Design Consultation

Consumer Consent Solution

Published 11 February 2026

Contents

1 Executive Summary

1.1 The Retail Energy Code Company (RECCo), acting on Ofgem's direction, is progressing the development of a new Consumer Consent Solution (CCS), a central, standardised and trusted mechanism for capturing, managing, and validating consumer consent for the sharing of energy data. This consultation document presents RECCo's proposed approach for delivering the Minimum Marketable Product (MMP) of the CCS, together with the technical architecture, governance framework, assurance model, and user experience (UX) foundations required to support a trusted, scalable, and future-proof consent ecosystem.

1.2 The CCS responds directly to longstanding challenges in the energy sector, where fragmented and inconsistent data sharing consent processes have created barriers to innovation, increased costs for market entrants, and undermined consumer confidence in data sharing. Ofgem's 2024 consultation[1] and its April 2025 Consumer Consent Decision[2] confirmed the need for a hybrid model combining a central consent portal, standardised authentication and verification processes, and decentralised data exchange between Authorised Third Parties (ATPs), which use consumer data to provide services to consumers and Energy Data Providers (EDPs), which are organisations that hold or control access to consumers' energy data. RECCo has been appointed as the delivery body to design, implement, and govern this new framework.

1.3 The proposed CCS MMP will provide consumers with a central, secure interface to view, grant, manage, and revoke their consents, while enabling ATPs and EDPs to rely on a consistent, interoperable, and UK General Data Protection Regulations (GDPR) aligned consent mechanism. The MMP will initially support the sharing of half-hourly metered data, leveraging existing and emerging Data Sharing Arrangements (DSAs) such as Smart Energy Code (SEC) Other User access and Elexon's Smart Data Repository (SDR), subject to approval. The solution has been designed to be flexible and extensible, enabling future expansion to additional datasets, use cases, and consumer segments.

1.4 To support timely delivery and reduce delivery risk, RECCo intends to deliver the CCS using a proven, off-the-shelf technical solution. The technical design set out in this consultation reflects insights gained through market engagement and prototyping, and represents RECCo's current view of the most appropriate architecture to meet Ofgem's objectives. The technical design includes a central consent management system, a secure token model, and a Directory and Registry enabling ATPs and EDPs to discover one another and integrate using open, interoperable Application Programming Interfaces (APIs). RECCo proposes the use of open standards to support implementation, enhance interoperability, and align with established security practices. Data itself will continue to flow directly between ATPs and EDPs, with the CCS acting as the central trust framework confirming that consent is valid, current, and linked to the correct Data Subject.

1.5 The CCS has been designed to support inclusive and accessible user experiences, guided by the development of Customer Experience Guidelines (CEGs) developed by RECCo as part of the CCS Governance Framework. The CEGs will set clear and consistent expectations for how consent is presented, explained and managed, ensuring transparency, accessibility, and alignment with GDPR requirements and government accessibility standards. UX design will be informed by consumer research, usability testing, and ongoing feedback during delivery to ensure CCS journeys reflect real consumer behaviours and accessibility needs and can be refined over time.

1.6 The CCS will be embedded within the Retail Energy Code (REC) through a new CCS Arrangements Schedule, a CCS Service Definition, a CCS API Technical Specification, and consequential updates across key REC artefacts. A

[1] Consumer Consent Solution Consultation, Ofgem, October 2024

[2] Consumer Consent Decision, Ofgem, April 2025

structured accreditation model, building on existing qualification processes, will apply to all ATPs and EDPs to ensure robust information security, data protection, and technical readiness. The governance framework includes dispute-resolution pathways, monitoring and reporting requirements, an escalation route to the REC Performance Assurance Board, and coordination with Ofgem, the Department for Energy Security and Net Zero (DESNZ), the Information Commissioner's Office (ICO), and other relevant bodies.

1.7 The CCS will be delivered through a phased approach, with the MMP targeted for go-live in March 2027. The initial scope will focus on domestic consumers and the sharing of half-hourly metered data via existing and forthcoming arrangements. The CCS is being designed to scale to additional datasets (such as tariff data and Priority Services Register (PSR) data) where consent is required, new user types, expanded identity verification (IDV) options, non-domestic consumers, delegated authority models, and cross-sector smart-data interoperability. These future capabilities are set out within the CCS Product Roadmap.

1.8 Initial costs will continue to be recovered through the REC cost recovery model, with future funding arrangements to be reviewed as adoption grows. RECCo will continue to work closely with Ofgem, DESNZ, industry stakeholders, and consumer groups throughout the design, procurement, implementation, and post go-live evolution.

1.9 This consultation seeks stakeholder views on the proposed technical design, governance model, policy positions, user experience principles and CEGs, and governance framework. Feedback will inform the detailed REC drafting and technical specification development to be consulted on in summer 2026. RECCo invites all interested parties to contribute to the development of a secure, interoperable, and consumer-centric consent solution that will underpin the next generation of energy data services.

2 Introduction

Background

2.1 In its August 2024 Consumer Consent Solution Consultation, Ofgem explained that current approaches deployed in the energy sector for retrieving and providing consent are inconsistent, causing barriers for new market entrants who need to develop their own consent solutions and resulting in negative consumer experiences. Ofgem proposed that a new consent solution should be developed to provide a standardised and system-wide consent process. The CCS would include a consumer-facing interface, such as a dashboard or portal, that would contain all the consumer's permissions data in one location with backend technologies that enable existing and new market entrants to utilise this consent solution as their consent management system.

2.2 In its April 2025 Consumer Consent Decision, Ofgem confirmed its position to progress with the development of a CCS, with RECCo selected as the delivery body. The rationale for this decision was to ensure the CCS has a clear and robust mechanism of redress, trusted providers, and a proven regulatory framework to ensure the critical component of consumer trust.

2.3 The Consumer Consent Decision document also confirmed the preference for a hybrid model to be developed which would have a central consent retrieval portal and centrally governed authentication and verification processes, with decentralised energy data sharing and API specification.

2.4 The CCS has been designed to operate in compliance with GDPR and to support consistent, transparent, and lawful consent-based data sharing across the energy sector. The CCS provides a central mechanism for capturing, recording, and managing consent, together with supporting technical controls, governance, and assurance arrangements.

2.5 The CCS does not replace or assume the legal responsibilities of organisations that rely on consent as a lawful basis for processing personal data. Responsibility for determining whether consent is required, obtaining valid consent where applicable, and ensuring compliance with GDPR and other relevant legal and regulatory requirements, remains with the organisation accessing or sharing data.

2.6 Through standardised processes, IDV, consent lifecycle management, monitoring, and assurance, the CCS is intended to reduce fragmentation, improve consistency, and strengthen consumer trust, while preserving clear accountability for data protection compliance.

What are we consulting on?

2.7 This RECCo-led consultation represents the next step in the process for developing and implementing the CCS. The consultation includes details of the proposed delivery approach and sets out the scope of the MMP that will form the first phase of implementation. Following this, we will utilise the REC change process to deliver against a roadmap of change to expand the data sets and use cases facilitated by the CCS.

2.8 The consultation provides a comprehensive explanation of the proposed CCS, including the following:

- **REC Policy Positions** – defining the legal position to be reflected in the REC, relating to the granting and revocation of consent, alongside the proposed minimum standard for IDV and our approach to use open standards to preserve interoperability, ease of implementation, and a strong security posture;
- **Technical Design** – covering the key technical design assumptions that underpin the solution, with details of the overall solution architecture and security controls;

- **User Experience Design** – with a strong focus on consumer outcomes, this section defines the proposal to develop CEGs to ensure a clear and consistent approach is followed across all consumer engagements; and
- **Governance Design** - defining the governance framework that will underpin the CCS, including the approach to funding, change control, accreditation, assurance, and issue resolution.

2.9 We are seeking views from industry and other interested parties on each of these core elements of the enduring solution. The output from this consultation will support the development of the detailed solution design, including the CCS API technical specification, CEGs, and proposed REC drafting. These elements will be subject to further consultation during the summer.

How have we developed the proposed approach?

2.10 To support the development of the CCS, Ofgem established three working groups focused on:

- Implementation and Governance;
- Consumer Protection and Accessibility; and
- Technical Design and Security.

2.11 These working groups, chaired by Ofgem, have considered a wide range of design questions to support the design assumptions underpinning the proposals within this consultation.

2.12 As part of the agreed handover in responsibility for managing the working groups from Ofgem to RECCo in December 2025, Ofgem produced three working group papers[3] reflecting the discussions that have taken place over the preceding six months. The purpose of these papers is to provide transparency and help the wider industry understand the considerations explored so far.

2.13 Outside the working group considerations, RECCo has engaged with a wide range of interested parties including existing organisations accessing half-hourly consumption data through the SEC Other User route. We have also continued to work closely with other programmes that rely on data sharing such as Tariff Interoperability, Smart Secure Electricity System (SSES), Data Sharing Infrastructure (DSI), Smart Data Repository (SDR), and Flexibility Market Asset Registration (FMAR).

2.14 To support development of the technical requirements, we have worked with potential technical partners to develop functional prototypes that demonstrate working functionality and de-risk the overall delivery plan by proving, in advance, that the proposed solution will work in practice. This activity has enabled us to explore the various elements of the solution design, whilst also supporting our ongoing technical partner procurement.

2.15 As has been discussed throughout the working groups and other industry engagement, RECCo's approach to delivering the CCS is to procure a solution that has most of the specialist functionality required 'out-of-the-box'. Having completed prototypes with multiple providers, RECCo is still in a formal procurement process with a Request for Proposal (RFP) having been issued in early January 2026. As a result, RECCo is unable to reveal a complete picture of the low-level design of the CCS in this consultation. Further detail will be shared through

[3] https://www.retailenergycode.co.uk/our-programmes/consumer-consent-solution/

working group meetings in the coming months with the detailed design issued as part of the REC drafting consultation, currently scheduled for July 2026. Nevertheless, there is still a significant amount of information on a proposed technical design driven by our work with our potential suppliers contained in this document.

Consultation Stages

2.16 This consultation will be open to responses for six weeks, until **25 March 2026**. After the consultation period ends, all responses will be considered and weighted appropriately, with each response evaluated on its own merits.

2.17 All non-confidential responses will be published following a review and consolidation exercise completed by RECCo following the end of the consultation period. An update will be presented at a CCS working group following this publication. Please let us know in your response whether you'd like your response, or any specific elements of it, to be treated as confidential or anonymous.

2.18 Consultation responses will be considered by RECCo, in discussion with Ofgem and DESNZ, and used to support development of the detailed design (Technical and UX CEGs) and associated REC drafting, which will be the route to clarify RECCo's settled position post consultation. A further consultation will be progressed at a later stage, with proposed changes to the REC.

How to respond

2.19 We welcome responses to this consultation from anyone interested in the Consumer Consent Solution. Please complete the response form (Annex A) and send your response to **consumerconsent@retailenergycode.co.uk**

2.20 Where possible, we kindly request that responses are submitted as a Word (.docx) document. Please be assured that your responses will not be edited or amended in any way.

2.21 Whilst we request that consultation responses are submitted using the response form (Annex A), we have included the relevant questions at the top of each applicable section within this document for the purpose of simplicity when reviewing the content.

2.22 We will publish non-confidential responses on our website at https://retailenergycode.co.uk/consultations/

Your response, data and confidentiality

2.23 Responses can be submitted in one of three ways:

- Non-confidential – the full response along with the submitting organisation's name and category, will be published; or
- Confidential – responses will only be shared with RECCo and its CCS project team, the REC Code Manager and the Authority (where relevant). We will respect this request for confidentiality, subject to any obligations upon us to disclose information. Confidential responses will not be published, and details will not be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation; or
- Anonymous – the full response will be published, but the submitting organisation's name will be omitted (the organisation category will still be published). Details of the response may be referenced in any consultation summary report(s) or subsequent REC Change Proposal documentation, and the organisation name will be shared with RECCo and its CCS project team, the REC Code Manager, and the Authority (where relevant).

2.24 If you submit a non-confidential response but wish to keep part of your response confidential or anonymous, please clearly mark those sections as "confidential" or "anonymous" as appropriate.

2.25 If you wish to respond confidentially, we'll keep your response itself confidential within the bounds of paragraph 2.23, but we will publish the number of confidential responses we receive. We won't link responses to respondents if we publish a summary of responses, and we will evaluate each response on its own merits without undermining your right to confidentiality.

2.26 All responses will be treated as non-confidential unless otherwise indicated.

2.27 RECCo recommends submitting only financial or commercially sensitive information as confidential, and using anonymous for other cases where the submitting organisation does not wish to be identified. This approach ensures that response details can be included in any consultation summary report(s) and that RECCo's comments on the responses can be published.

3 CCS Design Principles

3.1 In its August 2024 consultation, Ofgem detailed five core principles that should underpin the CCS. These were:

- Consumers should be able to trust that data sharing is safe and secure;
- Organisations need to clearly outline the value and benefits of data sharing in a way that all consumers can understand;
- It should be clear to consumers what they are giving consent for and to whom – this needs to be explained upfront and not hidden in legalistic language or fine print;
- The process should be accessible for all and not leave the digitally excluded behind; and
- The consent solution should have the capability for cross-sector operation, with the potential to benefit consumers within and beyond the energy sector.

3.2 These core principles were then reflected in a set of design principles that Ofgem defined within their consultation document:

- Simple and Low Friction;
- Interoperable;
- Agile, Flexible, and Scalable;
- Transparent and Informative;
- Inclusive by Design; and
- Secure by Design

3.3 Respondents to the Ofgem consultation proposed a number of additional design principles. We have set these out in Annex C together with our assessment. The final proposed principles have been discussed with the CCS working groups and are set out below.

- **Simple and Low Friction** - each element of the proposed solution has been developed to minimise negative friction for both consumers and CCS Users (ATPs and EDPs). Throughout this consultation document we have sought to explain how we have balanced the need for a robust, secure solution that protects consumer data (positive friction), with the need to avoid unnecessary barriers (negative friction), in order to enhance the consumer experience and maximise uptake. This is supported by the development of CEGs, which are further detailed in Section 7.
- **Interoperable** - the technical solution has been developed using an API-first approach and open standards, to facilitate interoperability with other data sharing initiatives and future expansion outside the energy sector.
- **Agile, Flexible, and Scalable** - recognising the direction from Ofgem to deliver a minimum set of requirements, with future iterations, we have defined a phased approach which focuses on the delivery of an MMP that can be iterated and scaled as market adoption grows.
- **Consistency** - a key focus of the CCS design has been to remove existing fragmentation and develop a consistent approach to consent management, through the delivery of centralised elements developed and delivered by RECCo and its service providers, this will be facilitated by the CEGs.

- **Privacy by Design** - the design of the consent mechanism is underpinned by the GDPR principles for consent to be freely given, specific, unambiguous, explicit, and time-bound. CEGs are a core part of the CCS design which will ensure interactions with consumers reflect these GDPR principles with clear and transparent communication protocols.

- **Inclusive by Design** - the CEGs will also focus on accessibility within the user interface. We will ensure that the user interfaces meet the government's POUR accessibility standard (i.e., that information is Perceivable, Operable, Understandable, and Robust).

- **Secure by Design** - security will be built into the CCS from the start. Throughout the design phase we will undertake risk analysis of cyber threats, with input from the National Cyber Security Centre and produce and maintain a Data Protection Impact Assessment to underpin the solution. We will also use recognised security standards within the solution design for managing the sharing of data and authenticating organisations interacting with the CCS.

- **Promotion of Effective Competition** – whilst a key focus of the CCS development work has been the consumer journeys, we have also been cognisant of the impact on market participants wishing to share or access data to enhance services offered to consumers. The CCS has been designed to enable fair access to data, preventing anti-competitive practices, and encouraging innovation, which will, in turn, enable consumers to benefit from a dynamic, competitive energy market.

3.4 We will continue to evolve these design principles as the project progresses, taking into account information gathered through stakeholder engagement and any direction received from Ofgem and/or DESNZ.

4 Scope of the CCS

Consultation Questions

Q1. Do you agree with the proposed MMP scope, including the core functional components and the inclusion of SEC Other Users and the BSC SDR?

Q2. Do you have any comments on the assumption that SEC Other Users would not need to migrate existing consents to the CCS and would instead move to using the CCS as existing consents are renewed?

4.1 In developing the solution, we have been mindful of the direction from Ofgem to deliver an initial product to facilitate the sharing of consumption data, with extension through later phases to include integration with additional DSAs facilitating access to wider data sets, and also development of consumer profiles which utilise PSR data.

4.2 We have referred to this initial phase as delivery of the MMP (i.e., the smallest version of the CCS that includes the core features which enable it to deliver value to the consumer). Whilst the terminology has changed since the original Ofgem consultation, the expectation for the CCS MMP is aligned with the vision set out within the Minimum Viable Product (MVP) referenced by Ofgem.

4.3 The scope of the MMP has been driven by the vision set by Ofgem in its August 2024 consultation. Ofgem determined there was a need to deliver a consumer-facing interface enabling consumers to view their existing consents, together with a consent management system, that existing and new market entrants can utilise, thus removing the need to build their own system and ensuring that consumers are not faced with numerous different methods for obtaining consent. Ofgem's view was that this solution would help build consumer trust, increase consumer engagement, and lower barriers to healthy competition in the energy market.

4.4 The technical design proposed in this consultation reflects what RECCo has identified as the most suitable solution based on all of the inputs outlined above. With the solution, our aim is to protect consumers by ensuring there are appropriate controls on personal data sharing, whilst minimising the impact on existing and potential future DSAs themselves. This is in line with Ofgem's preference for a 'hybrid model' stated in their decision paper. Further information on the hybrid model is included in Section 6 and Annex D.

Functional components

4.5 The scope of the MMP includes the following functional components. Each of these components is further defined in Section 6 of this document:

- A mechanism for onboarding accredited CCS Users and new DSAs;
- A directory of ATPs (i.e., organisations wishing to access energy data) and EDPs (i.e., organisations wishing to share data);
- A registry of DSAs, allowing ATPs to view the available data and associated EDP, as well as enabling access to data via published API specifications;

- A mechanism for registering consent by verifying a consumer's identity and matching them to the specific Meter Point X Number(s) (MPxN) at an address, as well as providing ongoing account login functionality for monitoring or managing consents;
- A mechanism for recording, storing, and validating that consent is in place as part of wider DSAs; and
- A consumer portal where consumers can view active consents and revoke or dispute consents as required.

4.6 In addition to these functional elements, a core component of the MMP is the development of a set of CEGs, setting a standardised approach for consumer-facing platforms requesting consent. These guidelines will be developed with the expectation that ATPs will apply the agreed lexicon and format within their systems. Further information on the CEGs is included within Section 7.

Authorised Third Parties, Energy Data Providers and Data Sets

4.7 As directed by Ofgem through its April 2025 decision document, the initial solution will be limited to the sharing of half-hourly metered data, with the prospect of expansion to other datasets, such as tariff data, in the near future. MMP scope will also be limited to energy data relating to domestic consumers, with expansion to include microbusiness and small businesses at a later date.

4.8 To demonstrate the CCS functional components in enabling the sharing of half-hourly metered data, we have considered existing and imminent DSAs for inclusion in the CCS MMP. This approach will enable us to deliver the CCS in a timely manner, without over-reliance on one data sharing arrangement.

4.9 The two DSAs to be taken forward for MMP include:

- Existing scenarios where SEC Other Users, with access to gas and electricity smart metering data, are sharing half-hourly metered data with one or more ATPs that engage directly with consumers to gain consent; and
- The new SDR arrangements, where Elexon is accessing half-hourly metered data used for the purposes of electricity settlement, and making this available to SDR users who will engage directly with consumers to gain consent. Inclusion of the SDR within the scope of the CCS arrangements is subject to BSC Panel and Ofgem approval of Modification P494.

4.10 Based on our ongoing discussions with SEC Other Users, Smart Energy Code Company (SECCo), and Elexon, we are confident that one or both of these mechanisms will be available for inclusion in the CCS to support our proposed go live date of Q1 2027.

4.11 In addition to the DSAs and engagement with prospective EDPs, we are continuing to identify potential ATPs to volunteer as early adopters of the CCS. Should any organisation wish to participate in the CCS MMP, please contact RECCo to enable bilateral discussion using the link included in the footnote[4].

[4] CCS MMP - Get Involved as an ATP

Granting of Consent

4.12 The technical solution and associated business processes will be underpinned by an API Technical Specification defining, amongst other things, the Consent Data Schema for sharing consent data. This data schema will ensure a standardised and transparent approach is in place, enabling interoperability between the CCS and wider industry DSAs.

4.13 The technical solution will determine the Consent Data Schema for all DSAs. Minimum requirements for this data schema are listed below:

- The data subject i.e., the individual matched to the MPxN;
- the purpose of the consent, as defined by the ATP;
- the status of the consent i.e., given, revoked, expired etc;
- the specific data set that will be requested, as recorded within the CCS registry;
- the duration of the consent e.g., one time consent or a time bound consent with associated expiry date; and
- the start time and end time, where required e.g., the consumer may have moved into the property 5 months ago and therefore only 5 months of historic data can be accessed.

4.14 In developing the proposed approach to the granting of consent, RECCo has undertaken a review of the relevant legislative framework, including the applicable provisions of GDPR. The development of these proposals has been informed by specialist legal advice to ensure that the CCS approach to consent is aligned with data protection requirements and regulatory expectations. The resulting REC policy position on the granting of consent is set out in Section 5.

4.15 Under GDPR, the granting of consent is one of a number of lawful bases by which personal data can be shared. The sharing of energy data across the industry often relies on other lawful bases e.g., legal obligation where data is shared in order to meet licence obligations. Although there is a benefit to consumers in understanding all organisations accessing their personal data via a single solution, the CCS MMP will focus on instances where explicit consent is required. Extension to include the visibility of wider data sharing activities will be delivered in future iterations.

Use Cases

4.16 The CCS is providing a mechanism for managing consumer consent to support a variety of DSAs. Therefore, the focus of the MMP is not use case dependent. The use cases facilitated by the CCS will be determined by the specific data sets included within the CCS directory from day one. For example, Elexon has indicated that the SDR may include an API for sharing 12 months of half-hourly consumption data to support price comparison, or an API for sharing consumption data on a daily basis to support energy efficiency initiatives. There will also be scenarios where multiple data sets from one or more EDPs are required to facilitate a single use case. To facilitate this, our proposed API-first data ecosystem is being designed to enable immediate and automated discovery of data and services through the directory to facilitate open access for those accredited within the scheme.

4.17 Whilst the CCS MMP scope is not targeting specific use cases, it's important to recognise the range of use cases that could be facilitated through the delivery of a centralised consumer consent mechanism. These include:

- **Informed Tariff Selection** – enabling consumers to switch to tariffs that align with their financial, lifestyle, and environmental priorities. This includes price comparison, green energy selection, time of use

optimisation, lifestyle matching for consumers who have electric vehicles or work from home, and auto switching services;

- **Energy Insights Services** – enabling consumers to manage and reduce energy usage to reduce costs and support the move to net zero. This includes organisations providing personalised tips and analytics to reduce consumption, carbon footprint monitoring, demand side response, smart appliance integration to allow third party control or monitoring of devices or solar panel / battery adoption through visibility of forecast savings; and

- **Other use cases** - such as facilitating audits for insulation/heating upgrades, detecting abnormal energy usage patterns that could indicate faulty appliances, budgeting apps to help individual manage finances, and consumer research to support the development of new energy solutions and consumer focused innovations.

Recording Existing Consent within the CCS

4.18 Ofgem's April 2025 decision document explicitly referenced the expectation that existing consents should be recorded within the CCS in order to provide a single version of the truth. These existing consents mainly relate to energy suppliers who have obtained consent for accessing half-hourly metering data for the purposes of billing and settlement, in accordance with Supply Licence Condition (SLC) 47. It has been agreed with Ofgem that the inclusion of existing consents will not be part of MMP. We have included RECCo's current understanding and thinking on this topic within the Product Roadmap Section 9 of this consultation.

4.19 Whilst supplier consents represent the majority of existing consents, we also recognise that existing SEC Other Users already hold consent for a significant volume of consumers. Our expectation is that SEC Other Users will choose to engage with the CCS project on a voluntary basis and use the CCS for the granting of new consents as the service is rolled out. Given the time-bound nature of existing consents, we do not currently believe that it would be necessary to migrate existing SEC Other User consents into the CCS and instead we would expect new consent records to be established within the CCS as and when existing consents are due to be renewed. We are keen to understand from SEC Other Users whether this assumption is correct. We are also keen to understand if this approach is acceptable to industry considering it would mean any historical consents with the same consumer and SEC Other User before the consent was first recorded into the CCS, would not be represented in the CCS.

5 REC Policy Positions

Q3. Do you agree with the position that consent for access to half-hourly metered data should be provided by the occupier rather than the bill payer, where these are different individuals? If not, please provide your rationale.

Q4. Do you agree with the position that for multi-occupancy households, a 'lead occupant' may provide consent on behalf of other occupants only where they confirm they have the authority to do so and have obtained agreement from all other adult occupants? If not, please provide your rationale.

Q5. Do you agree with the proposed approach and standard for identity verification? If not, please provide a rationale.

Q6. Do you agree with the position that consumers should have the option to establish an account with the CCS or grant consent via the 'guest' approach? If not, please provide a rationale.

Q7. Do you agree that consumers should have the option to revoke or renew consent directly with the relevant ATP or via their CCS account? If not, please provide a rationale. If not, please provide rationale.

Q8. Do you agree with our position that EDPs should explicitly check that active consent is in place within the CCS each time they share data with an ATP? If not, please provide a rationale.

Q9. Do you agree that if the CCS is unavailable, the EDP should continue to share data unless the CCS outage extends for a significant period of time? If not, please provide a rationale.

Q10. Do you agree that the FAPI 2.0 standard should be adopted for the CCS, which includes use of mTLS for all data sharing? If not, please provide a rationale.

5.1 This section sets out the CCS policy positions developed by RECCo through industry working group engagement, discussion with Ofgem, and review by internal information security and data protection specialists. The development of the policy positions has also been informed by specialist external legal advice, to support alignment with the applicable data protections and regulatory expectations.

Responsibilities for Granting Consent

5.2 The CCS will provide a central, standardised mechanism for capturing, recording, and managing consumer consent, together with CEGs that define minimum requirements for how consent must be sought and presented to consumers.

5.3 However, responsibility remains with the organisation seeking consent (i.e., the relevant ATP) for:

- determining whether consent is required;
- seeking that consent for a defined data sharing purpose;
- ensuring that consent is obtained from an individual who has the appropriate right or authority to provide it; and

- relying on that consent as a lawful basis for processing.

5.4 In all cases, consent must be obtained from the relevant Data Subject, as defined under GDPR, in relation to metered data associated with energy consumed or generated at a premises during the period for which the Data Subject has the appropriate rights or authority. Consent must not extend beyond the Data Subject's period of occupancy or entitlement. This aligns with the then Department for Business, Energy & Industrial Strategy (BEIS) 15 September 2017 letter to SEC Parties[5], which notes that where smart metering data is personal data, the Data Subject is likely to be the individual living at or occupying the premises, and that situations may arise where the Data Subject is not the bill-payer. We note that previous research has indicated that 10 – 15 percent of renters have their energy costs included in their rent.[6]

5.5 The provision of these mechanisms and guidelines by the CCS does not transfer responsibility for lawful reliance on consent, or for compliance with GDPR and other applicable legal and regulatory requirements, away from the organisation accessing the data. Organisations utilising the CCS must therefore ensure that their consent journeys, representations to consumers, and reliance on consent are compliant with applicable legal, regulatory, and REC requirements e.g., conform to the CCS CEGs.

5.6 For the purposes of the MMP, the following scenarios define who may provide consent in relation to metered data:

- Domestic premises – single occupancy: For domestic premises where a single individual occupies the property, consent must be provided by the occupying energy consumer (i.e., the individual to whom the energy consumed or generated at the premises relates). The consenting individual must be verified as residing at the property and having the right to provide consent for the relevant period of occupancy;

- Domestic premises – multi-occupancy (shared households / HMOs) where a single MPxN (or supply point) serves the premises: Where more than one individual occupies a property and metered data relates to energy consumed or generated collectively through a single MPxN (or supply point), the data cannot be attributed to a single individual. In these circumstances, consent must be obtained from an occupant with a verified right or authority to provide consent. Under the proposed approach, a qualified "lead occupant" model applies: one occupant may provide consent on behalf of other occupants only where they confirm they have the authority to do so and have obtained agreement from all other adult occupants; and

- Domestic premises – multi-occupancy where multiple MPxNs exist and supply is provided separately to individual occupants: Where multiple MPxNs exist and supply is provided separately to individual occupants, each occupier is treated as a separate energy consumer and Data Subject for the purposes of consent. Each individual must therefore provide consent in respect of metered data associated with their own MPxN, and consent cannot be provided by another occupant for a different MPxN.

5.7 Consent cannot be provided by landlords, property owners, or off-site bill payers who do not reside at the premises and who are not the Data Subject. Where access to energy data is exercised under an alternative lawful basis, such as contractual necessity or through a valid Power of Attorney, that access would not be consent-based.

---

[5] Letter to SEC Parties regarding privacy and smart metering energy consumption data

[6] Tenant Survey pt.2: Energy bills and efficiency | NRLA

5.8 To support transparency and reduce the risk of disputes in multi-occupancy premises, individuals who are verified and matched to the relevant MPxN(s) will be able to view whether there are active consent records associated with that MPxN and identify the organisations accessing data. Where an individual believes that a consent record should not be active (for example, where they are the sole occupant or have not agreed to a shared consent arrangement), they will be able to raise a dispute in respect of the unexpected consent for investigation by the relevant organisation, with this dispute automatically leading to the consent being terminated.

5.9 The detailed process for investigation and resolution of consent disputes (including roles, timescales, and any implications for service continuity) is addressed separately within Section 8.

Minimum IDV Requirements

5.10 A key element of the CCS is the inclusion of a robust mechanism for verifying that the individual granting consent is who they purport to be. As with other elements of the CCS, we are not starting from scratch when it comes to developing a mechanism for IDV, therefore we have considered the existing mechanisms for IDV both within the energy industry and more widely. We have also considered the Good Practice Guidelines (GPG) produced by the Government Digital Services function, specifically GPG 45[7] which focuses on IDV.

5.11 GPG 45 defines four levels of confidence in a person's identity from low confidence through to very high confidence. Based on these confidence levels, individual organisations will determine the level of confidence required for their own specific purposes. Organisations such as the NHS and financial services require high confidence, whereas organisations signing individuals up for newsletters or registering for online courses tend to operate at low confidence levels.

5.12 The level of confidence required for granting of consent within the CCS will differ depending on the specific data being accessed. For example, access to tariff data may require a low level of confidence; whereas access to PSR data would require a higher level of confidence.

5.13 In determining the level of confidence required for the CCS MMP, we recognise the need to minimise friction for consumers, to facilitate maximum engagement levels. However, we have also taken into account the importance of consumer trust in the CCS and the fact that consumers interacting with the CCS are granting access to half-hourly metered data which, in the wrong hands, could result in negative consumer impacts e.g., exposing personal occupancy habits. We therefore believe a high level of confidence is required through IDV under the MMP. Based on the GPG 45 examples this means that identity IDV would as a minimum, need to include initial verification via a mechanism that has utilised photo identification.

5.14 A number of mechanisms already exist that provide IDV services, with platforms such as Yoti[7] and organisations such as Stripe for online verification. In addition, UK government schemes such as GOV.UK One Login could be used. For the MMP, the CCS will integrate with a minimum of one IDV provider, with the number of available IDV options expected to be limited initially. Over time, the CCS is expected to support a broader range of IDV mechanisms, giving consumers greater choice and allowing them to choose a mechanism they trust.

5.15 As and when new data sets are added to the scope of the CCS, an assessment will be carried out to determine the appropriate level of IDV based on GPG 45 considerations and we will then determine the IDV service(s) required to

[7] How to prove and verify someone's identity - GOV.UK

support this use case. This will enable us to expand to over time, enabling multiple IDV options as the CCS further develops.

5.16 In determining the proposed approach, we have considered the existing arrangements in place, in particular the mechanisms that SEC Other Users and their customers have developed in line with the SEC Privacy Controls Framework. We agree that these mechanisms could all be valid ways to confirm both the individual's identity and also match the individual to the specific MPxN(s). However, we are mindful of the direction from Ofgem to develop centrally governed authentication and verification processes that removes the need for new entrants to develop bespoke consent arrangements.

5.17 We also note that current IDV mechanisms are subject to ongoing audits to provide assurance that the mechanism for verifying identity and managing consent is appropriate. This assurance activity is not expected to be applied within the enduring REC CCS arrangements as REC performance assurance activities will focus on the participants ability to manage information security and data protection risks rather than the mechanism for gaining consent. Therefore, it would not be appropriate for RECCo to rely on IDV checks carried out by individual ATPs as part of the initial MMP.

5.18 This position will be considered further as the CCS develops, with the expectation that in future it may be possible for the CCS to rely on IDV activities completed by CCS Users where these have met the minimum threshold. For example, banks accessing energy data will have already completed robust 'Know Your Customer' (KYC) checks, including photo identification, when establishing the customer account.

Consumer Access to the CCS

5.19 As set out above, Ofgem described a vision for the CCS in its August 2024 consultation which included both a solution to be used by ATPs as their consent management system and also a consumer facing interface where a consumer can view consent data.

5.20 The CCS technical solution is underpinned by a central database that holds consent records for all individuals who have granted consent via the solution. These consent records are linked to the Data Subject i.e., the individual whose data is being accessed, by the creation of a unique entity at the point the individual undergoes an initial IDV check. For the purposes of managing consent relating to half-hourly metered data, this entity will be linked to one or more address locations and also to one or more MPxNs where they are deemed to be the appropriate individual i.e., the Data Subject as defined in GDPR.

5.21 Where an individual engages with an ATP regarding access to data that requires consumer consent, the consumer will be redirected to the CCS to manage the consent granting step in the customer journey. Working group discussions have highlighted that some consumers will be keen to establish an account within the CCS to enable them to log in and manage their consents directly on an ongoing basis. However, other consumers will be more comfortable with their engagements being driven through the specific ATP, particularly in the early days as the CCS is being rolled out and trust in the solution is building.

5.22 In order to minimise friction and design a customer journey that minimises consumer drop-off rates, we are proposing that consumers will be given the choice to either:

- grant consent without a CCS account (guest approach), which will be the default journey for the MMP;
- log in to the CCS to grant consent (where they have already established an account); or
- sign up to the CCS in order to establish a new account.

5.23 Unless the consumer has chosen to establish a CCS account, the consumer will be diverted to the IDV solution to confirm that they are authorised to provide consent in relation to the specific MPxN(s). They will then be asked to confirm that they consent to the data being shared with the relevant ATP. We refer to this as the 'guest' approach.

5.24 Where a consumer logs into their CCS account to grant consent, they will not be required to undergo a full IDV check. However, they will be asked to confirm their address data is still valid before providing consent in relation to linked MPxNs.

5.25 Where a consumer opts to sign up to the CCS, where they do not currently have an account, they will be diverted to the IDV solution to enable their unique identity to be recorded within the CCS. As detailed above, we expect the consumer to be provided with multiple IDV options to allow them to choose an option they trust. Once IDV is complete and they are matched to one or more MPxNs they can grant the required consent. Any future requests for consent will allow them to sign in and grant consent in line with the bullet above.

5.26 In defining the three routes available to consumers it's important to understand that the level of IDV required for granting access to half-hourly metered data will not differ depending on the route chosen. If it is agreed that access to half-hourly metered data requires photo identification as a minimum level of verification then this will be applied regardless of the route chosen. If the consumer chooses to use the guest approach then this same IDV check will be carried out each time they grant consent. This is a core safeguard built into the CCS framework to ensure individuals who do not have the right to grant consent do not seek to bypass the robust checks in place by not setting up an account with the CCS. We see this as similar to open banking where an individual can log into their online shopping account which holds the individual's specific information, including bank details, however they must still confirm through the bank's verification steps that they are authorising payment; or they can use guest checkout and fill in all their details each time. This gives each consumer the choice to follow the journey that best fits with their objectives and preferences rather than mandating one journey over another.

5.27 In providing an option to consumers for a guest checkout journey, we are providing an alternative route to consent that does not necessitate the creation of an account. Our goal with this option is to minimise consumer drop-off rates as we expect some reluctance to create accounts immediately, particularly if consumers are using the CCS for a one-off consent service.

5.28 We intend to develop a mechanism in partnership with our technical suppliers that allows consolidation of actions by a guest user when they eventually wish to create an account. More work is required to confirm feasibility and develop designs for this which will commence once we have selected a technical partner. This is unlikely needed for MMP so will form a consideration for a future feature.

Consent Revocation and Renewal

5.29 One of the core benefits of the CCS is visibility of consent information to consumers. The level of consent information held in the CCS will increase over time as new consents are granted via the CCS and existing consents are recorded within the CCS. This increased level of transparency will provide consumers with greater opportunity to control who is accessing their data, with mechanisms built into the CCS enabling revocation and renewal of consent.

5.30 As set out above, we recognise that some consumers will not wish to establish an account with the CCS and we are therefore proposing that the consumer will have two options for managing their consent:

- Those consumers with a CCS account will be able to view their consents directly through the consumer interface. This will show all active consents in place relating to data where they have been verified as the Data Subject, noting that this may include consent that they didn't themselves provide e.g., for multi-

occupancy households. Through this route the consumer would be able to revoke any active consent or renew any timebound consent that was due to expire; or

- Those consumers who choose not to establish a CCS account will need to manage their consent bilaterally with each individual ATP. ATPs will have clear requirements on how they manage consent revocation and renewal, with the CEGs ensuring consistency on how the consumer interactions are delivered. Where a consumer revokes or renews consent directly with the ATP, the ATP will notify the CCS via webhooks, allowing the CCS to update the relevant consent record.

5.31 Revocation of consent within the CCS may also be initiated directly by the relevant ATP where they become aware that the consent is no longer valid. A key example of this will be where the ATP is informed that the consent granter has moved out of the property and is therefore no longer the relevant Data Subject. In line with GDPR, the ATP should immediately cease access to data and should notify the CCS that consent has been revoked.

Consent Checking by EDPs

5.32 In the delivery of a secure and robust consent management solution, a key consideration has been the level of trust that EDPs can place on the information they hold regarding active consents. One option is that the ATP shares a valid consent token with the EDP and once validated against the CCS, the EDP continues to provision data until that consent token expires or has been revoked.

5.33 The other option follows a 'zero trust' model, where the EDP is required to verify that consent is active each time it shares data with the relevant ATP. This may include individual requests for data from the ATP which the EDP is responding to; or it could cover the scenario where the EDP issues data on a regular basis in line with a longer-term service agreement.

5.34 We have determined through discussions with the working groups that the latter option would be preferable, with EDPs explicitly checking that there is an active consent in place before sharing data with an ATP. However, this option introduces additional risk and dependence on the CCS for delivery of end-to-end customer journeys, which may drive up costs associated with the central solution. For example, a central system with 99.999% availability would be extremely reliable with approximately 5 minutes of downtime per annum, compared to a central system with 99.9% availability with approximately 8 hours of downtime per annum. The cost of this additional availability could however lead to a fourfold increase in technical costs. For reference, the central solution facilitating secure data exchange in UK Open Banking, the OBL, states it has a benchmark availability of 99.5% and this is deemed satisfactory.[8]

5.35 To ensure we deliver a cost effective solution we are proposing an availability requirement of 99.9% with defined processes established to enable sharing of data whilst the CCS is not available. This means introspection of tokens will be mandatory in all cases, except when the CCS server is not online and the retry strategy has been exhausted. The CCS would remain the authoritative record of consent but where the CCS is unavailable, the EDP would treat existing consents as valid by default for the defined period of the previously granted consent. This allows service continuity and reduces the risk of cascading failures across dependent services. Further consideration will be given

[8] Data-collection-framework-for-API-availability-and-performance.pdf

to the inclusion of an overall cap should the CCS be unavailable for a significant length of time e.g., as part of the Business Continuity and Disaster Recovery (BCDR) arrangements.

5.36 To support this model, we are proposing that a notification of revocation should also be issued to both ATPs and EDPs by the CCS to remove the total reliance on the point of access check.

5.37 An alternative to continuing data sharing in the event of system outage would be to simply halt data sharing temporarily. We do not believe that mission-critical services will be delivered using the CCS, requiring precise 'live' personal energy data. Therefore, it may be beneficial for industry overall to prioritise data protection and integrity at the expense of relinquishing the use of energy data for their services temporarily.

5.38 We welcome respondent views on this proposal given the trade-off detailed above. The continued sharing of data when the CCS server is offline introduces risk for data exposure and may threaten data integrity, however ceasing data sharing during a CCS outage, whilst consent is likely to remain in place could have downstream impacts on services reliant on access to data.

Open Standards and use of FAPI 2.0

5.39 Through deployment of the CCS, RECCo is offering an essential capability to support a flexible market environment for industry players to create and interact with new and existing data services. Our approach is grounded in trust, adoption and interoperability, which RECCo considers can be best achieved through the adoption of proven open standards. By using standards that are widely recognised and thoroughly documented, we intend to:

- Reduce the effort and risks associated with implementation. Open standards benefit from public documentation and wide catalogues of supporting material and tooling to support implementation;
- Enhance interoperability both within the industry and with external partners; and
- Ensure robust security measures that align closely with policy objectives that will protect ecosystem participants as well as consumers.

5.40 We appreciate that there are intelligent and useful proprietary technologies that currently underpin consent management and energy data exchange in the UK today. We also benefited from close work with proprietary technology during our ongoing procurement activities. Whilst we value the approaches that have been developed, we believe that the right solution for a market wide solution is to leverage an open standard.

5.41 The use of open standards was discussed in working group meetings, particularly with reference to security posture. There was a recognition of the need for a standard that balances encouragement for using the CCS with avoiding unnecessary barriers to participation, rather than prohibiting use through data protection systems.

5.42 Our extensive work to design a solution that will meet Ofgem's requirements has led us to view the Financial-grade API (FAPI) standard as a strong candidate for the CCS, based on its proven capability for enabling significant data sharing ecosystems securely (including Open Banking UK, Open Finance Brazil, and Consumer Data Right in Australia, among many others).

5.43 In particular, we are looking for feedback on the use of FAPI 2.0 as the preferred standard, given its improved security posture and simplified implementation requirements compared with its previous iteration.

5.44 Most recent implementations of secure data ecosystems have used the FAPI 2.0 standard. FAPI 2.0 has been implemented to secure medical data sharing in Norway under the HelseID programme, and Open Banking UAE has

adopted FAPI 2.0. Both of these ecosystems have referenced significant benefits compared with FAPI 1.0 or Advanced FAPI 1.0 (currently used in Open Banking in the UK).

5.45 We believe that the adoption of the FAPI 2.0 standard offers a range of benefits for industry and consumers:

- It is a proven technology choice, reducing risk through its evidenced success in other data sharing ecosystems. FAPI itself benefits from years of operational experience and innovation achieved in real-world implementation.
- Use of a publicly accessible, widely understood and documented standard will reduce effort for implementation through the provision of documentation and tooling, as well as Software Development Kits, that can aid engineers in implementation. FAPI 2.0 offers all of this documentation;
- Use of well-documented standards such as FAPI 2.0 should enhance interoperability within the ecosystem by reducing the risk of inconsistent implementation;
- Adoption of FAPI standards will enable future interoperability with other data sharing ecosystems, such as Open Banking. The FCA has stated an intention to develop more connections with other sectors[9] . We believe there is an opportunity to ensure future interoperability with other sectors for the benefit of consumers and the ecosystem by aligning with the FAPI standard for the CCS and, given likely evolutions over time, implementation of FAPI 2.0 now will avoid future retrofitting work;
- FAPI is built on top of OIDC, which is a renowned and dominant standard for authentication that will allow future consumer benefits (such as Single Sign-On) and federated IDV;
- FAPI includes the use of Mutual Transport Layer Security (mTLS) and cryptographic signing of tokens, which will massively strengthen the ecosystem's security posture if universally implemented. Implementation of mTLS will secure data exchange, and sender-constrained tokens will mitigate against the risk of token exposures. Failing to secure data at the Transport layer would undermine other security controls; therefore, RECCo is proposing it as a minimum for all data exchange in the ecosystem. Our thinking behind this position is outlined further in Section 6 below; and
- FAPI 2.0, compared with FAPI 1.0, benefits from an enhanced security profile in addition to simplified implementation.

5.46 An additional benefit of FAPI 2.0 versus FAPI 1.0 is that it has comprehensive threat modelling conducted by the University of Stuttgart[10]. Capitalising on existing robust threat modelling will ensure regular external assessment of cyber risks can be conducted for CCS mechanisms at no extra cost to industry. The alternative approach of using proprietary technology would require RECCo to conduct extensive threat modelling to prove the robustness of the bespoke security model. This would introduce more time, risk and cost to our project plan and given recent events

[9] Research Note: Open banking and open finance in the UK

[10] Formal Security Analysis of the OpenID FAPI 2.0: - Uni of Stuttgart

and a broad policy-driven move to improving cyber security, we believe that implementation of FAPI 2.0 would represent a significant shift towards stronger security across the industry.

5.47 RECCo's proposal to adopt FAPI 2.0 is based on its ability to support simplified implementation, interoperability, and strong security across the ecosystem. The initial preference for open standards was driven by the need to minimise additional burden on industry, while leveraging established approaches used in other large-scale data-sharing initiatives. Subsequent prototyping and design activity has refined our understanding of the potential needs to the CCS, and FAPI 2.0 has become a clear preferred standard, reflecting its security capabilities and potential to support future interoperability.

5.48 Adoption of FAPI 2.0 as the standard for the CCS will necessitate the use of mTLS for all data exchange within the ecosystem. This will mean mandatory use of mTLS for data sharing between ATPs and EDPs, as well as when interacting with the CCS. We view this as necessary to secure the Trust Framework, provide the relevant security posture and deliver on Ofgem's objectives. Failing to do so will have a range of negative impacts on the CCS ecosystem, including:

- Reduced overall trust in the ecosystem due to weaker and inconsistent security standards;
- Reduced interoperability for ATPs and EDPs as there will not be a consistent standard for data exchange;
- Increased risk of consumer data exposure through weaker encryption and a lack of sender-constrained token mechanism;
- More complicated implementation and duplicated implementation activities owing to a lack of consistency; and
- Incomplete adoption of FAPI 2.0 would negate the benefits drawn from tooling and documentation.

5.49 We are therefore seeking views from industry on the adoption of FAPI 2.0 (which includes mTLS) to underpin secure data exchange for the CCS.

6 Technical Design

Q11. Do you have any comments on the proposed overall solution architecture and the component descriptions?

Q12. Do you agree with the proposed approach to matching MPxN to the address? If not, please provide rationale.

Q13. Do you have any comments on the non-functional requirements detailed within Annex D?

Q14. Do you have any comments on the split between centralised and decentralised elements of the overall solution outlined in Annex D?

Q15. Do you have any comments on the technical diagrams and / or business process diagrams set out within Annex E?

6.1 This section describes each of the functional components of the CCS and how these will be developed to reflect the agreed design principles.

6.2 As outlined in Section 2.15, due to ongoing procurement activities, we are only able to describe our solution from a functional and high-level technical perspective. More information will be shared as soon as we have selected a preferred supplier.

6.3 In developing the proposed technical design, RECCo has undertaken extensive market scanning, supplier engagement, prototyping, and procurement activity, informed by the programme timelines for delivery of the CCS. As a result, the design set out in this section reflects a mature and well-developed approach. While feedback on the proposed design and opportunities for refinement are actively encouraged, the scope for fundamental changes to the overall technical architecture is limited, as a significant redesign would introduce material risk to the delivery of the CCS by March 2027. The proposed design has been developed in collaboration with prospective delivery partners, which RECCo considers to represent strong and credible options for delivery on behalf of the market.

6.4 The section also includes a table summarising how the proposed design aligns to the Ofgem direction for a hybrid model, with a mix of centralised and decentralised components. More information on our decision-making approach for these elements can be found in Annex D.

Overall Solution Architecture

6.5 The diagram below reflects the overall CCS solution architecture at a high level. This demonstrates the core functional components and how these integrate to deliver a secure, transparent, and consumer-friendly solution. Each of these components is described in detail, with reference to the minimum functionality we consider essential for the CCS, as well as other options that have been or are being considered. More detailed diagrams and high-level business processes have been included to demonstrate how these components fit together to support end-to-end consent management arrangements.

6.6 Given ongoing procurement activities, the discussion of the solution design and its components has to remain largely functional. Lower-level technical designs will be shared as soon as it is appropriate to do so.

6.7 A set of lower-level diagrams overviewing how each component interacts with each other can be found in Annex E.

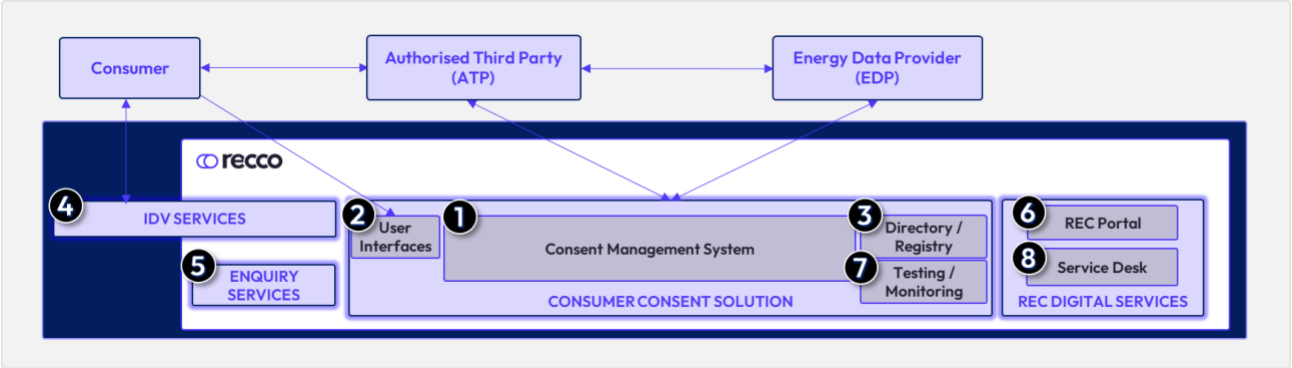


Figure 1: CCS Solution Architecture

Consent Management System (1)

6.8 At its core, the consent management system of the CCS is being designed to ensure that personal energy data is only shared by EDPs when appropriate consent and proof of occupancy have been verified centrally. More detailed designs of how the consent management system will work can be expected during future technical working group sessions, but we have identified the following minimum functionality:

- The CCS will expose a single endpoint that will communicate with ATPs and EDPs;
- For the purposes of providing tokens to allow ATPs to request data, the CCS will generate a token that is tied to the ATP. This token will contain all necessary data about the consent, drawn from the Consent Data Schema;
- An ATP will then make a request for data directly to the relevant EDP, using the token provided by the CCS;
- The CCS will expose an introspection endpoint to allow EDPs to validate if a token is still active before sending data. Only after a successful introspection can data be returned to the ATP. This introspection will include assessment of token validity, as well as checking that the information contained within the object relating to the consent allows for the request being made (for example, what is the scope of the request); and
- The CCS will provide PKI services, including the issuance of certificates to ATPs and EDPs for their communication across the ecosystem.

6.9 RECCo is proposing the use of robust, industry-recognised security standards across the ecosystem. This includes the use of mTLS for interactions between participants, including where data is exchanged, and cryptographic signing of messages to provide assurance that messages originate from known senders and have not been altered in transit.

6.10 These measures are proposed in recognition of the sensitivity of energy consumption data and the potential risks associated with malicious interception, including the exposure of information about consumers' behaviours within the home. Together, these controls are intended to provide a strong baseline level of security and trust across the CCS.

6.11 These measures form a key part of the FAPI 2.0 standard, and so implementation would be included within all implementation guides and tooling; breaching the standard just to unsecure data exchange would introduce risk to consumers and the ecosystem and represent more work than adoption of the FAPI 2.0 standard in its entirety.

6.12 RECCo recognises that not all DSAs currently utilise mTLS for their data exchange, and this may represent an increase in scope. However, to ensure consistent data integrity and to support the use of sender-constrained access tokens, mTLS is considered a necessary component of a secure ecosystem. All ecosystem participants will, in any event, be required to establish mTLS in their communications with the CCS centrally. Extending this approach to data exchange, therefore, represents an incremental step that delivers proportionate, ecosystem-wide security benefits.

6.13 In this context, we equate the implementation of mTLS for data requests and provisions as the difference the CCS operating solely as a consent management mechanism, and the CCS functioning as a secure Trust Framework for consent-based data sharing across the market.

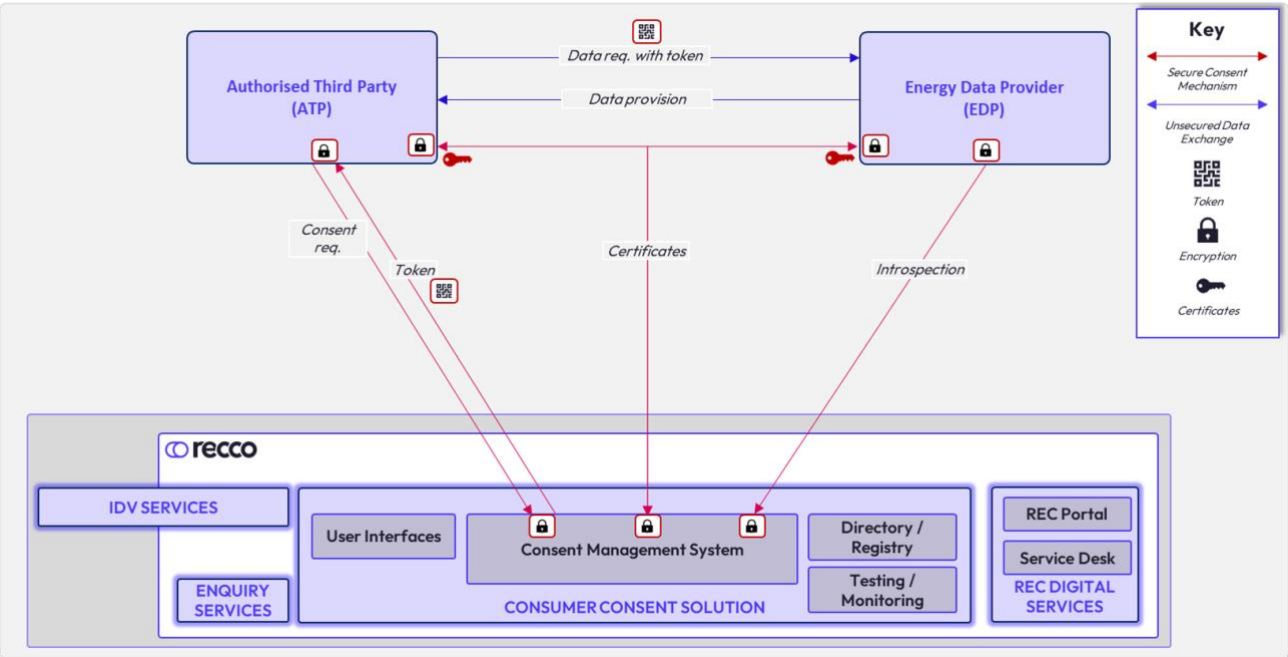


Figure 2: Consent Mechanism

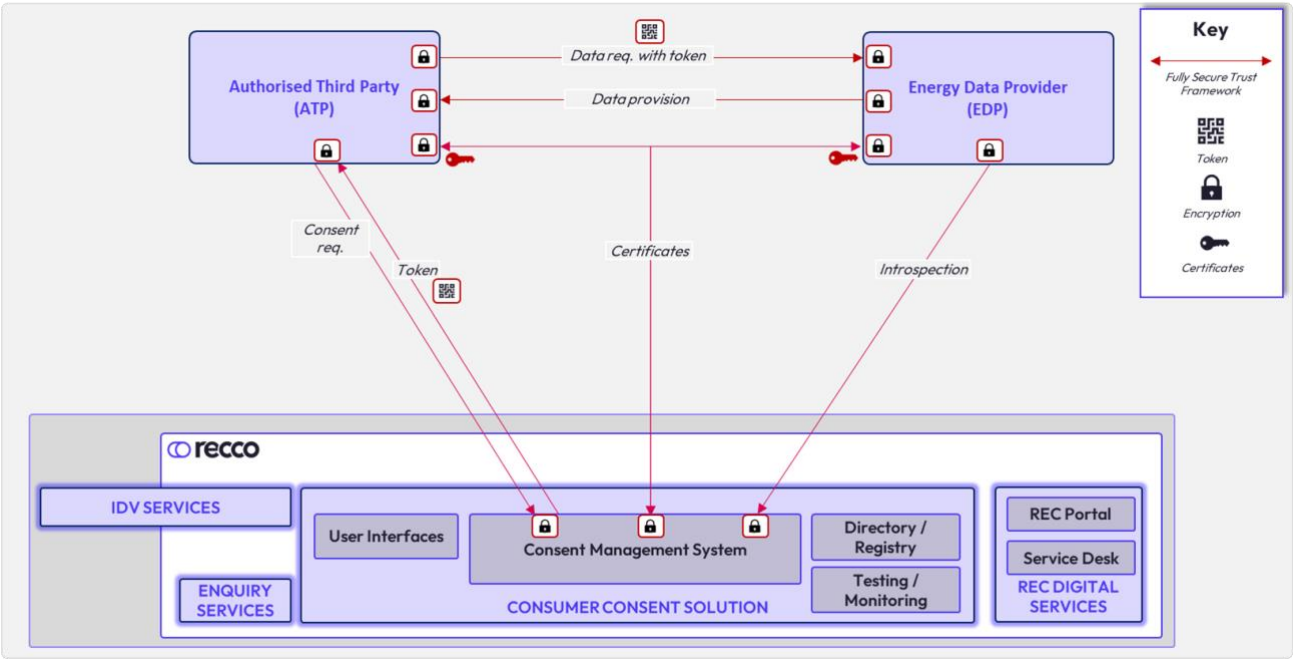


Figure 3: Secure Trust Framework

6.14 The above security standard focuses on ensuring the security of data in transit. Our other key consideration in the design of the CCS has been to ensure data at rest is also secure. This will be delivered through the inclusion of the following:

- defined Role-Based Access Controls (RBAC) to manage the ability of users to access and amend data;
- use of Multi-Factor Authentication (MFA) to provide an additional layer of protection where individuals are accessing the data held within the CCS, e.g., when consumers log in to view and manage their consents;
- maintenance of an encrypted backup in a separate secure location and regular testing of disaster recovery plans to ensure data can be restored safely;
- ensuring alignment with wider legislation, i.e., GDPR; and
- requiring the technical service provider to be ISO 27001 accredited, or equivalent.

User Interfaces (2)

6.15 Ofgem has been clear in stating a central portal is a 'must-have' requirement to ensure consumer visibility and empowerment. The exact mechanism for achieving this is still being refined: we are investigating white-labelling a CCS portal to be presented under a more recognisable brand (to be defined), versus creating a new, bespoke brand identity to represent the impartial body for energy data management in the UK.

6.16 Producing and maintaining a consumer portal for a potential consumer base of the UK's population will necessitate a high availability, reliable, responsive, and scalable platform. We discuss our views on the impact of scalability requirements later in this section.

6.17 We have identified a minimum of two distinct User Interfaces that will need to be delivered for the CCS: a central portal for consumers to view, manage, and revoke their consents, as well as an admin portal to facilitate management of the ecosystem by RECCo and CCS Users.

6.18 Consumer Portal – the following minimum functional requirements will be delivered via the consumer portal:

- The consumer portal will be API-driven to ensure ATPs are able to easily create their own version to enable direct-to-consumer relationships.
- The portal will enable consumers to view all active consents where they are the Data Subject, with options to renew or revoke where appropriate. Historic consents will also be visible where they were the individual responsible for granting that consent;
- Individuals will not have visibility of DSAs in place within a property prior to their own period of occupancy;
- The solution will facilitate consumer queries regarding consent data, as well as support consumers with any disputes. Further information on dispute management is included in Section 8;
- The solution will allow consumers to notify the CCS when they have moved, or are moving, out of a property. This would trigger the revocation of any consents granted by that consumer in relation to the property;
- The solution will allow consumers to notify the CCS of a change of address, or imminent change of address, to trigger further address-matching activities; and
- This portal will be user-friendly and designed according to the CEGs (see Section 7).

6.19 Admin Portal – the following minimum functional requirements will be delivered via the admin portal:

- The admin portal will be used by RECCo personnel to manage and observe the CCS ecosystem. Activities may include enabling access to accredited organisations, reviewing and publishing new DSAs, and administering the CCS operational functions;
- The admin portal will also provide controlled self-serve functionality for CCS Users, allowing them to self-manage their own organisational metadata in the Directory (including certifications, etc.), as well as their registered datasets in the Registry. CCS Users will only be able to view or amend information relating to their own organisation;
- The admin portal will have Role-Based Access Controls to allow various user types to manage data only according to their access rules. There will be a clear separation between RECCo administrative roles and CCS User self-service roles; and
- Given the privileged nature of certain administrative activities, administrative actions within the portal will be logged and auditable, with monitoring in place to support operational oversight and assurance in line with existing REC governance and performance assurance arrangements.

Directory / Registry (3)

6.20 A fundamental component to enable seamless discovery and access to data through the CCS will be a central Directory and Registry. The CCS Directory / Registry will have the following minimum capabilities:

- Organisations will be able to interact with the Directory/Registry either using the admin portal or through APIs;

- The Directory will allow organisations to publish metadata such as Organisation IDs (which will be unique across the ecosystem) and certificates (such as transport certificates for mTLS);
- The Registry will allow organisations to register their datasets with associated metadata, as well as facilitate publication of endpoints so ATPs know where they can access data;
- Additionally, organisations will be able to register webhooks with the CCS in the Registry to enable immediate updates to consent records when there is a change to the data held within the CCS;
- The Directory / Registry will be an API-first solution which any organisation within the ecosystem can access and discover the information within it; and
- The Directory / Registry will allow organisations to configure their DSAs to reflect existing or new relationships. These arrangements will be reviewed by RECCo before publication. This will enable continuation of existing relationships in the energy market for data sharing, with appropriate transparency to promote wider data usage.

6.21 We are working towards refining how the Directory / Registry will incorporate both open data discovery, datasets and APIs that are publicly viewable, and other tiers (for example, the potential for private commercial APIs that can be queried according to access conditions).

6.22 Deeper technical design work will take place following onboarding of the technical service provider to outline the low-level details of what information organisations will be required to register and publish in the Directory / Registry. This will be further discussed with industry via working group meetings

IDV Services (4)

6.23 A central IDV capability will be delivered as part of the CCS. RECCo is still undergoing deeper technical assessment of the requirements for this capability but it is expected that the following technical requirements will form the basis of the future IDV capability for the CCS:

- The MMP will include a central IDV solution at a minimum for MMP. We are aiming to offer multiple options to minimise consumer drop-off, but it is subject to timelines whether this will be available for MMP;
- When authenticating consumers, we will adhere to Good Practice guidelines produced by the Government Digital Services function (see Section 5); and
- The IDV capability will need to produce or align with unique identifiers created by the CCS; the exact mechanism for this is still being considered. A unique identifier will be essential to ensure the solution maintains an individual consumers' records across multiple actions with multiple services and ATPs. We are yet to determine if this unique identifier will need to be equivalent across the industry, and if so, who master's it. More work is needed to reach low-level designs and this issue will be approached in upcoming working group meetings. We recognise the importance of ensuring this works effectively, and will work with industry and future IDV partners to find the best solution.

6.24 Consumers will be redirected to the IDV solution when authentication is necessary. The cases where this is required will be:

- When a consumer is consenting for the first time and therefore the CCS has no record of the consumer;
- Where a consumer has used the CCS before, but without registering an account with the solution. This would force a reauthentication to prove their identity and occupancy of a property when granting consents for any new services; and

- When a consumer has been prompted to reauthenticate based upon periodic reauthentication processes.

6.25 In future, as the CCS scope expands, we will consider the potential for federated IDV only where there is sufficient confidence in the level of IDV undertaken by other ecosystems of Identity Providers. Federated IDV in this case would allow consumers to prove their identity using another service, such as through their bank with Open Banking or through a Government-backed identifier such as Gateway ID or the NHS . In this scenario, the CCS effectively 'trusts' the other ecosystem or service, removing the need for the user to prove their identity directly to the CCS. In order to achieve such federation, we are keen to ensure the backend systems we design for the CCS are interoperable with other such systems as a guiding principle.

Enquiry Services (5)

6.26 In addition to verification of an individual's identity, the sharing of energy data linked to a physical device e.g., consumption data at a specific metering point, also requires a mechanism for linking that individual to the specific address and associated MPxN(s).

6.27 It is proposed that this matching activity is carried out by the CCS itself using the gas and electricity enquiry services, with a direct API feed into the CCS. The enquiry services are owned and governed under the REC, displaying addresses matched to MPxNs by the Central Switching Service address management function.

6.28 If possible, we plan to utilise the Retail Energy Location (REL) Address to support this matching activity as this is the address used for supplier interactions with consumers. However, we recognise that the use of this address data is currently limited to use for switching purposes only. We are currently engaging with Data Communications Company (DCC) and Ordnance Survey to understand the existing licence arrangements relating to use of the REL Address with the aim of extending this usage to cover matching for the purposes on managing consumer consent. If we are unable to get access to the REL Address, in time for MMP delivery, our fallback position will be to utilise the Meter Point Location (MPL) Address.

REC Portal (6)

6.29 Our working position is that the best option for accreditation and onboarding of organisations into the CCS will be to uplift the existing Non-Party REC Service User application process, utilising existing functionality within the REC Portal, rather than developing a stand-alone onboarding mechanism directly into the CCS. This will enable a streamlined accreditation process for Non-Party REC Service User applications, effectively enabling access to multiple services though a single application form (for example, organisations can apply to access Enquiry Services and the CCS simultaneously).

6.30 Once the initial application has been processed and the applicant has been approved as a CCS User (in accordance with the accreditation arrangements described in Section 8), details will need to be included within the CCS itself.

6.31 The following minimum functionality will be delivered within the REC Portal:

- Provision of streamlined application forms, amended from existing forms and enabling multi-service access, to allow Non-Party REC Service Users to apply for access to services
- Provision of communication channels for access and support for organisations that are applying to become CCS Users
- Provision of ongoing communication channels for accredited organisations

Testing / Monitoring (7)

Testing Capabilities

6.32 It has been made clear throughout working group discussions and through observation of other data sharing ecosystems across the globe, that comprehensive testing capabilities within the enduring solution will bolster compliance and maximise the effectiveness and success of the ecosystem as a whole.

6.33 RECCo is considering three distinct testing capabilities to be included in the CCS MMP:

- Sandbox testing environments to allow organisations going through the accreditation process to start building and testing their integrations in parallel.
- Pre-production testing capabilities, potentially self-serve using the central portal, to allow ATP and EDP developers to test new APIs prior to release and mitigate risk of downtime in the live environment.
- 'Live' testing capabilities including automated testing within the central solution to test against agreed metrics, as well as scripted scenarios to test end-to-end business processes. This also could potentially be delivered in a self-serve platform to aid ecosystem developers.

6.34 With regards to the potential inclusion of 'live' testing capabilities, we understand that CCS Users need to be confident that when they call an API, the appropriate data will be returned within expected timelines and according to expected specifications. Continuous testing can proactively identify issues and alert teams to respond, maximising uptime. Additionally, by implementing automated testing, additional burdensome assurance activities may be removed delivering a net benefit for industry. However, more work is needed to map out the precise testing capabilities that will be needed to ensure the success of the CCS programme. This will include assessment of the cost and benefits associated with the 'live' testing capabilities as RECCo progress through procurement and low-level design phases.

Monitoring and Reporting

6.35 Effective monitoring and reporting will be central to ensuring that the CCS operates reliably, securely, and in line with consumer expectations. The REC provisions will therefore define a monitoring and reporting framework that provides transparency across the full CCS ecosystem-covering system performance, CCS User behaviour, consumer experience, and data protection outcomes. The approach is designed to maximise uptime of APIs, detect issues early, support a data-driven assurance model, and provide evidence for the REC Performance Assurance Framework (PAF).

6.36 The key objectives of monitoring and reporting in relation to the CCS are to:

- ensure compliance with the REC, CCS Arrangements Schedule, and CEGs;
- identify emerging risks relating to system performance, security, data protection, or consumer experience;
- support proportional and risk-based performance assurance under the REC PAF (see Section 8);
- provide early visibility of behaviours that may undermine consumer trust;
- enable Ofgem and other regulatory bodies to understand the effectiveness of the CCS framework; and
- inform continuous improvement of the CCS design, processes, guidance, and technical implementation.

6.37 Further information on the proposed monitoring approach is included in Annex D.

6.38 The CCS monitoring approach is built on the principle that data should be collected automatically wherever possible. Automation reduces administrative burden, increases accuracy, and allows RECCo to identify issues in near real time. Automated monitoring will appropriately distinguish between CCS system metrics and CCS User metrics.

6.39 Manual reporting will only be required where automation is not technically feasible or where qualitative insight is needed.

6.40 Monitoring outputs will be used to update risk assessments, trigger assurance activities, and inform escalation through the REC PAF. The detailed operation of assurance, escalation and enforcement mechanisms is set out separately within the REC PAF.

6.41 Monitoring will form a key input into ongoing development of the CCS. Insights will guide updates to technical specifications, consent journeys, accreditation requirements, and the CEGs. Monitoring processes will evolve as the CCS expands to additional consumer segments or incorporates new DSAs.

6.42 CCS-level insights will support infrastructure scaling, technology updates, and service reliability improvements, while CCS User-level insights will support evolution of accreditation requirements, onboarding controls, and behavioural expectations.

6.43 Should ecosystem participants have any queries relating to reports or monitoring, they will be able to raise these through the single Service Desk functionality being designed for the CCS

Service Desk (8)

6.44 We recognise the importance of service desk capabilities to support organisations in their implementation and ongoing operation of DSAs within the CCS. Alongside effort to streamline how industry interfaces with the REC, this service desk will form part of the existing REC service desk functionality.

6.45 The service desk will perform various important roles in maximising the success of the ecosystem, including:

- Being the single point of contact to handle requests and queries from organisations in the ecosystem to support onboarding and business as usual operation from both a technical and governance perspective;
- Providing updates, alerts or notifications to organisations within the ecosystem where required, such as to update on issues, consent queries, incidents, outages, or performance issues;
- Providing updates, alerts, or notifications to end consumers when queries have been raised; and
- Providing service line support functions in the event of incidents including 1st line and ticket management services, as well as 2nd / 3rd line software support where required.

6.46 The service desk is expected to be available 24/7 x 365 to support resolution of high priority (P1) issues in accordance with the overall availability of the CCS. This high availability is designed to ensure prompt and suitable support for energy industry organisations, facing issues with the CCS functionality which is preventing real time consent management activities. Lower priority (P2 and lower) query resolution will be managed within the standard RECCo business hours aligned with the approach applied to existing REC Services (typically Monday to Friday, 9am to 5pm). RECCo is in the process of determining the precise Service Level Agreements and more work is needed to identify the low-level design of the operational support functionality.

Non-Functional Requirements

6.47 A strong focus of discussions to date has covered the functional elements of the CCS and the mechanisms for managing consent data. We have also initiated high level discussions regarding the non-functional requirements that will need to be defined, both for the CCS technical solution and also requirements on both ATPs and EDPs required to make the end-to-end consumer journey effective.

6.48 We expect the national adoption of services requiring personal energy data sharing to scale over time. As a result, we are looking to procure and manage a solution that is capable of scaling to meet demand which we forecast as modest initially but with the potential to grow into a solution meeting the needs of a significant portion of the UK population.

6.49 This scalability requirement extends beyond simply handling increased traffic. It is imperative that as uptake of the tool grows amongst consumers, and its importance to CCS User activities increases through a bigger scale of delivery, that the availability of the solution increases as well. We are therefore intending to design and procure a CCS that can flex in its capacity and availability to deal with a significant increase in demand over time.

6.50 We have provided an initial view of the areas we are seeking to cover through non-functional requirements, within Annex D Through this consultation we are seeking feedback on the completeness of this list and welcome any views on the potential values that should be applied against these requirements.

6.51 This table of non-functional requirements is additional to the security requirements that will be defined for the CCS itself as set out above.

Technical Diagrams

6.52 You can find technical views of the following solution aspects in Annex E:

- IDV;
- Consumer Consent Management;
- Data Sharing Interactions;
- Ecosystem Management;
- Directory / Registry Interactions; and
- Full Proposed Solution Design

Centralised versus Decentralised Components

6.53 Through the August 2024 consultation, Ofgem explored views on whether the CCS should be fully centralised or decentralised, with the final conclusion pointing to a hybrid model, as reflected in the diagram below.

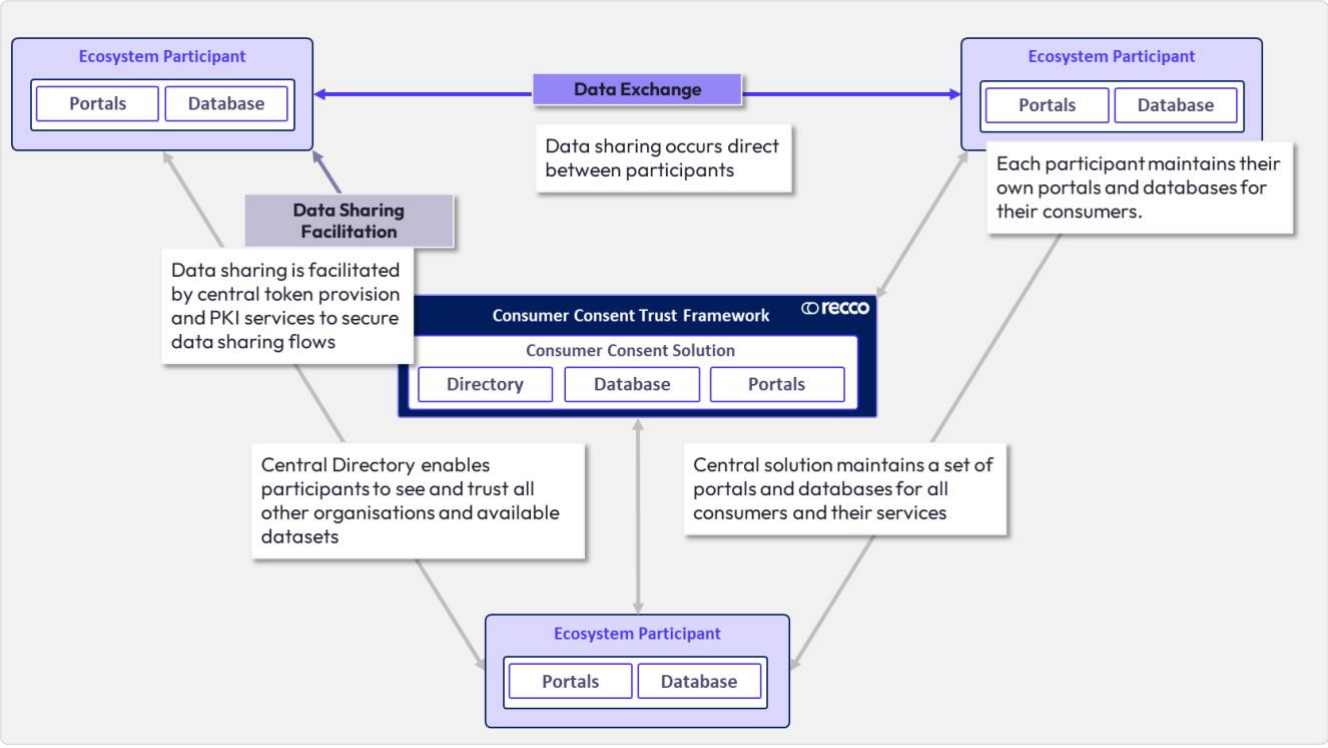


Figure 4: Hybrid CCS Model

6.54 The following table outline some key boundaries where we see the hybrid design as fitting best for industry and Ofgem's aims with the CCS. Please note, more information regarding our approach to these aspects of the proposed solution can be found in Annex D.

Component	Centralised Elements	Decentralised Elements	Our Rationale
Token Provision and Ledger	• Central issuance of tokens (FAPI 2.0 + mTLS) • Central consent ledger	• ATPs are able to allow ongoing consent management directly with their customers, with updates provided to central ledger	• Ofgem requires a single source of truth for consent records. • Centralisation improves auditing, standardisation, and arbitration.
Identity Verification	• Central IDV solution	• Suppliers could upgrade their own KYC—but not favoured short-term	• Energy sector lacks universal KYC standards, increasing misappropriation risk in a decentralised model. • Central verification raises security standards without requiring all suppliers to build new capabilities immediately.
Data Sharing	• CCS enforces minimum security & interoperability requirements	• Actual energy data exchanged directly between EDPs and ATPs	• CCS governs trust and security between EDPs/ATPs within the Trust Framework only. • Beyond that point, GDPR governs how ATPs share data further • No central data lake; reduces single-point-of-failure risk.
Data Formats and Structures	• Central "Consent Data Schema" • Standard lexicon via CEGs	• ATPs and EDPs free to format structure data as they wish • Proposal to develop centralised data formats through the Energy Market Data Specification if needed	• Interoperability needed for consent management necessitates Consent Data Schema • Full half hourly metered data schema impractical due to diverse use cases, but development of a standard may be beneficial for interoperability. • Some datasets (e.g., SDR) remain under originating body governance.
Directory / Registry	• Central Directory of ecosystem participants • Registry of accessible datasets	• Participants still allowed bespoke commercial agreements	• Supports API-first, open data discovery. • Facilitates interoperable data sharing across energy sector. • Commercial arrangements are allowed but must be approved by RECCo.

Data Storage	• Central consent record storage • Central database for assurance & arbitration	• Energy data itself not stored centrally • Organisations retain their own GDPR-required consent copies	• No centralised data lake by design. • Webhooks keep local and central consent records synced.
User Interfaces	• Central consumer portal • Central admin portal for CCS Users	• ATPs can maintain direct relationships and interfaces with customers	• Ofgem states a consumer portal is a 'must-have' requirement • Consumers can use the CCS portal or use ATP interfaces if they wish for consent management. • Admin portal enables self-serve certificate, API and dataset management for ecosystem participants.
Model Summary	• Hybrid model with centralised trust & identity functions	• Data remains decentralised and flows directly between participants	• Balance between consistency, security, and flexibility. • Reduces duplication while respecting diverse data origins and use cases.

Business Processes

6.55 The functional components built into the overall solution architecture are used to support a number of operational business processes for managing consent. These business processes are summarised below and mapped out through indicative CCS Business Process Diagrams (BPDs) included in Annex E. As part of this consultation, we are seeking industry feedback on these BPDs which will then be baselined and reflected within the REC code drafting being developed in 2026.

- E2E granting of consent (consumer is registering, or is registered within the central portal);
- E2E granting of consent (consumer chooses not to register within the central portal);
- Consent management through the ATP - revocation and renewal;
- Consent management via the central portal – revocation and renewal;
- ATP onboarding;
- EDP onboarding; and
- Queried consent.

7 User Experience (UX) Design

Q16. We have identified four groups of people who will use the consent system, each with different needs (Annex F – Behavioural Archetypes). Have we missed any important user groups? Are there any needs we haven't considered for any of these groups? If yes to either, please tell us what's missing and why it matters.

Q17. Do the proposed inclusion requirements adequately address the needs of vulnerable customers, digitally disadvantaged consumers, and consumers with limited English proficiency (Annex F – Accessibility and device constraints)? If not, what additional requirements should be included?

Q18. Do you agree that consumers need to know who is requesting consent, what data they want, and for how long? If not, what's missing? Is there a risk of information overload?

Q19. Where should additional verification steps or friction be introduced to protect consumers? Where might such steps create disproportionate barriers? (Refer to figures 7–10: User journey stage)

Q20. Do you agree that showing consumers which organisations hold consent, what data is shared, when consent was granted, and when it expires provides adequate visibility? If not, what's missing? What limitations should be communicated to manage expectations

Q21. Do you agree that consumers need to understand which services will be affected, what happens to their data, how long changes take, and whether revocation is reversible? If not, what's missing? Is there a risk of information overload at the point of revocation?

Q22. Do you agree that assisted journeys should enable consumers to grant consent, review active consents, revoke consent, and receive the same information as digital users? If not, what additional outcomes are needed to achieve equivalence?

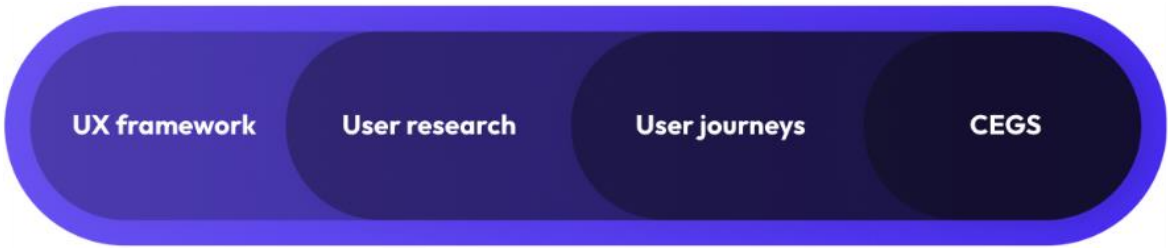
Q23. For consumers who are unable or choose not to use digital services, what outcomes should an assisted or alternative consent service journey deliver to be considered fair and equivalent?

Overview

7.1 This section sets out the proposed approach to UX within the CCS. Its purpose is to establish a coherent and proportionate minimum standard for how consumers encounter CCS-governed consent interactions, ensuring clarity, trust, and accessibility across the market. The approach reflects the CCS Design Principles and is intended to support a consistent baseline experience while allowing ATPs flexibility in how they design their wider customer journeys and service propositions. This section is presented for consultation to test whether the proposed approach is proportionate, implementable, and sufficient to support consumer trust at MMP.

The Role of the UX Framework

7.2 The UX Framework acts as the foundation for all consumer-facing consent interactions. It focuses on the moments where the CCS is brought into play and defines how those moments should function and be understood from a consumer perspective.



Purpose	Sets the foundation for how consent should be experienced across the CCS	Ground UX standards in real consumer behaviour and risk, in collaboration with industry	Translate principles and research into concrete consent interactions	Enable consistent, trustworthy implementation across ATPs
Key outputs	• CCS UX Framework • Design Principles applied to consent interactions • Defined scope of CCS UX application	• Consumer needs and pain points • Validated design assumptions • Identified trust, comprehension and inclusion risks	• Core consent lifecycle stages (Grant, Renew, Review, Revoke) • Expected consumer outcomes per stage • Consideration of guest and full account access models	• CEGs • Minimum UX requirements and guardrails for CCS touchpoints
Key outcomes	• Shared baseline for "good" consent experience • Reduced risk of fragmented or inconsistent journeys	• Evidence-based UX standards • Proportionate expectations aligned to real consumer behaviour	• Shared understanding of how CCS consent should work • Clear bridge from principles to implementation	• Recognisable and consistent consent experiences • Greater consumer trust and reduced implementation ambiguity

Figure 5: The approach to define the UX solution for the CCS

7.3 The Framework has been informed by early consumer research, behavioural insight, and working group input. It recognises that although consumers will typically enter the CCS journey through an ATP service, the CCS must provide a clear, predictable and recognisable experience wherever it appears.

7.4 The Framework is therefore structured around transparency, accessibility, and consistent communication. Rather than prescribing detailed screen designs or mandating channel-specific layouts, it sets out the patterns, expectations and safeguards required to ensure confidence in the CCS as a trusted mechanism for managing consent to share personal energy data. It represents the current stage of understanding and is expected to evolve as further consumer research, usability testing, and behavioural evidence emerge during the CCS development.

7.5 The CEGs will translate this framework into practical standards for implementation.

The Role of the CEGs

7.6 The CEGs will serve as the binding tool for implementing the UX Framework. They will provide structured guidance for ATPs and other ecosystem participants on how the CCS interactions should be delivered, including expectations around language, accessibility, trust signals, error handling, and framing of purpose. While the CEGs will not govern ATPs entire service journeys, they are intended to ensure that the moments involving the CCS consent are consistent, recognisable, and compliant with REC requirements.

7.7 Compliance with the CEGs will be monitored through the REC Performance Assurance Framework, with provision for periodic review and refinement as the CCS evolves.

Minimum UX Expectations for the CCS

7.8 In defining minimum expectations for the MMP, the emphasis is on proportionality, clarity, and the appropriate use of friction. The consent process must be straightforward, with information presented in a way that enables informed decision-making without overwhelming consumers. Consumers must clearly understand who is requesting access to their data, what is being requested, and why. Explanations should be presented in plain English and remain concise, with the option to explore more detail where consumers wish to do so. This is intended to support informed, explicit consent in line with applicable data protection requirements.

7.9 The CCS will require identity verification at key points, and consumers must understand both why verification is necessary and how the process protects them. This includes an explanation of when identity re-verification is required and when existing verification can be relied upon. Where consumers operate as guests rather than establishing a CCS account, the experience should remain simple and predictable, with the same level of identity assurance applied to protect the integrity of the consent record.

7.10 At each interaction point, granting, reviewing, renewing, or revoking consent, the CCS should supply a clear narrative explaining the purpose of the action, the consequences of proceeding or not proceeding, and any relevant timeframes or conditions. Lists of data fields, legal terms, or technical descriptions should be avoided unless they are strictly necessary. The aim is to support comprehension and reduce cognitive load, not to replicate the internal structures of the system.

Supporting Different Consumer Needs

7.11 The UX Framework has been informed by behavioural archetypes that capture how different consumers approach decision-making, risk, effort, and comprehension. These archetypes are not demographic groups, but behavioural patterns observed across a diverse range of users. They are analytical tools used to interpret behaviour and test risk, not categories applied to individual consumers. They include consumers who are comfortable and confident with digital services, those who are financially cautious or anxious, those who manage significant personal or cognitive load, and those who are time-constrained.

7.12 The four behavioural archetypes include Comfortable Data Enthusiast, Careful Budgeteer, Surviving Juggler, and Time-Poor Professionals, further information on the behavioural archetypes is included in Annex F.

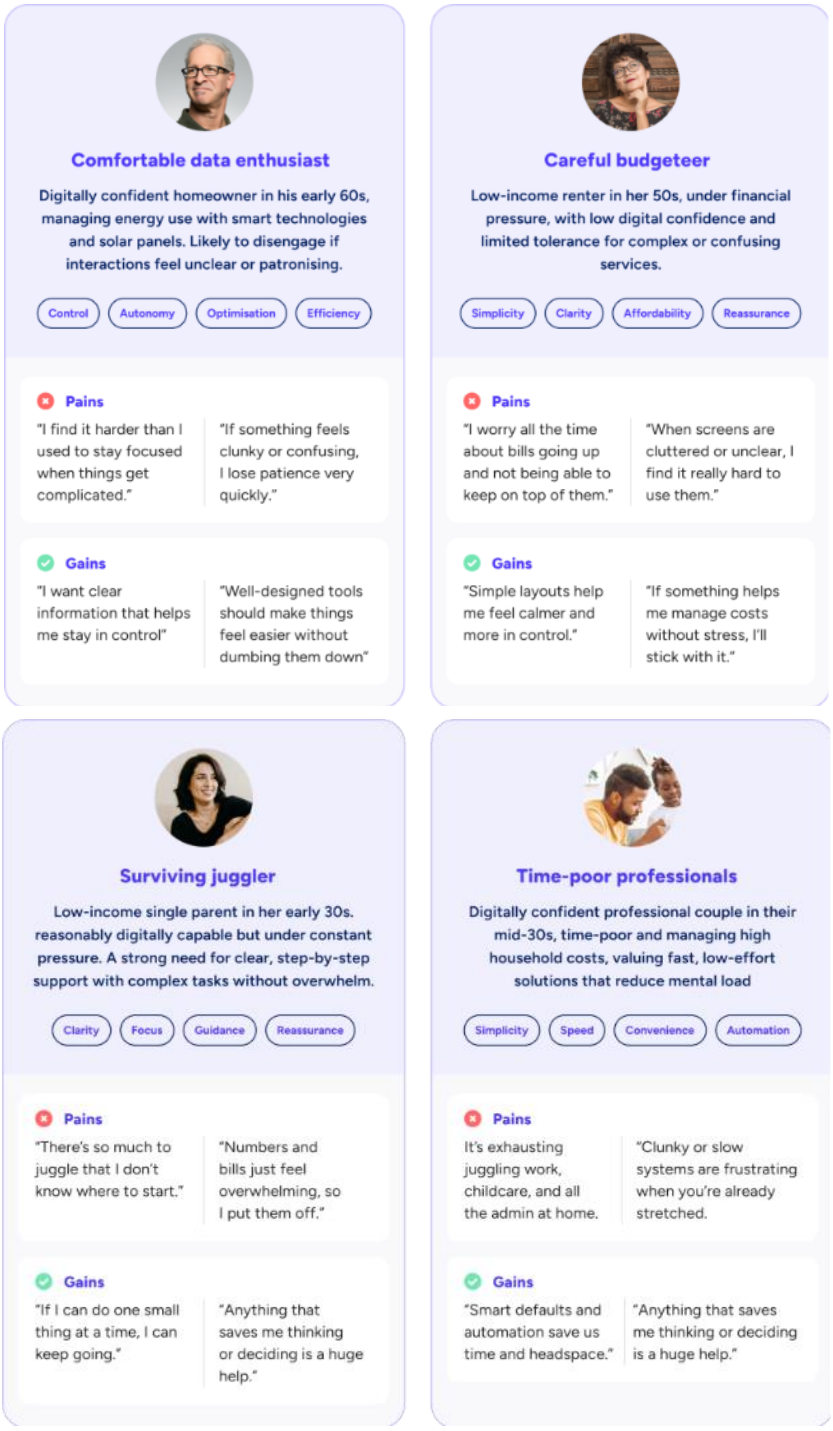


Figure 6: Behavioural archetypes used to interpret consumer needs, risks, and design considerations when developing the CEG

7.13 The CCS must work effectively for all of these users. This requires that key information be provided in a direct and digestible manner, journeys do not rely on assumed technical fluency, and the ability for consumers to pause, return, or seek support where needed. It also requires that additional details be made available to consumers who wish to access it, without imposing unnecessary complexity on others.

7.14 Accessibility is treated as a cross-cutting requirement rather than a characteristic of specific archetypes. Consumers may face temporary, situational or permanent barriers, including reduced cognitive capacity, limited dexterity, low literacy, sensory impairments, or limited English proficiency.

7.15 Journeys must therefore be designed to support these needs through clear language, consistent structure, predictable patterns, and alignment with WCAG 2.2 AA accessibility standards, further information is included in Annex F. Where digital channels are not appropriate or available, assisted or alternative journeys must provide equivalent outcomes.

Experience Across the Consent Lifecycle

7.16 The CCS consent journey is structured around four core lifecycle stages that reflect how consumers grant, manage, and revoke consent over time. These stages represent the key moments where consumers are asked to make a decision, review their understanding, or take action in relation to their consent. The core lifecycle stages are:

- Grant: giving consent;
- Renew: continuing consent;
- Review: checking and managing consents; and
- Revoke: withdrawing consent.

Granting consent

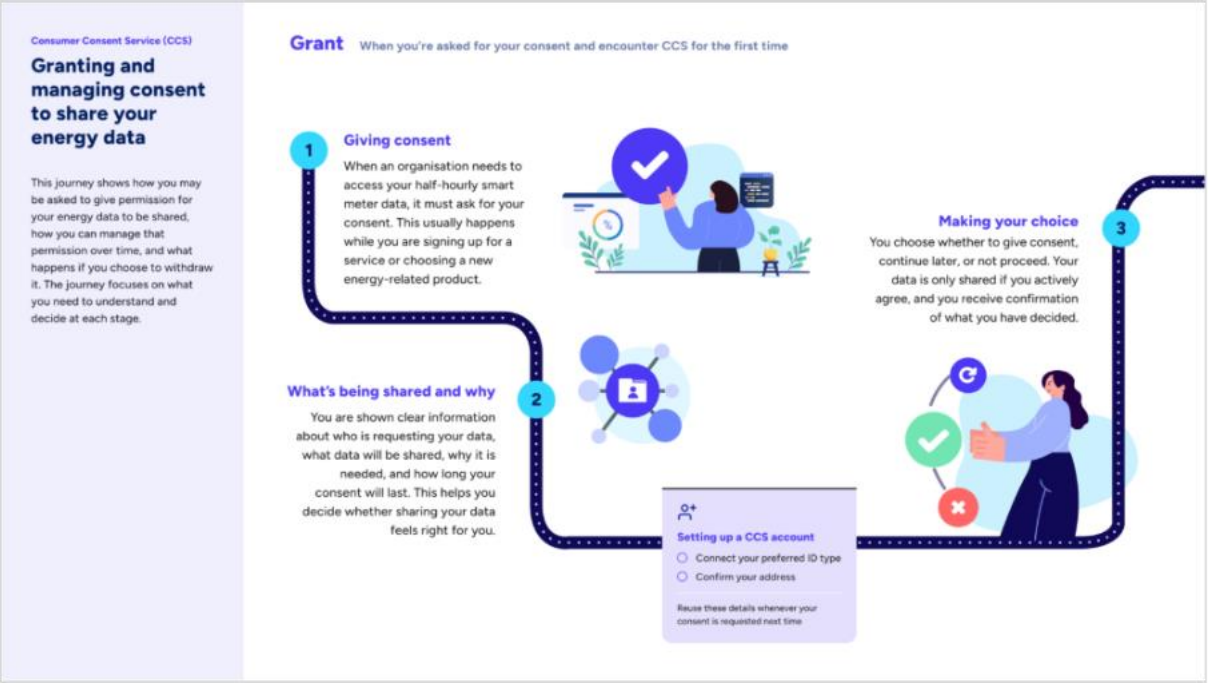


Figure 7: User journey Stage: Grant Access

7.17 When granting consent, consumers must understand what they are agreeing to and the implications of that consent. This is typically the point at which trust and reassurance are most critical. At this stage, consumers should be able to:

- Identify who is requesting access to their data, what will be shared, why, and for how long;
- Give consent in an informed and explicit manner, in line with applicable data protection requirements;
- Receive confirmation when their consent has been granted, or when they choose not to proceed;
- Be supported across both 'guest' and 'full account' experiences, with clear explanations of any differences; and
- Exit the journey safely, without unexpected consequences.

Renewing consent

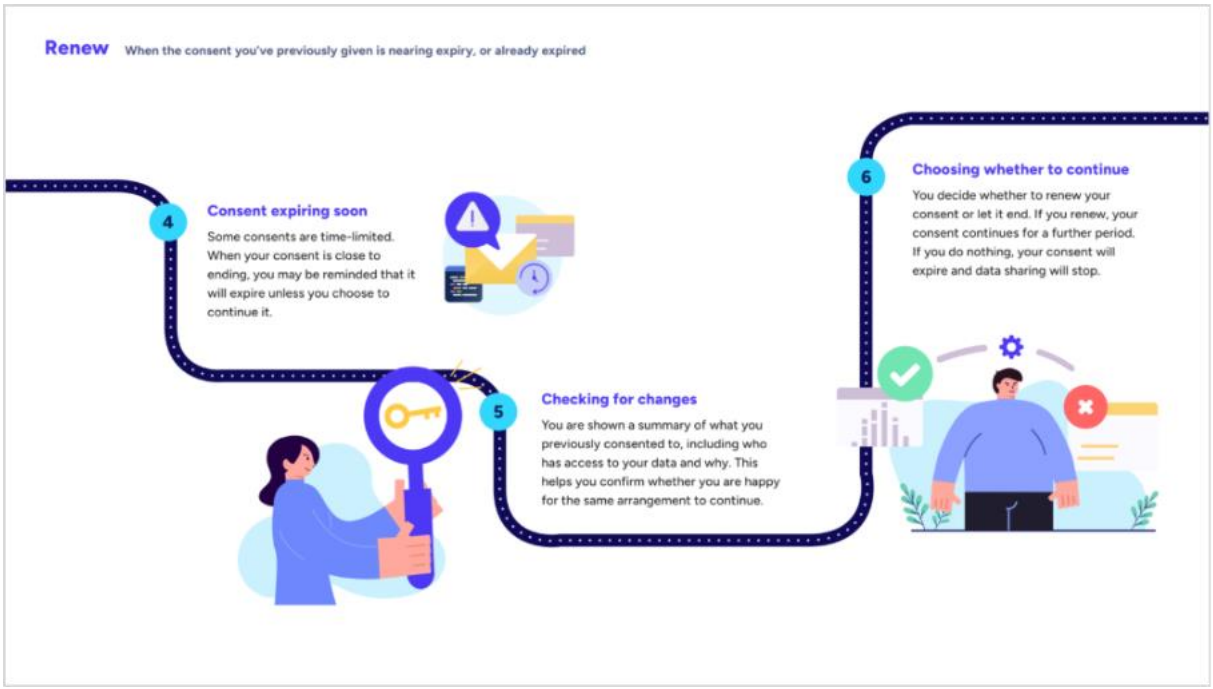


Figure 8: User journey Stage: Renew Consent

7.18 Consumers should understand when their existing consent is coming to an end and the implications of renewing or taking no action. This stage is intended to maintain continuity and control, while avoiding unnecessary friction where the scope of consent remains unchanged. At this stage, consumers should be able to:

- Understand when consent is expiring, what will happen if no action is taken, and allow consent to expire without unintended consequences;
- Renew consent through a simple confirmation where there has been no material change, with access to a clear summary of their existing consent if they choose to review it; and
- Receive clear confirmation of the outcome of their decision, with explanations and recovery options where renewal cannot be completed due to system or validation constraints.

Reviewing consent

Figure 9: User journey Stage: Review Consent

7.19 Consumers must be able to understand the consents currently in place and identify any unexpected elements. At this stage, consumers should be able to:

- View active consents, including which ATPs have data access, what is shared, and consent duration;
- Feel reassured that consent details are accurate and clearly displayed;
- Take action as needed: renew, withdraw, or raise concerns about consents (see Section 8 for Issue and Dispute resolution); and
- Manage consents in various ways based on access, such as through an ATP's service or the CCS Consumer Portal.

Revoking consent

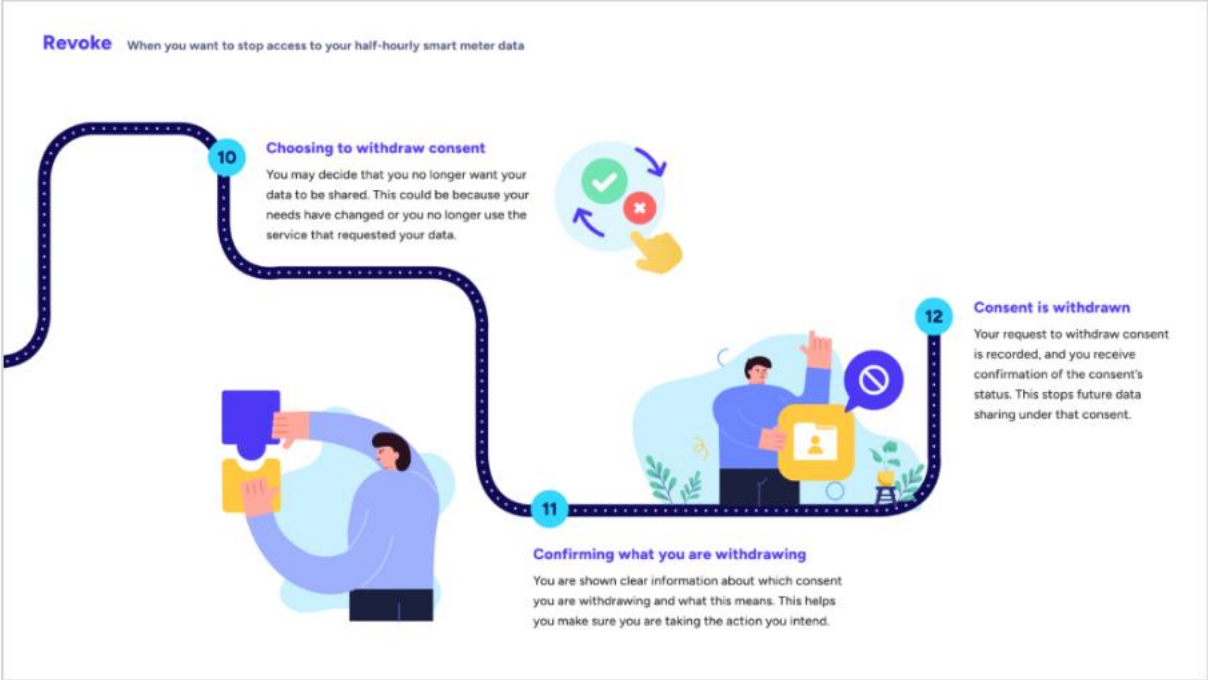


Figure 10: User journey Stage: Revoke Consent

7.20 At this stage, consumers must be able to withdraw their previously granted consent. Revocation should be straightforward and include an explanation of both immediate and longer-term consequences, including any impact on services consumers currently use. Additionally, consumers should be able to:

- Find and choose to revoke consent, with revoking being as easy and visible as granting it, no matter how users access the service;
- Understand what revoking consent means for future data sharing and dependent services;
- Receive clear confirmation that their request to revoke consent has been recorded and know its status; and
- Be informed if there are processing constraints for revocation, including what this means and what steps to follow.

7.21 Across all stages, the CCS must handle errors, incomplete actions, and identity mismatches in a clear and supportive way. The intent is not only to avoid consumer confusion but also to build confidence that the system is robust, predictable and aligned with consumer rights under data protection legislation, further information on common experience components is in Annex F.

Visibility and Boundaries of the CCS

7.22 Consumer confidence will be reinforced through a clear understanding of what the CCS does and does not display. Consumers will be able to view active consents associated with MPxNs to which they are matched, including the purpose of the access and the organisation accessing the data.

7.23 The CCS will not display the identities of other individuals associated with the same MPxN, nor will it surface data-sharing instructions that fall outside consent-based mechanisms, such as data sharing under legal obligation. Clear messaging is therefore required to prevent misinterpretation of the information presented.

7.24 Responsibility for investigating and resolving concerns relating to consent validity in multi-occupancy scenarios will remain with ATPs. The CCS will provide mechanisms that allow consumers to raise and flag concerns where they believe a consent may not be valid, without exposing information that could infringe on another individual's privacy.

8 Governance Design

Q24. Do you have any comments on the proposed REC drafting approach, including the creation of a new REC CCS Arrangements Schedule, a new CCS Service Definition, the Customer Experience Guidelines, consequential changes to existing REC artefacts, and the new CCS API Technical Specification?

Q25. Do you agree with the proposed initial funding model, including the ability for the cost of qualification and breach investigation activities to be recovered from the individual organisations? If not, please provide rationale.

Q26. Do you agree with the proposed CCS Accreditation model? If not, please provide rationale.

Q27. Do you agree that a minimum standard should be set whereby all CCS Users should be Cyber Essentials Plus certified or ISO 27001 accredited? If not, please provide rationale.

Q28. Do you have any comments on the application of the existing REC change process to cover management of the CCS arrangements?

Q29. Do you have any comments on the application of the existing REC performance assurance framework to cover assurance of the CCS arrangements?

Q30.Do you have any comments on the proposed issue/dispute resolution paths defined for management of CCS issues?

8.1 This section sets out the proposed approach to incorporating the new CCS arrangements within the REC and defines the five core elements of the CCS governance framework. Feedback on this consultation will inform the development of detailed REC drafting, which will be raised as a formal REC Change Proposal and taken through the standard REC change management process, including further consultation and decision in line with REC governance.

8.2 The fundamental principle underpinning the CCS governance design is that we will develop an open, transparent, and robust governance framework, with a clear focus on consumer trust. This reflects Ofgem's position that the CCS is first and foremost a consumer-protection mechanism, and therefore, its governance must provide assurance that consent is captured, stored, shared, and revoked in a manner that is consistent, auditable, and safe across all market participants. This will build and maintain trust in the appropriate sharing of data, which should enable further data sharing to support innovative services that rely on consumer data.

8.3 With direction from Ofgem that the governance of the CCS should fall under Ofgem's regulation, and the selection of RECCo as the delivery body; we have defined the proposed CCS governance design to utilise, where appropriate, existing REC arrangements. To avoid creating parallel or inconsistent frameworks and to minimise the time and costs required to deliver the solution, our approach has been to adopt and extend proven REC mechanisms wherever they are already established, and to introduce new governance components only where CCS-specific requirements demand it.

8.4 As we progress with the development of REC provisions, we will continue to be mindful of the ongoing work under the Energy Code Reform[11]. In particular, we recognise that the code reform programme proposes that RECCo will become a licensed Code Manager, which will introduce new statutory obligations and require the REC to transition to the future arrangements introduced through Code Reform. Whilst we do not anticipate direct impacts, we will continue to work closely with Ofgem and the Performance Assurance Board to ensure that draft CCS provisions remain fully aligned and dovetail with the evolving Code Reform changes.

REC Drafting Approach

8.5 The REC itself comprises of a Main Body, which defines the core governance arrangements, party obligations, and legal provisions that underpin the operation of the retail energy market; together with a number of operational schedules and technical specifications that support underlying business processes.

8.6 We do not currently anticipate that any changes to the REC Main Body will be required in order to introduce the CCS arrangements. The main focus of the REC drafting will include the introduction of a new operational schedule, associated technical documentation, and consequential changes to other REC artefacts detailed below.

8.7 However, we recognise that the CCS introduces new terminology, new categories of users (such as Authorised Third Parties), and new interactions with existing REC Services. As such, these terms will be added to REC Schedule 1: Interpretations and Definition.

8.8 One of the main elements of the REC Change Proposal will be the creation of a new operational schedule. The new 'CCS Arrangements Schedule' will cover:

- the purpose of the CCS;
- who can access the CCS, this will include ATPs and EDPs;
- the accreditation mechanism for organisations wishing to become CCS Users, detailed further in paragraphs 8.38-8.53 below;
- the requirement to sign up to specific terms and conditions, linking to the Non-Party REC Service User Access Agreement;
- bespoke performance assurance arrangements, including monitoring and reporting requirements;
- interactions between the CCS and the associated DSAs;
- the mechanism for adding new DSAs to the CCS – detailed further in paragraphs 8.35-8.37 below;
- RECCo's role to deliver the CCS and any associated monitoring and reporting requirements; and
- the obligation on ATPs and EDPs to provide reporting information.

[11] Energy Code Reform

8.9 In line with working group feedback, the drafting will also clarify the boundary between the CCS obligations and the obligations that sit with individual EDPs, who will define the mechanism for data access associated with individual DSAs, to avoid duplication or ambiguity in compliance expectations.

8.10 In addition to the introduction of the REC Schedule, consequential changes will also be required to the following REC artefacts:

- Schedule 1, 'Interpretations and Definitions', which contains defined terms and how they should be interpretated;
- the Performance Assurance Reporting Catalogue, which defines reporting requirements to support performance assurance;
- Schedule 9, 'Qualification and Maintenance', which defines the qualification requirements associated with Non-Party REC Service Users, and specifically the provisions relating to the REC Information Security and Data Protection assessments; and
- Schedule 10, 'Charging Methodology', which defines the approach to charging for costs associated with REC Services and other REC related activities.

8.11 Process maps will be published alongside the CCS documentation, setting out the interactions between the CCS, EDPs, ATPs, and Consumers. These process diagrams will support industry assurance activities and provide a clear, end-to-end view of how consent events are captured, validated, stored, and made available to downstream systems.

8.12 The content of the CCS Arrangements Schedule and associated consequential drafting will be developed following this consultation, in discussion with the consumer consent working group, and subject to a further consultation in 2026 to provide transparency to wider stakeholders before introducing into the formal REC change process. We are therefore seeking views on the elements listed above and welcome any comments regarding the content that should be captured.

REC Service Definition

8.13 To support the retail energy market, RECCo is responsible for a number of REC Services including the Electricity and Gas Enquiry Services and the Secure Data Exchange Service. In addition, the REC governs the Central Switching Service which is delivered by the Data Communications Company (DCC) under its own Licence. With the introduction of the CCS, we are proposing to create a new REC Service, which will deliver the technical solution defined in Section 5 above.

8.14 The REC can, where appropriate, mandate the use of these REC Services by REC Parties to support operational activities delivered in line with REC obligations. In addition to this mandatory use, some REC Services are available to other organisations who wish to make use of the service on a voluntary basis. A key example of this is the Gas and Electricity Enquiry Services, where organisations wishing to access market data can qualify to become Non-Party REC Service Users. Further information on the mechanism for this qualification activity is set out in paragraphs 8.43 and 8.46.

8.15 Under the REC, the functional and non-functional components of each REC Service are documented within individual service definition documents.[12] These service definition documents do not place requirements on REC Parties or Non-Party REC Service Users themselves, but are complementary to REC Schedules which do. We are therefore proposing to introduce a new CCS Service Definition as part of the CCS code drafting. This will include:

- provision of consumer consent functionality covering the functional components defined in Section 5 above;
- details of CCS Users and associated access requirements;
- details of Non-Functional Requirements;
- service management expectations e.g., service desk service levels; and
- provision of any service monitoring tooling, to support assurance of the CCS.

8.16 The Service Definition will also clarify how the CCS interacts with the Enquiry Services for the purposes of MPxN and address matching. This may also require a change to the EES and GES Service Definitions to ensure that obligations are transparent and consistent across REC artefacts.

Technical and Data Specification

8.17 The REC baseline includes a number of defined artefacts to support Parties and Non-Party REC Service Users interactions with each other and with REC Services. This includes API Technical Specifications to enable organisations to build their internal solutions to interact with API based REC Services; Data Item and Market Message Catalogues defining the metadata for sharing information; and ad hoc documents setting out rules that organisations must comply with to facilitate interoperability e.g., Address Population Rules.

8.18 A key deliverable for the CCS will be a new CCS API Technical Specification which will form part of the REC baseline and will enable ATPs and EDPs to design, build and test their individual solutions. In addition to the physical definition of API interactions, details of the data items and messages defined within the CCS API Technical Specification will be included within the overall Energy Market Data Specification, with updates to the Data Item and Market Message Catalogues.

8.19 The CEGs described in Section 7 will be included within the formal technical specification documents to enable RECCo to monitor and manage compliance.

8.20 To address working group feedback on clarity and completeness, the Technical Specification will also:

- define the minimum data attributes required to support IDV, address matching, and consent creation;
- provide a standardised schema for recording consent type (e.g., one-off vs. enduring), expiry, revocation, and purpose;
- clarify which data items are mandatory vs. optional to support consistent implementation across all CCS Users;

[12] Service Specifications - REC Portal

- include versioning rules for API updates, ensuring a smooth transition for CCS Users when technical changes occur; and
- establish minimum performance and availability requirements for API endpoints to support a reliable consumer journey.

8.21 To support future growth, and in line with the API Technical Specification described above, the CCS technical solution will use an API-first, modular design.

Governance Framework

8.22 The remainder of this section focuses on the five core elements of the CCS governance framework as shown in the diagram below. Each of the elements has been discussed at the Implementation and Governance working group, with input reflected in the proposed approach.

8.23 We have also considered the recommendations within the working group papers provided by Ofgem and the expectation that the CCS will be designed with consumers and governance in mind i.e., that the solution should consider the consumer and consent seeker journey, and ensure sufficiently robust controls, assurance and protections are in place to ensure a safe, transparent, and trusted solution with the minimum of friction and burden.

8.24 One of the key principles across the CCS design has therefore been to leverage existing proven approaches and not 're-invent the wheel'. This applies to both the technical solution and elements of the governance design set out below. By incorporating the CCS within the REC, we have been able to build on the existing REC model, which will be enhanced to recognise the additional interactions required with the CCS and its users.

8.25 This approach supports consistency across the REC, reduces implementation complexity for industry participants, and ensures that the CCS governance model is scalable and adaptable as new services, data sets, and use cases emerge.

Figure 11: The five core elements of the CCS Governance Framework

Funding

8.26 The April 2025 Consumer Consent Decision document considered the most appropriate funding model for development of the CCS. It was confirmed that initial development of the CCS would be funded through the existing REC cost recovery model[13] and determined that it was too early to decide on the funding mechanism for enduring cost recovery.

8.27 Further discussions on the enduring cost recovery mechanism through the working groups have identified 4 potential options outlined in the figure below.

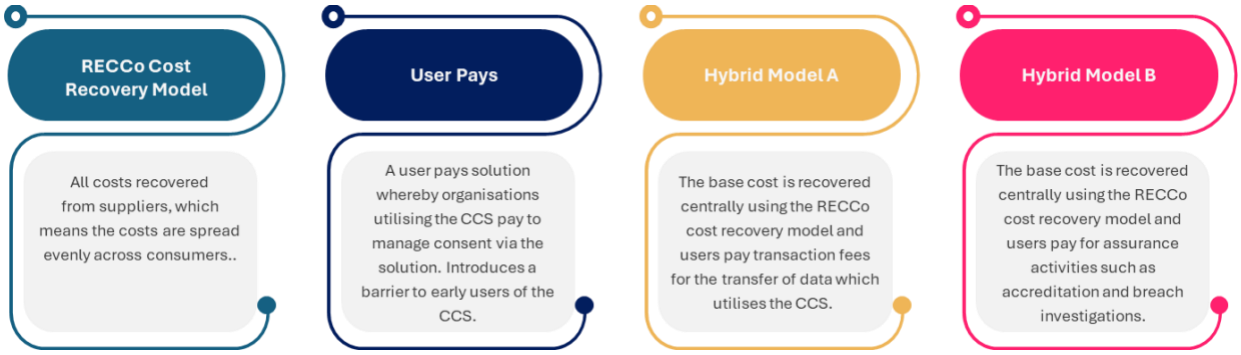


Figure 12: CCS Funding Options

8.28 In assessing the preferred approach for the CCS, we recognise ongoing discussions regarding new DSAs such as the SDR where the funding arrangements are being considered as part of BSC Modification P494[14]. We see a clear distinction between the solutions being delivered through both the new SDR arrangements and also DSI which is facilitating the sharing of data. In these cases, users are obtaining data for use in ongoing commercial and / or regulated services. Whereas the key principle underpinning the CCS is not sharing data itself; instead, it is focused on delivering a trusted consumer focused mechanism for obtaining and managing consent. We therefore believe the inclusion of a transactional cost for the CCS under Hybrid Model A would create a scenario where users may be charged multiple times for a single instance of data sharing.

8.29 However, we note feedback received through the working group discussions regarding the benefits commercial organisations will receive when utilising the CCS for consent management purposes which points towards the inclusion of an element of user pays funding. This is counter-balanced by concerns that the full cost of the CCS enduring model is not yet known and the phased implementation approach will limit the number of organisations utilising the CCS from go live which may create disproportionate costs being levied on a small number of organisations.

8.30 Therefore, we are proposing that the current approach of funding by suppliers through the RECCo cost recovery model should continue to apply for the initial time period after MMP go live. This will encourage voluntary use of the CCS and prevent disproportionate costs on early adopters. This aligns to the approach taken for UK open banking,

[13] REC Schedule 10 - Charging Methodology

[14] P494 Establishing a Smart Data Repository (SDR) - Elexon BSC

where the initial funding mechanism relied on cost recovery from banks and is now in the process of moving to a solution where all participants pay into the running of the model as participation has increased.

8.31 As part of this consultation, we are seeking views from respondents on the initial time period or other pre-conditions before this position is re-considered and whether a specific requirement to review the funding mechanism should be defined within the REC or remain flexible to enable RECCo to consider the wider evolution of the market e.g., mandating the use of the CCS across the wider market.

8.32 In reaching this conclusion, we recognise that there will be organisation specific costs incurred through the application of assurance activities e.g., qualification audits and investigations into breach. We therefore propose to adopt Hybrid Model B following the initial MMP delivery and apply the standard approach currently set out in the REC, where RECCo may recover individual costs for assurance activities. Further information on the scope of the qualification and ongoing assurance activities is included below.

Change Control

8.33 Schedule 5 of the REC defines the existing change management arrangements.[15] The fundamental principles underlying the REC change process (which are not expected to change as a result of Code Reform) are:

- Openness and transparency - any individual or organisation is able to raise a change. Clear documentation is published ensuring that impacted parties understand the rationale, impacts, and timelines for each change;
- Consumer focused – changes to the REC must better facilitate the REC objectives which includes requirement to ensure customers interests and data is protected in the operation of the REC. The ultimate test of any change is whether it improves outcomes for consumers;
- Inclusiveness and engagement – there is a high level of stakeholder engagement with regular updates provided through REC communication channels, such as weekly bulletins. Impacted parties also have the opportunity to contribute to the development of proposed changes through consultation, with stakeholder feedback actively sought and considered before decisions are made; and
- Proportionality - the level of assessment and governance applied to a change depends on its scale and impact. Minor changes may follow a streamlined process, while major changes undergo more rigorous review.

8.34 The introduction of the CCS arrangements will be delivered through a REC Change Proposal, which will be progressed in 2026. Once the new REC Schedule and associated technical documents have been introduced into the REC baseline, they will be subject to REC change control. We do not believe any changes to the existing REC change process are required with the introduction of the CCS arrangements, as there is already engagement with consumer bodies such as Citizens Advice and sufficient flexibility to manage interactions with Non-Party REC Service Users.

[15] Schedule 5 Change Management

New Data Sharing Arrangements

8.35 The CCS technical solution includes a directory which will hold details of EDPs and the DSAs that they offer. To protect the integrity and trust of the solution, it is proposed that the CCS Arrangements Schedule will define a process for approving the inclusion of new DSAs before they can be added to the CCS directory.

8.36 The following areas have been identified as key considerations to be captured within the process for assessing new DSAs:

- Legal basis – whether the EDP has the relevant legal basis for holding and / or accessing the data and sharing it with ATPs. This may include a review of the EDPs Data Protection Impact Assessment or equivalent evidence;
- Scope – whether the data being shared is appropriate for inclusion within the CCS e.g., is it consumer owned data requiring consumer consent;
- Controls – the technical and organisational controls the EDP has in place for sharing data with an ATP. This may include an assessment of security controls if these are defined bilaterally and do not utilise the standard CCS mechanism and security certificates;
- Terms – the contractual terms governing the relationship between the EDP and the ATP, including requirements on the ATPs in relation to downstream sharing of data;
- Accreditation – whether there are any additional qualification or verification steps an ATP is required to complete to obtain the new data set;
- Data retention – the arrangements in place for the retention and deletion of data once consent expires or the purpose for processing the data has been fulfilled;
- IDV – the confidence level associated with the data set in line with the GSP 45 guidelines;
- CEG impacts – whether the new DSA requires amendments to the CEGs, for example, if the new DSA expands the scope into a new type of data which may need bespoke guidance; and
- Data Source – whether a single organisation is providing a bespoke data set or multiple organisations are providing access to standardised set of data e.g., all suppliers providing access to their tariff data in a standard format.

8.37 Two distinct categories of DSA have been identified and we are seeking views on whether the proposed criteria are appropriate and any differences which should apply dependent on the type of DSA:

- Code Governed DSAs - Where DSAs are governed by an Industry Code. Examples include Elexon's SDR where the content and mechanism for sharing data will be governed under the BSC; and
- Market Governed DSAs - Where DSAs are based on commercial agreements between organisations. Examples include SEC Other Users sharing data with third party service providers.

Accreditation

8.38 Any organisation operating as either a EDP or an ATP will be required to undertake a process of accreditation. Accreditation will include verification that the onboarding organisation is who they say they are; and qualification to provide assurance that the organisation has robust systems and processes to meet its REC obligations. These checks are essential to maintaining consumer trust and ensuring that consented data is accessed and used safely, securely, and lawfully.

8.39 Where possible accreditation checks will be automated to streamline the process from a CCS User perspective, minimise the central resource requirements, ensure a consistent approach to verification, and lower the risk of error. In developing the accreditation approach, we will consider where automated checks can be used e.g., using the Companies House API to validate registration and using the Information Assurance for Small and Medium Enterprises (IASME) API to validate Cyber Essentials certification.

8.40 Consideration of the appropriate accreditation mechanism has been a key discussion point for the Implementation and Governance working group with focus on the need for a robust accreditation mechanism so that EDPs can be confident that data shared to ATPs will be managed appropriately; and also to mitigate the risk that data breaches and poor data management systems and processes will negatively impact consumer trust.

8.41 This is reflected in the diagram below which explains why it is critical that the CCS is seen as more than just a technical solution for managing consumer consent and how the technical solution is coupled with the governance framework to build a trust framework that industry participants and consumers can rely on.

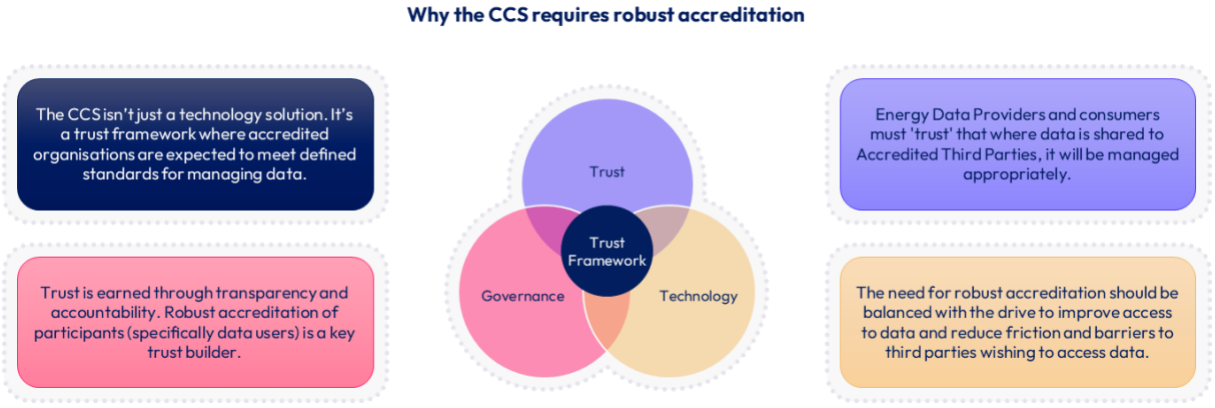


Figure 13: Why the CCS requires robust accreditation

8.42 The need for a robust accreditation mechanism is further supported by the Implementation and Governance working group paper, which recommends that a clear accreditation process is required, combining effective standards with a minimum of burden and barrier to entry. The paper also recommends that reuse of existing frameworks and technologies ought to be a key feature.

8.43 With this in mind, we are proposing to base the CCS accreditation arrangements on the existing risk-based approach used for the qualifying Non-Party REC Service Users wishing to access data via the Electricity and Gas Enquiry Services. The benefit of this approach is twofold:

- The relevant regulatory framework is already defined, well established, and understood by RECCo and industry.

- There is likely to be significant overlap between organisations wishing to become CCS Users and those that already are, or may in future, want to become Enquiry Service Users. A single accreditation / qualification process will therefore be applicable to organisations wishing to become both CCS and Enquiry Service Users.

8.44 The diagram below shows the five core components of the proposed CCS accreditation process which have been defined in more detail in the paragraphs below.

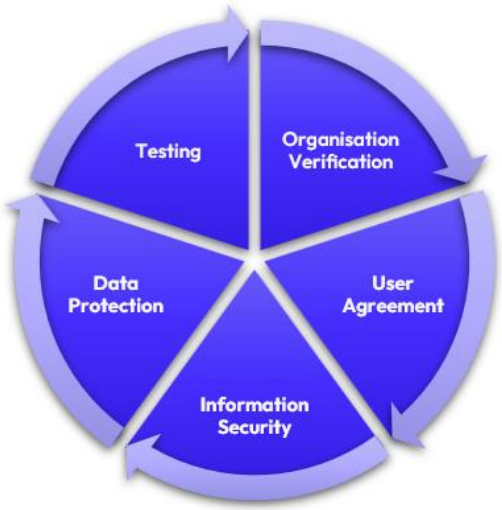


Figure 14: The 5 components of CCS accreditation

8.45 Organisation verification – to identify the organisation applying to become a CCS User. We propose using the existing checks which include the submission of an application form containing the organisation's companies house registration number. As with the current Enquiry Service Users, there is no requirement for an organisation to have a UK registered office. However, they will be required to be registered within the EEA to ensure compliance with GDPR. Where an organisation doesn't have a UK registered office, the registration number will be validated against the equivalent European company registration body. They will also need to demonstrate that they have a UK presence.

8.46 User Agreement – each CCS User will be required to sign a user agreement which will bind them to the relevant provisions within the REC. This avoids the need for organisations wishing to become CCS Users having to accede to the REC itself. We propose using the existing Non-Party REC Service User Access Agreement which is included as Appendix 1 within the Qualification and Maintenance Schedule in the REC[16]. The agreement sets out the legal requirements regarding confidentiality, data protection, and compliance, and also includes provisions enabling the agreement to be terminated where obligations are breached.

8.47 Information security – the proposed CCS solution recognises that there are a number of existing accreditations/certifications covering information security. We are therefore proposing that where possible, RECCo will place reliance on existing certifications. Based on recent advice from government regarding Cyber Essentials

[16] REC Schedule 9 Qualification and Maintenance

certification[17] we have assessed the scope of existing certifications and concluded that CCS Users should, as a minimum have Cyber Essentials Plus certification. Organisations that have ISO 27001 accreditation, but do not have Cyber Essentials Plus certification, will be deemed to have met the minimum requirement.

8.48 Data Protection – protecting consumer data is the fundamental purpose of the CCS, so it is essential that any organisation accessing data through the CCS has appropriate controls to prevent data leakage or misuse and policies and procedures that ensure compliance with data protection legislation and the REC user agreement. With this in mind, we are proposing to use the existing risk-based assessment mechanism to assess each new CCS User's data management systems and processes before they become CCS Users. This initial assessment will then inform the ongoing maintenance of qualification activities with CCS Users confirming ongoing compliance with requirements, supported by a schedule of ongoing audits, the frequency of which would be determined based on the level of risk posed by the organisation, Further information on the existing REC Information Security Data Protection Assessments can be found in the Qualification and Maintenance Schedule and associated guidance information on the REC Portal[18].

8.49 Testing – the final element of the CCS accreditation process would be testing the technical solution to demonstrate that the CCS User can integrate with the CCS, manage consumer consent token exchange, and comply with the relevant security requirements. The scope of the testing requirements will be defined post consultation, once the end-to-end technical solution is known.

8.50 In determining the appropriateness of using the existing REC qualification mechanism, we have considered wider interactions with other industry codes, in an attempt to minimise duplication and reduce the burden on organisations engaging in multiple codes. We are working with both NESO (DSI), Elexon (SDR and FMAR), and SECCo to consider how we can streamline the initial application process and whether information provided by applicants can be shared, to avoid an organisation submitting the same information multiple times.

8.51 The other area where we see current overlaps relates to the information security and data protection assessment. We are planning to minimise the level of REC information security assessment through reliance on Cyber Essentials Plus certification. However, as stated above, we believe a robust data protection assessment is a critical part of the CCS governance framework. We would therefore expect all CCS Users to undergo the REC data protection assessment, with other organisations placing reliance on this check. For example, we are continuing to discuss with Elexon whether they could rely on the CCS accreditation checks when determining whether data held within the SDR can be shared with an organisation.

8.52 Interactions with the SEC are more complicated as we are not expecting all SEC Other User data sharing activities to use the CCS from day one. We understand the SEC data privacy arrangements have a strong focus on whether the SEC Other User (and the third party they are sharing data with) has appropriate mechanisms in place for gaining consumer consent. Where a SEC Other User chooses to rely on the CCS for validating consent, we expect this to be recognised within the SEC as a valid consumer consent mechanism, removing the need for additional validation of these consents by the SEC Independent Privacy Auditor (IPA). Over time, we therefore assume the SEC privacy assessments will reduce in scope with the focus being organisations who are not utilising the CCS for all of their

[17] Ministerial letter on cyber security - GOV.UK

[18] Market Entry and Exit User Guide

consent validation. We are continuing to discuss with SECCo, how we can work together to minimise duplication for participants active within both arrangements.

8.53 Recognising the steer from Ofgem to minimise barriers to entry, we have considered whether the REC can rely on the SEC privacy assessments for SEC Other Users wishing to become CCS Users. Unfortunately, we do not believe the scope of the SEC privacy assessments would sufficiently address the risks we are seeking to mitigate through the REC e.g., the ongoing management of data beyond the point of consent capture. This is based on our understanding that SEC privacy assessments focus on the mechanism for managing consumer consent, rather than the wider controls in place to prevent data breaches. We would therefore expect all organisations wishing to become CCS Users to undergo a full REC data protection assessment, regardless of whether they have already been subject to assessment under another industry code.

Assurance

8.54 Assurance of the CCS itself and CCS Users will fall within the scope of the REC Performance Assurance Framework (PAF), overseen by the Performance Assurance Board (PAB) and defined within the REC Performance Assurance Schedule[19]. The REC PAF is underpinned by a Retail Risk Register which identifies and assesses risks that could impact the effective operation of the retail energy market, ensuring transparency, accountability, and continuous improvement.

8.55 From an enduring system delivery perspective, the existing Retail Risk Register recognises the risk associated with retail market systems not being effective or efficient. To mitigate this risk, REC Service Providers provide monthly reporting against key performance indicators which is monitored by the REC performance assurance team, with escalation to PAB if required. This monthly reporting and monitoring cycle will be expanded to include monitoring of the CCS using the metrics defined within the agreed non-functional requirements and reflected in the CCS Service Definition.

8.56 From a wider process perspective, the Retail Risk Register recognises risks relating to key retail market processes, consumer interests and data protection. These risk areas will be expanded to explicitly reflect the new CCS arrangements.

8.57 Mitigation of retail risks is delivered through a variety of performance assurance techniques, ranging from preventative techniques such as accreditation arrangements and provision of training and high quality guidance, through to escalation mechanisms for managing events of default. Further detail on the REC performance assurance techniques can be found in the Performance Assurance Methodology and Techniques document[20].

[19] REC Schedule 6 Performance Assurance

[20] Performance Assurance Methodology and Techniques

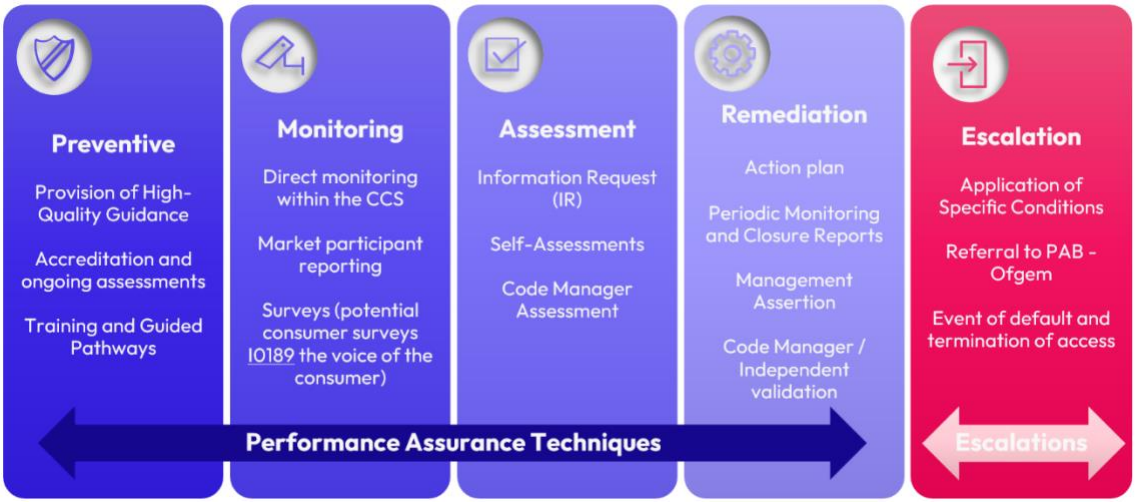


Figure 15 : REC performance assurance techniques

8.58 Initial consideration of the CCS has identified the following potential performance assurance techniques:

- Accreditation of CCS Users as set out in paragraphs 8.38-8.53 - to ensure ATP and EDPs have robust systems and processes in place to meet their obligations under the REC;
- Monitoring and reporting - where possible direct monitoring will be built into the central solution with the output provided to the performance assurance team. We expect this direct monitoring to include monitoring of CCS Users against non-functional requirements and timeliness of query resolution (see paragraphs 8.67-8.75 for further information). Where this is not possible, CCS Users will be required to provide reporting. For example, we propose to place a requirement on ATPs to run a monthly reconciliation of consents held in their own systems against consents held within the CCS, and to actively resolve discrepancies. Regular reporting into the performance assurance team on these reconciliation activities will help to identify issues with the overall consent mechanism and any issues with specific ATPs;
- Customer surveys – REC Issue I0189 'Voice of the Consumer' is currently being progressed through the REC change process. This change is seeking to expand on the current smart metering installation surveys by adding additional direct customer surveys relating to the effectiveness of the switching arrangements and prepayment arrangements. We propose to use this new mechanism to introduce a further survey to engage with consumers on their consent journeys. This will provide feedback on the CCS arrangements and will also facilitate monitoring of compliance with the CEGs;
- CEG checklist – compliance with the CEGs will be a core requirement for ATPs. We expect to develop a checklist to allow ATPs to carry out self-assessments prior to commencing operations within the CCS arrangements, with further self-assessments reported annually. We are also considering the use of independent verification of the CCS arrangements with 'mystery shoppers' engaging directly with ATPs and granting consent, to test the consumer journey. This will help to identify issues with the CCS arrangements themselves and also identify potential areas of non-compliance with the CEGs;
- Information requests and action plans – where any of the above techniques identifies potential areas of concern, the performance assurance team may issue information requests or carry out a deeper dive audit into an individual CCS User. In these instances, the organisation will be required to comply with the request and support the proposed remediation activities; and
- KPI monitoring – to ensure the CCS technical solution meets its functional and non-functional requirements, alongside REC service management activities to deal with any performance issues.

8.59 The performance assurance techniques detailed above are intended to mitigate the risk of negative consumer outcomes and to provide assurance that the CCS arrangements are operating in line with REC requirements and policy intent. These techniques will be applied proportionately, using defined monitoring, reporting, and escalation mechanisms. CCS Users will be expected to engage with RECCO's performance assurance activities in accordance with REC obligations to support effective oversight, transparency, and continuous improvement of the CCS.

8.60 However, we recognise that there will be instances where the standard performance assurance techniques will not be sufficient e.g., where individual organisations continually fail to comply with the REC obligations, despite the interventions detailed above, or where consumer data is being misused and the organisation is in breach of GDPR.

8.61 The REC PAF includes mechanisms for escalating issues to the PAB, or if appropriate, referring organisations to Ofgem. For Non-Party REC Service Users, escalation may lead to termination of the Access Agreement which will prevent access to consumer energy data governed through the CCS. Further consideration will be given to how we manage Access Agreement termination in practice, to minimise impacts on consumers utilising services provided by the non-compliant ATP.

8.62 Finally, we recognise that many of the organisations engaging with the CCS will not be regulated and therefore will sit outside Ofgem's licencing remit. As we further develop the CCS arrangements, we will engage with the ICO to understand the best route for highlighting broader GDPR compliance concerns, ensuring that risks identified through the CCS assurance activities can be escalated appropriately. We are also engaging with the Energy Ombudsmen to understand any role they may play to support the resolution of issues raised in relation to the CCS.

Issue and Dispute Resolution

8.63 The final element of governance is the mechanism for managing issues and resolving queried consents. We have split this section into two discrete areas covering issues with the technical solution which will be addressed through service monitoring and management activities, and issues with the consent itself. The latter covering consumer facing activities and mechanisms for redress.

Technical Issues

8.64 The CCS itself will incorporate internal monitoring capabilities. As set out above, this monitoring will be used to support assurance activities by assessing compliance against non-functional requirements. Internal monitoring may also identify issues requiring operational resolution and management e.g., unexpectedly high usage by an individual organisation could indicate a potential security breach.

8.65 RECCo will provide service management capability to enable issues identified through internal monitoring to be raised with the impacted CCS User(s). This service management capability will also be available for CCS Users to raise their own queries in relation to the CCS itself, ensuring a consistent and auditable route for issue handling.

8.66 As the CCS is not a fully centralised solution, with the physical sharing of data between EDPs and ATPs outside its scope, queries relating to the data itself and issues with the data sharing APIs should be managed on a bilateral basis. To support issue resolution, EDPs and ATPs will be required to provide operational contact details e.g., details of their own service desk or a key contact. Clear guidance will be provided to CCS Users to help them determine whether a query should be submitted to the CCS service desk or directed to the relevant ATP or EDP, ensuring efficient routing and reducing friction in the issue management process.

Queried Consent – where the consent record shows the consent was granted by the individual consumer

8.67 Designing a solution that builds consumer trust must have clear and transparent mechanisms for identifying and resolving queried consents. This is facilitated through the delivery of a central consumer consent portal enabling consumers to view active consents and directly revoke any consents linked to their individual account, where they do not want the relevant ATP to access their data.

8.68 For some consumers, this level of control will sufficiently address any concerns they have with access to their data. However, there may be instances where a consumer has deeper concerns regarding how access to their data was granted in the first place or where initial consent should no longer be active, for example where a consent record relates to an organisation that they do not recognise.

8.69 Whilst the CCS is a consumer facing solution enabling access to consent records, it is not intended to investigate or adjudicate individual consumer consent queries. Instead, we expect any such consumer concerns to be addressed directly with the organisation accessing the consumer's data. To facilitate this arrangement, ATPs will be required to provide and maintain operational contact details for issue resolution within the CCS directory. These details will be publicly accessible, enabling a consumer to identify and initiate contact with an organisation bilaterally. ATPs will also be required to have a formal complaints procedure for managing data issues. Whilst RECCo will not be actively involved in the resolution of these consumer complaints, we anticipate that monitoring will be included in the solution to understand how often ATP operational contact details are accessed, as a potential indicator of poor consent management procedures.

8.70 Where a consumer remains dissatisfied with the situation, they may wish to make a formal complaint about the handling of their personal data. As access to consumer data falls under GDPR, any concerns relating to potential misuse, unlawful processing or a personal data breach should be directed to the ICO, which is the UK regulator for data protection. It should be noted that the ICO expects a consumer to have exhausted any formal complaints procedures before approaching them if they remain dissatisfied or have received an unsatisfactory response or resolution. The CCS and associated guidance will provide signposting to support consumers wishing to take this route, although the CCS will not assess or determine whether a breach has occurred.

Queried Consent – where the consent record shows the consent was not granted by the individual consumer

8.71 The scenario above, where a consumer has a concern regarding a consent that the CCS has recorded against their account, should address the majority of consent related consumer issues. However, we anticipate that there may also be instances where multiple consents, granted by different individual consumers, are active against a single MPxN. This could arise for a number of reasons, including:

- consent was granted by another individual living in a multi occupancy household;
- consent was granted and the consumer moved house without the consent being revoked; or
- one of the consents held within the CCS is invalid due to issues with the IDV and matching process.

8.72 The proposed technical solution enables a consumer accessing the CCS to be able to view all consents relating to the MPxN(s) that they have been matched to i.e., where they are the Data Subject. Where a consumer identifies an unexpected consent, which was granted by another consumer (whose identity will not be visible), they will have the ability to dispute the unexpected consent. This dispute would automatically result in the consent being terminated within the CCS which would cease the provision of data, and would generate a notification to the relevant ATP for investigation.

8.73 As part of its ongoing requirements under the REC, an ATP will be required to investigate disputes and respond within the CCS within (x) working days (value to be confirmed as part of REC drafting). As part of this investigation, the ATP would:

- Initially validate that the consent record aligns to their internal systems and if not then they should formally revoke the queried consent directly through the CCS. This would cover scenarios where a consumer granted access to data at a point in time but has no enduring relationship with the ATP e.g., data provided for price comparison;
- If their internal records indicate that they have in place a valid consent, then they should contact the original consent granter to determine whether they are still an occupant at the address linked to the relevant MPxN. The ATP may request additional evidence from the consumer to confirm they are the occupier and have the appropriate rights to grant consent e.g., a copy of a recent utility bill. This would cover scenarios where the ATP is delivering an ongoing service with an agreement in place with the consumer e.g., for optimisation at the property. If the consent is no longer valid then the ATP should formally revoke the queried consent directly through the CCS to ensure there is a clear record of query closure for reporting purposes;
- If the ATP believes they still have a valid consent in place in relation to the MPxN they should respond to the original query confirming their view that consent is valid. Additional information could be provided setting out their rationale e.g., if there is a multi-occupancy household and consent was granted by a different individual. In order to re-instate access to the required data, the ATP would need to initiate the creation of a new consent record; and
- If the ATP believes there may be a wider issue with consent for a specific MPxN e.g., two unrelated consumers who have both been linked to a single MPxN, then the ATP can raise a query to the CCS service desk to enable an investigation into the IDV and matching process. We expect this action to be a backstop solution and ATPs will be encouraged to manage issues themselves and only raise service desk queries where the CCS functionality needs to be investigated.

8.74 As highlighted above, if the consumer remains dissatisfied with the outcome of the investigation, they will be able to access the ATPs contact details and raise a query directly. Where a consumer believes their personal data has been misused or unlawfully accessed, they may escalate the matter to the ICO, which regulates GDPR compliance. Further consideration is being given to the resolution paths for escalations not linked to data breach e.g., where a consumer believes they have suffered financial loss. We will be engaging with the energy ombudsman to consider whether they may facilitate resolution of disputes of this nature.

8.75 In defining the issue resolution arrangements above, we recognise concerns regarding the position that a consumer could cease access to data where consent has been granted by another individual validly linked to the MPxN. However, based on external legal advice, we concluded that it would not be appropriate for the CCS to retain an active consent record where a Data Subject under GDPR does not give consent for their data to be processed. This position has been taken in line with Article 18 (Right to restriction of processing) under UK GDPR which states that processing must be paused while validity is checked.

Link to REC Assurance

8.76 Management of disputes and potential queried consents will be a key area for performance assurance monitoring. The CCS Arrangements Schedule will include clear requirements for ATPs, with associated resolution timescales monitored within the CCS itself, enabling independent reporting to be shared with the performance assurance team.

8.77 In addition, the performance assurance team will be able to monitor the number of disputes raised against individual ATPs which may indicate weaknesses with the organisation's underlying systems and processes.

8.78 Finally, each ATP and EDP will have a REC requirement to report any ICO data breach referrals to RECCo. This will feed into any wider escalation and breach activities undertaken through the REC PAF.

9 Product Roadmap

Q31. Do you have any comments on the approach to defining the future roadmap within the consultation or the content of the draft roadmap in Annex G?

Purpose of this section

9.1 This section sets out RECCo's proposed Product Roadmap for the CCS delivery of the MMP and the enhancements that could follow. It explains how the solution is expected to evolve, how this development will be structured, and how future enhancements may be progressed. The roadmap is intentionally high-level: it communicates direction rather than delivery commitments, with detailed design and sequencing to be shaped through future engagement and governance.

Purpose of the Product Roadmap

9.2 The CCS is intended to be an enduring trust framework, capable of evolving as market needs, regulatory priorities, and data sharing opportunities develop over time. As Ofgem noted in the Consumer Consent Decision (April 2025), the CCS should provide a foundation for future expansion, new datasets, improved consumer experiences, and wider cross sector interoperability.

9.3 The Product Roadmap provides a structured way to:

- describe how the CCS capabilities may evolve over time;
- organise future enhancements within a clear and predictable model;
- support transparency for industry participants and consumers;
- guide longer term technical and governance development; and
- ensure that future expansion remains aligned to the CCS Design Principles.

9.4 The roadmap is not a project plan and does not indicate delivery dates. These continue to sit within the CCS project now and REC change processes in future.

How to Read the Roadmap and the Horizon Model (Now → Next → Later)

9.5 To support clarity, the Product Roadmap uses a simple three horizon model. This aligns with established digital product practice and mirrors the way Ofgem framed the MMP and future expansion in the Decision paper.

- **Now: MMP / REC Baseline** - Capabilities required to establish a secure, trusted, and operable CCS. These form the baseline that must be delivered ahead of go live and incorporated into the relevant REC artefacts.
- **Next: Enhancements & Adoption** - Capabilities that improve the efficiency, usability, resilience, and market adoption of the CCS once the service is live. These will be shaped through continued industry engagement, user feedback, governance insight, and the practical experience of authorised CCS Users. Some of these

enhancements may require REC Change Proposals; others may be delivered through configuration, operational improvement, or technical iteration.

- **Later: Expansion & Future Capabilities** - Capabilities that unlock broader potential for the CCS, including additional datasets, future lawful bases, new categories of participants, and cross sector interoperability with wider Smart Data initiatives. These areas will only progress where supported by Ofgem's direction, stakeholder need, and future REC governance considerations.

9.6 This horizon-based approach avoids over-specifying timing but provides industry with a clear and consistent structure for understanding how the CCS may evolve beyond MMP.

CCS Product Pillars as the Structure for Roadmap Evolution

9.7 To provide a clear and stable structure for how the CCS develops over time, RECCo will organise all future enhancements using ten CCS Product Pillars. These pillars group related functionality into meaningful deliverables and outcomes so that changes can be understood in terms of the value they create rather than low-level technical components. This approach allows stakeholders to see where developments sit, ensures consistent planning and governance, and provides a framework that can scale as the CCS expands. The CCS Product Pillars are:

- **Identity, Access & Verification** - Establishes who is interacting with the CCS and under what authenticated rights. It includes identity proofing, secure authentication and verification of a consumer's relationship to an address, asset, or data set. The focus is ensuring a trusted, secure entry point into the consent ecosystem.
- **Consent Lifecycle Management** - Defines the complete lifecycle of consent, how it is created, structured, validated, renewed, suspended, or revoked. It ensures consent remains transparent, precise, and reliable at the moment data is accessed or shared across the ecosystem.
- **Consumer Portal & Experience (incl. CEGs)** - how consumers interact with the CCS to understand, view, and manage their consents. It sets the baseline for usability, accessibility, trust, and clarity through the CEGs, ensuring a consistent consumer experience wherever consent is granted or reviewed.
- **Ecosystem & Data Access Framework** - Defines how organisations participate in the CCS. It covers the Directory and Registry, dataset registration, metadata standards, role separation, and permissions models that govern how CCS Users operate within the CCS trust framework.
- **APIs & Authorisation** - Governs the technical integration layer that enables secure, machine-readable exchanges between CCS, ATPs and EDPs. It includes API standards, token models, consent schemas, and security protocols that underpin interoperability and secure authorisation.
- **Monitoring, Audit & Assurance** - Ensures that the CCS activity is transparent, observable, and accountable. It includes event logging, behavioural analytics, performance dashboards, and the evidence base that supports ongoing assurance within the REC governance framework.
- **Platform Resilience & Operations** - Ensures the CCS is reliable, secure, and performant. It covers availability, scalability, incident management, cyber-security controls, and operational environments that support the CCS as a market-critical service.
- **Governance & Trust Framework** - Defines the rules, obligations, roles, and enforcement mechanisms that underpin the CCS as a REC Service. It covers obligations for CCS Users, accreditation rules, dataset approval processes, and compliance expectations that maintain a trusted ecosystem.

- **Communication, Transparency & Education** - Covers how information about the CCS is communicated to consumers and industry stakeholders. It includes the standards for language, transparency, and education that build trust and help consumers understand consent, data use, and their rights.

- **Cross-Sector Interoperability & Future Data Capabilities** - Sets the forward-looking direction of the CCS, including alignment with other trust frameworks, potential new datasets, future lawful bases, business permissions, and opportunities arising from Smart Data or wider cross-sector initiatives.

9.8 Using the pillars in this way provides a consistent structure. It allows industry participants to clearly identify where changes may impact them and promotes transparent expansion over time.

CCS Product Roadmap – Capability Evolution Matrix

9.9 To support transparency, RECCo has developed a capability evolution matrix that illustrates how CCS functionality may develop across the three roadmap horizons and Product Pillars. The matrix represents RECCo's current view, based on information available at this stage and the defined scope of the MMP. It is indicative only and is intended to signpost potential areas of future enhancement or expansion rather than commit to specific capabilities, sequencing, or delivery.

9.10 The full capability evolution matrix is provided in Annex G. The detailed content will continue to be refined through CCS implementation, working group engagement, and REC governance.

9.11 In summary, RECCo will extend the MMP into an enduring, market-wide smart data trust framework. Over time, the CCS will implement enhanced IDV capabilities (including federated and inclusive IDV and delegated authority models), a richer and more automated consent lifecycle (covering non-domestic use cases, delegated permissions, historic consent migration and alternative lawful bases), and an expanded consumer experience delivered through advanced accessibility, assisted journeys, and trusted third-party portals.

9.12 The roadmap also delivers broader ecosystem and data access capabilities, including new datasets (such as tariff and PSR data), participant types and cross-sector interoperability (linking to the DSI and FMAR initiatives), underpinned by mature API lifecycle management, monitoring, assurance, and resilience.

9.13 Governance, accreditation, education, and transparency will evolve in parallel to support new datasets, participants, and lawful bases, ensuring the CCS remains secure, trusted, and aligned with REC governance, while providing a clear pathway toward full smart data interoperability and "one-version-of-the-truth" consumer data control.

Dependencies, Assumptions and Caveats

9.14 The evolution of the CCS will be shaped by several factors. To support transparency, RECCo highlights the following overarching assumptions and dependencies.

- **Procurement and Technical Design** - The roadmap reflects the intended direction of the CCS but does not pre-empt detailed design or the capabilities offered by the procured technical solution. Sequencing and feasibility may evolve following service provider onboarding, MVP level prototyping, and detailed technical discovery.

- **Regulatory Direction and Ofgem Priorities** - Future development will remain aligned to Ofgem's Consumer Consent Decision and any subsequent regulatory guidance. Expansion to additional datasets, cross sector functions, or new lawful bases will only occur where supported by Ofgem's direction and appropriate within the scope of the REC.

- **REC Governance and Change Control** - Where future capabilities require changes to the REC, these will be developed through the established REC governance processes. However, not all enhancements will require formal REC modification. Some may be implemented through configuration, operational updates, or updates to non-binding artefacts such as guidance or patterns. The roadmap therefore represents direction rather than a commitment to REC change for every capability.
- **Wider Industry Dependencies** - The CCS sits within a broader system landscape, including SDR, DSI, FMAR, Tariff Interoperability, and SEC arrangements. Progress within these programmes may influence sequencing of roadmap areas or the prioritisation of future phases.

Recording Existing Consent within the CCS

9.15 Development of the CCS delivery plan highlighted issues with the inclusion of this requirement within the initial MMP delivery based on the following constraints:

- The technical solution for recording supplier consents within the CCS would require additional development work both centrally through the CCS technical solution and for energy suppliers;
- The timing of the MMP overlaps with a number of other supplier-impacting industry programmes, in particular the migration of metering points to the Market-wide Half Hourly Settlement (MHHS) arrangements and the delivery of the Tariff Interoperability arrangements;
- The CCS arrangements are based on the introduction of a minimum standard for IDV which may not align with existing practices undertaken by energy suppliers. This will need to be factored into any migration of pre-existing consents into the CCS;
- SLC47 requirements on suppliers relate to the energy customer i.e., the account holder, rather than the occupant within a specific property; and
- The scale of consent data held by suppliers would be significant which would introduce risk to the overall delivery of the CCS, where RECCo is proposing a phased implementation with a gradual ramp up in the number of consumers and consents held.

9.16 On this basis it has been agreed with Ofgem that the inclusion of existing consents will not be part of MMP. However, the expectation remains that pre-existing consents will be included within the CCS at the earliest appropriate time. Ofgem intends to engage with suppliers during 2026 to understand in more detail existing consent arrangements. In addition, there is an expectation that Ofgem will progress a change to the Supply Licence to capture any specific obligations on suppliers regarding the use of the CCS. In parallel, RECCo will ensure that the CCS is developed with sufficient flexibility to incorporate records for consent that was not granted via the CCS at a future date.

Maintaining and Updating the Roadmap

9.17 The Product Roadmap will be maintained as an enduring CCS artefact. RECCo expects to update it periodically to reflect:

- regulatory guidance and prioritisation;
- industry recommendations;
- CCS User feedback and consumer insight;

- monitoring data and assurance findings; and
- opportunities arising from new datasets or Smart Data initiatives

9.18 Any significant or material roadmap change that requires amendment to REC artefacts will be progressed through the REC Change management process, with appropriate consultation. Other changes may be incorporated through operational updates, technical configuration, or updates to supporting documentation such as CEGs and technical specifications.

9.19 The roadmap will be republished following material updates to ensure stakeholders always have a clear and current view of the CCS evolution.

Summary

9.20 The CCS Product Roadmap provides a clear and structured view of how the service will evolve beyond the MMP. By organising future capabilities into ten established product pillars and using a simple three horizon model, the roadmap supports transparency, stability, and long term planning across the market. It enables stakeholders to understand future direction without pre-empting detailed design decisions or committing to specific timelines, while ensuring alignment with Ofgem's expectations and REC governance.

10 Conclusion and Next Steps

10.1 We welcome the views of interested parties on the specific questions asked within this consultation, and general thoughts on our proposals. These views will inform the ongoing development of the CCS and associated changes to the REC.

10.2 We have selected a six week period for responses to this consultation, due to the complexity and involved nature of what we are consulting on. While the consultation is open, we will continue to engage with interested parties through working group discussions and bilateral meetings, whilst we will also host a CCS Engagement Day to review the proposals set out within the consultation. Planned engagement sessions include:

- CCS Solution Group: Consultation – Spotlight on Policy Positions and Governance Design (12 February 2026);
- CCS Solution Group: Consultation – Spotlight on Technical Design (26 February 2026);
- CCS Solution Group: Consultation – Spotlight on User Experience Design (12 March 2026);
- CCS Webinar: Consultation headline outcomes and REC Change next steps (16 April 2026); and
- CCS Engagement Day (4 March 2026)

10.3 We aim to further consult on the detailed technical specification and code drafting during summer 2026.

11 Annexes

11.1 Annex A – Consultation Response Form

11.2 Annex B – Glossary

11.3 Annex C – Design Principles

11.4 Annex D – Technical Design

11.5 Annex E – Technical Diagrams and Business Process Diagrams

11.6 Annex F – User Experience (UX) Design

11.7 Annex G – Product Roadmap