

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.



DP272 'SMKI Document Set Changes 2024'

Modification Report

Version 0.1

10 September 2024

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



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	6
4.	Impacts	6
5.	Costs	7
6.	Implementation approach.....	8
7.	Assessment of the proposal	8
8.	Case for change	9
	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:

Elizabeth Woods

020 4566 8335

elizabeth.woods@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA).

The SMKI PMA is required to periodically review the SMKI and Data Communications Company (DCC) Key Infrastructure (DCCKI) Document Sets as stated in SEC Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure' paragraph 1.17.

Historical reviews were undertaken in early 2021 and 2023, which resulted in [MP173 'SMKI & DCCKI Document Set reviews'](#), [MP198 'Further Changes from the Review of the SMKI and DCCKI Document Set'](#) and [MP245 'SMKI Document Set Changes 2023'](#) being raised to implement the recommendations made by these reviews.

The SMKI PMA has conducted a further review in 2024 on the document sets and identified minor inconsistencies or improvements to be made. They also noted one aspect (the removal of SMKI Portal via the Internet (SPOTI)) has some urgency to it, due to the DCC re-procurement of the Trusted Service Provider (TSP).

The Proposed Solution of this modification will address the concluding observations and recommendations of the SMKI Document Set review 2024.

The costs of this proposal are limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort to implement the changes. This modification will indirectly impact all SEC Parties by giving greater clarity and transparency to the SMKI and DCCKI Document Sets, and minor process changes.

This modification is targeted for the November 2024 SEC Release. This is a Self-Governance Modification.

2. Issue

What are the current arrangements?

Review of the SMKI and DCCKI Document Sets

The SMKI PMA has an obligation in SEC Section L1.17 to periodically review the effectiveness of the SMKI Document Set (which is defined in SEC Section L9.3) and the DCCKI Document Set (which is defined in SEC Section L13.31). Historical reviews were undertaken in early 2021 and 2023, and [MP173 'SMKI & DCCKI Document Set reviews'](#), [MP198 'Further Changes from the Review of the SMKI and DCCKI Document Set'](#) and [MP245 'SMKI Document Set Changes 2023'](#) were raised to implement the recommendations made by these reviews.

What is the issue?

The review of the SMKI document sets in 2024 has identified minor inconsistencies or improvements to be made. One aspect (the removal of SPOTI) has some urgency to it, due to the DCC re-procurement of the TSP.

The findings from the 2024 review are identified in the table below.

Summary of issue	SEC Sections and Appendices affected	Proposed change
The DCC re-procurement of the TSP and removing the requirement for SPOTI	Appendices D, K, M and N	Remove requirement for SPOTI.
Identified process improvements following a recent SMKI Recovery exercise	Appendices V and AI	Replace existing clauses referring to 'Internet Explorer' with new paragraph to detail reference to DCC Browser Policy.
SMKI and S1SPKI assurance requirements	Appendices C and AO	Broaden the SMKI Independent Assurance Scheme criteria to minimise the single provider dependency risk.
DCCKI Tokens for Admin Users	Section G; Appendices S, T, V and W	Broaden the options for DCCKI Tokens to include hard and soft tokens as well as smart card tokens.

The DCC re-procurement of the TSP and removing the requirement for SPOTI

The origin of the requirement for the SPOTI was to enable Gas Networks, that were not DCC Users (and therefore without a DCC Gateway connection) to be a SMKI Subscriber and obtain SMKI Organisation Certificates. [MP128A 'Gas Network Operators SMKI Requirements'](#) removed the need for Gas Network Operators (GNOs) to be SMKI Subscribers and SPOTI has not been used for over two years. In April 2024, SECAS wrote to SEC Parties, and specifically the GNOs that have used SPOTI in the past, asking if there was a continuing need for the service. SECAS received no response. Developing and maintaining SPOTI has been a considerable expense for provision by the TSP. As the TSP is being re-procured, there is an opportunity to reduce the unnecessary costs of providing SPOTI, when it is no longer a requirement for GNOs to be SMKI Subscribers. The SMKI PMA proposes that the SPOTI requirement is removed from the SEC, as the SPOTI has not been used for two years this is unlikely to impact any Party.

SMKI PMA noted that this change needs to be in place before the DCC sets new TSP contracts, and the tenders can be made 'subject to' this modification being in place before contracts are awarded.

Identified process improvements following a recent SMKI Recovery exercise

In a recent SMKI Recovery exercise, it was noted instances where the term 'Internet Explorer' is noted as an acceptable web browser however this has now replaced by Microsoft Edge and so this term is no longer valid. To ensure futureproofing, the instances of this term should be changed to refer to the DCC's Browser Policy published on the DCC website DCCKI for acceptable web browsers. There is no direct impact to SEC Parties.

SMKI and S1SPKI assurance requirements

The original requirements for the SMKI Independent Assurance Scheme specified in SEC Appendix C 'SMKI Compliance Policy' and SEC Appendix AO 'S1SPKM Compliance Policy', were based on very tight quality criteria. These criteria can only be met by one assurance scheme and one accredited provider, and is only applied to two other Public Key Infrastructures (PKIs) in the UK. There is a risk that this scheme and the single provider could withdraw from the provision of this scheme (as recently occurred when National Cyber Security Centre (NCSC) withdrew the Commercial Product Assurance (CPA) Scheme) and the SMKI PMA wishes to broaden the criteria to minimise the risk. There is no direct impact to SEC Parties.

DCCKI Token Changes

The Universal Serial Bus (USB) tokens defined in the SEC are reliant on Java applets being executed within web browsers in order to encode and maintain the DCCKI Admin User Certificates. Once a Personnel Authentication Certificate is encoded onto the USB token via the Self-Service module, the Java applet is no longer required to access Self-Service Interface (SSI)/ Self-Service Management Interface (SSMI). It is only then required when managing or in the renewal process for the Personnel Authentication Certificate.

Leading browser providers have redacted support for Java applets from the latest versions of their products. Java is not supported by Microsoft Edge (the replacement for Internet Explorer), nor in the latest versions of Chrome or Firefox. The impact of this is that Administrators cannot enrol new or replacement certificates, as well as their Entrust¹ USB Token unless they install the Entrust client software or run a legacy unsupported version of the browsers. This is prevented in many instances by standard build processes and security policies. The SEC currently only caters for hard tokens, the SMKI PMA supports the DCC proposal to broaden the use of DCCKI Admin Tokens to also include soft tokens. This will have a positive impact on SEC Parties, as it would allow Administrators to enrol their new or replacement certificates on leading browsers.

What is the impact this is having?

If these issues are not resolved, the SMKI and DCCKI Document Sets will contain some unnecessary or inappropriate requirements. These vary in nature but include reduced expenditure and future proofing assurance, web browser and DCCKI Token details.

If these continue to remain, it could make it harder for Parties to comply with these documents and make the obligations in these documents unnecessary, inappropriate or impossible.

Cost reductions are achievable by removing the requirement for SPOTI and process improvements are achievable and independent assurance risks can be mitigated.

Impact on consumers

The issues outlined in this proposal do not impact consumers.

¹ Entrust is an authentication and identity assurance platform. It is used within the DCC Data Systems to authenticate users and provide two factor authorisation.

3. Solution

The Proposed Solution is to implement the changes identified from the SMKI and DCCKI Document Set review. These changes have been identified by the DCC and SMKI PMA Members and are supported by the SMKI Specialist and reviewed and recommended by the SMKI PMA Working Group. 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

All Parties will indirectly benefit from this modification as the SMKI and DCCKI Document Sets will have greater clarity, transparency and align with current processes. There are no expected negative impacts to SEC Parties as these changes are to processes that are no longer used in the case of SPOTI, or no direct changes to processes. There is an expected positive impact to SEC Parties for DCCKI Admin Tokens to allow new or replacement certificates on leading browsers and including soft tokens.

DCC Systems

There will be no impacts on the DCC System from this modification.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section A 'Definitions and Interpretation'
- Section G 'Security'
- Appendix C 'SMKI Compliance Policy'
- Appendix D 'SMKI Registration Authority Policies and Procedures'
- Appendix K 'SMKI and Repository Test Scenarios Document'
- Appendix M 'SMKI Interface Design Specification'

- Appendix N 'SMKI Code of Connection'
- Appendix S 'DCCKI Certificate Policy'
- Appendix T 'DCCKI Interface Design Specification'
- Appendix V 'DCCKI Code of Connection and DCCKI Repository Code of Connection'
- Appendix W 'DCCKI Registration Authority Policies and Procedures'
- Appendix AI 'Self-Service Interface Code of Connection'
- Appendix AO 'S1SPKM Compliance Policy'

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

Devices

The issues outlined in this proposal do not impact Devices.

Consumers

The issues outlined in this proposal do not impact consumers.

Other industry Codes

The issues outlined in this proposal do not impact other industry Codes.

Greenhouse gas emissions

The issues outlined in this proposal do not impact greenhouse gas emissions.

5. Costs

DCC costs

There are no additional DCC costs associated with this modification. The removal of SPOTI will reduce DCC costs.

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 new version to the industry.

SEC Party costs

There will be no other costs for SEC Parties from this modification.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **7 November 2024** (November 2024 SEC Release) if a decision to approve is received on or before 23 October 2024; or
- **Ad hoc SEC Release** if a decision to approve is received after 23 October 2024.

As this is a text-only change which needs to be in place as soon as possible, for alignment before the DCC TSP re-procurement begins, the earliest possible SEC Release that can be targeted for is the November 2024 SEC Release.

7. Assessment of the proposal

SECAS has engaged with the Chairs from the Operations Group (OPSG), Privacy Sub-Committee (PSC), Smart Meter Device Assurance Sub-Committee (SMDASC), the SMKI PMA, the Security Sub-Committee (SSC), the Technical Architecture and Business Architecture Sub-Committee (TABASC), and Testing Advisory Group (TAG) 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	No input required
PSC	No input required
SDMASC	No input required
SMKI PMA	The SMKI PMA have requested this modification be implemented.
SSC	No input required
TABASC	No input required
TAG	No input required

Observations on the issue

The changes in this modification report have been identified by the DCC and the SMKI Specialist. Both the SMKI PMA and some members of the SSC provided input into the SMKI and DCCKI Document Set reviews and agreed the observations and recommendations should be addressed.

The SMKI PMA has noted that cost reductions are achievable by removing the requirement for SPOTI and process improvements are achievable and independent assurance risks can be mitigated.

8. Case for change

Business case

The purpose of the proposed revisions to the SMKI and DCCKI Document Set is to bring the documents in line with current procedures and incorporate minor updates that have been identified. There is minimal cost to implement these changes and minimal impact to SEC Parties.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that this modification will better facilitate SEC Objective (g)² by aligning inconsistencies and incorrect references to improve security of Data and Systems.

Industry views

The SMKI PMA has agreed with the DCC that the minor changes identified require to be addressed.

Views against the consumer areas

Improved safety and reliability

This change is neutral in this area.

Lower bills than would otherwise be the case

This change is neutral in this area.

Reduced environmental damage

This change is neutral in this area.

Improved quality of service

This change is neutral in this area.

Benefits for society as a whole

This change is neutral in this area.

² To facilitate the efficient and transparent administration and implementation of this Code.

Appendix 1: Progression timetable

Timetable	
Event/Action	Date
Draft Proposal raised	10 Sep 2024
<i>CSC converts Draft Proposal to Modification Proposal</i>	<i>17 Sep 2024</i>
<i>Modification Report approved by CSC</i>	<i>17 Sep 2024</i>
<i>Modification Report Consultation</i>	<i>18 Sep – 8 Oct 2024</i>
<i>Change Board Vote</i>	<i>23 Oct 2024</i>

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
CSC	Change Sub-Committee
CPA	Commercial Product Assurance
DCC	Data Communications Company
DCCKI	Data Communication Company Key Infrastructure
GNO	Gas Network Operator
NCSC	National Cyber Security Centre
OPSG	Operations Group
PKI	Public Key Infrastructure
PSC	Privacy Sub-Committee
S1SPKI	SMETS1 Service Provider Public Key Infrastructure
S1SPKM	SMETS1 Service Provider Key Management
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMDASC	Smart Meter Device Assurance Sub-Committee
SMETS	Smart Metering Equipment Technical Specifications
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SPOTI	SMKI Portal via the Internet
SSC	Security Sub-Committee

Glossary	
Acronym	Full term
SSI	Self-Service Interface
SSMI	Self-Service Management Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group
TSP	Trusted Service Provider
USB	Universal Serial Bus

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.

DP272 ‘SMKI Document Set Changes 2024’

Annex A

Legal text – version 0.1

About this document

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

Section A ‘Definitions and Interpretation’

These changes have been redlined against Section A version 38.0.

Amend Section A1.1 as follows:

A DEFINITIONS AND INTERPRETATION

A1. DEFINITIONS

A1.1 In this Code, except where the context otherwise requires, the expressions in the left hand column below shall have the meanings given to them in the right hand column below:

<u>One Time Password (OTP) Token</u>	<u>has the meaning given to that expression in Annex A of the DCCKI Certificate Policy.</u>
---	---

Section G ‘Security’

These changes have been redlined against Section G version 23.0.

Amend Section 2.37 to 2.39 as follows:

G2. **SYSTEM SECURITY: OBLIGATIONS ON THE DCC**

Cryptographic Credential Tokens~~, and~~ Smart Card Tokens and OTP Tokens

- G2.37 Before supplying any Cryptographic Credential Token~~, or~~ Smart Card Token or OTP Token to any person in accordance with the provisions of this Code, the DCC shall ensure that the version of the software which forms part of that Cryptographic Credential Token~~, or~~ Smart Card Token or OTP Token:
- (a) operates so as to generate Public Keys each of which is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated; and
 - (b) has been adequately tested for the purpose of ensuring that it fulfils its intended purpose.
- G2.38 The DCC shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of any Cryptographic Credential Tokens~~, or~~ Smart Card Tokens or OTP Tokens to be supplied by it in accordance with the provisions of this Code, arrangements designed to ensure that the DCC will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software or firmware.
- G2.39 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which form part of any Cryptographic Credential Token~~, or~~ Smart Card Token or OTP Token which has been supplied by it in accordance with the provisions of this Code, it shall notify the Subscribers for Certificates associated with the use of Cryptographic Credential Tokens~~, or~~ Smart Card Tokens or OTP Tokens and (wherever it is reasonably practicable to do so) the manufacturer of the hardware or (as the case may be) developer of the software or firmware.

Appendix C 'SMKI Compliance Policy'

These changes have been redlined against Appendix C version 3.0.

Amend Section 2.2 as follows:

2 SMKI INDEPENDENT ASSURANCE SCHEME

Quality Requirements

2.2 The quality requirements specified in this Part 2.2 are that the SMKI Independent Assurance Scheme must be a scheme:

~~(a) which is recognised as an accreditation scheme for the purposes of the eIDAS Regulation (No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market);~~

~~(b)(a)~~ _____ which is based on ISO 27001; and

~~(c)(b)~~ _____ is an accredited scheme approved by the SMKI PMA, the provider of which:

~~(i) is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and~~

~~(ii) requires all its scheme assessors to be UKAS certified.~~

Appendix D ‘SMKI Registration Authority Policies and Procedures’

These changes have been redlined against Appendix D version 7.0.

Amend Section 5.4 as follows:

5. Detailed Party, RDP, Manufacturer, SECCo and DCC (as DCC Service Provider) registration procedures and processes

Each Party, RDP, Manufacturer, SECCo and DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

5.4 Procedure for provision of credentials to AROs for accessing SMKI Services and the SMKI Repository Service and file signing

The procedure and processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to provide credentials for accessing SMKI Services and/or the SMKI Repository Service or for file signing to Authorised Responsible Officers in respect of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider). The SMKI Registration Authority shall not provide such credentials to an individual on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider), other than where the organisation has completed SMKI and Repository Entry Process Tests and such individuals have become Authorised Responsible Officers.

Step	When	Obligation	Responsibility	Next Step
5.4.1	During ARO verification meeting and after becoming an ARO	IKI credentials for submission of CSRs in respect of Organisation Certificates using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Organisation Certificates and/or Device Certificates, and where the Party, RDP, Manufacturer, SECCo or DCC Service Provider has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal interface, provide the ARO with: If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Organisation Certificates and retrieval of corresponding Organisation Certificates via a DCC	SMKI Registration Authority	5.4.2

Managed by

		Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of CSRs in respect of Organisation Certificates and retrieval of corresponding Organisation Certificates. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via a DCC Gateway Connection. Where the Party, RDP, Manufacturer, SECCo or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
5.4.2	During ARO verification meeting and after becoming an ARO	IKI credentials for submission of CSRs in respect of Device Certificates using SMKI Portal via DCC Gateway Connection If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority	SMKI Registration Authority	5.4.3

		shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with: If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Device Certificates and retrieval of corresponding Device Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. Where the Party, RDP or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
--	--	---	--	--

Amend Section 7.1 as follows:

7. Submission of CSRs and Issuance of Certificates

7.1 Submission of Certificate Signing Requests

The SMKI Interface Design Specification (SMKI IDS) and the Code sets out the provisions in respect of:

- a) the mechanism established for this purpose is in accordance with the procedure in PKCS#10;
- b) naming restrictions in respect of the Subject of each Certificate in accordance with the relevant Certificate Policy;
- c) the circumstances in which an Authorised Subscriber may submit a Certificate Signing Request (CSR) in respect of a Device Certificate and the means by which it may do so (SMKI IDS sections 2.3.1.6, 2.4.1.1 and 2.5.1.1);
- d) the circumstances in which an Authorised Subscriber may submit a CSR in respect of an Organisation Certificate and the means by which it may do so (SMKI IDS sections 2.3.1.1 and 2.6.1.1);
- e) the circumstances in which an Authorised Subscriber for an IKI Certificate may submit a CSR in respect of an IKI Certificate and the means by which it may do so (SMKI IDS sections 2.4 and 2.5); and
- f) requirements in respect of validation of the format of a CSR, checking that the submitting organisation is an Eligible Subscriber for the Certificate and rejection if such requirements are not met.

Managed by

The SMKI Registration Authority shall validate the Subject of each CSR in respect of an Organisation Certificate to ensure that each CSR corresponds with an EUI-64 Compliant identifier range that is applicable to the relevant User Role, as provided in the Organisation Information Form.

Subject to the provisions of the Code and this SMKI RAPP, the DCC shall accept requests for copies of Organisation Certificates and/or Device Certificates from non DCC Users by phone via the Service Desk ~~or, in the case of Organisation Certificates, via the SMKI Portal via the Internet~~. The DCC shall, following such a request, provide the relevant information as soon as is reasonably practicable, via a secured electronic means.

Appendix K 'SMKI and Repository Test Scenarios Document'

These changes have been redlined against Appendix K version 4.0.

Amend Section 2 as follows:

2. Scope

Section 5 of this document sets out which Test Scenarios a Relevant Party or RDP must successfully complete, depending upon:

- which SMKI interfaces or SMKI Repository Interface the Relevant Party or RDP will access and whether this is for Device Certificates or Organisation Certificates; and
- whether access to the SMKI interfaces will be through a DCC Gateway Connection ~~or using the SMKI Portal interface via the Internet.~~

Amend Section 6 as follows:

6. Appendix A: Test Artefacts

6.1. Relevant Party or RDP Documents & Reports

6.1.1 Test Preparation Document Set

The following documentation must be produced by a Relevant Party or RDP before Testing commences:

- Test Readiness Report
- Scope of SREPT testing
- Test Plan
- Test Data Plan
- Test Schedule
- Requirements Traceability Matrix
- Test Scripts

Note regarding scope of SREPT testing - which SREPT test scenarios need to be undertaken is determined by:

- which SMKI interface or SMKI Repository Interface the Relevant Party or RDP will access and whether this is for Device Certificates or Organisation Certificates; and
- whether access to the SMKI interfaces will be through a DCC Gateway Connection ~~or using the SMKI Portal interface via the Internet.~~

Amend Section 8 as follows:

8. Appendix C: Test Scenarios

~~8.2. SMKI & Repository Entry Process Test Scenarios without DCC Gateway Connection~~

~~The following sub-sections contain the SMKI & Repository Entry Process Test Scenarios that are applicable to each prospective user of SMKI & Repository Services that do not have access to a DCC Gateway Connection.~~

8.2.1 ~~Security Credentials Access Tests to SMKI~~

ID	SMKI-04
Title:	Access the Test SMKI Service, through the SMKI Portal interface over the internet.
Description	For a Party without a DCC Gateway Connection, a SMKI ARO accesses the Test SMKI Service, through the SMKI Portal interface using the security credentials supplied by the DCC.
Objective	To prove that the SafeNet Client Installed on the SMKI ARO's computer validates their security credentials. To prove that a Party's ARO can use the FIPS Token which is registered to them and their organisation when accessing the SMKI Portal interface via the internet.

Amend Section 10 as follows:

10. Appendix E: Test Completion Certificate

TEST COMPLETION CERTIFICATE

To: [Party / RDP] [SEC Party / RDP ID]

From: [DCC]

[Date]

Dear Sirs,

TEST COMPLETION CERTIFICATE

The relevant tests have been successfully completed to provide the following credentials:

Test Scenarios for Parties or RDPs with a DCC Gateway Connection

IKI credentials for submission of Organisation CSRs using SMKI Portal via DCC Gateway Connection

IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection

IKI credentials for Ad Hoc Device CSR Web Service

IKI credentials for Batched Device CSR Web Service

Credentials for SMKI Repository Portal

Credentials for SMKI Repository Web Service

Credentials for SMKI Repository Portal SFTP

Test Scenarios for Parties without a DCC Gateway Connection

~~IKI credentials for submission of Organisation CSRs using SMKI Portal via the Internet~~

We confirm that the relevant tests have been executed in accordance with the relevant Test Documents. We confirm that the relevant Exit Criteria have been achieved.

Yours faithfully

[Name]

[Position]

Acting on behalf of the DCC

Appendix M ‘SMKI Interface Design Specification’

These changes have been redlined against Appendix M version 6.0.

Amend Contents as follows:

Contents

2.6	SMKI Portal interface via the Internet	16
	General obligations	16
	Establishing a secured web browser connection to the SMKI Portal interface via the Internet	18
	Submission of Organisation CSRs and retrieval of resulting Organisation Certificates	18

1. Introduction

1.2 Target Response Times

For the purposes of supporting the measurement of Target Response Times in accordance with Section L8.3 of the Code, the terms “sending” and “receipt” should be interpreted as follows:

- a) for the Ad Hoc Device CSR Web Service interface:
 - i. “receipt” means the receipt of a Device CSR in the DCC Systems that is submitted by an Authorised Subscriber via the Ad Hoc Device CSR Web Service interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specification in relation to ad hoc Device CSRs submitted through the Ad Hoc Device CSR Web Service interface; and
 - ii. “sending” means the submission of a Device Certificate or CSR processing error messages from the DCC Systems to the Authorised Subscriber within the synchronous response to the corresponding request; or
- b) for the Batched Device CSR Web Service interface:
 - i. “receipt” means the receipt of a Batched Certificate Signing Request (Batched CSR) in the DCC Systems that is submitted by an Authorised Subscriber via the Batched Device CSR Web Service interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specification in relation to Batched CSRs submitted through the Batched Device CSR Web Service interface; and
 - ii. “sending” means making available the files containing Device Certificates and/or CSR processing error messages via the Batched Device CSR Web Service interface, for download by the Authorised Subscriber; or
- c) for a Batched CSR via the SMKI Portal interface (via DCC Gateway Connection):
 - i. “receipt” means the receipt of a Batched CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specification in relation to Batched CSRs submitted through the SMKI Portal interface; and
 - ii. “sending” means making available the files containing Device Certificates and/or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber; or
- d) for an ad hoc Device CSR via the SMKI Portal interface (via DCC Gateway Connection):

- i. “receipt” means the receipt of an ad hoc Device CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface following successful completion by DCC of all validation and verification checks set out in the SMKI Interface Design Specification in relation to ad hoc Device CSRs submitted through the SMKI Portal interface; and
 - ii. “sending” means making available the Device Certificate or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber.
- e) for an Organisation CSR via the SMKI Portal interface (via DCC Gateway Connection ~~or via the Internet~~):
 - i. “receipt” means the receipt of an Organisation CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface following successful completion by DCC of all validation and verification checks set out in the SMKI Interface Design Specification in relation to Organisation CSRs; and
 - ii. “sending” means making the Organisation Certificate or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber.

2. SMKI interfaces

2.2 General obligations

The DCC shall ensure that PKCS#10 certification request standard is used for the submission of Certificate Signing Requests (CSRs). Authorised Subscribers shall submit Certificate Signing Requests according to the CSR structures as defined in Appendix F of this document.

In accordance with Sections L11.5 - L11.7 of the SEC, unless an Authorised Subscriber immediately notifies the DCC of Certificate rejection, the Certificate shall be deemed to be accepted.

The DCC shall ensure that the URLs of the interfaces to SMKI Services shall remain unchanged in the event of the failure of a component of interfaces to the SMKI Services, or invocation of business continuity or disaster recovery measures. The DCC shall ensure that disaster recovery systems are functionally identical to the main interface.

Error codes and examples of error messages in relation to:

- a) the SMKI Portal interface via DCC Gateway Connection ~~and SMKI Portal interface via the Internet~~ are set out in the SMKI User Guide;
- b) the Ad Hoc Device CSR Web Service interface are set out in Appendix A of this document; and
- c) the Batched Device CSR Web Service interface are set out in Appendix C and Appendix D of this document.

2.3 SMKI Portal interface via DCC Gateway Connection

Submission of Organisation CSRs and retrieval of resulting Organisation Certificates

2.3.1.1 Submission of Organisation CSRs by Authorised Subscriber

~~Subject to the provisions of 2.3.1.1 A,~~ Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they:

- a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and
- b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface.

~~A. Network Parties who are Authorised Subscribers accessing the SMKI Portal via the Internet may optionally elect not to populate the value field of the "Subject Unique Identifier" with a 64 bit EUI-64 Compliant identifier, in which case:~~

- ~~a) — they shall leave the value field of the “Subject Unique Identifier” blank, and otherwise proceed in accordance with the requirements of 2.3.1.1 (b);~~
- ~~b) — a submission made in accordance with 2.3.1.1 A(a) shall be treated for the purposes of the Code (including this Appendix M) as a CSR and be processed accordingly by the DCC, provided that:~~
- ~~c) — the Authorised Subscriber must subsequently provide a human readable hexadecimal representation of the EUI-64 value to be included within the Certificate (so using 0..9, a..f, A..F) to the DCC through the SMKI Portal interface via the Internet and re-submit the fully completed CSR via that interface;~~
- ~~d) — the DCC shall ensure that a suitably authorised member of Registration Authority personnel confirms that:

 - ~~i. — the representation of the EUI-64 Compliant identifier that has been provided is a representation of an EUI-64 Compliant identifier that has been allocated by the SEC Panel to the Authorised Subscriber, and~~
 - ~~ii. — the Authorised Subscriber is a Network Party, and~~~~in either case, if not, the DCC shall not Issue an Organisation Certificate to the Authorised Subscriber.~~~~
- ~~B. — The provisions of 2.3.1.1 A shall not apply until such time as the DCC notifies the Security Sub Committee that the DCC Systems capability to support the provisions of 2.3.1.1 A has been adequately tested and is ready to be used.~~
- ~~C. — Following a notification from the DCC to the Security Sub Committee in accordance with the provisions of 2.3.1.1 B, sub-Clause 2.3.1.1 B and this sub-Clause 2.3.1.1 C shall automatically be deleted from this Appendix M.~~

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 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;~~
- ~~d) provides a separate static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download a file in .zip format as defined in Appendix F to this document, updated as necessary, containing the base set of Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the north Region;~~
- ~~e) provides a separate static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download a file in .zip format as defined in Appendix F to this document, updated as necessary, containing the base set of Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the central Region and south Region;~~
- ~~f) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest IKI CRL;~~
- ~~g) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest Organisation CRL;~~
- ~~h) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest IKI ARL;~~
- ~~i) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest Organisation ARL;~~
- ~~j) provides a web form, as set out in the SMKI User Guide, where persons with access to the SMKI Portal via the Internet can request information held within the SMKI Repository. The DCC shall process such requests and provide information via electronic means; and~~
- ~~k) is only accessible via the Internet.~~

~~Provision of a connection to the Internet is the responsibility of the Authorised Subscriber.~~

~~The DCC shall ensure that the Organisation Certificates and OCA Certificates contained within the two Device anchor slot Certificate files shall be the same, other than the Organisation Certificates required to populate the WAN provider Device anchor slot.~~

~~The DCC shall lodge a document in the SMKI Repository, which sets out details of which of the base set of Organisation Certificates and OCA Certificates may be placed in specific Device anchor slots.~~

~~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 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 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.~~

~~Submission of Organisation CSRs and retrieval of resulting Organisation Certificates~~

~~Submission of Organisation CSRs by Authorised Subscriber~~

~~Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they:~~

- ~~a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and~~
- ~~b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface.~~

~~Receipt and validation of Organisation CSRs by the DCC~~

~~Following receipt of an Organisation CSR, the DCC shall:~~

- ~~a) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;~~

~~b) either accept, or reject the CSR:~~

- ~~i. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or~~
- ~~ii. where the CSR is rejected, log an error and return an error message via the SMKI Portal interface to the Authorised Subscriber.~~

~~Actions following acceptance of Organisation CSRs by the DCC~~

~~Where an Organisation CSR is accepted, the DCC shall:~~

- ~~a) verify the content of the CSR, which shall include checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the Authorised Responsible Officer submitting the CSR is authorised to submit CSRs; and~~
- ~~b) either approve the CSR for further processing or reject the CSR;~~
 - ~~i. where the CSR is approved, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or~~
 - ~~ii. where the CSR is rejected, notify the Authorised Subscriber via the SMKI Portal interface of the errors and reasons for the rejection of that CSR.~~

~~If an Organisation CSR is rejected by the DCC, the Authorised Subscriber must, if they still wish to be issued with a relevant Organisation Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber does not need to generate a new Key Pair in respect of the Organisation CSR.~~

~~Actions following approval of Organisation CSRs by the DCC~~

~~Where an Organisation CSR is approved by the DCC, the DCC shall:~~

- ~~a) process the CSR;~~
- ~~b) Issue a corresponding Organisation Certificate;~~
- ~~c) lodge the resulting Organisation Certificate in the SMKI Repository; and~~
- ~~d) make the Organisation Certificate available for download via the SMKI Portal interface via the Internet and the SMKI Repository.~~

~~Actions following download of an Organisation Certificate by an Authorised Subscriber~~

~~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 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 CRL in the SMKI Repository in accordance with Appendix B of the Code.~~

Appendix F Certificate Signing Request Structure

Information to be contained within an Organisation CSR

Table 1 - Section	Table 2 - Attributes	Table 3 - Value
Table 4 - Version	Table 5 -	Table 6 - Version 0
Table 7 - Subject	Table 8 - Common Name Table 9 - (id-at-commonName)	Table 10 - This field shall only be populated where, should it be placed in an Organisation Certificate produced using this CSR's details, it would comply with the requirements for the Subject X520 Common Name field in such Organisation Certificates, where those terms have their Appendix B Organisation Certificate Policy meaning.
	Table 11 - Organisational Unit Table 12 - (id-at-organizationalUnitName)	Table 13 - Remote Party Role Code of the Subject of the Certificate (2 character hexadecimal representation of the Remote Party Role Code). E.g. for supplier, value = '02'
	Table 14 - Subject Unique Identifier Table 15 - (id-at-uniqueIdentifier)	Table 16 - The 64 bit EUI-64 Compliant identifier of the subject of the Certificate
Table 17 - Subject Public Key Information	Table 18 - Public Key Algorithm	Table 19 - id-ecPublicKey
	Table 20 - Prime256r1 (256 bit)	Table 21 - Public Key Value
Table 22 - Key Usage	Table 23 - Criticality	Table 24 - True
	Table 25 - Key Usage	Table 26 - digitalSignature Table 27 - or Table 28 - keyAgreement
Table 29 - Signature Algorithm	Table 30 -	Table 31 - ecdsa-with-SHA256

CSR forms submitted to the SMKI Portal via DCC Gateway Connection ~~and the SMKI Portal via the Internet~~ will be accepted in PKCS#10 format Base64 encoded. The standard format for

CSR forms submitted to the SMKI Portal via DCC Gateway Connection ~~and the SMKI Portal via the Internet~~ will be ASN.1 DER, including either styles of PEM header (i.e. -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----). The following variants for CSR forms submitted to the SMKI Portal via DCC Gateway Connection ~~or SMKI Portal via the Internet~~ will also be accepted:

- a) No PEM headers
- b) Base64 all in one line
- c) Base64 with line breaks at 64 or 76 characters
- d) If line breaks are used the \n and \r\n are both acceptable

Information to be contained within a Device CSR

Table 32 - Section	Table 33 - Attributes				Table 34 - Value
Table 35 - Version	Table 36 -				Table 37 - Version 0
Table 38 - Subject	Table 39 -				Table 40 - Empty
Table 41 - Subject Public Key Information	Table 42 - Public Key Algorithm				Table 43 - id-ecPublicKey
	Table 44 - Prime256r1 (256 bit)				Table 45 - Public Key Data
Table 46 - Key Usage	Table 47 - Criticality				Table 48 - True
	Table 49 - Key Usage				Table 50 - digitalSignature Table 51 - or Table 52 - key Agreement
Table 53 - Subject	Table 54 - General Name	Table 56 - Other Name	Table 57 - id-on-	Table 59 - hw Type	Table 60 - Object Identifier, OID

Table 32 - Section	Table 33 - Attributes				Table 34 - Value
Alternative Name	Table 55 -		hardwareModuleName Table 58 -	Table 61 - hw SerialNum	Table 62 - Device ID (EUI-64)
Table 63 - Signature Algorithm	Table 64 -				Table 65 - ecdsa-with-SHA256

CSR forms submitted to the SMKI Portal via DCC Gateway Connection will be accepted in PKCS#10 format Base64 encoded. The standard format for CSR forms submitted to the SMKI Portal via DCC Gateway Connection will be ASN.1 DER, including either styles of PEM header (i.e. -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----). The following variants for Device CSRs submitted to the SMKI Portal via DCC Gateway Connection will also be accepted:

- No PEM headers
- Base64 all in one line
- Base64 with line breaks at 64 or 76 characters
- If line breaks are used the \n and \r\n are both acceptable

CSRs submitted via the Ad Hoc Device CSR Web Service interface or the Batched Device CSR Web Service interface shall not use PEM headers, as set out in Appendix A and Appendix C respectively.

Appendix N 'SMKI Code of Connection'

These changes have been redlined against Appendix N version 3.0.

Amend Section 1.1 as follows:

1. Connection Mechanism

1.1. Browser Policy

The DCC shall publish and keep up to date the web browsers and versions which the SMKI Portal interface via a DCC Gateway Connection, ~~and SMKI Portal interface via the Internet~~ supports.

The DCC shall not be required to continue to support any browser versions from which the browser's vendor removes support.

Browsers other than those published may also be compatible, though they will not be supported.

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 published browsers on different operating systems. The DCC shall publish and keep up to date the list of operating systems that have been tested.

Operating systems other than those listed above may also be compatible, though they will not be supported.

The browsers (and versions) and operating systems supported by the DCC shall be reviewed from time to time. The DCC shall seek views from Parties and RDPs prior to the withdrawal of support for any version of a browser, a browser itself, or an operating system set out above.

Amend Section 2.2 and 2.3 as follows:

2. SMKI Services interfaces

2.2. ~~[No longer in use] SMKI Portal interface via the Internet~~

~~The DCC shall at all times (subject to Planned Maintenance) provide and maintain an interface where a Party or RDP may connect to the SMKI Portal interface via the Internet using a compatible web browser.~~

~~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.~~

2.3. Authentication to SMKI Services interfaces

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

The DCC shall secure the SMKI Portal interface via a DCC Gateway Connection ~~or SMKI Portal interface via the Internet~~ through a mutually authenticated TLS session as set out in the SMKI Interface Design Specification.

The DCC shall publish to Parties and RDPs a 'SMKI User Guide' meeting the requirements of this document.

In order to authenticate to the SMKI Portal, Cryptographic Credential Tokens shall be issued in accordance with the procedures set out in the SMKI RAPP.

Each Party or RDP wishing to access the SMKI Portal interface shall install the Authentication Client software on each ARO's computer used to access the SMKI Portal interface.

The DCC shall make the Authentication Client software available to Parties and RDPs and ensure that the software:

- (a) is accessible via a URL that shall be specified and updated from time to time in the SMKI User Guide, using One Way Authentication which can be validated using a 'CA Browser Forum' server certificate that is signed by a 'Root CA' that is present in the Windows 'Trusted Root Certification Authorities' certificate store';
- (b) is compatible with published operating systems;
- (c) is digitally signed using the private key associated with a code signing certificate that is signed by a root CA that is present in the Windows 'Trusted Root Certification Authorities' certificate store'; and
- (d) is supported by instructions as to how to install the Authentication Client software, as set out in the SMKI User Guide.

The Party or RDP may download, and verify the authenticity and integrity of, the Authentication Client software on first use by checking the digital signature used to sign the software and validating the 'CA Browser Forum'¹ server certificate using the certification authority certificates present in the Windows 'Trusted Root Certification Authorities' certificate store'. If such checks are successful, the Party or RDP may install the Authentication Client software on each computer that they wish to use to access the SMKI Portal. In Windows, "Administrator" privileges are required to install the Authentication Client software but are not required to run such software.

The DCC shall ensure that each Cryptographic Credential Token issued contains the appropriate IKI Certificate and Private Key for that Party or RDP, which is needed to authenticate the ARO to the SMKI Portal interface via the DCC Gateway Connection ~~or the SMKI Portal via the Internet~~.

Furthermore, the DCC shall ensure that:

- (a) access to the Cryptographic Credential Token is PIN-protected and the Private Key corresponding with the IKI Certificate used for authentication cannot be removed from the Cryptographic Credential Token;
- (b) the Authentication Client software is made available for use by AROs to enable authentication to the SMKI Portal in conjunction with the Cryptographic Credential Token;
- (c) it provides support for the Authentication Client software via the Service Desk;
- (d) updates are made available to the Authentication Client software accessible via a URL, as set out in the SMKI User Guide; and
- (e) ensure that all browsers listed in section 1.1 of this document are capable of supporting the requirements set out in this section.

The process for TLS1.2 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.

¹ <https://cabforum.org/>

Amend Section 3.1 as follows:

3. Managing Demand

3.1. Capacity Management

3.1.1 SMKI Portal via a DCC Gateway Connection ~~and SMKI Portal via the Internet~~

Organisation CSRs

The Registration Authority shall process Organisation Certificate Signing Requests received via the DCC Gateway Connection ~~or via the Internet in the same manner.~~

Appendix S 'DCCKI Certificate Policy'

These changes have been redlined against Appendix S version 7.0.

Amend Section 6.2 as follows:

6 TECHNICAL SECURITY CONTROLS

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.6 Private Key transfer into or from a Cryptographic Module

- (a) The DCCKICA shall ensure that no DCCKICA Private Key is transferred or copied other than:
 - (i) for the purposes of:
 - (1) backup;
 - (2) restoration; or
 - (3) addition of new hardware, software, or firmware to a Cryptographic Module; and
 - (ii) in any event, in accordance a level of protection that is compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard.
- (b) The DCCKICA shall ensure that Private Keys associated with Personnel Authentication Certificates:
 - i. are transferred from the DCCKICA Systems to the systems of DCCKI Eligible Subscribers in a PKCS#12 format and protected with a password; and
 - ii. following such transfer, that any copies held are verifiably destroyed by the DCCKICA.
- ~~(c)~~ The DCCKICA shall ensure that Private Keys associated with Personnel Authentication Certificates for use by Administration Users are generated on a Personal Identity Verification (PIV) compliant Smart Card Token or OTP Token.
- ~~(e)(d)~~ The DCCKICA shall ensure that upon the User Personnel Certificate expiry, the Smart Card Tokens will become redundant and replaced with OTP Tokens.

Amend Annex A as follows:

ANNEX A

DEFINED TERMS

In this Policy, except where the context otherwise requires:

- expressions defined in Section A (Definitions and Interpretation) of the Code have the same meaning as is set out in that section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A (Definitions and Interpretation) of the Code and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Definitions for this Policy

<u>One Time Password (OTP) Token</u>	<u>a hardware or software based security token used to assist authentication of User Personnel</u>
Personal Identity Verification	a Smart Card Token <u>or OTP Token</u> compliant with Federal Information Processing Standard (FIPS) 201.

Amend Annex B as follows:

ANNEX B

DCCKI CERTIFICATE PROFILES

Requirements Applicable to Personnel Authentication Certificates only

Personnel Authentication Certificates that are issued by the UI DCCKICA for the purposes of Authenticating Administration Users to the Self Service Interface shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of digitalSignature. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain a two policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy and the OID for validation policy of the Smart Card Token or OTP Token PIV Authentication Key;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 of RFC 5280. This extension shall be marked as non-critical;
- include the Subject name as a meaningful name or other means of identifying an individual as provided by the DCCKI Eligible Subscriber; and
- have a Validity Period of 3 years.
- Upon expiry of a Smart Card token, the DCCKICA will only issue OTP Tokens.

Root DCCKICA Certificate DCCKI Certificate Profile

Interpretation

subjectPublicKeyInfo.

The Public Key algorithm shall be RSA as defined in NIST FIPS 180~~4~~-6.

Appendix T 'DCCKI Interface Design Specification'

These changes have been redlined against Appendix V version 4.0.

Amend Section 2.7 to 2.14 as follows:

2. DCCKI SERVICE INTERFACE

Issuance of Personnel Authentication Certificates to Administration Users

Initial Issuance of a Personnel Authentication Certificate to Administration Users

- 2.6 In order to obtain an initial Personnel Authentication Certificate, an Administration User shall log onto the Personnel Credentials Interface via the Self Service Interface using the supplied username, and single use password as provided in accordance with the DCCKI RAPP.
- 2.7 Upon initial login, the SSI Administration User shall be required to:
 - (a) change the password for the user account from that provided; and
 - (b) provide answers to security questions that will subsequently be used to confirm the identity of that Administration User if their password is forgotten, their Personnel Authentication Certificate has expired, ~~or~~ the Smart Card Token or OTP Token provided to that Administration User is lost or stolen.
- 2.8 On successful change of the user account password, the Administration User shall be able to request initialisation of the Smart Card Token or OTP Token which will result in a Personnel Authentication Certificate Application.
- 2.9 In order to initialise the Smart Card Token or OTP Token, the Administration User shall:
 - (a) request an OTP on the OTP Token or connect the Smart Card Token to the system that the Administration User is using to access the Personnel Credentials Interface. The system shall be configured in accordance with sections 2.5 (b) and (c) of this DCCKI IDS; and
 - (b) request initialisation of the Smart Card Token or OTP Token by following the instructions displayed on the Personnel Credentials Interface.
- 2.10 Following a successful request for initialisation of the Smart Card Token or OTP Token the DCC shall ensure that, where the Smart Card Token or OTP Token generates a Personnel Authentication Certificate Application, this shall automatically be submitted to the UI DCCKICA.
- 2.11 The Administration User shall be notified via the Personnel Credentials Interface as soon as reasonably practicable of the Issuance of a Personnel Authentication Certificate for that Administration User.

Subsequent Issuance of a Personnel Authentication Certificate to Administration Users

- 2.12 Prior to the expiry of a Personnel Authentication Certificate Issued to an Administration User, that Administration User may:

- (a) log onto the Personnel Credentials Interface via the Self Service Interface, using their Smart Card Token, username and password or OTP Token; and
 - (b) reinitialise the Smart Card Token or OTP Token by following the steps set out in section 2.9 of this DCCKI IDS, which will result in the Issuance of a new Personnel Authentication Certificate.
- 2.13 In the event that a Personnel Authentication Certificate Issued to an Administration User has expired prior to their obtaining a new Personnel Authentication Certificate, that Administration User may:
- (a) log onto the Personnel Credentials Interface via the Self Service Interface and obtain a new Personnel Authentication Certificate by:
 - (i) using their Administration User username and password; and
 - (ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and
 - (b) reinitialise the Smart Card Token or OTP Token by following the steps outlined in section 2.9 above which will result in the Issuance of a new Personnel Authentication Certificate.
- 2.14 In the event that the Smart Card Token or OTP Token is lost or stolen, an Administration User may:
- (a) obtain a new ~~Smart Card~~OTP Token from their DCCKI ARO in accordance with the DCCKI Code of Connection;
 - (b) log onto the Personnel Credentials Interface via the Self Service Interface:
 - (i) using the Administration User's username and password; and
 - (ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and
 - (c) initialise the ~~Smart Card~~OTP Token by following the steps outlined in section 2.9 of this DCCKI IDS which will result in the Issuance of a new Personnel Authentication Certificate.

Issuance of Personnel Authentication Certificates to other User Personnel

Initial Issuance of a Personnel Authentication Certificate to other User Personnel

- 2.15 The initial Issuance of a Personnel Authentication Certificate to a User Personnel shall be via the Personnel Credentials Interface following the creation of an account for that User Personnel by an Administration User.
- 2.16 In order to provide Authentication credentials to User Personnel, (which shall comprise a single use password and a username) an Administration User may:
- (a) log onto the Self Service Interface using their Smart Card Token or OTP Token, username and password in accordance with the Self Service Interface Access Control Specification and Self Service Interface Code of Connection;
 - (b) create additional user accounts for other User Personnel; and
 - (c) provide details to those User Personnel including a username and single use password that allows them to log onto the Personnel Credentials Interface via the Self Service Interface.

Appendix V 'DCCKI Code of Connection and DCCKI Repository Code of Connection'

These changes have been redlined against Appendix V version 2.0.

Amend Section 3.7 as follows:

3. THE DCCKI INTERFACE CODE OF CONNECTION

Management of Smart Card Tokens and OTP Tokens

- 3.5 Parties shall physically protect the Smart Card Token or OTP Tokens from unauthorised access and shall ensure the Smart Card Token is only used for the purpose for which it is intended.
- 3.6 In the event that an Administration User loses a Smart Card Token, that Administration User shall notify a DCCKI ARO for the DCCKI Subscriber. That DCCKI Subscriber shall ensure that the notified DCCKI ARO notifies the Service Desk.
- 3.7 DCC shall provide a replacement ~~Smart Card~~OTP Token where it receives a reasonable request for such replacement from a DCCKI ARO.
- 3.8 Where a Smart Card Token is no longer required, DCCKI Subscribers shall destroy that Smart Card Token beyond use and may subsequently discard it. DCCKI Subscribers shall notify the DCC of any such destruction.
- 3.9 Where an Administration User no longer requires access to the Self Service Interface, the DCCKI ARO shall raise an Incident in accordance with the Incident Management Policy in order to request retirement of the Self Service Interface account for that Administration User. The DCC shall ensure that this results in the revocation of the Personnel Authentication Certificate previously Issued to that Administration User.

Amend Annex A as follows:

ANNEX A

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- any expressions not defined here or in Section A of the Code have the meaning given to them in the DCCKI Certificate Policy, the DCCKI Registration Authority Policies and Procedures or the Self Service Access Control Interface Specification.

<u>One Time Password (OTP) Token</u>	<u>a hardware or software based security token used to assist authentication of User Personnel</u>
--------------------------------------	--

Smart Card Token	a physical security device used to assist authentication of User Personnel
Supported Web Browser	a web browser version that the DCC supports for use with the Self-Service Interface as listed, and as updated from time to time, in the DCC Browser Policy section of and published on the DCC Website

Appendix W ‘DCCKI Registration Authority Policies and Procedures (DCCKI RAPP)’

These changes have been redlined against Appendix W version 4.0.

Amend section 3 as follows:

3. PARTY AND REGISTRATION DATA PROVIDER ENROLMENT

Submission of Administration User Credentials Requests

- 3.19 A DCCKI ARO of a DCCKI Authorised Subscriber that meets the conditions set out in section 3.18 of this DCCKI RAPP may submit an Administration User Credentials Request to the DCCKI Registration Authority using the form provided for the purpose on the DCC Website, which shall be substantively in the form set out in Annex A (A5) to this DCCKI RAPP.
- 3.20 In submitting an Administration User Credentials Request, a DCCKI ARO of a DCCKI Subscriber shall provide the required details of the User Personnel who are to be provided with Smart Card Tokens or OTP Tokens, single use passwords and usernames for the purposes of establishing access to the Personnel Credentials Interface, and submitting a Personnel Authentication Certificate Application as Administration Users.

DCCKI Registration Authority processing of Administration User Credentials Requests

- 3.21 On receipt of an Administration User Credentials Request, DCCKI Registration Authority Personnel shall;
- (a) confirm via the Service Desk to the DCCKI ARO that submitted the request that such request has been received, where this notification may be made via telephone or in writing using the contact details established as part of enrolment to the DCCKI Services;
 - (b) ensure that the submitting organisation meets the conditions set out in section 3.18 of this DCCKI RAPP; and
 - (c) ensure that all required information has been provided.
- 3.22 Where the Administration User Credentials Request is valid, the DCCKI Registration Authority shall in relation to that request:
- (a) ensure that single use passwords and usernames are generated for each member of User Personnel whose details are provided;
 - (b) provide, via a secured electronic means as set out on the DCC Website, the usernames to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface;
 - (c) provide, via secure post or secure device, the single use passwords to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface; and
 - (d) provide one Smart Card Token or OTP Token for each member of User Personnel identified:
 - (i) to the DCCKI ARO that submitted the request or their named alternative, whose details have been provided by that DCCKI ARO at the time the request was made. This delivery may be in person, via a nominated employee, or via a commercial courier service. (Any person delivering the materials shall have information that enables verification of the materials and the sending organisation, and allows authentication of that person’s identity); and
 - (ii) ensure that the DCCKI ARO that submitted the request (or their named alternative) is advised in advance of any such delivery, including the means of delivery, and the name of the person that shall be making that delivery. This notification may be made via telephone

or in writing using the contact details established as part of enrolment to the DCCKI Services.

- 3.23 If the Administration User Credentials Request is not valid, the DCCKI Registration Authority Manager shall ensure that a DCCKI SRO of the submitting organisation and the DCCKI ARO who submitted that request is notified of the reasons for its rejection.

Establishment of Administration User credentials

- 3.24 On receipt of the Smart Card Tokens, usernames and single use passwords from the DCCKI Registration Authority, the DCCKI ARO shall ensure the distribution of the required materials to the relevant User Personnel within their organisation. Those User Personnel may then use the materials to access the Personnel Credentials Interface for the purposes of submitting a Personnel Authentication Certificate Application and obtaining a Personnel Authentication Certificate in accordance with the procedures set out in the DCCKI Interface Design Specification.
- 3.25 Following successfully obtaining a Personnel Authentication Certificate, the User Personnel nominated by that DCCKI ARO shall be an enabled Administration User who may then create usernames and single use passwords for other User Personnel within their organisation in accordance with the DCCKI Interface Design Specification.
- 3.26 In the event that, following provision of Smart Card Tokens, usernames and single use passwords by a DCCKI ARO, relevant User Personnel are unable to successfully obtain a Personnel Authentication Certificate, that DCCKI ARO shall raise an Incident in accordance with the Incident Management Policy, in order to resolve the matter.

Amend Annex B as follows:

ANNEX B DEFINED TERMS

In this DCCKI RAPP, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of this document.

Definitions for this DCCKI RAPP

Administration User Credentials Request	means a request submitted by a DCCKI ARO for the provision of Smart Card Tokens <u>or OTP Tokens</u> , usernames and single use passwords to be utilised by User Personnel nominated to be an Administration User.
<u>One Time Password (OTP) Token</u>	<u>a hardware or software based security token used to assist authentication of User Personnel.</u>
Smart Card Token	a physical security device used to assist authentication of User Personnel.

Appendix A1 ‘Self-Service Interface Code of Connection’

These changes have been redlined against Appendix A1 version 3.0.

Amend Definitions as follows:

Definitions

In this document, except where the context otherwise requires:

- expressions defined in Section A1 of the Code (Definitions) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- any expressions not defined here or in section A1 of the Code have the meaning given to them in the Self-Service Interface Access Control Specification, the SSI Baseline Requirements Document or the DCC User Interface Specification.

Supported Web Browser	
	a web browser version that the DCC supports for use with the Self-Service Interface as listed, and as updated from time to time, in the DCC Browser PolicyInternet Explorer versions 9, 10 and 11, and a minimum of 2 other browsers as listed and published on the DCC Website (such list as updated from time to time).

Appendix AO 'S1SPKM Compliance Policy'

These changes have been redlined against Appendix AO version 2.0.

Amend Section 2.2 as follows:

2 S1SPKI INDEPENDENT ASSURANCE SCHEME

Quality Requirements

2.2 The quality requirements specified in this Part 2.2 are that the S1SPKI Independent Assurance Scheme must be a scheme:

- ~~a) which is recognised as an accreditation scheme for the purposes of Article 3(2) of Directive 1999/93/EC on a Community framework for electronic signatures;~~
- ~~b)a) _____ which is based on ISO 27001; and~~
- ~~e)b) _____ is an accredited scheme approved by the SMKI PMA, the provider of which:~~
 - ~~(i) _____ is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and~~
 - ~~(ii) _____ requires all its scheme assessors to be UKAS certified.~~