recco

The Consumer Consent Solution

CCS Engagement Day Q&A

Published: 12th March 2026

Contents

Will CCS sit alongside, rather than replace, existing consent solutions already live in the market (e.g. DCC Other User arrangements)?

The proposed CCS is intended to provide a central, standardised mechanism for capturing, recording and managing consent, while operating within a hybrid model where data continues to flow directly between market participants. For MMP, RECCo's approach is to minimise the impact on existing and future DSAs, not to replace all existing arrangements overnight. Existing SEC Other User consents are not proposed to be migrated into MMP; instead, the current assumption is that new consent records would be created in CCS as existing consents come up for renewal. The consultation is also explicit that organisations remain responsible for determining when consent is required and for lawful reliance on that consent.

Are SEC-approved ID&V models considered valid?

The consultation recognises that existing mechanisms used by SEC Other Users and their customers may, in some cases, provide a valid means of confirming identity and linking an individual to the relevant MPxN. For the initial MMP, the current design assumption is that the CCS would use centrally governed authentication and verification processes rather than relying on ID&V checks conducted by individual ATPs. The consultation also leaves open the possibility that this could be revisited in future, where ID&V undertaken by CCS Users is shown to meet the required minimum standard.

A guest account is usually used to buy a one-off product on a website, not for this level of data. How will this work in practice?

The consultation recognises that some consumers may wish to grant consent through a simpler, one-off interaction, without creating a full CCS account. The proposed guest journey is intended to support this type of use case by reducing friction in the consumer journey, particularly where a consumer only needs to grant consent once or infrequently.

Importantly, using a guest journey would not reduce the level of identity assurance required. Consumers would still be redirected to the CCS and complete the same identity verification process to confirm they are authorised to provide consent for the relevant MPxN(s).

The guest route is designed to simplify the account creation aspect of the journey, while identity verification and consent requirements would remain consistent regardless of whether a consumer uses the guest journey or creates a CCS account.

How will ID&V work for people without a photo ID?

For the Minimum Marketable Product, the consultation proposes that access to half-hourly metered data should be supported by a high level of identity verification confidence, aligned with the Government's Good Practice Guide 45 (GPG45). The current proposal is to include a mechanism for photo identification in the ID&V process. The CCS is expected to initially integrate with at least one identity verification provider, with the potential to support a broader range of trusted ID&V solutions over time. While this approach aims to provide strong assurance for consumers and market participants, RECCo recognises the importance of accessibility and will continue to consider additional trusted ID&V options as the solution evolves.

How will consumers manage consent when using the guest journey?

Where a consumer grants consent through a guest journey rather than creating a CCS account, they will

manage that consent directly with the Authorised Third Party (ATP) that granted it. ATPs will be required to support clear, consistent processes for consent management, including renewal, revocation, and dispute handling. RECCo is also exploring whether a future enhancement could allow consent records created through guest journeys to be linked to a CCS account if a consumer later creates one, enabling them to view and manage these consents centrally.

If a customer has a guest account, how will they get back to the consent and be able to revoke access to the dispute consent?

Where a consumer chooses to grant consent using the guest approach instead of creating an account, consumers will be able to view and manage their consent directly with the relevant ATP to which the consent was provided. ATPs will have clear requirements for managing consent revocation and renewal, with the CEGs ensuring consistency in how consumer interactions are delivered. If a consumer has a query or issue with the consent record, they would need to raise this directly with the ATP, with requirements placed on ATPs to have appropriate query and dispute processes in place.

We're exploring the feasibility of a mechanism that would allow consolidating consent records created through the CCS if the consumer later chooses to create an account. This would allow them to view and manage consent records through the CCS central portal. However, more work is required to confirm if this can be done safely and securely once the technical partner has been selected.

What will a consumer need to provide to meet ID&V checks?

The consultation proposes that the ID&V process should meet a high-confidence assurance level, including mechanisms that use photo identification. The specific documents or processes that may be accepted will be confirmed during procurement and detailed technical design.

Will a different legal framework apply to monthly or annual data?

The CCS MMP is focused on access to half-hourly metered data for domestic premises. The CCS roadmap sets out expectations regarding the phased extension beyond MMP. One of these future phases is expected to include access to data relating to non-domestic premises, with permission to access such data also expected to be recorded within the CCS. With regard to monthly or annual data, the risks and required controls around data sharing are lower than for half-hourly data and are therefore not treated as a priority use case.

Does ISO27001 or Cyber Essentials scope matter?

Organisations wishing to participate in CCS will be required to hold Cyber Essentials Plus or ISO27001 certification.

Where ISO27001 certification is relied upon, the scope of certification must cover the systems, processes and activities relevant to CCS participation and the handling of associated data.

Does the ICO guidance obtained include re multiple occupancy, considering it's unlikely to remain personal data?

In developing the CCS approach, we have considered relevant Information Commissioner's Office (ICO) guidance, wider UK GDPR principles, and legal advice, including how personal data should be treated in circumstances where information may relate to multiple individuals at the same address.

There is no specific ICO guidance on the treatment of energy data in multi-occupier premises. However,

we have had regard to a range of ICO guidance that is relevant to the issues raised, including the ICO's Guide to the UK GDPR, in particular guidance on what constitutes personal data and when information is considered to "relate to" an identifiable individual; guidance on lawful bases for processing personal data; and guidance on data minimisation and the prevention of unauthorised disclosure.

This proposal has been developed in reference to the current UK GDPR framework. The Data (Use and Access) Act 2025 amends but does not replace the UK GDPR, and it does not alter the core definition of personal data or the requirement that a lawful basis must apply where personal data is processed. The Act introduces further clarification around the application of data protection concepts, including proportionality and reasonableness in assessing identifiability, and we will continue to take account of relevant ICO guidance as those provisions are implemented.

We recognise that data protection considerations in multi-occupier premises are complex and context-dependent. We therefore intend to engage with the ICO to discuss the approach taken and will consider any relevant feedback or guidance alongside the wider regulatory framework.

Can more than one person at a premises have a CCS account?

Yes. Individuals will be verified independently to confirm whether they have the right to provide consent for access to data relating to a specific MPxN.

In some cases, particularly in multi-occupancy households, more than one individual may legitimately be associated with a single MPxN.

Where this occurs, the approach set out in the consultation for multi-occupancy consent management will apply.

When a consumer checks CCS to see who is accessing data, would it show details on all data being accessed on the premises, regardless of who gave consent?

Yes, provided the consent was granted through the CCS. This is set out within paragraph 8.72 of the consultation document.

How long will it take to get the data spec and schedule through? There is not much time until Q1 27 if people need to build APIs and connection points?

The current plan is to issue the draft API technical specification, defining the interactions required for granting and validating consent, for industry consultation in summer 2026, alongside the proposed changes to the data specification. Whilst the legal drafting will not be formally approved until January 2027, we expect early adopters to commence their build and test activities using the baselined API technical specification, which will be made available later in quarter 2, early quarter 3 2026, based on current timing estimates. As the REC is not mandating that CCS replace pre-existing processes from day one, it will be for individual organisations to determine when to commence their delivery activities and when to start using the CCS (subject to any wider mandates, e.g., for the inclusion of tariff data consent).

What will the requirements be for EDPs, etc, to be able to connect to CCS? How will this link to the data tokens and receive the data?

The consultation proposes that organisations wishing to participate in the CCS ecosystem, including ATPs and EDPs, will need to complete an accreditation process. This is expected to include verification of

organisational identity, confirmation of appropriate information security and data protection arrangements, and technical onboarding and testing.

From a technical perspective, the CCS will issue a consent token linked to the authorised party. When an ATP requests data from an EDP, it will present this token as evidence that valid consent has been granted. The EDP will then be able to check the status of that token with the CCS before sharing the requested data.

Further details on the technical specifications and onboarding requirements will be shared during the detailed design and implementation phases.

What timeline do you have for the user pays introduction? Will these user pay charges be published publicly to ensure costs are fair and not supplier-heavy?

The position relating to CCS funding is set out in consultation paragraphs 8.26 to 8.32. There is currently no policy position indicating that CCS will move to a user-pays mechanism; however, this is one of the options under consideration. Views are being sought on the most appropriate enduring funding mechanism, as well as the initial time period or other pre-conditions, before the agreed position is reconsidered. The agreed funding mechanism will be transparently reflected within the REC Charging Methodology, with lower-level details included in the annual REC Charging Statement.

Has data that is accessed via a CAD over the HAN been considered?

This is not a scenario we have considered in detail. The consultation document sets out the core scenario captured by the MMP: an EDP shares data with an ATP that provides a service to a consumer. It would be helpful for respondents to provide details of scenarios which do not fit into this model to support our ongoing work.

Why does CCS accreditation seem low for a platform aiming to build trust in data sharing, and how will enforcement and monitoring be handled?

The proposed accreditation approach seeks to balance the need for a robust assessment to ensure organisations have appropriate processes and controls in place for managing consumer data, with the need to minimise barriers to entry for organisations seeking to access consumer data to offer services that facilitate consumer-led flexibility.

The proposed accreditation arrangements will work in parallel with ongoing monitoring and assurance to mitigate the risk of data breaches and help build consumer trust. This monitoring and any required enforcement action will be managed via the existing REC assurance framework.

Will the portal show all parties involved? For example, if an ATP provides data to a PCW with an app, will it show all three parties, or just the ATP?

The consultation proposes that consumers will be able to see which organisation is accessing their data and the purpose for which consent has been granted. This is intended to provide consumers with clear visibility of who is using their data under the consent record. At this stage, the minimum expectation for MMP is transparency around the organisation accessing the data under consent.

Further details on how additional parties may be represented, where relevant, will be considered through the detailed technical design and REC drafting process as the CCS design is developed.

How does CCS become aware that a consumer no longer has the right to provide access to data (e.g. no longer the consumer at the premises)?

As the Data Controller under GDPR, the ATP will have overall responsibility for ensuring that data is accessed only where consent is in place. Therefore, where the ATP becomes aware that the consumer is no longer the data subject in relation to a specific MPxN, they should ensure consent held within the CCS is revoked.

In addition, consumers will be required to confirm they are still living at the property when new consent is granted. Where the CCS becomes aware that the individual is no longer the data subject for a specific MPxN, all associated consents will be treated as revoked.

Rather than using mTLS, could we simplify and achieve the same with strong signing and TLS 1.3 for all, except for to CCS-to-EDP integration, which is the highest risk?

The consultation seeks stakeholder views on adopting FAPI 2.0 as part of the CCS security model. Under this approach, mutual TLS (mTLS) would be used for data exchange across the ecosystem.

The proposed rationale for this approach is to support a consistent and robust trust framework, including sender-constrained tokens, strong authentication between parties, and interoperability across the ecosystem. The consultation notes that consistently applying mTLS helps maintain the integrity of the security model and the benefits of the FAPI 2.0 standard.

Stakeholders are encouraged to share their views through the consultation on the proposed security approach, including whether alternative models could deliver equivalent levels of assurance while maintaining interoperability and security across the CCS ecosystem.

What happens when a consumer revokes consent? How will this be communicated to data-sharing parties?

When a consumer revokes consent directly through the CCS, the associated token will be updated to reflect the revocation. This change would then be communicated to the relevant Energy Data Provider (EDP) and Authorised Third Party (ATP).
Where consent is revoked directly with the ATP, the ATP would be required to notify the CCS so that the corresponding token can be updated to reflect the revocation. This update would, in turn, inform the relevant EDP.
The specific mechanisms for how these notifications will operate are still to be determined, and further details will be developed as part of the ongoing design. As such, the description above should be considered indicative at this stage.
It should also be noted that EDPs will be required to confirm that valid consent is in place (via token introspection) before sharing data. As a result, they should not rely solely on the receipt of revocation notifications.

Does this have the potential to overwrite existing PSR (Priority Services Register) obligations?

The CCS is not expected to directly overwrite any existing REC obligations. However, if it is determined that access to PSR data should be managed via the CCS, a change to the existing PSR requirements will be progressed in line with any required changes to the CCS to support consent for sharing PSR data.

When will the procurement process be completed? 1 year is not much time for parties if they need to build APIs, etc., to connect to this solution?

The consultation confirms that RECCo is currently progressing through a formal procurement process, with the request for proposals issued in January 2026. As procurement is still underway, some elements of the detailed solution design cannot yet be shared. RECCo recognises the importance of providing sufficient implementation time for market participants. To support this, the programme is exploring ways to reduce delivery risk, including the use of established technical solutions where possible and early design prototyping. Further details on the technical specifications and REC drafting are expected to be shared through stakeholder working groups and as part of the planned consultation on the detailed design in summer 2026, which will help participants prepare for implementation.

What happens when the data does not match for MPAN, MPxN? What will the consumer need to do to achieve the desired low-friction journey?

We recognise that there will be instances where it will not be possible to match the consumer to a specific MPxN and that this will require an exception process. Further work will be undertaken, in consultation with the working groups, to map exception processes and resolution mechanisms.

Data accuracy across the industry is a challenge now. How will this be addressed in CCS?

The inclusion of the CCS within the REC enables RECCo to understand how the CCS will be affected by broader retail data issues, e.g., addressing data quality. It also allows us to consider how data captured through CCS processes can be used to facilitate the resolution of these wider retail data issues. The CCS team is working closely with RECCo colleagues and feeding into wider performance assurance activities to ensure any risks associated with the CCS are reflected in the overall Retail Risk Register, and that activities to mitigate these risks are captured in the Performance Assurance Operating Plan.

Given the potential complexity of disputes in this area, what arrangements will be in place to ensure the Ombudsman can effectively consider and resolve these cases?

Discussions with the Energy Ombudsman are ongoing. Further information regarding the approach to customer redress will be shared through the working groups.

How will consumers learn about the portal, and who will be responsible for publicising this? Will there be an equivalent to Smart Energy GB, and who pays for it?

The consultation recognises the importance of ensuring that the CCS portal is trusted, recognisable and accessible to consumers. As part of the design work, RECCo is considering how the portal should be presented to consumers, including whether it may be delivered under a recognisable brand or a dedicated identity

The consultation does not yet set out a specific approach to consumer awareness activity or confirm whether there would be a programme equivalent to Smart Energy GB. Similarly, arrangements for funding any future awareness or communications activity have not yet been finalised.

These aspects will be considered further as the CCS design develops, and stakeholder views on how best to support consumer awareness and engagement are welcome through the consultation process.

What does a consumer see in the CCS? For example, service provider (not ATP), what data is being accessed and when? Or is it just a record of ATP consent?

The consultation proposes that consumers will be able to view key information about the consents associated with their data through the CCS portal. This is expected to include details such as which organisation holds consent to access the data, what data is being shared, when consent was granted, and when it is due to expire.

Consumers would also be able to manage their consents, including the option to renew or revoke consent and to raise concerns if anything appears unexpected.

CCS will focus specifically on consent-based data access. For example, it would not display the identities of other individuals linked to the same MPxN, nor would it provide visibility into wider data-sharing arrangements that fall outside the CCS consent framework.

If there are all similar initiatives, all of which will be a cost to consumers, how does all this happen whilst also reducing energy bills?

The Ofgem April 2025 directive outlines the vision for a centralised consumer consent solution to manage consumer permissions and provide consumers with visibility and control. While RECCo collaborates with other organisations advancing smart data initiatives, such as Elexon's delivery of the Smart Data Repository and NESO's development of the Data Sharing Infrastructure, we do not believe there is duplication between these projects and the delivery of the CCS. These smart data initiatives are connected by a shared goal to enable broader access to energy data, which should lead to increased consumer-led flexibility, benefiting consumers and helping the government achieve its Clean Power 2030 action plan.

How do you make the distinction between domestic and commercial?

The CCS MMP is intentionally scoped to support only domestic consumers. It is the responsibility of the ATP to determine whether consent is required for the service they are providing, including whether the individual is a domestic consumer and whether the data required falls within the scope of the CCS.

Where the ATP determines that:

- The individual is a domestic consumer, and
- consent is the appropriate lawful basis for accessing the required energy data.

The ATP must utilise the CCS to obtain and validate that consent.

The CCS, therefore, serves as the mechanism for capturing and managing consent, but it does not replace the ATP's responsibility to determine whether consent is required or whether the scenario falls within the domestic MMP scope.

Where the ATP determines that the consumer is non-domestic/commercial, or that access to data is based on another lawful basis, at MMP, the CCS would not be used.

Lots of very qualitative concepts presented today based on 'the research'; moving

forward, could we see more quantitative basis/justifications for decisions?

RECCo recognises the importance of continuing to build a strong evidence base as the CCS design progresses. Consumer research and usability testing have played an important role in shaping the current proposals, particularly around the consumer experience and consent journeys.

Looking ahead, the CCS approach is expected to include ongoing monitoring, reporting, and evaluation, which will provide clearer quantitative insights into areas such as system performance, user behaviour, consumer experience, and data protection outcomes. This will help ensure that future decisions are informed not only by qualitative insight but also by measurable data and operational evidence.

The consultation also notes that the CCS roadmap will continue to evolve over time, drawing on monitoring data, assurance findings, stakeholder feedback and consumer insight as the solution moves from design into implementation and live operation.

Is consent just for HH consumption data, or also for HH export data? HH export data permissions have been overlooked in the past, but interest is growing.

The consultation deliberately refers to half-hourly metered data (rather than consumption data) because the solution is expected to cover both import and export data.

Who can I contact for more information?

Whether you have a question, concern, or want to stay informed, our dedicated Consumer Consent Solution team is here to help and collaborate with you. Contact us at:
consumerconsent@retailenergycode.co.uk