

**Code Subsidiary Document**

**No. 0406:**

**Service Management Interface**

September 2015

## Table of Contents

1.	Introduction.....	4
1.1	Purpose and scope .....	4
1.2	Structure of this CSD .....	4
2.	Description of the interface.....	5
2.1	Overview.....	5
2.2	User authorisation.....	7
2.3	Raising service management incidents .....	7
2.4	Updating service management incidents.....	9
2.5	Viewing service management incidents .....	9
2.6	Closing service management incidents.....	10
2.7	Service desk calls .....	10
2.8	Service management dashboard .....	10
2.9	Market Operator service alerts.....	11
2.10	Market Operator service reports.....	11
2.11	Report archiving.....	12
2.12	Certificate management.....	12
2.13	Anomaly detection thresholds .....	12
2.14	Retrospective Amendment requests .....	12
2.15	Market Operator documentation.....	13
3.	Technical specification and standards .....	14
3.1	Common requirements.....	14
3.2	Service Management incident response times .....	14
3.3	Error handling .....	14

## 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;
- (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; and
- (c) capitalised terms relating to definitions set out in CSD 0400 (Common interface technical specifications) shall also apply.

# 1. Introduction

## 1.1 Purpose and scope

1.1.1 This CSD describes the functionality of the service management interface, in order for Trading Parties to be able to understand the services that are provided by the Market Operator. The CSD also sets out the key requirements for the Market Operator and Trading Parties wishing to use the interface.

1.1.2 Common technical specifications and standards are described in CSD 0400 (Common interface technical specifications).

1.1.3 This CSD should be read in conjunction with:

- (a) CSD 0006 (Trading Party Administration and Notification Processes);
- (b) CSD 0400 (Common interface technical specifications); and
- (c) CSD 0404 (Interface for the provision of non-transactional Data Items from Trading Parties).

## 1.2 Structure of this CSD

1.2.1 This CSD is structured as follows:

- (a) Section 1: Purpose and scope – this section;
- (b) Section 2: Description of the interface – describes the interface in terms of the functions available to Trading Parties; and
- (c) Section 3: Technical specification and standards – describes the technical specifications specifically for this interface.

## 2. Description of the interface

### 2.1 Overview

2.1.1 The interface will provide Trading Parties with access to information and data across the Market Operator's operations. It will be the first point of contact for general Trading Party queries and raising service requests and management incidents.

2.1.2 The interface will contribute to the reduction in calls that need to be made to the Market Operator's service desk but will not in any way remove the ability for Trading Parties to telephone the Market Operator service desk during a Business Day or Extended Hours. The interface will complement and enhance the services and the response times provided to Trading Parties by the Market Operator.

2.1.3 The interface is interactive allowing users to:

- (a) raise service management incidents;
- (b) update and close service management incidents;
- (c) view service management incidents;
- (d) view Market Operator service alerts;
- (e) view service audit trails;
- (f) request operational reports;
- (g) request access to archived reports;
- (h) submit new Trading Party organisation Digital Certificates and retrieve new Market Operator organisation Digital Certificates;
- (i) submit and update anomaly detection thresholds; and

- (j) access to documents that the Market Operator is required to maintain - as specified in CSD 0400 (Common interface technical specifications) and CSD 0001 (Market Entry Assurance and Market Re-assurance).

2.1.4 Both the Market Operator and Trading Parties service management interface users will be subject to user authorisation and user privilege controls specified in CSD 0400 (Common interface technical specifications).

2.1.5 It is the responsibility of each Trading Party and Market Operator to appoint an Administrator to manage individual user accounts and associated privileges.

2.1.6 The interface will include Role Based Access Control which will enable Trading Parties and the Market Operator to allocate appropriate privileges to individual users based on their role within their organisation. Trading Parties will appoint an Administrator to manage all user access within their organisation as set out in CSD 0006 (Trading Party Administration and Notification Processes).

2.1.7 Cryptographic Protections include Mutual Authentication. The Market Operator will perform a series of access control checks including Authentication of a Trading Party's organisation Digital Certificate to ensure that all Sessions that are established through the Interface are secure.

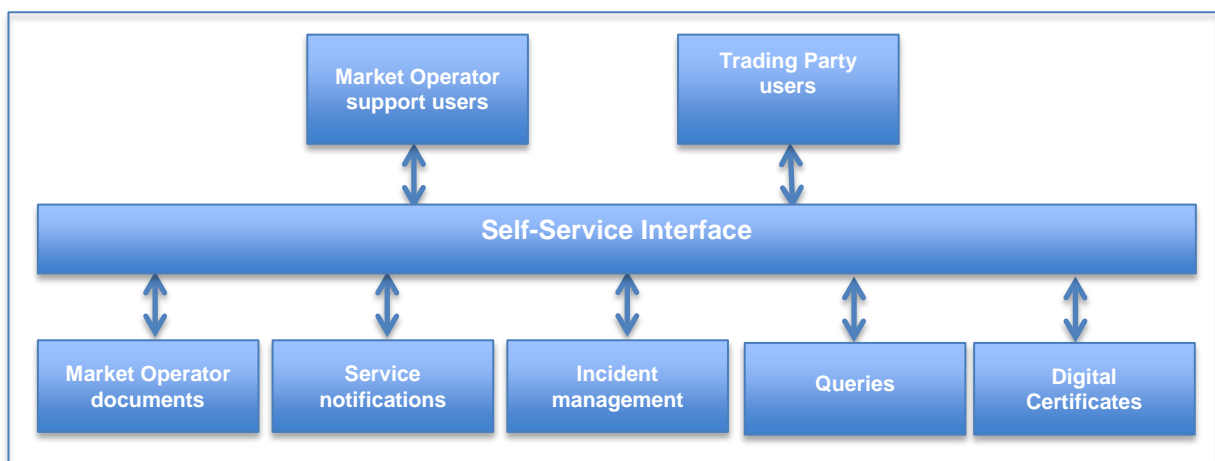


Figure 1: Basic service management interface architecture

## 2.2 User authorisation

- 2.2.1 A user's access to different functions within the interface will be based on their individual user role, related privileges and Trading Party identifier.
- 2.2.2 Trading Party users will be able to view and update information related to their own activity on the interface.
- 2.2.3 A Trading Party Administrator will be able to view and update all activities undertaken on the interface by users within their organisation. For example, updating of activities could include changing or updating details relating to a service management incident that has been raised.
- 2.2.4 Market Operator users will be able to view and update information related to any Trading Party using the interface.

## 2.3 Raising service management incidents

- 2.3.1 The interface will allow Trading Party users with the correct privileges to:
- (a) log all details of a service management incident against a unique reference number which will be automatically generated by the interface;
  - (b) include a related unique Transaction reference / Session reference at the point at which the incident occurred;
  - (c) categorise a service management incident in terms of:
    - (i) the business impact on their Trading Party's operations; and
    - (ii) the resolution priority required based on the impact to their Trading Party's operations and possibly other service management incidents / operational constraints that are being experienced at that time;
  - (d) provide a description of the service issue being experienced and append supporting evidence (if appropriate); and

(e) provide contact details such as telephone number and email address.

2.3.2 At the point at which a user submits a service management incident the interface will:

(a) present an on-screen message to the user confirming that the service management incident has been successfully submitted;

(b) reconfirm the unique reference that the interface has generated; and

(c) automatically generate and send an email confirmation to the Trading Party user who raised the incident containing:

(i) confirmation that a service management incident has been successfully submitted;

(ii) the unique reference number that has been allocated; and

(iii) a summary of the details submitted.

2.3.3 The interface will allow a user to add and remove service management incidents under a single service management incident reference:

(a) where multiple service management issues have been identified by a Trading Party relating to a common issue; or

(b) where additional service management issues have been identified which relate to a service management incident that has already been raised with the Market Operator through the interface or the service desk.

2.3.4 The resolution priority of an existing service management incident will not be affected where a user appends or subsequently removes any additional incidents which have been grouped under a single common issue.

2.3.5 The interface will not limit the number of service management incidents that can be raised under a single reference number; however a significant number would suggest that an incident may have occurred. The Market Operator will closely



monitor the service incidents raised by Trading Parties and if necessary invoke its Business Continuity Plan as set out in CSD 0007 (Business Continuity Management) if it has not already done so.

## **2.4 Updating service management incidents**

2.4.1 The interface will allow users to update open service management incidents that they or other users within their Trading Party have submitted to the Market Operator.

2.4.2 Users will be able to select, edit and resubmit in real-time all elements of the service management incident details previously submitted to the Market Operator using the interface screens. This may include:

- (a) the provision of more detailed information describing the problem and the impact that it is having on their Trading Party's operations; or
- (b) the reclassification of the impact and priority (in the context of their Trading Party).

2.4.3 The Market Operator will refresh the status of all service management incidents that have been submitted through the interface within one (1) hour during a Business Day or Extended Hours.

## **2.5 Viewing service management incidents**

2.5.1 The interface screens will allow users to view and filter all service management incidents relating to their organisation in a logical format including:

- (a) all service management incidents (and groupings of service incidents) relating to their Trading Party that are currently active; and
- (b) all service management incidents relating to their Trading Party that have been closed within the last three (3) months.

## **2.6 Closing service management incidents**

- 2.6.1 Market Operator service desk users and Trading Party users will select a select reason code before closing down a service management incident.
- 2.6.2 Where service management incidents have been grouped, all service management incidents raised under a single service management incident number must be closed down before the overall incident can be closed.
- 2.6.3 The interface will allow previously closed service management incidents to be re-opened during a period of ten (10) Business Days after closure.
  - (a) The interface will display the initial closure date and the date at which the service management incident was reopened.
  - (b) Users will be limited to editing the impact and priority.

## **2.7 Service desk calls**

- 2.7.1 The interface will allow a Market Operator Administrator to generate a service management incident on behalf of a Trading Party as a result of a call to the service desk.
- 2.7.2 Service management incidents can also be closed by a Market Operator Administrator with a Trading Party's approval.

## **2.8 Service management dashboard**

- 2.8.1 The interface will include a service management dashboard which will provide a near-real time overview of the Market Operator Systems and general service availability.
- 2.8.2 The service management dashboard will also be used by the Market Operator to provide updates to Trading Parties during a business continuity invocation as described in CSD 0007 (Business Continuity Management).

## **2.9 Market Operator service alerts**

2.9.1 The Market Operator will publish service management alerts through the interface as described in CSD 0006 (Trading Party Administration and Notification Processes).

2.9.2 Service management notifications will be managed in conjunction with the service management dashboard described in section 2.8 of this CSD.

## **2.10 Market Operator service reports**

2.10.1 Once compiled, the Market Operator will email the requested reports to the requesting Trading Party Administrator.

2.10.2 The interface will allow Trading Party Administrators to query Market Operator service audit trail data held within Market Operator Systems.

(a) Data supporting the service audit trails will provide a record of all service activity for a minimum period of three (3) months up to the end of the previous Business Day.

(b) User access will be limited to the Interactions / Sessions relating to their Trading Party.

(c) The interface will support configurable search parameters.

(d) This function shall not be viewed as a substitute to the requirement for Trading Parties to retrieve and process all synchronous and asynchronous Market Operator responses through a transactional or non-transactional interface.

2.10.3 In addition to 2.10.3(a) above, the Market Operator will ensure that service statistics are held for a minimum of twenty-four (24) months in accordance with the data retention requirements set out in section 7.5 of CSD 0400 (Common interface technical specifications).

## **2.11 Report archiving**

2.11.1 As set out in CSD 0403 (Interface for the provision of Reports from the Market Operator), Reports will remain accessible to Trading Parties for a minimum period of three (3) months.

## **2.12 Certificate management**

2.12.1 The interface will allow Trading Party Administrators to provide the Market Operator with new organisation Digital Certificates as described in CSD 0006 (Trading party Administration and Notification Processes).

2.12.2 The interface will also allow Trading Party Administrators to retrieve new Market Operator organisation Digital Certificates made available by the Market Operator.

## **2.13 Anomaly detection thresholds**

2.13.1 The interface will allow Trading Parties to notify the Market Operator of initial and revised anomaly detection thresholds following the process set out in CSD 0006 (Trading Party Administration and Notification Processes).

2.13.2 The notification of anomaly detection thresholds only applies to Trading Parties submitting high volumes of Data Transactions through the interface described in CSD 0401 (Transactional interface for Trading Parties having a high volume of Data Transactions).

## **2.14 Retrospective Amendment requests**

2.14.1 The interface will allow Trading Party users to submit Retrospective Amendment requests in order to amend Data Items as set out in CSD 0105 (Error Rectification and Retrospective Amendments).

2.14.2 Once a Retrospective Amendment request has been processed and confirmed by the Market Operator, Trading Parties will be able to access the requested Data Items through the interface described in CSD 0404 (Interface for the provision of non-transactional Data Items from Trading Parties) following the process as described in section 2.9 of the same CSD.

## **2.15 Market Operator documentation**

- 2.15.1 The interface will allow Trading Party users with the correct privileges to access documentation relating to the Interface CSDs as set out in section 9 of CSD 0400 (Common interface technical specifications) and documentation relating to CSD 0001 (Market Entry Assurance and Market Re-assurance).

## **3. Technical specification and standards**

### **3.1 Common requirements**

3.1.1 Trading Parties must configure access and ensure correct use of the interface in accordance with the requirements set out in CSD 0400 (Common interface technical specifications).

### **3.2 Service Management incident response times**

3.2.1 The Market Operator will establish an incident management policy which will include:

- (a) categorisation of the types of potential incident;
- (b) an initial response to all service management incidents through the interface within two (2) hours during a Business Day or Extended Hours;
- (c) a target resolution time for each incident category identified; and
- (d) refresh of an incident status on the service management dashboard at least every one (1) hour during a Business Day or Extended Hours.

3.2.2 The Market Operator will present the policy to the Panel.

### **3.3 Error handling**

3.3.1 Common error handling requirements are described in CSD 0400 (Common interface technical specifications).

3.3.2 The following table sets out possible error scenarios and outcomes specific to this interface.

Error	Outcome
Interface user identifier / password invalid	Interface user is notified that their user identification and/or password are invalid, and is advised to contact their Administrator in the first instance before raising a service management incident as set out in CSD 0406 (Service Management Interface).

Table 1: Interface specific error scenarios