

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.



MP259 'Triage System Interface Definition'

Modification Report

Version 1.0

20 December 2023



About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views, and conclusions.

Contents

1. Summary.....	3
2. Issue.....	3
3. Solution	5
4. Impacts	6
5. Costs	7
6. Implementation approach	8
7. Assessment of the proposal	8
Appendix 1: Progression timetable	10
Appendix 2: Glossary	10

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

If you have any questions on this modification, please contact:

Georgiana Severin

020 7770 6921

Georgiana.Severin@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of Security Sub-Committee (SSC).

Triage Facilities require secure channels for communication to carry out Triage Activities on Use Cases approved by the SSC. The SEC definition of a Triage System Interface currently only allows Internet Protocol Security (IPsec) as an approved method of securing data connection between Triage Facilities and the Manufacturer. However, one Manufacturer has made a case to employ a Transport Layer Security (TLS) Virtual Private Network (VPN) between individual machines instead. This has been approved by the SSC and by the National Cyber Security Centre (NCSC) subject to use of versions of TLS approved by NCSC and mandatory mutual authentication.

The Proposed Solution would include a TLS encrypted VPN as an approved method of securing data, alongside an IPsec VPN. Additionally, we would look to futureproof the SEC by removing references to the specific version of TLS stated in the SEC, instead referring Parties to SSC guidance on which version to use.

There are no impacts to Parties associated with this modification. The costs would be limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort. This is a Self-Governance Modification, and, if approved, will be implemented in the February 2024 release.

2. Issue

What are the current arrangements?

How is Device Triage achieved?

Approved Triage arrangements were introduced because of the growing need to refurbish Devices to avoid unnecessary waste. Previously, the SEC did not include any guidance on Device Triage and how Triage Facility Providers should operate.

The Triage Facility was specifically designed to refurbish removed Devices and have them ready for re-installation and communication through the Data Communications Company (DCC) network. To be able to do so, Triage Facilities require secure channels for communication.

Relevant Specifications and regulations

The Commercial Product Assurance (CPA) Triage Security Characteristic Overlay document specifies the security controls required to be designed into a Device with relevant SSC approved Use Case Triage capability to enable the Device to achieve CPA Certification.

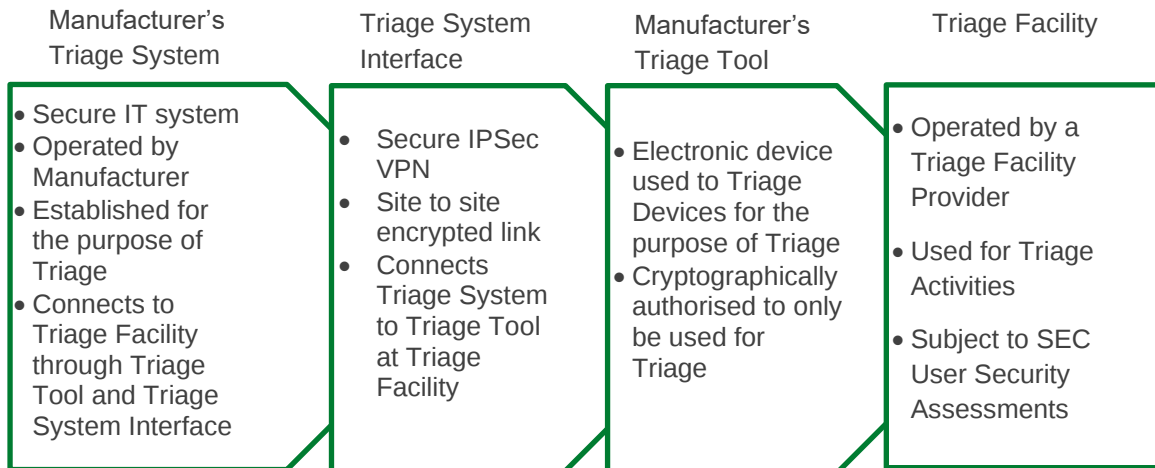
The CPA Build Standard is used by accredited CPA Test Laboratories to assure the Triage Tool and Triage System Interface.

The SEC Section G12 specifies the arrangements for a Triage Facility Provider to be subject to an independent Security Assessment to be approved to carry out Triage Activities.

The SSC Guidance on Device Security Assurance and Triage Part 2 provides the overview of all the activities that may be carried out for SSC approved Use Cases.

What is the process?

At present, Use Case 004 (Factory Reset) is the only Use Case to which SEC Section G12 applies. The Manufacturer provides the Triage Facility Provider with a Triage Tool and Triage System Interface that is connected to the Manufacturer's Triage System as shown in the flow below.



Triage System Interface Security

As part of [MP203 'Security Assurance of Device Triage Facilities'](#) the SSC Guidance for Device Security Assurance and Triage has been created to support Device Triage when the Device has been removed from consumer premises. This defines the process for approved Use Cases and the SEC defines certain tools/equipment that must be used.

The Triage System Interface currently requires an IPsec VPN site-to-site encrypted link that Manufacturers use to communicate with the Triage Facility.

The IPsec site-to-site encrypted protection enables the Triage Facility Provider to communicate with a Manufacturer to set up an entire site access to its systems. By doing this, the communication between Manufacturer and Triage Facility can be done through several endpoints.

Transport Layer Security

TLS is a type of host-to-host encryption which narrows down the communication channels between two parties. The difference between TLS and the current IPsec used by Manufacturers is that TLS would limit access to the Manufacturer's system to single endpoints in the Triage Facility. This would provide a more granular level of security and control over shared data.

Currently, TLS is detailed elsewhere in the SEC as an acceptable method of encrypting communications but is not allowable under the current definitions for Triage Interface Systems.

What is the issue?

The SEC currently defines a Triage System interface as a *"secure IPsec virtual private network, site to site encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a Triage Facility, which provides confidentiality and integrity of communications"* (SEC Section G12.9).

Whilst this arrangement keeps the information secure on a site basis, a Manufacturer has requested an additional option to use TLS to limit the access to specific machine endpoints that would allow it to access the Triage System. The SSC and NCSC have accepted that, subject to use of the correct NCSC approved version and use of mutual authentication, TLS provides a satisfactorily secure alternative option to operate alongside IPsec VPN.

TLS is therefore proposed as an alternative protocol for a virtual private network, and this would provide an acceptable level of security between the Manufacturer's Triage System and Triage Facilities.

Additionally, TLS would be a host-to-host type of encryption, as opposed to the current IPsec site-to-site configuration, which SSC believes is justified, provided mutual authentication was used.

The SSC and NCSC are content with the change to TLS provided both parties can mutually authenticate when using this method and that the TLS version is approved by NCSC.

The SSC has also noted that current references to TLS in the SEC contain specific version numbers to be used. This also limits SEC Parties to accessing the latest version, which could be necessary (in the case of DCC for example) or best practice to access Federal Information Processing Standard Publication 140-3 (FIPS140-3), the latest standard applicable to Hardware Security Models (HSMs).

The SSC would like to futureproof these references by removing specific version numbers and including the allowable versions within SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website. This enables changes to be made to this list when new versions come into effect, or old versions are no longer supported.

What is the impact this is having?

TLS is already used within the SEC however it is not currently included in the definition of a Triage System Interface, limiting Manufacturers to IPsec when establishing secure connections with Triage Facilities.

As a result, Manufacturers are currently unable to limit and control access to the Manufacturer's Triage Systems to specific endpoints within a Triage Facility for the use of Triage.

References to TLS already within the SEC, state that version 1.2 should be used. This is no longer the latest version. As such, wherever TLS is required, SEC Parties should be using the latest or most appropriate version. The inclusion of the specific version number would have a rolling impact as it would require a modification when new versions are released, which would restrict SEC Parties' ability to update their systems.

Impact on consumers

This modification will not impact consumers.

3. Solution

Proposed Solution

The Proposed Solution is to expand the Triage System Interface definition to include both the existing IPsec method, as well as an alternative direct TLS VPN.

As well as the SEC, the CPA Triage Security Characteristic Overlay document and the SSC Guidance on Device Security Assurance and Triage to include TLS as an approved method of establishing secure communication between Manufacturers and their Triage Facility will also be updated by the SSC.

Additionally, to futureproof the SEC Guidance, it is also proposed that references to TLS v1.2 are changed to generic wording referring SEC Parties to the SSC Guidance on which version of TLS to use.

The legal text to implement these changes can be found in Annex A.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
	Electricity Network Operators		Gas Network Operators
✓	Other SEC Parties	✓	DCC

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
✓	Device Manufacturers		Flexibility Providers
	DCC Other Users	✓	MAPs/ MAMs

This modification will impact Device Manufacturers who choose to employ TLS as their preferred method of securing data with a Triage Facility. Meter Asset Providers (MAPs) and Suppliers will only be impacted if they are operating a Triage Facility and choose to employ TLS.

As TLS 1.2 is not yet deprecated, Suppliers, Network Operators and the DCC will not be immediately impacted by this modification, however when newer versions come into force, they would then be able to update.

DCC Systems

DCC System changes

There will be no System changes from the modification.

DCC System traffic

This modification will not impact DCC System traffic.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section G 'Security'
- Appendix M 'SMKI Interface Design Specification'
- Appendix O 'SMKI Repository Interface Design Specification'
- Appendix S 'DCCKI Certificate Policy'
- Appendix T 'DCCKI Interface Design Specification'
- Appendix X 'Registration Data Interface Specification'
- Appendix AI 'Self Service Interface Code of Connection'
- Appendix AL 'SMETS1 Transition and Migration Approach Document'

The changes to the SEC required to deliver the proposed solution can be found in Annex A.

Devices

This modification will not impact Devices.

Consumers

This modification will not impact Consumers.

Other industry Codes

This modification will not impact other industry Codes.

Greenhouse gas emissions

This modification will not impact greenhouse gas emissions.

5. Costs

DCC costs

There are no DCC costs associated with this modification.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day of effort, amounting to approximately £600. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the updated version to the industry.

SEC Party costs

There are no Party costs associated with this modification.

6. Implementation approach

Approved implementation approach

The Change Sub-Committee (CSC) has approved an implementation date of:

- **29 February 2024** (February 2024 SEC Release) if a decision to approve is received on or before 15 February 2024; or
- **27 June 2024** (June 2024 SEC Release) if a decision to approve is received after 16 February 2024 but on or before 13 June 2024.

It is recommended that the modification is targeted for the February 2024 release as there are no System impacts on the DCC, SEC Parties, or costs associated with implementing this modification (aside from SECAS costs). Providing Triage Facilities with alternative security arrangements will ensure that there is no delay to the triage of meters.

7. Assessment of the proposal

Areas for assessment

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC) and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums. SECAS believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	None
SMKI PMA	None
SSC	Input on legal text and Proposed Solution
TABASC	None

Observations on the issue

A Manufacturer raised the issue when trying to set up security arrangements that did not fit the current definition in SEC Section G12.9. The SSC acknowledged this and noted that provided mutual

authentication was employed, the TLS VPN would be an acceptable alternative to access the Triage System.

Solution development

The changes in this Modification Report were brought to the attention of SSC in a meeting on 25 October 2023. Following the SSC meeting, discussions have been held between NCSC, the Department of Energy Security and Net Zero (DESNZ), the TABASC Chair, Cybersecurity Solutions (CyTAL) and the SSC Chair to review various iterations of drafting for the amended definitions.

As part of the development, they noted that where TLS is mentioned in the SEC outside of Triage Facilities, it included the version (TLS 1.2). This has not been deprecated, but a new version of TLS (1.3) is available and will likely replace 1.2 in future. It was therefore proposed that moving forward, the TLS version should not be mentioned in the SEC, instead it would refer Parties to the relevant guidance as to which version to use.

The intent is to ensure that secure communication between Manufacturers and Triage Facilities are in place and that the SEC covers the appropriate methods in which this can be achieved. Additionally, referring SEC Parties to SSC Guidance as opposed to clearly stating the TLS version required would futureproof the SEC.

8. Case for change

Business case

The modification does not impact SEC Parties, but it would benefit the Triage Facilities who do wish to utilise it. It can be delivered into the SEC as a legal text change and therefore the costs are limited to SECAS implementation.

Views against the General SEC Objectives

Proposer's views

The Proposer believes this Modification Proposal will better facilitate SEC objectives (f)¹ as it will reduce security risks and futureproof the SEC and better support the refurbishment of Devices.

Views against the consumer areas

Improved safety and reliability

This modification will have a neutral impact on this area.

Lower bills than would otherwise be the case

This modification will have a neutral impact on this area.

¹ Ensure the protection of Data and the security of Data and Systems in the operation of this Code.

Reduced environmental damage

This modification will have a neutral impact on this area.

Improved quality of service

This modification will have a neutral impact on this area.

Benefits for society as a whole

This modification will have a neutral impact on this area.

Final conclusions -

NCSC and SSC have agreed the amendments to the definition of Triage System Interface to include TLS as an appropriate alternative to IPsec provided both parties use mutual authentication when using TLS.

The NCSC has also agreed to the text change required.

The SSC support the changes to the amendment of TLS v1.2 to a generic description and referral to the SSC Guidance to ensure future uplifts to the protocol do not require a full Modification to implement.

Appendix 1: Progression timetable

Timetable	
Event/Action	Date
Draft Proposal raised	11 Dec 2023
CSC converts Draft Proposal to Modification Proposal	19 Dec 2023
Modification Report approved by CSC	19 Dec 2023
Modification Report Consultation	20 Dec 2023 – 15 Jan 2024
Change Board Vote	24 Jan 2024

Italics denote planned events that could be subject to change.

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	Full term
CPA	Commercial Product Assurance
CSC	Change Sub-Committee

Glossary	
Acronym	Full term
CyTAL	Cybersecurity Solutions
DCC	Data Communications Company
DCCKI	Data Communications Company Key Infrastructure
DESNZ	Department for Energy Security and Net Zero
FIPS 140-3	Federal Information Processing Standard Publication 140-3
HSM	Hardware Security Module
IPsec	Internet Protocol Security
MAM	Meter Asset Manager
MAP	Meter Asset Provider
NCSC	National Cyber Security Centre
OPSG	Operations Group
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Equipment Technical Specifications
SMKI	Smart Metering Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TLS	Transport Layer Security
VPN	Virtual Private Network

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.

MP259 ‘Triage System Interface Definition’

Annex A

Legal text – version 0.1

About this document

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

This document contains the changes required to deliver the Proposed Solution.

Section A ‘Definitions’

These changes have been redlined against Section A version 34.0.

Amend Section A1.1 as follows:

Transport Layer Security	means TLS 1.2 <u>TLS in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website as defined in the Internet Engineering Task Force (IETF) Request for Change (RFC) 5246 or any equivalent to that document which updates or replaces it from time to time.</u>
---------------------------------	---

Section G ‘Security’

These changes have been redlined against Section G version 21.0.

Amend Section 12.9 as follows:

Triage System Interface	means a secure IPsec -virtual private network, site-to-site -encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a Triage Facility, which provides confidentiality and integrity of communications. <u>The Triage System Interface:</u> <u>Must use either TLS or IPsec, and</u> <u>If using TLS then must include client authentication.</u>
Triage System	means a secure IT system established for the purposes of Triage and operated by a Manufacturer, as part of its Device manufacturing capability, which the Triage Facility Provider connects to using the Triage Tool and Triage System Interface, and which is compliant with the requirements of the NCSC Commercial Product Assurance (CPA) Scheme and the associated CPA Security Characteristics.
Triage Tool	means an electronic device provided by a Manufacturer, which is used to Triage Devices in accordance with SSC Guidance for Device Security Assurance and Triage, and which is cryptographically authorised such that it can only be used for Triage Activities and cannot be given additional capabilities by an operator in a Triage Facility.

Appendix M 'SMKI Interface Design Specification'

These changes have been redlined against Appendix M version 5.0.

Amend Section 2.3 as follows:

2.3 SMKI Portal interface via DCC Gateway Connection

General obligations

The SMKI Portal interface via DCC Gateway Connection provides an asynchronous mechanism for Authorised Responsible Officers (AROs) to submit Organisation CSRs, and Device CSRs in batch or ad-hoc form on behalf of their Authorised Subscriber.

The DCC shall ensure that the SMKI Portal interface via DCC Gateway Connection:

- a) uses the HTTPS protocol, secured by mutually authenticated TLS ~~1.2~~ in line with the cryptographic standards set out in Appendix G of this document;
- b) uses Javascript, Cascading Style Sheets (CSS) and images;
- c) is compliant with the W3C "Web Content Accessibility Guidelines" (v2) at "AA" level; and
- d) is only accessible using a DCC Gateway Connection.

The process for obtaining a DCC Gateway Connection is detailed in Section H15 of the Code.

Establishing a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection

In order to establish a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection, an Authorised Subscriber shall:

- a) access the SMKI Portal landing page via a defined URL (as set out in the SMKI User Guide), which shall be secured using HTTPS;
- b) then select the relevant link to access the SMKI Portal page supplied to enable submission and retrieval of Organisation CSRs/Certificates or Device CSRs/Certificates; and
- c) having selected the relevant link in b), ensure the web browser connection is secured by establishing a mutually authenticated TLS ~~1.2~~ session by entering the PIN code used to enable use of the relevant Cryptographic Credential Token, and presenting the IKI Certificate (which has been Issued in accordance with the SMKI RAPP for the purposes of accessing the SMKI Portal via DCC Gateway Connection) to the DCC for either:

Authorised Subscribers for Organisation Certificates, for the purposes of submitting Organisation CSRs and retrieval of resulting Organisation Certificates; or

Authorised Subscribers for Device Certificates, for the purposes of submitting Device CSRs and retrieval of resulting Device Certificates.

Amend Section 2.4 as follows:

2.4 Ad Hoc Device CSR Web Service interface

General obligations

The Ad Hoc Device CSR Web Service interface provides a synchronous mechanism for an Authorised Subscriber's systems to submit individual Device CSRs.

The DCC shall ensure that the Ad Hoc Device CSR Web Service interface:

- a) is only accessible to Authorised Subscribers for Device Certificates acting on behalf of Parties in the User Role of either Import Supplier or Gas Supplier, or the DCC;
- b) uses the HTTPS protocol, secured by mutually authenticated TLS ~~1.2~~, in line with the cryptographic properties set out in Appendix G of this document;
- c) uses Extensible Markup Language (XML) over REST for Device CSR message requests and responses;
- d) provides message responses which are consistent with Appendix A of this document;
- e) uses the XML schema for CSR message requests and responses defined in Appendix B of this document; and
- f) is only accessible using a DCC Gateway Connection.

Establishing a secured connection to the Ad Hoc Device CSR Web Service interface

In order to establish a secured TLS ~~1.2~~ connection to the Ad Hoc Device CSR Web Service interface, an Authorised Subscriber for Device Certificates acting as an Import Supplier or Gas Supplier, or the DCC, shall:

- a) configure its system(s) to connect to the Ad Hoc Device CSR Web Service interface URL, as set out in the SMKI User Guide;
- b) establish a TLS ~~1.2~~ session by presenting the IKI Certificate which has been Issued in accordance with the SMKI RAPP for the purposes of TLS ~~1.2~~ mutual authentication to secure access to the Ad Hoc Device CSR Web Service interface; and
- c) configure its systems such that the TLS ~~1.2~~ session renegotiation timeout is set to 5 minutes for each connection to the Ad Hoc Device CSR Web Service interface.

In order for a secured connection to the Ad Hoc Device CSR Web Service interface to be established, the DCC shall ensure that the Ad Hoc Device CSR Web Service presents the CA/Browser Forum certificate referenced in the 'General obligations' part of section 2.4 of this document, for the purposes of allowing the Authorised Subscriber's systems to authenticate the server as part of establishing the mutually authenticated TLS ~~1.2~~ session.

Amend Section 2.5 as follows:

2.5 Batched Device CSR Web Service interface

General obligations

The Batched Device CSR Web Service interface provides a synchronous mechanism for an Authorised Subscriber's systems to submit Batched CSRs containing Device CSRs and subsequently a synchronous mechanism to retrieve the resulting Device Certificates.

The DCC shall ensure that the Batched Device CSR Web Service interface:

- a) uses the HTTPS protocol, secured by mutually authenticated TLS ~~1.2~~, in line with the cryptographic properties set out in Appendix G of this document;
- b) uses Extensible Markup Language (XML) over REST for Batched CSR message requests, Batched CSR responses and provision of Device Certificates;
- c) provides message responses corresponding with submission of Batched CSRs which are consistent with Appendix C of this document;
- d) provides message responses in relation to the processing of individual Device CSRs that are contained within a Batched CSR which are consistent with Appendix D of this document;
- e) uses the XML schema for Batched CSR message requests and responses defined in Appendix E; and
- f) is only accessible using a DCC Gateway Connection.

Amend Section 2.6 as follows:

2.6 SMKI Portal interface via the Internet

General obligations

The SMKI Portal interface via the Internet provides an asynchronous mechanism for Authorised Responsible Officers (AROs) not accessing the SMKI Service through a DCC Gateway Connection to submit Organisation CSRs and to retrieve resulting Certificates, on behalf of their Authorised Subscriber.

The SMKI Portal via the Internet also provides a mechanism by which Authorised Subscribers may access certain SMKI Repository content.

The DCC shall ensure that the SMKI Portal interface via the Internet:

- a) uses the HTTPS protocol, secured by mutually authenticated TLS ~~1.2~~ in line with the cryptographic standards set out in Appendix G of this document;
- b) uses Javascript, Cascading Style Sheets (CSS) and images;
- c) is compliant with the W3C "Web Content Accessibility Guidelines" (v2) at "AA" level;

Establishing a secured web browser connection to the SMKI Portal interface via the Internet

In order to establish a connection to the SMKI Portal interface via the Internet, an Authorised Subscriber shall:

access a SMKI Portal landing page via defined URL (as defined in the SMKI User Guide) which shall be secured using HTTPS;

then select the relevant link to access the SMKI Portal page supplied to enable submission and retrieval of Organisation CSRs/Certificates; and

having selected the relevant link in b), ensure the web browser connection is secured by establishing a mutually authenticated TLS ~~1.2~~ session by entering the PIN code used to enable use of the relevant Cryptographic Credential Token, and presenting an IKI Certificate (which has been Issued in accordance with the SMKI RAPP for the purposes of accessing the SMKI Portal via the Internet) to

the DCC for Authorised Subscribers for Organisation Certificates, for the purposes of submitting Organisation CSRs and retrieval of resulting Organisation Certificates.

In order for a secured web browser connection to the SMKI Portal interface via the Internet to be established, the DCC shall ensure that the SMKI Portal via the Internet presents to the user a x.509 v3 certificate that is recognised by the CA/Browser Forum for the purposes of allowing the Authorised Subscriber's systems to authenticate the server as part of establishing the mutually authenticated TLS ~~1.2~~ session.

The DCC shall ensure that the SMKI Portal via the Internet denies access where the user does not present a valid IKI Certificate for authentication.

Amend Appendix G as follows:

Authentication Credentials

The SMKI Portal for Users, Ad-Hoc Device CSR Web Service interface and Batched Device CSR Web Service interface shall use server and client certificates with the following cryptographic properties:

Criteria	Version
Protocol	TLS 1.2 *
Protocol Cyphers	ECDHE-RSA-AES256-GCM-SHA384
	ECDHE-RSA-AES256-SHA384
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-SHA256
Client Certificate Key	RSA 2048 bit
Client Certificate Hash Algorithm	SHA256
Server Certificate Key	RSA 2048 bit
Server Certificate Hash Algorithm	SHA256

* TLS ~~1.2~~ should be implemented in accordance with Java and Apache standards and the SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website. ~~Java 7 and above supports TLS 1.2.~~ The TLS version is specified in the HTTP client protocol initialisation. To enable AES256, the Java runtime should be patched with "JCE Unlimited Strength Jurisdiction Policy Files" for the version of Java being used. This is obtained from the public Oracle Java download web pages.

Appendix N 'SMKI Code of Connection'

These changes have been redlined against Appendix N version 3.0.

Amend Section 2.3.1 as follows:

2.3.1 Authentication to SMKI Portal interface via a DCC Gateway Connection or via the Internet

The process for TLS~~1.2~~ mutual authentication to the SMKI Portal interface via the DCC Gateway Connection or the SMKI Portal via the Internet is as set out in the SMKI Interface Design Specification.

Amend Section 2.3.2 as follows:

2.3.2 Authentication to Ad Hoc Device CSR Web Service interface

The DCC shall secure the Ad Hoc Device CSR Web Service interface through a TLS~~1.2~~ mutual authenticated session to the SMKI Portal in accordance with the SMKI Interface Design Specification.

Parties require an appropriate IKI Certificate, in order to authenticate to the Ad Hoc Device CSR Web Service interface. This IKI Certificate shall be issued by the DCC on successful completion of the process as set out in the SMKI RAPP and in accordance with the SMKI Interface Design Specification.

Amend Section 2.3.3 as follows:

2.3.3 Authentication to Batched Device CSR Web Service interface

The DCC shall secure the Batched Device CSR Web Service interface through a TLS~~1.2~~ mutually authenticated session to the SMKI Portal as set out in the SMKI Interface Design Specification.

Parties require an appropriate IKI Certificate in order to authenticate to the Batched Device CSR Web Service interface. This shall be issued by DCC on successful completion of the process as set out in the SMKI RAPP in accordance with the SMKI Interface Design Specification.

Appendix O ‘SMKI Repository Interface Design Specification’

These changes have been redlined against Appendix O version 6.0.

Amend Section 2.1.1 as follows:

2.1.1 General Obligations

The DCC shall ensure that the SMKI Repository Portal interface available via a DCC Gateway Connection:

- a) uses the HTTPS protocol, secured by TLS ~~1.2~~ in line with the protocols set out in Annex C of this document;
- b) is accessed via URLs that are set out in the SMKI Repository User Guide;
- c) uses Javascript, Cascading Style Sheets (CSS) and images;
- d) is compliant with the W3C Web Content Accessibility Guidelines (v2) at “AA” level; and
- e) is only accessible using a DCC Gateway Connection.

Amend Section 2.1.2 as follows:

2.1.2 Establishing connection to the SMKI Repository Portal interface via a DCC Gateway Connection

In order to establish a connection to the SMKI Repository Portal interface, a DCC Gateway Connection user shall:

- a) ensure that their browsers have Javascript enabled;
- b) verify the ‘CA/Browser Forum’ server certificate presented by the SMKI Repository Portal, as described below and, if successfully verified by the browser, accept the certificate;
- c) enter a username and password that has been issued for the purpose of authenticating the user to the SMKI Repository Portal interface; and
- d) establish a TLS ~~1.2~~ session.

Amend Section 2.1.3 as follows:

2.1.3 Retrieval of SMKI Repository content

The DCC shall ensure that the SMKI Repository Portal interface enables DCC Gateway Connection users to search for and download via a web form the following files that are lodged in the SMKI Repository, where they have successfully established a secured TLS ~~1.2~~ connection to the SMKI Repository Portal interface (as set out in the SMKI Repository User Guide):

- a) Organisation Certificates and OCA Certificates;
- b) Device Certificates and DCA Certificates;
- c) the latest Organisation CRL and the latest Organisation ARL; and
- d) other documents lodged in the SMKI Repository.

Amend Section 2.2.1 as follows:

2.2.1 General Obligations

The DCC shall ensure that the SMKI Repository Web Service interface enables DCC Gateway Connection users' systems to search for and obtain content lodged in the SMKI Repository, as set out in section 2.2.3, Annex A and Annex B of this document.

The DCC shall ensure that the SMKI Repository Web Service interface via DCC Gateway Connection:

- a) uses the HTTPS protocol, secured by TLS ~~1.2~~ in line with the protocols set out in Annex C of this document;
- b) is accessed via URLs that are set out in the SMKI Repository User Guide;
- c) uses Extensible Markup Language (XML) over POST for message requests and responses;
- d) provides XML message responses which conform with the details set out in Annex A of this document and the XML schema set out in Annex B of this document;
- e) conforms with the XML schema set out in Annex B for message requests and responses; and
- f) is only accessible using a DCC Gateway Connection.

Amend Section 2.2.2 as follows:

2.2.2 Establishing connection to the SMKI Repository Web Service interface via DCC Gateway Connection

In order to establish a connection to the SMKI Repository Web Service interface, a DCC Gateway Connection user shall submit a request to establish a secured TLS~~1.2~~ session which:

- a) accesses a URL as set out in section 2.2.1 of this document; and
- b) includes its API Key in the querystring, in order that the SMKI Repository Interface can authenticate the user before attempting to parse the XML request document in accordance with Annex A and Annex B of this document; and
- c) configures its systems such that the TLS session renegotiation timeout is set to 5 minutes.

Amend Annex C as follows:

Annex C: Authentication Credentials

The SMKI Repository Portal Interface via DCC Gateway Connection, SMKI Repository Web Service interface and SFTP interface shall use server certificates with the following properties:

Criteria	Version
Protocol	<i>TLS1.2*</i>
Protocol Cyphers	<i>ECDHE-RSA-AES256-GCM-SHA384</i>
	<i>ECDHE-RSA-AES128-GCM-SHA256</i>

	<i>ECDHE-RSA-AES128-SHA256</i>
Client Certificate Key	<i>RSA 2048 bit</i>
Client Certificate Hash Algorithm	<i>SHA256</i>
Server Certificate Key	<i>RSA 2048 bit</i>
Server Certificate Hash Algorithm	<i>SHA256</i>

* TLS ~~1.2~~ should be implemented in accordance with Java and Apache standards and the SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website. ~~Java 7 and above supports TLS1.2.~~ The TLS version is specified in the HTTP client protocol initialisation. To enable AES256, the Java runtime should be patched with “JCE Unlimited Strength Jurisdiction Policy Files” for the version of Java being used. This is obtained from the public Oracle Java download web pages.

Appendix S ‘DCCKI Certificate Policy’

These changes have been redlined against Appendix S version 5.0.

Amend Annex A as follows:

ANNEX A

DEFINED TERMS

Transport Layer Security (or TLS)	means TLS 1.2- <u>TLS in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines published on the SEC website as defined in the Internet Engineering Task Force (IETF) Request For Change (RFC) 5246</u>
-----------------------------------	--

Appendix T 'DCCKI Interface Design Specification'

These changes have been redlined against Appendix T version 3.0.

Amend Section 2 as follows:

Submission of Personnel Authentication Certificate Applications and Issuance of Personnel Authentication Certificates

2.5 The DCC shall make a Personnel Credentials Interface accessible via the Self Service Interface for the purpose of accessing DCCKI Services in order to obtain a Personnel Authentication Certificate. The DCC shall ensure that:

- (a) the Personnel Credentials Interface uses the HTTPS protocol;
- (b) the Personnel Credentials Interface uses Java 7, update 6 (or greater);
- (c) the Personnel Credentials Interface supports JavaScript, CSS and images;
- (d) initial access to the Personnel Credentials Interface will be authorised through use of username and single use password, the provision of which shall be detailed in the DCCKI RAPP and shall be secured by server side authentication using TLS ~~1.2~~;
- (e) subsequent access to the Personnel Credentials Interface is secured by mutual authentication using TLS~~1.2~~ between the supported browser being used by the DCCKI Eligible Subscriber and the Personnel Credentials Interface;
- (f) DCCKI Certificates are used for the TLS authentication and shall support the following cipher suites:
 - i. ECDHE-RSA-AES256-GCM-SHA384
 - ii. ECDHE-RSA-AES128-GCM-SHA256
 - iii. ECDHE-RSA-AES256-SHA384
 - iv. ECDHE-RSA-AES128-SHA256;
- (g) access to the Personnel Credentials Interface is denied without a valid credential for Authentication; and
- (h) User Personnel are provided with the means to view and update their password and user account information as set out in the Self Service Interface Access Control Specification.

Appendix X 'Registration Data Interface Specification (REGIS)'

These changes have been redlined against Appendix X version 3.0.

Amend Section 2 as follows:

2. REGISTRATION DATA INTERFACE

File Exchange Mechanism

2.7 The DCC and each Registration Data Provider shall secure the FTP session using TLS, in a standard format conforming to the following internet standards as defined in the referenced RFC as published by the IETF and the Internet Society:

- (a) RFC 4217 - Securing FTP with TLS; ~~and~~
- ~~(b) RFC 5246 - TLS version 1.2.~~

Appendix AI 'Self Service Interface Code of Connection'

These changes have been redlined against Appendix AI version 3.0.

Amend Section 'Definitions' as follows:

TLS	means transport layer security version 1.2 in accordance with RFC5246 in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website.
------------	---

Amend Section 1 as follows:

1. SELF-SERVICE INTERFACE CODE OF CONNECTION

Connection Mechanisms

1.10 Each User shall establish a TLS ~~1.2~~ connection between their User Personnel browsers and either the Self-Service Interface or an Identity Provider Service, in accordance with clause 1.14.

1.11 The DCC shall provide access to the Self-Service Interface to each User using a Supported Web Browser with a minimum screen resolution of 1280x1024 pixels.

1.12 The DCC shall provide reasonable notice to Users of changes to the list of Supported Web Browsers.

Communications Authentication

1.13 Each User shall install a valid Root DCCKICA Certificate, UI DCCKICA Certificate and Personnel Authentication Certificate in its User Personnel's browser prior to establishing a TLS ~~1.2~~ connection to the Self-Service Interface in accordance with the Self-Service Interface Access Control Specification, where such DCCKI Certificates shall be obtained as set out in the DCCKI RAPP.

1.14 The User shall secure the connection between its User Personnel browser and the Self Service Interface or the Identity Provider Service used by the User, using TLS ~~1.2~~ in accordance with RFC5246 and will make use of:

(a) for the Identity Provider Service, mutual authentication using PKCS #3 Ephemeral Diffie Hellman key exchange to generate a shared secret for communications encryption, utilising one of the following cipher suites:

- (i) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDHE-RSA- AES128-SHA256;
- (ii) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDHE-RSA- AES256-SHA384;
- (iii) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDHE- RSA-AES128-GCM-SHA256; or
- (iv) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDHE-RSA-AES256-GCM-SHA384; or

(b) for the Self Service Interface, server-side authentication.

Appendix AL ‘SMETS1 Transition and Migration Approach Document’

These changes have been redlined against Appendix AL version 27.0.

Amend Section 3 as follows:

3 Transitional Application of Sections of the Code

Application of Section A (Definitions and Interpretation)

Transport Layer Security	means TLS <u>in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website. 1.2</u> as defined in the Internet Engineering Task Force (IETF) Request For Change (RFC) 5246 or any equivalent to that document which updates or replaces it from time to time.
--------------------------	--