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_0716**
DATE	**16 July 2026, 14:30**
LOCATION	**By teleconference**

1. INTRODUCTIONS

MPW welcomed Members to the meeting of the Consumer Consent Topic Specific Solution Group (CCTSSG). This session would focus specifically on User Experience and Technical Design.

2. TRANSITIONING FROM CONSENT TO PERMISSION

MPW advised that RECCo are proposing to transition from using the term “consent” to “permission” within CCS governance and REC documentation. They explained that this change is intended to future-proof the solution by supporting a broader range of data-sharing scenarios beyond GDPR consent, while still retaining the term consent in Consumer-facing journeys and in the short-term project name, Consumer Consent Solution.

A member questioned whether retaining “consent” in the project name could create confusion if the solution is ultimately designed to support wider permissioning models, including data sharing based on legal bases other than consent. They suggested adopting “permission” more consistently throughout to provide clearer and more flexible language for consumers and industry alike. MPW advised that a longer-term Consumer-facing name for CCS is under discussion, which should alleviate any concerns of confusion.

A member sought clarification on whether “permission” was intended to encompass all legal bases for data sharing. MPW confirmed that the terminology is intended to support both current and future use cases, including additional legal bases and non-domestic data-sharing scenarios that may fall outside GDPR consent requirements. The member broadly welcomed the move, noting that consent is increasingly seen as a limited model.

Another member argued that changing terminology mid-project could create unnecessary complexity and inconsistency, suggesting that the project name and terminology should remain stable until any future Consumer-facing branding work. Another member agreed and warned that introducing a new term could generate significant confusion across industry governance documentation unless supported by clear justification and guidance. They encouraged the project team to set out the benefits, drawbacks and legal reasoning more explicitly. MPW acknowledged the feedback and agreed that RECCo would provide greater detail on the

rationale, legal considerations and intended application of the terminology change before progressing further

Another member supported the proposed shift based on their own similar experiences, where “permission” was adopted to accommodate both GDPR and non-GDPR scenarios. However, they cautioned against extending the term too broadly, stressing that permission should remain linked to data flows controlled by the data subject rather than being used as a catch-all term for any data-sharing arrangement.

3. ATP ACCOUNT CREATION AND RENEWAL

MPW provided an update on RECCo’s stance on account creation for MMP. They explained that both the previous design consultation and Solution Group meetings had explored both account-based and guest-user journeys. However, subsequent development of the technical solution and a better understanding of ID&V requirements had led RECCo to reconsider that approach. The current position is that Consumers will need to create an account when first interacting with CCS, as guest journeys would require Consumers to repeat ID&V checks every time they access the service. RECCo’s assessment is that implementing a secure guest journey would introduce additional complexity, cost and delivery risk that cannot be accommodated within the MMP timeline. While the option remains open for future development, the working assumption is that account creation will be the sole route into CCS at launch.

A member challenged the proposal, noting that it represented a significant design decision and requesting greater visibility of the supporting analysis. They questioned whether removing the guest option could negatively affect Consumer uptake and sought assurance that the rationale, trade-offs, assumptions and potential impacts would be fully documented and consulted upon. MPW confirmed that the proposal would form part of the forthcoming summer consultation and that the supporting evidence and assessment would be set out in more detail.

A member suggested that CCS should consider approaches commonly used by modern digital platforms, such as a "remember me" functionality, which could provide a more streamlined user experience without requiring a traditional account creation process. MPW acknowledged the point and agreed that the team would revisit earlier assessments to ensure that such options had been fully considered. GR added that any solution would need to balance usability with security requirements, particularly the ability for Consumers to access their account across devices and recover access if a device is lost.

CE highlighted additional security considerations, particularly around multi-factor authentication (MFA). They noted that guest journeys could undermine security controls because Consumers resuming a guest journey may only be required to verify possession of an email address, and CCS would have limited visibility over whether MFA protections existed on the associated email account. CE added that comparable smart data schemes, including Open Banking, generally avoid guest access models for journeys involving personal identifiable information due to similar security concerns.

There was also discussion on a separate assumption relating to consent renewal journeys. MPW presented a proposed process whereby renewals would be initiated and managed through an ATP rather than directly through CCS. Under the proposed model, Consumers seeking to renew an existing permission would be redirected from CCS to their ATP, which would then initiate the renewal request and redirect the consumer back to CCS to complete the confirmation process. MPW explained that this approach would help ATPs manage the wider services linked to the permission and ensure that renewals are considered in the context of any ongoing contractual or service relationships.

A member questioned whether Consumers would realistically begin a renewal journey directly within CCS, suggesting that the vast majority would instead receive prompts from the ATP application they were actively using. They also identified a potential issue in the proposed process flow, noting that if a Consumer started but did not complete the renewal journey prior to expiry, notifications to ATPs could be misinterpreted as a withdrawal of consent rather than a failure to renew. MPW agreed both points were valid and confirmed that the process flow and associated communications would be reviewed and clarified, noting that ATP-led prompts were likely to be the most common entry point for the renewal journey.

4. USER EXPERIENCE: CEG REQUIREMENTS

LB reminded Members of the Customer Experience Guidelines (CEGs), which form part of the wider CCS legal documentation alongside the CCS Arrangement Schedule, Service Definition and API artefacts. The CEGs are intended to set out requirements and recommendations for ATPs at each stage of the Consumer permission lifecycle. Although presented as a linear journey, it was recognised that in practice Consumers may move between granting, reviewing, renewing and revoking permissions in a non-linear manner.

LB emphasised that the CEGs focus specifically on interactions where Consumers engage with CCS. ATPs will remain responsible for their own branding, tone of voice and broader customer journeys. To support implementation, requirements are categorised as Must, Should and May, with "Must" representing mandatory requirements, "Should" representing recommended good practice, and "May" representing optional enhancements that could further improve the consumer experience.

A member asked whether the requirements had been established before the solution design or developed in parallel with it. LB explained that both the solution and the requirements have evolved iteratively together, informed by ongoing design work and stakeholder engagement. They stressed that the requirements remain working assumptions and that stakeholder feedback is actively sought before formal consultation. MPW confirmed that the CEGs will be subject to public consultation and remain open to refinement.

A member questioned whether mandatory requirements would be audited. MPW noted that the precise compliance and assurance arrangements are still being developed but indicated that mandatory requirements would likely be subject to some form of validation, albeit through a proportionate REC-style risk-based assurance approach rather than extensive auditing.

The first set of requirements considered were cross-cutting requirements applicable across all stages of the consumer journey. Examples included expectations around accessibility, such as compliance with WCAG 2.2 AA accessibility standards, and the use of plain language in consumer communications.

A member asked whether the requirements had been derived from established frameworks. LB explained that the project team had reviewed approaches taken by Open Banking and the Australian Consumer Data Right (CDR) programme, while also drawing on CCS Consumer research and lessons learned from other smart data initiatives. The intention is to strike a balance between providing sufficient standardisation for Consumer trust and allowing ATPs flexibility in designing their own customer experiences.

A member raised concerns that several requirements, as currently presented, were open to interpretation. They suggested that terms such as "plain language" and references to WCAG compliance should be clearly defined and supported by explanatory guidance and examples. They also questioned whether some requirements, particularly accessibility requirements, should be stronger than a "Should" obligation if the long-term aim is universal compliance. LB confirmed that the summer consultation would include additional explanation, definitions and illustrative examples to provide greater clarity. They explained that WCAG compliance had been positioned as a "Should" because organisations are at different levels of accessibility maturity and may require time to reach full compliance. However, they reiterated that the ambition is to support highly inclusive consumer journeys. MPW added that the project team had also debated internally whether accessibility should be a "Must" or a "Should". While there is agreement on the importance of WCAG compliance, there remains an open question as to whether CCS should mandate broader accessibility requirements across ATPs' wider digital platforms.

Several members questioned the practical value of non-mandatory requirements. One noted that many energy industry websites currently fail to meet WCAG 2.2 AA standards and questioned what consequences would exist if ATPs simply chose not to follow a "Should" requirement. They suggested that aspirations without any assurance mechanism may have limited impact.

Another member that the guidelines should not seek to dictate how organisations run their businesses. They suggested that even non-mandatory recommendations can promote better customer experiences by encouraging organisations to consider accessibility and usability improvements they may not otherwise have prioritised. Another member similarly supported retaining flexibility, noting that organisations are best placed to design customer journeys that meet their customers' needs. They emphasised that the purpose of the guidelines should be to encourage simple, understandable and transparent permission journeys rather than prescribe detailed website design requirements.

Another member noted that the primary objective for CCS is not strict compliance with individual wording requirements but rather the creation of a consistent and recognisable experience that Consumers can trust. By encouraging common patterns and approaches

across ATPs, the guidelines aim to increase consumer confidence, familiarity and adoption of CCS-enabled services over time.

LB introduced the first set of pre-consent CEGs covering the "inform and request" stage of the consumer journey. A member questioned how many of the proposed "Must" requirements could be objectively assessed. They noted that many appeared to rely on subjective concepts such as whether information had been explained sufficiently or whether language was reasonable and understandable, making it difficult to determine how compliance could be consistently measured. MPW explained that the immediate purpose of the session was to validate whether the right activities had been identified as mandatory, recommended or optional, rather than to finalise assurance methodology. They reiterated that the requirements remain design assumptions and would continue to evolve through stakeholder engagement and consultation.

A member raised concerns regarding one of the proposed requirements relating to ID&V for access to meter data. They noted that the wording appeared to imply that ID&V is always required to access meter data, which is not necessarily consistent with existing SEC arrangements. The member added that data can currently be accessed through Other Users without the same ID&V processes envisaged by CCS and suggested that the requirement could mistakenly imply a broader change to existing access arrangements. MPW responded that the CEGs are intended to be sufficiently future-proof to support CCS across a range of data-sharing scenarios, including future developments beyond the initial scope of MMP. However, they agreed that terminology would need to be carefully reviewed to ensure consistency with existing SEC processes and to avoid creating confusion about the relationship between CCS and existing data access routes.

The discussion expanded into the distinction between meter data, personal meter data, and consumption data. A member highlighted that only a relatively narrow subset of smart meter data currently requires Consumer consent, with many other data items capable of being accessed under alternative legal bases. They argued that references simply to "meter data" were too broad and risked creating ambiguity. Another member agreed and added that requirements should clearly identify the specific data types intended to fall within CCS scope. They suggested that terms such as "consumption data" or another more precise description would reduce confusion and prevent misinterpretation.

Another member cautioned against viewing the CEGs in isolation, noting that the guidelines form part of a broader package of REC documentation, onboarding processes and governance controls. They added that they thought the intent of the requirements was largely appropriate and designed to support organisations participating in CCS rather than impose standalone obligations disconnected from the wider framework. MPW agreed, emphasising that the requirements would be accompanied by additional documentation, context and supporting processes. They noted that the project team is attempting to strike an appropriate balance between specifying mandatory behaviours within REC governance documents and retaining sufficient flexibility to evolve supporting guidance over time without requiring formal code changes.

LB moved onto the redirect and return stage which concerns the point at which an ATP hands a Consumer over to CCS to complete account creation, ID&V and the granting of permission, and then receives the Consumer back into the ATP environment once that CCS interaction has concluded. The requirements shown for this stage were largely categorised as Must, with a smaller number categorised as May.

A member asked whether the proposed journey had been modelled as a demonstrable end-to-end Consumer experience, including the number of screens and steps that a Consumer would need to complete. They warned that if the journey becomes too lengthy or information-heavy, Consumers may abandon it before completing the permission process. MPW confirmed that the team is developing and iterating journey concepts and intends to make them available alongside REC drafting to show how the requirements would work in practice, although they were not ready to be shared during this session.

A member queried why a reference to plain language appeared within a May requirement, given that Consumer-facing communications should be clear and understandable as a baseline. LB clarified that the intended emphasis of that requirement was not on plain language itself, but on whether ATPs provide an additional purpose description alongside the purpose code. MPW added that there is already an overarching plain-language requirement elsewhere and agreed that the wording in this particular requirement may be creating unnecessary confusion. They agreed to review and clarify the drafting.

LB then moved to the granting stage, which concerns the point after a consumer has completed the CCS journey and granted permission, and is then returned to the ATP. MPW clarified that CCS itself will confirm the outcome of the consent journey, but ATPs may wish to provide further context about what that successful permission means for their own service or product journey.

A member suggested that where a Consumer chooses not to grant permission, the ATP should be required to explain the impact on the service or contract, rather than this being expressed only as a Should. They noted that, depending on the service, the Consumer may not be able to proceed without granting the relevant permission. LB explained that the original drafting had considered possible alternative routes or services that might be available if permission was not granted.

A member raised a broader concern about the relationship between CCS screens and ATP screens. They had understood that CCS would define the consumer-facing consent journey, but the requirements appeared to suggest that ATPs might also provide success or outcome screens. LB explained that CCS would provide confirmation that permission had been granted, while an ATP might choose to provide additional service-specific information once the consumer returns to its own environment. The member cautioned that duplicative or overly granular screens could make the journey interruptive and reduce completion rates, drawing on experience from financial services where excessive permission prompts caused consumers to abandon journeys. MPW agreed that the full Consumer journey needs to be considered from the user's perspective, rather than treating the CCS and ATP elements in isolation. They noted that

any ATP outcome screen should avoid duplicating what CCS has already told the Consumer and should only add value in the context of the ATP's service.

A member suggested that one of the granting-stage requirements, relating to data being retrieved after permission is granted, might sit more naturally earlier in the journey, before consent is granted, so that the consumer understands the consequence before making a decision. MPW acknowledged that this aligns with ongoing internal discussions about the consent scheme and confirmed that this point would be considered further in a future Solution Group meeting.

5. TECHNICAL DESIGN: TOKEN LIFETIME (JWT)

GR advised that the group would revisit the previously proposed approach of mandatory token introspection and seek feedback on a new preferred approach based on JSON Web Tokens (JWTs). GR explained that the original design relied on opaque tokens and mandatory introspection. Under this model, the token itself contains no meaningful information and acts only as a reference. Each time an EDH receives a request, it must contact CCS to validate the token and retrieve the associated consent details.

While this approach supports strong security and data minimisation principles, feedback from stakeholders highlighted drawbacks. In particular, mandatory introspection creates a hard dependency on CCS being available whenever data is requested. To address these concerns, the team is now proposing the use of JWTs, which can contain the relevant consent information within the token itself and therefore reduce the need for real-time validation calls to CCS.

Members generally welcomed this direction. One member noted that the overall impact depended heavily on what information would ultimately be included within the token, while another expressed support for moving towards JWTs because they are widely adopted industry standards and reduce unnecessary API calls.

Discussion focused on how much information would need to be embedded within JWTs. A member observed that, for an EDH to make a sharing decision without checking CCS, the token would need to contain details relating to the data requested, the associated consent and some form of property or service identifier.

GR and CE clarified that the detailed schema is still being developed and will be discussed further at a dedicated session. They stressed that the current discussion is primarily about the validation mechanism rather than the exact content of the token. CE further noted that whether CCS uses introspection or JWTs, the EDH ultimately needs access to consent information to determine whether data should be shared.

CE outlined the key trade-offs between introspection and JWTs, focusing on four areas: sharing during a CCS outage, consent revocation delays, additional ecosystem and API load, and overall platform availability. Under an introspection model, every data request requires a live validation call to CCS, meaning data sharing would stop entirely during an outage. Under a JWT model, a valid token can continue to be used while it remains active, meaning data sharing can continue even if CCS is temporarily unavailable. However, this introduces a trade-off. If a Consumer

revokes a consent while a token remains valid, the consent revocation cannot fully take effect until the token expires. The token lifetime therefore directly determines the maximum delay before a revocation is enforced across the ecosystem.

To balance resilience and consumer protection, the project team proposed a 30-minute token lifetime, broadly aligned with half-hourly settlement data intervals. Under this model, data sharing can continue for up to 30 minutes during a CCS outage. A revoked consent could, in theory, continue to allow data sharing for up to 30 minutes if a valid token already exists.

A member questioned whether a 30-minute token lifetime may be unnecessarily short, particularly given the projected availability levels for CCS and the relatively low likelihood of consent-relevant events such as a change of tenancy occurring within that timeframe. They suggested that longer lifetimes, potentially up to a day, may warrant consideration. CE explained that longer token lifetimes increase the maximum period during which revoked consents could remain effective. MPW confirmed that the proposed 30-minute lifetime remains a working assumption rather than a final decision. They noted that many comparable smart data ecosystems operate with even shorter token lifetimes and that interoperability with future cross-sector data-sharing schemes remains an important consideration.

A member questioned the practical value of JWTs in scenarios where ATPs require ongoing access to data. They noted that if tokens had short lifetimes, ATPs would still need to contact CCS regularly to obtain new access tokens before retrieving data. In such circumstances, they suggested the reduction in CCS dependencies may be less significant than it initially appears.

CE and MPW acknowledged the point, explaining that this follows the standard FAPI and Open Banking model whereby long-lived refresh tokens are used to request short-lived access tokens. The refresh token remains associated with the underlying consent, while access tokens provide the mechanism by which ongoing consent validity is continually checked.

A member sought clarification on consent duration. MPW explained that the current thinking is for consents to have a maximum lifetime of three years, although this remains subject to further discussion. Refresh tokens would remain aligned with the duration of the underlying consent while access tokens would operate on much shorter timescales.

A member asked how EDHs would validate JWTs locally. CE explained that JWT validation would follow established internet standards. Tokens contain a cryptographic signature which can be checked against CCS public signing keys. EDHs would cache CCS signing keys and perform local validation without needing to contact CCS for each request. A member highlighted the importance of ensuring that signing-key refresh policies remain aligned with token lifetimes.

CE highlighted that the CCS platform is being designed around a contracted availability target of 99.9%, with deployments and maintenance intended to follow a zero-downtime approach. They noted that similar architectures are already used successfully in large-scale smart data ecosystems internationally, including Open Banking and Open Finance implementations handling millions of consents and billions of requests.

A member asked whether these technical decisions would be presented through consultation in a way that allowed both technical and non-technical stakeholders to understand the implications. MPW confirmed that future consultation documents would include both the technical proposals and plain-language explanations of the rationale, trade-offs and impacts, ensuring stakeholders can provide informed feedback regardless of their level of technical expertise.

6. FORWARD PLAN

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

The next Topic Solution Group meeting on 22 July will be held instead of the planned Engagement Webinar, which will be rescheduled to a date in September MPW advised that agendas for the Topic Solution Groups scheduled for 22 and 29 July will be confirmed 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.

RETAIL ENERGY CODE

ATTENDEE ORGANISATIONS

Attendee	Representing	Initials	Role
Matt White	Retail Energy Code Company	MPW	Chair
Liana Bakar	Publicis Sapient	LB	Presenter
George Roberts	Retail Energy Code Company	GR	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
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