usage model, e.g., id-kp-clientAuth for clients. This extension MUST contain either id-tcg-kp-attestInit or id-tcg-kp-attestLoc.
Basic Constraints	If Subject is an ECA then this field MUST contain cA:TRUE and pathLengthConstraint as appropriate. Otherwise, the certificate SHOULD NOT contain BasicConstraints.
Attestation Extensions	A future TCG specification may address attestation extensions.

Table 4: Attestation Identity certificate profile

Previous Table 4:

FIELD NAME	CONTENTS
Issuer	MUST contain the name of the embedded CA that issues the Subject Public Key certificate. The Issuer may be an ECA (i.e., the previous TCB layer) or an external CA. If the Issuer is an ECA, the Issuer MUST identify the TCB that issues this certificate.
Subject	MUST identify a TCB class or instance.
Subject Public Key Info	MUST contain a current TCB attestation public key and algorithm identifier.
Key Usage	If Subject is an ECA then this field MUST contain keyCertSign and MUST NOT contain cRLSign. Otherwise MUST NOT contain keyCertSign.
Extended Key Usage	May contain any appropriate values for the usage model, e.g., id-kp-clientAuth for clients.
Basic Constraints	If Subject is an ECA then this field MUST contain cA:TRUE and pathLengthConstraint as appropriate. Otherwise the certificate SHOULD NOT contain BasicConstraints.
Policy OIDs	MUST contain either tcg-dice-kp-attestInit or tcg-dice-kp-attestLoc.
Attestation Extensions	See Section **Error! Reference source not found.** – *Attestation Extensions*

Table 4: Attestation Identity certificate profile

