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~~ 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.~~

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. The Triage System Interface: • Must use either TLS or IPsec, and • If using TLS then must include client authentication.
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	*TLS~~1.2~~**
Protocol Cyphers	*ECDHE-RSA-AES256-GCM-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 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~~ 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~~

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 in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website. ~~1.2 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.~~