RETAIL
ENERGY
CODE

Secure Data Exchange Service Definition

Contents

Part A - General

Part B - Secure Data Exchange Portal (SDEP)

Part C - Crossed Meter Resolution Portal (CMRP)

Part D - New Metering Point Requests

Secure Data Exchange Service (SDES)

Service Definition

Version: 2.0 Effective Date: 1 September 2021

Change History

Version Number	Implementation Date	Reason for Change
0.1	N/A	Draft version for December 2020 consultation
2.0	September 2021	Final version for RCC implementation

Part A: General

1 Introduction

1.1. The Secure Data Exchange Service (SDES) consists of several web-based services that enable Parties to securely exchange data. These services comprise:

(a) the Secure Data Exchange Portal (SDEP) which is described further in Section B;

(b) the Crossed Meter Resolution Portal (CMRP) which is described further in Section C; and

(c) New Metering Point Requests which are described further in Section D.

1.2. Generic provisions relating to the overall Secure Data Exchange Service are included in this Part A, with specific information regarding users and service functionality included within Parts B to D.

1.3. This Service Definition should be read in conjunction with the Secure Data Exchange Schedule, which sets out the process for Market Participants to become SDES Users.

2 System Access and User Management

2.1. In this Service Definition, the term 'SDES User' refers to the organisation granted access to the service in accordance with the Secure Data Exchange Schedule; and the term 'Authorised Person' refers to the individual representative of an SDES User accessing the service.

2.2. Each Authorised Person shall have an individual user account, which shall only be accessed via entry of the correct username and password. Where the SDES User is also an Electricity Enquiry Service Users, they shall have a single username and password that allows access to both services.

2.3. On creation of a new user account, the SDES shall generate a single use randomly generated password to the user's email account as stored on the SDES, and the user shall be required to change this password when they first log on. An Authorised Person can only be granted access to the SDES for one SDES User.

2.4. The SDES Provider shall create for each SDES User, a single Master Admin User (MAU). Where an SDES User is also an Electricity Enquiry Service User, the MAU for the EES will also be the MAU for the SDES. The MAU must be a named individual with an identifiable email address which will be their username.

2.5. The MAU is responsible for maintaining data for individual Authorised Persons and can assign and remove Authorised Persons from an SDEP business process and use case as follows:

(a) a single Authorised Person may be assigned to multiple use cases; and

(b) at least one Authorised Person is assigned to each use case.

2.6. An SDES User's MAU can manage and create credentials for individual Authorised Persons using the 'Maintain Assigned Users List' function and will also have the rights to assign privileges to other individual Authorised Persons in their organisation.

2.7. Inactive accounts will be deleted after 90 days, as follows:

(a) deletion may include all Authorised Persons assigned in relation to an SDES User, or business process / use case for the SDES;

(b) an email notification is sent to the individual Authorised Person who is about to be deleted every day for 7 days before the deletion, reminding them to sign in; and

(c) where the Authorised Person who is about to be deleted is the only user assigned to the business process / use case in the SDEP, the MAU will be assigned as a default point of contact for that level.

2.8. Where an Authorised Person is being deleted, an automated email is sent to the MAU 7 days before the deletion date providing details of the business process / use case and the Authorised Person who will be deleted. This email highlights whether the 'last user' assigned to an escalation level is going to be deleted. The email is sent to the MAU on a daily basis over the 7 days until either another Authorised Person is assigned to the escalation level or the Authorised Person signs on to the SDES to prevent the automatic deletion.

3 Availability

3.1. The SDES shall be available 24 hours a day, 7 days a week, except during scheduled maintenance periods and unplanned outages.

3.2. The SDES shall have 99% availability between 08:00 and 18:00 hours on Working

Days over each calendar month.

3.3. Where reasonably possible, the SDES Provider shall notify the Code Manager with a minimum 10 days' notice of scheduled maintenance. The Code Manager will notify SDES Users as soon as reasonably practicable.

3.4. Any unplanned suspension in the availability of the SDES shall be notified by the SDES Provider to the Code Manager as soon as is practicable. Such notification shall also include an estimate for the restoration of services, with further confirmation provided when services are restored.

4 User Support

4.1. The SDES Provider shall provide a service desk to provide technical support. This service desk will manage all user service contacts such as reporting issues and queries.

4.2. The SDES shall ensure the SDES service desk is available:

Item	**Requirement**
Standard Operational Hours	08:00 to 18.00 on Working Days.
Out of Hours Critical Support	For supporting critical severity issues outside of standard operating hours.

4.3. Issues will be categorised as follows:

Severity	Description	Target Response Time	Target Resolution Time
Critical	The service is not usable. Primary functions do not work and there is no known workaround. Business is impacted severely. All critical severity issues must be reported by telephone.	1 hour (95%) 2 hours (100%)	4 hours (95%) 1 WD (100%)

Severity	Description	Target Response Time	Target Resolution Time
Major	The software is still functional, but at least one primary function has been impacted and a workaround, if available, is severely time consuming.	2 hours (95%) 3 hours (100%)	1 WD (95%) 2 WDs (100%)
Minor	Inconvenience increased. Functionality not highly affected and workaround is an acceptable alternative	4 hours (95%) 8 hours (100%)	3 WDs (95%) 5 WDs (100%) or fix in next software release
Cosmetic	Intended functionality not impacted Including fonts, colours, labels, etc and involving workarounds / patches that can be held in abeyance pending a combined release.	4 hours (95%) 8 hours (100%)	Fix in next software release

5 Service Levels

5.1. None currently defined.

6 Maximum Design Volumes

6.1. The SDES shall allow for 16,000 concurrent Authorised Persons without detrimental effect to performance; this volume of concurrent users includes both EES Users and SDES Users. The SDES Provider shall monitor its available capacity and ability to accommodate end user demand for the service.

6.2. Any increase in overall demand, peak demand or storage requirements that may impact available system capacity shall be notified to the Code Manager as soon as possible, with details of any preventative measures and/or system enhancements that may be required.

7 Business Continuity/Disaster Recovery

7.1. Penetration testing of the SDES infrastructure shall be undertaken at least once in each 12 month period, and a report provided to the Code Manager regarding the outcomes of this test, to include any observations or findings, and recommendations for any required remedial actions.

7.2. A test of the business continuity plan for the SDES shall be undertaken at least once in every 12-month period, and a report provided to the Code Manager regarding the outcomes of this test, to include any observations or findings, and recommendations for any required remedial actions.

8 Security

8.1. The SDEP can only be accessed where a valid username and password is provided. Access is via a secure HTTPS connection. Application between the client and the application server shall be encrypted.

8.2. Files being uploaded to and downloaded from the SDEP shall be secure in transit. Secure transfer of all communications between the server and client is managed through a TLS v1.2 connection protocol, providing robust encryption for data in transit across the public internet.

8.3. Once a file has been received, it shall be stored through Azure Blob Storage and is encrypted using 256-bit Advanced Encryption Standard. The file shall be encrypted at rest on the disk as well as any backup of the database that is taken.

8.4. Following an upload, attachments will only be visible and able to be downloaded once they have passed a virus check. The virus check shall be run on a regular schedule, and:

(a) while awaiting virus check, the name of the file will be available and it will be marked as ‘pending’ on screen;

(b) if a virus is detected, the marker will be updated to ‘failed’; and

(c) if it passes the virus check, the attachment will be available for download.

Part B: Secure Data Exchange Portal (SDEP)

9 Service Description

9.1. The Secure Data Exchange Portal (SDEP) is a web-based service that enables Parties to securely exchange data.

9.2. The SDEP shall provide, as a minimum:

(a) a secure user interface accessible to relevant SDES Users via the public internet;

(b) an application layer, being the infrastructure that will support interactions between parties via secure means;

(c) a platform to securely exchange data between SDES Users in both a structured and unstructured format, including the functionality to attach and download supporting documentation;

(d) robust security protocols, compliant with Data Protection Legislation, and which are designed to ensure the data exchanged between SDES Users is not accessible to persons other than those intended by the sending SDES User;

(e) robust user access controls, allowing a SDES User to provide access to the SDEP to duly authorised individuals on their behalf;

(f) production of reports detailed in Paragraph 12; and

(g) secure processing and storage of relevant data in accordance with the security requirements in Paragraph 8.

10 Service Users

10.1. The SDEP shall be accessible to:

(a) Energy Suppliers;

(b) Distribution Network Operators; and

(c) the Code Manager.

10.2. Energy Suppliers and Distribution Network Operators need to become and (remain) Qualified as SDES Users.

11 Service Functionality

11.1. The SDEP enables SDES Users to perform the following functions:

(a) View communication list – an Authorised Person who is assigned to at least one business process, can view the communication list screen for those business processes. The list screen shows a list of all communications relating to the processes the Authorised Person is assigned to. The information displayed in the list is subject, attachment names, created/last message date, archive date, current escalation level, last message sent direction and owner. The communication list can be searched by subject, message text, search tags and bespoke data items; and filtered by: sent, received, process type, sender/recipient company group, messages assigned to the user and messages assigned to the Authorised Person at a specific escalation level.

(b) View communication details - a user can view the communication details, for a specific communication by clicking on the communication in the communication List. The communication details screen provides the following functionality:

(i) assign / change the ownership of the communication to another Authorised Person assigned to the business process;

(ii) view full audit history including when the communication was viewed;

(iii) add message;

(iv) escalate;

(v) maintain search tags (SDES User specific);

(vi) archive;

(vii) download entire message transcript in .csv format; and

(viii) download individual attachment(s). The state of the attachment, i.e. pending virus scan, failed virus scan, is also displayed. If an attachment has passed the virus scan it will be available for download. All available attachments can be downloaded as a single .zip file.

(c) Send new communication - the system allows the Authorised Person to send out new communications, with the following available options:

(i) choose the Market Role the communication is being sent from;

(ii) choose a business process (refer to the Data Specification for the processes that utilise the SDEP);

(iii) choose the Energy Company and Market Role the communication is being sent to;

(iv) enter communication subject;

(v) enter message text;

(vi) enter a search tag e.g. RMP or an internal reference;

(vii) enter any bespoke data items configured for the business process;

(viii) upload attachment(s); and

(ix) see the system generated unique reference once the communication has been sent.

(d) Reply to a communication - the system allows the Authorised Person to reply to a communication, with the following available options:

(i) add attachment(s);

(ii) add a search tag (this is added to the overall communication); and

(iii) enter response message text.

(e) Escalate communication - an Authorised Person has the option to escalate a communication if the business process has more than one escalation level and has not reached the maximum level. An Authorised Person can only escalate a communication by one level at a time. The escalate functionality is not available for: a general query; UTRN Contact; or Retrospective Amendment Request. If the time period for the escalation recipient to respond to the communication has lapsed, or the escalation recipient has responded, the Authorised Person is able to escalate the communication to the next level.

(f) Receive & set email / message notifications - an Authorised Person logged into the SDEP, will receive a notification if a message has been sent to them or their use case level. Authorised Persons have the option to set up email notifications for each time a new message is received. This option is only available to verified non-proxy email addresses. The frequency of the email notifications can be set to never, immediately, every hour, or every day. An email notification will only be sent if the Authorised Person has not visited the SDEP since the activity occurred.[5]

[5] Where the business process agreements require a quick response rate to a message, the user's email notification setting will be overridden. For example, the ‘Smart Prepayment CoS Exceptions’ process requires a response within 3 operational hours, so the system will send the email notification within 5 minutes of a new message being received, even if an Authorised Person has set their email notifications to ‘never’.

(g) Adding attachments - each attachment will be virus checked. If any attachment is found to contain a virus it will not be attached to the communication and the user will be alerted. A limit on the size of attachments sent in a single message is set to 10 MB. The following files will be accepted:

(i) .7z

(ii) .csv

(iii) .dat

(iv) .doc

(v) .docx

(vi) .gif

(vii) .jpeg

(viii) .jpg

(ix) .pdf

(x) .png

(xi) .txt

(xii) .xls

(xiii) .xlsx

(xiv) .zip

12 Reporting

12.1. The following reports will be available to SDES Users and can be downloaded once logged into the SDEP:

Report Name	**Timescale**	**Description**
Messages Sent and Received	Where required	Available to users with the 'user reports and secure communications administration' system functions. Returns a list of sent and received communications per MPID and business process for a given date range.
Messages Exceeding Response Time	Where required	Available to users with the 'user reports and secure communications administration' system functions. Returns a count of communications that have been sent and responded to per MPID and business process for a given date range and optional username.
Exceeding Response Time	Where required	Available to users with the 'user reports and secure communications administration' system functions. Returns a list of communications that have not received a response within the required time frame, per MPID, for a given date range.
Messages Sent No Response	Where required	Available to users with the 'user reports and secure communications administration' system functions. Returns a list of communications sent without response, per MPID and business process, for a given date range.
SDES User Process Types	Where required	Available to users with the 'user reports and secure communications administration' system functions. Returns a list of assigned business processes and MPIDs for a given user.
SDES User Process Types	Where required	Available to users with the 'user reports and secure communications administration' system functions. Returns a list of assigned business processes and MPIDs for the current user's entire SDES User.

12.2. The following reports will be made available to the Code Manager on a monthly basis:

(a) details of all current SDES Users and individual Authorised Persons with access to the system; and

(b) summary reports relating to the total volume of messages sent using the SDEP and the business processes they relate to.

13 System Audit

13.1. For the purposes of audit management, the SDEP will retain the following audit data, even after communications have been deleted:

(a) Authorised Persons who interacted with the communication;

(b) nature of interaction (send, view, add message, escalate, archive);

(c) relevant fuel and business process; and

(d) time and date stamps.

14 Data Handling

14.1. Each communication will be archived after 30 days since the latest message in the communication. An Authorised Person can view archived communications. If another message is added to an archived communication, its status will change from 'archived' to 'active'.

14.2. Where a communication is archived the status will be set to 'archived' for both the sender and recipient. Where an Authorised Person manually archives a communication using the functionality on the 'communication details' screen a warning message will appear to advise that this will also archive the communication for the other party.

14.3. Where a communication has been archived with an unread message, a badge will display next to the archive folder with the number of unread communications that have been archived to alert the SDES User.

14.4. Each communication will be permanently and irrecoverably deleted 30 days after the latest message has been archived. Even after a communication is deleted, the audit data will always remain.

Part C: Crossed Meter Resolution Portal (CMRP)

15 Service Description

15.1. The Crossed Meter Resolution Portal (CMRP) is a service that enables Energy Suppliers to create, investigate and resolve a Crossed Meter case and associate this with impacted RMPs and associated Electricity Suppliers and Metering Equipment Managers.

15.2. The CMRP shall provide, as a minimum:

(a) the ability to create a Crossed Meter case, and link this with the associated RMPs, Electricity Suppliers and Metering Equipment Managers;

(b) use of data from the Electricity Enquiry Service to identify impacted Electricity Suppliers based on the confirmed Meter Serial Number, and allow Electricity Suppliers to override this to manually associate additional RMPs;

(c) the ability to send messages, exchange information, record site visit results and upload files relating to the Crossed Meter case with associated Electricity Suppliers and Metering Equipment Managers to assist in the resolution of the case;

(d) access controls to restrict information to those organisations involved in the Crossed Meter case, with the ability to further restrict messages to specific organisations;

(e) robust user access controls, allowing access to the CMRP to be managed by the organisation's MAU and Authorised Persons on their behalf; and

(f) secure processing and storage of relevant data in accordance with the data retention requirements.

16 Service Users

16.1. The CMRP shall be available to Electricity Suppliers and Metering Equipment Managers that are users of the Electricity Enquiry Service.

17 Service Functionality

17.1. The CMRP enables Authorised Persons to perform the following functions:

(a) Crossed Meter case list - provides all cases where the current SDES User is associated to the case i.e. where the SDES User is the current Metering Equipment Manager or Electricity Supplier or has been the Metering Equipment Manager or Electricity Supplier since the case was opened. Any case linked to any of these cases will also appear in this list. The Crossed Meter case list can be searched by RMP, Meter Serial Number, MPL Address and case reference and filtered by last updated date from, last updated date to, 'My Cases' and case status.

(b) Crossed Meter case detail - provides the Authorised Person with all details of the case, including providing access to all linked cases. When a case is created, a note will be added to the case. Whenever there is a change of status on a case a note will be added to a case detailing what has occurred. Notes and questions flagged as private will only be visible to intended users. Private notes will appear in the event timeline even if the Authorised Person is not the intended recipient, however, any attachment's name and the note text will be obfuscated. It will not be possible to download the attachment if you are not the intended recipient of a private note. If a question has been asked of an SDES User, then it will be highlighted, and the obligation date will be shown. Adding a new note / question will fulfil the obligation.

(c) Meter Serial Number update - the current Electricity Supplier can amend a Meter Serial Number as confirmed on site. Where this is amended, all linked cases will have a note added detailing the change in Meter Serial Number. Where a new Meter Serial Number is entered the date of confirmation is mandatory. The system will search the Electricity Enquiry Service for RMPs that are associated with the entered Meter Serial Number. If the system finds any RMPs that have the entered Meter Serial Number as their current Meter Serial Number, then it will prompt the user to allow the system to create new linked cases for each RMP found.

(d) Adding attachments - each attachment will be virus checked. If any attachment is found to contain a virus it will not be attached to the communication and the Authorised Person will be alerted. A limit on the size of attachments sent in a single message is set to 2 MBs and a maximum of 5 attachments can be added to a single message. The following files will be accepted:

(i) .7z

(ii) .csv

(iii) .dat

(iv) .doc

(v) .docx

(vi) .gif

(vii) .jpeg

(viii) .jpg

(ix) .pdf

(x) .png

(xi) .txt

(xii) .xls

(xiii) .xlsx

(xiv) .zip

(e) Linked case management – an Authorised Person can navigate to the linked case management screen from the Crossed Meter case details screen, which lists all cases that have been linked. Case links are bi-directional i.e. if CMC00001 is linked to CMC00002 then CMC00002 is linked to CMC00001. Only Electricity Supplier users can manage case links. Where a case is unlinked, both of the unlinked cases will have a 'case un-linked' note added to the event timeline showing the detail of the removed link. When linking a new case, an Authorised Person can search for the case by case reference, RMP, Meter Serial Number or MPL Address. The matching cases will be listed, and the Authorised Person can choose the case they want to link. The Authorised Person must enter a link reason and each linked case will have a 'case linked' note added to the event timeline showing the detail of the new link.

(f) Create case – Electricity Supplier users can create new cases for RMPs where they are the Registered Supplier. There can only be one active case for each RMP. Electricity Suppliers can search for the RMP on the Electricity Enquiry Service by RMP, MPL Address or the current Meter Serial Number; only Metering Points where the SDES User is the Registered Supplier will be available for selection. The RMP's MPL Address, designation, Meter Serial Number(s), energisation status and disconnected icon will be displayed to allow the Authorised Person to select the required Metering Points. Once the case is created a case reference will be generated which will consist of the capital letters "CMS" followed by a five-digit number e.g. "CMS00001".

(g) Daily refresh – a job will be run each night following the provision of the MPAS Upload File to the Electricity Enquiry Service, which updates the current Metering Equipment Manager, the current Electricity Supplier and the current Electricity Enquiry Service Meter Serial Number(s) for every active case. The full Metering Equipment Manager history and Electricity Supplier history from case creation will be stored. It is possible that the number of meters associated with an RMP is changed by the daily update.

(h) Crossed Meter email notification - A job will be run each day to search for cases created since the job was last run. If there are any cases created since the job was last run that have yet to be viewed by the current Electricity Supplier for that case, then an email will be sent to all Authorised Persons with access to the CMRP for that SDES User. The email will also contain details of any case where the current Electricity Supplier has changed, and the Gaining Supplier has yet to view the case. The email will list the case reference(s) and contain a link to the CMRP sign-on screen.

18 Reporting

18.1. None

19 System Audit

19.1. For the purposes of audit management, the CMRP will retain the following audit data, even after the case has been deleted;

(a) Authorised Persons who interacted with the communication;

(b) nature of interaction (create/link case, send message, add attachments, archive); and

(c) time and date stamps.

20 Data Handling

20.1. A case is archived, with notes and attachments permanently and irrecoverably deleted 30 days after the case has been closed. Only the audit data is available for the case thereafter.

Section D: New Metering Point Requests

21 Service Description

21.1. New Metering Point Requests is a service that allows Electricity Suppliers to request the creation of a new or additional Metering Point from a Distribution Network Operator and allows the Distribution Network Operator to accept or reject the application or request more information.

22 Service Users

22.1. New Metering Point Requests shall be available to Electricity Suppliers and Distribution Network Operators that are users of the Electricity Enquiry Service.

23 Functional Requirements

23.1. New Metering Point Requests allow Authorised Persons to perform the following functions:

(a) Requesting new Metering Points - new or additional Metering Points are requested using a form wizard to collect the required information as specified in the Data Specification. The Electricity Suppliers may cancel a request that has a status of ‘Submitted’.

(b) Responding to Metering Point requests - following receipt, the Distribution Network Operator may view and accept, reject or request more information for Metering Point requests. The Distribution Network Operator may enter new Meter Point Administration Numbers to requests received and assign a request to the appropriate Market Participant Identifier.

(c) Bulk uploads – the Distribution Network Operator has the ability to bulk update Metering Point requests with new Meter Point Administration Numbers.

23.2. The system will allow Authorised Persons to:

(a) view a list of all Metering Point requests that are related to their SDES User;

(b) search, sort and filter the list of existing Metering Point requests that are related to their SDES User;

(c) download a list of their existing Metering Point requests in an excel friendly format;

(d) see a detailed view of an existing Metering Point request including all communications between parties via a ‘timeline’ view;

(e) amend their existing Metering Point requests, update their contact details and add notes to the Metering Point request at any point in the Metering Point request timeline; and

(f) alert Authorised Persons when a request/response requires their attention.

24 Reporting

24.1. Authorised Persons will be able to download results of a search in either .xlsx or .csv format by selecting the ‘Download’ button. Where a list is filtered, only the filtered results will be downloaded.

25 System Audit

25.1. For the purposes of audit management, the CMRP will retain the following audit data, even after the case has been deleted:

(a) Authorised Person who interacted with the communication;

(b) nature of interaction (create/link case, send message, add attachments, archive); and

(c) time and date stamps.

26 Data Handling

26.1. A request is archived 28 days after achieving a status of ‘Cancelled’, ‘Rejected’, 'MPAN Registered’ or ‘MPAN Disconnected’. Authorised Persons will be able to search for archived requests using the ‘Archived Status’ filter option.