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_0812**
DATE	**12 August 2026, 14:30**
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 the CCS Business Process Maps (BPMs).

2. CONSUMER USER JOURNEY – EXAMPLE SCREENS

MPW presented an early-stage demonstrator of the CCS User Journey, emphasising that the demonstrator was developed to help members visualise the Consumer experience and understand how CCS processes align with the business processes being developed elsewhere in the programme, rather than represent the final solution design or user interface.

MPW advised that the journey begins with an ATP, which explains to the Consumer what energy data will be shared, the purpose of the sharing arrangement, the duration of the permission, and introduces CCS as the platform through which permissions can be managed. From the ATP's platform, the Consumer is transferred into CCS.

Within CCS, the Consumer is introduced to the service, including the account creation process, identity and address verification requirements, and the eventual decision to share energy data with the ATP. The Consumer creates a CCS account using an email address, which can be pre-populated from information provided by the ATP but can be amended by the Consumer. A one-time password is used to verify the email address.

The Consumer is then taken through identity and address verification. Two methods are illustrated: bank-based verification and photo ID verification, although additional methods may be introduced in future. The preferred route uses Open Banking-style authentication, allowing Consumers to log in through their bank. The bank shares only the Consumer's name, address and date of birth for ID&V purposes. MPW reiterated that no financial information is shared. ID&V is completed using a credit reference agency check to establish occupancy and enable energy data matching. Once verification is successful, the Consumer creates credentials to secure their CCS account. The demonstrator uses a password-based approach, although CCS is also exploring more modern authentication methods such as passkeys.

The Consumer is then presented with a consent screen showing the data requested, the period of access, and the organisation requesting it. The Consumer can then grant consent, after which CCS confirms the permission and redirects them back to the ATP to continue accessing the service they originally requested. MPW highlighted that the solution is being designed as a fully API-driven service, allowing ATPs to integrate CCS directly into their own digital journeys and enabling seamless handovers between systems. They confirmed that future iterations of the Consumer journey would continue to be shared as development progresses.

A member asked whether independent security penetration testing would be completed and published before the solution goes live. MPW explained that the CCS solution is being built on top of FAPI 2.0 standards, which already benefit from extensive threat modelling and security assessments. CCS will nevertheless undertake its own reviews and assurance activities to validate that the architecture remains appropriate. Any additional threat modelling or assurance undertaken will be communicated transparently to industry. CE added that Raidiam's platform is subject to regular penetration testing and that relevant reports may be available.

A member questioned whether CCS had considered future scenarios where consent is granted by autonomous digital agents rather than by humans directly, noting that agentic interactions are becoming increasingly common. MPW confirmed that the current MMP does not include agentic journeys. However, they stated that the platform architecture is sufficiently flexible to support such developments and that discussions are already underway regarding how CCS may need to evolve in the future to accommodate AI-driven and agent-based interactions. They acknowledged that the industry is moving rapidly in this area and confirmed that CCS is actively considering future requirements beyond the initial scope.

3. BUSINESS PROCESS MAPS – WALKTRHOUGH OF CONSUMER JOURNEYS

EVS presented the latest CCS Consumer Journey BPMs, bringing together recent design work on ID&V, occupancy verification and the shared signals framework ahead of the upcoming consultation.

The grant permission journey begins when a Consumer requests a service from an ATP. The ATP provides permission details and redirects the Consumer to CCS, where their email address is verified and checked against any existing CCS account.

For new users, CCS initiates an identity and occupancy verification process through an ID&V provider. Consumers can verify their identity using either online banking or photo ID, with banking verification being the preferred route. If one method fails, the Consumer can attempt the alternative route. Following successful identity verification, occupancy checks are completed using credit reference and address data.

Where verification is successful, CCS stores the validated identity details and matches the consumer's address to MPxNs using REC Enquiry Services data. If successful, the Consumer is recorded as the verified occupant of those supply points and completes account creation by setting login credentials. If identity or occupancy verification or MPxN matching cannot be completed, the consumer is returned to the ATP, and the ATP is informed of the outcome.

EVS noted that CCS is exploring options to allow Consumers to save partially completed accounts where later verification steps fail, reducing the need to repeat successful checks in future journeys.

EVS then took members through the process for returning Consumers who already have a CCS account. Consumers log in using their existing credentials and may be required to complete multi-factor authentication (MFA), although the use of passkeys is expected to reduce the need for additional authentication steps.

A key part of the journey is confirming that the Consumer's address remains accurate. CCS compares any address information provided by the ATP against the address already held by CCS. Where there is a mismatch, the Consumer is asked to confirm which address is correct. If a new address is identified, the Consumer enters a change of address journey.

The change of address process removes the Consumer's verified occupancy status from their previous property and verifies occupancy at the new address. Because ID&V has already been completed, the Consumer only needs to repeat the occupancy verification stage. Following successful occupancy verification, CCS matches the address to the relevant MPxNs and updates the Consumer's account records. EVS noted that many of these checks are intended to happen in the background with minimal Consumer effort.

A member asked what information CCS expects ATPs to provide. EVS explained that ATPs may optionally provide information such as first name, last name, email address, postal address and potentially a telephone number. This is intended to reduce data re-entry for Consumers and improve the user experience. MPW added that MPxN matching is performed by CCS after address verification has been completed.

Before consent can be granted, CCS validates the permission request against the verified occupancy and associated MPxNs. The Consumer is then presented with a consent screen showing the data requested, the purpose of the request, the period of consent and the period of data access. Consumers retain the ability to decline consent at this stage.

Where consent is granted, CCS creates the permission record and returns the Consumer to the ATP with an authorisation code. The ATP exchanges this for refresh and access tokens, which are used to request energy data from the EDH.

The EDH validates the access token before providing the requested data. In some use cases, particularly those involving scheduled data sharing or tariff event notifications, the EDH may also store permission information to support ongoing notifications. Once validated, the requested energy data is shared with the ATP, enabling them to deliver the requested service to the consumer.

EVS went through the BPM for revoking permissions and managing ongoing data access under an active consent. Two revocation routes are proposed:

- ATP-led revocation: Either the Consumer asks the ATP to end data sharing, or the ATP identifies a reason why access should cease (for example, the service or contract has ended). Consumers may optionally provide a revocation reason. The ATP notifies CCS,

which updates the permission record, prevents further token issuance, confirms the revocation to the ATP, and where applicable notifies EDHs via the Shared Signals Framework (SSF).

- CCS-led revocation: Consumers can also revoke permissions directly through the CCS portal. CCS updates the permission record and notifies ATPs and any relevant EDHs in the same way as the ATP-led process.

Following consent, ATPs use a refresh token to obtain short-lived access tokens from CCS. Each time data is requested, CCS checks that the permission remains active before issuing an access token. The ATP then presents the access token to the EDH, which validates the token before sharing data. EVS emphasised that the access token is the key control mechanism ensuring data cannot be accessed once consent has been withdrawn.

EVS also discussed scenarios where data cannot be provided immediately, such as scheduled or batch requests. Under the proposed approach, an ATP submits an access token to an EDH to establish the request but must obtain a new valid access token when the data becomes available. This ensures consent remains valid at the point the data is actually accessed. EDHs may also use SSF notifications to monitor whether permissions have been revoked before releasing scheduled data.

A member questioned whether the proposed process could become overly complex and restrictive for real-world data-sharing scenarios, particularly where ongoing consent already exists and EDHs need efficient ways to validate permissions. They suggested the focus should be on ensuring consent validity can be checked efficiently rather than creating additional operational steps.

EVS acknowledged the feedback and noted that the current approach is a proposal intended to align with the programme's move away from mandatory token introspection following earlier stakeholder feedback. They highlighted that there are trade-offs between different token models and consent validation approaches. MPW reiterated that the proposal reflects the programme's current thinking and its alignment with open standards used in wider smart data schemes. They encouraged members to provide alternative approaches where they believe a better solution exists, particularly where practical operational considerations suggest the proposed model may not work effectively.

A member sought clarification on the EDH role. EVS confirmed that different organisations could act as EDHs depending on the use case, including Suppliers in the future TI arrangements. MPW added that live repositories may be able to provide data within a single token lifetime, whereas other routes, such as some smart meter data retrieval processes, may require scheduled requests and additional token validation.

A member suggested that earlier publication of the meeting materials would enable more informed discussion and feedback during meetings. MPW acknowledged the point and explained that the project team aims to publish materials as early as possible. However, given the current stage of design development, documents are evolving rapidly and are often being updated close to publication. They noted that while the BPMs had been shared on the day of

the meeting, stakeholders are encouraged to review them offline and provide feedback after having time to digest the material. They encouraged members to send feedback to Consumerconsent@retailenergycode.co.uk and added that the project team would be happy to arrange a call with members to discuss any aspects further.

EVS presented the query permission process, which is designed for situations where a Consumer identifies a consent record they do not recognise or wish to challenge.

Consumers can query either:

- A permission they personally granted but no longer recognise or understand.
- A permission associated with their property that was granted by another occupant, such as another household member or a previous resident.

Where the consent belongs to the Consumer, they can choose to revoke it through the standard revocation process. Consumers are also provided with ATP contact details and the relevant grant ID to enable direct discussions with the ATP if they require further information.

Where the query relates to a consent granted by someone else, the Consumer can submit a query through CCS and optionally provide a reason. Once submitted, CCS records the query and revokes the associated permission to prevent further data sharing while the issue is investigated. The ATP is notified of the revocation and query details and is expected to investigate the consent record and provide an outcome within a defined timeframe. CCS records the outcome for monitoring, reporting and assurance purposes. Where applicable, EDHs are also notified through the SSF that the permission has been revoked.

A member asked whether the CCS journeys and interfaces would be tested with Consumers before implementation. EVS confirmed that elements of the query journey have already been included in Consumer research activities. MPW explained that REC has completed two phases of Consumer research involving participants from a range of Consumer backgrounds and that further testing is planned. Future work will include usability and user acceptance testing using working prototypes, subject to future budget approval.

A member raised questions about whether ATPs would be able to provide additional contextual information through the CCS portal to help Consumers understand what a consent relates to before revoking it. EVS explained that, for MMP, ATPs will not directly provide information through the CCS portal. Instead, CCS will present standard information based on the original consent record and provide ATP contact details so Consumers can seek clarification directly from the ATP. MPW added that Consumers will be shown as much information as possible from the consent record to support informed decision-making.

The member also asked whether revoked permissions could be reinstated. MPW clarified that there is currently no concept of restarting a consent. Instead, if appropriate, the Consumer would complete a new consent journey, creating a new permission record.

CE noted that ATP and EDH information will be maintained within the CCS directory and trust framework, ensuring participant information remains up to date and available to support these processes.

A member asked whether Consumer research had explored attitudes toward CCS if Consumers understood that implementation costs might ultimately be recovered through energy bills. MPW responded that the decision to establish CCS stems from an Ofgem policy decision and therefore REC's consumer research is focused on how Consumers interact with the solution rather than whether the solution should exist. The Chair noted that Ofgem's impact assessment concluded that the anticipated benefits outweighed the costs under the scenarios assessed, although they acknowledged that questions around funding and Consumer bill impacts are primarily matters for Ofgem rather than the CCS project team.

4. FORWARD PLAN

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

The next Topic Solution Group meeting on 26 August will focus on the Consent Token Model and how this works with shared signals. The next Engagement Webinar is due to be held in September. The Chair advised that the schedule of meetings during the upcoming consultation period is under review and will be communicated to members as soon as possible.

MPW advised that any members with queries are welcome to email consumerconsent@retailenergycode.co.uk, and the RECCo project team will be happy to respond. They 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.

ATTENDEE ORGANISATIONS

Attendee	Representing	Initials	Role
Michael Walsh	Retail Energy Code Company	MJW	Chair
Matt White	Retail Energy Code Company	MPW	Presenter
Eva Von-Schaxmann	Retail Energy Code Company	EVS	Presenter
Christian Eloysio	Raidiam	CE	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

Attendee	Representing	Initials	Role
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		