Consultation Response

Response to the Consumer Consent Solution Design Consultation

Published 28 May 2026

Contents

Response to the Consumer Consent Solution Design Consultation

Introduction

Thank you to all stakeholders who responded to RECCo's consultation on the Consumer Consent Solution (CCS) Design. We received 31 responses across the 32 questions set out within the consultation document. Allowing for no-comment and null responses, this resulted in 645 individual comments, all of which have been reviewed and considered. Full copies of the individual non-confidential responses have been published on the RECCo website here:https://retailenergycode.co.uk/our-programmes/consumer-consent-solution/

We appreciate the time, expertise and care stakeholders invested in their responses. Many respondents welcomed the ambition to give consumers clearer control over consented access to their energy data and supported developing a centralised solution to enable wider, secure access to that data. Others challenged key aspects of the proposed design, including the overall case for CCS, its proposed scope, the approach to identity verification, alignment with existing Smart Energy Code (SEC) arrangements, cost and implementation burden, and the risk of excluding consumers who cannot easily use digital journeys.

This feedback has directly influenced our next phase of work. In some areas, it has reinforced the proposed direction of travel; in others, it has identified issues that require further evidence, legal clarification, policy consideration or design iteration before final positions are reached. This document, therefore, sets out what we heard, how that feedback is shaping the CCS design, where RECCo is changing or refining its approach, and where further input will be sought before final REC drafting is consulted on in summer 2026.

The positions below should be read as an interim response. They do not close down further engagement. RECCo will continue to work with Ofgem, DESNZ, delivery partners, consumer representatives and market participants through bilateral discussions and working groups as the lower-level CCS design, operational model and REC drafting are developed.

How stakeholder feedback is shaping the CCS design

A clear message from the consultation is that stakeholders want RECCo to show not only that feedback has been heard, but also how it is being used. In response, the next phase of CCS design will focus on four areas:

- clarifying the legal and operational basis for who can give consent, including the interaction between occupiers, bill payers, suppliers, landlords and multi-occupancy households;
- reducing avoidable duplication between REC and SEC arrangements, particularly around assurance, accreditation and existing consent processes;
- testing the proportionality and usability of the consent journey, including IDV, MPxN association, consent confirmation, consumer messaging and trust signals; and
- making the implementation pathway clearer, including continued cost transparency, the development of robust transition arrangements, focused EDH adoption planning and the evolution of the future roadmap beyond the Minimum Marketable Product (MMP).

The CCS Design Consultation set out high-level design positions across policy, technical design, user experience, governance and the future roadmap. We have carefully considered all consultation responses and stakeholder feedback received. This response does not address every individual consultation question. Instead, it focuses on the most prominent or frequently raised themes from stakeholders and explains how RECCo is responding to them. A

more detailed analysis and our overall conclusions will be provided alongside the proposed REC legal text within the summer REC drafting consultation.

Summary of Consultation Themes

The table below summarises the main themes. A more detailed analysis and our overall conclusions will be provided alongside the proposed REC legal text within the summer REC drafting consultation.

Table 1: Overarching themes

Theme	What stakeholders told us	How is this shaping the CCS design
MMP Scope	Many respondents supported a phased MMP scope. However, others challenged whether the CCS scope goes far enough, highlighting the importance of providing consumers with visibility of all organisations accessing their data. Respondents noted that careful messaging will be needed during the transition period to ensure consumers understand that only a subset of consents may initially be visible. Some respondents also questioned the case for a centralised consent solution, suggesting CCS should build on existing consent mechanisms already implemented by SEC Other Users. Views were similarly mixed regarding the inclusion of Elexon's Smart Data Repository (SDR) and SEC Other Users as Energy Data Holders (EDHs). Some respondents felt CCS should focus primarily on interactions with Smart DCC, while others suggested the SDR should act as the sole EDH. From a technical perspective, concerns were raised that some requirements extend beyond the original intent of CCS, including the introduction of minimum technical thresholds such as mTLS. Further detail on the use of mTLS is included under the security standards theme below. Several respondents also referenced the potential extension of CCS into the non-domestic market. Views were mixed, with some supportive of expansion, while others highlighted the need for careful consideration, particularly in relation to identity verification (ID&V) requirements.	We recognise the concerns raised regarding the limited scope of delivery through the CCS MMP, and we understand the ambition expressed by some stakeholders, particularly consumer bodies, that CCS should ultimately give consumers visibility of all organisations accessing their energy data. We agree that this is an important objective and the inclusion of CCS as a foundational part of the future energy digital ecosystem within the Energy Digitalisation Framework[1] should give additional confidence that CCS will iterate beyond MMP. However, stakeholder feedback has also emphasised the need to carefully manage delivery complexity, operational risk, and consumer trust. On that basis, we continue to believe that a phased approach, beginning with the MMP and supported by a defined future roadmap, is the most effective way to deliver a secure, scalable and implementable solution. As detailed design progresses, we will continue to explore whether appropriate "quick wins" can be incorporated where feasible and without compromising delivery confidence. We will also place particular emphasis on the UX workstream to ensure consumer communications are clear and transparent, especially during the transition period when only a subset of consent arrangements may initially be visible. This will be important in helping consumers understand what CCS does, what it does not yet cover, and how its scope is expected to develop over time. We recognise that there are differing interpretations of Ofgem's decision to adopt a "hybrid" model, with some respondents interpreting this as implying a more decentralised approach to

[1] Energy Digitalisation Framework: A vision for a coordinated and connected energy system

Theme	What stakeholders told us	How is this shaping the CCS design
		both consent management and data sharing. Ofgem's decision establishes two key principles: a system-wide mechanism for consumers to grant and manage consent, and a data model that retains decentralised characteristics. On this basis, CCS is being developed as a centralised consent layer, while data sharing continues across a decentralised ecosystem of data holders. This approach provides a single, consumer-centric and trusted framework for consent, reducing fragmentation across multiple ATP journeys and avoiding the need for consumers to repeatedly establish their identity when engaging with different services, without centralising the underlying data itself. We will continue to work with Ofgem and stakeholders to ensure the CCS design reflects the intent of the decision while remaining practical and interoperable. Regarding Energy Data Holders (EDHs) within the MMP, the CCS project team continues to assess EDH participation and adoption pathways, including ongoing engagement with Smart DCC and Elexon. This work is being considered alongside the wider DESNZ and Ofgem scoping activity on access to smart metered data, so that CCS design decisions remain aligned with the broader policy and delivery landscape. We also acknowledge the mixed views received regarding any future expansion into the non-domestic market. These perspectives will be considered as part of future CCS roadmap development, particularly in relation to identity verification, proportionality and the practical differences between domestic and non-domestic customer arrangements. CCS is being developed using a phased approach, with an initial focus on the domestic market, recognising that additional considerations will be required as the service expands into the non-domestic sector. We will establish specific engagement with those experienced within the non-domestic sector when our scoping work begins on this expansion. The non-domestic market covers a broad range of premises and customer types. Some — such as sole traders operating from home — may relate to identifiable individuals and therefore engage UK GDPR considerations. Others are purely commercial or organisational premises, where half-hourly metered data would not constitute personal data under UK GDPR. We therefore

Theme	What stakeholders told us	How is this shaping the CCS design
		recognise the importance of fully exploring how the CCS model should operate within the non-domestic market, ensuring robust and secure access arrangements while avoiding unnecessary or impractical requirements for non-domestic consumers and their authorised representatives.
Consumer (occupier) versus Customer (bill payer)	Most respondents agreed with the position that, under UK GDPR, the occupier is the data subject in relation to half-hourly metered data. However, a number of respondents qualified their support by highlighting the practical implications of moving to an occupier-led consent model. In particular, respondents noted that existing arrangements under the SEC Privacy Controls Framework do not explicitly distinguish between the occupier and the bill payer. Suppliers also explained that their systems and processes are generally built around the account holder, and that they do not routinely hold information about non-account-holder occupants. Several respondents, therefore, questioned how an occupier-led consent model would work in practice, including who would be responsible for identifying and recording occupier details where they differ from the account holder. Some suggested that a pragmatic compromise may be needed, noting that the occupier and account holder are expected to differ only in a minority of cases. Respondents also raised concerns that introducing an occupier-led model alongside existing consent arrangements could create parallel or conflicting consent frameworks, increasing complexity for consumers and market participants. Further questions were raised about multi-occupancy households, including how CCS would establish or evidence that an individual has the appropriate authority to provide consent in those circumstances.	This is one of the areas where consultation feedback has prompted further work before a final design position is confirmed. In light of the existing arrangements for managing consumer consent, RECCo is reviewing its previous legal advice and engaging with the ICO to test the consultation position that consent for access to half-hourly metered data can only be provided by the occupier. This work will consider whether practical compromises are available that focus on demonstrating a link between the individual providing consent and the relevant consumer premises or MPxN, rather than requiring confirmation that the individual is the occupier. It will also consider the position for HMOs and other multi-occupancy scenarios, including circumstances where a non-occupier landlord may be able to access data under an alternative lawful basis, while not being able to provide consent for that data to be shared more broadly. RECCo is also engaging with SECCo to support alignment between the REC and SEC positions. This position will be developed in discussion with Ofgem and DESNZ, informed by feedback from the ICO. In parallel, Ofgem is gathering further evidence from suppliers on current practice, with this feedback expected to inform any future Supply Licence changes. The summer consultation will set out the proposed position, the evidence relied on, and any remaining areas where further stakeholder input is needed.
Smart Energy Code (SEC) Alignment	A strong and repeated theme was the need for greater clarity on how CCS will interact with existing SEC consent and assurance arrangements. The specific issues relating to the occupier and	We agree that CCS cannot be designed in isolation from existing SEC arrangements. We are working with SECCo to define the boundary between REC and SEC assurance and accreditation activities, to provide clarity on the scope of assurance under each

Theme	What stakeholders told us	How is this shaping the CCS design
	bill payer position are addressed above and are not repeated here. Respondents encouraged RECCo to carefully consider how any transition between existing arrangements and CCS would be managed, particularly where parallel consent models may operate for a period. They noted that this could create additional complexity for market participants and may be difficult for consumers to understand without clear communication and guidance. Some respondents also asked for further clarity on the intended long-term relationship between CCS and existing SEC consent mechanisms, including whether CCS is expected to replace aspects of current arrangements over time and how this would be reflected in the SEC. Assurance was another area where respondents sought further detail. In particular, they asked how the boundary between CCS and SEC assurance would be defined, so that onboarding, accreditation and assurance activities are proportionate, coordinated and avoid unnecessary duplication of activities and costs.	code, avoid duplication and costs, and retain appropriate safeguards for consumer data. We recognise the importance of a robust assurance framework for CCS Users, particularly to ensure that organisations accessing data through CCS have appropriate controls to prevent data misuse or leakage and can meet their obligations under data protection legislation and the REC Access Agreement. This needs to work alongside SEC assurance activities, which focus on the mechanisms by which Other Users collect consumer consent. We are working with SECCo to agree on an approach that recognises CCS within the SEC and to consider whether there are opportunities to reduce the burden associated with the SEC privacy audits where Other Users are obtaining consent via the CCS. We also agree that the transition will need to be carefully managed when SEC Other Users participate in both SEC and REC arrangements. The summer consultation will set out more clearly how existing SEC processes will interact with CCS, where responsibilities sit, and how CCS is expected to support the direction of travel under the Energy Digitalisation Framework.
Identity Verification	Respondents expressed mixed views on the proposed approach to identity verification (IDV). Some supported strong IDV as an important safeguard to protect consumers from unauthorised access to half-hourly metered data. Others questioned whether the proposed approach was proportionate in all circumstances, particularly where the consent journey or data access request may present a lower level of risk. A number of respondents raised concerns that IDV could introduce friction into the consumer journey, particularly if it relies heavily on photo ID or digital verification routes. They noted that this could disadvantage consumers who are digitally excluded, do not hold suitable identity documents, or find digital verification difficult to complete. Several respondents asked whether identity checks already performed by suppliers or SEC participants could be reused, rather than requiring consumers to complete a separate CCS identity process. Others cautioned against relying on a single	We are continuing to assess the level of IDV required for the CCS MMP, including the proportionality of the approach across different consent journeys and data access scenarios. This includes reviewing solutions used in other high-trust environments, such as government and banking, where both assurance and consumer participation are important. We recognise the suggestion that existing identity checks carried out by suppliers or SEC participants could potentially be reused. However, A core benefit of a centralised IDV model, compared with individual ATPs carrying out their own IDV processes, is that the CCS will hold the consumer verified identity centrally. In practice, this means that once a consumer has completed the initial IDV process, they should be able to authorise future data sharing requests without having to repeat identity verification each time regardless of the ATP or EDH in use for any data sharing – helping reduce friction and create a more streamlined consumer experience. Additionally, we need to ensure that the

Theme	What stakeholders told us	How is this shaping the CCS design
	IDV provider, arguing that this could create a closed, centrally controlled model that may not align with open data principles. Respondents also encouraged RECCo to consider whether the level of IDV should vary depending on the type of access being requested, for example, distinguishing between one-off access and enduring consent arrangements. Whilst the majority of respondents supported the use of the Enquiry Services to match the address to the specific MPxN; some respondents expressed caution around reliance on the Retail Energy Location, citing concerns regarding address data quality.	IDV approach provides a consistent level of assurance and consumer protection across CCS. We have listened to your feedback, we are exploring whether multiple IDV providers or a federated IDV model could form part of the MMP, helping to support consumer choice, resilience and reduced reliance on a single verification route. Alongside this, we are continuing to assess how the overall design can minimise unnecessary friction while still maintaining appropriate security and assurance safeguards. Alongside this, we are continuing to assess how the overall design can minimise unnecessary friction while still maintaining appropriate security and assurance safeguards. We note the concerns raised regarding address data quality and the potential impact on identifying the correct MPxN. Address data quality is an area where targeted assurance activity is progressing, and we are working with RECCo colleagues to further understand the impacts of this wider activity on the CCS arrangements. We recognise that the MMP will not address every inclusion challenge from day one. However, accessibility and inclusivity remain important design considerations, and further iterations will consider how more inclusive routes, including non-digital or assisted journeys, can be best supported by CCS over time.
Zero-trust consent checking model	Respondents broadly recognised the importance of strong, real-time consent assurance as a core principle underpinning trust in CCS. Many acknowledged that transaction-level consent validation provides greater confidence that each data share is supported by an active and valid consent record. However, respondents also raised concerns that real-time, per-transaction consent checks — referred to as introspection — could create performance, scalability and integration challenges as CCS usage grows. In particular, respondents questioned whether consent would need to be checked for every individual transaction, noting that some existing data-sharing patterns, such as scheduled or bulk access, may not align easily with a strict real-time introspection model. ATPs and EDHs also highlighted the potential for increased technical overhead,	We have carefully listened and considered concerns raised regarding mandatory introspection, particularly around performance, scalability and implementation impacts. We have sought bi-lateral discussions with a number of key potential adopters to better understand these concerns, and have worked closely with Raidiam to identify if there are any possible ways to flex or optimise the approach while maintaining the required security outcomes. Following further technical review, our current view is that introspection should remain a core part of the CCS design. However, we recognise the importance of providing stakeholders with clear guidance on how it will operate in practice, alongside reassurance on how the operational impact should be minimal.

Theme	What stakeholders told us	How is this shaping the CCS design
	alongside additional monitoring, resilience and error-handling requirements. Some respondents asked whether CCS could permit short-lived caching of consent status as a pragmatic way to balance assurance with operational efficiency. Others sought clarity on expected behaviours where CCS may be temporarily unavailable, including whether a strict zero-trust model could unintentionally disrupt legitimate access during outages or service degradation. At the same time, there was support for the proposed policy approach, with some respondents noting that mandatory introspection is the only mechanism that can provide full confidence that every data share is linked to an active consent. Alternative approaches — such as reliance on webhooks or caching consent for the duration of the consent lifetime — were viewed by some as insufficient safeguards for highly sensitive data and as introducing additional risk.	Importantly, introspection is not intended to require consumers to repeat the consent journey every time data is accessed. Instead, it operates as a very lightweight API validation call using refresh tokens, aligned to established OAuth and FAPI-based approaches already used in other regulated sectors. The intent is to provide real-time confirmation that valid consent remains in place at the point where data is shared, while introducing minimal latency and negligible impact on capacity and system overheads. We also recognise the need for a pragmatic approach to operability. Webhooks or cached consent states may have a role as supplementary signals, but our current view is that they should not replace validation of active consent at the point of data sharing. Webhooks alone will not be a sufficiently reliable replacement for a targeted introspection model and would put greater pressure on the latency, uptime, and refresh rates of other systems across the ecosystem. More broadly, we are seeking to balance implementation costs and operational impacts against the potentially far greater consequences of inappropriate data sharing, GDPR breaches and loss of consumer trust. Mandatory introspection forms an important part of the FAPI 2.0 security profile and supports the overall integrity of the trust framework. Moving away from this approach could weaken the ecosystem's security posture and reduce confidence in CCS as a trusted consent service. A key reason for embedding zero trust is that it protects the integrity of the Trust Framework while enabling the future we are collectively working towards: trusted, secure data sharing at scale. Overtime, CCS will need to federate beyond individual organisations and across sectors, supporting Government's wider ambition for more connected data sharing across the UK. That ambition will only be achievable if participants have confidence that the framework is secure, resilient and consistently enforced. A strong zero trust posture is therefore not just a security requirement; it's a foundation for the trust, confidence and interoperability needed to unlock wider cross-sector collaboration.

Theme	What stakeholders told us	How is this shaping the CCS design
		There is also an important trust consideration across both consumers and CCS Users. ATPs and EDHs need confidence that CCS represents a reliable and authoritative source of consent status. In particular, EDHs must be able to trust that every data share is supported by a valid and active consent. In the event of a data breach or inappropriate access, confidence in the wider ecosystem could be quickly undermined. Our current view is that mandatory introspection provides the strongest safeguard against this risk, while the lightweight technical design keeps system-level impacts proportionate and manageable. Further technical guidance will be developed to provide greater clarity on expected operational behaviours and implementation expectations. We are also engaging with the ICO regarding outage scenarios, including whether there should be defined parameters around how long data sharing may continue if CCS is temporarily unavailable. Our current working assumption is a maximum period of 12 hours, aligned with the position currently being considered by Elexon in relation to the SDR, although this position will continue to be tested and refined before final design decisions are confirmed.
Use of mTLS as a minimum security standard for data sharing	There was strong support for open standards, and for FAPI 2.0 and mTLS between CCS Users and CCS. However, some respondents questioned whether mandating mTLS between ATPs and EDHs exceeds the intended scope of CCS and aligns with the 'hybrid' model envisaged by Ofgem, suggesting that minimum security requirements for energy data sharing should be carefully considered in light of existing arrangements and participant-specific security obligations. Specific concern was raised that the existing Smart DCC security profile, reflecting their role as Critical National Infrastructure, may already provide a robust baseline. Further work is therefore needed to map compatibility between CCS security requirements and existing DCC arrangements, and determine how the systems can work together without lowering security standards or introducing unnecessary change.	We understand the concerns raised about the scope and practical impact of mandating mTLS, particularly between ATPs and EDHs. We also welcome the strong support for open standards and agree that the CCS security model needs to be both robust and implementable. This supports interoperability, consistency and future cross-sector alignment. NESO have confirmed that they will also be using mTLS to secure data sharing in the DSI, and RECCo have been working alongside them to ensure the same security controls are in place, where relevant, to ease complexity for data sharing in the UK energy market. Through alignment across the sector with mTLS – in line with DESNZ and UK Government pushes towards enhanced cyber security controls – we are ensuring that the CCS will be able to operate securely cross-sector, given the ability to build hierarchical Root and Certificate Authority structures. Whilst interoperability beyond energy is a key driver for use of open standards, interoperability within CCS is also an essential

Theme	What stakeholders told us	How is this shaping the CCS design
		goal and driver of our proposed designs. By mandating a baseline security profile which all parties have to adhere to, organisations will be able to register and manage certificates for their organisation within the framework, enabling automatic compliance and access to all datasets. ATPs and EDHs will be able to trust their connections, and particularly ATPs will not need to modify their systems for different EDHs, there will be immediate interoperability. Assessing the scope of CCS in isolation, our current position is that mTLS should remain the CCS baseline security control for consumer-consented data sharing. Building on years of real-world experience underpinning data sharing across the world, the FAPI protocol has been evolved and the most recent and advanced standard, FAPI 2.0, specifies a fundamental requirement for sender-constrained tokens. It accepts either the use of DPoP or mTLS as mechanisms to achieve this and given mTLS is more prevalent, relatively straightforward to implement and can achieve cross-framework and cross-sector interoperability, it has been identified as a preferred approach. RECCo are working together alongside Elexon, DCC and other key industry Energy Data Holders to ensure the adoption of mTLS fits with existing and future data sharing arrangements. Particularly with regards to DCC, the use of mTLS will not impact DCC's existing CNI systems and will not interfere with how data is pulled from smart meters. We will continue working closely in parallel with other industry bodies and initiatives and will share more detailed technical details in due course and we recognise that stakeholders will need clear guidance on how this applies in practice, particularly where existing security arrangements are already in place. To support implementation, RECCo plans to develop practical guidance for market participants. This may include sample code, installation guidance and, where appropriate, tooling to help CCS Users implement the protocol more easily. The solution we have procured has simplified, self-serve certificate management features that will greatly reduce the burden on organisations to implement certificates for transport and signing. We will develop

Theme	What stakeholders told us	How is this shaping the CCS design
		this material with the technology provider and continue to engage stakeholders as the detailed design progresses.
Consumer experience and uptake	Respondents provided thoughtful feedback on the importance of getting the consumer experience right. A clear message was that CCS will only build trust if consumers understand what they are being asked to do, why consent is needed, and what benefit they can expect from CCS-enabled data sharing. It was noted that the combined steps required to provide consent, including identity verification, MPxN association and consent confirmation, could feel burdensome, particularly for simpler data-sharing use cases, encouraging RECCo to ensure the journey feels proportionate and avoids unnecessary friction. Respondents also highlighted the risk of overwhelming consumers with too much information at the point of consent. Given that many consumers may only engage with CCS occasionally, they emphasised the importance of making first-time journeys clear, intuitive and confidence-building. A further theme was consistency. Respondents noted that inconsistent implementation by ATPs could lead to uneven consumer experiences, potentially eroding trust in the CCS framework as a whole.	As set out above, we are currently reviewing our previous legal advice regarding who can provide consent, whilst also engaging with the ICO to test the consultation position. We are also continuing consumer research to better understand consumer needs, expectations and potential points of friction within CCS journeys. This work is informing ongoing design iteration and is being supported by a UX partner with relevant experience in consent, trust and digital service design Alongside this, we are engaging with a range of consumer and stakeholder bodies, including Citizens Advice and Money & Mental Health Policy Institute, to help ensure the CCS design reflects broader consumer perspectives and real-world challenges. This includes consideration of vulnerability, accessibility, trust, consumer understanding and the potential risks of consumer harm or exploitation. We also recognise the feedback that additional consumer archetypes and scenarios should continue to be explored as the research develops, particularly in relation to vulnerable consumers, differing property tenure arrangements and circumstances where consumers may be at greater risk of pressure, exclusion or misuse of consent processes. These areas will continue to be considered through future research waves, usability testing and ongoing stakeholder engagement. Following the consultation, we have also initiated a trust mark workstream to explore which trust signals could support consumer understanding and confidence throughout the journey. Finally, we believe the Customer Experience Guidelines (CEGs), anchored within the REC and given effect through the ATP Access Agreement, will ensure that the consent experience is standardised, transparent and trustworthy, while still allowing ATPs to maintain their own branding and customer relationships. The CEGs will be focussed on the interactions within the journey between the ATP's wider journey and the CCS at the specific point this happens only. There is no wider intention with the CEGs

Theme	What stakeholders told us	How is this shaping the CCS design
		to impact ATP journeys beyond ensuring CCS is uniform and recognisable where is appears within a journey.
Inclusion and Accessibility	A clear theme was that the CCS model should not assume all consumers have the same level of digital access, confidence or capability, particularly consumers who may be vulnerable, digitally excluded or unable to complete standard digital journeys Respondents asked for greater clarity on how non-digital or assisted journeys would operate, including which channels may be available, how support would be provided, and how those routes would offer an appropriate level of equivalence with digital journeys. Some respondents also noted that meeting accessibility expectations could create delivery and cost challenges, particularly for smaller or newer market participants. Others questioned whether inclusive design was being treated as a later-phase enhancement rather than a core consideration for the MMP, and asked where responsibility would sit for ensuring inclusive access across the CCS framework	We recognise the concerns raised and agree that inclusion and accessibility must be considered from the outset. For the MMP, RECCo is designing CCS to be digitally accessible and is using consumer research to understand where consumers may experience barriers, confusion or additional support needs. This research is informing the MMP design and will help ensure the initial digital journey is as clear, accessible and usable as possible. At the same time, we recognise that a fully inclusive solution, including non-digital and assisted journeys, cannot realistically be delivered in full from day one. These routes require careful design, testing, and operational considerations to ensure they are effective, secure, and proportionate. For that reason, further development of non-digital and assisted journeys has been included in the product roadmap for iteration beyond MMP. CCS is an enabling solution for consented access to digital energy data. In many cases, consumers will access CCS through an ATP's own website, app, or customer journey, and the way in-person or assisted support is provided may depend on how ATPs engage with their customers. RECCo will continue to consider how CCS can consistently support those journeys, while maintaining appropriate safeguards for consent and data access.
Governance Arrangements	Respondents were broadly supportive of the proposed REC drafting approach, including the suite of artefacts planned for consultation in summer 2026. There was also general support for using existing REC governance arrangements to manage change and apply assurance mechanisms. However, respondents sought greater clarity on how ATPs and EDHs will participate within REC governance processes, particularly where future changes may impact their obligations, technical implementation or operational activities. Some respondents also raised concerns regarding the proposed Customer Experience Guidelines (CEGs). In particular, there were questions around whether the CEGs could become overly	We appreciate the general support for the approach to leverage existing REC governance to support change and assurance activities and have continued to developed REC drafting on this basis. We recognise the concerns raised about the proposed Customer Experience Guidelines and agree that they should support, rather than constrain, effective consumer journeys. The CEGs will therefore be developed through the CCS working groups, with the aim of supporting a transparent, consistent and GDPR-compliant consent experience without being overly prescriptive or limiting ATPs' own branding and customer relationships.

Theme	What stakeholders told us	How is this shaping the CCS design
	prescriptive or potentially conflict with the wider move toward more outcomes-based regulation. Respondents encouraged RECCo to ensure that any guidance supports a clear, transparent and consistent consent experience, while still allowing ATPs sufficient flexibility to design customer journeys and branding approaches that meet the needs of their users. Respondents also emphasised that clear, timely and accessible customer redress arrangements will be essential to maintaining trust and confidence in CCS. Feedback highlighted the importance of a well-defined process that enables consumers to understand: • where to raise issues, • how those issues will be handled, • and what remedies may be available where something goes wrong. Many respondents stressed that responsibilities across RECCo, Suppliers, ATPs and other market participants must be clearly defined to avoid consumers being passed between organisations or facing uncertainty about who is accountable for resolving issues.	From an engagement perspective, RECCo already has arrangements for involving Non-Party REC Service Users in REC governance processes. We intend to build on these arrangements for ATPs and EDHs, so that they can engage appropriately where changes may affect their obligations, technical implementation or operational processes. We have also raised the REC Issue I0318[2] and will use the associated communication channels to engage with interested parties to support wider understanding of the CCS and REC governance. In relation to customer redress, we expect the CCS to embed a customer-centric approach to issue resolution, helping ensure that problems are resolved quickly, fairly and with minimal friction for consumers. We are continuing discussions with Ofgem and DESNZ regarding appropriate dispute arrangements, and are also engaging with the Energy Ombudsman to identify potential routes for managing complaint escalation and consumer support where issues cannot be resolved through standard operational processes.
Cost, funding and value for money	Respondents asked for stronger evidence that CCS costs will be proportionate and deliver value for consumers, particularly while adoption is still developing. A clear theme was the need for transparency on early expenditure, expected benefits and how costs may evolve over time. Several respondents highlighted the cumulative impact of flexibility-related schemes funded through suppliers, with costs ultimately flowing through to consumers. This increased the importance of demonstrating clear consumer benefit and avoiding unnecessary duplication. Some respondents supported the proposed approach of recovering initial CCS costs from suppliers, with accreditation	We recognise that cost and value for money remain central concerns for stakeholders, particularly while CCS adoption and participation continue to develop. The CCS Business Case was updated and republished in January 2026, with revised budget figures reflecting updated delivery assumptions, although the overall delivery cost profile remained broadly consistent with the original position. These figures informed Ofgem's Impact Assessment during 2025. To ensure a balanced assessment, the Impact Assessment also considered a range of higher-cost and lower-benefit scenarios, concluding that CCS would continue to represent a viable and value-for-money solution even under materially less favourable assumptions.

[2] I0318 - Introduction of Consumer Consent Solution

Theme	What stakeholders told us	How is this shaping the CCS design
	and assurance costs recovered from individual CCS Users. Others raised concerns that CCS and SEC accreditation requirements could duplicate assurance and increase costs for participants. A number of respondents also asked for more clarity on future funding arrangements, including the potential triggers and timing for a post-MMP review, and whether a user-pays model may be more appropriate once CCS adoption has developed.	RECCo continues to apply robust cost controls across the programme, with value for money remaining a key consideration throughout delivery. The CCS programme is being delivered within approved funding parameters and does not include a contingency fund to accommodate overspend, reinforcing the importance of disciplined cost management and phased delivery. We also recognise stakeholder interest in ensuring that expenditure remains proportionate, appropriately phased and clearly linked to demonstrable consumer and market benefits. We welcome ongoing challenge and scrutiny in this area and will continue to provide transparent reporting on current delivery activity, post-MMP development considerations and the basis on which future investment decisions are assessed and prioritised. We also heard concerns that CCS sits alongside a number of wider smart data, flexibility and digitalisation initiatives, many of which may ultimately be funded through consumers' bills. RECCo will continue working with Elexon and NESO through the Digitalisation Delivery Group to support alignment across related initiatives and will continue engaging with Ofgem and DESNZ to ensure the CCS funding approach remains aligned with wider policy direction and market objectives. In relation to accreditation and assurance costs, we understand the concern that CCS and SEC arrangements could create overlapping requirements or duplicate effort for participants. We will therefore continue to work closely with SECCo to define clear boundaries between the respective frameworks, helping minimise unnecessary duplication while maintaining appropriate assurance over organisations accessing consumer data through CCS. The summer drafting consultation will also provide further detail on how the CCS cost recovery mechanism may evolve beyond the MMP phase, including the factors that may inform any future review or amendment to the funding approach.

Conclusion and next steps

The consultation has provided valuable and, in several areas, challenging feedback. We are grateful for that challenge. It has helped identify where the CCS design is sufficiently well supported, where the rationale needs to be explained more clearly, and where further evidence or engagement is needed before final positions are taken.

As a result of the consultation, RECCo is giving particular focus to the occupier/bill payer question, SEC alignment, IDV proportionality, consumer messaging, inclusion and accessibility, and cost transparency. Some elements of the design, such as centralised consent validation and the use of open security standards, remain important to the overall trust model. However, the way these elements are implemented, explained and governed will continue to be shaped by stakeholder input.

The next stage is to develop the lower-level CCS design, operational artefacts and draft REC legal text. RECCo will continue engagement through working groups and bilateral discussions before issuing the summer REC drafting consultation. That consultation will set out the proposed final positions, the supporting rationale, and the areas where further views are specifically requested.

This interim response is being issued following RECCo webinar 1st week of June 2026. Questions on this document or the CCS more generally can be sent to: consumerconsent@retailenergycode.co.uk