Version: P1.0

APPENDIX P

SMKI Repository
Code of Connection

Purpose and Scope

The SMKI Repository Code of Connection sets out the way in which the Parties, the RDPs, the Panel and the SMKI PMA may access and communicate with the SMKI Repository Interface as set out in Section L6.5 of the SEC,

1.   Connection Mechanism

1.1.   Interface access

The DCC shall ensure that only persons who are Authorised Responsible Officers (AROs) and have been issued with credentials, in accordance with the SMKI RAPP, used to access a SMKI Repository interface, shall be able to access that interface on behalf of their organisation.

DCC Gateway Connection users may connect to the SMKI Repository interfaces as set out in sections 3.1 to 3.3 of this document, via that DCC Gateway Connection, and where they have been issued with credentials to authenticate to such SMKI Repository interfaces. The means by which a connection is made to the SMKI Repository interfaces is set out in the SMKI Repository Interface Design Specification. DCC Gateway Connection users may connect to the SMKI Repository interfaces using:

(a)   a web browser as set out in sections 1.2 and 2.1.1 of this document;

(b)   an automated System-to-System interface to access the SMKI Repository Web Service interface, as set out in section 2.1.2 of this document and the SMKI Repository Interface Design Specification; or

(c)   a SSH File Transfer Protocol (SFTP) client, as set out in section 2.1.3 of this document and the SMKI Repository Interface Design Specification.

Where Systems, are used to access the SMKI Repository Portal interface, SMKI Repository Web Service interface or SFTP interface via a DCC Gateway Connection:

(i)   the Party or RDP shall ensure their Systems negotiate connections using TLS, as set out in the SMKI Repository Interface Design Specification; and

(ii)   the DCC shall ensure that unencrypted HTTP requests will not be responded to by the SMKI Repository Portal interface or SMKI Repository Web Service interface, other than to redirect them to their equivalent secure URLs.

Any Party or RDP without a DCC Gateway Connection may access SMKI Repository content as set out in section 2.2 of this document and the SMKI Repository Interface Design Specification.

1.2.   Browser Policy

The DCC shall ensure that the SMKI Repository Portal Interface supports as a minimum the following web browsers and versions:

(a)   Google Chrome version 34.

(b)   Microsoft Internet Explorer versions 9, 10 and 11; and

(c)   Mozilla Firefox version 27.

The DCC shall ensure that future releases of each of the web browsers set out above are also supported.

Browsers and versions other than those listed above may also be compatible, though they will not be supported and access to the SMKI Repository Portal interface using other such browsers and versions cannot be guaranteed. No browsers shall be explicitly blocked or denied access to the SMKI Repository Portal interface, though there may be unexpected behaviour when a browser or version other than those listed is used.

The browsers supported by the DCC shall be reviewed from time to time. Except as set out in the paragraph below, the DCC shall seek views from Parties or RDPs with access to the SMKI Repository Portal interface prior to the withdrawal of support for any browser or version set out above.

The DCC shall not be required to support browser versions that are not supported by that browser's vendor.

1.3. Lodging Information in the SMKI Repository

The DCC shall ensure that any persons as set out in Section L5.3 of the SEC may lodge information in the SMKI Repository. Such persons acting on behalf of the SMKI PMA or Code Administrator must be an ARO and shall contact the DCC Service Desk in order to lodge information into the SMKI Repository.

Prior to lodging any such information in the SMKI Repository, the DCC shall authenticate the identity of the ARO wishing to lodge information in the SMKI Repository by confirming such information from the relevant ARO Nomination Form, in order to provide confidence that the request is from an authorised ARO.

The DCC shall lodge all information in the SMKI Repository as soon as is practicable upon receipt, subject to the above identity checks.

2. SMKI Repository interfaces

2.1. SMKI Repository interfaces via DCC Gateway Connection

2.1.1 SMKI Repository Portal interface

Where Parties or RDPs connect to the SMKI Repository via the SMKI Repository Portal Interface, the DCC shall make available to download or view online a copy of all documents set out in section 2.1 of the SMKI Repository Interface Design Specification.

2.1.2 SMKI Repository Web Service interface

The DCC shall make available via the SMKI Repository Web Service interface those documents lodged in the SMKI Repository as are set out in section 2.2 of the SMKI Repository Interface Design Specification. The DCC shall implement the XML schema for the SMKI Repository Web Service interface as set out in the SMKI Repository Interface Specification.

The DCC shall ensure that inputs and outputs to the SMKI Repository Web Service interface are XML documents, with the exception of the Application Programming Interface (API) Key used to establish a TLS connection in accordance with the SMKI Repository Interface Design Specification. Such API Key is provided by the DCC via the SMKI Repository Portal as set out in the SMKI Repository Interface Design Specification.

2.1.3   SFTP interface

The DCC shall make available via the SFTP Interface, those documents lodged in the SMKI Repository as are set out in section 2.3 of the SMKI Repository Interface Design Specification.

2.2.   SMKI Repository content access for users without a DCC Gateway Connection

Parties, RDPs or representatives of the SMKI PMA, Panel or Code Administrator wishing to obtain information lodged in the SMKI Repository, other than via a DCC Gateway Connection, may do so by contacting the DCC Service Desk as set out in the SMKI Repository User Guide, via personal visit, e-mail, signed fax, signed letter or telephone for the purposes of viewing, and/or obtaining a copy of a document lodged in the SMKI Repository. Following such contact, the DCC shall ensure that the relevant requested copies of Certificates or other information is provided via optical media such as CD, DVD or, where appropriate, email.

Parties or RDPs may also access the SMKI Portal via the Internet to retrieve SMKI Repository content, as set out in the SMKI Interface Design Specification.

3.   Authentication

The DCC shall ensure that credentials to access the SMKI Repository interfaces are provided, following successful completion of the registration processes required to become an ARO, as set out in the SMKI RAPP.

Access to the SMKI Repository interfaces for persons who do not have access to a DCC Gateway Connection is set out in section 2.2 of this document.

3.1.   Authentication to the SMKI Repository Portal interface

The DCC shall provide DCC Gateway Connection users with a username and password in accordance with the SMKI RAPP. Upon first login or after a password reset completed by the DCC, the DCC Gateway Connection user shall be required to ensure that the ARO's account password is changed via the SMKI Repository Portal, as set out in the SMKI Repository User Guide.

If the DCC Gateway Connection users enters an incorrect password five times within a one hour period, the DCC shall ensure that the account will automatically lock for one hour from the first failed authentication attempt, or until it is manually unlocked by an administrator on request by an ARO to the DCC Service Desk. Upon request from an ARO to unlock its SMKI Repository Portal interface password, the DCC shall authenticate the identity of the ARO by confirming such information from the relevant ARO Nomination Form, in order to provide confidence that the request is from an authorised ARO.

3.2.   Authentication to the SMKI Repository Web Service interface

The DCC shall secure the Ad Hoc Device CSR Web Service interface through a secured TLS1.2 session to the SMKI Portal in accordance with the SMKI Interface Design Specification.

The DCC shall, in relation to the SMKI Repository Web Service Interface, ensure that:

(a)   Authentication of the client to the SMKI Repository Web Service interface uses an API key to authenticate the DCC Gateway Connection user for each web service request. Requests not containing a valid API key will be rejected;

(b)   API keys have a one-to-one mapping with DCC Gateway Connection user accounts, and the user may view or choose to regenerate their API key through the SMKI Repository Portal interface;

(c)   Authentication using an API key must be used for each web service request;

(d)   The format of the API key is a 15 character pseudo-random, case insensitive string. API keys are automatically generated by the SRI, and cannot be specified by the Party. The API Key shall remain valid until a new API Key is generated by the Party using the SMKI Repository Portal and shall be invalid thereafter; and

(e)   the SMKI Repository Web Service interface presents to the user a x.509 v3 certificate that is recognised by the CA/Browser Forum for the purposes of allowing the DCC Gateway Connection user's systems to authenticate the server as part of establishing the TLS session. This certificate shall be provided as set out in the SMKI RAPP.

3.3. Authentication to the SFTP interface

The DCC shall provide each DCC Gateway Connection user with a username and password to access the SFTP server.

Each DCC Gateway Connection user can view or change the password within the profile page on the SMKI Repository Portal. The password shall remain valid until manually modified by the Party using the SMKI Repository Portal and is invalid thereafter.

4. Managing Demand

Each DCC Gateway Connection user shall provide a forecast of the number of certificates that the DCC Gateway Connection user anticipates retrieving from any SMKI Repository Interface either individually or in bulk. Such forecasts shall be a reasonable estimate of the DCC Gateway Connection user's intended usage. The scope of requests in relation to which a forecast is required is set out in Appendix A of this document.

Each DCC Gateway Connection user shall take all reasonable steps to ensure that their usage does not exceed 120% of their forecast in Table 1.

When a DCC Gateway Connection user's actual number of requests for a particular type of access, as set out in Table 1, to the SMKI Repository exceeds 120% of its forecast, the DCC Service Desk may inform the DCC Gateway Connection user via secured electronic means as set out in the SMKI Repository User Guide.

Each DCC Gateway Connection user shall notify the DCC Service Desk of any short term or long term usage which is expected to exceed 120% of its forecast and the DCC shall make reasonable attempts to meet this additional demand which may include proposal of a schedule when this additional demand can be met without adversely affecting the provision of the service.

4.1. Error Responses

The DCC shall ensure that where an error occurs in the use or operation of the SMKI Repository Portal interface, an error message shall be generated. This error message shall be communicated to the DCC Gateway Connection user. The error message shall include a clear reason for the error.

The DCC shall ensure that where an error occurs in the use or operation of the SMKI Repository SFTP Interface an error message is returned as defined in SSH File Transfer Protocol, Draft 13, July 2006 and the SMKI Repository Interface Design Specification section 2.3.1.

The DCC shall ensure that where an error occurs in the use or operation of the SMKI Repository Web Service interface, an error message shall be generated. This error message shall be communicated to the DCC Gateway Connection users as defined in the SMKI Repository Interface Specification.

In cases where there is a failure of the service or infrastructure, or a delay in the processing of a request that causes the DCC Gateway Connection user's browser or a device upstream of the SRI to abandon the request before the SRI begins to execute the request, the generation or delivery of a SMKI Repository Interface error message may not be possible.

Appendix A   Templates for Information to be supplied by Parties

Each DCC Connection user shall provide to the DCC via the DCC Service Desk, using the mechanism as set out in the SMKI Repository User Guide, the forecast information identified in this Appendix in regard to their proposed use of the DCC Gateway Connection user's connection to the SMKI Repository.

1.   Usage Forecast

DCC Gateway Connection users shall forecast their usage of the SMKI Repository in relation to the request types in the table below.

The first table identifies the forecasts required of the number of requests for web services requests and SMKI Repository Portal requests.

Request type	Maximum Number of Requests per 24 hour period
SMKI Repository Web Service interface requests	< value >
SMKI Repository Portal interface requests	< value >

Table 1 Daily Usage Forecast

An assumption has been made that the daily delta file will be downloaded by each DCC Gateway Connection user each day and one download of the full database file per week. DCC Gateway Connection users shall enter the day of the week that they will download the full database file. All additional attempts to download the delta file or full database file or attempts to download the database file outside of the agreed day must be communicated and agreed with the DCC. The DCC shall make reasonable attempts to meet this additional demand, or change in schedule, which may include proposing a day and time frame when this will be possible without adversely affecting the provision of the service.

Request type	Download Day
SFTP Full Download	< Day >

Table 2 SFTP Full Download Forecast

The following table is provided for the DCC Gateway Connection users to set out their forecast of the reasonable maximum usage during any 24 hour period.

	Off Peak		Core	Non-Core (evening)
Mode of Operation	00:00 – 07:00	07:00 - 08:00	08:00 - 20:00	20:00 – 00:00
SMKI Repository Portal interface requests	< Percentage of total requests via SMKI Repository Portal interface>	< Percentage of total requests via SMKI Repository Portal interface>	< Percentage of total requests via SMKI Repository Portal interface>	< Percentage of total requests via SMKI Repository Portal interface>
SMKI Repository Web Service interface requests	< Percentage of total requests via SMKI Repository Web Service interface >	< Percentage of total requests via SMKI Repository Web Service interface >	< Percentage of total requests via SMKI Repository Web Service interface >	< Percentage of total requests via SMKI Repository Web Service interface >
SFTP interface daily delta file request	< Percentage of total requests to download delta files>	< Percentage of total requests to download delta files >	< Percentage of total requests to download delta files >	< Percentage of total requests to download delta files >
SFTP interface full file request	< Percentage of total requests to download full files>	< Percentage of total requests to download full files>	< Percentage of total requests to download full files>	< Percentage of total requests to download full files>

Table 3 % of Daily Forecast

Appendix B   Definitions

Term	Meaning as defined in SEC
API Key	Means an application programming interface key, used for the purposes of identifying the user of the SMKI Repository Web Service interface