Code Subsidiary Document

No. 0400:

Common interface technical specifications

Change History

Version Number	Date of Issue	Reason For Change	Change Control Reference	Sections Affected
~~20150511~~	~~11 May 2015~~	~~For industry consultation~~		
~~20150714~~	~~14 July 2015~~	~~For pre-vendor MAP~~		
~~ICP Housekeeping~~	~~25 August 2015~~	~~Non -material housekeeping changes~~	~~ICP/WRC/CP001~~	~~All~~
~~ICP Quality Assurance~~	~~22 September 2015~~	~~Clarificatory and syntax changes following review of the texts~~	~~ICP/WRC009~~	~~Definitions, 2.3.1, 2.8.1(d), 4.2.5, 4.3.1, 5.3.1, 6.1.2, 7.5.1, 7.5.2, 7.6.1, 7.7.1, Appendix A – Table 4~~
~~ICP Encryption and Non Repudiation of Message Content~~	~~15 September 2015~~	~~Encryption and Non Repudiation of Message Content~~	~~ICP/WRC006~~	~~Definitions, 2.5, 4.3, 5.3.1, 7.2.4, 8.2.1(a), 8.4.1(Table 3)~~
~~20150930~~	~~30 September 2015~~	~~For post-vendor MAP~~		~~As per Quality Assurance and Encryption and Non Repudiation versions~~
~~ICP Document and transaction headers supporting sequential processing~~	~~12 January 2016~~	~~Document and Transaction Headers Supporting Sequential Processing~~	~~ICP/WRC011~~	~~Definitions, 7.6.1, 7.6.2, 7.6.3, 7.7.1~~
~~ICP Password policy and account~~	~~23 February 2016~~	~~Password Policy and Account~~	~~ICP/WRC012~~	~~2.9.1~~ ~~2.9.3~~

Version Number	Date of Issue	Reason For Change	Change Control Reference	Sections Affected
~~management~~		~~Management~~		~~2.10.1~~
~~ICP Housekeeping changes~~	~~23 February 2016~~	~~Non-material housekeeping changes~~	~~ICP/WR019~~	~~2.3.1(b)~~
~~20160223~~	~~23 February 2016~~	~~For 20160223~~		~~As per ICP/WRC011, ICP/WRC012 and ICP/WRC019~~
~~ICP Housekeeping Changes~~	~~21 September 2016~~	~~Changes to reflect ICP Change Proposal ICP/WRC049~~	~~ICP/WRC049~~	~~2.9.1 (a)~~
~~20160921~~	~~21 September 2016~~	~~For 20160921~~		~~As per ICP/WRC049~~

Table of Contents

Definitions

Unless expressly stated otherwise, for the purposes of this CSD:

(a) terms defined in the Wholesale-Retail Code Part 1 (Objectives, Principles and Definitions) shall apply; and

(b) capitalised terms relating to the titles of Data Items or Data Transactions described in CSD 0301 (Data Catalogue) shall have the meaning attributed therein.

For the purposes of this CSD and all other Interface CSDs only, the following capitalised terms shall have the following meaning:

Definitions	
Term	**Definition**
"Administrator"	the person and deputy appointed by each Trading Party to manage Interface access and account privileges for users within their organisation enforcing Role Based Access Controls for interfaces with screen based access functionality;
"Anomaly Detection"	the identification of items, events or observations which do not conform to an expected pattern;
"Authenticity"	the ability for the Market Operator or a Trading Party to be sure that the communications which they receive are from an authentic source and "Authentication". "Authenticate" and "Authenticated" shall be used accordingly;
"Certificate Authority"	the trusted third-party that certifies the identity of the Market Operator or a Trading Party who rely upon a Digital Certificates and issue Digital Certificates;
"CSV" – Character Separated Value File	the mechanism by which to collect data from a table. A CSV file is a Character Separated File and is the format in which reports are generated by the Market Operator for retrieval by Trading Parties as described in CSD 0403 (Interface for the provision of Reports from the Market Operator to Trading Parties);
"Confidentiality"	a security end-to-end trust principle. Confidentiality ensures that confidential data is not shared inappropriately with unauthorised parties, nor data is obtained by unauthorised methods;

Definitions	
“Cryptographic Protections”	the secure mechanisms by which interactions between Trading Parties and the Market Operator can be Authenticated and kept Confidential by the application of Digital Certificates;
“Digital Certificate”	certifies the ownership of a public key by the named subject of the Digital Certificate. This allows others (relying parties) to rely upon organisation Digital Signatures or on assertions made by the private key that corresponds to the certified public key;
“Document”	the file within which single or multiple Data Transactions are submitted to the Market Operator, or within which the Market Operator provides responses or notifications to Trading Parties through the interface described in CSD 0401 (Transactional interface for Trading Parties having a high volume of Data Transactions). Where a Document contains multiple Data Transactions, the Data Transactions may be of different types. A Document includes information to identify and Authenticate the Trading Party or the Market Operator, a time and date stamp and a unique identifier for the Document;
“Document Reference Number”	a unique identifier by which every Document submitted to the Market Operator can be identified;
“HTTPS”	a communications protocol for secure communication over a computer network, with especially wide deployment on the internet. HTTPS provides Authentication of the website and associated web server with which the party is communicating, and therefore protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, providing protection against eavesdropping and tampering with and/or forging the contents of the communication;

Definitions	
“Interaction”	a uniquely identifiable exchange of data or information between a Trading Party and the Market Operator or vice versa through the Market Operator interfaces. An Interaction can be an exchange of Documents containing single or multiple Transactions; a data query; requesting and retrieval of a report or raising a service management incident. “Interactions” shall also be used accordingly;
“Integrity”	a security end-to-end trust principle that provides assurance that a communication received through the interface by either the Market Operator or a Trading Party remains as it was initially sent and has not been changed accidentally or maliciously whilst in transit;
“Internet Protocol”	specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine Internet Protocol with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source;
“ISO 8601”	the standard for date and time representation oras amended or replaced from time to time;
“Key Revocation”	the withdrawal of a cryptographic key by either the Market Operator or a Trading Party either as part of a routine key management policy or where it has been identified that security integrity has been compromised;
“Local Time”	the time convention used for any references to time that are visible to interface users and/or used within Reports provided to Trading Parties by the Market Operator;
“Non-Repudiation”	a security end-to-end trust principle providing assurance that at all times the sender of a communication (Market Operator or Trading Party) cannot successfully claim that they did not send it;
“Open Standards”	allows multiple parties to develop their own solutions without requiring the use of specific technologies which are only available under commercial terms. An Open Standard must not prohibit conforming implementations in open source software;

Definitions	
“Policy Enforcement Point”	is a level of applied discipline to control access to a network. The criteria under which an end system is allowed to access the network is set out in a policy;
“Public Key Infrastructure”	is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke Digital Certificates and enables the binding of public keys with respective Market Operator and Trading Party identities by means of third-party Certificate Authority;
“Planned Outage”	where a Market Operator service is unavailable due to planned maintenance. The outage period has been notified to all Trading Parties by the Market Operator in advance;
“Processing Return Codes”	are Market Operator Systems codes providing a meaningful explanation of a processing failure/error/rejection;
“Processing Status Code”	a Market Operator provided processing code indicating pass/fail of a processing activity;
“Push Service”	the process by which web application servers push data to another web application server;
“Rekeying” (Digital Certificate)	the creation of a new Digital Certificate with the same name and authorisations as the old one, but a new validity period and a new serial number and “Rekeying” or “Rekeyed” shall be used accordingly;
“Role Based Access Control”	the means by which a Trading Party or a Trading Party user is assigned one or more roles, and each role is assigned one or more privileges to the user in that role;
“Session”	the establishment of a valid connection between the Market Operator and a Trading Party through a Market Operator interface. During a Session tasks can be simple or complex but limited by access control, individual user requests (limited by pre-defined user privileges) and the specific functions of the interface;
“SOAP” – Simple Object Access Protocol	the specification for exchanging structured information in the implementation of web services in computer networks. It uses eXtensible Mark-up Language (XML) as the message format;
“Support”	relates to the Marker Operator’s Business Day and Extended Hours where help desk support will be available to Trading Parties using the Market Operator interfaces;

Definitions	
“Transaction”	a package of information exchanged between a Trading Party and the Market Operator or vice versa and is compliant with CSD 0301 (Data Catalogue). The definition is only relevant to CSD 0401 (Transactional interface for Trading Parties having a high volume of Data Transactions) and CSD 0402 (Transactional interface for Trading Parties having a low volume of Data Transactions). All Transactions submitted via these interfaces are encapsulated within Documents, where each Document contains one (1) or more Transactions. Where Transactions are referred to within CSDs in general terms, it is implicit that they will be encapsulated in a Document for submission via the interfaces defined in CSD 0401 (Transactional interface for Trading Parties having a high volume of Data Transactions) and CSD 0402 (Transactional interface for Trading Parties having a low volume of Data Transactions). For a Transaction to be completed and its contents to be made permanent in the Market Operator System, a Transaction has to be processed in its entirety and where necessary “Transact” shall be used accordingly;
“Transmission Control Protocol”	establishes a virtual connection between a destination and a source;
“TLS” – Transport Layer Security	creates a secure connection between a client and a server using encryption;
“Unplanned Outage”	where an interface is unexpectedly unavailable but not as the result of any Planned Outage / maintenance activities;
“UTC” – Coordinated Universal Time	the primary time standard by which clocks and time are regulated. It is the time convention used for the Market Operator Systems;
“Verify”	means confirming that a Session meets all of the applicable requirements of the interface and the Market Operator prior to submission, including compliance with CSD 0301 (Data Catalogue) and any other appropriate CSD that is referenced, and where necessary “Verified” or “Verification” shall be used accordingly;
“WSDL” – Web Services Description Language	is an XML-based language that provides a model for describing Web Services. It describes services as a collection of network endpoints or ports;

Definitions	
“X.509”	is the recognised cryptography standard for Public Key Infrastructure; and
“XML” – eXtensible Markup Language	is a set of rules for encoding documents in a machine-readable format. The use of XML provides simplicity and usability of the Internet for all Trading Parties and the Market Operator.

1. Introduction

1.1 Purpose and scope

1.1.1 The Interface CSDs taken together describe all interfaces to all Market Operator Systems used by Trading Parties, including any test and development systems which may be made available by the Market Operator from time to time.

1.1.2 This CSD sets out the basic technology and associated technical requirements, terminology and standards which are common to all the Market Operator interfaces. The other Interface CSDs describe the additional information relevant to each interface.

1.1.3 This CSD should be read in conjunction with other Interface CSDs that describe the individual interfaces made available to Trading Parties by the Market Operator and as set out in Table 1 below.

Interface CSD	Description
CSD 0400	Common interface technical specifications
CSD 0401	Transactional interface for Trading Parties having a high volume of Data Transactions
CSD 0402	Transactional interface for Trading Parties having a low volume of Data Transactions
CSD 0403	Interface for the provision of Reports from the Market Operator to Trading Parties
CSD 0404	Interface for the provision of non-transactional Data Items from Trading Parties
CSD 0405	Data Query Interface
CSD 0406	Service Management Interface

Table 1: List of Interface CSDs

1.2 Structure of this CSD

1.2.1 The remainder of the CSD is structured as follows:

(a) Section 1: Purpose and scope – this section.

(b) Section 2: Interface standards, describes the standards that all of the Market Operator interfaces must support.

(c) Section 3: Technical infrastructure, describes the technical infrastructure that will support the Market Operator interfaces and the requirements placed on both the Market Operator and connecting Trading Parties.

(d) Section 4: Security Principles, describes the security requirements with which the Market Operator and each Trading Party must comply.

(e) Section 5: Access control and Document Authentication, describes the access controls and Document Authentication measures implemented in terms of Market Operator checks and Trading Party requirements.

(f) Section 6: Interface and processing availability, describes the Market Operator services that will be available during a Business Day and Extended Hours.

(g) Section 7: Transactional processing, describes the way in which Transactions will be submitted by Trading Parties and subsequently processed by the Market Operator Systems. Any additional requirements will be addressed within a technical specification section in each Interface CSD.

(h) Section 8: Processing outcomes and failure responses, describes the common processing outcomes and failure responses that Trading Parties will receive from the Market Operator.

(i) Section 9: Documentation requirements, describes the documents relating to the Market Operator interfaces which the Market Operator must maintain on an on-going basis and will be accessible through the service management interface as described in CSD 0406 (Service Management Interface).

2. Common technical standards

2.1 Overview

2.1.1 This section sets out the common technical standards that the Market Operator and Trading Parties must observe.

2.2 Open Standards

2.2.1 All Market Operator Interfaces will utilise common, secure and robust Open Standards.

2.3 Time

2.3.1 The Market Operator System clock will be synchronised to Coordinated Universal Time (UTC). All references to the point in time at which the Market Operator receives and processes data will be based upon the Market Operator's System clock:

(a) all references to time that are visible to interface users will be in Local Time;

(b) all Reports extracted from the Central Systems will be synchronised to Local Time as set out in Section 6.1.2.

2.4 Security

2.4.1 Trust (Authenticity, Integrity and Non-Repudiation) will be maintained at all times between Trading Parties and the Market Operator Systems and Interfaces.

2.4.2 Confidentiality will be maintained at all times within the Market Operator Systems and Interfaces by which data is submitted and retrieved.

2.5 Data structures

2.5.1 Data structure standards are set out in CSD 0301 (Data Catalogue).

2.6 CSV file format

2.6.1 [Intentionally left blank.]

2.7 Date/time presentation

2.7.1 The following date or time references will conform to the ISO 8601 standard:

(a) date;

(b) combined date and time (where time may be in any of the formats below);

(c) Coordinated Universal Time (UTC); and

(d) local time with no UTC relation information. Where no UTC relation information is provided, the time provided is the local time in the UK time zone (which can be either GMT or BST depending on the time of year).

2.8 Use of interfaces

2.8.1 Depending on their operational requirements, Trading Parties may choose to use both the high volume transactional interface, as described in CSD 0401 (Transactional Interface for Trading Parties having a high volume of Data Transactions), and the low volume transactional interface, as described in CSD 0402 (Transactional interface for Trading Parties having a low volume of Data Transactions), or the low volume transactional interface only depending on their operational requirements.

2.8.2 Where a Trading Party uses a combination of the high and low volume transactional interfaces, it is the Trading Party's responsibility to ensure that all Market Operator responses are retrieved through the interface from which the Data Transactions were originally submitted, as set out in section 7.2.1 of this CSD.

2.8.3 Trading Parties using either the high volume transactional interface, the low volume transactional interface, or a combination of both, will have full access to all other non-transactional interfaces listed in section 1.1.3 of this CSD.

2.9 User names and passwords

2.9.1 For interfaces which require individual user Authentication, each user name will be at least seven (7) characters long.

2.9.2 Interfaces which require individual user authentication will support passwords which must be at least eight (8) characters long and contain at least three (3) of the following four (4) types of characters:

(a) lower case letters (a-z);

(b) upper case letters (A-Z);

(c) numbers (0-9); or

(d) special characters (e.g.: !@£#%&)

2.9.3 User names and passwords must be used in conjunction with a valid Digital Certificate to enable organisation level Authentication. Initial Trading Party Administrator account passwords will be set by the Market Operator and will remain valid for ninety (90) days. If a user logs in with an expired password they will be required to change their password in line with the instructions provided.

2.10 User accounts

2.10.1 Administrators should undertake a regular review of user accounts to identify and disable inactive users, and to identify and update changes to privilege levels. The Market Operator will provide access to a report to assist with such review.

2.10.2 The process for maintaining Trading Party user accounts is set out in Section 4 of CSD 0006 (Trading Party Administration and Notification Processes).

2.11 Interface presentation

2.11.1 Market Operator interfaces that allow human interaction will remain of a clear and consistent structure. Navigation tools provided across these interfaces will be clearly and consistently labelled with meaningful names.

3. Technical infrastructure

3.1 System environments

3.1.1 The Market Operator will make a number of system environments available to Trading Parties for various purposes which may include, but not be limited to:

(a) production (i.e. the live Market Operator Systems);

(b) market scenario testing (Market Entry Assurance or Market Re-assurance);

(c) Trading Party internal system testing to allow Trading Parties to verify changes made within their own systems which connect to the Market Operator System[1];

(d) user training; and/or

(e) user acceptance testing of new Market Operator System software releases as described in CSD 0501 (Change Management).

3.1.2 The technical infrastructure described in this CSD applies to the production Market Operator interfaces.

3.1.3 Depending on the purpose of any non-production environment, the interfaces may or may not be provided in accordance with the security and technical standards set out in this CSD. For example, some non-production environments may not require the full security standards to be deployed. The Market Operator will advise Trading Parties of the specific security and technical standards that apply to non-production environments.

3.2 Interface connection

3.2.1 Each Trading Party must ensure that any transport layer connection to an interface is secured in accordance with the standards described in this CSD and other relevant Interface CSDs.

3.2.2 Trading Parties will be unable to connect to and use interfaces to the Market Operator Systems until they have successfully completed the relevant elements of Market Assurance as set out in CSD 0001 (Market Entry Assurance and Market Re-Assurance).

3.2.3 The Market Operator will notify all Trading Parties in advance of any changes to the connection arrangements to an interface in accordance with CSD 0006 (Trading Party Administration and Notification Processes).

---

1 The Market Operator will put in place procedures to ensure that the availability of such test environments remains on a fair and proportionate basis.

3.2.4 The Market Operator will ensure that all Trading Parties connect to and use the same production version of an interface at any given time. This shall be achieved through change and release management processes set out in CSD 0501 (Change Management).

3.3 Transport mechanism

3.3.1 The interface transport mechanism will conform to TLS over HTTPS. The Trading Party's client application must establish a mutual TLS session with the interface.

3.3.2 Each Trading Party will put in place a boundary protection device that is capable of enforcing the agreed transport layer security controls.

3.3.3 TLS versioning shall be maintained in accordance with good industry practice guidelines.

3.4 Connection details

3.4.1 The Market Operator will ensure that the uniform resource locator (URL) web address of the Market Operator interfaces remains constant.

3.4.2 Each Trading Party is responsible for establishing a connection with the Market Operator and the mechanism by which their systems establish a connection.

4. Security principles

4.1 End to end trust model

4.1.1 Communication between the Market Operator and individual Trading Parties will require different methods of interaction depending on the interface that is being used. In all cases the Market Operator and the connecting Trading Party will ensure that the following security principles are maintained:

(a) Authenticity;

(b) Integrity;

(c) Confidentiality; and

(d) Non-Repudiation.

4.2 Public Key Infrastructure

4.2.1 Digital Certificates will be used to enable Trading Parties and the Market Operator to Authenticate themselves to each other, and to provide Integrity, Confidentiality and Non-Repudiation in Interactions between the Trading Parties and the Market Operator.

4.2.2 Each Trading Party and the Market Operator will establish and maintain its own Public Key Infrastructure capabilities. The Market Operator will not act as the Certificate Authority and therefore third-party Certificate Authority services will need to be procured by the Market Operator and each Trading Party.

4.2.3 All Digital Certificates must comply with the X.509 Public Key Infrastructure certificate standard.

4.2.4 Trading Parties and the Market Operator will establish robust Public Key Infrastructure policies and procedures to ensure that the Market Operator interfaces and all Transactions across them remain secure.

4.2.5 Neither a Trading Party nor the Market Operator will send any Document through the interface described in CSD 0401 (Transactional interface for Trading Parties having a high volume of Data Transactions) where it is aware that the security of any component of that Document has been compromised.

4.2.6 Trading Parties and the Market Operator will ensure that their Digital Certificates do not have an infinite lifetime and are subject to expiration.

4.2.7 Trading Parties and the Market Operator will have appropriate security policies in place which will require Digital Certificates to be Rekeyed every three (3) years as a minimum.

4.2.8 When a Digital Certificate is retired, Trading Parties and the Market Operator will notify each other of the new public element of the public/private key pair in order to ensure that exchanges through the interface do not fail.

4.2.9 Trading Parties and the Market Operator will notify each other of public key changes in accordance with CSD 0006 (Trading Party Administration and Notification Processes) and CSD 0406 (Service Management Interface).

4.2.10 If a Trading Party fails to notify the Market Operator appropriately, access control checks will fail and Documents will be rejected by the Market Operator. Equally if a Trading Party cannot Authenticate a response from the Market Operator as a result of an unnotified key change, it will be rejected.

4.2.11 Trading Parties and the Market Operator will establish robust Key Revocation policies and procedures. Upon detection of a compromise or key withdrawal, the Trading Party or the Market Operator will notify each other of the replacement public key to ensure that access control Verification can continue. This will be undertaken in accordance with CSD 0006 (Trading Party Administration and Notification Processes).

4.2.12 Trading Parties may require multiple valid Digital Certificates where a sub-contractor is managing transactional activities on a Trading Party's behalf, as set out in Section 2.2.7 of CSD 0006 (Trading Party Administration and Notification Processes).

4.3 Digital Signatures

4.3.1 Each Trading Party will apply a valid Digital Signature to all Documents submitted via the interface described in CSD 0401 (Transactional interface for Trading Parties having a high volume of Data Transactions).

4.3.2 The Market Operator will apply a valid Digital Signature to all responses to ensure end-to-end trust is established between individual Trading Parties and the Market Operator. It is the responsibility of Trading Parties to Validate the Market Operator's organisation Digital Signature.

4.4 Anomaly Detection

4.4.1 Anomaly Detection requirements only apply to the high volume transactional interface as set out in CSD 0401 (Transactional Interface for Trading Parties having a high volume of Data Transactions).

4.4.2 The Market Operator will use estimated peak daily volumes provided by each Trading Party to establish an overall anomaly detection threshold for all Transactions being submitted to the Market Operator through the interface.

4.4.3 The process Trading Parties will follow for notifying the Market Operator of anomaly detection threshold values is described in CSD 0006 (Trading Party Administration and Notification Processes).

5. Access control and Document Authentication

5.1 Restrictions on access

5.1.1 All Interactions through the Market Operator interfaces will conform to the following access control principles:

(a) Authentication of every Interaction;

(b) Validation of every Interaction; and

(c) Authorisation of every Interaction.

5.2 Mutual Authentication

5.2.1 Mutual TLS Authentication is used to Authenticate both the client and server using a Digital Certificate in order that both the Trading Party and the Market Operator can be assured of each other's identity.

5.2.2 It is the responsibility of individual Trading Parties to procure, implement and continue to maintain a solution, which enables them fully to comply with Mutual TLS Authentication requirements.

5.3 Document Authentication

5.3.1 The Market Operator will authenticate all Documents received through the interface set out in CSD 0401 (Transactional interface for Trading Parties having a high volume of Data Transactions) by validating the Trading Party's organisation Digital Signature and Trading Party unique identifier. If the Market Operator identifies that the organisation Digital Signature is invalid or does not correspond to the Trading Party unique identifier held by the Market Operator, the Authentication process will fail.

5.3.2 If Authentication fails, the Market Operator will stop all processing of that Document at that point and no further checks will be performed. In this scenario, the Market Operator will generate a Processing Status Code and Processing Return Code(s) informing the initiating Trading Party of the processing status and the reason for failure. Processing failure responses are described in section 8.2 of this CSD.

6. Interface availability

6.1 Interface and processing availability

6.1.1 Details of Market Operator interfaces and processing availability are set out in appendix A of this CSD.

6.1.2 The Market Operator System clock is the basis upon which the date and time of submission is calculated i.e. the date and time of the submission is the date and time that a Trading Party's submission is received completely and not the date and time that the Trading Party initiated a submission.

(a) All Reports provided by the Market Operator will be in Local Time.

(b) Any references to time that are visible to interface users through an interface will be presented in Local Time.

6.2 Interface support arrangements

6.2.1 The Market Operator will provide the following support to Trading Parties using the Market Operator interfaces:

(a) a service desk which can be contacted by telephone during the Business Day and Extended Hours.

(b) a service management interface as described in CSD 0406 (Service Management Interface) which will be actively monitored during the Business Day and Extended Hours.

6.3 Planned Outages

6.3.1 The Market Operator will notify all Trading Parties of any planned outages, by email or telephone notification to the named Trading Party contacts. The communication will include details of the maintenance activities that are to be undertaken and confirmation of any requirements on Trading Parties to carry out actions prior to and/or upon restoration of the Markey Operator interfaces.

6.3.2 The Market Operator will use reasonable endeavours to limit Planned Outages to a period outside Extended Hours. Any Planned Outages as a result of changes to Market Operator Systems will be agreed as set out in the release management process described in CSD 0501 (Change Management).

6.3.3 Planned Outage notifications will be in accordance with CSD 0006 (Trading Party Administration and Notification Processes).

6.3.4 If the interface is otherwise unavailable during Extended Hours, this should be regarded as an incident as described in CSD 0007 (Business Continuity Management).

7. Transactional processing

7.1 Transaction responses

7.1.1 All Documents submitted to the Market Operator will receive a synchronous response to confirm that the Document has been received and passed initial access control checks. The synchronous response will be provided by return during the hours of interface availability as shown in the table in Appendix A of this CSD.

7.1.2 A subsequent asynchronous response will be issued by the Market Operator once all data processing validation has been completed for each Transaction contained within a Document. The asynchronous response will be provided in accordance with the timeframes associated with each Transaction as defined in the relevant CSDs.

7.2 Retrieval of Market Operator responses

7.2.1 It is the responsibility of Trading Parties to retrieve Market Operator responses through the interface that the initial Transaction was submitted.

7.2.2 For each Transaction submitted, Market Operator response will contain the initiating Data Transaction reference number, a Processing Status Code, and, should the content of a Data Transaction fail to be processed, a Processing Return Code(s).

7.2.3 Where a processing failure has occurred at a Document level, the Processing Return Code returned by the Market Operator will be directly related to the Document that has failed. Data Transactions that are contained within the failed Document will not be processed.

7.3 Retrieval of unsolicited Market Operator notifications

7.3.1 The Market Operator may also issue unsolicited notifications to Trading Parties (i.e. those which are not in response to a corresponding Transaction from that Trading Party). All such notifications must also be collected and processed by Trading Parties, and upon collection Trading Parties will confirm to the Market Operator that these notifications have been collected for processing.

7.4 Transaction completion

7.4.1 Both the Trading Parties and the Market Operator will monitor interactions to ensure that acknowledgements are always received. This principle should ensure that there are no incomplete Interactions. Should any incomplete Interactions be identified, these will be investigated and an incident will be raised. The affected Trading Party should notify the Market Operator of a

suspected incident and similarly the Market Operator should notify the relevant Trading Party.

7.4.2 Trading Parties will ensure that:

(a) initial acknowledgements in the form of synchronous responses are received and correspond to all initiating Document submissions; and

(b) subsequent acknowledgements in the form of asynchronous responses are received and correspond to the initiating Transactions submitted.

7.4.3 The use of synchronous and asynchronous messaging requires that:

(a) for all submissions retrieved from the Market Operator, whether in response to an initiating submission or unsolicited notification, Trading Parties will ensure that they are positively acknowledged with a receipt which is returned to the Market Operator through the interface; and

(b) for all submissions from the Market Operator to a Trading Party, the Market Operator will ensure that it receives a positive confirmation of collection from the Trading Party. This confirmation of receipt will be stored by the Market Operator System to ensure a chronological processing history is recorded and any outstanding actions (e.g. a Trading Party failing to process an error response and subsequently attempting to resubmit an unresolved Transaction) can be identified.

7.5 Data retention

7.5.1 For the avoidance of doubt all Transactions, Authorisations and associated logs which are submitted through the appropriate Market Operator interfaces and impact settlement will be retained by Trading Parties and the Market Operator for a rolling period of seven (7) years.

7.5.2 All interface logs which have no relationship to settlement and the requirements set out in 7.5.1 above will be retained by the Market Operator for a rolling period of twenty-four (24) months.

7.6 Unique reference numbering

7.6.1 Each Trading Party will ensure that a unique Data Transaction reference Number, is applied to every Document and every Transaction prior to submitting to the Market Operator. The Data Transaction Reference Number is unique across all interfaces.

7.6.2 Consideration of transactional interface failures is set out in Section 8.5 of this CSD.

7.7 Sequencing

7.7.1 CSD 0401 (Transactional Interface for Trading Parties having a high volume of Data Transactions) supports the processing of Data Transactions in sequence based on the unique numbering of Documents and Data Transactions.

7.7.2 Other Market Operator interfaces used for either transactional or non-transactional data submission will not support sequencing. It will be the responsibility of the initiating Trading Party to ensure Data Transactions or other data sets are submitted to the Market Operator in the correct order.

7.7.3 Where a Trading Party submits Data Transactions through both the high volume and low volume transactional interfaces, it is the Trading Party's responsibility to ensure that Data Transactions are submitted to the Market Operator in the correct sequences.

7.7.4 Equally, it will be the responsibility of each Trading Party to process all responses from the Market Operator applying the same principles in order to ensure the Central Systems and the Trading Party's systems remain in alignment.

8. Processing outcomes and failure responses

8.1 Error handling scenarios

8.1.1 The following table sets out possible high-level error scenarios and possible outcomes.

Error	Outcome
World-wide-web is unavailable	This is outside the control of either the Market Operator or Trading Parties wishing to use the interface. In such circumstances, the Market Operator and Trading Parties should establish that this is a common problem notified via the established incident management processes and procedures. In such circumstances the Market Operator, will co-ordinate 'market start-up'.
Market Operator Systems / Interface is unavailable	If the Market Operator System/interface is persistently unavailable, the connecting Trading Party should raise an incident.
Access control failure or invalid Transaction - non-conformance with CSD 0301 (Data Catalogue)	Response as described in the remainder of this Section 8.
Market Operator is unable to respond to Trading Party	If the outage is determined to be such that the Market Operator is likely to fail to meet its performance standards, the Market Operator will contact affected Trading Parties Contract Managers out of band.
No response received from Trading Party confirming collection of synchronous / asynchronous responses	The Market Operator shall record no response and after two (2) Business Days contact the Trading Party's Contract Manager by telephone having first checked whether an incident has been raised.

Error	Outcome
Delay in response from the Market Operator	If a Transaction has been submitted, outside Extended Hours, it will be registered as being submitted at the beginning of the next Business Day and a synchronous response returned. The Market Operator will then have a further Business Day to respond with an asynchronous response. If no response is received within this timeframe, the Trading Party should raise a service management incident.

Table 2: Possible interface error scenarios

8.2 Error processing – transactional interface access control failure or invalid Transaction

8.2.1 Where a Transactional interface access control failure occurs, or a Trading Party submits an invalid Document or Transaction, a Processing Status Code will be generated by the Market Operator for subsequent retrieval and processing by the Trading Party. Each error response from the Market Operator will contain:

(a) the Trading Party's unique identifier;

(b) the unique Document reference number;

(c) the unique Transaction reference number of the affected Transaction (if only a single Transaction is affected);

(d) a failure Processing Return Code; and

(e) a date and time stamp.

8.2.2 Where the Market Operator identifies issues with an interface; or where issues are brought to the Market Operator's attention, the Market Operator will notify all Trading Parties in accordance with CSD 0006 (Trading Party Administration and Notification Processes) and update the service management dashboard described in CSD 0406 (Service Management Interface).

8.2.3 Trading Parties will collect and process all processing responses generated by the Market Operator and make all reasonable steps to rectify the error if it is deemed to be an error within the Trading Party's own system(s) or processes.

8.2.4 Trading Parties will ensure that where any Transactions need to be resubmitted to the Market Operator the unique reference number has been incremented to avoid further Transaction processing failure as set out in Section 9.4.1 Table 2.

8.2.5 Under exceptional circumstances Trading Parties may be required to resubmit Transactions using the same unique reference number, however this would

need to be agreed with the Market Operator. Such scenarios are set out in Section 8.5 of this CSD and CSD 0007 (Business Continuity Management).

8.3 User interface specific error handling

8.3.1 Where an interface allows for human interaction, user errors will be communicated by displaying meaningful error messages on the user's screen.

8.4 Market Operator interface access control or processing failures

8.4.1 Table 2 details the responses provided to Trading Parties following interface access control or processing failure:

Process	Processing activity	Failure outcomes	Mechanism	Processing Return Code
Access control checks	Has the Interaction been initiated via a trusted connection (i.e. has a valid Trading Party certificate been used for mutual TLS Authentication)?	No = Fail	Dependent on technology deployed	Dependent on technology deployed
	Is the initiating Trading Party as determined by the Digital certificate authorised to use this interface?	No = Fail	Dependent on technology deployed	Dependent on technology deployed
Document Processing Validation	Is the Document wrapper consistent with the specified format (i.e. can Trading Party ID; time and date Stamp; unique Document Reference Number be identified)?	No = Fail	Dependent on technology deployed	Dependent on technology deployed
	Is the Trading Party ID valid?	No=Fail	Synchronous response	AA

Process	Processing activity	Failure outcomes	Mechanism	Processing Return Code
	Does the Document pass Authentication and Integrity checks?	No=Fail	Synchronous response	MC
	Is the Document valid and complete?	No=Fail	Synchronous response	MD
	Has the unique Document reference number been incremented (an increment of 1 from the previous submission)?	No=Fail	Synchronous response	ME
Transaction processing Validation	Has the unique Transaction reference number been incremented (an increment of 1 (one) from the previous submission)?	No=Fail	Asynchronous response	MF
	Are all the mandatory fields populated?	No=Fail	Asynchronous response	MG
	Are there any data formatting exceptions?	Yes=Fail	Asynchronous response	MH
System processing error	Market Operator Systems performs access control checks	Unavailable to perform necessary access control checks or do not complete processing	Dependent on technology deployed	Dependent on the technology deployed
	Market Operator Systems perform Document / Data Set processing	Unavailable to perform necessary validation	Synchronous response	MI

Process	Processing activity	Failure outcomes	Mechanism	Processing Return Code
	validation	checks or do not complete processing		
	Market Operator Systems perform Transaction processing validation	Unavailable to perform necessary validation checks or do not complete processing	Asynchronous response	MJ

Table 3: Market Operator interfaces error response codes

8.5 Recovery from transactional interface failure

8.5.1 Upon resolution of a Market Operator transactional interface failure, all outstanding acknowledgements and/or error codes will be processed in chronological order, i.e. in the order in which they were received by the Market Operator.

8.5.2 This may result in a separate process being agreed between the Market Operator and each affected Trading Party should there be a large backlog of Transactions to clear.

8.5.3 If a Trading Party needs to re-submit Transactions following a processing failure, they must first ensure that the relevant Transaction has not already been received and processed in any way by the Market Operator. Any attempts to resubmit a Transaction which has already been processed by the Market Operator will fail.

8.5.4 Under certain circumstances following failure, the Market Operator may request Trading Parties to re-submit previously submitted Transactions without changing the unique reference number that was allocated to a Transaction. Under such circumstances, Trading Parties must fully comply with the Market Operator's instructions.

8.5.5 Recovery from transactional interface failure will be in accordance with CSD 0007 (Business Continuity Management).

8.6 Recovery from Trading Party failure to transact

8.6.1 Where a Trading Party is unable to transact for whatever reason for a period of time, it is the affected Trading Party's responsibility to notify the Market Operator and agree a specific Transaction Recovery Plan, as described in CSD 0007

(Business Continuity Management), should it need to submit a higher volume of transactions than normal upon recovery.

8.6.2 It is the Market Operator's responsibility to manage the Transaction Recovery Plan, as described in CSD 0007 (Business Continuity Management), and communicate with affected Trading Parties on a regular basis to ensure the use of the affected interface can return to normal operation as quickly as possible.

8.6.3 Recovery from Trading Party failure to normal operations will be in accordance with CSD 0007 (Business Continuity Management).

9. Documentation

9.1.1 The Market Operator is responsible for ensuring that the documentation of all Market Operator interfaces is appropriately maintained and easily accessible and made available to Trading Parties. Any change to the technical and other information set out in the CSDs will follow the change process as set out in CSD 0501 (Change Management).

9.1.2 Documents that the Market Operator will be responsible for maintaining include:

(a) Interface CSD functional specifications;

(b) Interface CSD design specifications;

(c) Interface CSD implementation/integration requirements; and

(d) Interface user training guides.

9.1.3 All documents will be maintained by the Market Operator in either Microsoft Word or PDF format.

A. Market Operator interface and processing availability

The following table should be read in conjunction with section 7.1 of this CSD.

Interface	Availability					
	Business Day			Extended Hours		
	Supported Trading Party activities	**Market Operator synchronous response**	**Market Operator asynchronous response**	**Supported Trading Party activities**	**Market Operator synchronous response**	**Market Operator asynchronous response**
CSD 0401(Transactional Interface for Trading Parties having a high volume of Data Transactions)	Transaction submissions	Yes	Yes	Transaction submissions	Yes	Yes (may be received on the next Business Day)
CSD 0402 (Transactional Interface for Trading Parties having a low volume of Data Transactions)	Transaction submissions	Yes	Yes	Transaction submissions	Yes	Yes (may be received on the next Business Day)
CSD 0403 (Interface for the provision of Reports from the Market Operator	Report retrieval	N/A	N/A	Report retrieval	N/A	N/A

Interface	Availability					
	Business Day			Extended Hours		
	Supported Trading Party activities	Market Operator synchronous response	Market Operator asynchronous response	Supported Trading Party activities	Market Operator synchronous response	Market Operator asynchronous response
to Trading Parties)						
CSD 0404 (Interface for the provision of non-transactional Data Items from Trading Parties)	Data Item construct	N/A	N/A		N/A	N/A
	Data Item and admin submission	Yes	Yes	Transaction submissions	Yes	Yes (may be received on the next Business Day)
	Data Item authorisation	Yes	Yes	Yes	Yes	Yes
CSD 0405 (Data Query Interface)	Data query construct and execution	N/A	N/A	Data query construct and execution	N/A	N/A

Interface	Availability					
	Business Day			Extended Hours		
	Supported Trading Party activities	Market Operator synchronous response	Market Operator asynchronous response	Supported Trading Party activities	Market Operator synchronous response	Market Operator asynchronous response
CSD 0406 (Service Management Interface)	Queries Service management requests Service management incidents Admin	N/A	N/A	Queries Service management requests Service management incidents Admin	N/A	N/A

Table 4: Market Operator interface and processing availability