

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

MP303 ‘Aligning DCC Certificate processes with SMKI standards’

Annex A

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Appendix A ‘Device Certificate Policy’

These changes have been redlined against Appendix A version 4.0.

Amend Annex B ‘Device Certificate Profile’, ‘Root DCA Certificate Profile’ & ‘Issuing DCA Certificate Profile’ Tables as follows:

CHANGES TO THE ISSUER

Device Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String <u>PrintableString</u>	Globally unique common name of Issuing DCA of up to 4 Octets (as defined in the Issuing DCA Certificate Profile)	

Root DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the	UTF8String <u>PrintableString</u>	Globally unique common name of Root DCA of up to 4 Octets	

“Issuer X520 Common Name”)			
----------------------------	--	--	--

Issuing DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String <u>PrintableString</u>	Globally unique name of Root DCA of up to 4 Octets (as defined in the Root DCA Certificate Profile)	

Amend Annex B ‘Root DCA Certificate Profile’ & ‘Issuing DCA Certificate Profile’ Tables as follows:

CHANGES TO THE SUBJECT

Root DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the	UTF8String <u>PrintableString</u>	Globally unique name of Root DCA of up to 4 Octets (same as Issuer name)	

“Subject X520 Common Name”)			
--------------------------------	--	--	--

Issuing DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndV alue structure within the subject field whose type is id-at- commonName (the “Subject X520 Common Name”)	UTF8String <u>PrintableString</u>	Globally unique name of Issuing DCA of up to 4 Octets	

Amend Annex B ‘Device Certificate Profile Table’ as follows:

Device Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAnd Value structure within the subject field whose type is id-at- commonName (the “Subject X520 Common Name”)	UTF8String <u>EMPTY</u>	EMPTY	

Amend Annex B ‘subjectAltName’ description as follows:

The ~~non~~-critical subjectAltName extension shall contain a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-hardwareModuleName) as defined in RFC 4108 section 5. The hwSerialNum field shall be set to the Device ID.

Appendix B ‘Organisation Certificate Policy’

These changes have been redlined against Appendix B version 10.0.

Amend Annex B ‘Organisation Certificate Profile’, ‘Root OCA Certificate Profile’ & ‘Issuing OCA Certificate Profile’ Tables as follows:

CHANGES TO THE ISSUER

Organisation Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String <u>PrintableString</u>	Globally unique common name of Issuing OCA of up to 4 Octets (as defined in the Issuing OCA Certificate Profile)	

Root OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the	UTF8String <u>PrintableString</u>	Globally unique common name of Root OCA of up to 4 Octets	

“Issuer X520 Common Name”)			
----------------------------	--	--	--

Issuing OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String <u>PrintableString</u>	Globally unique name of Root OCA of up to 4 Octets (as defined in the Root OCA Certificate Profile)	

Amend Annex B ‘Root OCA Certificate Profile’ & ‘Issuing OCA Certificate Profile’ Tables as follows:

CHANGES TO THE SUBJECT

Root OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String <u>PrintableString</u>	Globally unique name of Root OCA of up to 4 Octets (same as Issuer name)	

Issuing OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
The value field of the AttributeTypeAnd Value structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String <u>PrintableString</u>	Globally unique name of Issuing OCA of up to 4 Octets	

Appendix M 'SMKI Interface Design Specification'

These changes have been redlined against Appendix M version 7.0.

Amend Clause 2.3.1.7 as follows:

Following receipt by the DCC of an ad hoc Device CSR or Batched CSR to the SMKI Portal via DCC Gateway Connection, the DCC shall:

- a) for an ad hoc Device CSR submission:
 - i. validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10 (the criticality of the extensions is not validated);
 - ii. apply the Eligible Subscriber checks as set out in Section L3.16 of the Code; and
 - iii. either accept, or reject the CSR; and
 - A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or
 - B. where the CSR is rejected, log an error and return an error message that is in accordance with "Response Status" table in Appendix A of this document, via the SMKI Portal interface to the Authorised Subscriber; or
- b) for a Batched CSR submission:
 - i. validate that the structure of the submitted .zip file is in accordance with the format set out in Appendix F to this document (the criticality of the extensions is not validated);
 - ii. validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000;
 - A. should the Batched CSR contain more than 50,000 CSRs, the DCC shall reject the Batched CSR (including all of the Device CSRs contained within the Batched CSR); or
 - B. should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below;
 - iii. either accept, or reject the Batched CSR and/or each constituent Device CSR, log relevant errors and return a synchronous response via the SMKI Portal interface to notify the Authorised Subscriber as to:
 - A. where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR; or
 - B. where the Batched CSR is rejected, relevant error messages that are in accordance with "Response Status" table in Appendix C of this document.

Amend Clause 2.3.1.8 as follows:

If a Device CSR is accepted, the DCC shall:

a) for an ad hoc Device CSR submission:

- i. perform such additional checks as DCC determines is necessary on the Device CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;
- ii. check that less than 100 Device Certificates have previously been Issued for the Device ID to which the Device CSR relates;
- iii. either approve, or reject the Device CSR; and
 - A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or
 - B. where the CSR is rejected, log an error that is in accordance with “Response Status” table in Appendix A of this document, and return an error message via the SMKI Portal interface to the Authorised Subscriber; or

b) for a Batched CSR submission:

- i. validate the format, and verify the signature of each Device CSR contained within the Batched CSR in line with Appendix F of this document and PKCS#10 (the criticality of the extensions is not validated);
- ii. perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;
- iii. apply the Eligible Subscriber checks as set out in Section L3.16 of the Code;
- iv. check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates;
- v. either approve, or reject each Device CSR in the Batched CSR; and
 - A. where the CSR is approved, include a notification in the Batched CSR response file, as set out in section 2.3.1.9d) of this document, to the Authorised Subscriber; or
 - B. where the CSR is rejected, log an error that is in accordance with “Response Status” table in Appendix C of this document, and include an error notification in the Batched CSR response file, as set out in section 2.3.1.9d) of this document.

Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it.

If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition.

Amend Clause 2.4.1.2 as follows:

Following receipt of a Device CSR to the Ad Hoc Device CSR Web Service interface, the DCC shall:

- a) validate that the format of the XML document complies with the XML schema as set out in Appendix B of this document;
- b) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10 (the criticality of the extensions is not validated);
- c) either accept, or reject the CSR; and
 - i. where the CSR is rejected, log an error and return an error message in the synchronous XML response, to the Authorised Subscriber's systems.

Amend Clause 2.5.1.3 as follows:

Upon acceptance of a Batched CSR as set out immediately above, the DCC shall:

- a) validate the format, and verify the Digital Signature of each CSR in line with Appendix F of this document and PKCS#10 (the criticality of the extensions is not validated);
- b) perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;
- c) apply the Eligible Subscriber checks as set out in Section L3.16 of the Code;
- d) check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates;
- e) either approve, or reject each Device CSR in the Batched CSR and include (where applicable) resulting Device Certificates, notifications and error messages in a Batched CSR XML response file that is separate from the synchronous response file described in section 2.5.1.2 of this document; and
 - i. where the CSR is approved, include a notification in the Batched CSR XML response file, to the Authorised Subscriber; or
 - ii. where the CSR is rejected, log an error and include an error notification in the Batched CSR XML response file.

Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it.

If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition.

Amend Appendix F ‘Information to be contained within a Device CSR’ Table as follows:

Section	Attributes				Value
Version					Version 0
Subject					Empty
Subject Public Key Information	Public Key Algorithm				id-ecPublicKey
	Prime256r1 (256 bit)				Public Key Data
Key Usage	Criticality				True
	Key Usage				digitalSignature or keyAgreement
Subject Alternative Name	<u>Criticality</u>				<u>True</u>
	General Name	Other Name	id-on-hardwareModuleName	hwType	Object Identifier, OID
				hwSerialNum	Device ID (EUI-64)
Signature Algorithm					ecdsa-with-SHA256

Appendix T 'DCCKI Interface Design Specification'

These changes have been redlined against Appendix T version 5.0.

Amend Section 3.9 as follows:

3.9 Prior to Digitally Signing the DCCKI Certificate Signing Request, the DCCKI Eligible Subscriber shall append to the footer of the PKCS#10 file, the Issuer which shall be URL encoded (as specified in the ~~IETF RFC 4~~RFC 1738 and RFC 2253) and serial number of the Organisation Certificate with preceding “,” separators.