Technical Specification Document

Central Switching Service (CSS) Service Definition

Version: XX Effective Date: TBC

Domestic Suppliers	N/A
Non-Domestic Suppliers	N/A
Gas Transporters	N/A
Distribution Network Operators	N/A
DCC	Mandatory

Change History

Version Number	Implementation Date	Reason for Change
1.0	TBD	[To be completed with reference to any relevant CPs]

Contents Table

[To be included]

1 Description of service

1.1 The Retail Energy Code (REC) Technical Specification is a key governance document comprising a number of components, including several Service Definitions. This Service Definition document provides information defining the Central Switching Service (CSS) which forms part of the end to end Switching Arrangements.

1.2 The CSS is one of a number of Switching Data Service Providers, as defined in the Interpretations Schedule and is therefore captured within the scope of the overall switching service management arrangements, as defined in the Service Management Schedule.

1.3 The CSS comprises a Registration Service and an Address Management Service. These will operate alongside the existing industry registration services (Electricity Retail Data Service (ERDS) for electricity and Gas Retail Data Service (GRDS) for gas).

1.4 The diagram below – Figure 1 - shows the systems that will participate in the end-to-end Switching Solution.

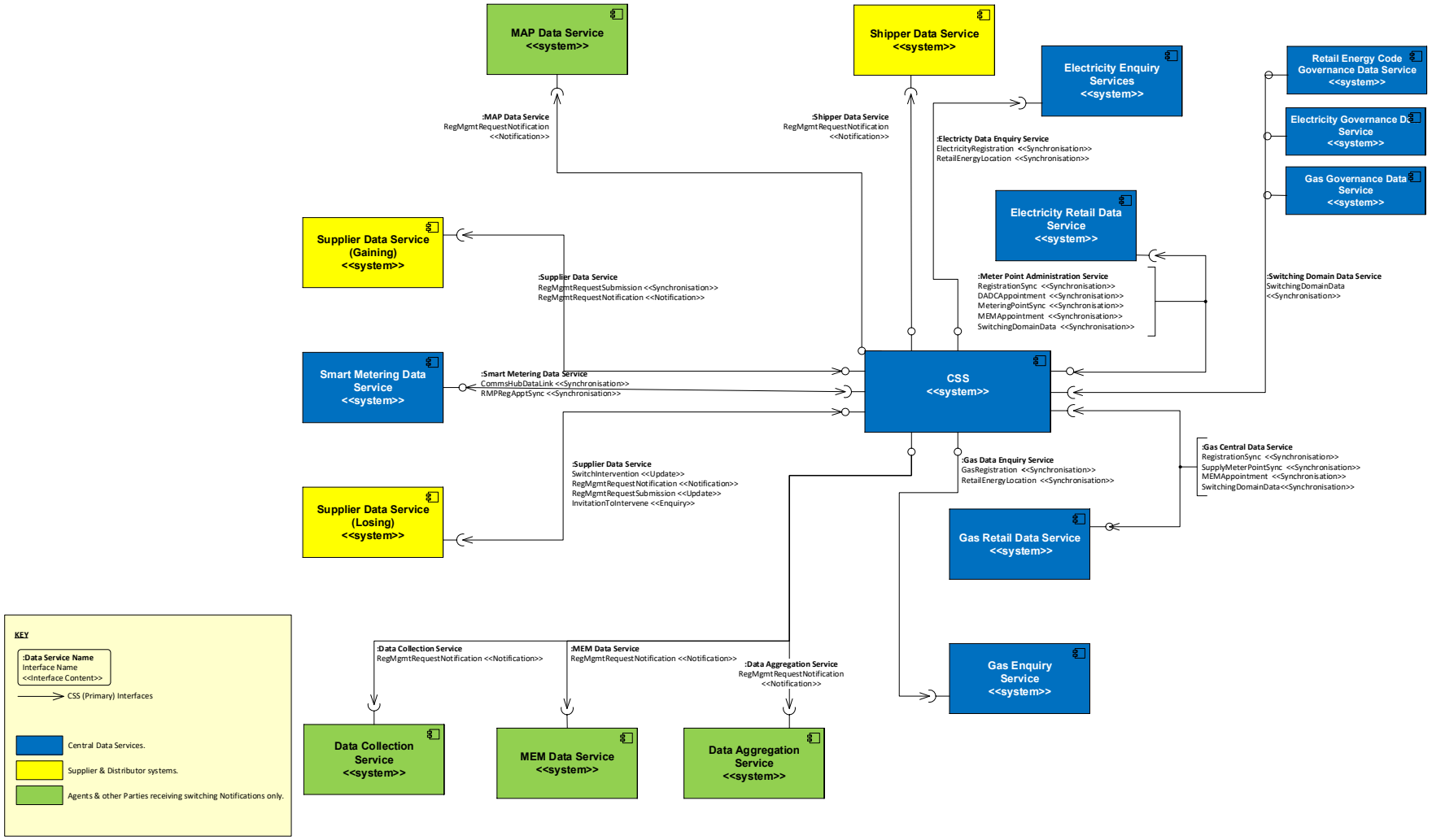

Figure 1 – CSS Primary Interfaces

1.5 The CSS comprises:

(a) a Registration Service; and

(b) an Address Management Service.

These are explained in further detail below.

Registration Service

1.6 Management of Registrations and associated data is the core purpose of CSS. CSS maintains a central database for electricity and gas Registrations.

1.7 Registrations can be created, amended and de-activated by an Energy Supplier's submission of a Registration Service Request. The process for Registration management is described in the REC Registration Services Schedule.

1.8 The Registration Service Requests and corresponding CSS responses are described in the REC Data Specification.

1.9 CSS validates the Registration Service Requests that it receives using data provided to it by the following external governance services:

(a) Electricity Market Participant Data provided by the Supplier Volume Allocation Agent under the BSC;

(b) Gas Market Participant Data provided by the Gas Retail Data Agent (GRDA); and

(c) REC Governance Data provided by the Code Manager.

1.10 Validation also uses Regulatory and Commercial Alliance data provided by ERDS (electricity) and GRDS (gas) as set out in the Data Management Schedule.

1.11 The CSS must have the following details in order to validate Registration Requests:

(a) qualification status of each Energy Supplier and whether there are any Market Sanctions in place;

(b) associations of Market Participant Identifier (MPID)/Market Role to Energy Company to [Energy Company OFAF Group]; and

(c) associations of MPID/Market Role to other MPID/Market Role based on Regulatory and Commercial Alliances.

1.12 For every Registration Request submitted, the CSS maintains the Registration Request Status (as defined in the Data Specification).

1.13 Further detail on the Registration Request and validation process is found in the REC Registration Services Schedule.

Address Management Service

1.14 Another core feature of the CSS is its use of an address related to a Registrable Measurement Point (RMP) which has, as far as is possible, been matched by the Address Management Service to a set of "standardised" Great Britain addresses, to create a unique address, called the Retail Energy Location (REL) Address. The REL Address is used for all energy RMPs at a given premises

and is the principal address that Consumers are likely to provide (e.g. to an Energy Supplier or a Price Comparison Website).

1.15 CSS's principal purposes with regard to addresses are to:

(a) Create, store and maintain a REL Address for each RMP; and

(b) Manage the quality of the addresses held.

1.16 The REL Address held in CSS may be one of the following types:

Type	Description
Meter Point Location (MPL)	The MPL address represents the Network Operator's view of the address associated with the energy supply point installation. If the MPL is not matched in the Address Management Service, a REL Address is created using the MPL Address.
Match	The REL Address is derived from the MPL Address, matched by the CSS Provider to an address in the Address Management Service.
Manual-Entered (ME)	When a Registered Supplier indicates the accuracy of the REL Address could be improved and provides address information to the CSS for the REL to be updated.

1.17 The following diagram illustrates at a high level the distinction between the Registration Service and Address Management Service functions.

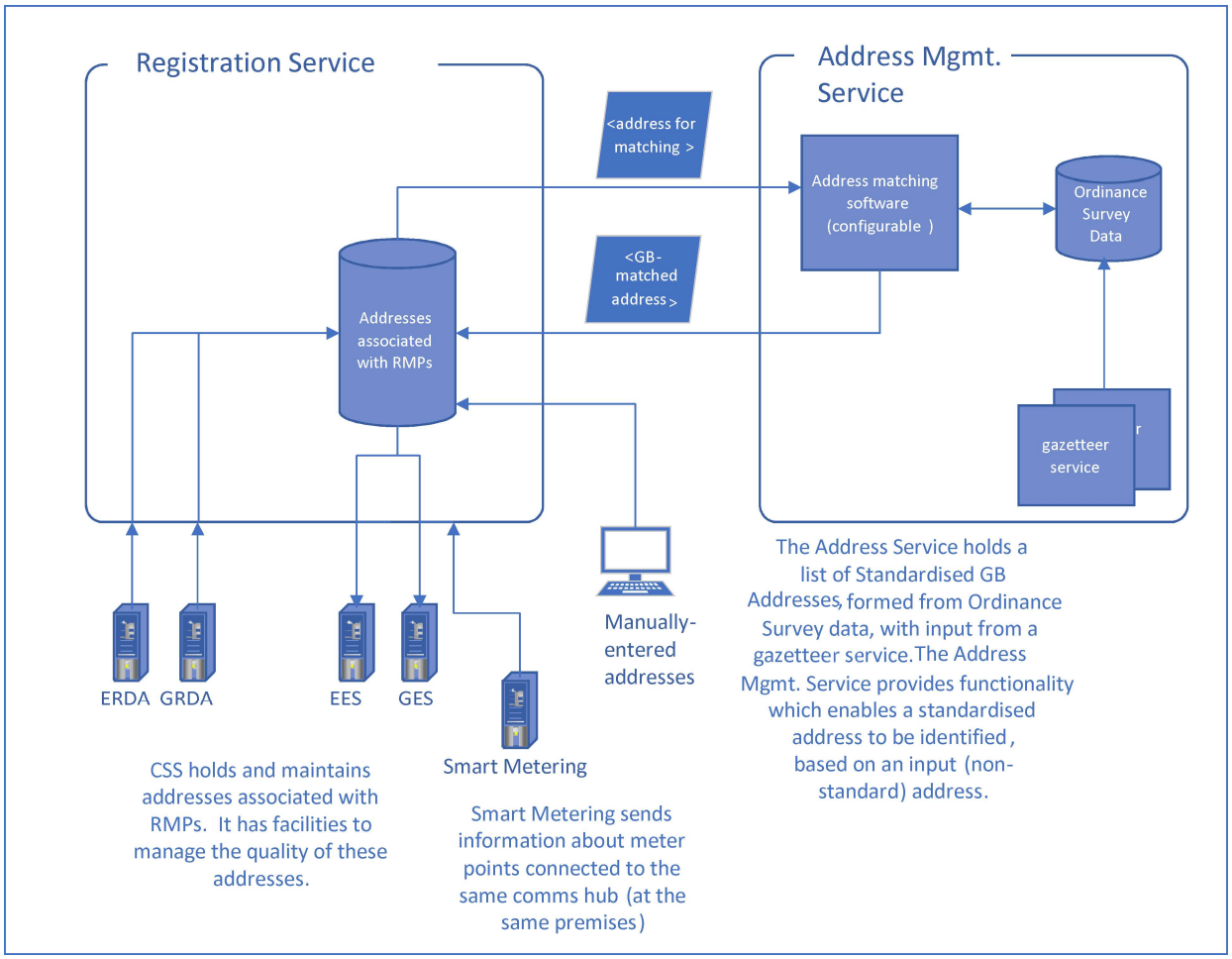

Figure 2 – Distinction between Registration and Address Management Service functions

1.18 The Address Management Service consists of:

(a) **GB Standardised Address List** – a complete set of all domestic and commercial GB addresses, plus as many other locations to which energy is supplied as is practicable (such as locations with a supply point but no address), held in a widely-recognised standardised form, compliant with BS7666 and ISO 639-2:1998, in all official GB languages. The GB Standardised Address List is formed from Ordnance Survey data, which uses AddressBase Premium; and

(b) **Address-matching software** – a set of algorithms, configuration settings and related software which, given an input address, searches the GB Standardised Address List and produces a match, together with a reference number that uniquely identifies the matched address (for example, the UPRN) and an Address Quality Confidence Score (degree of certainty) for the match.

1.19 The principal purpose of the Address Management Service is to:

(a) Store and maintain an up-to-date list of GB standardised addresses; and

(b) Find the standard GB Standardised Address List that most closely matches an address passed to it by the Registration Service (either in English, or an officially-recognised language).

1.20 CSS passes the MPL Address or the ME Address to the Address Management Service to find a GB-matched address in the GB Standardised Address List. If a perfect GB-matched address is found, CSS records this as the REL Address, together with the Address Quality Confidence Score of the REL Address (and language indicator if appropriate). If no GB-matched address is found, then CSS records the MPL Address or ME Address as the REL Address, with a corresponding Address Quality Confidence Score. A full process for REL Address creation can be found in the REC Address Management schedule.

1.21 The Address Quality Confidence Score returned by the Address Management Service is intended to be used by CSS to manage the quality of its addresses. It represents the level of certainty associated with a particular address match and is likely to be based on a number of different factors, such as whether the house number and postcode are identical (high quality indicator) or house number and street name match but the postcode does not (lower quality indicator).

1.22 Addresses stored by the Address Management Service, are kept up to date through updates from an external gazetteer service, which acts as the primary source of GB geographical data. The Address Management Service informs the Registration Service of address updates so that the REL Address can be amended to match the new address (e.g. following a re-allocation of postcodes).

1.23 Addresses matched to the GB Standardised Address List and returned to the Registration Service will form the REL Address mastered by CSS. REL Addresses will be synchronised to the EES and GES so that Switching Parties (including Price Comparison Websites)[1] can raise enquiries against them for the purpose of enabling switching (including without limitation) for the purpose of design, development, testing, integration and live operational use. No REL Address information may be displayed on public facing websites unless it is the website of a Switching Party that is a Price Comparison Website, and with prior permission from Ordnance Survey.

2 Definition of users

2.1 The CSS provides an application interface to enable the exchange of registration and address information between the CSS and the following Market Participants and their roles:

(a) Energy Suppliers;

(b) Gas Retail Data Agent;

(c) Gas Enquiry Service Provider;

(d) Shippers;

(e) Electricity Retail Data Agent;

(f) Electricity Enquiry Service Provider;

[1] The Switching Parties that can access the REL Address are stipulated in an agreement between DCC and Ordnance Survey. These include any party to the REC, any entity providing services to the Switching Programme for time to time, and Users (as defined in the REC) and in each case their respective employees, agents and contractors from time to time.

(g) Smart Metering Data Service Provider (SMDSP);

(h) Data Collectors;

(i) Data Aggregators;

(j) Meter Asset Providers (MAP);

(k) Metering Equipment Managers (MEM);

(l) Switching Data Service Providers; and

(m) REC Code Manager.

Market Participants are required to become CSS Users before they can exchange messages with the CSS. The CSS User Onboarding and Maintenance Schedule defines the process Market Participants must follow in order to become CSS Users and defines the associated CSS User obligations.

3 System access and user management

Communication Channels

3.1 The communication channel options available to interact with the CSS are:

(a) Internet Access; or

(b) Private Network Access, connecting via a Microsoft ExpressRoute.

3.2 Internet access – The CSS applications run in the Microsoft Azure Cloud which includes a series of internet gateway servers. Behind the internet gateway servers there is a bank of firewalls providing protection to the CSS application and supporting infrastructure. These firewalls are configured to manage the connections for all inbound and outbound CSS messages.

3.3 At the other end of the internet connection will be the CSS User application domain where the user application resides. Note this could be part of the CSS User's data service or that of an agent, for example a switching adaptor service. If the CSS User wishes to use the internet for connecting to the CSS, then its chosen environment will need to include both a Policy Enforcement Point (PEP) (i.e. firewall) and one or more internet gateways, depending on its capacity and resilience requirements.

3.4 Private Network access – CSS Users may choose to use a private network, connecting via a Microsoft ExpressRoute to send and receive CSS messages, rather than relying on the public internet. This requires the private network service provider to physically deploy a boundary gateway (or edge router) into the CSS User's chosen datacentre where the private network cables are terminated. Note this could be directly into the CSS User's data centre or that of an agent, for example a switching adaptor service provider. For the CSS environment the private network service provider will deploy boundary gateways in an Azure connection partner's datacentre. These boundary gateways will then be connected to Microsoft ExpressRoute transit connections from the connection partner to the Azure cloud. Traffic via the private network/ExpressRoute will then be processed in the Azure cloud in a similar way to traffic over the internet, all of which will be transparent to the CSS application.

3.5 CSS Users are responsible for deciding which communication channel they will use to interface with the CSS.

Certificate requirements

3.6 Each CSS User is required to obtain digital certificates from the relevant Certificate Authority in accordance with the process set out In the CSS User Onboarding and Maintenance Schedule. These certificates are digitally signed by the Certificate Authority (CA) and bind certificate owners with their public keys (and, optionally, with a comprehensive list of properties).

3.7 Organisations can opt to take on the role of a local registration authority, thus controlling the registration and issuance of certificates to their subordinate organisations.

3.8 Two types of certificate are provided by the Certificate Authority:

(a) Transport Layer Security (TLS) Certificates - to secure either end of the network connection, ensuring the transfer of messages across the communication channel is via a secure encrypted channel; and

(b) Message Signing Certificates - to authenticate individual messages sent across the communication channel through the application of a digital signature.

Certificate Authorities

3.9 The interface to the CSS from the SMDSP will use two Certificate Authorities:

(a) To secure TLS connections, certificates must be issued and signed by the DCC Key Infrastructure (DCCKI) Certificate Authority; and

(b) Certificates for message signing must be issued and signed by the Smart Metering Key Infrastructure (SMKI) Certificate Authority.

3.10 All non-SMDSP interfaces will use the REC Certificate Authority to obtain both TLS and Message Signing Certificates.

Certificate and public/private key requirements for CSS

3.11 The certificate requirements for individual CSS Users (i.e. the certificates that they need to request) will depend on the connection option they choose to connect to CSS and whether they send messages to CSS or just receive notifications:

(a) When sending messages to the CSS, the network connection is secured using the CSS' TLS Certificate (public key);

(b) When receiving messages from CSS, the network connection is secured using the CSS User's TLS Certificate (public key);

(c) When sending messages to CSS, the messages will need to be signed with the CSS User's Signing Certificate (private key);

(d) If a CSS User is using an adaptor service, the adapter service will require a TLS Certificate to secure the network connection when sending and receiving messages on behalf of CSS Users and will require the CSS User's Message Signing Certificate to sign messages sent to CSS on behalf of the User. Therefore, CSS Users that choose to use an adaptor service will not require a TLS certificate to send and / or receive messages from the CSS, but will require a Message Signing Certificate if they want the adaptor service to send messages to the CSS on their behalf;

(e) TLS Certificates and Message Signing Certificates use different keys and algorithms, so must be different:

(f) TLS Certificates and Message Signing Certificates are environment-specific (i.e. System Integration Testing (SIT), User Integration Testing (UIT), Production (PROD)) to ensure messages cannot traverse between environments. Certificates therefore cannot be re-used in different environments.

Key Generation

3.12 Public/Private key pairs will need to be created as part of a CSS Service User's on-boarding process. Each CSS Service User will be responsible for the generation of signing keys and certificates used by their message service interface

3.13 The owner of the Public/Private key pair must first engage in a registration process with the Certificate Authority such that the Certificate Authority is able to verify the identity of the owner and hence bind the certificate to the owner.

TLS Requirements and Configuration

3.14 To secure the exchange of data between the CSS and CSS Users TLS v1.3 protocol standard is applied where possible (TLS v1.2 is the minimum standard) and will make use of authentication using PKCS #3 Ephemeral Diffie Hellman key exchange to generate a shared secret (TLS-RSA) with AES-256-GCM-SHA256 for communications encryption.

3.15 If this authentication step fails, an "HTTP 401 Unauthorized" error will be returned to the CSS User. The error codes are referenced in the Data Specification.

4 Service availability

4.1 [A full set of Service Levels and Performance Measures are being defined and will be included in the Spring/Summer 2020 consultation]

4.2 The CSS will have 99.75% overall availability and 99.99% CSS-connection availability, outside scheduled maintenance periods.

Resilience and Failover

4.3 In the event of an unplanned outage, the CSS system will resume normal operations within 1 hour. In the event of corruption of business-critical data, the CSS is capable of restoring uncorrupted data from back-up to a suitable point where resumption of processing can continue without loss or duplication of inbound or outbound messages.

Upgrades and Outage

4.4 Any upgrades or maintenance to the CSS will be managed via CSS Service Management. If any service outage is required as a result of this maintenance, this will be managed by the Switching Operator.

5 User support

5.1 The CSS does not have an externally facing service desk. Any service management incidents and contacts will be raised via the Switching Service Desk. The CSS shall provide second line support in accordance with the Service Management Schedule.

6 Service Levels

[This section will include details of service levels against which the service has been designed. For example, this will include timescales for sending an initial response following receipt of a Market Message; and the timescales associated with any resultant processing steps, such as the update to internal systems or the onward sharing of data.

Non-functional requirements have been agreed as part of DB4 baseline, which we would expect to form the basis of the enduring service levels. Additional service levels to those set out in the NFRs may be added where this adds required certainty on the required standards of performance. We will finalise the service levels with stakeholders for inclusion in the Spring 2020 consultation. Note that any change to the NFRs included in the DB4 baseline would need to be agreed through Switching Programme governance].

7 Maximum Demand Volumes

Expected Volumes

7.1 The CSS is capable of processing 250,000 switches a day, which may occur in exceptional circumstances, for example to deal with a collective switch.

7.2 Expected CSS volumes:

(a) average daily volume of 42,300;

(b) peak daily volume of 281,600;

(c) average hourly volume of 3,500;

(d) peak hourly volume of 25,300; and

(e) annual volume of 15,450,000.

Capacity Management

7.3 The system, will be capable of the following:

(a) Storing information related to a combined total of 55.3 million RMPs;

(b) Supporting a 375,800 increase in the number of RMPs in each year of operation;

(c) Adding and removing system resources dynamically, as resource requirements vary;

(d) Holding 28 months'-worth of transactions online (for auditing purposes); and

(e) Holding 7 years' worth of transactions in total (online and in archive), from which information can be recovered within 1 Working Day.

7.4 Overall, capacity is such that all the other non-functional requirements placed on the system are efficiently met.

8 Reporting

8.1 [List of reports to be agreed – included for illustrative purposes]

8.2 CSS reports are available to Users on the Switching Portal.

Registration Service Reports
▪ Performance assurance; [list reports to be added]
▪ Market monitoring; [list of reports to be added]
▪ Aggregate data – aggregate number of:
▪ Accurately completed switch requests;
▪ Rejected switch requests by the rejection reason;
▪ Switch request objections on a monthly, quarterly and annual basis;
▪ Switch request annulments;
▪ Switch request withdrawals;
▪ Resolved erroneous transfers;
▪ Switches analysed between domestic and non-domestic;
▪ Domestic switches from large to large, large to small and small to large suppliers;
▪ Domestic switches where the Change of Occupier (COO) indicator was set – split between objected and not objected; and
▪ Initial registrations and deactivations;
▪ Supplier Portfolio Information – Aggregate data at the individual supplier level and at a Market Participant Role level.

Address Management Service Reports	Comments
Unmatched RMPs	RMPs unmatched to GB Standardised Addresses listed together with their meter point location address
Unchanged Plot Addresses	Addresses that have not changed from a plot address (no postcode assigned) for a predetermined length of time. Corresponding historical values/trends.
Address Quality Analysis	Quantitative analysis of address quality, including numbers of RMPs matched and unmatched, summaries of their quality indicator values and corresponding historical values/trends. The number of addresses with a quality indicator of less than *x* in each postcode district and area (district being the letters of the first part of the postcode and area being the numbers of the same district; using SE1 as an example, SE would be the district and 1 would be the area).
Updated ME Addresses	Addresses whose derivation is “ME” and for which the MPL has been updated. This is used to indicate those ME derived addresses that may need to be deleted and the MPL Address used instead to derive the

	REL Address, since the MPL Address has been updated to a better quality.
Updated Addresses	A report of addresses that have been created or changed since the previous report, for possible use by external parties who are interested in the use of REL Address. Each MPxN is listed together with its current REL Address, if: ▪ REL Address has been established (as a result of an initial registration); or ▪ REL Address has changed for any reason (because of the introduction or removal of an ME Address, update of MPL Address or updated address passed to CSS by the Address Service.

8.3 The CSS will provide the information required by the Switching Operator to allow it to meet its requirements under the REC.

9 Business Continuity/Disaster Recovery

9.1 The CSS utilises a public cloud offering, with data centres in two UK locations. This configuration provides the ability to switch between primary and secondary locations with minimum impact and downtime. It also provides the capability to failover from one to the other in the event of a catastrophic failure.

9.2 The CSS platform is protected against catastrophic failures pertaining to the hosted components that make up the entirety of the service. This includes both the Address Management Service and Registration Service. The granular monitoring of each of the applications and underlying infrastructure is paramount to providing a continuous, truly highly available platform. The granular monitoring is provided by either the CSS Provider or the Microsoft Azure cloud environment.

10 System Audit

10.1 CSS maintains an audit trail of requests received and responses sent (inbound and/or outbound messages).

11 Data Handling

11.1 For CSS Data Handling, see Capacity Management, paragraph 7.3, ‘d’ and ‘e’.

12 Security

12.1 The security requirements for the CSS Interface are intended to minimise the risks to the CSS infrastructure and its users.

12.2 The CSS itself is certified against ISO/IEC 27001 and is subject to certification using a UKAS-certified auditing body.

12.3 The CSS’s cloud base infrastructure is assured with SOC Type 2 security certification.

12.4 It is a fundamental prerequisite to approval for a connection to the CSS is that the connecting organisation has reliably identified and appropriately managed all risks associated with the proposed servers and networks for the interface.

12.5 Security requirements for CSS Users are described in the CSS User Onboarding and Maintenance Schedule.