

REC Drafting Consultation

Consumer Consent Service

Published 07 September 2026



Contents

1	Executive summary	5
1.1	A phased route to the full consumer vision	5
1.2	Design conclusions	6
1.3	Value for money and policy alignment	6
1.4	What we are consulting on	7
2	Introduction.....	8
2.1	Background	8
2.2	What is the long-term vision for CCS?.....	8
2.3	Alignment with Energy Digitalisation Framework	8
2.4	Interaction with Smart Secure Electricity Systems (SSES) Tariff Interoperability	9
2.5	Interaction with DESNZ Energy Smart Data Framework consultation.....	10
2.6	What is in scope for CCS MMP?	10
2.7	What has changed since the February 2026 Design consultation?	11
2.8	What are we consulting on?	11
2.9	How have we developed the proposed approach?	12
2.10	Consultation stages.....	12
2.11	How to respond.....	12
2.12	Your response, data, and confidentiality	13
	PART A - Outcomes from Design Consultation.....	14
3	CCS design conclusions	14
3.1	Engagement since the February 2026 Design consultation	14
3.2	CCS scope evolution and Minimum Marketable Product (MMP)	15
3.2.1	Why is RECCo adopting a phased approach?	15
3.2.2	What is the MMP scope?.....	16
3.2.2.1	Initial EDHs.....	16
3.2.2.2	Gas scope.....	16
3.2.3	Future evolution of SEC and DCC arrangements	17
3.2.4	Tariff Interoperability.....	18
3.2.5	Long-term roadmap.....	18
3.3	Key CCS design decisions.....	19
3.3.1	Permission to access domestic half-hourly (HH) metered data.....	20
3.3.2	Treatment of domestic HH metered data within the CCS permission model.....	21

3.3.3	Who may grant permission for domestic HH metered data (occupier vs bill payer)	22
3.3.4	Multi-occupancy properties: lead occupier model	23
3.3.5	Consumer complaints, permission revocation, and query resolution	24
3.3.5.1	Complaints	25
3.3.5.2	Permission revocation and queries through the CCS	25
3.3.5.3	Complaint escalation and redress	26
3.3.6	Identity and occupancy verification	27
3.3.6.1	Assurance standard	29
3.3.6.2	Address and meter-point matching	29
3.3.6.3	Where sufficient evidence cannot be established	29
3.3.6.4	What will be finalised before implementation	30
3.3.7	Consumer interaction with the CCS	30
4	Revised technical design	31
4.1	Development of the technical design since the February 2026 consultation	31
4.2	Supporting technical information available with this consultation	34
4.3	Overview of target architecture	35
4.4	Applying the CCS design principles	36
4.5	Allocation of central and decentralised responsibilities	38
4.6	Security and interoperability framework - FAPI 2.0 and mTLS	38
4.7	CCS Directory and trust enablement	40
4.8	Permission initiation and authorisation flow	42
4.9	Identity, occupancy verification and property-to-meter-point matching	45
4.10	Permission and authorisation model	46
4.10.1	Services involving more than one EDH	47
4.11	How EDHs validate permission	47
4.11.1	Local validation instead of mandatory introspection	47
4.12	Access-token lifecycle, revocation, and CCS availability	48
4.12.1	Access-token lifetime and refresh	48
4.12.2	Revocation and lifecycle notifications	49
4.12.2.1	Use of Shared Signals Framework (SSF) for grant status updates	49
4.12.3	CCS availability and data sharing during an outage	50
4.13	Permission visibility and interaction with ATP interfaces	51
4.14	Operational assurance, testing, and support	51
5	User Experience (UX) Design	52

6	Governance Design	54
6.1	Funding.....	54
6.2	Change management.....	55
6.3	Assurance	56
6.4	Accreditation.....	57
PART B - REC Drafting Proposals.....		61
7	Summary of REC Drafting.....	61
7.1	Supporting Category 3 documents.....	62
7.2	Interactions with Tariff Interoperability	63
8	REC drafting	64
8.1	Main Body and Operational Schedules.....	64
8.2	Main Body	65
8.3	CCS Arrangements Schedule	65
8.4	Schedule 10 Charging Methodology	69
8.5	Schedule 9 Qualification and Maintenance	70
8.6	Information Security and Data Protection (ISDP) Assessment.....	70
8.7	External CCS testing	71
8.8	Performance assurance reporting and monitoring	72
8.9	Enquiry Service Definitions.....	73
8.10	Consumer Experience Guidelines	74
8.11	Technical and Data Specifications	75
	8.11.1 CCS API Technical Specification.....	75
	8.11.2 Energy Market Data Specification.....	76
	8.11.3 Standards Definition Document.....	77
	8.11.4 Summary.....	77
8.12	CCS Service Definition.....	77
9	Conclusion and next steps.....	79
10	Annexes.....	81

1 Executive summary

The Retail Energy Code Company (RECCo) is developing the Consumer Consent Service (CCS) following Ofgem's decision¹ to establish a common, trusted mechanism through which consumers can control access to their energy data. The CCS will provide a standardised permission, trust, and authorisation framework, establishing a trust framework for energy data. The CCS Minimum Marketable Product (MMP) will be introduced as a REC Service and will therefore be governed through the REC, including the applicable change, qualification, assurance, and performance arrangements. As the service evolves after the MMP release, additional data sources will be added, including: asset information, asset control, Data Communications Company (DCC) flows and existing consents. In each case these will be subject to confirming value for money, industry consultation, and validation through the REC Change Process. Energy data movement will remain outside the CCS, flowing directly between Energy Data Holders (EDHs) and Authorised Third Parties (ATPs) under the hybrid architecture confirmed through consultation.

The proposals in this consultation form part of the wider implementation of the energy smart data scheme enabled by the Data (Use and Access) Act (DUAA). In particular, the CCS is being developed as a common capability to enable consumers to authorise, manage and withdraw access to their energy data in a secure and consistent way. The wider Energy Smart Data Framework consultation and subsequent secondary legislation will establish the broader governance, regulatory and interoperability arrangements required for the scheme to operate as well as mandating the sharing of data by EDHs. These activities are intended to work together as part of a single approach to delivering smart data in the energy sector and should not be viewed as separate or overlapping solutions.

1.1 A phased route to the full consumer vision

The long-term vision, aligned with Ofgem policy, is a single place through which consumers can understand and manage access to their energy data, replacing today's fragmented permission arrangements. RECCo's consumer research has consistently identified trust, transparency, and control as the key consumer considerations for such a framework. The MMP, expected to go live in March 2027, is the first implementation of that vision, not the end state: its capabilities will be reused across later phases, and the service is designed to support new entrants and new consumer services. Value for money and consumer benefit will be paramount throughout.

The MMP will not, at launch, deliver the full consumer proposition envisaged in Ofgem's earlier Consumer Consent work, which included a more complete view of existing permissions, including those granted before the CCS was implemented. The design, developed through Ofgem's decision-making process; RECCo's February 2026 Design consultation; industry working groups; consumer research and detailed technical and regulatory assessment; has instead led to a phased implementation. The common permission, trust and authorisation capabilities are established first, with additional data sources and existing permission arrangements incorporated as the regulatory, technical and delivery dependencies are addressed. The long-term objective is unchanged.

Initially the MMP will support permissions for domestic electricity consumption data through a digital consumer journey, with Elexon's Smart Data Repository (SDR) anticipated as the first EDH and metering-point matching via the Electricity Enquiry Service (EES). We expect gas data to become available through CCS at a future date due to the unavailability at MMP of an EDH who holds gas data. This is a sequencing matter.

The first material enhancement to the MMP is expected in Q4 2027 when account-specific tariff data will follow through Tariff Interoperability Phase 1b, with premises asset information and control thereafter. The capabilities being built are

¹ [Consumer Consent decision | Ofgem](#)

intended in the future to extend to DCC data flows and permissions granted before CCS launch. RECCo and Smart Energy Code Company (SECCo) are working on recognition of the CCS as an approved permission mechanism under the Smart Energy Code (SEC) arrangements. The inclusion of non-domestic use cases, direct DCC integration and assisted journeys are sequencing decisions, not exclusions. These developments will be progressed through the applicable REC Change arrangements, with timing dependent on the readiness of both the CCS and the relevant data holders, services, and regulatory arrangements.

1.2 Design conclusions

Part A sets out RECCo's conclusions on the principal design matters raised through the February 2026 Design consultation, including where the approach has changed or developed:

- The CCS will manage regulatory permission and provide auditable evidence of it, helping organisations meet their UK General Data Protection Regulation (UK GDPR) obligations; lawful basis and wider data protection responsibilities remain with each organisation.
- Permission for domestic half-hourly data will be occupier-led (account holder or bill payer status alone will not suffice) and granted through a verified CCS account. Any verified adult occupier may grant permission in their own capacity; none may do so on behalf of another.
- MMP will not include a 'guest journey' capability because it would remove account creation but not the required identity and occupancy checks. A verified CCS account gives consumers a single, secure route to view, manage and revoke permissions throughout their lifecycle.
- Identity and current occupancy will be verified separately, benchmarked to Government Digital Service Good Practice Guide 45 (GPG45) Medium for identity, with multiple routes and photographic identification optional.
- EDHs will validate short-lived, signed access tokens locally (maximum 30-minute lifetime); energy data may be disclosed only while a valid token exists. Financial-grade API (FAPI) 2.0 and mutual Transport Layer Security (mTLS) form the security baseline. As a REC Service, the CCS will operate within the existing REC governance framework. Existing REC qualification, assurance, and performance arrangements will be extended to the CCS where appropriate, not replicated in a separate regime. Cyber Essentials Plus (CE+) will form the minimum cyber-security baseline, supplemented by risk-based Information Security and Data Protection (ISDP) assessment arrangements.

The technical design comprises the core components needed to operate a permission service: permission management; consumer, CCS User, and administrator portals; the Directory; identity and occupancy verification; enquiry-service integration for metering-point matching; and testing, monitoring, and service support. Ofgem's decision requires a service through which consumers control permissions granted to allow access to their data, not one that only reports it: each component is needed for permission to be granted by the right person, bound to accredited parties, and enforced at the point of data access. These capabilities will serve each further permission-based dataset without redesign; this design is not a point solution for one dataset.

1.3 Value for money and policy alignment

RECCo has tested CCS costs against Open Banking, the closest comparator, whose initial implementation was not expected to exceed £20m at 2016 prices; the current published RECCo budget for implementation of CCS to MMP status is £6.2m. Consultation feedback has already reduced cost and central dependency, for example, replacing mandatory online introspection with local token validation. Cost transparency will continue through delivery and enduring operation.

All future developments will be assessed to determine if they deliver value for money and demonstrate consumer benefit. Business cases will continue to be published and the RECCo budget will be consulted on in February each year. Any changes to the scope or governed arrangements of the CCS will be progressed through the REC Change process and associated governance, providing transparency and scrutiny before implementation.

The CCS supports the Department for Energy Security and Net Zero (DESNZ) and Ofgem Energy Digitalisation Framework and forms a key component of the implementation of the Energy Smart Data Scheme Legislation Framework enabled by the DUAA.

1.4 What we are consulting on

Part B sets out the proposed REC drafting: a new CCS Arrangements Schedule, amendments to existing REC products, and supporting service, technical, data, and consumer documentation. It primarily seeks views on whether Part B translates the Part A design into clear, complete, and workable REC arrangements, with appropriate responsibilities and no unnecessary duplication or prescription. Respondents may also raise new evidence, or a material issue not previously considered, that affects a Part A conclusion. Where possible, please provide supporting evidence and identify the artefact or clause to which comments relate and propose alternative drafting.

The consultation closes on **19 October 2026**. Responses will inform the final drafting, which will progress through the REC change process (continuing REC Issue I0318), with implementation expected in March 2027, subject to that process and Ofgem's decision.

2 Introduction

2.1 Background

In its August 2024 CCS Consultation, Ofgem explained that energy-sector approaches to retrieving and providing consent are inconsistent, causing barriers for new market entrants. Ofgem proposed that a new consent solution should be developed to provide a standardised and system-wide consent process. In its April 2025 Consumer Consent Decision, Ofgem confirmed it would progress the development of a CCS, with RECCo selected as the delivery body.

During 2025, RECCo worked with Ofgem, Consumer Bodies and industry, through the Consumer Consent Working Groups, to design the technical and governance solution, including user experience elements. In February 2026 we consulted on the initial design ([February 2026 Design consultation](#)), with a [CCS Design Consultation Webinar](#) held on 28 May 2026 to share an initial summary of consultation responses, focusing on key themes and next steps for design.

2.2 What is the long-term vision for CCS?

The long-term vision for the CCS is a single, trusted place where consumers can understand which organisations are accessing their energy data and on what basis. This includes access that the consumer has explicitly permitted, as well as access undertaken through regulated energy-market arrangements connected with the supply of energy to, or operation of, their premises. Where access requires a consumer permission, the CCS will also enable the consumer to grant, review, and manage that permission. Information about energy-data access is currently fragmented across separate arrangements, so no consumer has a complete view. The CCS is designed to provide a more consistent and transparent framework through which those different forms of access can be understood and, where permission applies, controlled by the consumer.

The core capabilities around a verified consumer, permission management, identity and occupancy verification, participant trust and directory, authorisation and token issuance, governance and assurance will be delivered in MMP. Over time it is intended to reach beyond electricity consumption data to gas, tariff information, DCC data flows, pre-existing consents, Priority Services Register data and, as the service matures, premises asset information and control. It should also support more participants and more inclusive routes, including for consumers who cannot complete a digital journey. The permission, trust, verification, and authorisation capabilities being built now are designed to be reused and adapted for each of these rather than rebuilt.

These remain directions of travel rather than commitments: realising them depends on each data-sharing arrangement adopting the CCS through the relevant policy, regulatory and governance processes. The timing will also depend on the readiness of the relevant EDHs and other services to integrate with and make use of the CCS. The reusable CCS capabilities are intended to allow additional EDHs, data products and use cases to be introduced as those external dependencies are met, without requiring the core service to be redesigned.

2.3 Alignment with Energy Digitalisation Framework²

The CCS forms a key component of the wider energy digitalisation landscape. DESNZ and Ofgem described that landscape in the Energy Digitalisation Framework: A Vision for a Coordinated and Connected Energy System. The Framework identifies the need to move from a collection of individual digitalisation initiatives towards a more coordinated and

² [Energy Digitalisation Framework: A vision for a coordinated and connected energy system](#)

interoperable ecosystem, built on common governance, standards, and trust arrangements. It emphasises the importance of secure and informed data sharing, enabling consumers to participate confidently in a digitalised energy system while supporting innovation, flexibility, and market competition

The Framework recognises consumer data as a distinct data domain requiring clear governance, trusted access arrangements, and consistent approaches to consumer control. The CCS directly supports these objectives by providing a standardised mechanism through which consumers can grant, review and revoke permissions for access to their energy data.

The Framework also identifies interoperability as a core design principle, alongside common approaches to trust, accreditation, technical standards, and governance. RECCo has therefore designed the CCS to operate within a wider ecosystem of digital energy services rather than as a standalone solution. It aligns with initiatives such as the Data Sharing Infrastructure (DSI), Smart Data Repository (SDR), Flexibility Market Asset Registration (FMAR), and Tariff Interoperability.

The CCS uses a central trust framework, consistent participant onboarding, and assurance arrangements, and recognised open standards such as FAPI 2.0. This supports interoperability between initiatives and minimises duplication of participant onboarding, accreditation, and technical integration activities. It provides a practical foundation for the longer-term CCS vision, while keeping immediate delivery focused on a use case that can provide consumer and market benefit.

In line with this framework and the original Ofgem decision, the CCS is being built to provide the trust, permission and authorisation capabilities required to support data sharing where access is subject to a person's or business's permission. The initial MMP will apply these capabilities to one dataset: domestic half-hourly electricity metered data made available through the SDR.

2.4 Interaction with Smart Secure Electricity Systems (SSES) Tariff Interoperability

Tariff Interoperability and the CCS are complementary initiatives within the wider energy digitalisation and smart data landscape. The CCS is a cross-sector permission management service and associated trust framework designed to support consumer-controlled access to energy data. Tariff Interoperability is focused on standardising tariff data for the purposes of wider sharing. Together, the two initiatives will enable consumers to share their tariff data, via permission, with other organisations so they can receive better products and services. Tariff data will follow on from the MMP phase of CCS, adding the second data source. This was confirmed in DESNZ response to the November 2025 Tariff Interoperability consultation³.

Although Tariff Interoperability Phase 1b is not part of the CCS MMP, the proposals in this consultation are directly relevant to energy suppliers that will be Tariff Interoperability Energy Suppliers. Under the proposed arrangements, those suppliers will be required to become CCS Users and will have a specific role within the CCS verification journey for account-specific tariff information. This includes providing account-holder verification as part of the CCS identity verification process and performing the associated account and metering-point matching. Suppliers will also need to support the relevant CCS technical interactions required to perform these functions.

Tariff Interoperability Energy Suppliers should therefore review the CCS Arrangements Schedule and the relevant CCS technical and data specifications included with this consultation, to understand and provide feedback on the CCS requirements that will apply to them. The Tariff Interoperability Phase 1b consultation is currently expected to be published in October 2026 and will set out the complementary Tariff Interoperability requirements. Suppliers should also review that

³ [Tariff-Interoperability-MVP-Consultation-Government-Response.pdf](#)

consultation when it is published, as the requirements relevant to Tariff Interoperability implementation are split across the two consultations.

Section 7.2 explains how the associated code drafting has been divided between the CCS and Tariff Interoperability projects.

2.5 **Interaction with DESNZ Energy Smart Data Framework consultation**

The CCS forms a key component of the implementation of the energy smart data scheme enabled by the DUAA. In particular, CCS is being developed to provide the common mechanism through which consumers can authorise, manage and withdraw permissions for the sharing of their energy data with authorised third parties, as well as the trust framework, supporting the operation of a trusted, secure and scalable smart data ecosystem. The broader Energy Smart Data Legislative Framework consultation and the subsequent secondary legislation under the DUAA will establish the statutory roles, governance arrangements, participation and data sharing requirements, interoperability expectations and associated obligations necessary for the operation of the scheme. The CCS should therefore be viewed as an integral component of the forthcoming DUAA implementation programme. Together these initiatives form part of a single approach to delivering smart data in the energy sector and are not intended to create separate or overlapping solutions.

2.6 **What is in scope for CCS MMP?**

The table below provides a high-level summary of the CCS MMP scope. Further information, including the rationale for any changes made since the February 2026 Design consultation, is included in section 3.2.

Area	MMP position in this draft
Core capability	Central permission management, consumer account, identity and occupancy verification, participant trust, and token issuance, with energy data exchanged directly between Authorised Third Parties (ATPs) and Energy Data Holders (EDHs)
Initial metered data scope	Domestic half-hourly electricity metered data. “Domestic” follows the applicable supply licence classification and Ofgem guidance.
Initial participants	The early EDH categories described in section 3.2.2.1, including the Smart Data Repository (SDR) and participating SEC Other Users where the relevant arrangements can be supported
Not in scope for MMP (included in future roadmap)	Gas consumption-data provision and the associated MPRN-matching journey, direct DCC integration, integration with a DCC Smart Meter Data Repository (SMEDR) as an EDH if progressed, non-domestic metered - data use cases, assisted/ non-digital consumer journeys, and Tariff Interoperability Phase 1b.

Table 1

This scope statement describes the first implementation of the CCS, not the boundary of the enduring service. Where a section refers to an approach applying 'for the MMP', this means it is the approach proposed for the initial implementation. The common CCS capabilities are designed to be reused as further datasets, participants and consumer journeys are introduced, although the permission rules and verification requirements may be adapted to the characteristics and regulatory arrangements of each future use case.

2.7 What has changed since the February 2026 Design consultation?

- CCS MMP will initially support domestic electricity consumption data.
- Rather than relying on a single high-confidence photographic-ID route, the CCS will use a centrally governed, outcome-based, and risk-based approach to identity and occupancy verification.
- EDHs will validate signed access tokens locally, rather than checking with the CCS for every data request. Tokens will have a maximum 30-minute lifetime (see section 4.12.1).
- Terminology has been updated to align to the wider smart data arrangements and to address legal review comments. Changes include:
 - the term “consent” has been replaced with “permission” to access data, to better reflect the wider regulatory framework and avoid confusion with specific GDPR consent requirements. Consumer-facing language is considered separately through the Consumer Experience Guidelines (CEGs), so it can reflect what is clearest and most understandable for consumers;
 - Energy Data Providers are now referred to as Energy Data Holders (EDHs);
 - the term energy data subject has been introduced as a generic term that captures either the occupier at a property or the energy supply account holder.

2.8 What are we consulting on?

This RECCo-led consultation document has two purposes:

- **Part A** explains the conclusions reached following the feedback received through the February 2026 consultation.
- **Part B** explains how the technical and governance design has been translated into the formal REC baseline. Part B seeks views on the proposed REC code drafting approach and supporting REC products required to implement the CCS.

Respondents are welcome to identify any new evidence or material issue not previously considered that they believe could affect the conclusions set out in Part A. However, the primary focus of this consultation is the proposed REC drafting in Part B. Part B includes sections on each core part of the proposed solution, with associated consultation questions:

- **REC Schedules:** a new ‘CCS Arrangements Schedule’ setting out obligations on ATPs and EDHs and requirements applicable to Tariff Interoperability Energy Suppliers, including CCS Account Holder Verification, and the operational arrangements in place to facilitate permission management and use of the CCS. This REC Schedule sits alongside the proposed redlined changes to existing REC Schedules required by the introduction of CCS.
- **Technical and Data Specifications:** CCS API Technical Specification which will enable ATPs and EDHs and relevant Tariff Interoperability Energy Suppliers to design, build and test their individual solutions. The data items and messages defined within the CCS API Technical Specification are also set out through proposed updates to the Data Item and Market Message Catalogues that form the Energy Market Data Specification (EMDS).
- **Service Specification:** the CCS is being introduced into the REC as a new REC Service. The proposed CCS Service Definition sets out the service provided, including externally facing functional and non-functional requirements.

- **Consumer Experience Guidelines (CEGs):** a new REC product providing guidance for ATPs developing their consumer-facing interfaces. This includes details of the key steps within permission journeys.

We are seeking views from industry and other interested parties on each of these products, to enable us to finalise the drafting. Following consideration of consultation responses, RECCo will baseline the resulting REC drafting and finalise the associated CCS design and technical implementation material before submitting the changes for progression through the applicable REC change governance process.

At the time of publication, the CCS project is continuing to plan against the current REC change arrangements. Under these arrangements, the changes would progress from REC Issue I0318 into Change Proposal R0318, which RECCo currently anticipates formally raising later in 2026.

The CCS changes will in all cases need to progress through the REC Change process. However, Ofgem's Energy Code Reform⁴ is introducing changes to REC change governance and the change process during this period. RECCo is managing the CCS change activity with this transition in mind so that the drafting and supporting work developed through the CCS project and I0318 can be carried forward into the relevant change process without unnecessary duplication or disruption.

2.9 How have we developed the proposed approach?

The conclusions in this document have been informed by a range of evidence and engagement, rather than by any single forum. RECCo has considered consultation responses, topic-specific industry working groups, consumer research, external legal advice, engagement with the Information Commissioner's Office (ICO), and discussions with Ofgem and DESNZ. RECCo has also participated in the Digitalisation Delivery Group (DDG), which helps coordinate relevant smart-data and energy-digitalisation activity across programmes. The DDG has informed the development of the proposals but has not acted as the decision-making forum for the CCS. Where a particular source of evidence has played an important part in shaping a conclusion, this is highlighted in Part A.

2.10 Consultation stages

This consultation will be open to responses for six weeks, closing on 19 October 2026. After the consultation period ends, all responses will be considered and weighted appropriately, with each response evaluated on its own merits.

All non-confidential responses will be published. An update will be presented at a CCS working group following this publication. If you require your response to be treated as Confidential, either in whole or in part, it must be identified as such.

Consultation responses will be considered by RECCo, in discussion with Ofgem and DESNZ, with updates to drafting made where appropriate. Finalised REC drafting will then be progressed through the standard REC change process, resulting in the Change Proposal being issued to the Authority for final decision.

2.11 How to respond

We welcome responses to this consultation from anyone interested in the CCS. Please complete the response form (Annex A) and send your response to consumerconsent@retailenergycode.co.uk before the consultation closing date.

⁴ [Energy code reform | Ofgem](#)

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.

To aid the reader, 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.

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

2.12 Your response, data, and confidentiality

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;
- **Confidential** - responses will only be shared with RECCo and its CCS project team, and the Authority / DESNZ (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).

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.

If you wish to respond confidentially, we'll keep your response itself confidential, 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.

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

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.

PART A - Outcomes from Design Consultation

3 CCS design conclusions

In our February 2026 Design consultation, we set out high level design positions in the following areas:

- The future roadmap, explaining how the CCS MMP is the first stage in the CCS rollout with expansions to include additional datasets and other lawful bases for accessing consumer data.
- responsibilities for granting permission and approach to identity verification (IDV);
- the architectural model including mandatory introspection and use of specific security standards;
- User Experience (UX) design, including the approach to engaging with consumers and the development of CEGs; and
- governance design including the change management, funding, assurance, and issue / dispute resolution approach.

This section provides a summary of the consultation responses received, activities which have taken place since then and how these have informed the resulting CCS design and the REC drafting discussed in Part B. The full suite of responses is available on the REC Portal⁵.

Key supporting design information, including the business process diagrams and selected machine-readable technical definitions available through the CCS section of the RECCo Developer Portal, is being provided to support respondents' understanding of the design.

3.1 Engagement since the February 2026 Design consultation

Stakeholder engagement has continued throughout the development of the CCS following the February 2026 Design consultation. The **31** consultation responses and **645** individual comments provided an important starting point for this next phase of design development, identifying areas requiring further clarification, testing, or refinement.

Since the consultation closed, RECCo has tested and developed the proposed approach through a combination of CCS working groups and topic-specific sessions, bilateral stakeholder engagement, consumer research, regulatory and policy engagement, and specialist technical and legal input. This has included continued engagement with Ofgem and DESNZ, the Information Commissioner's Office (ICO), relevant industry bodies and organisations involved in related energy-data and smart-data initiatives.

⁵ [Your Responses To: Consumer Consent Solution Design Consultation - The Retail Energy Code Company](#)

A CCS Design Consultation Webinar⁶ was held in May 2026 to share the headline themes emerging from the consultation and explain the areas requiring further development. Subsequent engagement has focused increasingly on detailed implementation, including identity and occupancy verification, consumer journeys, technical architecture and security, governance and assurance, and alignment with related initiatives such as the Smart Data Repository and Tariff Interoperability.

This engagement has helped RECCo to test the feasibility and practical implications of the February proposals and, where appropriate, refine the design before translating it into the REC drafting presented in Part B. The sections that follow explain the resulting conclusions and highlight where stakeholder feedback and subsequent engagement have led to material changes in the proposed approach.



Figure 1

3.2 CCS scope evolution and Minimum Marketable Product (MMP)

This section explains how the MMP delivers the first implementation of the wider CCS vision. It distinguishes the enduring capabilities being established now from the initial domestic electricity use case, explains the rationale for the proposed MMP scope and its principal dependencies, and sets out how the same framework may be extended over time. For the purposes of the CCS MMP, "domestic" refers to premises classified as Domestic Premises under the applicable gas or electricity supply licence, taking account of Ofgem's published guidance on the classification of premises. Premises classified as non-domestic under the applicable licence conditions and guidance remain outside the scope of the MMP.

3.2.1 Why is RECCo adopting a phased approach?

Some respondents to the February 2026 Design consultation supported the phased implementation model, recognising that establishing a focused MMP would reduce delivery complexity and implementation risk whilst enabling consumer benefits to be realised sooner. However, respondents, questioned whether the proposed MMP would provide sufficient consumer value if it only reflected a limited number of energy data sharing arrangements. Respondents also expressed concern that consumers may incorrectly assume the CCS provides visibility of all organisations accessing their energy data, when in practice the initial scope would only represent a subset of regulated energy data sharing arrangements.

⁶ [Round-Up: CCS Design Consultation Webinar - 28 May - The Retail Energy Code Company](#)

Respondents therefore encouraged RECCo to provide greater clarity regarding the long-term direction of the CCS and how additional capabilities would be introduced over time.

RECCo has carefully considered this feedback. Whilst a broader initial scope could increase transparency from the outset, RECCo considers that attempting to accommodate all anticipated future use cases within the MMP would significantly increase delivery complexity, introduce additional implementation risk and materially increase time to market, delaying consumer and market benefits realised through the initial service.

This matters most when considering permissions that already exist. Relevant permissions, and the data they cover, may already sit within industry systems, but that alone does not determine whether they should be brought into the CCS. Adding a dataset also requires RECCo to consider how the information can be presented to consumers meaningfully and understandably, the policy and regulatory framework governing access to and use of it, and how the resulting transparency and control functions would work.

Some consumer bodies have been clear about the risk: if consumers cannot see who is accessing their data in plain language and then act on it, trust in the service will erode. Focusing on existing permissions would also do nothing to help new entrants bring new services to market.

RECCo conclusion: a phased implementation remains the most appropriate approach. The MMP will establish the enduring capabilities the CCS requires: permission management, the consumer account, trust and directory services, identity and occupancy verification, tokenised authorisation, and the supporting operational, governance and assurance arrangements. It will apply those reusable capabilities first to domestic half-hourly electricity metered data, prioritising direct consumer control from the outset so that consumers gain access to new and better services sooner. Existing permissions and further datasets will follow in later phases, where there are clear consumer and market benefit and the relevant policy, regulatory, design and implementation dependencies have been addressed. The MMP should therefore be regarded as the first implementation of the CCS, rather than its intended end state.

3.2.2 What is the MMP scope?

The scope of the CCS MMP is summarised in the MMP scope table in section 2.6. In summary, the MMP is focused on domestic half-hourly electricity metered data and the core capabilities required to support permission-based data sharing, with additional data sources to come in later phases. A number of potential future capabilities and use cases, including gas consumption data, are not proposed for the MMP.

The sections below explain the key considerations underpinning the initial EDH and electricity-first scope.

3.2.2.1 Initial EDHs

Elxon's SDR is the anticipated first EDH for MMP. RECCo and SECCo are continuing work to enable CCS to be recognised as an approved mechanism for obtaining permission under the SEC arrangements. Participation by SEC Other Users can be considered once those arrangements enable them to use CCS for the relevant data-sharing activities.

3.2.2.2 Gas scope

Under the MMP design, three distinct functions are required. The relevant EDH holds and provides relevant data; the CCS manages permission and issues tokens; and an enquiry-service integration supports matching the consumer and premises to the relevant metering point. The Enquiry Service supports property-to-meter-point matching and is not the source of consumption data.

For electricity, Elexon's SDR is the anticipated first EDH and CCS MMP will support matching to electricity metering points held in the Electricity Enquiry Service. This provides a deliverable first use case for MMP.

An equivalent end-to-end gas consumption-data journey is not currently available and therefore the CCS MMP does not include that functionality. No gas EDH has been identified as ready to support MMP.

In the absence of a gas EDH, the implementation of gas related functionality and the associated cost, including matching gas consumers and premises to gas metering points, would not meet the REC objective of delivering positive consumer outcomes. This is a sequencing decision and the future gas support will be considered as the relevant data source, Energy Data Holder model, MPRN-matching capability, user demand, and business case become clearer. The introduction of gas functionality will be achieved through later iterations.

RECCo conclusion: CCS MMP will initially support domestic electricity consumption data. For the MMP, property-to-meter-point matching will therefore be provided through the Electricity Enquiry Service only. This is the supported delivery direction and a sequencing decision based on what can provide usable consumer benefit now. Future gas support will be considered as the relevant data source, Energy Data Holder model, MPRN-matching integration, user demand, and business case become clearer.

3.2.3 Future evolution of SEC and DCC arrangements

RECCo and SECCo continue to discuss how permission management and data access transparency capabilities may evolve beyond the MMP. Some existing SEC-governed data-sharing arrangements cannot currently be accommodated within the scope of the MMP e.g. bespoke non-digital journeys. RECCo does not consider that use of the CCS should be mandatory across all SEC-governed use cases at this stage, however it does consider it a solution to many of the requirements under the SEC Privacy Controls Framework and is ready for it to be adopted in due course. Any requirement for use of the CCS, as a solution to SEC requirements, would need to be progressed through the appropriate SEC governance.

RECCo, SECCo and industry stakeholders share a common objective of providing consumers with a coherent and consistent experience for granting, managing, and understanding permissions relating to their energy data. RECCo and SECCo are therefore progressing work to recognise CCS as a valid mechanism for obtaining permission under SEC Section I through changes to the Privacy Controls Framework. This will facilitate the incorporation of SEC-governed data-sharing arrangements within the CCS, and establish a pathway towards wider adoption by SEC Other Users, subject to future policy, regulatory and implementation decisions. RECCo and SECCo recognise the importance of clear and effective communication throughout any transition period. This will help minimise consumer confusion and maintain trust in the management of energy data permissions.

RECCo is also engaging with DCC regarding potential future participation in the CCS. Direct DCC integration is not proposed for the MMP. The CCS design is also intended not to prevent future integration with a DCC SMEDR acting as an EDH, should the SMEDR initiative progress and the relevant policy, regulatory, governance and implementation decisions support its inclusion.

RECCo conclusion: RECCo will continue to work with SECCo to enable CCS to be recognised as an approved mechanism for obtaining permission under the SEC arrangements. Participation by SEC Other Users can be considered once those arrangements enable CCS usage by them. RECCo will also continue to work with DCC and industry stakeholders on opportunities for wider future adoption of the CCS, subject to the relevant policy, regulatory, governance and implementation decisions.

3.2.4 Tariff Interoperability

A significant development since the February 2026 Design consultation has been the inclusion of Tariff Interoperability Phase 1b within the CCS roadmap as set out in section 2.4 above.

RECCo conclusion: REC drafting has been developed to accommodate Tariff Interoperability requirements from the outset with Phase 1b implementation planned for a later phase of CCS development. This includes provisions supporting account-holder verification and management of permissions relating to account-specific tariff information.

For Account Specific Tariff Information, account-holder verification will be undertaken by the relevant Tariff Interoperability Energy Supplier rather than through the identity and occupancy verification process used for domestic half-hourly metered data. The supplier will be required to provide a CCS-integrated account-holder verification capability through which an individual can be redirected to the supplier, authenticate with the supplier and be confirmed as the Account Holder for the relevant Registered Meter Point or Points (RMPs). The supplier will then provide the verification outcome and relevant RMP information to the CCS so that the CCS permission journey can continue.

This will require affected suppliers to develop and test technical interfaces with the CCS, including support for the secure authorisation and ID Token exchange used for account-holder verification. The enduring obligations and end-to-end process are set out in the CCS Arrangements Schedule, with the detailed interface, security and message requirements specified through the CCS API Technical Specification and associated Data Specification.

This approach provides suppliers and other participants with greater certainty regarding future requirements and avoids the need for material redesign once Tariff Interoperability Phase 1b is implemented.

3.2.5 Long-term roadmap

RECCo has updated the CCS Product Roadmap to reflect the current MMP scope, anticipated service evolution, and the wider CCS vision. The roadmap distinguishes the confirmed MMP and proposed REC baseline from potential future development, and is organised around ten CCS Product Pillars. It provides a structured view of how CCS capabilities may evolve over time and how future scope is currently prioritised. The roadmap is provided in Annex C and should be regarded as directional rather than a delivery plan. Future iterations remain subject to evidence of consumer and market need, stakeholder engagement, policy and regulatory direction, governance, funding, and implementation readiness. The roadmap annex also includes a requirement-level assessment of how the MMP and future roadmap treatment align with the scope and expectations established through Ofgem's Consumer Consent publications and subsequent CCS Working Group Advisory Paper recommendations.

These roadmap items should be regarded as potential future areas of development rather than commitments. Any future expansion of CCS scope will remain subject to further design work, stakeholder engagement, regulatory decisions, and consultation.

Future areas that may be considered include:

- gas data;
- behind the meter data and asset control;
- non-domestic use cases;
- Priority Services Register (PSR) data;

- direct DCC integration;
- integration with a DCC SMEDR as an EDH, if progressed;
- broader SEC-governed data-sharing use cases;
- assisted and non-digital consumer journeys;
- additional participant types; and
- enhanced consumer transparency and permission management capabilities, including the future treatment of pre-existing permissions.

RECCo will continue to work with Ofgem, DESNZ, SECCo, industry participants, and consumer representatives to refine the CCS roadmap.

3.3 Key CCS design decisions

The following sections set out the key design decisions that underpin the CCS. Each section identifies the final design decision, followed by the rationale for that decision, the feedback received through the February 2026 Design consultation and further evidence or engagement considered by RECCo. Where the final position differs materially from that consulted on in February 2026, this is explained.

The decisions should be read in the context of the particular data type or use case to which they apply. Some decisions, such as the occupier-led permission model, arise from the characteristics of domestic half-hourly (HH) metered data and should not be interpreted as a single permission model that will necessarily apply to every dataset or future CCS use case.

The principal design decisions explained in the following sections are:

- **Role of the CCS** - where permission is required by the applicable regulatory arrangements, including energy codes or energy licences, the CCS will provide the trusted mechanism for obtaining, managing, and evidencing that permission where those arrangements require or enable use of the CCS. The auditable permission record supports each ATP's and EDH's own compliance arrangements; determining and evidencing the UK GDPR lawful basis for processing remains a matter for the organisation concerned.
- **Domestic HH metered data** - the CCS will treat domestic HH metered data as personal data by default. This is an operational assumption, not a legal determination that the data is personal data in every processing context. Whether permission is required remains determined by the applicable regulatory arrangements.
- **Occupier-led permission for domestic HH metered data** - where permission is required, it may only be granted through the CCS by a verified occupier of the relevant premises. Account-holder or bill-payer status alone will not be sufficient. This approach is specific to domestic HH metered data.
- **Multi-occupancy properties** - the lead occupier model will not be adopted. Each verified adult occupier may grant permission only in their own capacity and cannot grant permission on behalf of another adult occupier.
- **Permission revocation, queries, and complaints** - consumers may revoke permissions they have granted. A verified occupier may query a permission granted by another occupier. A queried permission will be terminated and will not be reinstated; continued access will require a new permission. Complaints about an ATP's use of data will remain the responsibility of the ATP rather than the CCS.

- **Identity and occupancy verification** - identity and current occupancy will be treated as separate assurance outcomes. Both must be established before permission for domestic HH metered data can be granted. Verification will be centrally governed, outcome-based, and risk-based. Photographic identification will not be required as the default route.
- **Consumer interaction with the CCS** - consumers using the initial digital CCS journey will need a verified CCS account before granting, viewing, or managing permissions. A guest journey will not be provided.

Together, these decisions establish the permission, consumer-control and assurance principles that will apply to domestic HH metered data through the initial CCS implementation.

The common CCS governance and trust framework can apply different permission rules where these suit a different dataset or regulatory use case. For example, account-specific tariff information under Tariff Interoperability is account-holder-led rather than occupier-led, as explained in section 3.2.4.

The February 2026 consultation sought views on a number of important design questions underpinning the CCS, including how permission should operate, who should be able to grant permission, the treatment of multi-occupancy properties, identity and occupancy verification, and the relationship between the CCS and existing energy data-access arrangements.

Following that consultation, RECCo has undertaken further design development, considering consultation feedback alongside the existing regulatory framework and further evidence and engagement.

The following sections set out RECCo's conclusions on each of the key design decisions. They explain the position consulted on in February 2026, the material feedback and further evidence considered, and the resulting approach, including where this has changed or been clarified.

3.3.1 **Permission to access domestic half-hourly (HH) metered data**

Design decision: Where the applicable regulatory arrangements require an individual's permission before domestic HH metered data may be released, the CCS will provide the trusted mechanism for obtaining, managing, and evidencing that permission where those arrangements require or enable use of the CCS.

Permission managed through the CCS satisfies a regulatory permission requirement and sits alongside, without altering, an organisation's obligations under UK GDPR.

RECCo has considered this feedback alongside further engagement with Ofgem, the ICO and external legal advisers. This has reinforced the need to distinguish between the regulatory conditions governing whether energy data may be released and the separate data-protection obligations applying to organisations that process that data.

Where an applicable energy code, energy licence or other regulatory arrangement requires permission before domestic HH metered data may be released, the CCS will provide the mechanism for obtaining, managing, and evidencing that permission where use of the CCS is required or enabled by those arrangements. A permission recorded through the CCS therefore demonstrates that the relevant permission requirement has been satisfied through the CCS.

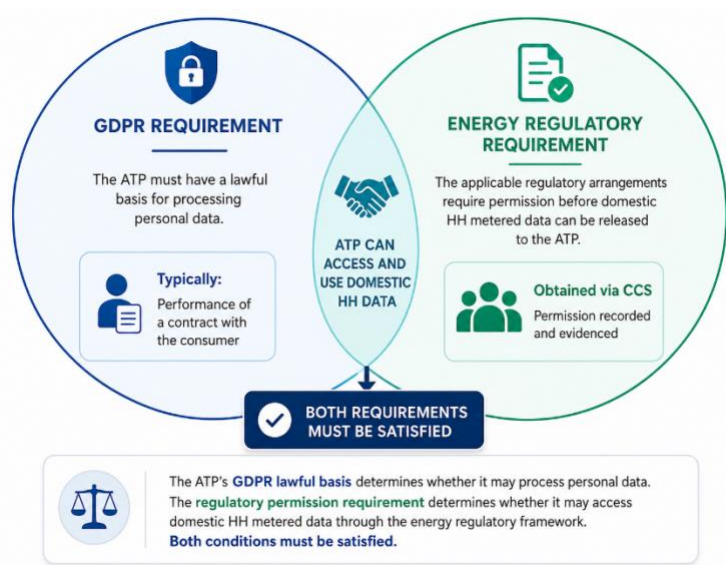


Figure 2

That record does not itself determine whether an ATP, EDH or other organisation has satisfied its full obligations under UK GDPR. Where UK GDPR applies, each organisation makes its own assessment of whether the information constitutes personal data in the context of its processing, identifies and documents an appropriate lawful basis and complies with its wider data-protection obligations. The CCS supports that work; the permission record shows what was permitted, by whom and when, and can be drawn on within the organisation's own compliance documentation.

Where an organisation determines that consent is the appropriate lawful basis for its processing, the CCS permission record may also form part of the evidence used to demonstrate that consent, provided the relevant UK GDPR requirements for valid consent are met. Responsibility for determining the appropriate lawful basis, and for ensuring those requirements are satisfied, remains with the ATP. Equally, the existence of a lawful basis under UK GDPR does not remove any separate requirement imposed by the applicable regulatory arrangements to obtain permission before the data may be released.

3.3.2 Treatment of domestic HH metered data within the CCS permission model

Design decision: RECCo will treat domestic HH metered data as personal data by default. This reflects the granularity of domestic HH metered data and its potential to reveal information about the occupancy, behaviour and activities of people living at a premises. This is an operational assumption used to support the consistent application of the CCS arrangements and is not a definitive legal determination that domestic HH metered data constitutes personal data in every processing context.

The February 2026 consultation proposed treating domestic HH metered data as personal data by default. Some respondents supported this as providing a clear and consistent basis for the operation of the CCS, while others considered that whether the data constitutes personal data should depend on the circumstances in which it is processed and whether

individuals are identifiable. Questions were raised particularly in relation to multi-occupancy households, where consumption data may reflect the combined activities of several occupants.

Further engagement with the ICO and external legal advisers reinforced that whether information constitutes personal data is ultimately a matter of data protection law and depends on whether an individual is identifiable in the circumstances in which the data is processed. RECCo has therefore distinguished between that legal assessment and the operational assumption required for the CCS to operate consistently.

RECCo considers that the operational assumption should be retained. Domestic HH metered data is associated with a domestic premises and, because of its granularity, can reveal information about occupancy, behaviour, and activities within that premises. In addition, certain existing energy data-sharing arrangements make the requirement for permission dependent upon whether the data being released constitutes personal data. Applying a common CCS assumption therefore avoids different classifications resulting in inconsistent application of the CCS arrangements.

This assumption does not replace the assessment that an ATP, EDH or other organisation must make in relation to its own processing of the data.

This design decision applies specifically to domestic HH metered data and is not an MMP-only position. Different datasets or future CCS use cases may require a different approach, taking account of the characteristics of the data and the applicable regulatory framework.

3.3.3 Who may grant permission for domestic HH metered data (occupier vs bill payer)

Design decision: Where the applicable regulatory arrangements require permission before domestic HH metered data may be released, permission through the CCS may only be granted by a verified occupier of the premises to whom the data principally relates. Status as an energy account holder or bill payer will not, by itself, entitle an individual to grant that permission. This decision is specific to domestic HH metered data and reflects the nature of that data and the individuals whose occupancy, behaviour and activities may be revealed by it.

The February 2026 consultation proposed an occupier-led approach for domestic HH metered data, rather than allowing permission to be granted solely on the basis that an individual is the energy account holder or bill payer. This reflected the proposed position that, where regulatory permission is required for access to this data, the person granting that permission should have a current connection to the premises as an occupier.

Responses highlighted differing views. Some respondents supported the occupier-led approach, while others questioned how it would align with existing industry processes, including SEC arrangements, which may focus on an individual's identity and association with the premises rather than expressly distinguishing between occupier and account-holder status. Respondents also noted that supplier interactions are generally based on the contractual relationship with the account holder and raised concerns about potential additional operational complexity.

RECCo has considered this feedback through further engagement with Ofgem, SECCo, the ICO and external legal advisers, alongside the existing SEC arrangements, the policy direction established through DESNZ's Data Access and Privacy Framework (DAPF) and current industry practice. RECCo also considered whether a broader test based on an individual's contractual relationship with the energy supply or other association with the premises could provide an appropriate alternative.

RECCo has retained the occupier-led approach because domestic HH metered data can reveal detailed information about patterns of occupancy, behaviour, and activity at a premises. Although the account holder or bill payer will often also be an

occupier, this will not always be the case. Around one-third (36%)⁷ of UK households live in rented accommodation. Separate research indicates that around 15%⁸ of private renters have energy bills included within their rent. An individual may, for example, retain a contractual or financial relationship with the premises without currently living there. Account-holder or bill-payer status alone therefore does not establish that the individual is one of the people whose activities may be reflected in the domestic HH metered data.

For this dataset, current occupancy therefore provides the more appropriate basis for determining who may grant permission. This links the permission decision to the individuals to whom the detailed consumption data may relate, rather than assuming that a contractual or financial relationship with the premises is equivalent to current occupancy.

This does not prevent an account holder or bill payer from granting permission. Where they are also a verified current occupier, they may grant permission in the same way as any other verified occupier. The distinction applies where account-holder or bill-payer status is being relied upon without evidence of current occupancy.

This is not intended to establish a universal rule for all data supported by the CCS. The appropriate person to grant permission will depend on the relevant dataset and regulatory arrangements. For example, account-specific tariff information under Tariff Interoperability uses an account-holder-led model, as explained in section 3.2.4.

3.3.4 Multi-occupancy properties: lead occupier model

Design decision: In a multi-occupancy property, each verified adult occupier may grant permission only in their own capacity and may not grant permission on behalf of another adult occupier. This is a change to the position set out in the February 2026 Design consultation.

The February 2026 Design consultation proposed that, in properties occupied by multiple adults, a verified lead occupier could grant permission on behalf of all adult occupiers, provided they had first obtained the agreement of the other occupiers. The proposed model also included measures to provide transparency to other occupiers and enable them to challenge permissions where appropriate.

Responses to the February 2026 Design consultation identified significant concerns with this approach. Whilst respondents generally recognised the need for a practical mechanism to support multi-occupancy households, several questioned whether one occupier could legitimately grant permission on behalf of others or reliably demonstrate that they had obtained the necessary authority to do so. Respondents also highlighted the practical difficulties associated with evidencing agreement between occupiers, resolving disputes and maintaining accurate records as occupancy changes over time.

RECCo has considered these responses alongside the wider industry engagement, as well as further engagement with the ICO and external legal advisers.

Although the ICO did not reach a concluded view on the lead occupier model, legal advice identified significant challenges with relying on one occupier to provide permission on behalf of other adults. It highlighted the evidential difficulties of

⁷ [Private rented sector statistics from across the UK - Office for National Statistics](#)

⁸ [Tenant Survey pt.2: Energy bills and efficiency | NRLA](#)

establishing and maintaining assurance that another adult occupier had authorised the lead occupier to act on their behalf and that such authority remained valid when the permission was relied upon.

RECCo has also considered whether these concerns could be addressed by requiring the lead occupier to provide additional confirmation or evidence of the other occupants' agreement. However, this would place the CCS in the position of having to establish and maintain evidence of authority between individual adults within a household. RECCo does not consider that this would provide a sufficiently clear or robust basis for the permission model.

The revised approach links the act of granting permission directly to the verified adult occupier exercising it. In a multi-occupancy property, any adult who independently satisfies the CCS identity and current-occupancy requirements may grant permission in their own capacity. Permission from every adult occupier is not required, but no occupier may grant permission on behalf of another adult. Another verified occupier may query an existing permission through the process described in the following section. This provides the operative model for multi-occupancy properties and removes the need for the CCS to determine whether one adult has authority to act for another.

This decision reflects the characteristics of domestic HH metered data and the occupier-led permission model described in the preceding section. It is specific to domestic HH metered data and is not an MMP-only position.

3.3.5 Consumer complaints, permission revocation, and query resolution

Design decisions: The CCS will distinguish between:

- revoking a permission previously granted by the consumer through the CCS;
- raising a query about data access under a permission granted by another occupier; and
- making a complaint or exercising wider rights in relation to the processing of personal data.

A consumer who granted a permission through the CCS will be able to revoke that permission through the CCS, preventing future sharing under that permission. Where a verified occupier identifies a permission granted by another occupier and does not agree to data relating to them continuing to be accessed under it, they will be able to raise a query through the CCS. The queried permission will be terminated immediately and will not be reinstated. Any continued access will require a new permission through the standard CCS permission journey.

Where a consumer wishes to exercise applicable data protection rights in relation to personal data that has been processed, including rights of access, erasure, objection or complaint, those rights are exercised separately against the organisation responsible for the relevant processing. The CCS will provide sufficient information to enable the consumer to identify the relevant ATP. Nothing in the CCS arrangements restricts a consumer's ability to raise a concern with another organisation responsible for its own processing of their personal data or, where appropriate, with the ICO.

The CCS will not act as the complaint resolution body for complaints about an ATP's use of energy data. The ATP will remain the primary operational point of contact for complaints relating to its use of the data.

For MMP RECCo does not currently propose to mandate participation in a particular alternative dispute resolution (ADR) or ombudsman scheme through the REC. This will be kept under review as the wider government framework for consumer protection and redress within energy and cross-sector smart data develops.

The February 2026 Design consultation proposed that consumers should raise concerns about an ATP's use of energy data directly with that ATP, not through the CCS.

Respondents generally supported this approach, but asked for greater clarity on the respective responsibilities of the CCS, ATPs, and EDHs. That clarity matters most where a complaint remains unresolved, or where the issue relates to the CCS rather than an ATP's actions. They also asked what route is open where a consumer cannot resolve a concern directly with the ATP. Some respondents considered that RECCo should have a clearer role where a concern relates to the CCS itself or indicates wider non-compliance. They did not see such matters as solely bilateral complaints between the consumer and ATP.

Respondents also asked for a clearer distinction between CCS functions and consumers' wider rights under UK GDPR. Revoking or querying a permission affects whether future data sharing may continue under that permission. It does not replace any rights an individual has over personal data already processed.

3.3.5.1 Complaints

RECCo remains of the view that responsibility for investigating and responding to complaints relating to the ATP's use of energy data should remain with the relevant ATP. The CCS will provide the consumer with information needed to identify and contact the ATP responsible for the relevant permission and data access.

During an investigation, an ATP may find that the issue relates to the operation of the CCS, such as the identity verification, occupancy verification, or permission management. The ATP may then raise a service desk ticket in accordance with the REC service management arrangements. This will enable RECCo to investigate and address issues relating to the CCS whilst ensuring that the ATP remains the consumer's primary point of contact throughout the complaint process.

Where an EDH receives a consumer complaint concerning an ATP's use of data, the consumer should be directed to the relevant ATP for investigation and response.

Where complaints or permission queries indicate a wider or recurring failure by an ATP to comply with the CCS requirements, this may also be considered through the REC Performance Assurance Framework and associated breach arrangements.

3.3.5.2 Permission revocation and queries through the CCS

The CCS provides separate functionality for consumers to manage permissions. This is distinct from the complaints process described above.

The February 2026 Design consultation set out arrangements for consumers to review active permissions via the CCS consumer portal. This included the ability for a consumer to revoke permission where they provided the original permission, or raise a query in relation to data access where the permission was granted by someone else.

Where the consumer granted the permission themselves, they may revoke it through the CCS, ending the permission for future sharing, with the relevant parties notified of the change through the CCS lifecycle notifications. Rights in relation to data already processed, including erasure, are exercised with the relevant organisation under data-protection law, and the consumer's CCS record of the permission and its revocation remains visible to them should they wish to pursue those rights.

Where a permission was granted by another occupier, the verified occupier will not revoke that permission as though they had granted it themselves. Instead, where they do not agree to data relating to them continuing to be accessed under the permission, they may raise a query through the CCS.

Some respondents expressed concern that terminating access could disrupt a legitimate service, particularly in multi-occupancy households where another occupier had granted the original permission. RECCo has considered these concerns but does not consider it appropriate for sharing under a queried permission to continue once a verified data subject has challenged it.

Before a consumer can raise a query, the CCS will have verified their identity established the required confidence that they are a current occupier of the premises and matched them to the relevant metering point, establishing that they are a data subject (a verified occupier) in relation to the metered data. A query in these circumstances therefore represents a verified data subject stating that they did not grant the permission and do not agree to data relating to them continuing to be accessed under it. This is particularly relevant following RECCo's decision that one adult occupier cannot grant permission on behalf of another adult occupier.

In those circumstances, RECCo does not consider it appropriate for the CCS to continue to represent the queried permission as active while its validity is investigated. Doing so could allow data relating to a verified data subject to continue to be shared under a permission that they have not provided and have expressly challenged.

RECCo conclusion: where an energy data subject raises a query on the basis that they did not grant a permission and do not agree to their data being accessed, that permission will be terminated immediately and will not be reinstated. Any future access to the energy data will require a new permission. The CCS will terminate the permission and issue the applicable permission revocation notifications to the relevant ATP and, where applicable, EDH so that further sharing under that permission ceases

The ATP will be required to investigate the circumstances surrounding the queried permission, including any change in occupancy, identity or occupancy verification issue, or other matter affecting the validity of the original permission. If the ATP considers that continued access is required, it must initiate a new permission request through the standard CCS permission journey.

3.3.5.3 Complaint escalation and redress

Since the February 2026 Design consultation, RECCo has engaged with the Energy Ombudsman and other stakeholders to explore potential approaches to complaint escalation and consumer support where issues cannot be resolved through standard operational processes. However, RECCo does not consider it appropriate to include provisions within the REC requiring specific alternative dispute resolution arrangements or mandating ATPs' participation in a particular ombudsman scheme.

RECCo is aware of ongoing DESNZ work relating to the development of an Energy Smart Data Scheme, including consideration of consumer protection and governance arrangements. Given that this work remains under development, RECCo considers it premature to prescribe additional complaint escalation or redress arrangements within the REC at this stage.

This position does not affect any statutory complaint or redress rights that a consumer may otherwise have.

3.3.6 Identity and occupancy verification

Design decision: For domestic half-hourly metered data, the CCS will centrally govern the verification needed before a consumer can grant permission. The CCS must establish two separate outcomes: first, sufficient confidence that the individual is who they claim to be (identity verification); and second, sufficient confidence that the individual is a current occupier of the premises to which the relevant metered data relates (occupancy verification). A consumer will only be able to grant permission where the required assurance has been achieved for both outcomes.

The February 2026 Design consultation proposed identity verification broadly equivalent to the GPG45 High Confidence standard, with photographic identity evidence forming part of the expected minimum journey. RECCo also recognised that identity verification alone would not establish whether an individual was entitled to grant permission for data relating to a particular premises and proposed separate evidence of occupancy.

Responses broadly supported the need for appropriate verification but questioned whether requiring photographic identification as the normal route was proportionate. Respondents raised concerns about consumer friction, accessibility, and digital inclusion, as well as whether existing trusted identity relationships could be reused. Questions were also raised about how current occupancy could be established where industry or other records are incomplete, out of date or demonstrate only a historic or financial connection with a property.

Further consumer research and product assessment reinforced concerns about making photographic identification the normal verification route. Those findings informed how the required assurance outcome should be delivered, but did not determine the identity confidence threshold. Separately, the completed identity-assurance assessment considered whether GPG45 High provides material additional assurance over GPG45 Medium when used within the wider CCS control model. It concluded that GPG45 Medium is the proportionate normal identity outcome for the MMP, with higher assurance retained as a targeted step-up where stronger claimant-to-identity binding is required.

RECCo conclusion: For the MMP, RECCo therefore proposes the following approach:

- identity and occupancy verification will remain centrally governed by the CCS rather than being delegated to individual ATPs;
- identity and occupancy will be assessed as separate assurance outcomes;
- the MMP assurance capability will support multiple evidence routes for establishing identity. A trusted bank or reusable identity assertion may provide the GPG45 Medium identity outcome where its provenance and evidence content are sufficient. Photographic identification will not be the default starting point, but may be available as a consumer choice, fallback or step-up route;
- the MMP will separately assess address confidence and current-occupancy confidence. No provider or evidence source reviewed provides complete occupancy verification on its own. The assessment will therefore combine independently sourced, reasonably current signals where practicable, which will include credit-reference address and record review, with the provenance, recency and weight of each signal governed by the CCS. Credit-reference checks do not leave any record or search against the consumer's credit file so will have no impact on their wider credit worthiness;
- no single source of information will, by itself, be treated as determinative of current occupancy. In particular, evidence of ownership, an energy account, another financial relationship, or a historic association with the address will not by itself demonstrate that the individual currently occupies the premises. As part of the permission journey, the consumer will also be required to declare that they are a current occupier and entitled to

grant the requested permission. That declaration supplements, but does not replace, independently sourced evidence;

- where identity evidence is insufficient, fraud or impersonation risk is elevated, evidence conflicts arise, or a permission is disputed, additional identity evidence or step-up verification may be required. Where address or occupancy evidence is insufficient, additional evidence relevant to that assurance outcome may be required before permission can be granted. This may include photographic identity verification, GPG45 High or another approved control appropriate to the identified risk. These processes will be developed over time as real data becomes available to allow CCS to address practically in real world scenarios; and
- the verification capability will provide an auditable outcome and evidence path showing that the applicable identity, address, and current-occupancy requirements have been satisfied. The model will also include controls to prevent a previous occupier's permission carrying forward and to restrict authorised data to the verified occupancy period.

This means that photographic identity evidence is no longer proposed as the default starting point for every consumer. Instead, consumers will have a choice of supported identity verification routes, with photographic identification available either where another route is unsuccessful or as an alternative to the primary journey. The change is therefore from prescribing a particular verification method to defining the identity and occupancy outcomes that the CCS must establish and the evidence requirements needed to support those outcomes.

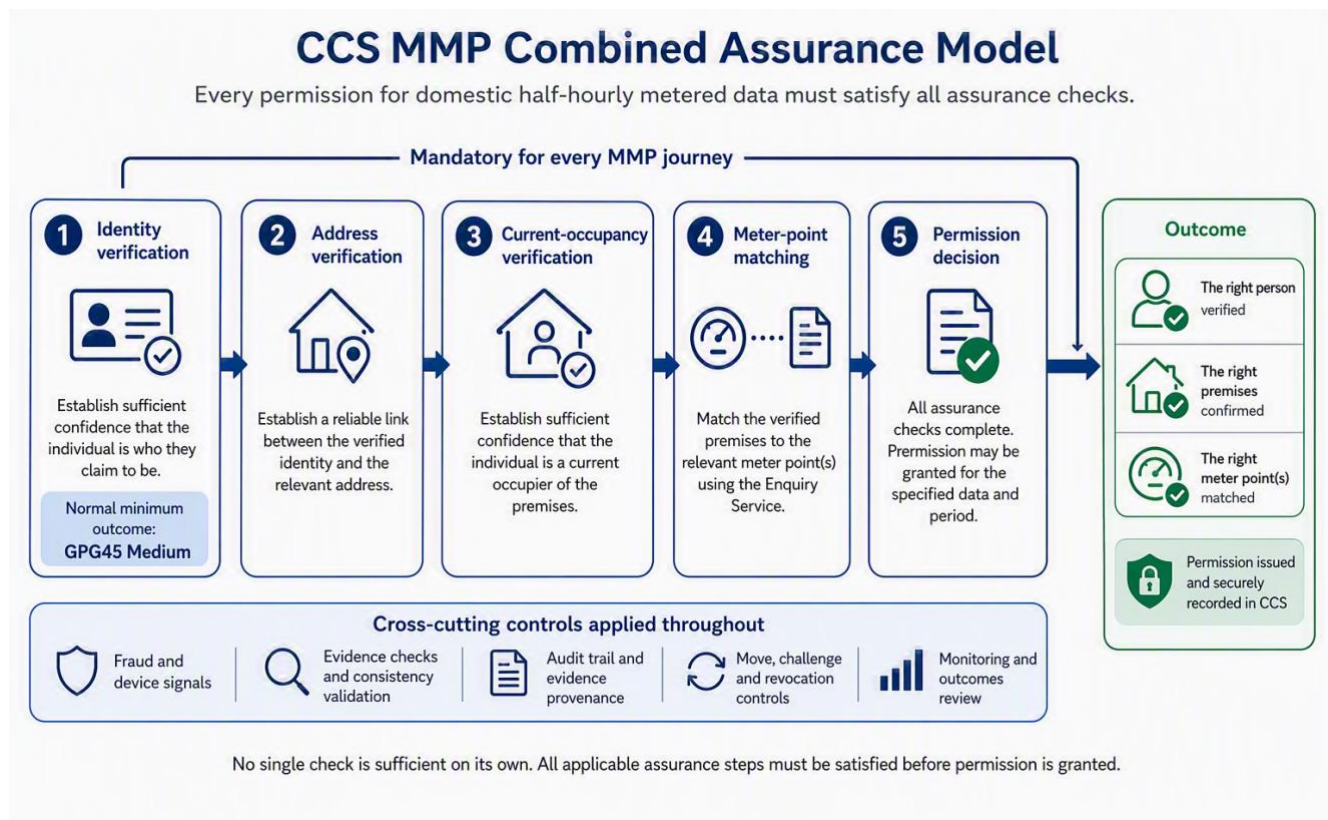


Figure 3

Figure 3 illustrates the MMP identity and occupancy assurance model. Identity, address, current occupancy and metering-point matching are established through separately governed checks. Permission may only be granted once all applicable checks have been completed.

For the MMP, RECCo expects these arrangements to be delivered through a centrally procured verification capability capable of supporting more than one evidence route. The CCS will govern the assurance requirements and evidence rules rather than allowing the service provider to determine what constitutes sufficient verification. This does not prevent additional approved verification providers, trusted identity schemes, or reusable identity assertions from being incorporated into the CCS in future.

3.3.6.1 Assurance standard

RECCo will adopt a demonstrable GPG45 Medium outcome as the normal minimum identity baseline for the MMP. GPG45 is outcomes-based, so the CCS may accept different evidence routes where the resulting profile is properly mapped and evidenced. GPG45 High or additional evidence will be used as a targeted step-up where defined risk or evidence conditions require it, rather than as a universal starting point.

The CCS assurance profile will also contain requirements that are specific to the CCS, in particular the requirement to establish sufficient evidence of current occupancy. GPG45 identity assurance alone does not establish that an individual is currently an occupier of the relevant premises.

3.3.6.2 Address and meter-point matching

Verifying occupancy is separate from identifying the meter points associated with the premises. Once the relevant property has been established, the verified property information will be used by the CCS to identify the associated electricity metering point or points through the Electricity Enquiry Service. For the MMP, a Unique Property Reference Number (UPRN) will be used as the preferred property reference where available. Where a UPRN is not available, the CCS will use the verified address information.

Consumers will not be expected to identify, enter, or select industry-specific meter-point identifiers as part of the standard permission journey.

A successful address or meter-point match does not, by itself, establish that the individual is a current occupier. The CCS must separately achieve the required occupancy assurance before the consumer can grant permission.

Where the CCS cannot establish a sufficiently reliable association between the verified property and the relevant electricity metering point or points, the permission journey cannot be completed for that energy data and the applicable exception process will apply.

3.3.6.3 Where sufficient evidence cannot be established

Where the primary verification route does not provide sufficient confidence, the consumer may be offered an available digital step-up route. If the CCS cannot establish the required identity and occupancy outcomes through the verification routes available within the MMP, the consumer will not be able to grant permission through the CCS at that time.

This may arise, for example, shortly after a consumer has moved into a property, where trusted data sources have not yet been updated sufficiently to establish current occupancy. RECCo recognises this as a limitation of the initial implementation. Assisted and non-digital verification journeys are not proposed for the MMP and will be part of the future development of the CCS.

The detailed consumer messaging and the technical status returned to an initiating ATP where verification is unsuccessful or cannot be completed will be defined within the CCS operational and technical arrangements.

3.3.6.4 What will be finalised before implementation

The design decisions described above establish the proposed MMP verification model. The GPG45 Medium identity baseline and the requirement for separate address and current-occupancy assurance are now established. RECCo is continuing to finalise the detailed evidence combinations, decision rules and implementation configuration required to deliver that model, including:

- the procurement of a suitable IDV provider or providers from a short list who have the capabilities outlined;
- the acceptable evidence combinations, provenance, recency and decision weight for identity, address, and current occupancy;
- the circumstances where step up evidence may be required;
- the wording and presentation of the consumer's declaration that they are a current occupier and entitled to grant the requested permission;
- the audit information retained in the CCS to evidence the verification outcome; and
- the detailed failure, retry and exception handling within the digital journey.

These matters will be specified through the CCS operational arrangements. They will not alter the underlying requirement that both identity and current occupancy must be established to the required level of confidence before permission for domestic half-hourly metered data can be granted. These configurations are not expected to impact the technical specifications ATPs and EDHs will need to interact with and will be for the CCS to manage through its implementation with any IDV provider.

The MMP represents the initial implementation of this framework rather than a permanent restriction on the verification methods available to the CCS. Future development may include additional trusted identity schemes, reusable identity assertions, assisted and non-digital routes and other verification methods, if they meet the CCS assurance requirements.

3.3.7 Consumer interaction with the CCS

Design decision: For the initial digital CCS journey, consumers will be required to create a verified CCS account before granting, viewing, or managing permissions. A separate guest journey will not be provided.

RECCo considers that an account-based approach provides the clearest basis for consumers to maintain ongoing visibility and control of their permissions. Although a guest journey could remove the specific step of creating an account, it would not remove the need for the CCS to establish the consumer's identity and occupancy before a valid permission could be granted. The principal verification requirements would therefore remain materially the same

The February 2026 Design consultation proposed that consumers should be able to interact with the CCS through either a verified CCS account or a guest journey. The guest journey was intended to provide a lower-friction route for consumers who wished to grant permission without creating a CCS account, whilst still completing the identity verification required to support the permission. The consultation also proposed that consumers would be able to view, manage and revoke existing permissions through the CCS.

Responses to the February 2026 Design consultation were mixed on the proposed guest journey. Whilst some respondents supported offering both an account-based and guest journey to maximise accessibility, others considered that consumers should instead be required to establish a CCS account, noting the benefits of providing a single view of existing permissions and a consistent mechanism for managing and querying permissions.

RECCo has undertaken further design development, supported by additional legal advice, consumer research, user experience analysis, and refinement of the end-to-end business processes. This work has focused on simplifying the consumer journey whilst maintaining a secure, transparent, and auditable permission management process.

Consumer research has reinforced the importance of minimising friction in the onboarding journey. Onboarding activities, including account creation, identity verification and occupancy verification, have been identified as potential points of consumer drop-off. RECCo has also engaged with consumer organisations to help ensure that wider consumer perspectives and accessibility considerations inform the developing service design.

These considerations have been balanced against the purpose of the CCS account. A consumer who grants permission may subsequently need to review that permission, revoke it, understand which organisations have active permissions, or raise a query about a permission associated with their premises. A persistent, verified account provides a single mechanism through which those functions can be accessed throughout the permission lifecycle. Furthermore, once an account is established, information and assurance already obtained through the CCS may be reused where it remains sufficiently current and applicable, reducing unnecessary repetition and providing a smoother journey for consumers.

A guest journey would reduce one element of onboarding by avoiding account creation, but it would not remove the identity and occupancy checks needed before permission can be granted. It would also require a separate approach for enabling the consumer subsequently to identify themselves and securely access or manage the permission they had granted.

RECCo considers that the benefits of a single verified account-based journey, particularly ongoing visibility, control, repeat permissions and secure management of permissions, outweigh the additional account-creation step.

4 Revised technical design

4.1 Development of the technical design since the February 2026 consultation

The February 2026 Design consultation presented the CCS technical architecture at a functional and principles-based level. It proposed a hybrid model combining centralised trust, permission, and authorisation capabilities with direct energy data sharing between Authorised Third Parties (ATPs) and Energy Data Holders (EDHs). It also proposed the use of recognised open standards, including FAPI 2.0 and mTLS and a model under which EDHs would validate permission through online token introspection with the CCS.

Respondents generally supported the overall architectural direction but requested further detail on its technical and operational implementation. Areas of feedback included:

- the operational dependency created by mandatory introspection;
- the proportionality of the proposed security controls;
- CCS outage arrangements;

- the allocation of responsibilities between the CCS and participant systems;
- identity and occupancy verification;
- property-to-meter-point matching;
- certificate management; and
- the information exchanged through the permission and token model.

RECCo has since developed the detailed technical design and specifications. The core hybrid architecture is retained, with a number of areas refined. The most significant change is that EDHs will locally validate short-lived, signed JSON Web Token (JWT) access tokens issued by the CCS. This replaces mandatory online introspection for each data request.

The principal developments are summarised below.

Area	February 2026 position	Current design	Development since February
Overall architecture	Hybrid architecture, with central trust, permission and token functions and direct ATP-to-EDH energy data sharing.	Hybrid architecture retained. The CCS operates the central Authorisation Server and authoritative permission/grant record; energy data remains outside the CCS. (Section 4.3)	Retained and further specified. Change in permission verification model represents a shift further towards hybrid by giving EDHs more autonomy.
FAPI 2.0 and mTLS	FAPI 2.0 proposed as the security baseline, with mTLS proposed for relevant CCS and ATP-to-EDH interactions.	FAPI 2.0 retained. The CCS-specific profile selects mTLS as the sender-constraining mechanism for permission-based energy data access. (Section 4.6)	Retained following further assessment of security, proportionality, interoperability, and implementation impacts.
EDH permission validation	EDHs would use mandatory online introspection with the CCS for each relevant data request.	EDHs locally validate short-lived, signed JSON Web Token (JWT) access tokens issued by the CCS. (Section 4.11)	Material change, reducing latency, transaction volumes, and request-time dependency on the central CCS.

Token lifetime, revocation, and outages	The detailed token lifetime and outage model had not been fully specified; the February model depended on central validation and proposed further consideration of outage arrangements.	Access tokens have a maximum 30-minute lifetime; refresh requires the underlying permission still to be valid. Revocation prevents further token issuance but does not retrospectively invalidate an existing token. There is no separate outage fallback without a valid token. (Section 4.12)	Further detail specified as a consequence of moving to local token validation.
Permission lifecycle notifications	Detailed lifecycle-event arrangements were not fully specified.	Shared Signals Framework (SSF) provides push-based notification of defined permission and grant lifecycle events. (Section 4.12.2)	New detailed design.
Identity, occupancy, and matching	Central verification and address-to-meter-point matching were proposed, with further work required on the detailed approach.	Centrally governed identity and occupancy verification is retained. Verified property information is used for matching, with a UPRN-first approach where available and electricity Enquiry Service integration for the MMP. (Section 4.9)	Retained but materially refined.
Permission model	The detailed technical representation of permission had not been finalised.	Rich Authorisation Requests (RARs) structure permission requests; the Permission Authorisation Details defines CCS-specific validation and enables an individual permission to contain one or more permission purposes; the CCS maintains the authoritative grant and issues resource-specific access tokens. (Section 4.10)	New detailed design.
Enabling multi-dataset services	Not fully specified.	A single consumer permission journey can support more than one dataset, even if the data comes from more than one EDH. Each subsequent token request identifies a single EDH, and the resulting Access token contains only the authorised information relevant to that EDH. (Section 4.10.1)	New detailed design.

Participant trust and discovery	A central trust framework, including Directory/Registry capabilities, was proposed.	The CCS Directory provides participant, application, endpoint, role, credential, and data product information to support trust establishment and discovery. (Section 4.7)	Retained and further specified.
---------------------------------	---	---	---------------------------------

Table 2

Each area is explained in the section indicated. Lower-level implementation requirements, including API structures, security controls, certificate arrangements and detailed message content, are set out in the proposed REC technical and data products described in Part B.

4.2 Supporting technical information available with this consultation

RECCo is publishing key supporting technical information alongside this consultation to help respondents understand the end-to-end CCS design and the technical interfaces that underpin it. This is not intended to be a comprehensive set of design documentation. The principal material includes:

- **Business process diagrams** - providing an end-to-end view of the principal CCS processes and the interactions between consumers, ATPs, EDHs, and central CCS capabilities. These diagrams illustrate the permission, authorisation, verification, token, and energy-data-access flows described in Part A. The process diagrams are included in Annex D.
- **CCS section of the RECCo Developer Portal** - providing machine-readable YAML for key elements of the CCS technical design. YAML provides a structured representation of the interfaces, data structures, and messages that developers can use to understand and implement the proposed CCS interactions. The material published includes:
 - **Connect API** - supporting discovery of the detailed technical information required for trusted interactions between CCS Users;
 - **Participants API** - supporting discovery of organisations and participants registered within the CCS ecosystem;
 - **Permission Authorisation Details** - defining the CCS-specific structure used to describe the permission being requested, including the applicable permission purpose or purposes and associated access requirements;
 - **Security Event Tokens** - defining the structure of signed event messages used to communicate relevant permission and grant lifecycle events to CCS Users.
 - **Authorisation Server API** – supporting secure permission authorisation, including requests, consumer redirection and token exchange;
 - **Shared Signals API** - supporting the management of event-notification streams between CCS Users; and
 - **Supplier IDV ID Token** – defining the identity information returned by an Energy Supplier following successful account-holder verification.

The CCS section of the RECCo Developer Portal can be accessed [here](#).

This supporting information is intended to provide sufficient additional detail for respondents, particularly technical stakeholders, to understand how the proposed CCS interactions and data structures operate.

The Developer Portal material represents the current CCS design baseline for the purposes of this consultation and may be refined through the remaining design, development, and implementation activity. Where technical requirements need to form part of the enduring REC baseline, these will be captured through the applicable REC-governed products described in Part B, including the CCS API Technical Specification and the EMDS.

The supporting technical information is therefore distinct from the proposed REC products described in Part B. Its publication or availability through the Developer Portal is intended to support understanding of the proposed design; it does not, in itself, mean that the supporting material forms part of the enduring REC baseline.

4.3 Overview of target architecture

The CCS has been designed as a reusable hybrid architecture rather than around a single dataset or participant model and can therefore accommodate further datasets after MMP go live. Functions that require a common, trusted and consistently governed approach are provided centrally, while existing responsibilities for holding and supplying energy data remain with the organisations that perform those functions. This enables the same core permission and trust capabilities to support different energy use cases without centralising the underlying energy data.

The proposed architecture comprises the following core components:

- **Permission management**, responsible for creating, maintaining, and recording consumer permissions;
- **A Consumer Portal**, enabling consumers to manage and review permissions granted through the CCS;
- **A CCS User Portal**, supporting CCS User onboarding and the management of organisational information and security credentials;
- **A CCS Administrator Portal**, enabling RECCo to access information and update the Directory;
- **A Directory**, enabling participant discovery and trust establishment across the ecosystem;
- **Identity and Occupancy Verification Services**, providing assurance that only appropriately authorised individuals can grant permissions relating to a property;
- **Enquiry Service Integration**, supporting the association of verified consumers with the relevant Meter Point Administration Numbers or Meter Point Reference Numbers (MPxNs);
- **Testing and monitoring**, supporting assurance, compliance, and operational transparency; and
- **Operational support arrangements**, with CCS-related queries and incidents raised through the REC portal to the REC service desk and supported through the existing REC service management arrangements.

Energy data itself will remain outside the CCS. EDHs will continue to hold and provide energy data through the data-access arrangements applicable to their particular service or data product, and ATPs will continue to operate the consumer services for which they require access to that data. The current design therefore retains the central/decentralised split consulted on in February while changing how EDHs validate the authority for individual data requests.

The CCS standardises the trust, permission, authorisation, and security controls required to support data sharing. For the MMP, it does not prescribe a single common API or data format through which every EDH must provide energy data to an

ATP. Existing or use-case-specific energy data interfaces can therefore continue to operate, provided that the applicable CCS authorisation and security requirements are satisfied.

The short-lived token model binds each data-access request to the permission managed through the CCS and is an enduring capability that can be applied to future datasets and use cases.

Under the proposed model, the CCS will manage permissions and participant trust centrally, while energy data continues to flow directly between ATPs and EDHs. RECCo considers that this approach strikes an appropriate balance between establishing consistent consumer protections and minimising central dependencies within the operational data-sharing ecosystem.

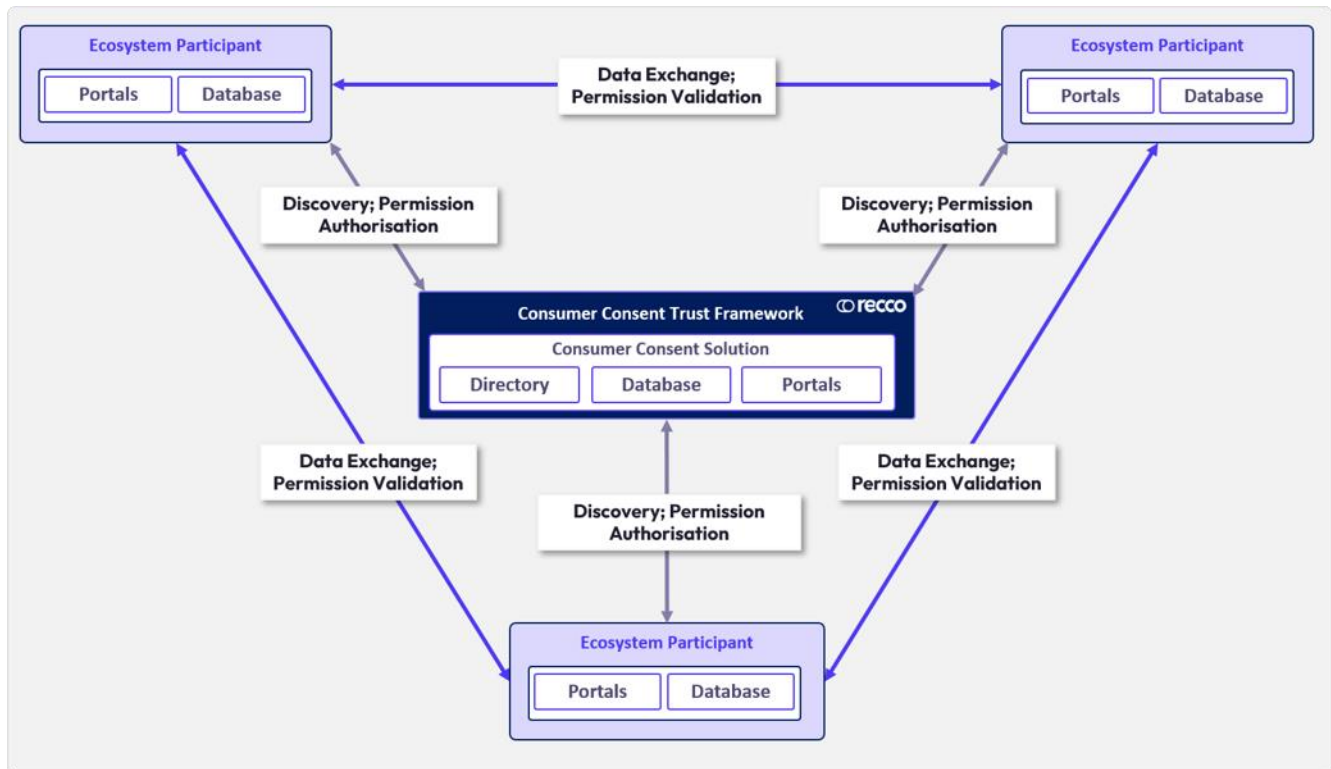


Figure 4

4.4 Applying the CCS design principles

The February 2026 Design consultation set out the design principles underpinning the CCS. These built on the principles established by Ofgem: that the CCS should be Simple and Low Friction; Interoperable; Agile, Flexible and Scalable; Transparent and Informative; Inclusive by Design; and Secure by Design. The February consultation also identified Consistency, Privacy by Design and Promotion of Effective Competition as important principles for the developing CCS.

These principles have continued to guide the detailed design undertaken since February and have informed both the architecture described above and the detailed technical decisions set out in the sections below. In particular:

- **Simple and Low Friction** - the design seeks to minimise unnecessary complexity for consumers and CCS Users while retaining proportionate safeguards. Consumers are not expected to identify industry-specific MPxNs themselves, and information already held by an ATP can, where appropriate, be used as a non-authoritative input

to reduce unnecessary re-entry. Common CCS trust, permission and authorisation arrangements also reduce the need for bespoke bilateral solutions.

- **Interoperable** - the CCS uses an API-based architecture and recognised open standards, including FAPI 2.0, OpenID Connect, OpenID Federation principles and SSF. The Directory provides common participant and service discovery. This also supports the wider interoperability objectives described earlier in relation to the Energy Digitalisation Framework.
- **Agile, Flexible and Scalable** - the core trust, permission and authorisation capabilities are not tied to a single data product or permission model. The architecture can support additional datasets and use cases, subject to future policy and governance decisions, without requiring the core CCS to be redesigned. This is already reflected in its ability to accommodate both the occupier-led MMP model and the different account-holder model required for Tariff Interoperability. Keeping energy data outside the CCS also avoids centralising the potentially much larger volumes of underlying data.
- **Transparent and Informative** - the CCS maintains the authoritative permission record and provides consumers with information about who is requesting access, what access is being requested and for what purpose. The Consumer Portal enables consumers to view and manage relevant permissions. The CEGs provide the detailed requirements for how this information is presented and explained.
- **Inclusive by Design** - consumer-facing CCS journeys are designed to minimise reliance on technical knowledge and to meet the applicable accessibility requirements. Consumers are not required to understand concepts such as MPxNs, tokens or API resources in order to use the service. For the MMP, this principle applies within the scope of the digital service being delivered; assisted and non-digital journeys remain potential areas for future development rather than part of the initial implementation.
- **Secure by Design** - security is embedded throughout the architecture. The CCS uses recognised security standards, registered participant credentials, sender-constrained access tokens and appropriate authentication and authorisation controls. The use of FAPI 2.0, mTLS, short-lived locally validated access tokens and the associated security controls is explained in more detail below.
- **Consistency** - the CCS provides common arrangements for participant trust and discovery, permission management, consumer controls, authorisation, and minimum security requirements. This reduces fragmentation while continuing to allow ATPs and EDHs to operate their own services and systems.
- **Privacy by Design** - the architecture seeks to minimise the information collected, centralised, and disclosed for each interaction. Energy data does not pass through or reside in the CCS as part of the data-sharing transaction, and resource-specific access tokens limit the information provided to an EDH to that required for its role. Identity, permission, and data-access information are separated where they do not need to be disclosed together.
- **Promotion of Effective Competition** - common trust, permission and security arrangements reduce the need for organisations to develop separate bilateral solutions before participating in CCS-enabled data sharing. Open standards reduce reliance on proprietary approaches, while ATPs remain able to differentiate their consumer propositions and EDHs retain responsibility for the data products and data-access services they provide. This reflects the February consultation principle of supporting fair access, reducing unnecessary barriers, and enabling innovation.

Taken together, these principles support the hybrid architecture described above. Functions are centralised where a common and consistently governed capability is needed to support trust, consumer protection, or interoperability, while functions that do not need to be centralised remain with CCS Users. In particular, permission management, participant trust

and discovery, token issuance and the coordination of identity and occupancy verification are provided through common CCS capabilities, while energy data continues to be held and exchanged directly between ATPs and EDHs.

4.5 Allocation of central and decentralised responsibilities

The February 2026 Design consultation sought views on the proposed balance between central CCS capabilities and functions remaining with market participants. Respondents generally recognised the logic of the hybrid architecture, although views differed on the extent to which functions should be centralised. Some respondents questioned the dependency created by central verification and token-validation services, while others supported common trust, permission, token, and identity controls being provided centrally with energy data sharing remaining decentralised.

The detailed design retains that overall split. The CCS provides the common capabilities required to establish participant trust, manage permissions and consumer controls, issue access tokens, coordinate identity and occupancy verification and support monitoring and assurance. EDHs remain responsible for holding and providing energy data, while ATPs remain responsible for the consumer services they provide and their use of authorised data.

The principal change since February is a reduction in the operational dependency on the central CCS. The February design proposed that EDHs would contact the CCS to validate permission whenever an access token was presented. Under the revised design, EDHs validate short-lived CCS-issued access tokens locally. The reasons for this change, and its implications for token lifetime, revocation and CCS availability, are explained below in section 4.11 and 4.12.

4.6 Security and interoperability framework - FAPI 2.0 and mTLS

The February 2026 Design consultation proposed FAPI 2.0 as the baseline security framework for the CCS and proposed mTLS as the common mechanism for securing relevant interactions, including permission-based data sharing between ATPs and EDHs.

Respondents broadly supported the use of recognised open standards and recognised the security and interoperability benefits of FAPI 2.0. Many respondents also supported the use of cryptographically bound access tokens and the additional protection provided by mTLS. However, a number of respondents questioned whether applying these controls to ATP-to-EDH interactions was proportionate, whether the additional implementation cost was justified and whether requiring a common security mechanism for data exchange extended beyond the intended scope of the CCS hybrid model.

RECCo has considered those concerns through the subsequent detailed design. The proposed position remains that FAPI 2.0 will provide the baseline security framework for permission-based CCS interactions, with a CCS-specific profile used to remove unnecessary implementation optionality and provide a consistent approach across the ecosystem.

In assessing proportionality, RECCo has considered the sensitivity of domestic HH metered data, the potential consumer impact of an access token being intercepted or replayed, the implementation burden on CCS Users, the need for interoperability and the alternative of allowing participants to establish different bilateral security arrangements. RECCo's conclusion is that a common sender-constrained token and participant-authentication model provides a proportionate baseline: it directly addresses the risk that possession of a stolen token could otherwise be sufficient to access consumer data, while reusing the participant trust and credential arrangements that CCS Users require in order to participate in the CCS.

RECCo considers the use of an established open security framework preferable to developing a CCS-specific protocol. FAPI 2.0 provides established security controls, implementation patterns, and threat modelling for high-value data-sharing interactions. It also supports the wider interoperability objective of enabling CCS Users to implement against a common

model rather than developing different security arrangements for individual bilateral relationships. The alternative considered was to develop an energy or CCS specific standard, this was ruled out as disproportionately costly and time consuming, whilst also limiting the potential wider economic benefit that comes from federating with other trust frameworks like Open Banking and other sectors.

An important requirement of this model is that access tokens are sender constrained. This means that possession of an access token alone must not be sufficient to use it. FAPI 2.0 supports different mechanisms for achieving this; the CCS-specific profile selects mTLS.

Under the proposed approach, an access token used to request energy data is cryptographically bound to the ATP's registered certificate. When the ATP subsequently presents that token to an EDH, it must also demonstrate possession of the corresponding certificate through the mTLS connection. An intercepted token cannot therefore be used simply by another party that obtains a copy of it. The CCS API Technical Specification requires the certificate used when the token is presented to correspond to the certificate to which the token was bound when it was issued.

RECCo considers that a common sender-constraining mechanism is preferable to allowing ATPs and EDHs to establish different arrangements for each data-sharing relationship. It provides EDHs with a consistent means of verifying that the party presenting a token is the ATP to which that token was issued and reduces the need for bespoke participant authentication arrangements.

The implementation burden of mTLS has also been considered in reaching this position. CCS Users will already require registered technical identities and credentials for protected interactions with the CCS, and the Directory provides the participant and public security information required to support trusted interactions. Extending that common certificate-based model to permission-based ATP-to-EDH data access avoids introducing a separate authentication framework for the subsequent energy data request.

The requirement is also more targeted than applying mTLS indiscriminately to every interaction with the CCS. It applies to the protected communications required to support permission-based sharing and associated secure interactions. Publicly available information within the CCS Directory is not subject to the same requirement. The proposed CCS Arrangements Schedule reflects this distinction.

The CCS security profile also incorporates established controls including private_key_jwt client authentication, Pushed Authorization Request (PAR), signed request objects using JWT Secured Authorisation Request (JAR), Proof Key for Code Exchange (PKCE), issuer and audience validation and certificate-bound access tokens. ATP public keys used for authentication are registered through the CCS Directory, providing a consistent mechanism for key registration and management.

The CCS publishes the public signing information required to validate its signed tokens through a JSON Web Key Set (JWKS) endpoint, allowing CCS Users to retrieve the appropriate public keys and accommodate key rotation without requiring separate bilateral key distribution.

The selection of FAPI 2.0 and mTLS does not alter the hybrid allocation of responsibilities described above. The CCS defines the common trust, authorisation, and minimum security arrangements, while energy data continues to be requested from and supplied directly by the relevant EDH. RECCo considers this to be a technical implementation of the secure and interoperable hybrid model rather than a centralisation of the underlying data-sharing service.

The detailed certificate issuance and management arrangements will be set out through the applicable CCS technical and operational products. The design requires CCS Users to operate with trusted, registered credentials that can be validated

consistently across the ecosystem; it does not depend on the CCS Provider itself necessarily performing every certificate-authority function.

Figure 5 illustrates how the FAPI 2.0 and mTLS controls described above are applied across the permission, authorisation, and subsequent energy-data-access flow. Section 4.8 describes the corresponding end-to-end flow in greater detail, using the P1-P19 interaction references shown in Figure 7.

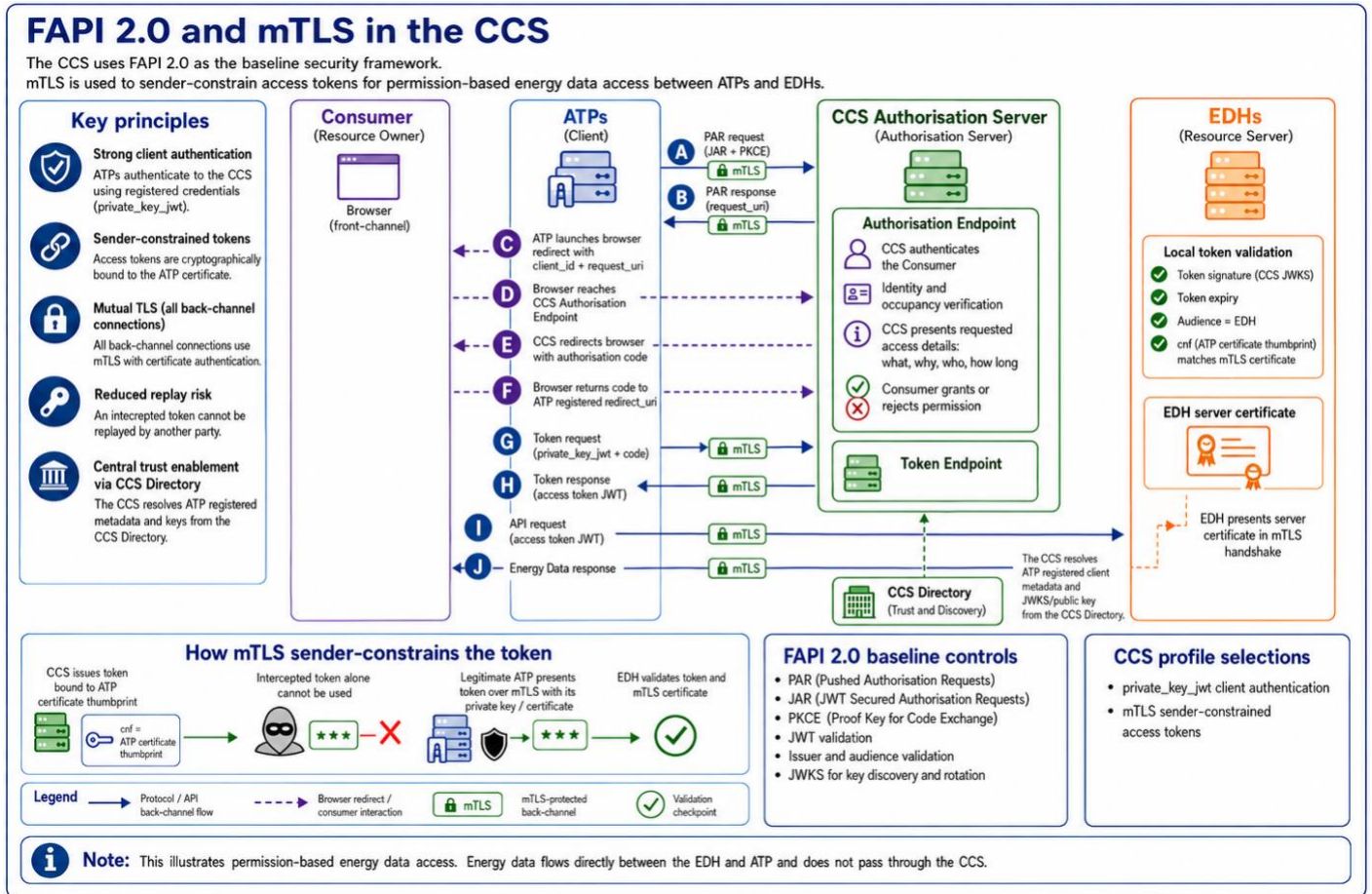


Figure 5

4.7 CCS Directory and trust enablement

The CCS Directory provides the common participant and technical information required for CCS Users to discover one another and establish trusted interactions. It is the authoritative CCS source for information about qualified CCS Users and the technical assets through which they participate in the CCS.

CCS Directory and trust enablement

Authoritative participant and technical information supporting trusted CCS interactions.

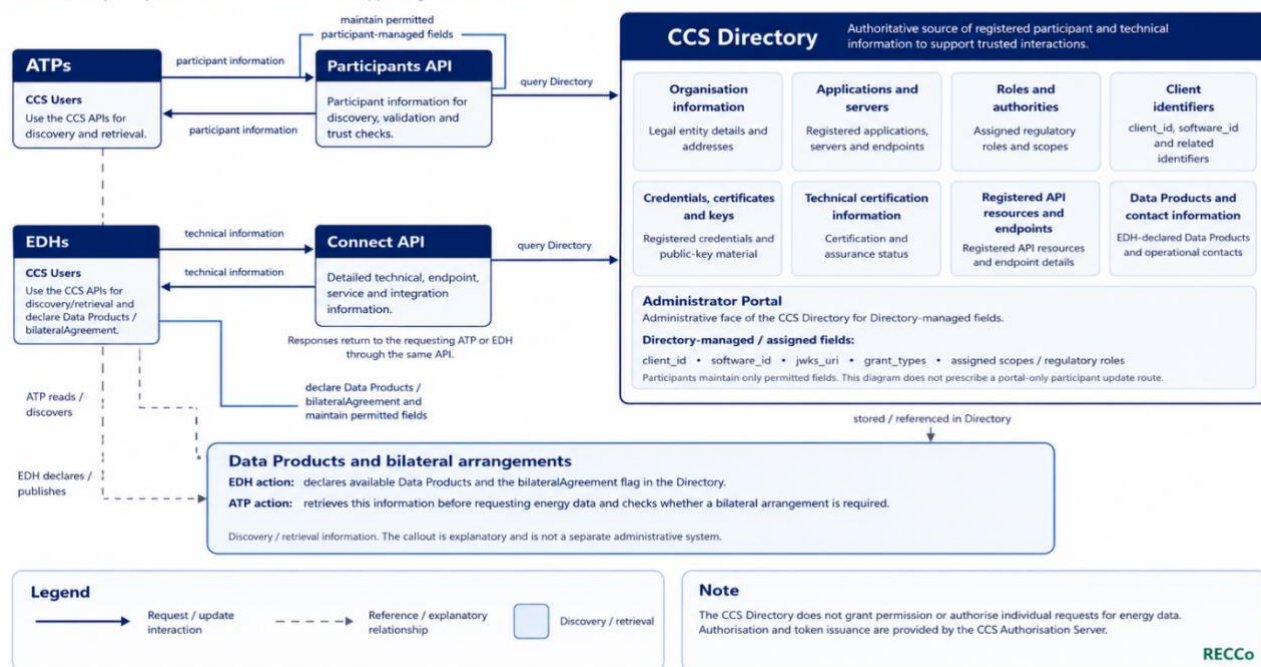


Figure 6

The process through which an organisation becomes qualified to participate in the CCS is described in section 6.4. The proposed REC requirements implementing that approach are described further in Part B (sections 8.3 and 8.5), including the changes to the Qualification and Maintenance Schedule and the “Becoming a CCS User” provisions of the CCS Arrangements Schedule.

During onboarding, records and technical information may be established within the CCS Directory to support the applicant's onboarding and testing activities. This should be distinguished from the organisation's live production status: production credentials and live access are only provided once the applicable qualification requirements have been completed. Once qualified, the Directory provides the authoritative CCS record of the qualified CCS User and the technical assets through which it participates in live operation.

The Directory holds the information required to support the organisation's participation in the CCS. This can include:

- applications and servers operated by the organisation;
- registered API resources and endpoints;
- participant roles and authority information;
- client identifiers;
- certificates and public keys;
- technical certification information; and
- Data products and operational contact information.

The Directory distinguishes the legal organisation from the individual applications, servers, and credentials it operates so that trust and access controls can be applied at the appropriate level. It does not hold private key material or energy data.

Energy data continues to be held by the relevant EDH and is exchanged directly between the EDH and ATP through the arrangements described below.

Registration, identification, and management of CCS Users is based on OpenID Federation principles. This allows participants and technical components to be associated with the roles, credentials and other information needed to determine whether they are trusted for a particular interaction. The CCS Directory therefore provides an important part of the CCS trust model, but it is not a separate permission-management system.

The Directory supports governed maintenance of participant and technical information, including onboarding information, registered technical assets, data products, and credentials, through the role-controlled portal and administrative functions and the applicable CCS APIs in accordance with the CCS Arrangements Schedule and CCS API Technical Specification. The Participants API and Connect API support the discovery of participant and technical information needed for CCS interactions.

The Participants API supports retrieval of participant information across the CCS ecosystem. The Connect API provides CCS Users with more detailed information about individual organisations and their registered technical assets, including relevant endpoints, certificates, keys, applications, roles, and technical certification information.

CCS Users can use this information to discover the relevant services and endpoints and to validate the participant, application, role, and security information needed to establish a trusted connection. For example, an ATP can use the Directory to identify the EDH associated with a relevant data product and obtain the technical information needed to interact with that EDH.

The Directory also identifies the data products made available by individual EDHs. Where access to a data product is subject to an additional bilateral arrangement between an ATP and EDH, this can be identified through the Directory so that the ATP can determine what additional arrangements are required before requesting the energy data.

A CCS User may use a third-party technical service provider to operate systems or manage interactions on its behalf. Under the proposed arrangements, that service provider operates using the CCS User's registered security credentials and does not become a separate source of authority for the interaction. The qualified CCS User remains accountable for compliance with the applicable CCS obligations.

The CCS Directory does not itself grant a consumer's permission or authorise an individual request for energy data. Its role is to establish who (ATPs and EDHs) and what (data products) is participating in the CCS, the technical capabilities and credentials associated with them and how trusted interactions can be established. The CCS Authorisation Server and the permission and token arrangements described below provide the separate authorisation mechanism for access to energy data. The API Technical Specification makes the same distinction: the Directory APIs provide participant and technical metadata but do not define the permission or energy data access transaction.

4.8 Permission initiation and authorisation flow

The February 2026 Design consultation described a model in which the ATP manages the wider consumer service relationship but the consumer is directed to the CCS for the permission-granting step. The subsequent design retains that approach. The February consultation did not envisage an ATP independently obtaining the CCS permission and then simply registering it with the CCS: it described the consumer being redirected into the CCS permission journey.

The current design makes this boundary more explicit. Figure 7 illustrates the end-to-end permission initiation, authorisation, and subsequent ATP-to-EDH energy-data-access flow. References P1-P19 below correspond to the numbered interactions shown in the figure.

Permission initiation and authorisation flow

CCS permission authorisation and direct ATP-to-EDH energy data access

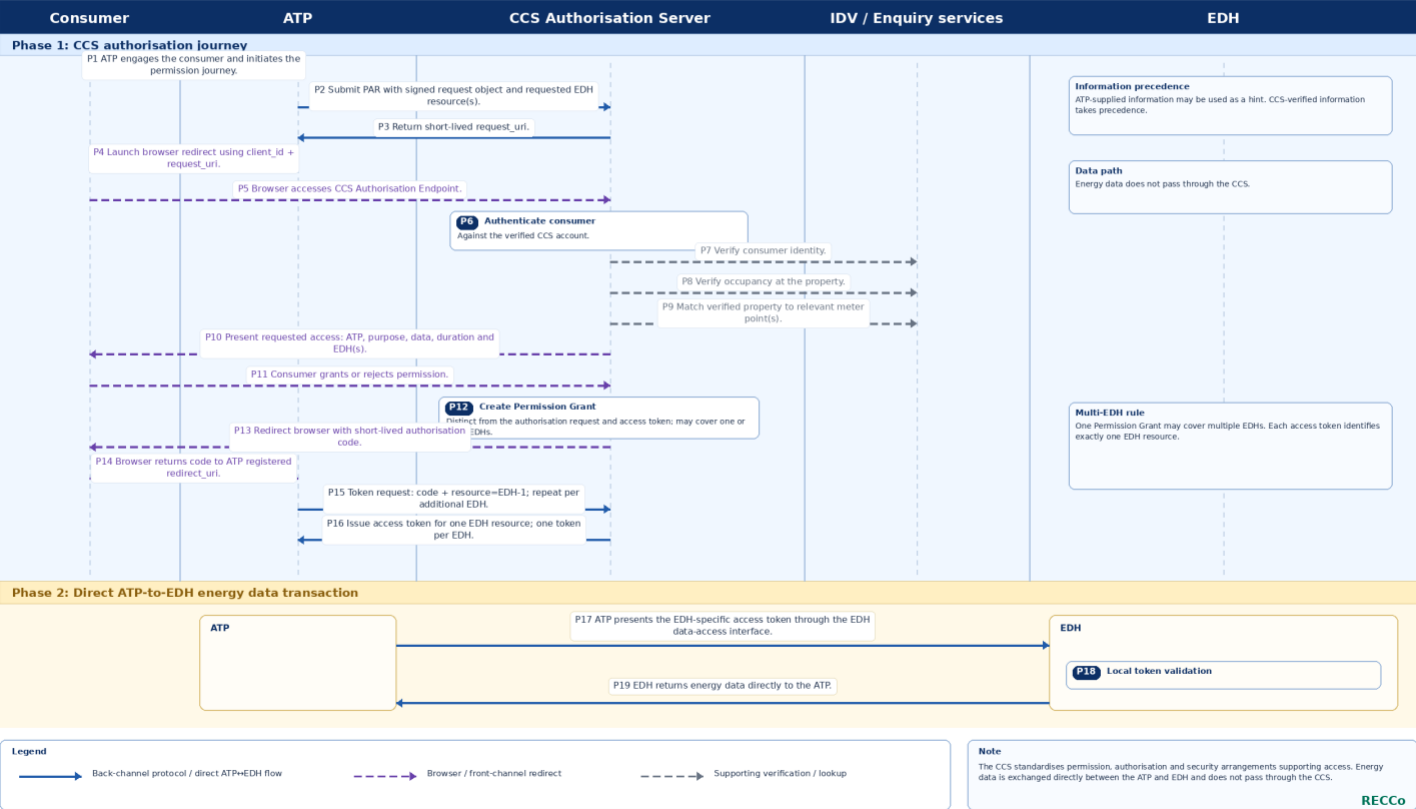


Figure 7

A consumer may begin their overall service journey through an ATP's website, application, or other consumer-facing interface. The ATP establishes the service the consumer wishes to receive and the access to energy data required to provide that service (P1).

Where CCS permission is required, the ATP initiates the authorisation process by submitting a PAR (Pushed Authorisation Request) directly to the CCS (P2). The initial permission details are contained in a signed request object and may include one or more permission purposes applicable to the access being requested. The request also incorporates PKCE to protect the subsequent authorisation-code exchange. An ATP may also request an ID token at this stage which will allow CCS to provide further information regarding the consumer.

The ATP may provide information already known to it where this can reduce unnecessary effort for the consumer. For example, permitted consumer or property information may be supplied to assist the subsequent journey. Any such information is treated as a non-authoritative hint. It does not establish the consumer's identity, occupancy or entitlement to the relevant energy data and may be superseded by information subsequently established by the CCS.

Where the PAR is valid, the CCS returns a short-lived request_uri (P3). The ATP then initiates a redirect in the consumer's browser using the client_id and request_uri (P4), and the browser accesses the CCS Authorisation Endpoint (P5).

The consumer interacts with the CCS to complete the relevant authentication and verification steps. For the initial digital MMP journey, the consumer will have or establish a CCS account and authenticate against that account (P6). Where required for the permission, the relevant CCS IDV process then establishes identity and current occupancy (P7-P8), and the verified property is matched to the relevant meter point or points (P9). The required verification outcomes must have been achieved before permission can be granted.

The CCS then presents the consumer with the access being requested, including the ATP, permission purpose or purposes, data, duration and relevant EDH or EDHs (P10). The information shown is based on the validated authorisation request and the information established through the CCS journey so that the consumer can understand what access is being requested before deciding whether to grant or reject the permission (P11).

Where permission is granted, the CCS creates and maintains the resulting permission and grant as the authoritative CCS record (P12) including the permission purpose or purposes granted by the consumer, and redirects the consumer back to the ATP with a short-lived, single-use authorisation code (P13).

The browser then returns the authorisation code to the ATP's registered redirect_uri (P14).

The authorisation code does not itself authorise access to energy data and is passed to the ATP through this front-channel redirect. The ATP then exchanges the code securely with the CCS token endpoint over an mTLS connection, identifying the relevant EDH through the resource parameter (P15). Subject to successful validation, the CCS issues the relevant access token (P16) and refresh token and, where the applicable OpenID Connect request has been made, an ID token.

When an ATP requires an access token to request energy data from an EDH, the token request identifies that EDH through the resource parameter. Each token request identifies one EDH, and the resulting access token contains only the authorised information for which that EDH is responsible.

The ATP then presents the CCS-issued access token directly to the relevant EDH through the EDH's data-access interface (P17). The EDH performs local validation of the token (P18), as described in section 4.11, and applies any other controls applicable to its data product before deciding whether the requested energy data can be released.

The EDH must ensure the access token is still valid when the energy data is disclosed. Where energy data is not immediately available and is prepared or processed over a longer period, a valid access token is still required before the energy data is ultimately released to the ATP. A previously valid token, or the existence of an earlier request for energy data, does not by itself authorise disclosure after that token has expired.

Where the request is authorised, the energy data is exchanged directly between the EDH and ATP (P19). It does not pass through the CCS.

The CCS does not prescribe a single common energy data API or format for the MMP. It provides the common trust, permission, authorisation, and security controls, while the underlying data continues to be provided through the interface applicable to the relevant EDH and data product. This preserves the hybrid architecture and avoids duplicating existing data-access capabilities.

Where the permission journey cannot be completed - for example because the consumer does not grant permission, the authorisation request is no longer valid, or the required verification or matching cannot be completed - the CCS does not issue an access token authorising the requested energy data. The applicable error or exception outcome is handled through the API and operational error-resolution arrangements described in the supporting technical material.

4.9 Identity, occupancy verification and property-to-meter-point matching

Before a consumer can grant permission for domestic metered data, the CCS must establish two assurance outcomes: that the person is who they claim to be (identity), and that they are a current occupier of the premises the data relates to, entitled to grant the permission. Both must be satisfied, and they are not interchangeable; proving identity does not prove occupancy. The normal minimum identity outcome is GPG45 Medium. Occupancy is governed by separate evidence rules and is assessed through the person's verified link to a specific address; that verified address is also what the CCS later uses to find the right meter point.

Verification remains centrally governed for the MMP, and is outcome-based and risk-based rather than prescribing a single method. RECCo will procure a capability that can orchestrate multiple evidence routes and return a separate, auditable outcome for each element it assesses; identity, address confidence, and current occupancy:

- **Identity** - a trusted bank or reusable identity assertion may deliver the GPG45 Medium outcome where its provenance and evidence content are sufficient. It will not, by itself, establish occupancy;
- **Occupancy** - assessed using independently sourced, reasonably current signals linking the person to the premises. No single financial, account, ownership or historic address association will be treated as conclusive;
- **The consumer's declaration** that they are a current occupier entitled to grant the permission supplements this evidence. It does not replace it; and
- **Information supplied by an ATP** may reduce unnecessary consumer input, but it is a non-authoritative hint.

Occupancy verification produces the verified property information; including a UPRN where one is available. Once both outcomes are achieved, the CCS uses that information to match the premises to the relevant RMP or RMPs.

The February 2026 consultation proposed using existing industry address information and the Enquiry Services for this matching. Respondents supported reusing existing infrastructure, but highlighted longstanding matching problems: inconsistent address records, complex properties, and the risk of either failing to match a legitimate consumer or matching them to a neighbour's meter point. RECCo has since tested alternative property references, data sources, and matching approaches. None removes the underlying data-quality risk while giving the coverage the initial service needs.

RECCo will therefore use the Electricity Enquiry Service, which offers established industry coverage and the meter-point information that matching requires. Matching will be UPRN-first: where verification returns a UPRN, that is the preferred property reference; where it does not, the CCS will use the verified address information under the applicable matching rules. Relying on a verified UPRN rather than unverified free-text addresses reduces the risk of false-positive matches. Consumers will not be asked to find, enter, or select an MPxN at any point.

Two limits on scope. The Electricity Enquiry Service performs matching only, consumption data comes from the relevant EDH, and the CCS separately manages permission and token issuance. It also relies on Retail Energy Location (REL) address data; the REC changes needed to permit that use are set out in section 8.9.

Where the CCS cannot establish a sufficiently reliable link between the verified property and the RMPs, the permission journey cannot be completed for that energy data and the applicable exception process applies.

Occupancy verification also bounds the data that may be authorised. Where the CCS verifies current occupancy but cannot establish that the consumer occupied the premises for the whole period the ATP has requested, the permission must not authorise access to data from before the verified occupancy period.

4.10 Permission and authorisation model

The detailed representation of permission was not fully specified at the time of the February consultation. This was one of the areas developed subsequently through the detailed technical design and industry engagement.

The current design uses RARs (Rich Authorisation Requests) to structure the authorisation requested by an ATP. Within a RAR, `authorization_details` describes the permission being requested. This expresses the relevant permission type, purpose, and service-specific access requirements, rather than relying on broad OAuth scopes alone. The CCS API Technical Specification defines permission at the level of permission type and purpose and then applies service-specific information appropriate to that permission type.

The CCS-specific structure and validation rules applying to `authorisation_details` are defined through the Permission Authorisation Details.

The Permission Authorisation Details is therefore a technical construct used to define and validate the CCS authorisation request. It is not the permission itself and it does not become the access token, although some of the same fields are used within the access token following CCS validation and enrichment and application of the field-level data-minimisation rules defined in the permission authorisation details

An individual permission may contain one or more permission purposes. This enables a consumer to authorise access required for a service where that access supports more than one defined purpose without requiring a separate permission journey for each purpose.

Each permission purpose included in a request must align with the applicable values governed through the Permission Purpose Catalogue, which provides the authoritative set of permission purposes available within the CCS.

As the authorisation journey progresses, the CCS may enrich the permission information using the outcome of identity, occupancy and RMP matching, validate information supplied by the ATP and remove or supersede non-authoritative hints where authoritative information has been established. The resulting grant is therefore the validated outcome of the CCS authorisation journey rather than simply a copy of the request initially submitted by the ATP.

The grant must also be distinguished from an access token.

The CCS maintains the authoritative grant describing the permission provided to the ATP. When the ATP requires access to a particular EDH, the CCS derives a resource-specific access token from that grant. The token response provided to the ATP can therefore contain a wider representation of the permission than the access token presented to an individual EDH.

The API Technical Specification expressly allows the `authorisation_details` within the token response and access token to differ. The access token contains only the information needed by the particular EDH to fulfil the authorised request. The Permission Authorisation Details specifies, at field level, whether information is included in the token response, access token, or both.

Aligning with the principles of security and privacy by design, this supports data minimisation. Information that the CCS or ATP requires in connection with the overall service does not need to be disclosed to an EDH where it is unnecessary for that EDH's part of the interaction.

Identity information is similarly kept separate. Where an ATP is entitled to receive verified identity information, this can be requested through the applicable OpenID Connect mechanisms rather than automatically reproducing that identity information within the EDH access token.

4.10.1 **Services involving more than one EDH**

Feedback during detailed design also highlighted the importance of avoiding a model in which a consumer has to complete multiple permission journeys simply because the service they want happens to depend on data provided by more than one EDH. The consumer's decision is principally about the service and the access being requested, rather than the technical decomposition of that service across underlying data providers.

The ability for a permission to contain more than one permission purpose is separate from this multi-dataset capability. A permission may contain multiple permission purposes whether the service requires access to one dataset or several, and whether the relevant data is provided by one EDH or more than one EDH.

The technical design allows the `authorisation_details` within a PAR to support access to multiple datasets by structuring the permission for each data type separately within the same overall request. This means a consumer can grant permission for different types of energy data as part of a single permission journey, while the specific requirements for each type are kept in separate entries. The Permission Authorisation Details applies the relevant validation to each entry and, where appropriate, to the request as a whole.

This does not result in a single access token being presented to every EDH.

Each subsequent token request identifies exactly one EDH through the resource parameter. The CCS then issues an access token containing only the authorised information for which that EDH is responsible, with the EDH identified through the token audience.

One overall consumer permission journey and grant can therefore contain the authorised elements needed for a service which requires one or more permission purposes, multiple datasets, and potentially multiple EDHs, while each subsequent access token remains specific to the EDH to which it will be presented.

4.11 **How EDHs validate permission**

One of the most material changes since the February consultation concerns how an EDH determines whether a request from an ATP is authorised.

4.11.1 **Local validation instead of mandatory introspection**

The February consultation proposed a model under which an EDH would contact the CCS each time an access token was presented in order to check that the associated permission remained active. This mandatory introspection model provided a strong link to the centrally held permission record and would have enabled permission status changes, such as revocation events, to be reflected immediately when the EDH next checked with the CCS.

Responses were mixed. Some respondents supported the high-assurance nature of the model and the associated auditability. However, a significant proportion raised concerns regarding proportionality, cost, latency, operational complexity and the resulting hard dependency on the availability and performance of the central CCS. Respondents also suggested alternatives including local token validation and caching.

RECCo has considered this feedback and does not propose to proceed with mandatory request-by-request introspection.

For permission-based access to energy data, the CCS will instead issue signed JWT access tokens which the EDH validates locally. The EDH therefore does not need to contact the CCS at the point of every individual energy data request.

The CCS Authorisation Server remains responsible for issuing the authorisation credential. EDHs do not independently issue or manage CCS permission tokens; their role in the energy data transaction is to act as the relevant resource server, validate the token presented by the ATP and apply the other controls applicable to their data product.

At a minimum, the EDH validates:

- the access-token signature using the CCS public signing key;
- that the token has not expired;
- that the token audience identifies the EDH receiving the request;
- that the certificate-binding information within the token corresponds to the ATP certificate presented through the mTLS connection; and
- that the energy data requested, including the applicable data period, is within the scope authorised by the access token.

These checks are defined in the CCS API Technical Specification.

RECCo considers that this substantially reduces request-time dependency on the CCS and removes the additional latency and transaction volume that mandatory introspection would have introduced, while retaining a common CCS-issued authorisation credential which can be cryptographically validated by the EDH.

The change does, however, create a trade-off: once a signed self-contained access token has been issued, the contents of that token cannot be retrospectively changed merely because the underlying permission subsequently changes. The access-token lifetime and lifecycle arrangements are therefore important elements of the revised model, since they govern the true maximum delay that can occur within the ecosystem between a consumer-initiated revocation and this being reflected ecosystem-wide.

4.12 Access-token lifecycle, revocation, and CCS availability

4.12.1 Access-token lifetime and refresh

Access tokens used for permission-based energy data access will have a maximum lifetime of 30 minutes. The purpose of the 30-minute maximum is to limit the period for which a token issued before a subsequent change in the underlying permission could continue to pass local technical validation.

The governing rule is that a valid access token must exist at the point energy data is disclosed:

- An ATP needs a token only when it is requesting or receiving energy data. It does not need to obtain a new token every 30 minutes regardless of need;

- The EDH must validate the token before releasing the data. A token that was valid when a request was made does not authorise disclosure after that token has expired; and
- Some energy data is not immediately available and must be fetched, prepared, batched or otherwise processed first. Where the data becomes available after the original token has expired, the ATP must obtain a new access token before the data may be released. How the ATP learns that the data is ready is a matter for the applicable data product and EDH arrangements; the token rule applies in every case.

Where an ATP needs a further access token, it uses the refresh token associated with the grant. Before issuing one, the CCS checks that the underlying permission remains active; if the permission has expired or been revoked, the request is rejected. A refresh token is also provided for a one-time permission. For a one-time permission, the CCS sets the permission expiry to 25 hours after its start, and the ATP must revoke that permission once it has been exercised. A one-time permission is not treated as exercised until the requested energy data has been received in full, including any data provided asynchronously by the EDH.

The 30-minute lifetime therefore bounds only the disclosure window for an individual token. It does not require energy data to be prepared within 30 minutes where that is not ordinarily achievable, and it should not be confused with the duration of the permission itself: a consumer permission may remain active for months or years, while individual tokens expire and are replaced.

4.12.2 Revocation and lifecycle notifications

Where a consumer revokes a permission, they previously granted, the CCS ends the relevant grant and prevents the associated refresh token from being used to obtain further access tokens.

Where the consumer gives that revocation instruction to the relevant ATP, the ATP submits the revocation to the CCS so that the authoritative CCS grant is ended. This is distinct from the original permission-granting process: the ATP can communicate the consumer's withdrawal of an existing permission to the CCS, but it does not independently create the authoritative permission record.

Revocation takes effect immediately against the grant held by the CCS. It does not, however, retrospectively invalidate an access token that has already been issued. The API Technical Specification expressly provides that ending the grant prevents further refresh-token exchanges but does not invalidate an existing access token.

The maximum 30-minute lifetime is therefore not a 30-minute delay in the CCS processing the revocation. It is the maximum possible residual technical lifetime of a token that was issued before the revocation occurred. In practice, the remaining lifetime may be materially shorter.

4.12.2.1 Use of Shared Signals Framework (SSF) for grant status updates

The CCS also uses SSF to communicate defined changes in permission and grant state only, they do not replace access tokens. Notifications are delivered as signed Security Event Tokens (SETs), allowing the receiving CCS User to verify the source and integrity of the event.

The current technical design uses push delivery. A receiver registers the endpoint at which it will receive events and the CCS delivers the relevant SET directly to that endpoint.

ATPs are required to receive and process the applicable permission lifecycle events; SSF is how ATPs can be kept up to date on the status of the grants relevant to them. Relevant EDHs receive those events where required by their role or

where they have registered to receive them under the CCS arrangements. SSF is intended to enable secure and lightweight lifecycle notifications to be shared regarding grants; it does not replace local cryptographic validation of an access token where an access token is presented for a data request. For request-time disclosure, the EDH must hold and validate a valid access token. Where an EDH undertakes future, scheduled or other activity under a permission without an access token being presented at that point, the CCS arrangements require the EDH to monitor the applicable permission revocation notifications and cease the relevant activity following revocation

SSF is also the mechanism to manage circumstances in which information about a permission has been received by the CCS, requiring CCS Users to be informed. This is particularly relevant where the consumer may no longer live at the property covered by an existing permission. For example, an ATP-led revocation indicates that the consumer may no longer occupy the verified premises, the proposed arrangements allow the CCS to issue a permission verification notification to other ATPs with active permissions that rely on that occupancy verification. The receiving ATP must verify whether its permission remains appropriate.

The notification is a trigger for verification; it does not itself revoke the other permission. This is important because a change affecting one ATP's permission should not automatically revoke all other permissions associated with the property, but nor should the CCS ignore information which may indicate that the basis on which those other permissions were established has changed.

These arrangements are particularly important where energy data requests involve delayed or scheduled processing. A permission may remain unchanged between the point an ATP establishes a request and the point at which the energy data becomes available for disclosure. SSF notifications enable ATPs and EDHs to become aware of relevant permission-state changes during that period.

4.12.3 CCS availability and data sharing during an outage

The February consultation also asked whether data sharing should be able to continue where the CCS is temporarily unavailable.

Views were mixed. Some respondents considered that service continuity should be protected where a short CCS outage occurred, particularly where the consumer had granted a longer-term permission. Others were concerned that allowing data sharing to continue without an up-to-date authorisation check could undermine consumer protection and create uncertainty about the circumstances in which an EDH remained entitled to share data.

The revised local-token validation model provides a clearer boundary. There is no separate fallback period during which energy data can be shared without a valid access token. If the CCS becomes unavailable, an ATP that already holds an unexpired access token can continue to present that token for the remainder of its normal lifetime, subject to the EDH's local validation.

Once that token expires, the ATP cannot obtain a replacement access token until the relevant CCS service becomes available again. The maximum continuation period is therefore the remaining lifetime of an access token that had already been issued when the outage began. It is not a separate 30-minute grace period and may be materially shorter.

In reaching this position RECCo has also considered experience from other regulated data-sharing ecosystems, including the historic use of separate backup arrangements in Open Banking. Due to the complexity and additional costs of setting up alternative arrangements, RECCo does not propose to introduce a separate backup authorisation mechanism at this time. Resilience is instead achieved by removing the request-time introspection dependency while retaining the requirement for a valid, normally issued access token and the security controls described earlier in this section.

RECCo considers this preferable to establishing a parallel fallback authorisation regime. It reduces the request-time central dependency compared with mandatory introspection but retains a clear rule that permission-based energy data access must be supported by a valid access token, without adding additional complexity and costs at this time.

4.13 **Permission visibility and interaction with ATP interfaces**

A further area on which respondents sought greater clarity was the relationship between the central CCS Consumer Portal and interfaces operated by ATPs.

The CCS maintains the authoritative central record of permissions granted through the service. Consumers with a CCS account can use the Consumer Portal to view and manage relevant permissions. This includes active and historic permissions and, where the consumer has been verified in relation to the relevant RMP, visibility of relevant permissions that may have been granted by another verified individual.

The property and RMP associations established through the verification and matching process enable the CCS to identify which permission records are relevant to that verified consumer. This is the technical basis for providing transparency where another verified occupier has previously established a permission relating to the same RMP. It does not give an ATP equivalent visibility of permissions belonging to other ATPs.

Where the consumer granted the permission themselves, they can revoke it through the CCS.

Where the permission was granted by another occupier, the consumer can use the separate permission-query process described above (section 3.3.5.2) rather than revoking the permission as though they were the original granter.

The Consumer Portal also enables a consumer to maintain relevant account information, including changes that may trigger further property matching. Under the CCS Arrangements Schedule, a consumer can also close their CCS account; closure results in withdrawal of active permissions associated with that account, subject to retention of information where required for legal, regulatory, security, audit, or operational purposes.

The existence of the central Consumer Portal does not prevent an ATP presenting information about permissions relating to its own service through its own consumer-facing interface.

The CCS Grant Endpoint enables an ATP to retrieve the current state of a grant associated with that ATP, including the permissions granted, relevant dates and whether the grant remains active. The information returned reflects the current enriched and validated grant held by the CCS rather than simply reproducing the ATP's original authorisation request. ATPs are also required to use this capability to reconcile their permission records with the CCS at least quarterly.

An ATP does not obtain general visibility of permissions granted to other ATPs. The ATP may present permission information relating to its own services, while the CCS Consumer Portal provides the consumer with the central view across relevant ATPs. The proposed consumer requirements reflect this boundary.

The detailed requirements governing how permission information is explained and presented to consumers are addressed through the CEGs rather than through the technical protocol itself.

This separation allows ATPs to retain ownership of their wider service and consumer relationship while maintaining a single authoritative CCS record and a common location through which consumers can review and manage their CCS permissions.

4.14 **Operational assurance, testing, and support**

The detailed technical design includes defined error and exception handling for interactions with the CCS, including unsuccessful identity or occupancy verification, unsuccessful property-to-meter-point matching, invalid or expired authorisation requests, token-validation failures, and unsuccessful delivery of lifecycle events. The applicable technical responses and error codes are defined in the CCS API Technical Specification, with retry, escalation and associated operational requirements set out in the CCS Arrangements Schedule, CCS Service Definition and will be included in the supporting CCS Error Resolution Paths document as applicable.

Operational requirements governing CCS User qualification and testing, performance assurance and monitoring, service levels and incident and support arrangements are addressed separately in the governance sections of Part A and through the proposed REC products described in Part B. They are therefore not repeated in this technical design section.

5 User Experience (UX) Design

The February 2026 Design consultation set out RECCo's proposed approach to UX design for the CCS, including the role of the UX framework and the development of CEGs. The consultation focused on how consumers should encounter CCS-governed interactions, the information they should receive before granting permission, the support required for consumers with different needs, and how the permission lifecycle should operate across grant, renew, review and revoke journeys.

Respondents agreed a key objective of CCS is to provide consumers with clear, consistent, and accessible information when they are asked to allow access to energy data. There was strong support for consumers being able to understand who is requesting access, what data is being requested, why it is needed and how long access will last. Respondents also supported the need for consumers to be able to review and revoke permissions easily and highlighted the importance of assisted or alternative journeys providing equivalent outcomes as those routes are developed.

However, responses also highlighted several important design considerations, warning that providing too much information at the point of decision could create information overload and reduce consumer engagement. Others emphasised that consumers must be given enough information to make an informed decision and that the solution should not reduce transparency in the interests of simplicity. RECCo has refined the CEGs, and the associated ATP consumer engagement requirements, to reflect a layered information approach, where essential information must be presented clearly at the point of decision, with additional detail available where consumers wish to review it.

Where an ATP requests a permission covering more than one purpose, the consumer journey must make each purpose sufficiently clear for the consumer to understand the different purposes for which access is being requested. The use of multiple permission purposes must not obscure the nature or scope of the access being authorised.

Since the consultation, RECCo has continued consumer research and UX analysis to understand consumer needs, expectations, and potential points of friction within CCS journeys, including the identity and occupancy verification steps. Following Wave 1 of research, the consumer archetypes have evolved to include more detail about participants' real experiences, including challenges with accessibility. The research programme has included two waves of qualitative consumer research and usability testing involving participants with a range of accessibility needs and levels of digital confidence. Consistent findings highlighted the importance of trust, transparency, consumer control, and verification journeys. While the findings are qualitative rather than statistically representative, they have provided a robust evidence base for the development of the CCS user journeys, CEGs and verification approach. Participants with accessibility issues have been included in the research to ensure vulnerable consumers' needs are considered from the start, even where some related adjustments may fall within post-MMP phases. RECCo has also been in dialogue with Citizens Advice and the Money & Mental Health Policy Institute to help ensure the service design reflects broader consumer perspectives and real-world challenges, and to test whether research findings align with the issues they are seeing. These findings have been used to inform the service design and support the right balance between delivering a secure, trusted service and minimising unnecessary friction for consumers. This has supported the move towards a proportionate, risk-based approach

to identity and occupancy verification, recognising that the service must provide sufficient assurance without creating avoidable barriers to participation. Research also highlighted onboarding, including account creation, identity, and verification, as the area most likely to drive consumer drop-off. These journeys have therefore been a particular focus of the UX research and design activity.

RECCo has refined the terminology used across the CCS arrangements. Our consumer research also considered the language used during consumer interactions. Research participants consistently demonstrated greater familiarity with the term "consent" when discussing the sharing of personal information. The proposed CEGs therefore allow consumer-facing journeys to continue using the term "consent", whilst the underlying governance arrangements use the term "permission". This approach is intended to maintain consistency with the regulatory framework while ensuring consumers are presented with language that is familiar, understandable and supports informed decision-making. Recognising the importance of this distinction, RECCo is seeking specific stakeholder views through a dedicated consultation question on whether consumer-facing interactions should use the term consent or permission (question 11)

The CEG document has been developed from the UX framework, consumer research, and consultation feedback, translating the consumer experience principles into practical requirements for the points at which ATP journeys interact with the CCS. The document is structured around the key permission journey stages: pre-permission, grant, renew, review and revoke. It focuses on the consumer-facing moments most critical to trust, comprehension, and controls, including how permission is explained before consumers are asked to grant access, how consumers are supported through the permission journey, and how they can review, renew, or revoke permissions across both CCS and ATP-operated interfaces. The CEGs are intended to establish clear expectations for these CCS-related interactions without prescribing ATPs' wider service journeys, branding, or customer relationships.

To support ATP development, the CEGs document will contain illustrative consumer-facing screens, demonstrating example wording and design approaches that can be used to support ATP compliance. These screens are under development and will be demonstrated via future stakeholder engagement, ahead of inclusion in the REC documentation post consultation.

Alongside the CEGs, RECCo has translated the consumer experience principles into practical requirements for the points where ATP journeys intersect with CCS around consumer-facing permission touchpoints. These cover the information presented to consumers before, during and after permission is requested or managed. These requirements have been incorporated within the REC CCS Arrangements Schedule, to establish clear governance obligations and support consistent implementation across ATPs. This responds to consultation feedback requesting clearer expectations on ATPs, while retaining flexibility for ATPs to design their wider service journeys and propositions in ways that work for their customers.

Accessibility and inclusion remain central to the proposed approach. Respondents supported the use of recognised accessibility standards, including WCAG 2.2 AA, but also emphasised that accessibility should be considered in practice and not treated as a compliance exercise. For the MMP, the CEGs therefore focus on supporting clear, accessible, and usable digital journeys, including clear language, predictable journey patterns, and accessible formats. The CEGs will be updated as assisted and/or alternative journeys are developed in future phases.

Respondents highlighted the importance of clearly explaining the boundaries of the CCS. Several respondents noted that the MMP will not provide a complete view of every organisation accessing energy data, because it will initially focus on the regulated permission arrangements within scope of the CCS. The CEGs and supporting consumer communications will explain clearly what consumers can expect to see through the CCS, the relationship between the CCS and ATP interfaces, and where data sharing may take place under other legal or regulatory arrangements outside the scope of the MMP.

RECCo considers that the CEGs and associated ATP requirements provide a proportionate approach for the CCS. Together, these provisions establish clear expectations for the consumer-facing interactions that are most important to trust, comprehension and control, while avoiding unnecessary prescription of ATP branding, customer relationships, and wider service design beyond the points where those journeys interact with the CCS.

6 Governance Design

Respondents were broadly supportive of the proposed REC drafting approach, including the suite of artefacts to be developed to incorporate the CCS within the existing REC governance framework. The primary area of concern related to the introduction of CEGs, with two respondents suggesting that this approach may be overly prescriptive and not fully aligned with the wider shift toward outcome-based regulation. We recognise the concerns raised and agree that the CEGs should support, rather than constrain, effective consumer journeys. The CEGs have therefore been developed with the aim of supporting a transparent, consistent, and GDPR-compliant experience without being overly prescriptive or limiting ATPs' own branding and customer relationships.

Taking account of the feedback received, we have progressed the code drafting activity and developed a new REC CCS Arrangements Schedule, alongside a CCS Service Definition, CCS API Technical Specification, and updates to the Energy Market Data Specification (EMDS). These products are described further in Part B of this consultation document.

A recurring theme highlighted throughout the February 2026 consultation responses was the need for REC drafting to include clear requirements on ATPs and EDHs. Respondents sought clarity on liabilities and operational interaction with the CCS, plus EDH requirements for permission validation and data provision. We intend to utilise the existing Non-Party REC Service User Access Agreement which provides the legal framework for inclusion of Non-REC Parties into the REC arrangements. This agreement includes provisions relating to liabilities and data protection. It also allows for third party rights, enabling signatories to manage disputes directly. Under this approach, both ATPs and EDHs will be required to comply with the CCS Arrangements Schedule. This will capture all CCS specific elements of the solution, including ATP and EDH requirements, operational interactions with the CCS and the requirement to exchange data in accordance with the CCS API technical specification.

Other comments relating to liabilities focused on how the CCS arrangements interact with existing legal and regulatory obligations, including where organisations act as data controllers or data processors under GDPR. RECCo recognises that the CCS forms part of a wider regulatory landscape: it complements, and does not remove or replace, obligations arising under GDPR, Energy Codes, Energy Licences, or other applicable legal frameworks.

The REC drafting described in Part B includes the creation of a new CCS Arrangements Schedule setting out the rights and obligations of both ATPs and EDHs participating in the CCS Arrangements. The drafting establishes a clear distinction between RECCo's responsibilities for the provision, operation and governance of the CCS and the responsibilities of individual CCS Users. RECCo is responsible for procuring and overseeing the CCS service, managing participant qualification arrangements, and maintaining the CCS governance framework, while ATPs and EDHs remain responsible for complying with their own legal, regulatory, security and data management obligations. The proposed drafting also clarifies that RECCo does not warrant the accuracy or completeness of energy data provided by EDHs and that responsibility for determining the lawful basis for processing personal data remains with the relevant participant. ATPs and EDHs are therefore accountable for ensuring that their use, sharing, retention, and protection of data complies with applicable legal and regulatory requirements, whilst the CCS provides the framework through which permissions are obtained, managed, and evidenced.

6.1 Funding

A key component of the future governance framework is the funding mechanism used to recover central costs associated with the ongoing management and operation of the CCS arrangements under the REC. In the consultation document, RECCo proposed that core CCS costs should be recovered from Energy Suppliers through the existing RECCo cost

recovery arrangements for the initial period after MMP go-live. This approach is intended to support voluntary uptake of the CCS and avoid placing disproportionate costs on early adopters.

Consultation responses were mixed, with several respondents emphasising the importance of transparent and proportionate costs. In relation to transparency, the REC sets out the annual budget consultation and approval process, providing stakeholders with visibility of RECCo costs and an opportunity for ongoing scrutiny and challenge. Any specific charges associated with the CCS will also be subject to the established REC Charging Methodology and Charging Statement arrangements.

Several suppliers raised concerns regarding the proposal to recover central costs from suppliers and effectively mutualise these costs across the market. We continue to consider that recovery of core CCS costs through the RECCo cost recovery arrangements is the most appropriate during the initial period after MMP. This approach supports early market adoption, avoids creating barriers for initial CCS Users and reflects the role of CCS as a cross-market enabling service intended to support wider smart data and digitalisation objectives.

We recognise the concerns raised regarding the increasing number of industry initiatives funded through supplier charges, which may ultimately flow through to consumer bills. RECCo remains a cost conscious organisation, following an annual transparent budgeting cycle. We have also tested our costs against Open Banking benchmarks, the closest comparator, which wasn't expected to exceed £20m at 2016 prices. The current CCS budget is at £6.2m for implementation.

We continue to believe that the individual costs of assurance activities, including accreditation, should be recoverable from individual CCS Users. The proposed amendments to the REC Charging Methodology provide for applicable CCS User charges to be specified in the REC Charging Statement. Estimated costs have been included within table 4 in section 8.6, recognising that these remain subject to ongoing commercial discussions. The specific costs applicable to CCS User accreditation will be set out in the 2027/28 REC Charging Statement. We recognise the concerns raised through the consultation regarding potential duplication and overlap in accreditation costs between the REC and SEC.

We recognise that the appropriate cost recovery approach may evolve alongside CCS adoption and market maturity, and a number of respondents requested further clarity regarding how the charging arrangements may be reviewed in future. The REC Charging Methodology provides the framework within which RECCo may apply specific charges to REC Service Users or other relevant parties, including charges that are dependent on usage. The applicable charges are set out in the REC Charging Statement, which is published before the start of each Financial Year and may also be revised from time to time.

RECCo therefore proposes to keep the CCS charging arrangements under review as adoption of the service develops, including whether wider user-pays or transactional charging may become appropriate. Where such a change can be accommodated within the REC Charging Methodology, it could be implemented through an update to the REC Charging Statement. A REC Change would only be required where the proposed funding approach required an amendment to the Charging Methodology or other REC provisions.

6.2 Change management

Respondents expressed broad support for applying the existing REC change management arrangements to the CCS. Many noted that using the well-established REC change management arrangements would avoid the need to create separate bespoke frameworks and would ensure that future changes are subject to thorough, transparent assessment, including the ability to designate changes as urgent status where appropriate. This approach was seen as promoting consistency, and minimising cost and disruption.

While supporting the overall approach, some respondents emphasised the importance of maintaining efficiency, to enable the CCS to evolve at pace, particularly given the expected rate of technology and user driven change. RECCo understands

the need for efficiency and is committed to ensuring the REC change process strikes an appropriate balance between industry capacity and the need for timely delivery. The framework already provides flexibility to utilise expedited routes where appropriate. We also note that, as part of the Energy Code Reform programme, enhancements are being made to the REC (and other codes) change processes to improve efficiency and strengthen prioritisation arrangements.

A minority of respondents raised concerns with the using the existing change process:

- One respondent expressed concern that future changes raised by parties could erode the data-sharing safeguards and risk mitigations underpinning the CCS. RECCo acknowledges this concern, however we believe there are sufficient safeguards within the REC to prevent this. Specifically, the REC objectives are explicitly linked to consumer outcomes, and we would not expect a change to be approved that undermines consumer protections or conflicts with the legal position established through the CCS delivery project. All legal or ICO advice relating to the CCS will be retained and considered when assessing future change, with further advice sought as required. Additionally, any change which materially impact consumers would be subject to Ofgem decision.
- Another respondent questioned whether the existing change process could accommodate significant future developments, such as the inclusion of suppliers within the CCS. RECCo considers that the REC change process is sufficiently robust to manage any significant changes to the CCS that may arise in the future. The CCS MMP establishes reusable permission, trust, authorisation, governance, and assurance capabilities so that additional energy datasets, participants and consumer journeys can be introduced without a fundamental redesign of the core service. The wider energy code governance arrangements also enable Ofgem to set strategic priorities for the REC and enable Ofgem and DESNZ to direct changes to energy codes where required. Across responses, stakeholders highlighted the importance of ensuring Non-REC Parties are fully included within the change governance process and that a clear engagement strategy is in place. RECCo has raised REC Issue I0318⁹ to provide greater transparency and will continue to work with the change team to ensure Non-REC Parties are fully engaged in the development and ongoing governance of the CCS. Under current REC arrangements Non-Party REC Service Users are already able to fully participate in all aspects of the change process, including impact assessment and working group involvement. Under the proposed Energy Code Reform arrangements, a Stakeholder Advisory Forum (SAF) will be established to support RECCo (as the licensed Code Manager) decision making. We expect SAF members to act impartially, ensuring that the interests and impacts on all affected stakeholders are fully and appropriately considered throughout the development of any change.

In conclusion, RECCo will proceed on the basis that a bespoke change process is not required for the CCS and changes to the REC-governed CCS arrangements will be managed through the REC Change Process. Changes required to deliver the future CCS roadmap will therefore be progressed through that framework, taking account of applicable statutory requirements, regulatory decisions and policy direction.

6.3 Assurance

Respondents expressed broad support for applying the existing REC assurance arrangements to the CCS. Stakeholders noted that assurance should continue to be risk-based and proportionate, with a clear focus on maintaining consumer trust, ensuring robust data protection, and safeguarding operational integrity. Respondents also highlighted that the current REC assurance process is well structured, providing appropriate pathways for addressing non-compliance, including escalation to the REC Performance Assurance Board (PAB) and, where necessary, recommending removal of accreditation.

⁹ I0318 - Introduction of Consumer Consent Solution

Some respondents reiterated concerns regarding potential duplication between REC and SEC assurance regimes. These points are addressed in more detail within the accreditation section below. Other respondents observed that removal of accreditation would require careful consideration due to the potential impact on consumer services. RECCo recognises the significance of this risk; the removal of accreditation, and the resulting cessation of data sharing, would represent a worst-case scenario. We therefore expect that lower-level performance assurance techniques would be deployed in the first instance to address performance issues.

Several specific considerations were raised for incorporation into the detailed assurance design. These will inform the development of the lower-level assurance thresholds:

- The need to consider the diversity of operating models when setting baselines and thresholds, recognising that powered self-service platform will have different usage patterns (higher volume, more automated, spikier traffic) compared with traditional broker models;
- A suggestion to consider the principles set out in the TPI Code of Practice as a potential framework for ATP assurance and to take account of cross sector risk drivers, particularly those from the financial markets;
- Consideration of additional levers to incentivise compliance, without relying on removal of CCS accreditation, which will be especially important while CCS participation remains voluntary; and
- Recognition that EDHs will place reliance on the CCS to validate permission prior to sharing energy data, meaning that high levels of operational resilience and availability are essential and should be monitored on an ongoing basis.

Respondents also emphasised the need for wider cross code collaboration, to ensure assurance activities are co-ordinated across code managers, reducing regulatory burden and avoiding duplication. By integrating CCS assurance activities within the broader REC assurance framework, the performance assurance team will be able to leverage this existing work and extend to cover any new CCS specific assurance requirements.

In conclusion, RECCo will proceed on the basis that CCS assurance activities will be incorporated within the existing REC performance assurance framework, utilising established performance assurance techniques. Development of detailed CCS assurance activities has been included within the draft 2026/27 Performance Assurance Operating Plan (effective from September 2026). RECCo will work with the performance assurance team to develop the detailed monitoring and reporting approach. High-level details of the proposed model are set out in sections 8.6-8.8 of this consultation to support further industry feedback.

6.4 Accreditation

Respondents who provided feedback, were generally supportive of the proposed accreditation approach, utilising the existing risk-based qualification process for Non-Party REC Service User. Respondents recognised the benefits of a clear and proportionate accreditation process, providing assurance that CCS Users operate in a way that protects consumer data and maintains confidence in the CCS framework.

The primary concern raised related to the potential overlap between REC and SEC arrangements. Since issuing the February 2026 consultation, RECCo has worked closely with SECCo to define and agree the boundaries between the SEC and REC assurance activities, with the aim of establishing a complementary assurance framework that recognises existing SEC and REC assurance processes. This approach seeks to avoid duplication while maintaining appropriate levels of oversight. This joint work has considered both information security and data privacy considerations.

As illustrated in the figure 8 below, we consider there to be a clear separation between the scope of assurance activities under the SEC and the REC. SEC security and privacy assessments focus on evaluating the security of organisations accessing smart metering data via DCC, and on confirming the approach used to obtain permission to access data is consistent with the Privacy Controls Framework. This includes the secure transmission and reception of messages to and from the smart meter, with a particular focus on the systems used to communicate with DCC services.

Conversely, the REC ISDP assessments focus on ensuring that organisations have appropriate controls in place to prevent data loss, misuse, or unauthorised access. These assessments set requirements supporting safe data access, including data handling, data governance, and operational controls. The REC assessment aims to evaluate compliance across data access arrangements specified under the SEC, REC, and BSC, enabling organisations to undergo a single assessment where they wish to access data under multiple frameworks.

The REC ISDP assessment is intended to provide a baseline level of assessment that EDHs can rely on when sharing data with accredited ATPs.

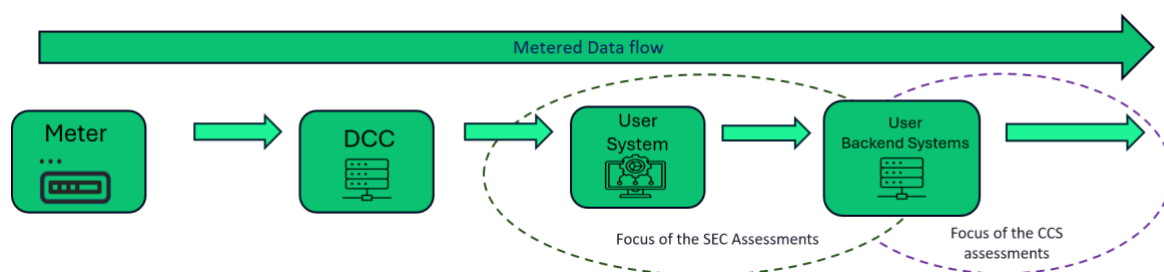


Figure 8

Respondents also highlighted the need to consider interactions between the CCS accreditation approach and other smart data initiatives, such as the DSI and SDR. These interactions have been considered through the Digitalisation Delivery Group, to support a streamlined and co-ordinated accreditation model, with RECCo leading on data privacy elements.

We have also assessed the potential interaction between REC accreditation and the governance arrangements being developed to support the new Load Control Licence. In this context, we are seeking to align with the proposed requirements wherever possible to minimise duplication for market participants and reduce unnecessary administrative burden. For example, where participants are already required to obtain and maintain recognised assurance certifications, such as Cyber Essentials Plus (CE+) we will seek to ensure these can be relied upon across multiple regulatory and governance frameworks where appropriate.

Our understanding is that the Load Control Licence does not include specific assessment or audit requirements relating to data protection compliance, instead relying on the statutory obligations under GDPR and the Data Protection Act 2018. We therefore do not consider there to be duplication between CCS and Load Control Licence requirements in this area. We will continue to engage with Ofgem and DESNZ as proposals develop to ensure there is a clear delineation of scope and that any overlapping assurance requirements are managed in a proportionate and coordinated manner.

In conclusion, RECCo continues to believe that access to CCS should be controlled to protect consumers from unauthorised access to their personal data, and that leveraging the existing REC approach to service user qualification is appropriate.

With regards to the specific question on setting a minimum standard, requiring all CCS users to hold CE+ certification, there was strong support from respondents. A minority of respondents suggested alternative approaches:

- One respondent proposed that Cyber Essentials, rather than CE+, would be a more proportionate requirement. RECCo does not consider Cyber Essentials alone to provide a sufficient minimum baseline because it is based on a self-assessment of the organisation's controls and does not include the independent technical verification provided through CE+. Having considered this alongside the wider feedback, RECCo continues to consider CE+ the most appropriate minimum standard because it provides independent verification that the required controls are operating effectively, including through external vulnerability assessment and internal testing.
- Another respondent suggested that ISO 27001 would be a more suitable minimum standard. RECCo continues to consider Cyber Essentials Plus (CE+) to be the appropriate minimum cyber-security baseline for CCS Users because it provides independently validated technical assurance in a proportionate and cost-effective manner. However, RECCo recognises that some organisations already hold appropriately scoped ISO 27001 certification covering the systems, services, and operational activities relevant to their participation in CCS. Where such certification provides equivalent assurance for the relevant CCS scope, RECCo may accept it in place of CE+, subject to the requirements of the qualification and assurance process.
- Some respondents re-iterated concerns regarding potential duplication with SEC assurance processes and suggested that RECCo should rely on existing SEC Other User accreditations. As set out above, the scope of SEC accreditation is specific to accessing smart metering data via DCC systems and does not cover broader controls assessed under CE+.

CE+ will form the minimum cyber-security baseline for organisations qualifying as CCS Users, including ATPs and EDHs. Organisations that already hold appropriately scoped ISO 27001 certification covering the systems, services, and operational activities relevant to their CCS participation may be permitted to rely on that certification as an alternative where RECCo is satisfied that it provides equivalent assurance. This will not replace the wider risk-based ISDP assessment. The ISDP assessment will consider the additional risks associated with an applicant's proposed use of the CCS and the data access it enables, including areas such as data protection, governance, third-party oversight, data minimisation, and controls intended to prevent inappropriate use of data.

The wider regulatory direction of travel also supports the use of an independently assured cyber-security baseline. Since the February 2026 consultation, DESNZ and Ofgem have published their response to the *Whole energy cyber resilience requirements: reshaping cyber regulation in downstream gas and electricity* consultation¹⁰. The response states that they intend to use the Cyber Essentials scheme as the foundation for developing baseline cyber-resilience requirements for all Ofgem licensees and that CE+ is intended to be used as that independently assured baseline. The detailed requirements and implementation arrangements have not yet been finalised and will be subject to further development and consultation led by Ofgem.

RECCo considers CE+ to be the appropriate and proportionate minimum cyber-security baseline for CCS based on the risks associated with participation in the service and the consultation feedback received. Where an organisation already holds appropriately scoped ISO 27001 certification, RECCo may accept that certification as providing equivalent assurance for the purposes of qualification. The subsequent government position provides additional confidence that this approach is consistent with the wider regulatory direction of travel, while also recognising the importance of avoiding duplication with existing assurance requirements.

¹⁰ [Whole energy cyber resilience requirements: reshaping cyber regulation in downstream gas and electricity - GOV.UK](https://www.gov.uk/government/consultations/whole-energy-cyber-resilience-requirements-reshaping-cyber-regulation-in-downstream-gas-and-electricity)

We recognise that this CCS minimum certification requirement does not currently apply across other REC Services. RECCo intends to consider separately whether any broader changes to REC qualification requirements may be appropriate, taking account of the development of the wider regulatory framework.

PART B - REC Drafting Proposals

7 Summary of REC Drafting

Consultation Questions

Q1. Do you agree the products identified in figure 9 and this Part B, represent the full scope of REC drafting required to deliver CCS MMP? If not, please provide details of other products you believe should be included in the scope of the REC Change Proposal.

As highlighted in the February 2026 consultation, RECCo has developed the governance arrangements for the CCS by extending existing REC governance arrangements wherever appropriate, rather than creating a standalone governance framework. This approach maximises consistency with existing REC Services, minimises unnecessary complexity, reduces implementation costs and enables the CCS to benefit from established REC governance, assurance, and change management processes.

The REC is a multi-party industry code governing key aspects of the retail energy market, including the switching of energy suppliers, the provision of metering services, the exchange of data between market participants and consumer protection processes. It establishes standards for a range of consumer and market data, including metering technical details, address data, and tariff information. These standards are supported by technical services such as the Central Switching Service, which manages supplier registration, and the Enquiry Services, which provide wider access to market data. Market participants, including energy suppliers, network parties and metering equipment managers, are required to accede to the REC and comply with the provisions relevant to their respective market roles.

Existing REC arrangements also allow organisations that are not REC Parties to access REC Services, including the Gas and Electricity Enquiry Services. These organisations participate as Non-Party REC Service Users and sign an Access Agreement that binds them to the relevant REC provisions on the same basis as REC Parties. This enables them to use the relevant REC Services without having to accede to the REC itself.

ATPs and EDHs will not be required to become REC Parties to use the CCS. Those that are not already REC Parties will participate as Non-Party REC Service Users and will be bound by the relevant provisions of the REC Main Body and REC Schedules through an Access Agreement. The term “CCS Users” is used collectively for ATPs and EDHs. The proposed CCS drafting included in this consultation document and its accompanying annexes should be read on the basis that the relevant provisions apply equally to CCS Users, whether they participate as REC Parties or Non-Party REC Service Users.

Figure 9 below provides a high-level summary of the REC products that will form part of the CCS REC drafting. These products have been developed from the detailed CCS design. Key information from that design is reflected in Part A, with the business process diagrams published alongside this consultation and selected machine-readable technical definitions made available through the CCS section of the RECCo Developer Portal. The remaining sections of Part B explain how the content of the draft REC products included in the accompanying appendices has been developed.

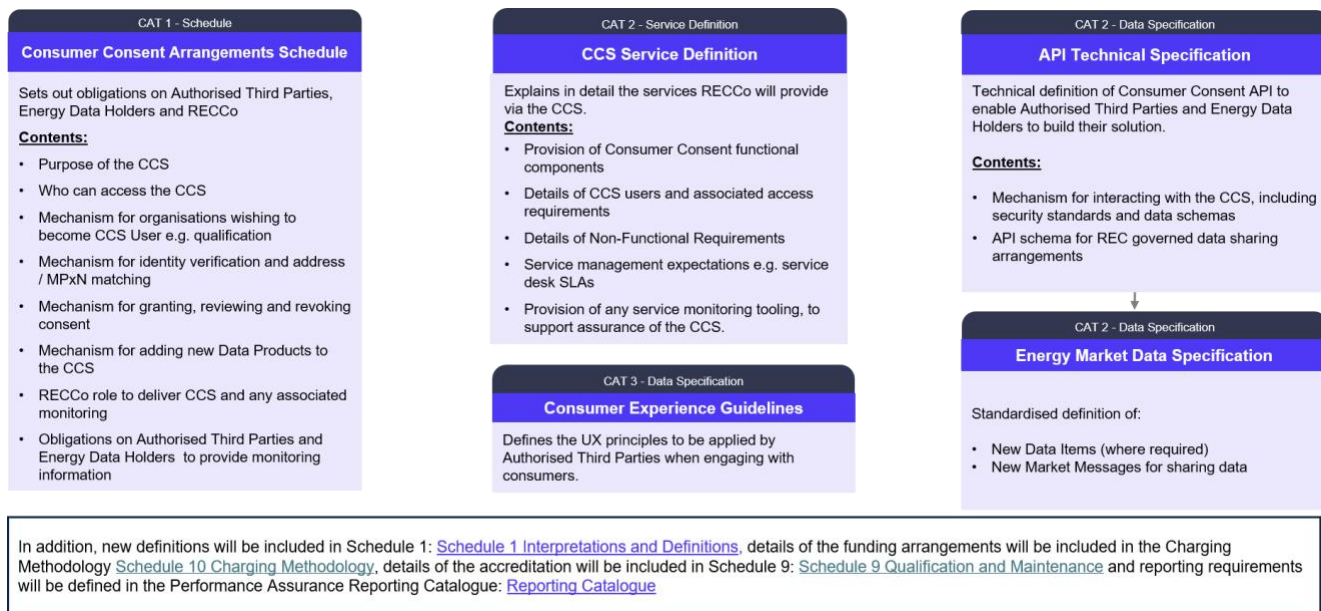


Figure 9

The rights and obligations of ATPs and EDHs will be captured by expanding the existing REC baseline to include a new operational REC Schedule, the CCS Arrangements Schedule, and by amending other existing REC Schedules where references to the CCS and CCS Users are required. At the centre of the CCS governance framework, the new Schedule will establish the enduring governance arrangements for the CCS. It will define the rights and obligations applying to CCS Users, together with the operational processes for becoming a CCS User, obtaining and managing permission, and interacting with the CCS.

Alongside the Category 1 CCS Arrangements Schedule, a complementary suite of Category 2 REC products will set out the detailed service, technical and data requirements needed to operate the CCS. These will include the CCS Service Definition and CCS API Technical Specification, together with amendments to existing technical REC products, including the relevant EMDS Data Item and Market Message Catalogues. The Category 3 Consumer Experience Guidelines will provide supporting guidance on the consumer experience. Allocating content to the product most appropriate for its purpose provides a clear separation between enduring obligations, service and technical requirements, reference data, and supporting guidance.

7.1 Supporting Category 3 documents

In addition to the REC products included in this consultation, further Category 3 documents will need to be developed or updated to support the implementation and ongoing operation of the CCS.

Category 3 documents provide operational information, detailed supporting material or guidance. They do not create obligations for REC Parties or REC Service Users in their own right. The applicable obligations and requirements will instead be established through the relevant Category 1 and Category 2 REC documents.

These additional supporting documents will be developed following this consultation, taking account of the final CCS design, and resulting REC changes. Their development and publication will form part of the CCS implementation and readiness activity, so that prospective CCS Users have the information they need to prepare for onboarding and operation ahead of go-live.

The principal documents expected to be developed or updated include:

- onboarding and assurance material, including the REC Entry Assessment Forms, REC Entry Assessment Information Pack, Service User Categorisation and Assessment Document, and Performance Assurance Methodology and Techniques;
- CCS Error Resolution Paths, providing practical information to support the identification, investigation, and resolution of CCS errors;
- permission-management material, including the Permission Purpose Catalogue, which will provide the authoritative list of permission purposes, and the supporting Permission Purpose Change Process;
- guidance relating to identity and occupancy verification and the use of the CCS and CCS Portals; and
- the REC Charging Statement and any other supporting documents that require amendment to reflect the introduction of the CCS.

This is not intended to be an exhaustive list, and further supporting material may be identified as the detailed implementation arrangements are developed. Responses to this consultation will inform the development of relevant Category 3 documents, particularly the initial Permission Purpose Catalogue. However, the additional Category 3 documents identified above are not themselves included in the consultation drafting pack and will be developed through the applicable governance and approval arrangements during implementation.

7.2 Interactions with Tariff Interoperability

The drafting described within this consultation contains provisions that support the delivery of Tariff Interoperability and should be considered alongside the Tariff Interoperability Phase 1b consultation. Tariff Interoperability is a DESNZ-led initiative under the Smart Secure Electricity Systems (SSES) Programme that aims to enable access to tariff information through a standardised and interoperable framework.

The associated REC changes are being implemented under DESNZ direction, rather than through the standard REC change process, the relevant provisions have been split across two consultations:

- The Tariff Interoperability Phase 1b consultation will propose amendments to the Tariff Interoperability Arrangements Schedule (Schedule 35). These include requirements for the sharing of account-specific tariff information, and registration obligations for organisations seeking access to tariff data. They also require Tariff Interoperability Energy Suppliers and Registered Tariff Interoperability Users to become CCS Users in accordance with the CCS arrangements. That consultation also updates the Tariff Interoperability API Technical Specification, and the associated EMDS, to support bilateral messaging between those two parties. This covers the exchange of account-specific tariff information and notifications about changes to that information.
- For account-specific tariff information, the supplier holds the relevant account and tariff information and performs the account and metering-point matching. This route is separate from MMP consumption-data provision and does not mean that CCS has implemented gas consumption-data provision or a gas MPRN-matching capability.
- This CCS consultation includes the CCS Arrangements Schedule, which sets out requirements applicable to all CCS Users, including Tariff Interoperability Energy Suppliers and Registered Tariff Interoperability Users. For Tariff Interoperability Energy Suppliers, this includes a requirement to develop the capability needed to undertake CCS Account Holder Verification. This will require the supplier to receive an account-holder verification request from the CCS, support the consumer's redirection to and authentication through the supplier's interface, confirm whether the individual is the Account Holder for the relevant RMP or RMPs, and securely return the verification outcome and RMP information to the CCS. The detailed end-to-end process is

set out in the CCS Arrangements Schedule, with the associated technical and message requirements set out in the CCS API Technical Specification and Data Specification.

As described in the sections 8.5 and 8.11.3, this CCS consultation also includes two targeted amendments to support the Tariff Interoperability delivery:

- updates to the Access Agreement in REC Schedule 9 to explicitly recognise Registered Tariff Interoperability Users as a category of CCS User; and
- updates to the Standards Definition Document which explicitly identify Registered Tariff Interoperability Users as a new data service type.

Organisations reviewing these proposals from a Tariff Interoperability perspective should ensure that feedback is submitted through the appropriate consultation to enable review by the relevant delivery teams and governance bodies.

8 REC drafting

8.1 Main Body and Operational Schedules

Q2. Do you agree with RECCo's assessment that no amendments to the REC Main Body are required to deliver the CCS MMP? If not, please identify the relevant changes you consider necessary and outline your rationale.

Q3. Do you have any comments on the content of the CCS Arrangements Schedule? If yes, please provide details, highlighting any specific clauses against which the comment relates and proposed drafting suggestions.

Q4. Do you have any comments on the redlined changes to REC Schedule 10 'Charging Methodology'? If yes, please provide details, highlighting any specific clauses against which the comment relates and proposed drafting suggestions.

Q5. Do you have any comments on the redlined changes to REC Schedule 9 'Qualification and Maintenance'? If yes, please provide details, highlighting any specific clauses against which the comment relates and proposed drafting suggestions.

Q6. Do you agree that the ISDP approach, including the draft questions and the considerations used to assess individual risk levels, provides an appropriate level of assurance to mitigate the risk of data protection and/or information security breaches? If not, please explain any gaps or changes you consider necessary, including whether assurance requirements should be strengthened, reduced, or differentiated.

Q7. Do you agree with the monitoring and reporting approach and that this should be reflected in a future change to the Performance Assurance Reporting Catalogue?

Q8. Do you have any comments on the redlined changes to the EES Service Definitions? If yes, please provide details, highlighting any specific clauses against which the comment relates and proposed drafting suggestions.

Q9. To support development of the initial Permission Purpose Catalogue, please provide (on a confidential basis if necessary) a list of the permission purposes currently used, or expected to be used, within your organisation for accessing or sharing consumer energy data.

For each permission purpose, please provide:

- the purpose or activity for which the data is accessed or shared;
- the party, role or type or organisation that requires access to, or receives, the data;

- a high level overview of the data required to support that purpose;
- a brief explanation of why that data is required for the stated purpose;
- where relevant, the frequency or duration of access associated with the purpose; and
- where you expect more than one permission purpose to form part of the same consumer permission, the purposes that you would expect to be combined.

This information will be used by RECCo to develop the initial draft Permission Purpose Catalogue and will not be published in a manner that identifies individual organisations without their agreement.

This section explains how the proposed REC drafting has been structured to implement the CCS governance framework and identifies the changes proposed to existing REC products. The full CCS Arrangements Schedule is included alongside this consultation document as part of Annex E, with redlined versions of existing REC Schedules. For ease of reading, new definitions have been included at the start of the CCS Arrangements Schedule. Amended definitions are included in a redlined version of Schedule 1 'Interpretations and Definitions'. All new definitions will be transferred into the existing Schedule 1 during the implementation of REC Change Proposal R0318.

8.2 Main Body

The REC itself comprises 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.

The Non-Party REC Service User Access Agreement binds REC Service Users to the relevant provisions within the REC, including elements on the Main Body relating to confidentiality, data protection, liabilities and includes provisions enabling the agreement to be terminated where obligations are breached. On the basis we are proposing to extend the scope of the existing Access Agreement to include access to the CCS, we have conducted a full review of the REC Main Body and do not believe any changes are required to the existing provisions to support the implementation of CCS. Where obligations are specific to CCS operation they have instead been included within the CCS Arrangements Schedule, maintaining consistency with the wider REC drafting approach of placing operational obligations within schedules rather than the Main Body.

8.3 CCS Arrangements Schedule

The CCS Arrangements Schedule provides a single, central point of governance for organisations seeking to access data via the CCS. It defines the rights and obligations of CCS Users, as well as the operational processes governing how CCS Users interact with the CCS and manage consumer permissions. The Schedule also reflects requirements on RECCo for the provision of the CCS and associated IDV services. For CCS Users who are not REC Parties, compliance with the Schedule is mandated through the Access Agreement. In turn, the Schedule requires CCS Users to adhere to relevant technical documentation, such as the CCS API Technical Specification.

The content of the Schedule has been developed based on the high-level design, governance and design principles outlined in Part A of this document, along with the input from Ofgem, DESNZ and RECCo's legal advisors. A summary of the CCS Arrangements Schedule is provided in table 3 below, with full drafting included in Annex E. The draft schedule includes key time-based provisions in square brackets, with proposed values based on working group discussion. Respondents are invited to highlight any concerns in relation to these values within their response to question 3.

Section of Schedule	Description
Introduction	Provides a high-level overview of the CCS arrangements and references to other REC products that should be read alongside the schedule. The introduction also includes a transitional provision applicable to Tariff Interoperability Energy Suppliers (i.e. those suppliers required to share Account Specific Tariff Information in accordance with relevant licence conditions). This provision brings Tariff Interoperability Energy Suppliers within the scope of the CCS arrangements to support design, build and test activities, in advance of the implementation of Tariff Interoperability Phase 1b.
Provision of CCS	Defines RECCo's obligations in relation to the governance and provision of the CCS, including the requirement to deliver the service. It also specifies that the CCS must be provided in accordance with the CCS Service Definition. This section further clarifies that RECCo is not responsible for the accuracy or completeness of data shared by the relevant EDH or the use of that data by ATPs. In addition, it recognises that ATPs may be required to enter into a bespoke data sharing agreement with an EDH, which falls outside the scope of the Consumer Consent Service Arrangements.
Becoming a CCS User	Defines the end-to-end process that ATPs and EDHs must follow in order to onboard to the CCS. This includes: • initial application and organisational verification; • qualification as a CCS User, including signing an Access Agreement and completing external CCS Testing; • provision of security certificates to facilitate data exchange; and • registration of required streams to send or receive event notifications in accordance with the CCS Shared Signals Framework.
CCS Directory	Explains the functional component of the CCS used to record CCS User details and catalogue the data products made available by EDHs. This section also sets out the mechanisms for updating such information via the CCS User Portal and applicable CCS APIs.
Suspension or Revocation of CCS User Access	Explains the role of the REC Performance Assurance Board in overseeing CCS User compliance with the terms of their Access Agreement, including its authority to suspend or revoke access to the CCS where appropriate. The Schedule reflects the principle that suspension or revocation represents a proportionate enforcement measure where other performance assurance techniques have not resolved the issue or where immediate action is required to protect the integrity or security of the CCS.

	This section also sets out the circumstances in which security certificates may be revoked by the CCS Provider in order to mitigate risks associated with security breaches.
External CCS Testing	Provides additional detail to support the CCS testing arrangements. This includes obligations on applicants to ensure that testing is completed in an efficient and timely manner, demonstrating that systems can successfully integrate with the CCS whilst maintaining compliance with the required security controls, without compromising the security of the CCS.
General CCS User Requirements	Defines the general requirements applicable to all CCS Users, including the requirement to be qualified and maintain qualification, and to ensure that all data exchanges comply with the CCS API Technical Specification. This section also: • sets out the security obligations of CCS Users, aimed at mitigating the risk of security or data breaches that could impact the CCS, other CCS Users, or consumers; • sets out technical requirements to enable robust, secure integration with CCS and data sharing between CCS Users in accordance with the FAPI 2.0 Security Profile and the CCS API Technical Specification. • defines non-functional requirements applicable to CCS Users, including the timing requirements for caching signing key material, and compliance with the prescribed retry strategy; and • confirms the obligations on CCS Users to submit performance data upon request as part of REC monitoring and reporting activities.
Specific ATP Requirements	Confirms each ATP's obligations under the CCS arrangements, including adherence to the ATP consumer experience requirements, the determination of the lawful basis on which energy data can be accessed, the circumstances in which the CCS must be used to obtain consumer permission prior to data access and requirements associated with direct consumer permission revocation. This section also requires ATPs to ensure that their internal permission records are aligned with CCS data, including undertaking regular reconciliation activities.
Specific EDH Requirements	Confirms each EDH's obligations under the CCS arrangements, including responsibility for determining whether permission via the CCS is required under any applicable Energy Code or Energy Licence prior to the release of energy data to an ATP. This section also requires EDHs to locally validate the CCS-issued access token presented by the ATP, and that the energy data and data period requested are authorised by the access token, before sharing energy data. Where an EDH undertakes future or scheduled activity without an access token being presented at that point, it must monitor applicable permission revocation notifications.

Addition of new Data Products	Defines the approach for adding new data products into the CCS Directory. This section focuses on the governance process required to determine whether changes to the CCS arrangements are necessary to accommodate and recognise the new data.
Governance of permission purposes	Defines the governance arrangements for establishing, maintaining, and publishing the Permission Purpose Catalogue together with the associated Permission Purpose Change Process. The catalogue provides the authoritative list of valid permission purposes, one or more of which may be referenced within an individual CCS permission record. The section also defines the governance route for introducing new permission purposes, distinguishing between changes that can be progressed through the operational Permission Purpose Change Process and those requiring progression through the REC Change Process.
Use of the CCS Logo	Defines the rules governing the use of the CCS Logo. This drafting is based on the approach established for the CoMCoP Logo which was recently introduced into the REC through Change Proposal R0307 'Release and Licensing of the CoMCoP Logo for Accredited Parties' ¹¹ .
CCS Identity Verification	Explains the processes for establishing the identity and relevant relationship to the premises or account required for the applicable permission journey, together with property-to-meter-point matching. For domestic half-hourly metered data, identity and current occupancy are treated as separate assurance outcomes under a centrally governed, outcome-based, and risk-based verification approach. For Tariff Interoperability, the Schedule also covers account-holder verification by the relevant energy supplier. Where required, verified property information is subsequently used with the relevant Enquiry Service to identify the associated metering point or points.
Operational Processes	Defines the end-to-end business processes covering the granting, review, and revocation of permission. These processes take the standard format used across other REC Schedules, with interface tables setting out the steps, triggers, actors, and associated market messages. Once implemented into the digital REC, references to market messages will hyperlink directly to the corresponding message definitions held in the EMDS. These interface tables have been developed based on the baselined business process diagrams, in Annex D Following implementation of the CCS, the diagrams will be published and maintained as part of the suite of CCS REC Products.
Appendix 1 ATP Consumer Engagement Requirements	ATP requirements are set out in a tabular format, as a practical compliance checklist. The requirements distinguish between mandatory requirements ("Must"), good practice recommendations ("Should"), and optional approaches ("May"). ATPs will be required to

¹¹ [R0307 - Release and Licensing of the CoMCoP Logo for Accredited Parties](#)

	confirm compliance with the applicable mandatory requirements as part of their annual compliance statement, under the maintenance of qualification arrangements.
--	--

Table 3

The CCS Arrangements Schedule establishes the governance arrangements for the Permission Purpose Catalogue and the associated Permission Purpose Change Process. Together these documents provide the operational framework for establishing, maintaining, and publishing permission purposes under the REC. This consultation seeks views on the proposed governance framework only. The initial Permission Purpose Catalogue will be developed separately following this consultation and will be subject to its own industry engagement and consultation prior to publication.

The Permission Purpose Catalogue will be established, maintained, and published by RECCo as a REC Category 3 Product. Each Catalogue entry will define a permission purpose together with the associated information required for consistent implementation by CCS Users, including a unique identifier, description, and applicability

RECCo will assess requests for new permission purposes in accordance with the published Permission Purpose Change Process. The assessment will determine whether the proposal can be implemented through operational governance or whether it should instead progress through the REC Change Process.

Where a proposal introduces a new permission purpose without creating implementation impacts for existing CCS Users, it is proposed that the change may be progressed through the Permission Purpose Change Process. Where a proposal would amend or remove an existing permission purpose, introduce wider implementation impacts, or otherwise constitute a breaking change, the proposal will continue to be progressed through the REC Change Process.

This approach is intended to support timely introduction of new consumer propositions whilst ensuring that changes affecting existing market participants remain subject to the appropriate level of REC governance. It also enables the Permission Purpose Catalogue to evolve over time through a proportionate governance process, while ensuring that the initial catalogue is developed collaboratively with industry and consulted on before implementation.

8.4 Schedule 10 Charging Methodology

As set out in Part A above, CCS funding will be based on a hybrid model, whereby core CCS operational costs are recovered centrally, while qualification and enforcement related activities are recovered from individual CCS Users. As with other REC Services, the high-level funding methodology is captured within Schedule 10, with the detailed charges set annually through the Charging Statement published by RECCo. The approach for CCS is reflected within a new section of the Charging Methodology (see Annex E).

The Charging Methodology establishes how costs of operating and maintaining REC Services are calculated, allocated, and recovered fairly and transparently from Parties. It points to the lower-level Charging Statement, which sets out the specific charges payable by Parties, applying the Charging Methodology to determine how costs are allocated and recovered in a given charging period.

It is not currently possible to confirm the final costs associated with CCS qualification activities; however, indicative costs have been provided in table 4 in section 8.6 below. Following this consultation, RECCo will finalise the qualification requirements and confirm the costs for inclusion in the 2027/28 Charging Statement. As a Category 3 REC product, the Charging Statement is updated and published through the standard annual governance process; its publication is not specific to the CCS.

8.5 Schedule 9 Qualification and Maintenance

The REC Qualification and Maintenance Schedule sets out the criteria that must be met by organisations seeking to become, or remain, qualified to access one or more REC Services. The provisions are designed to provide assurance that an applicant's systems and processes are fit for purpose.

The Schedule defines requirements both for market participants who are seeking to qualify in a particular market role (e.g. energy supplier) and for access to individual REC Services. The following changes are being proposed to the Schedule (see Annex E):

- Inclusion of references to CCS and the CCS Arrangements Schedule within the list of applicable REC Services (paragraph 2.10);
- Inclusion of CCS testing within the external testing section (paragraph 7) to provide assurance that CCS Users can interact with the CCS and meet the requirements set out in the Consumer Consent Service Arrangements Schedule;
- Inclusion of references to CCS within the Information Security and Data Protection (ISDP) assessments section (paragraph 8), to provide assurance that CCS Users have appropriate controls to manage information security and data protection risks;
- Inclusion of reference to CCS within the approval of qualification section (paragraph 9), to clarify that applicants may need to revisit aspects of the qualification process where system changes impact CCS interfaces;
- Inclusion of references to CCS Users within the maintenance of qualification section (paragraph 11), requiring completion of an annual ISDP assessment, either via a compliance statement or a full external assessment. See below for further details;
- Inclusion of references to CCS within the template Access Agreement, binding CCS Users to the relevant REC provisions. This section also includes reference to Registered Tariff Interoperability Users as a subset of CCS User, required to comply with the tariff interoperability provisions; and
- Inclusion of references to RECCo in section 7.1 of the template Access Agreement, reflecting that RECCo may act as a Data Controller in certain REC-governed processes (e.g. IDV processes).

As a result of the tariff interoperability phase 1b, a further change will introduce a requirement for energy suppliers to become CCS Users in accordance with the Consumer Consent Service Arrangements Schedule. The requirement applies only to Tariff Interoperability Energy Suppliers as defined by the Tariff Interoperability Licence Condition.

While the changes to the Schedule are relatively limited, the associated operational arrangements represent a key area of activity for CCS implementation. Since issuing the February 2026 consultation, RECCo has worked with the REC Qualification Service Provider to review the existing arrangements and define the approach applicable to the CCS, including both the ISDP assessments and the CCS testing arrangements.

8.6 Information Security and Data Protection (ISDP) Assessment

As set out in section 6.4 of Part A, RECCo considers CE+ to be an appropriate minimum requirement for CCS Users. However, CE+ alone is not sufficient to address all risks associated with CCS participation. The proposed qualification approach therefore builds on this baseline through the ISDP assessment, enabling additional assurance to be obtained in areas such as governance, data protection, third-party oversight, data minimisation, and the prevention of inappropriate data use. The level of evidence required through the ISDP assessment will be determined using a risk-based approach,

reflecting the nature, scale, and sensitivity of the applicant's intended use of the CCS and the associated energy data access that the CCS enables. The ISDP is focused specifically on downstream data management activities and provides assurance that ATPs maintain effective systems, processes, and controls to mitigate the risk of unauthorised access to data, thereby protecting consumer trust in the CCS arrangements. The framework is intended to be adaptable across different data use cases, beginning with HH metered data and allowing for future expansion. This layered approach is intended to balance the need to maintain consumer trust with avoiding unnecessary barriers to participation, while ensuring that access to HH metered data is subject to enhanced scrutiny where justified by risk.

RECCo has reviewed the existing ISDP framework to determine the changes required to assess applicants seeking access to HH metered data via the CCS, covering both initial qualification and ongoing maintenance of qualification. This includes consideration of the ISDP question set and the factors used to determine the level of evidence required and the frequency of reassessment, based on the associated risk profile.

The ISDP approach, including the proposed question set and factors that will be considered when determining the risk classification (high, medium, or low) for each individual applicant is included in Annex E. This approach has been reviewed by the REC PAB and discussed with Elexon and SECCo to ensure alignment with wider assurance activities and to prevent duplication across Energy Codes. Risk classification will also inform the frequency of ISDP reassessments: low risk organisations will typically be reassessed every three years, while higher risk organisations will be reassessed annually or biennially. Detailed requirements for maintenance of qualification will be discussed and agreed with the REC PAB following this REC drafting consultation and set out in the relevant REC category 3 documentation.

As set out in section 6.4, the cost of qualification post CCS MMP implementation, will be recovered from individual CCS Users. The specific ISDP-related costs will be set out in the REC Charging Statement and subject to annual review. While final costs cannot yet be confirmed, indicative values are provided in table 4 below:

	Cost Per Assessment	Rationale
Onboarding and assessing a new CCS User	High risk - up to £15k Medium risk - £8-10k Low risk - approx. £5k	Level of work is likely to vary by complexity and the level of follow ups.
Assessing an existing REC Enquiry Service User seeking access to CCS	High risk - up to £10k Medium risk - £6-8k Low risk - approx. £1k	Based on the incremental work needed over and above Enquiry Service qualification.
Ongoing CCS Maintenance of Qualification and reassessment activities Completed either annually, biennially or every three years depending on risk level	For external assessments High risk - up to £15k Medium risk: £8-10k Low risk - approx. £5k	Level of work is likely to vary based on the nature of the risk level, and whether an external assessment is needed.

Table 4

As part of this consultation, we are seeking views on the appropriateness of the ISDP questions and the proposed approach to determining individual CCS User risk levels. In particular, we welcome input from code bodies that expect to rely on the REC ISDP framework to provide sufficient assurance to mitigate risks associated with data and / or security breaches. Following the consultation, we will finalise the scope of the ISDP and agree commercial arrangements, with associated costs reflected in the 2027/28 REC Charging Statement.

8.7 External CCS testing

External testing under the Qualification and Maintenance Schedule refers to testing completed by an applicant to demonstrate that its internal systems and processes can integrate with central solutions. Under the REC, this is currently required for organisations seeking to use the Central Switching Service, Data Integration Platform, and the Data Transfer

Service. As set out in the February 2026 consultation, CCS external testing is required in order to demonstrate that a CCS User can integrate with the CCS, support the CCS interactions applicable to its role, and comply with the relevant security requirements.

We are proposing to take a similar governance approach to CCS external testing as that used for the Data Integration Platform. Under this approach, the REC will set out the requirement for applicants to undertake external testing as part of the qualification process, while the detailed test approach and scenarios will be defined in lower-level category 3 documentation. To support this, RECCo is developing a test approach and plan which will be shared with industry for consultation later in 2026.

8.8 Performance assurance reporting and monitoring

The February 2026 Design consultation set out that assurance of both the CCS and CCS Users will fall within the scope of the REC Performance Assurance Framework, overseen by the REC PAB. It recognised that effective monitoring and reporting will be critical to ensuring that the CCS operates reliably, securely, and in line with consumer expectations.

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

- ensure compliance with the REC;
- identify emerging risks relating to system performance, security, data protection, or consumer experience;
- support proportionate and risk-based performance assurance under the REC Performance Assurance Framework;
- 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.

The proposed monitoring regime is intended to provide visibility of the principal risks associated with CCS operation, including those relating to service availability, consumer trust, inappropriate data access, ineffective permission management, and systemic failures affecting market participants. Monitoring outputs will be used not only to assess service performance but also to identify indicators of potential consumer harm, emerging non-compliance, or weaknesses in operational controls.

RECCo has identified the following specific areas for monitoring to support ongoing oversight of the CCS arrangements and the application of performance assurance:

- CCS system availability and resilience;
- API performance (including latency, timeouts, and error rates);
- volumes of permission creation, updates, withdrawals, queries, and revocations;
- identity verification, address and MPxN matching success and failure rates;
- drop-off rates at key stages of the consumer journey, permission journey durations;
- trends in failed, repeated, or suspicious permission attempts;

- changes in behaviour patterns that may indicate misuse or security concerns;
- tracking of CCS-raised queries against subsequent system actions;
- demand and capacity metrics (e.g., throughput, peak utilisation) to identify bottlenecks and inform scaling;
- data governance, management, and retention; and
- disaster-recovery performance.

RECCo considers that many of these monitoring requirements can be met through centralised reporting. The CCS will retain an audit log of all system interactions, with a 'grant id' assigned for each permission journey to support post event tracking where issues arise. For example, reporting may identify instances where a CCS User is not meeting response latency requirements or is failing to resolve queries in a timely manner.

The detailed format and content of CCS Provider reporting are yet to be finalised. This will be agreed between RECCo and relevant service providers in line with obligations set out in the REC. The resulting changes to the Performance Assurance Reporting Catalogue (PARC) will be progressed through a separate REC Change Proposal after this CCS drafting consultation has closed.

There are, however, areas where centralised reporting will not provide sufficient visibility of CCS Users activities, including:

- adherence to the ATP consumer engagement requirements (e.g., clarity, transparency, accessibility);
- alignment of ATP's internal permission records and CCS records, including reconciliation outcomes;
- timely use of the CCS to update, correct, or revoke permissions where required;
- management of consumer complaints / queries raised outside the solution.

RECCo does not consider that these areas warrant routine (e.g. monthly) reporting from CCS Users. However, failures in these areas may adversely impact consumer outcomes. It is therefore proposed that CCS Users retain appropriate records relating to consumer-led revocations and complaints raised outside the CCS. This information would not be reported routinely but may be requested where performance assurance techniques are applied in response to issues identified through CCS Provider reporting or other assurance activities.

This will be reflected as 'on request' reporting within the Performance Assurance Reporting Catalogue (PARC) to ensure CCS Users retain the necessary information. Where monitoring identifies potential misalignment between ATP internal permission records and CCS records RECCo may initiate additional assurance activities (e.g. inclusion in data cleanse exercises).

In addition, it is proposed that compliance with the CEGs will form part of the annual compliance statement within the maintenance of qualification process, with ATPs required to provide explicit confirmation of compliance.

Through this consultation, we are seeking views on the scope of monitoring and reporting set out above. Responses will inform the development of updates to the PARC, including the definition of centralised CCS reporting and any 'on request' reporting requirements applicable to CCS Users.

8.9 Enquiry Service Definitions

As set out in Part A of this document, for the CCS MMP the verified property information established through the CCS verification process will be used to identify the relevant electricity metering point or points through the Electricity Enquiry Service (EES). Where available, the UPRN will be used as the preferred property reference. Where a UPRN is not available, the CCS will use the verified address information in accordance with the applicable matching rules.

The EES is used for property-to-meter-point matching only. It does not provide the electricity consumption data requested under a CCS permission. That data will continue to be provided by the relevant EDH.

Use of the REL Address under the REC is enabled through a licence with Ordnance Survey, which permits the Central Switching Service to use Ordnance Survey data to match Meter Point Location (MPL) Addresses provided by network operators with corresponding postal addresses. At present, the REC limits use of the REL Address data to activities required to support switching.

RECCo has confirmed that the existing Ordnance Survey licence permits the use of REL Address data to support internal CCS processing activities. The existing licensing arrangements therefore do not require external REL Address data rights to be extended in order to support the CCS MMP. However, the REC arrangements governing use of REL Address data need to be amended to recognise its use for the CCS property-to-meter-point matching process.

Consequently, changes to the EES Service Definitions have been developed and are set out in Annex E. These changes are limited to enabling the CCS operational processes and do not broaden the external licensing rights associated with REL Address data.

The CCS MMP does not include gas consumption-data provision or a CCS MPRN-matching journey. No equivalent Gas Enquiry Service change to enable CCS MPRN matching is therefore proposed as part of the MMP. Any future gas matching capability will be considered as part of the future development of the CCS and progressed through the applicable REC change arrangements.

8.10 Consumer Experience Guidelines

Q10. Do you have any comments on the draft Consumer Experience Guidelines? If yes, please provide details, highlighting any specific clauses against which the comment relates and proposed drafting suggestions.

Q11. Do you believe consumer-facing screens should use the term 'permission' to align with the REC drafting or use the term 'consent'? Please provide your rationale.

The CEGs will be introduced into the REC as a new Category 3 document, supported by illustrative guidance demonstrating consumer journeys and example consumer-facing content

The CEGs are structured around five stages of the permission lifecycle:

- **Discover and understand CCS (the pre-permission stage)** - where consumers are introduced to the CCS by the ATP before being asked to provide permission. This stage focuses on ensuring consumers are provided with sufficient information to understand the purpose of the CCS, the nature of the proposed data sharing arrangement and the choices available to them;

- **Granting permission** - where consumers decide whether to provide permission for a specific energy data sharing request. This stage focuses on supporting informed decision-making through clear information, transparency, and appropriate consumer controls;
- **Renewal of permission** - where an existing permission is due to expire and the consumer is asked whether they wish to continue data sharing arrangements. This stage focuses on ensuring consumers understand the implications of renewing or allowing a permission to lapse;
- **Review permission** - where consumers review their active permissions, either through the CCS Consumer Portal or through an ATP's consumer-facing channel. The CEGs set out expectations intended to make key information accessible and support consumers in understanding the permissions they have granted; and
- **Revocation of permission** - where a consumer chooses to withdraw a previously granted permission. This stage focuses on ensuring consumers are able to revoke permissions easily and understand the consequences of doing so.

The CEGs are intended to provide a common view of the consumer experience outcomes that should be delivered across CCS permission journeys, while allowing flexibility in how individual market participants design their wider products, services, and customer relationships.

As part of this consultation, we are seeking views on the CEG drafting, including whether it provides an appropriate and complete articulation of the intended consumer experience and whether the guidance supports consistent implementation across CCS journeys. We are also seeking views on the appropriate terminology for consumer engagement and whether references to "consent" should be retained or whether "permission" should be used throughout to align with the approach adopted in the REC drafting.

8.11 Technical and Data Specifications

Q12. Do you have any comments on the content of the CCS API Technical Specification? If yes, please provide further details.

Q13. Do you have any comments on the contents of the Energy Market Data Specification? If yes, please provide further details, highlighting the specific data item or market message against which the comment relates.

Q14. Do you have any comments on the redlined changes to the Standards Definition Document? If yes, please provide further details, highlighting any specific clauses against which the comment relates and proposed drafting suggestions.

8.11.1 CCS API Technical Specification

The CCS API Technical Specification provides detailed requirements governing how CCS Users interact with the CCS APIs and supports CCS Users in developing and implementing their technical solutions. The CCS API Technical Specification is derived from the technical design documents, and translates the relevant technical requirements into formal REC provisions, including the API interactions, validation requirements, security controls, and application of relevant open standards that form part of the CCS technical interface.

The CCS API Technical Specification principally covers two sets of API interactions: interactions with the CCS Authorisation Server, supporting permission and authorisation activities and the management of access tokens and refresh tokens; and interactions with the CCS Directory, supporting participant and technical discovery and the management of relevant organisational and technical information. It also defines the Shared Signals Framework arrangements used to communicate relevant permission and grant lifecycle events to CCS Users. It does not define the API through which an EDH provides energy data to an ATP; those interfaces remain specific to the relevant EDH and data product.

The CCS API Technical Specification also specifies the structure of the access token issued by the CCS and presented by an ATP to the relevant EDH when requesting access to energy data.

The proposed CCS API Technical Specification is provided at Annex E. Supporting machine-readable developer documentation is available via the CCS section of the RECCo Developer Portal¹².

The fundamental principle underpinning the development of the CCS API Technical Specification is that interactions required to support the granting and revocation of permission will be based on existing, proven functionality, rather than RECCo developing bespoke CCS specifications. As set out in Part A of this document, the CCS technical design will use existing open standards including FAPI 2.0, OpenID Connect and the OpenID Shared Signals Framework, together with the relevant supporting open standards, and augmented with CCS specific elements such as IDV. The following elements are included in the API Technical Specification:

- Permission initiation and authorisation using Rich Authorisation Requests (RAR) and Pushed Authorization Requests (PAR) - an ATP initiates the permission journey through a PAR containing the CCS-specific `authorisation_details`. The information may include non-authoritative information supplied by the ATP and is validated and, where applicable, enriched by the CCS following identity, occupancy, and RMP-matching activities;
- An OAuth 2.0 Authorisation Code flow - following the granting of permission, an authorisation code is returned to the ATP and exchanged securely with the CCS for the applicable access token and refresh token. Access tokens are issued for the relevant EDH and are sender-constrained to the ATP;
- Local validation of CCS-issued access tokens by EDHs - the Specification defines the requirements for EDHs to validate signed access tokens presented by ATPs before providing the authorised energy data;
- CCS Directory APIs - including the Participants API and Connect API, which support participant and technical discovery and provide the information required to establish trusted interactions between CCS Users; and
- The CCS Shared Signals Framework (SSF) - providing push-based notifications to relevant CCS Users when defined changes occur to a permission or grant, including revocation and other relevant lifecycle events.
- Account-holder verification for Tariff Interoperability - defining the interaction between the CCS and the relevant Energy Supplier through which the Account Holder is authenticated and the verification outcome and relevant RMP information are returned to the CCS.

In addition, the design incorporates FAPI 2.0 security controls including Proof Key for Code Exchange (PKCE), sender-constrained tokens (e.g. mTLS), and where appropriate JWT-secured request and response mechanisms.

8.11.2 Energy Market Data Specification

¹² dev-portal.retailenergycode.co.uk/projects/ccs/

Under REC governance, the content of the CCS API Technical Specification will be translated into the Energy Market Data Specification (EMDS) which defines data items and market messages used across a number of industry codes in a standard format. The EMDS allows users to view the plain English metadata in HTML format, or download the content as a BACPAC file to support system development activities. For the purposes of this consultation, the proposed content of the EMDS has been provided as a PDF document (Annex E). Post consultation, the approved content will be included in the wider EMDS product set as part of the R0318 delivery. The current EMDS product set, excluding CCS content, can be viewed here: [Data Specification Catalogue](#).

The EMDS content is split into two sections, within Annex E:

- The Data Item Catalogue which outlines each data item contained within the CCS API Technical Specification. It provides a reference, owner, a plain English and YAML / JSON name, details of length and data type format, along with any enumerations. Further detail on each of the attributes is set out in the Data Item Catalogue Explainer.
- The Market Message Catalogue details all the messages contained within the CCS API Technical Specification. It provides information on the required data items for each message, the description of the message, and any scenario variants on the use of that message. Further detail on each of the attributes is set out in the Market Message Catalogue Explainer.

8.11.3 Standards Definition Document

To support industry understanding of the EMDS content, the REC Standards Definition Document was created which defines the common standard for documenting all relevant industry data and messaging, associated with several different physical messaging standards. The Standards Definition Document is governed under the REC and subject to the REC change management process.

Minor changes to the Standards Definition Document have been proposed to reflect the new CCS arrangements. These changes include reference to the new CCS message standard and addition of two new market data services covering CCS Users and the CCS. These redlined changes are included in Annex E.

8.11.4 Summary

Through this consultation, we are seeking views on the content of the CCS API Technical Specification, the EMDS and the Standards Definition Document. Based on the decision to use open standards, respondents are encouraged to focus comments on CCS-specific elements within RECCo's control; where comments relate to the underlying open standards, respondents should explain any CCS-specific implementation impact.

8.12 CCS Service Definition

Q15. Do you have any comments on the scope and contents of the CCS Service Definition? If yes, please provide comments highlighting any specific clauses against which the comment relates and proposed drafting suggestions.

The CCS is being introduced into the REC as a new REC Service. As with other REC Services, a Service Definition will be required setting out the scope, functionality, and key characteristics of the CCS, including the roles and responsibilities of

service providers and users, the interfaces between systems, and the operational processes that underpin service delivery. The Service Definition is intended to provide a clear description of how the CCS operates within the REC framework, ensuring consistency in understanding across market participants and supporting the effective governance, implementation, and ongoing operation of REC Services.

REC Service Definitions focus on elements of the solution that fundamentally impact participants and require formal governance, including management of ongoing change via the standard REC change process. Lower-level detail may be included within accompanying guidance or RECCo contractual arrangements. REC Service Definitions do not include obligations on REC Service Users, with these captured within the relevant operational schedule i.e. the Consumer Consent Service Arrangements Schedule in this instance. This separation ensures that service functionality and operational obligations can be maintained independently, whilst remaining subject to the appropriate REC governance processes.

Each REC Service Definition follows a similar structure as set out in the table below. The content of the CCS Service Definition has been derived from the high-level design decisions covered in Part A of this document (e.g. the decision to use FAPI 2.0), the baseline solution functionality procured from the CCS Provider (reflecting the CCS design principle to use existing functionality rather than developing bespoke capabilities) and where optionality in the technical solution exists, working group discussions. A summary of the CCS Service Definition is provided in table 5 below, with full drafting included in Annex E:

Section of Service Definition	Description
Description of service	Provides a high-level overview of the CCS and references to other REC products which should be read alongside the service definition.
Entities who can access the CCS	Defines the entities that are expected to use the CCS, including CCS Users (ATPs and EDHs), consumers and IDV providers, and other authorised users where applicable.
Service functionality	Provides a high-level overview of each of the functional components of the CCS, including the mechanism for providing authorisation and sharing / validating access token and the consumer portal allowing consumers to view and manage their permissions.
System access and user management	Explains how users engage with the CCS, covering qualified CCS Users, IDV providers, consumers and other organisations / individuals seeking to view publicly available information.
Service availability	Reflects the contractually agreed availability targets.
User support and incident resolution	Reflects the contractually agreed service management response targets and the interaction with the existing REC service management arrangements, through which CCS-related queries and incidents are raised.
Service levels	Reflects the contractually agreed service levels covering message response latency and management of disaster recovery scenarios.
Maximum demand volumes	Reflects the contractually agreed capacity requirements, recognising the expectation that CCS is being delivered to enable scalability to expand in line with the future roadmap.

Reporting	Reflects the requirement on the CCS Provider to provide monthly performance reports and operational reporting to support REC governance and performance assurance activities.
System audit	Reflects the contractually agreed data retention and audit requirements.
Data handling	Reflects the specific approach to user interactions and data exchange.
Security	Reflects the agreed security profile, specifically the application of the FAPI 2.0 specification and the decisions taken regarding the optional elements defined within this specification.

Table 5

Through this consultation, we are seeking views on the content of the draft CCS Service Definition included in Annex E and whether there are other elements of the CCS design that should be captured within the artefact that require maintenance through the formal REC change process.

9 Conclusion and next steps

We welcome the views of interested parties on the specific questions asked within this consultation, together with general thoughts on our proposals. We recognise that there are a significant number of products, each with detailed content, some of which have not been previously shared. Accordingly, we request respondents provide their comments by reference to specific sections, clauses, data items, or market messages where possible, to enable us to address each comment received and provide traceability for any changes made post consultation.

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. This reflects that many of the proposed decisions are not new information and have been developed through the working groups. Should you or your organisation have missed workgroup sessions, information is contained on Consumer Consent Hub - REC Portal¹³. While the consultation is open, we will continue to engage with interested parties and will hold a REC Drafting Consultation webinar¹⁴ on 29 September 2026.

Following the conclusion of this consultation, we will consider all consultation responses and make any appropriate updates to the code drafting before progressing the drafting through REC change governance for decision and implementation. The REC change will be a continuation of REC Issue IO318.

Prior to progressing the Change Proposal, RECCo will complete a formal handover of the baselined drafting and supporting design documentation into REC governance. The Change Proposal will then progress through the standard REC change process, including consultation on the proposed REC drafting, consideration by the Code Manager, and submission to the Authority for determination, in accordance with the applicable REC governance arrangements.

¹³ [Consumer Consent Hub - REC Portal](#)

¹⁴ [CCS REC Drafting Consultation Webinar](#)

The REC Change Proposal is expected to progress at a similar time to the expected start of RECCo operating as the Licensed Code Manager. We are working to ensure any adjustments to the REC change process have a minimal impact on the progression and implementation of CCS. Clarity on process steps and decision-making timescales will be provided at the point that REC Issue I0318 progresses to Change Proposal R0318.

In parallel with the REC governance process, RECCo will continue to progress implementation planning for CCS, including finalising delivery arrangements, developing operational and support processes, and engaging with prospective ATPs, EDHs, and other industry participants to support implementation readiness and testing activities. Further detail on implementation milestones, industry engagement, testing arrangements and participant onboarding requirements will be communicated as the project advances towards the planned market implementation date.

10 **Annexes**

[Annex A - Consultation Response Form](#)

[Annex B - Glossary](#)

[Annex C - Product Roadmap](#)

[Annex D - Business Process Diagrams](#)

Annex E - Proposed REC Drafting (coming soon)

Additional supporting design documentation available within the CCS section of the [RECCo Developer Portal](#)