RETAIL ENERGY CODE

Consumer Consent Service (CCS) Service Definition

RETAIL ENERGY CODE

Contents

RETAIL ENERGY CODE

Technical Specification Document

Consumer Consent Service Definition

Version: 0.1 Effective Date: TBC

Change History

Version Number	Implementation Date	Reason for Change
0.1	N/A	Initial draft for CCS industry consultation

RETAIL ENERGY CODE

1 Description of Service

1.1. The Consumer Consent Service (CCS) provides a central, consistent mechanism for capturing, managing and evidencing Permission provided by an Energy Data Subject for the sharing of Energy Data across the retail market. It enables Authorised Third Parties (ATPs) to request and obtain Permission in a standardised manner and ensures that Energy Data Subjects retain visibility and clear control over how their Energy Data is used. The CCS also enables Energy Data Holders to receive, validate and act upon Permissions and Permission Revocations in a consistent and auditable manner, ensuring that Energy Data is only shared where the appropriate Permission has been granted by the Energy Data Subject.

1.2. The CCS Provider is not a Party under this Code. Where the CCS Provider is referenced within this Code, RECCo is obliged to ensure that the services are provided in line with this Code.

1.3. The CCS consists of:

(a) a mechanism for onboarding Qualified CCS Users;

(b) a CCS Directory recording details of ATPs i.e., organisations wishing to access Energy Data, and Energy Data Holders (EDHs) i.e., organisations wishing to share Energy Data, and details of available Data Products linked to individual EDHs, allowing ATPs to view the available data and associated EDH;

(c) a CCS User Portal allowing CCS Users to configure their own access controls and maintain their individual organisation details;

(d) a mechanism for obtaining Permission by verifying an Energy Data Subject's identity and, matching them to one or more Registrable Measurement Points (RMP), as required;

(e) a mechanism for recording and storing Permission for access to Energy Data, enabling EDHs to validate that Permission is in place before sharing Energy Data with an ATP; and

(f) a CCS Consumer Portal where Energy Data Subjects can grant Permission, view details of organisations who are accessing their Energy Data and renew or revoke Permission for access to Energy Data, in accordance with the Consumer Consent Service Arrangements Schedule (CCS Arrangements Schedule).

1.4. The CCS supports peer-to-peer data sharing between EDHs and ATPs by providing a central trust framework where EDHs can place reliance on the CCS confirmation that valid Permission is in place before sharing Energy Data. RECCo takes no responsibility for the accuracy of the Energy Data shared by the EDH or the use of that Energy Data by the ATP.

1.5. This Service Definition should be read in conjunction with:

(a) the CCS Arrangements Schedule, which sets out the rights and obligations of CCS Users;

(b) the CCS API Technical Specification, which defines the mechanism for exchanging data with the CCS;

(c) the Data Specification, which defines the Market Messages used to interact with the CCS and the associated Data Items; and

(d) the Customer Experience Guidelines (CEG) which sets out the principles, standards and expectations for how Energy Data Subjects should be supported, informed and treated when interacting with Authorised Third Parties.

2 Entities which can access the CCS

2.1. The CCS shall allow the following entities to access and use the CCS:

(a) CCS Users (ATPs and EDHs) who have Qualified as CCS Users in accordance with the Qualification and Maintenance Schedule;

(b) Energy Data Subjects who can log into the CCS Consumer Portal to manage Permission data and view details of organisations who have access to their Energy Data;

(c) CCS Identity Verification Providers who deliver CCS Identity Verification (IDV), and also in some cases, CCS Address Verification requests from the CCS and respond with verification outcomes in accordance with the CCS API Technical Specification;

(d) RECCo who manages information relating to CCS Users via the CCS Administration Portal, and may extract information from the CCS Directory for publication on the REC Portal; and

(e) Tariff Interoperability Users wishing to access publicly available TI Energy Supplier information held in the CCS Directory.

3 Service Functionality

3.1. The CCS must include the following functional components:

(a) The CCS Authorisation Server, designed to ensure that Energy Data is only shared by an EDH if Permission is in place. The CCS Authorisation Server communicates with ATPs and EDHs through secure API endpoints to support the authorisation of Permission-based access to Energy Data. Once the Energy Data Subject has granted Permission, in accordance with the CCS Arrangements Schedule, the CCS will issue the ATP an Access Token, tied to the ATP and the specific terms of the Permission, together with a Refresh Token which the ATP

uses to obtain replacement Access Tokens while the Permission remains active. An ATP may then request Energy Data directly from the relevant EDH, using the Access Token provided by the CCS. Where Permission is revoked before its expected expiry date, the CCS shall terminate the Permission and associated Refresh Token, preventing the provision of any further Access Tokens, to ensure the sharing of Energy Data ceases.

(b) The CCS Directory, is the authoritative source of CCS information, holding details of Qualified CCS Users (ATPs and EDHs) and the CCS itself. This includes EDH endpoints to allow ATPs to issue data requests, CCS information to allow message exchange with CCS Users, CCS security certificates for exchange of CCS Market Messages, CCS User Client Identifiers which underpin interactions between participants and the CCS and operational contact details to support the resolution of issues. The CCS Directory does not hold private key material or Energy Data. The CCS Directory is based on self-service functionality, enabling CCS Users to manage their own organisational information. The CCS Directory also holds details of Data Products available from each individual EDH, with the associated metadata. The CCS Directory allows ATPs to identify Data Products where additional bilateral arrangements are required before Energy Data can be accessed.

(c) The CCS Consumer Portal, where Energy Data Subjects can grant Permission for access to Energy Data, view details of organisations who are accessing their Energy Data and renew or revoke Permission as required. The Consumer Portal only shows details of organisations accessing Energy Data where the individual has been verified as the Energy Data Subject. This includes scenarios where the individual granted Permission using the CCS, or other individuals granted Permission in relation to Registrable Measurement Points (RMPs) that the individual has been matched to. The Consumer Portal allows the Energy Data Subject to revoke Permission which they previously granted and to query records where Permission was granted by another individual. The Consumer Portal also allows each Energy Data Subject to maintain their own personal details, for example to highlight a change of address which will trigger further address-matching activities, and to view historic Permissions that were granted through the CCS.

(d) The CCS User Portal, where CCS Users can view and manage organisational information, enabling updates to be made to the information held in the CCS Directory. The CCS User Portal also allows CCS Users to manage security credentials to support the exchange of data via APIs.

(e) The CCS Administration Portal, where RECCo can view and manage CCS User information and also verify the addition of new Data Products, enabling updates to be made to the information held in the CCS Directory. The CCS Administration Portal is also used by RECCo to carry out administrative activities relating to Energy Data Subject and Permission data held in the CCS itself.

(f) CCS RMP Matching, which uses the address provided through the CCS IDV activity and matches this to one or more specific RMPs. This matching activity will be carried out by the CCS using Enquiry Service data.

(g) CCS monitoring and reporting, including 24/7 monitoring of System functionality, with alerts in place to identify issues; and broader assurance-based monitoring and reporting on both the CCS internal performance and CCS User performance to support REC Performance Assurance activities.

4 System Access and CCS User Management

4.1. Once a new CCS User has been Qualified, in accordance with the CCS Arrangements Schedule and the Qualification and Maintenance Schedule, RECCo adds the CCS User to the CCS Directory. Once the CCS User record is created, an email is sent to the Master Admin User, enabling them to establish an individual account via the CCS User Portal.

4.2. Registration, identification and management of CCS Users within the CCS Arrangements is based on OpenID Federation principles which establishes trust between interacting entities through a trusted third party e.g., the CCS Directory.

4.3. Each CCS User is provided a unique Client Identifier to enable identification and authentication of the CCS User in all communications and transactions within the CCS Arrangements.

4.4. Access to the CCS Directory will be managed via role-based access controls, to allow different user types to manage data only according to their access rules. This will include a clear separation between RECCo administrative roles and CCS User self-service roles.

4.5. Each Authorised Person within a CCS User's organisation shall have an individual user account, which shall only be accessed via multi-factor authentication.

4.6. The CCS Provider shall create for each CCS User a single 'Master Admin User' (MAU). The MAU must be a named individual with an identifiable email address which will be their username. The MAU will have the ability to create additional Authorised Persons and assign them to different roles, including viewing records, managing operational queries and managing security credentials.

4.7. Once the CCS User is established within the CCS Directory, they can request CCS security certificates to enable API based communication with the CCS. This includes the ability for CCS Users to read their organisation's information within the CCS Directory via API, in accordance with the CCS API Technical Specification.

5 Service Availability

5.1. The CCS shall be provided 24 hours a day, seven days a week, except during Scheduled Maintenance periods and unplanned outages.

5.2. The CCS shall have 99.9% availability, including Scheduled Maintenance periods.

5.3. Any unplanned outage of the services shall be notified by the CCS Provider to RECCo 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.

5.4. During a service outage, the CCS User Portal and CCS Consumer Portal will include a message explaining that the service is unavailable. API requests will not be fulfilled i.e. specific requests will not be responded to during the outage and will need to be resent later.

6 User Support and Incident Resolution

6.1. The CCS Provider shall monitor the service 24 hours a day, seven days a week to ensure continuous availability and performance. This will include proactive management of alerts that indicate a potential unplanned outage. Where alerts relate to a Severity 1 incident, resolution will progress outside of operational hours.

6.2. The CCS does not have a dedicated service desk. Any queries and incidents must be raised via the REC service desk. The CCS Provider shall provide second line support between 08:00 to 17:00 hours on Working Days.

6.3. CCS related queries and incidents will be resolved based on the following Service Levels:

Priority	Description	Target Resolution Time
Severity 1	Critical – Consumer harm, data integrity, or System failure	4 hours (95%) 1 WD (100%)
Severity 2	High – major technical or functional impact, no workaround	1 WD (95%) 2 WDs (100%)
Severity 3	Medium – technical defect, workaround exists	3 WDs (95%) 5 WDs (100%)
Severity 4	Low – minor incorrect behaviour	6 WDs (95%) 10 WDs (100%)

7 Service Levels

7.1. The CCS shall meet a 95th percentile response time of 300 milliseconds measured across relevant API transactions in the reporting period within the CCS platform

boundary, excluding external-dependency processing time. This requirement applies to the synchronous response acknowledging receipt of the message, including the relevant HTTP response code, as defined in the CCS API Technical Specification.

7.2. This Service Level covers the following interactions:

(a) acknowledging receipt of the ATP's request to initiate a Permission journey, submitted using the Pushed Authorisation Request mechanism.

(b) issuance of the Access Token in response to receipt of a valid authorisation code; and

(c) issuance of a Permission Revocation Notification following revocation of Permission by the ATP or Energy Data Subject.

7.3. Where a CCS Event Notification is issued and the CCS receives a response indicating HTTP 429 (Too Many Requests) or HTTP 503 (Service Unavailable) the CCS shall re-attempt delivery in accordance with any 'retry after' value specified in the response, until the request succeeds or a period of 2 hours has elapsed. Where no 'retry after' value is provided, the CCS shall re-attempt delivery at intervals of 300 seconds until the request is successful or a period of 2 hours has elapsed from the initial submission. If the message is still undelivered after this period, the CCS shall raise a service desk query for consideration by the relevant CCS User.

7.4. Following receipt of a verification request from a CCS User, the CCS shall issue a verification Security Event Token within 5 minutes.

7.5. If a CCS Event Notification remains undelivered after all retry attempts have been exhausted, the notifications will be retained for 60 days before being permanently deleted.

7.6. If a CCS User with active Permissions, has been inactive for 7 days, this information is made available in RECCo's monitoring and reporting portal.

7.7. Where new security certificates are requested via the CCS User Portal, new certificates are expected to be available within 5 minutes of a valid request under normal operating conditions, with propagation through the CCS Directory within 60 seconds.

7.8. Where existing security certificates are revoked by the CCS User via the CCS User Portal, the CCS Directory will be updated automatically and the revocation is propagated within 60 seconds under normal operating conditions.

8 Management of BCDR events

8.1. Where a BCDR event is invoked, the Recovery Time Objective for the CCS will depend on the type of failure, as follows:

(a) availability zone failure: restore within 30 minutes where automated failover

applies;

(b) regional outage or degradation: restore within 4 hours;

(c) catastrophic region loss: restore within 48 hours.

8.2. Where a BCDR event is invoked, the Recovery Point Objective for the CCS will depend on the type of failure, as follows:

(a) availability zone failure: 0-5 minutes;

(b) regional outage or degradation: 15 minutes for critical stateful components where cross-region patterns apply;

(c) catastrophic region loss: 24 hours.

8.3. An availability zone failure is the loss of a single, physically isolated data centre location within a cloud region, where the remaining availability zones in that region continue to operate, allowing the CCS to fail over automatically with minimal disruption.

9 Maximum Demand Volumes

9.1. The CCS shall be capable of scaling to meet industry-wide adoption and a total Energy Data Subject uptake to meet Great Britain's national population. Initially, the CCS shall have capacity to manage up to 10 million API calls per month.

9.2. Where maximum demand volumes are breached within a given month the CCS Provider shall report the situation to RECCo as part of the monthly performance report. RECCo may initiate a Change Proposal to increase the maximum demand volumes or take remedial steps to prevent recurrence, as required.

10 Reporting

10.1. The CCS Provider shall provide RECCo with a monthly performance report setting out its service and contractual performance. These reports shall be made available to the Authority and the REC Performance Assurance Board (REC PAB) as required.

10.2. In addition, the CCS shall provide centralised reporting that can be used by RECCo to monitor CCS User compliance. The specific reporting requirements are set out in the Performance Assurance Reporting Catalogue.

11 System Audit

11.1. The CCS shall collect audit records relating to security-relevant events to support the analysis of potential or actual compromises. As a minimum, audit records shall include reports and alerts detailing user access patterns to enable the identification of changing trends, unusual usage and/or accounts accessing higher than average volumes of data.

11.2. In addition, the CCS shall apply the following approach to data retention:

(a) CCS User and organisational data shall be retained for the duration of the relevant user account and for a minimum of 30 days thereafter to support audit, security and dispute resolution;

(b) Permission records will be retained for as long as required to evidence valid Permission and demonstrate compliance with regulatory and audit requirements; and

(c) System and audit data will be retained in line with agreed retention schedules to support security monitoring and assurance activities.

11.3. Upon expiry of the applicable retention period, Personal Data will be securely deleted or irreversibly anonymised and will not be retrievable.

11.4. The CCS shall be capable of supporting formal and informal audits conducted by RECCo (or its agent), or any other person legally entitled to carry out such an audit.

12 Data Handling

12.1. The CCS is an API-first solution with data exchanges between the CCS and the relevant ATP / EDH via CCS Market Messages defined in the Data Specification.

12.2. CCS Users may access and amend account information held in the CCS Directory via the CCS User Portal or using defined APIs.

12.3. The CCS uses the CCS Shared Signals Framework to issue CCS Event Notifications, in the form of a Security Event Token, to CCS Users with the CCS itself acting as the transmitter.

12.4. The following events trigger a CCS Event Notification:

(a) Permission Revocation Notifications to ATPs and EDHs; and

(b) Permission Verification Notifications to ATPs where the identified Permission remains valid, but its continued validity requires investigation by the ATP.

12.5. The CCS Shared Signals Framework uses OpenID Shared Signals Framework 1.0 and the underlying IETF Security Event Token standards (RFC 8417, RFC 9493, RFC 8935).

12.6. Under the CCS Shared Signals Framework, notifications will be delivered using a push delivery model and issued directly to CCS Users. Direct interactions between the CCS and Energy Data Subjects will be managed via the CCS Consumer Portal, with notifications issued to Energy Data Subjects via email, where appropriate.

12.7. The CCS shall operate in UTC, and all datetimes shall be recorded in an ISO8601 compliant format, save that timestamps within Security Event Tokens shall be

expressed as numeric date values in accordance with RFC 8417.

13 Security

13.1. The CCS Provider's information security management system shall be certified to ISO/IEC 27001, with the scope of certification covering the CCS, and shall be certified by a UKAS-accredited certification body.

13.2. The CCS Provider shall be responsible for provision of security certificates to CCS Users, to sign the artefacts which the CCS API Technical Specification requires to be signed, unless RECCo has approved the use of security certificates issued by an external source.

13.3. The CCS shall apply the FAPI 2.0 Security Profile. This includes all mandatory elements defined in the FAPI 2.0 security profile, together with the following CCS specific requirements:

(a) CCS uses mutual TLS (mTLS) for secure transport and to bind Access Tokens to the ATP's certificate, and implements the private_key_jwt method for CCS User authentication;

(b) Access Tokens associated with Energy Data Permission will be issued as signed JSON Web Tokens (JWTs) and will have a 30-minute lifetime, with the ability for tokens to be refreshed at any time while the relevant Permission remains active;

(c) A Refresh Token is never issued with a life extending beyond the Permission it relates to;

(d) CCS uses the PS256 JSON Web Signature (JWS) algorithm (RSASSA-PSS with SHA-256) and 2048 bit RSA key pairs for the signing of tokens, request objects and event notifications;

(e) CCS exposes its public keys via JSON Web Key Set (JWKS) URI to support automated key retrieval and rotation;

(f) CCS requires the use of signed request objects compliant with the OAuth JWT-Secured Authorisation Request (JAR) standard to ensure the integrity and authenticity of authorisation requests;

(g) CCS issues authorisation responses using the query response mode;

(h) CCS uses x-fapi headers to support message logging and tracking; and

(i) CCS uses Rich Authorisation Requests (RAR) to define the Permission details in the authorisation request.

13.4. Penetration testing of the CCS shall be undertaken at least once in each calendar year, and a report produced regarding the outcomes of this test, to include any observations or findings, and recommendations for any required remedial actions.

13.5. If the CCS Provider detects a potential or suspected security breach impacting CCS related Systems, it shall notify RECCo as soon as reasonably practicable.

13.6. Security requirements for CCS Users are described in the CCS Arrangements Schedule.