

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.

MP290 ‘Incorporation of Category 3 Issue Resolution Proposal into the SEC – Batch 11 and GBCS Changes’

Annex B

Legal text – version 0.2

About this document

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

SEC Schedule 8 – GB Companion Specification

These changes have been redlined against Great Britain Companion Specification (GBCS) version 3.2

Amend 4.3.2.8.2 Device requirements as follows:

The requirements in this Section 4.3.2.8.2 shall apply only to Use Case CS02b (Update Security Credentials).

Where a Device has successfully completed all required Command Authenticity and Integrity checks on a Command of type covered by Use Case CS02b it has received, the Device shall undertake either:

- Certification Path Validation, including time checks; or
- Certification Path Validation, excluding time checks.

If the Device does not have Reliable Time (as defined in Use Cases GCS28 and ECS70 Set Clock) it shall always undertake Certification Path Validation, excluding time checks. Otherwise the validation to be undertaken shall be determined by the contents of the Remote Party Command instance. For clarity, Device types which are not required to have a clock, shall always undertake Certification Path Validation, excluding time checks.

The Device shall undertake Certification Path Validation, including time checks:

- either by using the algorithm specified in IETF RFC 5280 section 6.1; or
- by using functionality equivalent to the external behaviour resulting from that algorithm.

The Device shall undertake Certification Path Validation, excluding time checks:

- either by using the algorithm specified in IETF RFC 5280 section 6.1 but not applying the check at 6.1.3 (a) (2) ('the certificate validity period includes the current time'); or
- by using functionality equivalent to the external behaviour resulting from that algorithm where not applying the check that 'the certificate validity period includes the current time'.

The 'trust anchor' information (with the meaning in IETF RFC 5280) shall be in the root Security Credentials held on the Device.

If the Device's Certificate Path Validation does not confirm the required certification path validity, then the Device shall undertake no further processing of the Command, except for the issuance of a Message containing an execution Outcome (with its Section 13.3.4.6 meaning) notifying that the Command was unsuccessful in applying at least some of the changes in the Command.

The requirements in this Section 4.3.2.8.2 shall apply only to Use Case CS02b (Update Security Credentials).

Where a Device has successfully completed all required Command Authenticity and Integrity checks on a Command of type covered by Use Case CS02b it has received, the Device shall undertake either:

- Certification Path Validation, including time checks; or
- Certification Path Validation, excluding time checks.

If the Device does not have Reliable Time (as defined in Use Cases GCS28 and ECS70 Set Clock) it shall always undertake Certification Path Validation, excluding time checks. Otherwise the validation to be undertaken shall be determined by the contents of the Remote Party Command instance. For clarity, Device types which are not required to have a clock, shall always undertake Certification Path Validation, excluding time checks.

The Device shall undertake Certification Path Validation, including time checks:

- either by using the algorithm specified in IETF RFC 5280 section 6.1; or
- by using functionality equivalent to the external behaviour resulting from that algorithm.

The Device shall undertake Certification Path Validation, excluding time checks:

- either by using the algorithm specified in IETF RFC 5280 section 6.1 but not applying the check at 6.1.3 (a) (2) ('the certificate validity period includes the current time'); or
- by using functionality equivalent to the external behaviour resulting from that algorithm where not applying the check that 'the certificate validity period includes the current time'.

For clarity, Certification Path Validation shall only apply to replacement Certificates in the Command, not to an existing Certificate in a Trust Anchor cell.

The 'trust anchor' information (with the meaning in IETF RFC 5280) shall be in the root Security Credentials held on the Device.

If the Device's Certificate Path Validation does not confirm the required certification path validity, then the Device shall undertake no further processing of the Command, except for the issuance of a Message containing an execution Outcome (with its Section 13.3.4.6 meaning) notifying that the Command was unsuccessful in applying at least some of the changes in the Command.

Amend Table 13.3.4.1 Command Payload construction as follows:

applyTimeBasedCPVChecks	[1] IMPLICIT INTEGER	Disapply (1)	DEFAULT apply	Only to be present if the Remote Party sending the Command is instructing the Device not to apply time based checks as part
-------------------------	----------------------------	--------------	------------------	---

				of Certification Path Validation of <u>replacements</u> . This should only be in exceptional circumstances. (e.g. supplier credentials on the Device have expired without replacement for unforeseen reasons)
--	--	--	--	---

replacements	SEQUENCE OF	Disapply (1)	DEFAULT apply	Provide a list of the replacements <u>replacement Certificates</u> . Each <u>entry in replacements</u> contains a new 'end entity' Certificate and the identity of the Trust Anchor Cell which is to have its contents replaced using that Certificate.
--------------	-------------	--------------	---------------	--

trustAnchorCellUsage	INTEGER	prePaymentTopUp (1)}	DEFAULT management	Should be absent unless: - the deviceType is eSME or gSME; and - the supplier <u>Supplier</u> operating the Device wishes to use prepayment top up functionality on the Device, and this is a replacement of the corresponding certificate <u>corresponding Certificate</u>. Note the certificate <u>Certificate</u> specified for use in the {supplier, keyAgreement, prePaymentTopUp} Trust Anchor Cell may be the same key as that specified for the {supplier, keyAgreement, management} Trust
----------------------	---------	----------------------	--------------------	--

				Anchor Cell or may be different.
--	--	--	--	----------------------------------

certificationPathCertificates	SEQUENCE OF Certificate	The list of certificates needed for Certification Path Validation	At least one Certificate must be present	Provide the certificates <u>Certification Authority Certificates</u> needed to undertake Certification Path Validation against the root public key held on the Device. The number of these may be less than the number of replacements <u>replacement certificates</u> (e.g. a supplier <u>Supplier</u> may replace all of its certificates <u>Certificates</u> but may only need to supply one Certification Authority Certificate to link them all back to root
-------------------------------	-------------------------	---	--	---

Amend 13.3.5.9 Verifying the authenticity of replacement certificates as follows:

For each replacement Certificate in replacements, ~~the~~ The Device shall first apply the requirements of Section 12.6 (Device processing of Certificates). If any of those checks fail, the Section 13.3.5.9 check fails.