Technical Security and Design Working Group Advisory Paper

Publication date:	12th December 2025
Contact:	Jeff Finch
Team:	Energy System Digitalisation
Email:	digitalisation@ofgem.gov.uk

This document is for those interested in the progress of the Consumer Consent Solution as being designed and delivered by RECCo following the Ofgem decision. It follows the initial working groups set up from that decision and explains the advice given by the experts from the Technical Design and Security working group to RECCo as to what the solution should and could entail, and will feed into RECCo's Design Consultation, published in Q1 of 2026. This paper can and should be read in conjunction papers released from the other two Working Groups, Implementation and Governance, and Consumer Protection and Accessibility.

© Crown copyright 2025

The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the Open Government Licence.

Without prejudice to the generality of the terms of the Open Government Licence, the material that is reproduced must be acknowledged as Crown copyright and the document title of this document must be specified in that acknowledgement.

This publication is available at www.ofgem.gov.uk. Any enquiries regarding the use and re-use of this information resource should be sent to psi@nationalarchives.gsi.gov.uk.

Contents

Executive summary **3**

1. Key Critical Issues **4**

Trust Framework Adoption 4

Trust Framework Integration and Interoperability 5

Digital Tokenisation and Access to Consent 6

2. General Design recommendations **6**

Technical approach 6

Appendices **8**

Context and related publications 8

Frequently Asked Questions 8

Consumer Consent Glossary 8

Consumer Consent Digital Newsletters 8

Working Group Membership 9

Executive summary

The group was formed in response to the complexities identified during the Ofgem consultation phase of Consumer Consent and the need for expert input in developing a viable solution. Ofgem did not commit to a specific model in our April 2025 decision, whether centralised, decentralised, or hybrid, and has allowed RECCo the opportunity to explore all options. The goal is to accelerate delivery while ensuring that the solution is technically sound, secure, and aligned with any potential Smart Data Schemes.

This working group is advisory in nature and does not make formal decisions. Members have been encouraged to share insights within their organizations, and no non-disclosure agreements have been required at this stage. The default approach is openness, unless specific content is deemed commercially sensitive or security critical. The group's responsibilities have included providing feedback on technical design and security, advising on standards, and identifying risks and potential mitigations.

With regards the technical aspects of the design of the Consumer Consent Solution, the decision was taken to progress the project according to agile principles, rather than creating a strawman for testing, listing all feasible user specifications, and 'front loading' conditions for success. Instead, RECCo has taken an iterative develop and test approach based on procuring in relevant expertise.

As such, the technical specifications will be tested later in the development process. This working group has consequently fewer direct recommendations at the time of writing this paper but will continue to work with and advise RECCo throughout development and testing phases.

Key topics discussed in this working group have centred around the utility of a mostly decentralised system, underpinned by a trust framework, and expected use of tokenisation to manage the transfer of consent data. From these foundational views, RECCo is rapidly iterating development of the details which will underpin and inform greater technical specificity.

1. Key Critical Issues

Section summary

The working groups are still in a nascent stage where the impetus has been to provide a levelling of knowledge in each of the working group areas. With Technical Design &Security (TDS) Working group, and understandably, the level of knowledge we are imparting is prior to in depth technical design and concentrates of the higher-level perception of the project. Hence this short paper deals with one discussed and identified part of the project in Trust Framework.

1.1 This section covers the most important issues uncovered in the TD&S Working Group. the following are the highlighted issues for the design of the eventual Trust Framework Solution;

- Trust Framework Adoption
- Trust Framework Integration and Interoperability
- Digital Tokens and Access to Consent

Trust Framework Adoption

1.2 While the working group members agree the need for a trust framework to set the rules and requirements of accredited consent seekers, there has been significant discussion about the nature of this framework, be it technical, legal, or some combination of the two.

1.3 Further discussions were had regarding how the trust framework be enabled; should it be mandated under regulation, or a multi-party contract? To what degree would the Retail Energy Code (REC) form part of the framework, and how would this operate for non-REC adherents who wished to use the Solution? How would enforcement operate, and what levels of enforcement would apply, Assurance and compliance frameworks were also discussed.

Potential sub-optimal outcomes

1.4 Risks were identified in affecting trust and thence adoption rates of the Solution. Without a robust and understood redress process – which was similarly highlighted by the Consumer Protection and Accessibility (CPA) group, consumer trust in the Solution is unlikely to develop.

1.5 This was also tied to the security and cybersecurity aspects of security by design and ensuring that the technical protections in place complimented the framework.

Trust Framework Integration and Interoperability

1.6 There are a number of existing digital initiatives, such as NESO's Data Sharing Infrastructure (DSI) and Elexon's Smart Data Repository (SDR)[1] and Flexibility Market Asset Register (FMAR). These share common features and requirements. It is key that the digital infrastructure is compatible and interoperable.

1.7 Members reinforced this requirement and highlighted that integration and interoperability should apply whether data provider, data user/consent seeker or consumer (If applicable). The need for adaptability in design to ensure that future systems, or systems currently planned, would remain compatible with the Consent Solution was also discussed.

1.8 Further to this, the levels of privilege or access control ought to remain consistent across systems and, where appropriate and reliance can be placed on existing accreditation or validations, reuse of existing systems should be maximised. There was consideration given by members to what accreditation and validation process should take place for use of the Consent Solution for non-adherents to the Retail Energy Code or similar.

1.9 Discussions were had considering the security profile that is required to create a trusted solution. A trade-off was identified between specifying data sharing arrangement requirements to maintain security that may require standards adoption by the data users and providers.

1.10 References to previous data sharing ecosystems was consistent throughout, as the group sought to take lessons learned from other solutions and apply them to the design of the Consent Solution. The balancing of compliance with fostering innovation was acknowledged, with historic systems referenced as missing this balance resulting in low adoption.

Potential sub-optimal outcomes

1.11 In the event of siloed development, the Consent Solution will be unable, or sub-optimal in its interactions with other digital infrastructure, meaning that the sources of SM data available will be limited, reducing the scalability of the solution, and driving inconsistencies.

1.12 Use of bespoke or developed artifacts or systems will increase costs to consumers and likely result in duplication across the digitalisation efforts currently in flight. Similarly, consideration ought to be given for non-code/regulation routes to demonstrate accreditation to reduce friction and increase uptake.

[1] This initiative will develop subject to final decision on BSC code modification p494.

1.13 Compliance to standards would have to be monitored and enforced, however these requirements should not limit adoption and success of the overall project.

Digital Tokenisation and Access to Consent

1.14 There was considerable discussion across multiple meetings of the methodology of digitising and exchanging consent, particularly around the use of tokens or certificates. With existing providers able to meet the technical requirements, members were of the view there was no merit to generating a bespoke token or certification system.

1.15 Details regarding issuance, validity and expiration were explored, but the nascent nature of the project made it too early to offer concrete recommendations. Members of this group are expected to continue to advise RECCo through development and testing.

1.16 Reference was made to the potential use of the Enquiry Services as a way to validate MPxNs and addresses, given its existence within RECCo's existing architecture, however members pointed out the lack of a perfect solution and raised particular concern with ensuring RECCo data inputs are accurate reflections of what energy consumers would be requesting services for.

Potential sub-optimal outcomes

1.17 Current consent records are not fully understood, and there may be challenges in standardising formats of existing consents for ingestion into the CC Solution. This is being developed as part of design consultations. Similarly, it is too early to offer recommendations.

2. General Design recommendations

Technical approach

2.1 The design of the Consumer Consent Solution is still at a very early state to suggest mitigations or design recommendations prior to further investigative works, and the commencement of high-level system designs would be presumptuous.

2.2 There are already meetings in place that will discuss the interoperability of the Consent Solution in the arena of other digitalisation projects. There are already discussions with the providers of solutions that may be involved in the project.

2.3 The fact that these elements have been identified should be noted and sufficient until the next design level discussions. Further to this, the group has identified and agreed common aspects of the design which are as follows.

Minimal central components in a hybrid design

2.4 Members of this group agreed with the approach of minimal centralised components, recommending the minimum necessary to satisfy registers and directories, and the stated policy aims of a 'one version of the truth' available to consumers to view and manage their consents.

2.5 Members agreed that some standardisation will be necessary within this hybrid design to ensure interoperability.

Tokenisation

2.6 Following on from this, members are in agreement that a decentralised token or certification system is the most appropriate method to achieve the stated aims. While the technical detail of this approach is not yet ready for detailed recommendations, this design choice is supported by the working group.

Security

2.7 Members are in agreement that care needs to be taken to select appropriate security measures, both on an organisational level (accreditations/certifications) but also on a technical data sharing level (protocols/standards/specifications). The use of proven, well-adopted and documented standards was deemed preferable from a data protection, cyber resilience and ease of implementation perspective.

Appendices

Appendix 1 Context and related publications

These publications are intended to be read as part of the ongoing development of the Consumer Consent Solution policy. Below, we have listed the Call For Input, Consultation and subsequent decision, Impact Assessment and Advisory Papers from other Working Groups. Following these publications, RECCo will produce a Design Consultation which these papers inform.

2.8 List of related publications

- Data Sharing in a Digital Future | Ofgem
- Consumer Consent decision | Ofgem
- Consumer Consent Solution consultation | Ofgem
- Consumer Consent Impact Assessment (IA) consultation | Ofgem

Appendix 2 Frequently Asked Questions

https://recportal.co.uk/documents/20121/0/Consumer+Consent+Solution+Frequently+Asked+Questions.pdf/b122c5d9-99fa-3f08-a25c-cff4cadd32a1?t=1758196139387&download=true

Appendix 3 Consumer Consent Glossary

https://recportal.co.uk/documents/20121/0/The+Consumer+Consent+Solution+_+Glossary+_+September+2025.pdf/edccfb55-7d23-5504-d833-27ee3efcd8b6?t=1758196172747&download=true

Appendix 4 Consumer Consent Digital Newsletters

Published 08 October 2025
Published 10 September 2025
Published 13 August 2025
Published 16 July 2025

Appendix 5 Working Group Membership

Ofgem

RECCo

Electralink

GreenSynch

Kraken

Elexon

Hilderbrand

Energy UK

Cadent

Smart Energy Code (SEC)

Paypoint

Smart DCC

NESO

Citizens Advice

Centrica

Ovo

Icebreaker One

Radium

Department of Energy Security and Net Zero