RETAIL ENERGY CODE

This document is classified as **WHITE**.

Information is for public, unrestricted dissemination and publication.

REC CONSUMER CONSENT SOLUTION TOPIC SPECIFIC SOLUTION GROUP
MEETING MINUTES

MEETING	**REC CCTSSG_26_0226**
DATE	**26 February 2026, 10:00**
LOCATION	**By teleconference**

1. INTRODUCTIONS

The Chair opened the meeting, welcoming participants and outlining the group's purpose in supporting development of the Consumer Consent Solution (CCS) and industry engagement alongside the live consultation.

2. UPDATE ON FIRST CONSULTATION

MPW advised that the first CCS consultation was published on 11 February. The consultation period will run for six weeks, closing for responses on 25 March. Engagement activities, including working group discussions, will continue throughout this period. Following closure, responses will be analysed and inform the REC Change process.

3. SPOTLIGHT ON TECHNICAL DESIGN

GR took members through the technical design aspects set out in the consultation. They encouraged members to ask clarification questions during the meeting, but to express their opinions on the policy positions as part of their consultation responses.

They explained that the design had been informed by a feasibility study and procurement strategy completed prior to RECCo's appointment as delivery body, followed by a market scan, proof of concept activity, and a series of functional prototypes involving multiple vendors. GR confirmed that UX work and Trust Framework Advisory activity had been undertaken in parallel.

GR noted that the project entered the design phase during 2025 and that prototype activity was still ongoing. They explained that the consultation intentionally limited low-level technical detail due to active procurement. They reiterated that RECCo's strategic position remained to procure an off-the-shelf consent management solution that would be configured for the required use, rather than building a bespoke platform.

A member asked why detailed sequence diagrams had not been included in the consultation documentation. GR responded that detailed sequence diagrams could not yet be published due to the ongoing procurement process. They confirmed that business process diagrams had been included in the consultation and that further technical detail would be shared in later phases.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

GR explained that the CCS design aligned with Ofgem's hybrid model, under which data sharing would occur directly between CCS Users, while CCS would provide central trust and facilitation services. They confirmed that CCS responsibilities would include consent management, PKI services, and the provision of a directory and registry of organisations and services.

GR clarified that CCS Users would retain ownership of their customer relationships, portals, and databases. They also confirmed that CCS did not propose to standardise energy data sets at this stage. They highlighted that the use of a central token model introduced resilience considerations, particularly in the event of CCS outages.

A member asked whether maintaining central consent records could result in consumers or organisations being locked into a single authorised third party, potentially raising competition concerns. GR responded that the design did not lock consumers or ATPs into a single provider. They confirmed that CCS would not restrict movement between equivalent ATPs.

GR explained that the CCS design deliberately separated centralised trust functions from decentralised operational responsibilities. They stated that centralised responsibilities under CCS would include consent token issuance, the maintenance of a central consent ledger, identity verification (ID&V) for the Minimum Market Product (MMP), directory and registry services, PKI services, and monitoring and assurance to support REC governance.

GR further explained that decentralised responsibilities would remain with participants and would include ATP-held consent records, data storage and exchange mechanisms, and commercial and contractual arrangements. They reiterated that ATPs will be able to continue to own their customer relationships for the delivery of their services.,

A member asked how CCS would accommodate scenarios where ATPs and EDPs operated within the same organisation or group, or where secure file-sharing solutions were currently used. GR responded that the design recognised these scenarios and did not exclude them. They explained that organisations would be able to operate multiple roles within the ecosystem. MPW added that CCS aimed to standardise initial data access via APIs to improve interoperability and security, but that CCS would not dictate how data was shared beyond the trust framework boundary.

GR explained that the MMP would link to a centralised ID&V service. They stated that consumers who were not recognised by CCS would be redirected to the ID&V service, where their identity and address would be verified, with CCS then attempting to match the consumer to the relevant meter point using existing Enquiry Services.

A member asked whether ATPs could use their own existing ID&V solutions, such as those used in the banking sector. MPW responded that centralised ID&V would apply for the MMP. They explained that federation with trusted third-party ID&V providers was an aspiration for future phases but would not form part of the initial delivery.

A member expressed concern that centralised ID&V could introduce unnecessary friction and barriers to consumer consent. GR acknowledged the concern and stated that a key principle of the design is to build on top of the OIDC protocol which would enable federated IDV in the future. They also acknowledged the matching challenges and that unhappy paths were recognised and required further design work, which should be informed by consultation feedback.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

GR explained that interoperability would be achieved through mandatory registration in the CCS directory, standardised service descriptions, and machine-readable endpoints.

A member asked what interoperability meant in practice. GR responded that, once onboarded, participants would be able to interact predictably without bespoke integrations, because endpoints and security requirements would be standardised across the ecosystem and immediately discoverable across the ecosystem. Additionally, the implementation of consistent security and data sharing standards, with centralised PKI services,

GR explained that CCS proposed adopting the FAPI 2.0 Open Standard, including the use of mutual TLS (mTLS) and sender-constrained tokens by CCS Users. They confirmed that PKI certificates would be issued and managed centrally by CCS.

A member stated that the purpose of smart data schemes is to coalesce around secure methods of data sharing, and that this applied cross-sector as driven by government policy and departments. GR re-emphasised the intention of the CCS designs to enable cross-sector interoperability out of the box and reassured that the project team were staying aligned with DESNZ and government to ensure this.

A member asked whether REC-provided PKI would be mandatory. GR confirmed this.

A member asked whether FAPI 2.0 required formal certification. GR responded that CCS assurance would focus on correct implementation within the trust framework rather than on external certification.

A member asked how FAPI 2.0 aligned with a buy-rather-than-build approach. GR responded that REC intended to procure off-the-shelf solutions but could not comment further due to active procurement.

A member clarified that certified FAPI 2.0 solutions already existed and that certification requirements differed between providers and relying parties. GR thanked the member for the clarification.

GR described the end-to-end consent lifecycle and explained that consent would be required only where personal energy data was shared. They outlined that ATPs would determine whether consent was required, consumers would be redirected to CCS, consent information would be presented using the Customer Experience Guidelines, and a consent token would be issued. They explained that Energy Data Providers would introspect the token before releasing data.

GR further confirmed that consumers would be able to manage their consents either via a CCS consumer portal or via ATP platforms, and that CCS and ATP consent records would be synchronised.

A member asked whether consent tokens would contain personally identifiable information. GR responded that full consent details would be recorded centrally, while token contents were still being refined. MPW added that data-minimisation principles would apply.

GR explained that CCS proposed using the existing REC-managed Enquiry Services to support address-to-meter matching.

A member raised concerns that inaccuracies in REC Enquiry Service data could prevent valid consents from being granted. Another member raised concerns that insufficient

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

validation could result in GDPR breaches. GR responded that no single perfect industry solution existed and that multiple address standards were currently in use. MPW added that further work was required on governance, exception handling, and unhappy paths.

A member asked how CCS would interact with existing supplier-led correction processes under REC. GR confirmed that supplier-led correction processes under REC would remain unchanged.

GR confirmed that CCS onboarding would be managed through the REC Portal and would align with existing REC governance processes. They explained that sandbox testing would be provided prior to live participation. They further confirmed that accredited organisations would be published to the CCS directory and that ongoing monitoring would support assurance and ecosystem reliability.

4. FORWARD PLAN

The Chair outlined the forward plan for future industry engagement workshops in the coming months. They advised that the next Topic-Specific Working Groups would focus on the User Experience aspect of the current consultation.

The Chair advised that the central Webinar, originally scheduled for 05 March, has been replaced with a wider in-person engagement event on 04 March.

5. AOB

No AOB items raised and the Chair closed the meeting.

Next meeting date: 12 March 2026

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

RETAIL ENERGY CODE

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

Attendee	Representing	Initials	Role
Michael Walsh	Retail Energy Code Company	MJW	Chair
Matt White	Retail Energy Code Company	MPW	Committee Member
George Roberts	Retail Energy Code Company	GR	Committee Member
Eva Von-Schaxmann	Retail Energy Code Company	EVS	Committee Member
Hemant Mistry	Retail Energy Code Company	HM	Committee Member
Vicky Brown	Retail Energy Code Company	VB	Committee Member
Teresa Thompson	Retail Energy Code Company	TT	Committee Member
Nathan Gould	Retail Energy Code Company	NG	Committee Member
Harry Firth	REC Code Manager	HF	Secretariat

Ofgem	REC Code Manager
DESNZ	E.ON Next
CGI	Centrica
N3rgy	Citizens Advice
East Lothian Housing Association	Electralink
ESG Global	Kraken
SECCo	SDATA
Elexon	Which?
Publicis Sapient	Perse Energy
Raidiam	Icebreaker One
DCC	SSE
EnergyCode	Hildebrand

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.