Annex A: SMKI Document Set review – concluding observations & recommendations

1. Summary

These observations were specifically raised with the SMKI PMA sub-group, which had oversight of the review. The recommendations are as agreed by the sub-group and subsequently formally approved by the SMKI PMA.

There are proposed typographical corrections to all of the reviewed SEC Appendices, as reflected in the redlined versions provided. Those redlined proposals have associated comments to explain the rationale, where that may not be immediately apparent.

Note that where recommendations in this document are to change drafting in the SEC Appendix, those changes have been made in the redlined documents provided.

Specific recommendations in relation to IETF RFCs are included in the document ‘SMKI Document set - RFC analysis v005’. These have since been the subject of investigation by the SMKI Specialist and a conclusive recommendation has been agreed by the SMKI PMA and accepted by the DCC where appropriate.

2. SEC Section L

Document	SEC Section L
Reference	Section L observation 1
Observation	The SEC specifies that the SMKI PMA Chair will be deemed to have nominated the SMKI Specialist to act as an Alternate for the SMKI PMA Chair and it would be preferable to have the flexibility to adopt the same arrangement as for other sub-committees without this restriction.
Recommendation	Amend Section L1.12 to remove sub-section (a) and amend as below
Status	Removal reflected in SEC Section L1.12 - proposed changes v0001
Detail	
L1.12 Each SMKI PMA Member shall be entitled to appoint an Alternate in accordance with Section C5.19 (as it applies pursuant to Section L1.15~~). ; provided that:~~ ~~(a) the SMKI PMA Chair will be deemed to have nominated the SMKI Specialist to act as Alternate for~~ ~~the SMKI PMA Chair; and~~ ~~(b) where the SMKI Specialist is unavailable,~~ The SMKI PMA Chair must nominate another person to act	

as Alternate for the SMKI PMA Chair (which person may be the SMKI Specialist but may not be another SMKI PMA Member, and which person must be sufficiently independent of any particular Party or class of Parties).

Document	SEC Section L
Reference	Section L observation 2
Observation	To align with MP128B, the SEC needs to provide for the SMKI PMA to direct the DCC to undertake SMKI Recovery for purposes other than a Compromise or suspected Compromise e.g. correcting incorrect SMKI Certificates.
Recommendation	Add Sections L10.31 to L10.33 to specify the circumstances and requirements for the SMKI PMA to direct the DCC to undertake a SMKI Recovery exercise.
Status	Additional SEC Sections L10.31 to L10.33 - proposed changes v0001
Detail	
Further Use of the Recovery Private Key – see new draft text L10.31 – L10.33	

3. SEC Appendix A Device Certificate Policy

Document	SEC Appendix A Device Certificate Policy
Reference	Appendix A observation 1
Observation	Provisions stated as covered by the SMKI RAPP but not apparently covered by the SMKI RAPP
Recommendation	Set section 3.2.4 to 'Not used'
Status	Removal reflected in SEC Appendix A - Device Certificate Policy v2.0 - proposed typographical changes v0002
Detail	
Section 3.2.4 states: (A) Provision is made in the SMKI RAPP in relation to the Authentication of Devices. The definition of 'Authentication' is: means the process of establishing that an individual, organisation, System or Device is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly). There does not appear to be any provision in the SMKI RAPP in relation to Authentication of Devices and there is no way to 'Authenticate' that a Device is what is asserted in the CSR. Indeed, CSRs could be submitted before the corresponding Device even exists.	

Document	SEC Appendix A Device Certificate Policy
Reference	Appendix A observation 2
Observation	Provisions stated as covered by the SMKI RAPP but not apparently covered by the SMKI RAPP

Recommendation	Delete part (ii)
Status	Removal reflected in SEC Appendix A - Device Certificate Policy v2.0 - proposed typographical changes v0002
Detail	

Section 4.1.1 states:

> (A) Provision is made in the SMKI RAPP in relation to:
>
> (i) …
>
> (ii) in respect of a DCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain a DCA Certificate.

There appears no provision for obtaining DCA Certificates in the SMKI RAPP.

This is a mirror of Appendix B observation 1.

Document	SEC Appendix A Device Certificate Policy
Reference	Appendix A observation 3
Observation	Information Assurance Standard does not appear to be available anymore
Recommendation	Change the reference to be a URL (https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)
Status	Change reflected in SEC Appendix A – Device Certificate Policy v2.0 - proposed typographical changes v0002
Detail	

Section 5.1.7 states:

> (A) The DCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the DCA are disposed of only using secure methods of disposal in accordance with:
>
> (i) Information Assurance Standard No. 5:2011 (Secure Sanitisation);

This Information Assurance Standard does not appear to be available anymore.

This is a mirror of Appendix B observation 3.

Document	SEC Appendix A Device Certificate Policy
Reference	Appendix A observation 4
Observation	Standard superseded
Recommendation	Update the reference from 2008 to 2014
Status	Change reflected in SEC Appendix A - Device Certificate Policy v2.0 - proposed typographical changes v0002
Detail	

Section 5.4.4 states:

> (A) The DCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time

British Standard BS 10008:2008 appears to have been superseded by British Standard BS 10008:2014 (https://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/).

This same standard is referenced in 5.4.2.

This is a mirror of Appendix B observation 4

Document	SEC Appendix A Device Certificate Policy
Reference	Appendix A observation 5
Observation	RFC 4108 is 61 pages but the only part of relevance to Appendix A is section 5 and for clarity, this should be referenced to avoid confusion. RFC 4108 is also used more widely in GBCS.
Recommendation	Change the reference to ‘RFC 4108 section 5’
Status	Change reflected in SEC Appendix A – Device Certificate Policy v2.0 - proposed changes to RFC 4108 references
Detail	Affects pages 69, 72 and 74

Page 69
contain subjectAltName extension which contains a single GeneralName of type
otherName that is further sub-typed as a hardwareModuleName (id-onhardwareModuleName)
as defined in RFC 4108 section 5. The hwSerialNum field shall be
set to the Device’s Entity Identifier. In adherence to IETF RFC 5280, the
subjectAltName shall be marked as critical;

Page 72
subjectAltName OtherName contains a single
GeneralName of type
OtherName that is
further sub-typed as a
HardwareModuleNa
me (id-onhardwareModuleNa
me) as defined in RFC
4108 section 5. The
hwSerialNum field
shall be set to the

Device's Entity Identifier Page 74 The non-critical subjectAltName extension shall contain a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-onhardwareModuleName) as defined in RFC 4108 section 5. The hwSerialNum field shall be set to the Device ID.

4. SEC Appendix B Organisation Certificate Policy

Document	SEC Appendix B Organisation Certificate Policy
Reference	Appendix B observation 1
Observation	Provisions stated as covered by the SMKI RAPP but not apparently covered by the SMKI RAPP
Recommendation	Delete part (ii)
Status	Removal reflected in SEC Appendix B - Organisation Certificate Policy v3.0 - proposed typographical changes v002
Detail	

Section 4.1.1 states:

> (A) Provision is made in the SMKI RAPP in relation to:
>
> (i) …
>
> (ii) in respect of an OCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain an OCA Certificate.

There appears no provision for obtaining OCA Certificates in the SMKI RAPP.

Document	SEC Appendix B Organisation Certificate Policy
Reference	Appendix B observation 2
Observation	There does not appear any definition as to when a Certificate is treated as accepted
Recommendation	To note
Status	No further proposed action
Detail	

Section 4.4.1 states:

> (B) A Certificate which has been Issued by the OCA shall not be treated as valid for any purposes of this Policy or the Code until it is treated as having been accepted by the Eligible Subscriber to which it was Issued.

From the SMKI IDS section 2.3.1.5:

> Upon downloading the Issued Organisation Certificate, the Authorised Subscriber shall in accordance with L11.5 of the Code, establish that the information contained in the resulting

Organisation Certificate is consistent with the information contained in the corresponding Organisation CSR.

Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Organisation Certificate in accordance with L11.5 by notifying the DCC via the DCC's Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

Upon rejection of the Organisation Certificate by an Authorised Subscriber and subsequent notification to the DCC of such rejection, the DCC shall revoke the Organisation Certificate, place the Organisation Certificate on the Organisation CRL, and lodge the updated Organisation CRL in the SMKI Repository in accordance with Appendix B of the Code.

Thus, there does not appear any definition as to when a Certificate is treated as accepted by the Eligible Subscriber to which it was Issued.

Document	SEC Appendix B Organisation Certificate Policy
Reference	Appendix B observation 3
Observation	Information Assurance Standard does not appear to be available anymore
Recommendation	Change the reference to be a URL (https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)
Status	Change reflected in SEC Appendix B - Organisation Certificate Policy v3.0 - proposed typographical changes v002
Detail	

Section 5.1.7 states:

(A) The OCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the OCA are disposed of only using secure methods of disposal in accordance with:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation);

This Information Assurance Standard does not appear to be available anymore.

Document	SEC Appendix B Organisation Certificate Policy
Reference	Appendix B observation 4
Observation	Standard superseded
Recommendation	Update reference from 2008 to 2014
Status	Change reflected in SEC Appendix B - Organisation Certificate Policy v3.0 - proposed typographical changes v002
Detail	

Section 5.4.4 states:

(A) The OCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with: (a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or (b) any equivalent to that British Standard which updates or replaces it from time to time British Standard BS 10008:2008 appears to have been superseded by British Standard BS 10008:2014 (https://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/). This same standard is referenced in 5.4.2.

Document	SEC Appendix B Organisation Certificate Policy
Reference	Appendix B observation 5
Observation	Provisions stated as covered by the SMKI RAPP but not apparently covered by the SMKI RAPP
Recommendation	Amend documentation in SMKI RAPP
Status	Changes reflected in SEC Appendix D - SMKI Registration Authority Policies and Procedures - proposed typographical changes v002
Detail	
Section 4.9.3 states: (B) On receiving a Certificate Revocation Request, the OCA shall take reasonable steps to: (i) … (ii) … (iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy. There appears no provision to cover (iii) in the SMKI RAPP.	

Document	SEC Appendix B Organisation Certificate Policy
Reference	Appendix B observation 6
Observation	RFC 6318 references are unneeded
Recommendation	Remove RFC 6318 references
Status	Changes reflected in SEC Appendix D - SMKI Registration Authority Policies and Procedures - proposed typographical changes v002
Detail	
The three references to RFC 6318 are just to reference the OID. In all three cases the OID is directly referenced so reference to RFC 6318 is unneeded.	

Document	SEC Appendix B Organisation Certificate Policy
Reference	Appendix B observation 7
Observation	An addition to section 6.2.6 is needed
Recommendation	Add a sub-section (c) to Section 6.2.6
Status	The change is needed to support operational realities such as a change/migration of Trusted Service Provider (TSP) or datacentre
Detail	
The current re-platforming of the Trusted Service Provider (TSP) due to the existing Digicert platform being discontinued requires the OCA Private Key to be transferred to a different datacentre. Appendix B section 6.2.6 does not explicitly cover such a situation and allowing the SMKI PMA to give approval following SSC consultation is a sensible addition.	

5. SEC Appendix C SMKI Compliance Policy

Document	SEC Appendix C SMKI Compliance Policy
Reference	Appendix C observation 1
Observation	Section 5 'Subsequent Assurance Assessment' does not equivalent obligations to other compliance policy's – such as the S1SPKM Compliance Policy
Recommendation	Add additional obligations to section 5 to bring drafting in line with S1SPKM Compliance Policy
Status	Additional drafting added in 'SEC Appendix C - SMKI Compliance Policy - proposed changes v0002'
Detail	
Section 5 needs more detail to align with Appendix AO (S1SPKM Compliance Policy).	

6. SEC Appendix D SMKI Registration Authority Policies and Procedures

Document	SEC Appendix D SMKI Registration Authority Policies and Procedures
Reference	Appendix D observation 1
Observation	Requirement on submitting organisation appears not possible to meet
Recommendation	DCC to provide drafting to detail their actual process, and for that to be reflected in drafting. Updated: Agreed with DCC to amend the form in Appendix A1 of SEC Appendix D.
Status	Pending DCC input. Agreed subject to SMKI PMA approval in December 2021
Detail	
Section 5.1 states:	

> The applicant organisation shall complete the Organisation Information Form, as set out in SMKI RAPP Annex A (A1). In doing so, the applicant organisation shall ensure that:
>
> a. the information entered on the form is complete and accurate;
>
> b. the EUI-64 Compliant identifier range for any particular User Role is defined by the applicant organisation such that the range is continuous and does not overlap with the EUI-64 Compliant identifier range for any other User Role, other than where a particular EUI-64 Compliant identifier is allowed to be used for more than one User Role in accordance with H1.5;

The underlined text appears not possible as the form referred to does not allow the mapping of EUI64 identifiers to User Roles. Update: Agreed with DCC to amend the form subject to SMKI PMA approval. No SEC changes needed.

Document	SEC Appendix D SMKI Registration Authority Policies and Procedures
Reference	Appendix D observation 2
Observation	Unclear as to the role of SMKI PMA members in credential revocations
Recommendation	Withdraw this observation ~~Remove reference to SMKI PMA member~~
Status	Removal reflected in SEC Appendix D - SMKI Registration Authority Policies and Procedures - proposed typographical changes v002 since withdrawn
Detail	

Section 8.3.4.7 states:

> Notify DCC's CISO, SMKI Registration Authority Manager, or SMKI PMA Member who submitted the original Credential Revocation Request Form that the revocation has been completed.

However, Section 8.3.4.1 states:

> Complete the Credential Revocation Request Form as set out in SMKI RAPP Annex A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised:
>
> a. for a member of SMKI Registration Authority Personnel, by a SMKI Registration Authority Manager; or
>
> b. for a SMKI Registration Authority Manager, by the DCC's CISO.

~~Thus, it is not clear why SMKI PMA members are referred to in 8.3.4.7 / the circumstances in which a SMKI PMA member may submit a Credential Revocation Request.~~

On further review, the references in 8.3.4 are consistent with the requirements in 8.3.3 and should be maintained as per the original drafting.

7. SEC Appendix J Enduring Test Approach Document

<table>
<tr><td><b>Document</b></td><td>SEC Appendix J Enduring Test Approach Document</td></tr>
<tr><td><b>Reference</b></td><td>Appendix J observation 1</td></tr>
<tr><td><b>Observation</b></td><td>Unclear as to where the DCC publishes the Test Certificate Policy. The SEC requires it to be published but it is not currently available.</td></tr>
<tr><td><b>Recommendation</b></td><td>Clarify that the Test Certificate Policy should be published on the DCC Website as for other SEC references (App L 3.4.2(b) and many others)</td></tr>
<tr><td><b>Status</b></td><td>Amendment to Appendix J Section 3.2 as shown below</td></tr>
<tr><td><b>Detail</b></td><td></td></tr>
<tr><td colspan="2">3.2 For the purposes of clause 3.1, the Test Documents means:
(a) the Test Certificate Policy, which shall be a document published on by the DCC website and approved by the SMKI PMA which corresponds (insofar as relevant in respect of the Testing Services) in purpose, content and effect to the Organisation Certificate Policy, the Device Certificate Policy and the IKI Certificate Policy;</td></tr>
</table>

8. SEC Appendix K SMKI and Repository Test Scenarios Document

No observations but there are proposed typographical corrections reflected in the redlined version with associated explanatory comments.

9. SEC Appendix L SMKI Repository Procedure

<table>
<tr><td><b>Document</b></td><td>SEC-Appendix-L-SMKI-Recovery-Procedure</td></tr>
<tr><td><b>Reference</b></td><td>Appendix L observation 1</td></tr>
<tr><td><b>Observation</b></td><td>The scope of Appendix L seems more limited than that specified in SEC section L, in terms of the private keys within scope</td></tr>
<tr><td><b>Recommendation</b></td><td>Drafting changes to be made to align scope between Section L10.30 and Appendix L1.2, including to cover compromise of any Enduring CoS related private keys (so XML signing keys across the board).
In relation to L10.30 (vi) in Appendix L (S1SP private keys), drafting is to state that recovery is covered in the relevant CPS.</td></tr>
<tr><td><b>Status</b></td><td>Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005</td></tr>
<tr><td><b>Detail</b></td><td></td></tr>
<tr><td colspan="2">SEC L10.1 states that the SMKI Recovery Procedure sets out provisions ‘in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised’.

SEC L10.30 defines a Relevant Private Key as:
(i) the Contingency Symmetric Key;
(ii) a Private Key which is associated with a Public Key contained in any Organisation Certificate or OCA Certificate, Data from which is used to populate the Device Security Credentials of a Device comprising part of an Enrolled Smart Metering System;</td></tr>
</table>

(iii) a Private Key which is associated with a Public Key contained in any Organisation Certificate, Data from which is used to populate part of any Device Security Credentials held by an S1SP;
(iv) a Private Key which was used as part of the process of Issuing any OCA Certificate or Organisation Certificate referred to in paragraph (ii) or (iii) above;
(v) a Private Key which is used to Digitally Sign any XML Document, and which is associated with a Public Key that is contained within any Organisation Certificate; or
(vi) a Private Key which is associated with a Public Key contained in any certificate issued in accordance with an S1SPKI Certificate Policy, and which is determined by the SMKI PMA as being a Private Key for the purposes of this paragraph;

Appendix L 1.2 (scope) **states that the scope of Appendix L is more limited**:

a) Private Keys associated with Organisation Certificates stored on SMETS2+ Devices (other than those associated with a Recovery Certificate), where such SMETS2+ Devices have an SMI Status of 'commissioned' or Private Keys associated with S1SP Held Digital Signing Device Security Credentials;
b) the Contingency Symmetric Key;
c) the Contingency Private Key;
d) the Private Key associated with an Issuing OCA Certificate;
e) the Private Key associated with a Root OCA Certificate;
f) the Private Key associated with a Recovery Certificate; and
g) a User Role Signing Private Key

For example, SEC Section L would seem to cover the following, but Appendix L would not:

- Private Keys used by the DCC to sign XML
- Private Keys related to Certificates on Devices with statuses other than commissioned (e.g. recovered, installedNotComissioned, whitelisted)

Appendix L section 2 states that that it applies whenever a Relevant Private Key is Compromised but the Appendix L's scope appears more limited.

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 2
Observation	The scope of Appendix L section 3.2 (Notification and confirmation of a suspected Compromise) may be read as more limited than the scope of procedures to recover from Compromise.
Recommendation	The drafting is to be aligned to the scope of Appendix L section 1.2.
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	

The provision in Appendix L 3.2 covers:

> a Compromise or suspected Compromise of a Relevant Private Key or a Private Key associated with an Organisation Certificate that is used by a User to Digitally Sign any Service Request or Signed Pre-Command

As per section L, the definition of Relevant Private Keys includes 'a Private Key associated with an Organisation Certificate that is used by a User to Digitally Sign any Service Request or Signed Pre-Command', so the underlined text is unneeded and potentially ambiguous as to scope.

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 3
Observation	The definitions of categories of private keys (and so the associated recovery methods) overlap, and so there may be some ambiguity of interpretation.
Recommendation	The drafting is to be revised to remove the overlap.
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	

A Private Key is 'associated' with a Certificate if its Public Key is in the Certificate. Although the definition implies there is only one public key in a certificate, there are two in the Root OCA Certificate.

Both the 'root' private key and the Contingency Private Key are therefore associated with the Root OCA Certificate.

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 4
Observation	Prepayment factors
Recommendation	General provisions are to be drafted, and referred to from each relevant recovery method, to address prepayment related factors
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	

Section 4 Methods 2 & 3 locks out supplier functionality on affected Devices, since they set the SMI Status to 'Recovery' (which stops all device functionality apart from locally entered UTRNs) and places ACB certificates in supplier Trust Anchor Cells (which would also block locally entered UTRNs).

This suggests the risks to prepayment customers and those any attacker may have put into prepayment mode may be worth highlighting in the recovery procedures.

Further 4.2.1.3 would seem to require that Devices are locked out from all functionality (apart from locally entered UTRNs) before SMKI PMA has decided to proceed using this method:

> The DCC shall disable processing of communications destined for SMETS2+ Devices that it has been notified (in Step 4.2.1.2) are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status of those SMETS2+ Devices to 'Recovery'. The

> DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.

Note that 4.2.2.4 suggest Suppliers cannot choose to only use this option on a subset of Trust Anchor Cells, so the prepayment slot would be affected:

> The DCC shall send Commands to each affected SMETS2+ Device, Digitally Signed using the Recovery Private Key, in order to replace Organisation Certificates in all of the Supplier slots on SMETS2+ Devices as notified

Further, in the case where PMA decides not to proceed, setting the SMI Status back to what it was prior to 'Recovery' would appear to leave the Devices still inoperable, if the compromised private keys have been destroyed (e.g. as required by method 3)

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 5
Observation	Some section 4 provisions do not seem possible if it relates to a DCC compromise.
Recommendation	Section 5 and 6 are to be reviewed for technical accuracy & viability with DCC, and drafting updated accordingly. Updated: Discussions underway with DCC and SMKI PMA to agree the correct order of steps to achieve the aims of Appendix L Section 5 (see also observation 6)
Status	Pending DCC input to allow relevant sections to be redrafted to reflect what DCC have in place / would intend. Note that drafting as to global ADTs has been added to the Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 6
Observation	Section 4.1.2.6 requires that private keys should be destroyed and certificates revoked as soon as actions in relation to SMETS2+ Devices are completed.
Recommendation	As part of observation 4, add drafting to require those responsible for making decisions to factor in the range of risks before deciding whether to destroy / revoke and, if so, when. Updated: Discussions underway with DCC and SMKI PMA to agree the correct order of steps to achieve the aims of Appendix L Section 5 (see also observation 5)
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	
Section 4.1.2.6 requires that private keys should be destroyed and certificates revoked as soon as actions in relation to SMETS2+ Devices are completed. This may not always be advisable (e.g. if actions were still underway on SMETS1 Devices). It may be worth adding a caveat accordingly.	

Similarly, 4.1A.2.6 requires such actions from SMETS1 actions are complete. It may be worth adding a caveat similarly. Similarly for 4.2.2.10

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 7
Observation	Recovery method 1A: 4.1A.1.4
Recommendation	The requirement should be removed
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	
Recovery method 1A: 4.1A.1.4 requires that Suppliers are notified if the Network Operator's credentials are compromised. However, those credentials can only affect Network Operator access to SMETS1 information (they are not on Devices and are used only for access control). Thus, it is not clear why Suppliers would have an interest.	

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 8
Observation	Some of the statements of 4.2.1.1 / 4.3.1.1 appear incorrect
Recommendation	Drafting to be corrected as part of observation 4
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	
4.2.1.1 / 4.3.1.1 is a pre-recovery step but states that use of the compromised private key 'will either be constrained by the status of the Device in the SMI, or the fact that a DCC Access Control Broker Certificate is now on the Device.' These appear arguably misleading statements, as no actions have been taken by this step.	

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 9
Observation	Method 3 areas of risk
Recommendation	Drafting to be corrected as part of observation 4
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	
4.3.1.1 requires that 'as soon as possible' after the subscriber notifies its desire to use this method (so before the PMA has considered approving its use), the subscriber revokes the certificates and destroys the associated private keys. This may be an unwise course of action (e.g. for prepayment customers, if the PMA does not approve method 3 etc.). Note there is a caveat warning that this may not be the best course, but no exception in the requirement to align to the caveat. The	

requirement seems absolute, stating ‘The affected Subscriber shall destroy the Private Key associated with the revoked Organisation Certificate.’

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 10
Observation	Recovery using contingency
Recommendation	Drafting to be corrected as part of observation 4
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	

As required by 5.2.1, all remote access to Devices is disabled whilst this is underway. This means that the only prepayment functionality would be locally entered top ups. This is not currently recognised in the procedure but would appear to have significant implications. It may be that some provisions should be added (e.g. to put prepayment devices in a state where they will not disable before communications are blocked).

Further 5.2.8 requires that all supplier certificates are replaced with ACB ones. This would lock out all prepayment functionality even after the reset of SMI status at 5.2.9.

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 11
Observation	Recovery using contingency
Recommendation	Section 5 and 6 are to be reviewed for technical accuracy & viability with DCC, and drafting updated accordingly.
Status	Pending DCC input to allow relevant sections to be redrafted to reflect what DCC have in place / would intend
Detail	

The procedure appears to:

- Require at (5.1.6) that the Contingency Private Key and Contingency Symmetric Key have to be destroyed before they are used (5.2.7).
- Require that new recovery, acb and wanProvider Certificates have been created under the new root, but there appear no requirements to have generated any of the required keys, nor to certify them.
- Similarly, that that all network operators and suppliers have new certificates. Again, there appear no requirements on those parties to undertake the pre-requisite steps e.g. key pair generation.
- Stop suppliers from bringing their Devices back in to full use until the network operator has undertaken all the steps to create new certificates, and published details of those it wishes to use (in line with wider SEC obligations on suppliers using the correct NO certs).

There are similar questions as to some details in section 6.

Document	SEC-Appendix-L-SMKI-Recovery-Procedure
Reference	Appendix L observation 12
Observation	Supply chain implications
Recommendation	Drafting to be corrected as part of observation 4
Status	Changes reflected in SEC Appendix L - SMKI Recovery Procedure - proposed change v005
Detail	

Section 6.1 recognises that Contingency Key recovery would impact Devices in the supply chain and requires the SMKI PMA to consider this, including on deciding timing of destroying the compromised private keys.

The same points would appear to be more widely true, where it affects Certificates required on Devices at manufacture (e.g. root, recovery, acb etc). However, there appear to be no similar supply chain requirements.

10. SEC Appendix M SMKI Interface Design Specification

Document	SEC Appendix M SMKI Interface Design Specification
Reference	Appendix M observation 1
Observation	Requirement to notify number of Device CSRs submitted in a batch appears not possible to meet
Recommendation	Remove statement highlight in Detail.
Status	Change reflected in SEC Appendix M - SMKI Interface Design Specification v3.0 - proposed typographical changes v002
Detail	

Section 2.5.1.2 states:

> On receipt of an XML document containing a Batched CSR to the Batched Device CSR Web Service interface from an Authorised Subscriber's system, the DCC shall:
>
> a) …
>
> b) …
>
> c) either accept, or reject the Batched CSR, log relevant errors and return in the synchronous XML response to the Authorised Subscriber's systems, to notify the Authorised Subscriber as to:
>
> i. where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR

The underlined text appears not possible as the Batched Device CSR Web Service interface schema does not allow for a way for this number to be provided in response to a request.

Document	SEC Appendix M SMKI Interface Design Specification
Reference	Appendix M observation 2
Observation	RFC analysis: RFC 4648 only occurs in SEC Appendix M (SMKI Interface Design Specification) where it relates to a 'base 64' standard in a CSR and

	returned Certificate. A more relevant reference would be RFC 7468, which actually specifies the encodings for CSRs and Certificates and itself references RFC 4648. This would be a more correct reference to follow.
Recommendation	Make amendments where 'base64text' appears in in Appendices A, C and D.
Status	Change reflected in SEC Appendix M - SMKI Interface Design Specification v3.0 - proposed typographical changes v003
Detail	

Appendix A Device Certificate Signing Request: Element Table
This element contains the 'base64text' field (as defined in RFC7468 section 3) of the PKCS#10 Certificate Signing Request (CSR) without whitespace. The element shall NOT contain the 'preeb' and 'posteb' fields.

Appendix A Response to Ad Hoc Device Certificate Signing Request: Element Table
This element contains the 'base64text' field (as defined in RFC7468 section 3) of a DER X509v3 certificate without whitespace. The element shall NOT contain the 'preeb' and 'posteb' fields.

Appendix C Submit Batched CSR Message: Element Table
This element contains the 'base64text' field (as defined in RFC7468 section 3) of the PKCS#10 Certificate Signing Request (CSR) without whitespace. The element shall NOT contain the 'preeb' and 'posteb' fields.

Appendix D Batched CSR Result: Element Table
This element contains the 'base64text' field (as defined in RFC7468 section 3) of a DER X509v3 certificate without whitespace. The element shall NOT contain the 'preeb' and 'posteb' fields.

11. SEC Appendix N SMKI Code of Connection

Document	SEC Appendix N SMKI Code of Connection
Reference	Appendix N observation 1
Observation	Web browser versions are now outdated
Recommendation	Change obligation so that DCC is required to publish supported lists and consult before making any changes. This would avoid this section being constantly out of date.
Status	Changes reflected in SEC Appendix N - SMKI Code of Connection - proposed v0002
Detail	

Section 1.1 states:

> The DCC shall ensure that the SMKI Portal interface via a DCC Gateway Connection, and SMKI Portal interface via the Internet supports, as a minimum, the following web browsers and versions:
>
> - Google Chrome version 34.
> - Internet Explorer versions 9, 10 and 11.
> - Mozilla Firefox version 27.

These versions are outdated / unsupported by the vendors so should they be updated (e.g. https://www.theverge.com/2020/8/17/21372487/microsoft-internet-explorer-11-support-end-365-legacy-edge). IE will be completely unsupported, so should be removed for clarity?

Document	SEC Appendix N SMKI Code of Connection
Reference	Appendix N observation 2
Observation	Microsoft versions are now outdated
Recommendation	As per Appendix N observation 1
Status	Changes reflected in SEC Appendix N - SMKI Code of Connection - proposed v0002
Detail	

Section 1.1 states:

> The DCC shall ensure that the SMKI Portal interface via a DCC Gateway Connection and SMKI Portal interface via the Internet are tested with the browsers set out above on the Microsoft Windows 7 & 8.1 operating systems (along with applicable future versions).
>
> Operating systems other than those listed above may also be compatible, though they will not be supported.

Section 2.3.1 further states:

> The DCC shall make the Authentication Client software available to Parties and RDPs and ensure that the software:
>
> (a) …
>
> (b) is compatible with Microsoft Windows 7 and 8.1 operating systems;

Similar to Appendix N observation 1. Microsoft stopped Windows 7 support in 2020, so it is not clear if / how DCC are meeting this obligation.

Document	SEC Appendix N SMKI Code of Connection
Reference	Appendix N observation 3
Observation	Redundant / incorrect obligations
Recommendation	Delete part (b)
Status	Changes reflected in SEC Appendix N - SMKI Code of Connection - proposed v0002
Detail	

Section 2.2 states:

> The DCC shall enable Parties or RDPs with access to the SMKI Portal interface via the Internet to:
>
> (a) submit Organisation CSRs and retrieve resulting Organisation Certificates;
>
> (b) access the documents set out in section 2.6.1 of the SMKI Interface Design Specification.

Part (b) appears redundant as only CSRs and Certificates are accessible, which is covered by bullet (a). In addition, there is no section 2.6.1 in the SMKI IDS so it is unclear what documents are being referred to in the first place.

Document	SEC Appendix N SMKI Code of Connection
Reference	Appendix N observation 4
Observation	Obligations defined with regards to use of unsupported software
Recommendation	Delete on the basis that Internet Explorer is unsupported software.
Status	Changes reflected in SEC Appendix N - SMKI Code of Connection - proposed v0002
Detail	

Section 2.3.1 states:

> Once the Authentication Client software is successfully installed and where using the Internet Explorer browser to access the SMKI Portal, the Party or RDP shall, prior to any attempt to access the SMKI Portal, ensure that the web browser security settings on such computers are not set to 'High' and shall ensure that TLS1.2 is enabled in the web browser settings. If such security settings are set to 'High', some functionality, particularly in relation to search and ordering functionality, may not operate correctly.

Internet Explorer is unsupported software.

12. SEC Appendix O SMKI Repository Interface Design Specification

Document	SEC Appendix O SMKI Repository Interface Design Specification
Reference	Appendix O observation 1
Observation	RFCs 4251, RFC 4252, RFC 4253 and RFC 959 have been analysed and need an explanatory reference to ensure industry good practice is applied.
Recommendation	Add a sentence at the start to clarify that the recommended practices for management stated in NISTIR 7966 section 5 should be followed where RFC references are shown in this section.
Status	Change reflected in SEC Appendix O – SMKI Repository Interface Design Specification v3.0
Detail	

2.3.1 General Obligations (already amended for typographical changes:

The DCC shall ensure that the SFTP Interface to the SMKI Repository enables DCC Gateway Connection users' systems to download Organisation Certificates, OCA Certificates, Device Certificates, DCA Certificates, Organisation CRLs and Organisation ARLs lodged in the SMKI Repository, as set out this section and Annex C of this document. The recommended practices for management stated in NISTIR 7966 section 5 should be followed where RFC references are shown in this section.

Document	SEC Appendix O SMKI Repository Interface Design Specification

Reference	Appendix O observation 2
Observation	The current reference to (SSH) in 2.3.1(b)(i) could permit the use of SSH-1 which is no longer acceptable
Recommendation	Amend the reference to Secure Shell (SSH) protocol to (SSH-2)
Status	Change reflected in SEC Appendix O – SMKI Repository Interface Design Specification v3.0
Detail	

2.3.1 General Obligations

(b) is implemented in a standard format

i. conforming to Secure Shell (SSH-2) protocol, in accordance with RFC 4251, RFC 4252 and RFC 4253;

13. SEC Appendix P SMKI Repository Code of Connection

No observations but there are proposed typographical corrections reflected in the redlined version with associated explanatory comments.

14. SEC Appendix Q IKI Certificate Policy

Document	SEC Appendix Q IKI Certificate Policy
Reference	Appendix Q observation 1
Observation	Information Assurance Standard does not appear to be available anymore
Recommendation	Change the reference to be a URL (https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)
Status	Change reflected in SEC Appendix Q – IKI Certificate Policy - proposed typographical changes v0002
Detail	

Section 5.1.7 states:

> (A) The ICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the ICA are disposed of only using secure methods of disposal in accordance with:
>
> (i) Information Assurance Standard No. 5:2011 (Secure Sanitisation); or
>
> (ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time.

This Information Assurance Standard does not appear to be available anymore.

This is a mirror of Appendix B observation 3 and Appendix A observation 3.

Document	SEC Appendix Q IKI Certificate Policy
Reference	Appendix Q observation 2
Observation	Standard superseded
Recommendation	Update reference from 2008 to 2014
Status	Change reflected in SEC Appendix Q - IKI Certificate Policy - proposed typographical changes v0002
Detail	

Section 5.4.2 states:

> (ii) all ICA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:
>
> > (a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

British Standard BS 10008:2008 appears to have been superseded by British Standard BS 10008:2014 (https://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/).

This same standard is referenced in 5.4.4.

This is a mirror of Appendix B observation 4 and Appendix A observation 4.

Document	SEC Appendix Q IKI Certificate Policy
Reference	Appendix Q observation 3
Observation	IKI Certificate requirements appear to contradict one another
Recommendation	Remove the bullet as the drafting appears redundant
Status	Change reflected in SEC Appendix Q - IKI Certificate Policy - proposed typographical changes v0002
Detail	

Annex B states:

- IKI Certificates contain an X520OrganizationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under and a X520commonName attribute whose value will be set to the ARO's or system name.

All other bullets in this list are qualified, and relate to a subset of IKI Certificates only (i.e. "IKI Certificates issued by the IKI Administrator CA contain…" or "IKI Certificates issued by the IKI Registration Authority CA contain…". This one does not have a qualifier and so contradicts a number of other bullets. It would appear this drafting is spurious.

Document	SEC Appendix Q IKI Certificate Policy
Reference	Appendix Q observation 4
Observation	An addition to section 6.2.6 is needed
Recommendation	Add a sub-section (c) to Section 6.2.6
Status	The change is needed to support operational realities such as a change/migration of Trusted Service Provider (TSP) or datacentre
Detail	

The current re-platforming of the Trusted Service Provider (TSP) due to the existing Digicert platform being discontinued requires the IKI CA Private Key to be transferred to a different datacentre. Appendix Q section 6.2.6 does not explicitly cover such a situation and allowing the SMKI PMA to give approval following SSC consultation is a sensible addition.

15. SEC Appendix S DCCKI Certificate Policy

Document	SEC Appendix S DCCKI Certificate Policy
Reference	Appendix S observation 1
Observation	Information Assurance Standard does not appear to be available anymore
Recommendation	Change the reference to be a URL (https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)
Status	Change reflected in SEC Appendix S – DCCKI Certificate Policy - proposed typographical changes v0002
Detail	

Section 5.1.7 states:

> The DCCKICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions is securely disposed of in accordance with HMG Information Assurance Standard No 5 or an equivalent standard.

This Information Assurance Standard does not appear to be available anymore.

This is a mirror of Appendix B observation 3 and Appendix A observation 3.

Document	SEC Appendix S DCCKI Certificate Policy
Reference	Appendix S observation 2
Observation	Referenced document does not appear to exist
Recommendation	Update to refer to the SMKI PMA Guidance on “Verifying Individual Identity” published on the Website
Status	Change reflected in SEC Appendix S – DCCKI Certificate Policy - proposed typographical changes v0002
Detail	

Section 5.2.3 states:

(a) All DCCKICA Personnel shall be required to authenticate via a strong two factor Authentication in accordance with Level 2 of the HMG Authentication Framework before they can access any facilities.

It appears that ‘HMG Authentication Framework’ does not exist.

Document	SEC Appendix S DCCKI Certificate Policy
Reference	Appendix S observation 3
Observation	‘HMG Security Check’ is undefined
Recommendation	Align drafting to SEC section A definition of Security Check
Status	Change reflected in SEC Appendix S – DCCKI Certificate Policy - proposed typographical changes v0002
Detail	

Section 5.3.1 states:

(a) The DCCKICA shall ensure that all DCCKICA Personnel must:

(i) …

(ii) …

(iii) …

(iv) have, as a minimum, passed an HMG Security Check (SC) level of vetting, before commencing their roles.

HMG Security Check (SC) is not defined, making it unclear what level of vetting is actually required.

Document	SEC Appendix S DCCKI Certificate Policy
Reference	Appendix S observation 4
Observation	Standard superseded
Recommendation	Update reference from 2008 to 2014
Status	Change reflected in SEC Appendix S - DCCKI Certificate Policy - proposed typographical changes v0001
Detail	

Section 5.4.4 states:

(ii) to the extent to which the Audit Log is retained electronically, the DCCKICA event log Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with British Standard BS 10008:2008 (Evidential weight and legal admissibility of electronic information) or an equivalent standard; and

British Standard BS 10008:2008 appears to have been superseded by British Standard BS 10008:2014 (https://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/).

This same standard is referenced in 5.5.1.

This is a mirror of Appendix B observation 4 and Appendix A observation 4.

16. SEC Appendix T DCCKI Interface Design Specification

Document	SEC Appendix T DCCKI Interface Design Specification
Reference	Appendix T observation 1
Observation	Standard superseded
Recommendation	Update reference from RFC2253 to RFC4514
Status	Change reflected in SEC Appendix T - DCCKI Interface Design Specification
Detail	

Section 3.9 states:
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 4514~~2253~~)
and serial number of the SMKI Organisation Certificate with preceding "," separators.

The reference to IETF RFC 2253 has been superseded by IETF 4514

17. SEC Appendix U DCCKI Repository Interface Design Specification

No observations but there are proposed typographical corrections reflected in the redlined version with associated explanatory comments.

18. SEC Appendix V DCCKI CoCo and DCCKI Repository CoCo

No observations but there are proposed typographical corrections reflected in the redlined version with associated explanatory comments.

19. SEC Appendix W DCCKI Registration Authority Policies and Procedures

No observations but there are proposed typographical corrections reflected in the redlined version with associated explanatory comments.

20. SEC Appendix X Registration Data Interface Specification

Document	SEC Appendix X Registration Data Interface Specification
Reference	Appendix X observation 1
Observation	RFC analysis: RFC 959 is used in section 2.5 and needs to be clarified which is best achieved in the introductory paragraph. At present, the SEC section 2.5 just says “The Registration Data Interface shall utilise FTPS”.
Recommendation	To ensure FTPS is used correctly to ensure alignment with SMKI references in Appendix O, an addition should be made: The Registration Data Interface shall utilise FTPS following the list of recommended tasks for implementing an information exchange stated in NIST SP 800-47 revision 1 Section 3.2.2.
Status	Change reflected in SEC Appendix X – Registration Data Interface Specification.
Detail	
2.3.1(b) NIST SP 800-47 revision 1 Section 3.2.2 is included. 2.5 The Registration Data Interface shall utilise FTPS following the list of recommended tasks for implementing an information exchange stated in NIST SP 800-47 revision 1 Section 3.2.2.	