29/07/26

# *Consumer Consent Solution*
# Solution Group

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Agenda

| Item | Lead | Approx Timing |
|---|---|---|
| **Welcome & Intro** | Mike | 5 mins |
| **Bill Payer vs Occupier** | Matt | 20 mins |
| **IDV Approach** | Matt | 20 mins |
| **OIDC Registration Framework** | Christian / George | 30 mins |
| **Shared Signals Framework Profile** | Christian / George | 30 mins |
| **Forward Plan** | Mike | 5 mins |



This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have rece

# Housekeeping

- Please ensure that microphones remain switched off during the speaker sessions
- Raise your Hand in Teams if you have any questions – we will run through material and then pause on slides inviting feedback
- Please keep all questions relevant to the session and avoid referencing other organisations
- The slides & minutes will be circulated following the session



This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the s

# Bill Payer vs Occupier

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# From early distinction to settled CCS position

The consultation direction was already occupier-led; the work since then has made it more precise and operationally usable.

### 1 Consultation baseline

Occupier identified as the relevant person for domestic half-hourly data, including cases where they are not the bill payer.

→

### 2 Evidence tested

Stakeholder, ICO, legal, SEC/SECCo, Ofgem/DESNZ and product-design work tested this principle.

→

### 3 Matured rule

For MMP, CCS should recognise permission from the verified occupier; bill payer status is not sufficient on its own to evidence occupancy.

**So what?** **The direction has matured from a principle to an evidence-led, repeatable CCS rule.**

# Current CCS position: verified occupier permission

For domestic half-hourly metered data, this should be treated as the settled CCS MMP position.

## For domestic half-hourly metered energy data, CCS should treat the occupier of the premises as the appropriate person to grant permission.

Being the bill payer alone is not sufficient where that person is not the occupier.

### Consumer protection

HH data can reflect activity, behaviour and occupancy at the premises.

### Market consistency

CCS provides one governed route rather than relying on varied bilateral approaches.

### Operational clarity

The model separates payment/account relationship from authority to permit occupier data sharing.

### Design link

IDV must evidence identity and likely occupancy, not just a name or energy supply account link.

**Transition to IDV: once the permission rule is occupier-led, IDV must evidence identity + occupancy + MPxN linkage.**

# IDV Approach

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Same intent, better route to the outcome

CCS is changing the route to the bar — not lowering the bar.

**The outcome stays fixed**

**CCS must know that the person granting permission is identifiable, sufficiently linked to the premises as an occupant, and therefore appropriate to act for domestic HH data sharing.**

## Intent

### What remains unchanged

Central CCS IDV capability remains part of the trust framework
Consumer protection remains the purpose for HH data
The output must be governed, auditable and explainable

## Route to assurance

### What has matured

Move away from photo ID as the assumed ordinary route
Use trusted digital relationships and data signals where sufficient
Define evidence combinations and step-up conditions, not a single fixed method

## MMP design consequence

### What this means for IDV

Identity proofing alone is not enough for an occupier-led permission model
The journey must validate identity, address/occupancy confidence and MPxN linkage
Photo ID can still be offered as a consumer choice if evidence points to the value

**Design move: method-led verification → evidence-led**

Earlier emphasis **photo-ID-led route** → Matured route **bank / CRA / address signals** → Governed result **auditable assertion + step-up rules**

# What we heard and tested

Robust IDV was supported, but the route needed to be proportionate and usable.

| Evidence input | What it told us | Design response |
| --- | --- | --- |
| **Consultation feedback** | Maintain assurance, but test proportionality, duplication and friction. | **Move from method-first verification to outcome-led assurance.** |
| **Consumer research** | Photo ID emerged as a likely drop-off point, not IDV in principle. | **Avoid photo ID as the assumed default where equivalent evidence can be used.** |
| **Product review** | Multi-source routes can combine banking, CRA, telco, address and other support signals. | **Treat IDV as configurable evidence orchestration.** |
| **Occupier-led policy** | Identity & bill payer alone is insufficient; CCS must evidence likely occupancy. | **Support identity, occupancy confidence and MPxN linkage.** |

**The design response is to use existing trusted relationships and evidence sources where they can meet the CCS assurance outcome.**

# Current IDV assumption: evidence-led validation

Central IDV remains, but the delivery route should combine mechanisms that prove identity, strong occupancy and premises linkage.

**MMP assumption**

**Use a centrally governed IDV capability that orchestrates trusted evidence sources, rather than treating photo ID or bill payer status as the default answer.**
The capability should return an auditable assertion that the person is identifiable, linked to the address, and sufficiently likely to be the current occupier for the relevant MPxN.

## 1 Bank-verified identity

**Identity anchor**

**How it works**

Consumer authenticates through an existing banking relationship. The route can provide bank-held KYC attributes such as name, address and date of birth without starting from document scanning.

**What CCS gets**

**Confirms the person is identifiable and gives a trusted identity/address starting point.**

## 2 Background CRA + address intelligence

**Occupancy confidence**

**How it works**

Credit-reference and address signals are used behind the journey to assess whether there are sufficient records connecting the individual to the current premises.

**What CCS gets**

**Builds evidence that the verified person is highly likely to be a current occupier, along with how long they have occupied an address.**

## 3 Premises / MPxN matching

**Energy data linkage**

**How it works**

The verified identity and address evidence is matched to the relevant premises and MPxN with the utilisation of UPRNs (where available) to ensure a higher degree of matching is achieved.

**What CCS gets**

**Creates the auditable link between the person, the premises and the data sharing permission.**

**Solution Group Feedback**

**What are the views of the group on this approach?**
**Any existing practices or experience CCS should be aware of?**

# OIDC Registration Framework

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Where this session sits

This part of the session builds on how registration to the Trust Framework works, and what ATPs and EDHs keep in good order around the consent flow.

1. OIDC Federation — the concept
2. What it means for participants today
3. Onboarding journeys
4. The consent flow at a glance
5. What ATPs keep in place
6. What EDHs keep in place

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

SECTION 01

# OIDC Federation & Registration

How participants are identified, registered and kept current — without a registry that drifts.



REGISTRATION

# OIDC Federation — the concept

1

## The problem

How does the CCS know a participant is genuine, current and accredited — without keeping its own registry that drifts out of date?

2

## The answer

The Trust Framework signs each participant's metadata as an Entity Statement. Trust is verified cryptographically — not established by a registration call.

3

## One identity

Your client identifier is your identity on the Trust Framework. Nothing separate to register, no second identifier to manage.

4

## A proven pattern

The same model in live operation across modern data-sharing ecosystems.

IN ONE LINE

**The Trust Framework vouches for every participant — and the CCS checks that vouching cryptographically, every time.**

Signed metadata · verified against the Trust Framework's keys

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

REGISTRATION

# What this means for you today

### The CCS is your integration point

One central authorisation service for the whole ecosystem. You do not federate with other participants directly.

### Federation runs behind the scenes

Entity Statement signing, trust chains and refresh cycles are handled between the Trust Framework and the CCS.

### Nothing to build or operate now

No federation endpoints to stand up, no trust chains to resolve on your side. Awareness is enough at this stage.

**What you do own: your metadata.** Keeping your details current on the Trust Framework is what keeps you discoverable and operational.

*Why this design: accreditation status and technical access can never drift apart — what the Trust Framework says is what the CCS enforces.*

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

REGISTRATION

# Onboarding at a glance

## ATP

1. Apply for accreditation with RECCo.
2. Generate signing keys and obtain a transport certificate — key sets hosted via the Trust Framework.
3. The Trust Framework signs and publishes your Entity Statement.
4. The CCS picks you up on its next refresh — you're operational.

## EDH

1. Apply for accreditation with RECCo.
2. Publish resource endpoints, supported consent types and your bilateral-agreement flag; obtain a server certificate.
3. The Trust Framework signs and publishes your Entity Statement.
4. Listed and discoverable by ATPs — you're operational.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

SECTION 02

# Participant Obligations

Beyond the flow itself — what ATPs and EDHs keep in good order around it.



THE FLOW

# The consent flow at a glance

SIMPLIFIED

## 1 Discover

The ATP resolves endpoints, keys and metadata from the Trust Framework.

## 2 Push the request

The ATP submits the signed authorisation request (PAR) to the CCS.

## 3 Consumer consents

The CCS authenticates the Consumer, captures consent and returns a code.

## 4 Exchange the code

The ATP exchanges the code over mTLS and receives a certificate-bound token.

## 5 Call the EDH

The ATP presents the token to the EDH's resource endpoint.

## 6 Validate & serve

The EDH validates the token locally and returns the authorised data.

*Deliberately simplified — the rest of this section is about everything around this flow that keeps it working reliably.*

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Before and after the redirect

1

## Bind the request to the session

Keep the link between the outbound request — state, PKCE verifier, request reference — and the Consumer's session, so the redirect back is correlated, validated and used exactly once.

2

## Validate the return leg

Reject a mismatched state value. Treat denial and error redirects as outcomes to handle cleanly — not failures to retry.

3

## Keep clocks honest

NTP-synced clocks throughout. Signed request objects live inside a 10-minute validity window, and clock drift shows up as intermittent, hard-to-diagnose rejections.

WHERE THIS LIVES

**Steps 2–4 of the flow.**

Between pushing the request and exchanging the code, the Consumer is out of your hands. The state you hold on your side is what reconnects them safely when they return.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Tokens, keys & certificates

1

## Reuse tokens — don't churn them

Cache and reuse the access token within its 30-minute lifetime rather than requesting a new one per API call.

2

## Same certificate everywhere

Tokens are certificate-bound: present the same mTLS certificate to the EDH that you used at the token endpoint.

3

## Steward refresh tokens

Store them securely, handle rotation, and treat an invalid-grant response as the consent-revoked signal — clean up local state rather than retrying blindly.

4

## Rotate keys with overlap

Publish new signing keys to your Trust Framework-hosted key set with a 24-hour overlap, and keep an emergency path for compromised keys.

5

## Renew certificates early

Request transport certificate renewal around 30 days ahead of expiry, retaining the previous certificate through the overlap.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

ATP OBLIGATIONS · 3 OF 3

# Directory hygiene & operations

### Keep your directory entry current

Redirect URIs, application name, contacts. A stale redirect URI is a broken Consumer journey.

### Integrate via discovery only

Resolve CCS endpoints from its discovery document and EDH endpoints from the Trust Framework. Never hardcode — and use the mTLS endpoint aliases.

### Check the bilateral-agreement flag

Some EDHs need additional access arrangements in place before you call them. The flag tells you where.

### Send the interaction identifier

A unique x-fapi-interaction-id per request, logged on your side, so incidents can be correlated across parties.

**Back off sensibly.** Retry with backoff against CCS and EDH endpoints — formal rate limits may follow in the technical standards.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Validating a token you didn't issue

1

## Validate locally — authoritatively

Check the signature and the standard claims — issuer, audience, expiry — plus the meter-point and access-window details carried in the token.

2

## Check the certificate binding, twice

Match the token's certificate thumbprint to the certificate presented over mTLS — and confirm that certificate belongs to the client identified in the token.

3

## Cache the CCS keys with discipline

Hold CCS signing keys for no less than 5 and no more than 30 minutes, sourced via the Trust Framework.

4

## Check revocation on every handshake

Validate ATP certificates against the Trust Framework revocation services on each connection.

THE MENTAL MODEL

**The CCS issues. You validate.**

EDHs run no authorisation service of their own — a pure resource-server posture. It's the biggest mental-model shift for anyone coming from ecosystems where every data holder runs its own.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

EDH OBLIGATIONS · 2 OF 2

# Policy, directory & operations

### Apply your own policy where bilateral

If you've set the bilateral-agreement flag, enforce your own access policy on the calling ATP before serving data.

### Keep your directory data current

Resource endpoints, supported consent types, the bilateral flag — ATPs discover you from this.

### Echo the interaction identifier

Return x-fapi-interaction-id in responses and retain correlated logs for audit and traceability.

### Consistent error semantics

PROPOSED

A common vocabulary for rejected and out-of-scope requests, so ATPs see uniform failure modes across every EDH.

*And the same clock discipline as ATPs — expiry checks are only as good as the clock behind them.*

FOR DISCUSSION

Which of these areas would benefit from a deeper working session?

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Shared Signals Framework

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

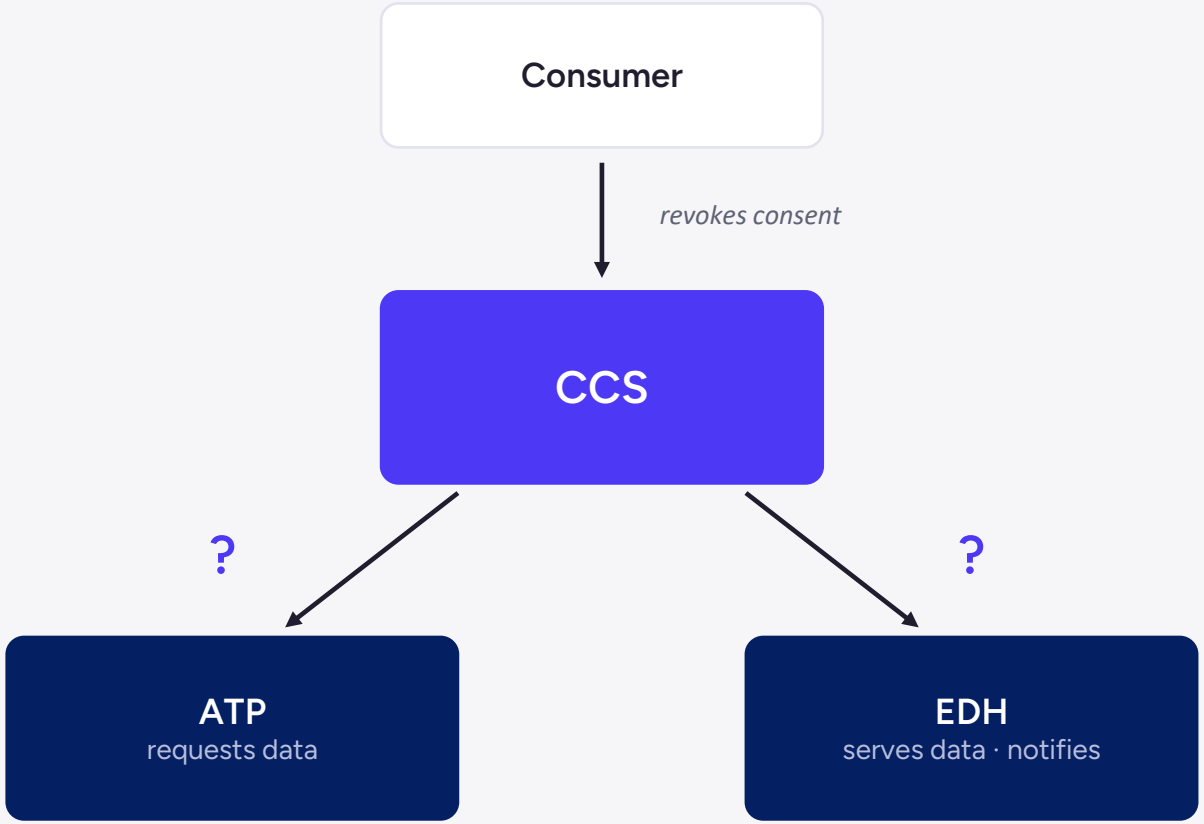
# When a Consumer revokes consent, how does everyone find out?

A revocation happens in one place — the CCS as the source of truth. But two other parties act on that consent every day:

**The ATP** requests the Consumer's energy data using tokens issued by the CCS.

**The EDH** serves that data — and, in some cases, sends notifications based on the consented data sharing arrangement.

**Both must stop, promptly and provably,** when the Consumer says stop. The question is how each of them learns that.




This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

WHERE ENFORCEMENT ALREADY LIVES

# The FAPI 2.0 token model already enforces revocation

## ENFORCED BY THE TOKEN MODEL

- **Every ATP data request presents a token**

  Validated at the EDH against a short-lived, sender-constrained access token — parameters set by the Security Profile.

  Access tokens are what represent the consent and are used to unlock access based on that consent.

- **Token issuance**

  The CCS refuses new tokens for a revoked consent — immediately.

## THE ONE RESIDUAL PATH

### EDH-initiated Consumer notifications

In some, but not all, cases, EDHs will need to maintain a data sharing schedule in order to inform ATPs of events. A good example is a tariff, where suppliers will notify ATPs of tariff events.

Here, the EDH pushes to the ATP- no token is presented, so nothing checks the consent at send time. The EDH acts on the sharing schedule it set up...

...which is exactly the schedule that goes stale when a revocation revocation happens elsewhere.

This residual path is what Shared Signals would mitigate — **best effort, clearly bounded**, with enforcement staying exactly where it is today: the token model.
Shared Signals Framework enables a check of consent validity before initiating a notification – **it does not replace use of access tokens.**

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Evolved thinking and design on webhook notifications

In our design consultation we presented the capability for CCS to notify ATPs and EDHs of changes to consent

### 1 Consultation baseline

ATPs and EDHs subscribe to webhooks to receive notifications of a state change of consents

General perception that EDHs would need record updates.

### 2 Design evolution

Detailed design work revealed most EDHs have no need to store consent information.

However, some use-cases have specific requirements for EDH-driven notifications to ATPs.

### 3 Refined solution

Shared Signals Framework (SSF) is an open standard allowing parties to share notifications securely.

Our key decision now is how should this mechanism be used

**So what?**

**SSF enables EDHs to test if a specific consent is still active** – this can enable **EDHs to prompt ATPs of a change in state**, inviting them to request data.

**This change in state could be related to a data change (**e.g. in the case of tariff changes for a consumer**) or potentially related to data becoming available.**

**SSF does not replace the use of tokens – SSF is for sharing signals only, tokens are what controls data access through consent.**

recco

THE CONCEPT

# Enter Shared Signals

An OpenID Foundation standard for telling another system — verifiably — that something has changed.



THE CONCEPT

# What the Shared Signals Framework is

1

## A standard way to say “something changed”

Signed security events exchanged between systems. An OpenID Foundation standard, finalised in 2025 — not an invention of this programme.

2

## A Transmitter and its Receivers

One party emits events (the CCS); subscribed parties consume them (EDHs and ATPs). The subscription is called a stream.

3

## Built on proven IETF plumbing

Each event is a Security Event Token — a signed JWT stating a fact (RFC 8417) — delivered over standard HTTP polling (RFC 8936).

4

## Self-describing and self-testing

The Transmitter publishes its capabilities at a well-known URL, and test events can prove the whole pipeline end-to-end at any time.

This email/document and its contents have been classified as ‘Internal & Partners’ by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

THE CONCEPT

# Three building blocks

## Security Event Tokens

A signed JWT stating one fact: “this Grant was revoked at time T.”

Same signature machinery as the rest of the ecosystem — verifiable, non-repudiable, tamper-evident.

## Streams

A per-EDH subscription managed over a small API.

The CCS scopes it automatically to every Grant the EDH holds — nothing to subscribe to per consent, ever.

## Discovery & Verification

The CCS publishes its capabilities at a well-known URL.

ATPs use the same discovery to subscribe.

Test events prove the pipe end-to-end — before it is relied on, and any time after.

Revocation is the first event type, not the only one. Future notifications - and EDH→ATP signalling if the TI team takes it forward - travel over the same wiring, with the same receiver.

This email/document and its contents have been classified as ‘Internal & Partners’ by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

ADOPTION LANDSCAPE

PRECEDENT

# Field-tested in enterprise identity

| | |
|---|---|
| **Apple** | Mandates SSF for identity providers integrating with Apple Business Manager — the adoption forcing function. |
| **Okta** | Full transmitter and receiver in production; revocation signals drive session termination across vendors. |
| **Google** | Receives SSF signals into Workspace; has run account-security event feeds (SSF's ancestor) for years. |
| **Cisco · SGNL · Jamf** | Interop-tested implementations, developer tooling, and live sandboxes across the vendor ecosystem. |

Live in production today on well-known platforms — albeit in settings quite different from an energy-data ecosystem.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

PROPOSED APPROACH

# How it would work in the CCS

01

### Consumer revokes

At the CCS — the single place consent lives.

*This may be initiated in CCS or through ATPs*

02

### CCS signs an event

'Consent revoked for Grant X at time T.' Event type, Grant ID and timestamp — nothing else.

03

### EDH polls its stream

Outbound call over mutual TLS. The EDH exposes no inbound endpoint at all.

04

### Notifications stop

The EDH updates its data sharing schedule; anything scheduled against it is halted.

### Poll-only, mutual TLS

The EDH always calls the CCS — never the reverse. Zero new attack surface at the EDH, anchored on Trust Framework certificates.

### Thin events, by design

Event type, Grant ID and timestamp. No revocation reason, no Consumer data — the EDH learns only what it needs to stop. Data minimisation as a principle.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

PROPOSED APPROACH

# Making “best effort” credible: the gate

Before any notification run, the EDH must prove its feed is healthy — with evidence, not assumptions.

01 **Verify** — Request a test event — a tracer — through the real pipeline.

02 **Drain** — Poll until the tracer arrives and the queue is empty. Everything queued before it — every revocation — is now in hand.

03 **Apply** — Update local consent state from what was drained.

04 **Run** — Only then send the notification batch.

**Fail closed.** If the gate cannot complete, the batch is deferred — never sent against stale state. A held batch is an operations incident; a wrong notification is a compliance incident. The proposal chooses the former, every time.

This email/document and its contents have been classified as ‘Internal & Partners’ by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

PROPOSED APPROACH

# Obligation follows capability

## EDHs THAT SEND NOTIFICATIONS TO ATPs

### Receive revocation signals from the CCS

Three things to build:

1. One outbound call to the CCS on a schedule, to collect signals.
2. Signature validation on what comes back - already built for FAPI, nothing new.
3. A stop rule: when a grant is revoked, halt anything scheduled against it.

Triggered by registering the notification capability - not by being a particular type or size of participant.

## EVERY OTHER EDH

### Nothing new to build

Revocation is handled by token validation, exactly as the Security Profile already requires.

If they add notifications later, they create a stream. No change at the CCS.

**The CCS builds the transmitter once to enable consent checking pre-notification, but there is nothing to build for EDHs that don't send notifications.**

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

THE RISK PICTURE

# How long can anything still happen after a revocation?

TOKEN ISSUANCE

## Immediate

The CCS refuses new and refreshed tokens the moment revocation is recorded.

**Enforcement**

ATP DATA ACCESS

## Token-bounded

An access token already held by the ATP stays valid until it expires. At the recommended 30-minute lifetime that is the worst case, after which no replacement can be obtained.

**Enforcement**

EDH NOTIFICATIONS

## Gate-bounded

The EDH drains its stream immediately before each notification run, so the window is not the gap between runs - it is the gap between the gate completing and the batch finishing.

**Best-effort mitigation**

*Small, explicitly accepted residuals - such as a revocation landing mid-batch - are named and recorded, not discovered.*

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

LESSONS FROM A NEIGHBOURING ECOSYSTEM

# UK Open Banking tried this — before the standard existed

## WHAT OBIE BUILT (2018)

Signed event notifications for consent revocation — the same building block (Security Event Tokens), invented ad hoc because no framework existed yet.

**Optional for every party.** No standard discovery, no verification events, retry rules bolted on after problems surfaced in production.

## WHAT THAT TEACHES US

**The need is real** — revocation signalling was worth building even without a standard.

But bespoke plumbing meant patchy adoption and bilateral maintenance. SSF is the standardised descendant of exactly that pattern — with the missing pieces built in.

The proposal: **adopt the final OIDF standard** with a short set of CCS rules for using it — standard machinery, as few CCS-specific choices as possible, each one with its rationale.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

PROPOSED APPROACH

FOR DISCUSSION

# What is proposed — and what to decide together

- Adopt SSF 1.0 with specific application — one event (consent revoked), poll-only delivery, mutual TLS via the Trust Framework
- Enforcement stays with the FAPI token model; SSF is a best-effort mitigation for the notification path only
- Conditional mandate: only notification-capable EDHs implement it — everyone else builds nothing
- Gate + fail-closed discipline makes the mitigation observable and bounded, with residual risks named and recorded

FOR DISCUSSION

1. Do you agree most EDHs do not require ongoing consent record storage/management/access - this is needed in particular cases?
2. Beyond tariff, where the need to notify ATPs of changes creates additional requirements, are there any additional use-cases we should consider for use of SSF as a mechanism for EDHs to notify ATPs of a state-change?
3. Are the named residual risks (e.g. a revocation landing mid-batch) acceptable to record and accept?


This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Forward Plan

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Forward Plan

**CCS Webinar:**

| Date | Agenda |
|---|---|
| September – date TBC | REC Drafting Consultation Webinar |

**CCS Topic Specific Solution Groups:**

| Date | Agenda |
|---|---|
| 22nd April 2026 ✅ | Tariff Interoperability & CCS alignment |
| 7th May 2026 ✅ | UX – CCS Wave 1 Research Findings & Accessibility |
| 21st May 2026 ✅ | Trust Framework Partner update following announcement |
| 4th June 2026 ✅ | Tech focused - Consent Record Schema (more topics to be added and notified by email) |
| 17th June 2026 ✅ | Policy position updates, CCS User platform R&R, RBAC, Auth Roles- Data Share Access |
| 1st July 2026 ✅ | SEC & REC alignment, Legal Access Agreement, CCS User requirements, CCS Definition |
| 16th July 2026 ✅ | ATP – account creation & renewals, UX CEG Requirements, Token Lifetime (JWT) |
| 22nd July 2026 ✅ | Consent Schema, Address / MPxN Misalignment |
| 29th July 2026 | Bill Payer / Occupier, IDV Approach, OIDC Registration Framework, Shared Signals Framework |
| 12th August 2026 | TBC |
| *Note: We will review whether Solution Groups will be maintained or temporarily stood down during and immediately-after REC Drafting consultation* | |

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Retail Energy Code Company

***Building a Retail Energy Market fit for the future***

*Involved in consumer data and consent in the energy sector?*

Let's connect.

The Consumer Consent Project is live, and we want to hear from you. Whether you have a question or concern or want to stay in the loop, our team is here to collaborate.

📩 **Reach us at: consumerconsent@retailenergycode.co.uk**

Your feedback plays a key role in shaping a secure, consumer-centric solution.

## Get Involved in Developing Consumer Consent (MMP)

*Help shape a practical, consumer-centred approach to consent*

*Scan me!*

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Appendix

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

# Consumer Consent Project Team

**Pete Davies**
Executive Sponsor

**Matt White**
Product Owner & SRO

**Michael Walsh**
Project Manager

**Vicky Brown**
PMO

**Eva Von-Schaxmann**
Business Analyst

**Teresa Thompson**
Stakeholder Engagement Mgr

**Nathan Gould**
Enterprise Architect

**George Roberts**
Technical Architect

**Sarah Jones**
Regulatory Compliance Lead

**Harriet Truss**
Change Lead

**Ann Perry**
Market Design Lead

**Project SME's**

**Alison Nickson**
InfoSec & Data Protection

**Hemant Mistry**
UX Lead

📩 **Reach us at: consumerconsent@retailenergycode.co.uk**

*N.B: Names & roles provided for transparency; not all roles are assigned 100% to CCS*

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.