RETAIL ENERGY CODE

This document is classified as **WHITE**.
Information is for public, unrestricted dissemination and publication.

REC CONSUMER CONSENT TOPIC SPECIFIC SOLUTION GROUP
MEETING MINUTES

MEETING	**REC_CCTSSG_26_0617**
DATE	**17 June 2026, 10:00**
LOCATION	**By teleconference**

1. INTRODUCTIONS

The Chair welcomed Members to the meeting of the Consumer Consent Topic Specific Solution Group (CCTSSG). This session would focus specifically on a demonstration of the CCS User Platform.

The Chair noted that no pre-meeting papers were issued to Members ahead of the meeting, advising that due to the fast-paced nature of the project, some information and developments are not ready far in advance of meetings. The Chair added that RECCo will continue to provide Members with information on the topics for each meeting ahead of time, to ensure organisations can send the individuals with the most relevant expertise to each meeting. Presentation slides will be made available straight after the meeting, and minutes will continue to be published five working days afterwards. MPW added that RECCo would welcome any feedback after meetings. They added that any feedback sent to consumerconsent@retailenergycode.co.uk by 26 June would allow RECCo to include this within the next Solution Group meeting.

2. UPDATES FOLLOWING LAST SOLUTION GROUP

GR provided an update on the consent schema, confirming that feedback from the last session has been incorporated into a revised draft. Work is ongoing with the Technical Partner to determine the most appropriate placement of certain elements to ensure system efficiency. This includes discussion around whether items such as the data controller should sit within the schema itself or be delivered via the Application Programming Interface (API). A more finalised version is expected to be shared with Members shortly.

GR also updated on FAPI configuration options previously shared for review. No major concerns have been raised, and seven of the eight options are currently considered agreed. However, the access token lifetime remains under review due to mixed feedback, and further analysis is being undertaken before a final position is confirmed.

GR thanked attendees for their feedback in the previous Solution Group meeting, noting it had been highly technical but valuable due to the strong level of collaboration and input from participants.

A member asked regarding the decision to use mTLS certificate bound access tokens, what does that mean for the choice of PKI, and does it effectively mandate use of a RECCo PKI for TLS certificates by all participants, including for data sharing between EDH and ATPs. GR responded that mTLS is mandated for data sharing but RECCo are still working out internally the best approach PKI on a lower level, with an aim to communicate this out formally soon in a similar format to the FAPI 2.0 configuration options.

3. POLICY POSITION UPDATE: CCS OUTAGES

MPW introduced an update on the CCS outage policy position. Following consultation feedback and further analysis with the Information Commissioner's Office (ICO) and legal teams, three options were considered: allowing only existing consents during an outage, suspending all data sharing, or allowing both new and existing consents. The recommended approach is option one: during an outage, existing consents can continue for up to 12 hours, but no new consents can be created.

A member sought clarification on how this would operate in practice. MPW confirmed that new consent cannot technically be created when the system is unavailable, while existing consent-based data sharing can continue between parties during the outage window. The member noted this would require organisations to ensure their systems and rules support that approach.

4. CCS USER PLATFORM DEMO

CE took Members through a live demonstration of the CCS User Platform that ATPs and EDHs will use when accessing the service. CE outlined that the demo would cover key user journeys including platform login, EDH activities (such as creating and managing servers and endpoints), and ATP interactions (as data requestors), all primarily demonstrated through the user interface with supporting API views. They noted that this functionality is commonly used across other data-sharing ecosystems and has been adapted for CCS. CE clarified that the demonstration would use a showcase version of the platform for illustrative purposes, with branding to be finalised later.

CE explained the core concept of the trust framework: replacing complex one-to-one technical integrations between ATPs and EDHs with a centralised "directory" or trust layer. This allows all parties to register certificates, roles, and technical details in a single location, significantly simplifying onboarding, updates, and ongoing management by removing the need for multiple bilateral technical agreements.

A member asked whether the model supports scenarios where the EDH and ATP are different parts of the same legal entity, noting this reflects current industry arrangements. SJ responded that while it can likely be supported from a technical perspective, RECCo have not made a final decision on this policy position yet. They confirmed that the position is still under discussion, including legal considerations.

CE demonstrated the login process, including the option for federated single sign-on via an organisation's identity provider. After logging in, CE showed how users navigate to their organisation (as a legal entity) and access different functional areas. They then moved into the EDH workflow, demonstrating how a data provider (server) is created and configured through a guided process. This included entering key details (e.g. name, description, logo) and more technical settings such as endpoints, certificates, and optional webhook notifications. A member asked whether the process being demonstrated requires manual input or can be carried out via an API. CE clarified that while the demo is being shown through the user interface, all functionalities can also be performed via APIs, which will be demonstrated later.

CE took members through the remaining EDH setup steps within the trust framework. They outlined how organisations can configure additional attributes when creating or managing a server, including setting deprecation and retirement dates, defining replacement providers, and configuring visibility within the ecosystem. These features support change management and allow providers to signal future updates or transitions.

CE demonstrated that all server details entered via the UI are exposed through a central discovery API, which acts as the shared directory for the ecosystem. This allows ATPs to identify available EDHs, their endpoints, and associated technical information without needing direct bilateral exchanges.

CE then showed how EDHs can register API resources and endpoints by selecting predefined data categories (e.g. energy data), adding endpoint URLs, and publishing them to the directory. Once registered, these endpoints become discoverable and accessible to other participants. Updates can be made easily through the UI (or API), and general ecosystem data refreshes periodically, while critical security elements such as certificates update more rapidly.

A member asked whether ATPs would still need to individually identify and understand each EDH's endpoints, or whether this would now be standardised. CE confirmed that endpoint discovery is centralised through the trust framework. ATPs no longer need to approach each EDH individually, as all endpoint information is published in the directory and can be accessed from there.

However, they clarified that while discovery, consent, and security (e.g. mTLS) are standardised, the underlying data structures (e.g. API responses/JSON formats) are not yet standardised. As a result, ATPs will still need to review each EDH's documentation to understand how to consume the data, even though that documentation and access points are now centrally available.

A member advised that they have found the demonstration useful and asked if this could be recorded for a video which could be shared internally by Members. The Chair responded that RECCo acknowledge that there is a range of technical expertise within the meeting and would look into this request.

CE moved on to demonstrate the ATP workflow. They showed that CCS Users will create "applications" within the platform to act as CCS clients. These applications represent entities

requesting data and interacting with the system. The process mirrors the EDH setup: users can create and edit applications through the UI (or APIs).

A key distinction is the use of roles, which define what an organisation or application is permitted to do within the ecosystem. Roles are centrally defined and assigned through accreditation, then cascaded from the organisation level down to individual applications. When creating an application, users must select the relevant role(s), which determine what data they are authorised to request. CE explained that these roles act as a control mechanism. When a client requests data, the CCS checks whether the assigned role permits access to that data type; if not, the request is rejected.

A member asked how ATPs would be assessed and permitted to access specific data types or scopes. CE clarified that this is primarily governed by the accreditation process, which sits outside the technical design. SJ added that accreditation will determine what data an organisation can access, based on the risk profile of that data. They explained that while there will be a standard accreditation process, different levels of access will apply. For example, an organisation approved to access tariff data would not automatically be granted access to more sensitive data (such as half-hourly consumption data). At launch, access is expected to focus on a single data type, but the framework is being designed to support more granular, risk-based access controls as additional data types are introduced in future.

CE explained that when creating an application, ATPs must configure protocol settings such as redirect URIs, which are pre-registered to ensure secure redirection during consent flows and prevent unauthorised interception. Authentication is standardised using secure methods (e.g. private key JWT) in line with FAPI 2.0 requirements.

CE demonstrated the certificate creation process, explaining that certificates are required for secure communication with the CCS. This involves generating a private/public key pair externally, submitting a certificate signing request (CSR) to the trust framework, and having it signed to produce a valid certificate. Organisations can manage certificates at either the organisation level or per application, depending on their design preference.

CE noted that while the platform technically supports different approaches (e.g. internal or external PKI), final decisions remain subject to policy and ongoing discussions.

CE explained how users interact with the directory APIs. They outlined that participants use the certificates they created to authenticate with the directory, following a machine-to-machine (client credentials) approach aligned with FAPI 2.0 standards. This involves generating an access token (using secure methods such as private key JWT) and then using that token to call directory APIs.

They demonstrated how, once authenticated, users can retrieve information such as participants and organisations from the central directory. The same APIs can also be used to carry out all actions previously shown in the UI (e.g. registering servers, applications, and endpoints).

CE reiterated the end-to-end process:

- Users log in (with optional federated identity integration).
- EDHs create and publish servers and endpoints.
- ATPs create applications, assign roles, and configure certificates.
- Participants use the directory to discover each other and connect.
- All functionalities can be accessed via APIs using access tokens.

CE confirmed that the solution standardises consent, security, and discovery, but not the downstream data exchange formats, which still require participants to consult individual provider documentation.

A member asked how the use of tokens relates to mTLS, questioning whether they are separate authentication mechanisms. CE clarified that they are linked through certificate-bound access tokens. When a token is issued, it is cryptographically tied to the certificate used in the mTLS connection. This means that the same certificate must be presented both when obtaining the token and when using it. As a result, authentication works as a combined approach:

- mTLS establishes the secure connection using the certificate.
- The bearer token is then used for API interactions.
- The system verifies that the token matches the certificate used in the mTLS session.

5. FORWARD PLAN

TT concluded the meeting by outlining upcoming sessions and encouraged ongoing feedback and engagement from all participants.

There is a provisional date for the next Engagement Webinar on 22 July, which will cover a review of RECCo's quarterly plan. The next Topic Solution Group meeting on 01 July will focus on SEC & REC alignment, Legal Access Agreement, CCS User requirements and the CCS Definition. TT advised that Topic Solution Groups will continue on a fortnightly basis, with future topics to be confirmed as soon as possible.

TT advised that any members with queries are welcome to email consumerconsent@retailenergycode.co.uk, and the RECCo project team will be happy to respond. TT added that RECCO are looking for early adopters of the CCS solution and asked any interested parties to scan the QR code at the end of the meeting slides.

RETAIL ENERGY CODE

ATTENDEE ORGANISATIONS

Attendee	Representing	Initials	Role
Michael Walsh	Retail Energy Code Company	MJW	Chair
Christian Eloysio	Raidiam	CE	Presenter
Teresa Thompson	Retail Energy Code Company	TT	Presenter
George Roberts	Retail Energy Code Company	GR	Presenter
Matt White	Retail Energy Code Company	MPW	Presenter
Sarah Jones	Retail Energy Code Company	SJ	Presenter
Harry Firth	REC Code Manager	HF	Secretariat

Ofgem	Publicis Sapient
Department for Energy Security and Net Zero	Centrica
Citizens Advice	CGI
Which?	SECCo
Consumer Scotland	SMS Energy
ScottishPower	PayPoint
Elexon	GreenSync
Perse Energy	National Energy System Operator
SSE	N3rgy
E.ON	Flock Associates
East Lothian Housing Association	One Utility Bill
Smart DCC	ESG Global
Raidiam	PRIME
Electralink	ScottishPower
Cadent	Ohme
Stark	Smart Energy GB