FINANCIAL CONDUCT AUTHORITY

Powering open finance infrastructure

Smart Data Accelerator

FCA research in financial regulation

FCA research

The FCA is committed to encouraging debate on all aspects of financial regulation and to creating rigorous evidence to support its decision-making. To facilitate this, we publish a series of papers, covering insights and findings from FCA work and projects.

If you want to contribute to this series or comment on these papers, please contact the Smart Data Accelerator (smartdataaccelerator@fca.org.uk).

Disclaimer

Authors

Josh Lowe, Associate, Smart Data Accelerator, FCA Innovation

Ekaterina Borisova, Technical Specialist, Smart Data Accelerator, FCA Innovation

Acknowledgements

We would like to thank Kyeyoung Shin, Pinar Ozcan, and Shuchita Prakash of Saïd Business School, University of Oxford, and John Heaton-Armstrong of Raidiam Services Limited for their work on the commissioned research.

All our publications are available to download from www.fca.org.uk.

Request an alternative format

Please complete this form if you require this content in an alternative format.

Or call 0207 066 1000.

Or write to Digital and Design, Financial Conduct Authority, 12 Endeavour Square, London E20 1JN.

Contents

At a glance

Secure and scalable data sharing requires infrastructure: the technical, operational and governance arrangements that enable participants to trust one another and exchange data.

The research commissioned by the FCA's Smart Data Accelerator from Saïd Business School and Raidiam examines three possible approaches to building the infrastructure to scale from open banking to a future proof open finance ecosystem: a fully centralised model, a fully decentralised model, and a hybrid of the two. Drawing on evidence from Brazil, Australia, the EU, and the UAE, it moves beyond theoretical models to examine practical choices that determine trust, resilience, and interoperability.

The research finds that a combination of approaches provides a credible proposition for further testing in the UK context. This could mean centrally coordinating the functions where consistency matters most, such as accreditation and trust, while giving firms and sectors flexibility over how they build and deliver services.

The findings are also relevant beyond today’s ecosystem. As AI-enabled services become more capable of acting on behalf of consumers and firms, open finance infrastructure needs to support new approaches for verification, delegation, and accountability. Future infrastructure choices should be assessed against their ability to remain interoperable as technology evolves.

The next stage of the Smart Data Accelerator’s work will test these questions. The objective is to build evidence on which infrastructure functions require common coordination, where flexibility is needed, and how future open finance infrastructure can support innovation at scale.

Introduction

Purpose

This research note sets out how the Smart Data Accelerator is advancing open finance by bridging the gap from high-level concepts to testable infrastructure models. The note summarises research commissioned from Saïd Business School, University of Oxford, and Raidiam Services Limited to develop reference architectures and models for open finance infrastructure. It forms part of the FCA's wider open finance and smart data programme and contributes to its evidence-led, collaborative approach to agile policy making.

The research compares the models' trade-offs, and considers whether their identity, permission, monitoring, and revocation arrangements could support AI-enabled services acting on behalf of consumers or firms.

The purpose of this paper is to summarise the findings of the full report, explain the Smart Data Accelerator's emerging thinking, and provide a basis for the next phase of work for the Smart Data Accelerator, and further industry engagement.

Key findings

The research finds that secure and scalable data sharing depends on operational choices about participation, verification, trust, permissions, and risk management. These functions may become more important where an AI-enabled service accesses data or acts for a consumer or firm, because the infrastructure may also need to establish the service's identity, authority, and permitted actions.

The research identifies coordinated trust functions with distributed delivery as a credible proposition for further UK testing.

Across all models, the research identifies a set of common technical and assurance foundations, including shared verification standards, API security, monitoring and revocation. Holding these constant allows comparisons to focus on how trust is anchored and responsibilities are distributed. The analysis sets out three model families (centralised, decentralised/federated and hybrid) each involving trade-offs between coordination, flexibility and interoperability.

For the Smart Data Accelerator, this report translates infrastructure design into a set of observable questions that can be tested, helping to build an evidence base to inform FCA thinking and future testing activity.

Design and methodology

Open finance as infrastructure design

The research explores the practical conditions that make data sharing usable, trustworthy, and scalable. In an expanded smart data ecosystem, it is imperative to understand how the system enables and encourages participation, how participants are verified and trusted, how permissions are enforced, and how risks are monitored across an expanding and diverse network. By looking beyond APIs as technical connections between firms, the report identifies wider infrastructure functions and the building blocks that shape how an ecosystem works such as:

- Credential issuance and validation
- Digital verification and authentication
- Participant status propagation
- Consent capture
- Incident monitoring
- Access revocation

These functions determine how trust, permissions, and accountability operate in practice. Where an AI-enabled service acts on behalf of a consumer or firm, they may also need to establish who operates the service, what authority it has and how that authority can be monitored or withdrawn.

The research indicates that governance and technology cannot be treated separately. Verification, authentication, certificates, trust metadata[i], participant directories, consent[ii] records and revocation mechanisms are not simply technical components: they are the practical means through which accountability, transparency and consumer control are exercised. For this reason, the report compares models at the level of operating mechanics rather than relying on abstract categories such as centralised, or hybrid.

Across all proposed models, the research points out that some technical components need to be treated as common foundations. These include, but are not limited to, widely recognised standard frameworks such as:

- OAuth 2.0[iii]
- OpenID Connect[iv]
- FAPI-style controls[v]
- Common assurance[vi]
- Monitoring[vii]
- Revocation capabilities.[viii]

Holding these elements constant allows the comparison to focus on what varies most meaningfully between models, including trust and liability.

International benchmarking and lessons learned

The research uses Brazil, Australia, the EU, and the UAE to illustrate trade-offs between standardisation, assurance, interoperability, and institutional fit. None provide a directly transferable UK blueprint.

The case studies also help evidence the three models considered in the report. The UAE model is most relevant to the centralised model, as it shows how a common trust framework, API hub, and shared infrastructure services can support consistency and reduce implementation friction, while also raising questions about concentration risk and dependency. The Australia and Brazil models are most relevant to the hybrid model as both combine central co-ordination, common standards, and assurance mechanisms with distributed implementation by ecosystem participants. The EU's PSD2 regime is most relevant to the decentralised / federated model, demonstrating the flexibility of a legal access framework, but also the interoperability risks that can arise where implementation is fragmented across markets and providers.

Overall, the research suggests that the UK should learn from international experience without replicating any single model, and that different ecosystem conditions require different approaches. The key lesson for the Smart Data Accelerator is that infrastructure design choices should be tested deliberately, with particular attention to technical standardisation, trust frameworks, proportional assurance, and interoperability. The ecosystem needs to remain scalable and flexible to support agentic finance as it develops.

Open finance infrastructure

This section sets out the three open finance infrastructure model families identified through the research: centralised, decentralised/federated, and hybrid. It first outlines the common foundations shared across all three models before examining the key characteristics and trade-offs of each approach.

Common foundations across all three models

The research identifies a set of common foundations that apply across all three infrastructure models. International examples suggest that successful regulated data-sharing ecosystems depend on shared standards, assurance, monitoring and trust mechanisms. These elements are therefore treated as constants across the centralised, hybrid and decentralised/federated models.

1

Digital verification, authentication, and delegated authorisation

The first common foundation is digital verification, authentication and delegated authorisation. In practice, this means customers can give a third-party app permission to access their financial data without handing over their password, and that app can confirm it is dealing with the right person. The report assumes the security protocols of OAuth 2.0 and OpenID Connect as constants that are complementary to each other. OAuth 2.0 supports delegated access, while OpenID Connect provides an interoperable identity layer. Testing could examine what additional information is needed where access is requested by an AI-enabled service, including its operator and scope of authority.

2

Strong user assurance

The second common foundation is strong user assurance. This means that for higher-risk actions, such as granting access to sensitive data or changing permissions, the system needs extra confidence that the person acting is who they claim to be: authentication should be anchored in Strong Customer Authentication (SCA)[ix]. Treating SCA as a baseline allows comparison to focus on how credentials are managed, assurance evidence is checked, and suspicious events feed into monitoring, revocation and liability.

3

High-assurance APIs and client security

The third common foundation is high-assurance APIs and client security. The research uses FAPI 2.0 as the security baseline for comparing sensitive open finance interactions, building on OAuth 2.0, supporting API security, client authentication and token protection[x]. This is the technical standard that determines how securely systems talk to each other and prove they are trustworthy when handling sensitive financial data. This allows the models to be compared on trust fabric questions, including who can participate, how credentials are recognised and how access is governed.

4

Assurance, monitoring, and revocation capabilities

The fourth common foundation is assurance, monitoring and revocation. This covers the ongoing checks needed to confirm participants remain trustworthy, spot problems early, and quickly cut off access if something goes wrong. All credible models need audit logging, conformance evidence, credential lifecycle management, operational monitoring and mechanisms for revoking access. Treating these as a baseline allows comparison to focus on which architectural choices provide better visibility, faster revocation, clearer evidence-sharing and proportionate monitoring.

5

Cryptographic agility and quantum resilience

This is about making sure the underlying security technology can be updated as threats evolve, including future risks from quantum computing, without breaking the system. The research suggests that considerations around cryptographic agility[xi] and quantum resilience[xii] are important for the future ecosystem. Open finance infrastructure may rely on signing keys[xiii], trust metadata, certificates, and secure transport mechanisms[xiv]. Architectures therefore need to consider adaptability over time instead of being locked into one set of cryptographic methods. This means using versioned keys[xv], planned migration paths[xvi], monitoring, testing, and rollback processes[xvii] so future changes can be introduced without breaking interoperability.

These common foundations provide a basis for comparative analysis between different models. By holding the baseline constant, comparisons can focus on core architecture questions and what varies most meaningfully. Without a baseline, differences in models could be confused with differences in security posture, technical maturity or implementation quality.

Centralised model

A centralised model features ecosystem functions that are concentrated in a single co-ordinating institution, or a tightly governed set of central services. This includes functions of participation, trust anchoring[xviii], authorisation, API access coordination, policy enforcement, and governance. The model does not require all data to be held centrally. Its defining feature is that the rules used to coordinate trust, access, and assurance across participants are centrally organised in a single control plane.

Technically, a centralised model operates across five linked layers:

1. Participant admission
2. Trust and credentialing
3. Consent and authorisation
4. API access coordination
5. Central monitoring and governance

At the participant layer, entry into the ecosystem is centrally controlled rather than contracted out to third parties. Within the trust layer, the model relies on a central

participant directory and managed credential lifecycle, so the authoritative list of participants, certificate issuance, validation, and revocation are concentrated in one place. At the consent and authorisation layer, users may still give permission through the customer journey, but the conditions under which consent is recognised, validated, and relied upon are standardised centrally. Within the API access layer, data remains with source institutions whilst access discovery[xix], trust validation, and conformance expectations[xx] are co-ordinated through common ecosystem rails. Finally, at the monitoring and governance layer, assurance becomes an operational function with components gathered through a common operational spine.

UAE Open Finance model

The UAE open finance framework is the main reference example for this model. The UAE approach is structured around a central trust framework, API hub, and common infrastructural services. Participation is mandatory for in-scope institutions, and core functions such as participant directories, certificate validation, and access through the API hub are coordinated centrally. This makes the UAE a useful example of a model that seeks to reduce fragmentation by creating a single set of ecosystem rails giving the Central Bank of the United Arab Emirates clear control over the ecosystem.

The research states that the centralised model is strongest for consistency, coordination, and rapid assurance. A central participant directory can provide a clear source of truth for who is authorised to participate. Centralised credential issuance and revocation can help ensure that compromised or non-compliant participants are suspended quickly across the ecosystem. The common API Hub also reduces variation in implementation by connecting to various data holders through a standardised interface.

These features are valuable where fragmentation could cause disproportionate cost, risk and uncertainty. The model also provides clear accountability. With ecosystem functions organised through a central control plane it is easier to identify those responsible for maintaining standards, monitoring operational performance, and co-ordinating incident response. This ensures trust and assurance are visible and enforceable.

However, the research highlights that the same features which make the centralised model attractive can also create risks. Concentrating trust, access coordination and revocation in one central layer can create operational dependency and concentration risk. If the central hub becomes a bottleneck, onboarding and change management may slow. If the central layer fails or is compromised, the impact could be felt across the whole ecosystem. The model may also create lock-in risks if participants become dependent on one operator, technical roadmap or fee structure. These risks are especially important in a UK context, where open finance and smart data may need to scale across multiple sectors, regulatory perimeters and institutional arrangements.

A further limitation is that centralisation may be harder to apply consistently across a broad open finance ecosystem rather than within a narrower or clearly defined perimeter. As open finance expands across different financial products, markets, and participant types, a single model of access, consent, accreditation, or technical coordination may not

reflect the specific requirements of each sector. While centralisation could improve consistency and assurance, it may also reduce flexibility where different parts of the financial services ecosystem require more tailored arrangements.

The centralised model demonstrates the benefits of strong coordination, standardisation and clear accountability, while also showing the risks of over-concentration, operational dependency and reduced sectoral flexibility. This allows us to consider core design needs, including the required common functions to support trust, resilience and interoperability, and those needed to preserve proportionality, flexibility and sector-specific innovation.

Federated/decentralised model

A decentralised or federated model is one in which the ecosystem operates through a common legal or policy framework, but without a single operational hub or central control plane coordinating all participants. Instead, responsibility is distributed across multiple authorities, standards bodies, market actors and participant implementations. In this model, interoperability depends on shared rules, mutual recognition, common technical standards and the ability of participants to implement those standards consistently.

European Union Second Payment Services Directive (PSD2)

The report uses the European open banking experience under PSD2 as the main comparator for this model, conscious of future developments as a result of the EU's Financial Data Access (FiDA) framework. PSD2 created a legal right for regulated third-party providers to access payment account data and initiate payments, subject to customer consent. However, it did not mandate a single technical API standard across Europe. This led to multiple standards and implementation approaches, including Berlin Group and STET, with variation across national markets and individual account providers. The PSD2 experience therefore shows that a common legal right of access does not automatically create a consistent operational ecosystem. It can, however, create opportunities for market-led initiatives to fill the gaps that a lack of standardisation leaves behind.

Agentic services may make these interoperability challenges more significant because they could depend on portable identity, machine-readable permissions and consistent approaches to the delegated authority. The PSD2 experience raised the question of whether legal access rights and distributed implementation are sufficient for AI-enabled services to operate across institutions.

The technical operating logic of this model is more distributed than in a centralised architecture. Participant authorisation and supervision may sit with different competent authorities or scheme actors. Trust and identification may rely on recognised certificates, registers or mutual recognition arrangements rather than one central trust anchor. API implementation is carried out by individual participants, often through different standards

or profiles. Consistency is therefore maintained through guidance, supervisory convergence, market coordination and standards alignment, rather than through a single ecosystem operator.

The main strength of a decentralised/federated model is flexibility. It can avoid dependency on a single central operator and allow different sectors or participant groups to adapt implementation to their own operational context. This may be valuable in a broader smart data environment, where different sectors may have different data types, customer journeys, regulatory requirements and levels of technical maturity. A distributed model can also support resilience by reducing reliance on one central infrastructure layer; the failure of one participant, interface or sectoral component does not necessarily prevent the whole ecosystem from functioning.

The model has the potential to encourage local innovation. Because implementation is not fully controlled through a single hub, standards communities and market actors may have more space to develop approaches that reflect specific use cases, products or sector needs. This can help preserve proportionality and adaptability, which are important if open finance and smart data are expected to support a wide range of firms, consumer journeys and future cross-sector services.

The research points to the potential risks of this model. For example, fragmented technical implementation can increase integration costs for third-party providers and make it harder for innovators to scale. Where API standards, user journeys, authentication flows and implementation quality vary, the practical value of data access rights can be reduced. In this sense, the research shows that decentralisation can create a gap between policy intent and operational delivery - access may exist in law but remain inconsistent or difficult to use in practice. A further limitation is the burden it places on governance and oversight. Where there is no single control plane, more effort is needed to align standards, monitor performance, identify obstacles and coordinate enforcement across participants.

Related to this, in a decentralised/federated model, trust portability[xxi] can also become harder. Participant status, accreditation, certificates, revocation and compliance signals may sit across different authorities or market actors, making it more difficult to ensure that trust information is current, machine-readable and consistently relied upon across the ecosystem.

For the UK, the decentralised model shows that flexibility and institutional fit matter, particularly in a broader smart data environment, but that this needs to be balanced against the need for common standards, reliable assurance and effective coordination.

Hybrid model

A hybrid model combines centralised coordination with distributed execution. It centralises the functions that benefit most from common assurance, such as:

- Accreditation
- Participant status
- Trust metadata
- Conformance

- Monitoring
- Revocation

Data custody, participant APIs, customer journeys and service delivery remain closer to firms, sectors and scheme participants. The value of the model lies in distinguishing between functions that require shared control and those that should remain distributed to preserve flexibility, proportionality and innovation.

Open finance and smart data will require stronger coordination than a loose federation but will be too complex and cross-sector for a single centralised hub to manage effectively over time. As the ecosystem expands across more products, actors, and sectors, the research suggests that the UK will need common standards and reliable assurance without forcing every function into one central operating model. The hybrid model offers a way to combine a robust common assurance spine with distributed implementation at the edge.

Australia's Consumer Data Right & Brazil's Open Finance Framework

Australia's CDR and Brazil's open finance regime are practical reference examples of hybrid design. Australia combines central accreditation, register services, conformance processes, and participant status controls with distributed data exchange between data holders and accredited recipients. Brazil similarly combines strong central governance, common standards, and participant obligations with dedicated interfaces operated by individual institutions. In both cases, trust and standards are coordinated centrally, but the data exchange and customer-facing journeys remain distributed.

The technical operating logic of a hybrid model is built around separating the trust and assurance layer from the execution layer. At the governance and accreditation layer, a central or commonly recognised authority determines who can participate and under what conditions. Within the trust metadata layer, shared registers, certificates, or signed trust information allow participants to identify and rely on each other. At the implementation layer, data holders, and service providers continue to operate their own APIs and customer journeys. Within the consent and authorisation layer, common rules define what valid consent and permissions should look like, but the user interaction may still take place through firm or sector-specific channels. At the monitoring and lifecycle layer, common observability, confirmation and revocation processes help ensure that distributed execution remains accountable.

This structure gives the hybrid model several strengths. It can reduce fragmentation by centralising the parts of the ecosystem where inconsistency would create the greatest risk, such as accreditation, participant status, trust metadata and revocation. It can also preserve flexibility by allowing firms and sectors to manage data custody, product-specific APIs and customer journeys in ways that reflect their own use cases and operational realities. This is particularly relevant for the UK because open finance is likely to involve different product markets, regulatory perimeters and potentially wider smart

data sectors, each with different data types, consumer needs and implementation constraints.

A further strength is that the hybrid model can support a more scalable approach to trust. The report identifies OpenID Federation[xxii] as a possible future-state architectural pattern because it could allow multiple trust anchors to coexist across different domains, which in practice means different sectors could each run their own trust arrangements while still recognising each other's participants. This matters for a future smart data ecosystem in which different regulators, sector authorities or scheme bodies may need to anchor trust in their own areas, while still enabling firms to operate across them. In practical terms, OpenID Federation could support portable trust across different use cases, including the exchange of information about an AI-enabled service's verification and authority, without requiring a single trust anchor for every interaction.

The research also highlights governance complexity as the main challenge of the hybrid model. Because responsibility is split between central and distributed actors, the model needs clear rules about who sets standards, who validates accreditation, who publishes trust metadata, who monitors performance, who handles incidents, and who has authority to suspend or revoke access. Without clarity in the allocation of responsibility and guidance for the ecosystem, the research points to a hybrid model that could inherit the weaknesses of both centralised and federated approaches - bottlenecks in the central layer and inconsistent implementation at the edge.

There is also a risk that distributed execution creates uneven user journeys or inconsistent technical performance if the common assurance layer is not strong enough. Australia and Brazil both show that hybrid regimes require ongoing monitoring, conformance and governance to maintain quality as participation scales. The model therefore depends on the central functions being treated as genuine infrastructure, not simply as coordination forums. Common standards, trust metadata, participant status, monitoring and revocation need to be operationally robust if distributed implementation is to remain reliable.

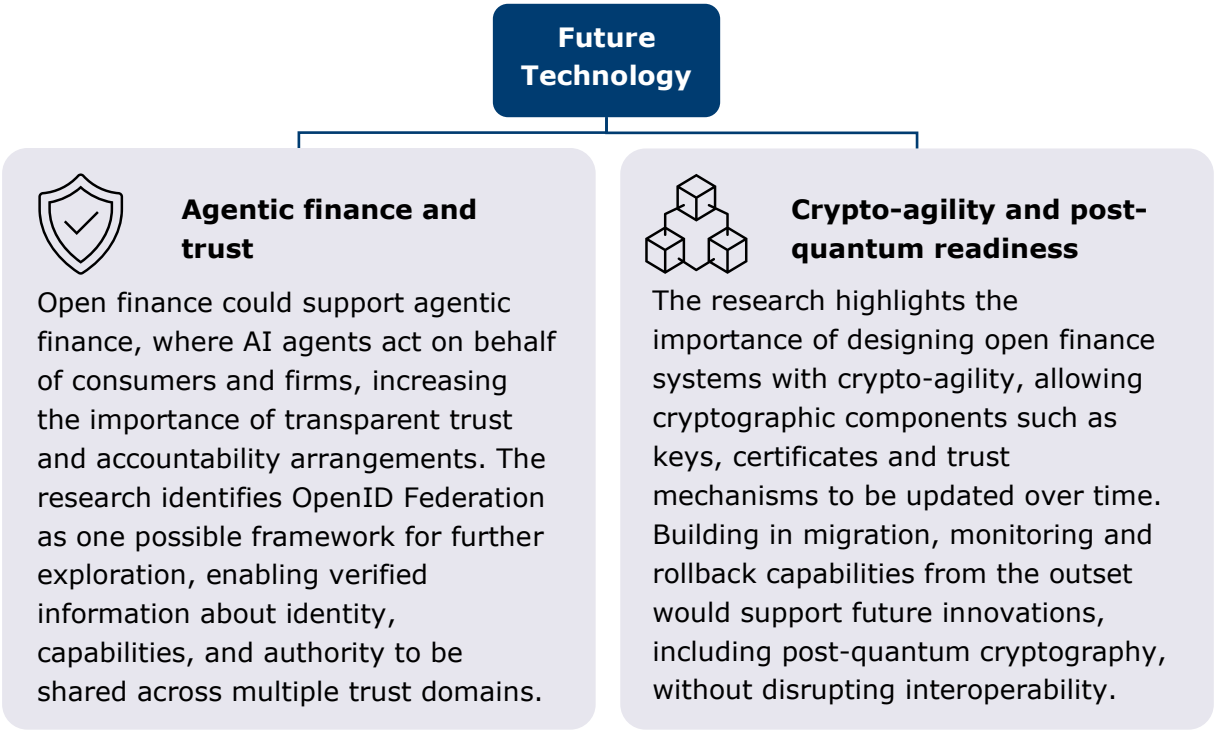
The hybrid model provides a relevant proposition for UK testing because no pure model addresses all the requirements identified by the research. A UK approach could centralise the functions that most require consistency and assurance, such as accreditation, participant status, trust metadata, conformance, monitoring and revocation, while keeping data custody, customer-facing journeys and sector-specific service logic distributed. Rather than choosing between a wholly centralised or decentralised approach, the key question for UK policy is which functions require central coordination and which are better delivered through distributed arrangements. The success of this approach would depend on the strength of the common assurance spine, clear governance responsibilities, and the ability to maintain interoperability as the ecosystem expands across products, firms and sectors.

Future technology interoperability

The research identified that the technology landscape is changing rapidly as emerging technologies such as artificial intelligence and quantum continue to grow. Artificial intelligence may change both how open finance data is accessed and what an authorised service can do with it.

An AI-enabled service could interpret data from several providers and then make recommendations and potentially take actions so interoperable identity, delegation, monitoring, and revocation become increasingly important. The Mills Review further underscores how data and data sharing are the foundation for a future agentic finance ecosystem, with open finance infrastructure as a key enabler.

This research states it is imperative that the open finance infrastructure remains interoperable as technology evolves independent of the infrastructure that is selected. This will enable the underlying trust architecture to accommodate new forms of identity, delegation, security, and cross-sector data sharing without undermining interoperability. The research sets out two areas that are particularly important: AI and quantum.



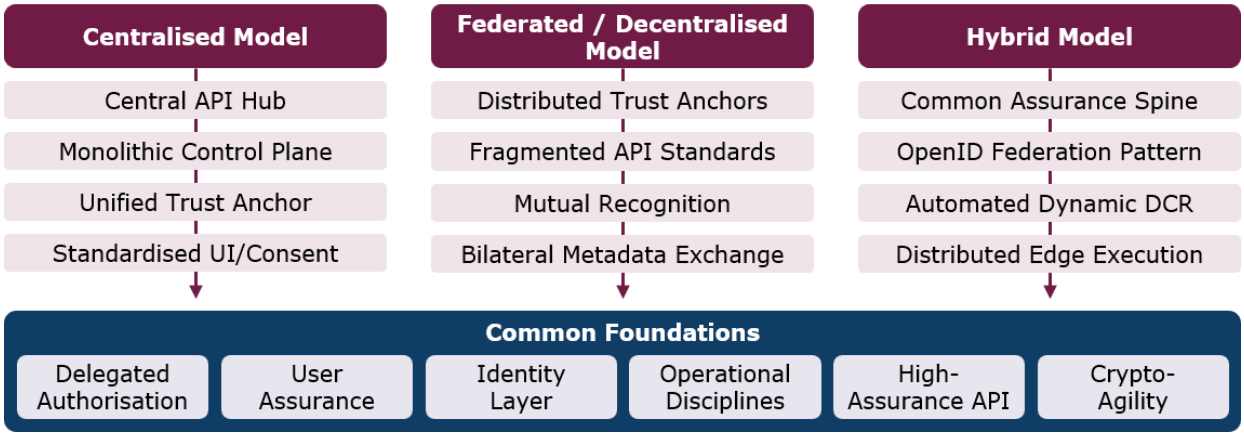
Comparative synthesis

The three models display how different infrastructure functions can work when sat within different architectures. The research implies that the design question facing UK open finance is which infrastructure functions require common coordination, and which should remain distributed to preserve flexibility, proportionality, and innovation. That is the core value of the research, as it moves away from abstract models and towards operational choices that determine the trust, scalability and interoperability of open finance.

The centralised model demonstrates the benefit of strong coordination. A common control plane can support clearer accountability, consistent standards, fast revocation, and stronger ecosystem-wide assurance. This is particularly important for those functions where fragmentation creates risk, such as accreditation, participant status, trust metadata, monitoring, and incident response. A single hub may create operational dependency, bottlenecks, and reduced flexibility, particularly as open finance expands into more products, sectors and smart data use cases.

The decentralised/federated model demonstrates the opposite trade-off, the value of flexibility, institutional adaptability, and resilience by distribution. This is displayed as attractive where different sectors, regulators, or market participants need space to develop approaches suited to their own context. The EU PSD2 experience shows that legal access rights alone do not guarantee practical interoperability. Without sufficient coordinating standards, trust signals, and implementation requirements, decentralised models can lead to fragmentation, inconsistent user journeys, higher integration costs and a heavier supervisory burden.

The hybrid model is suggested to be the most useful reference point for UK sequencing. It shows how the UK could combine the strongest elements of the two other models: centralised assurance where consistency and trust are essential, and distributed execution where flexibility, proportionality, and sector-specific innovation matter. In this model, functions such as accreditation, participant status, trust metadata, conformance, monitoring and revocation could be coordinated through a common assurance spine, whilst data custody, APIs, customer journeys, and service delivery remain distributed across firms and sectors.



The research points out that OpenID Federation may provide an example of a future state for supporting portable trust across multiple domains especially as open finance evolves towards wider smart data use cases. The research highlights that the UK is unlikely to be best served by a pure model, and a credible path is more likely to involve a combination of centralised, hybrid, and federated elements, sequenced over time. The immediate priority for the Smart Data Accelerator is to understand where common coordination is essential to support trust, resilience and interoperability, and where distributed implementation is needed to maintain flexibility and innovation. This identifies a clear basis for moving from conceptual model design and towards evidence-led decisions about the future infrastructure of open finance and smart data.

Next steps and testing priorities

The next phase of work will test the reference architecture through practical use cases, including participant verification, permission journeys, trust metadata, monitoring, revocation, and interoperability. Testing could also examine how authority is delegated to an AI-enabled service, interpreted across institutions and withdrawn by a consumer. The findings will identify technical, operational, and governance frictions for further consideration.

Appendix

International case studies

Comparative analysis enables the research to explore design patterns and implementation bottlenecks, in addition to understanding the governance and technical trade-offs in different architectural approaches. The research explores the approaches of Brazil's Open Finance framework, Australia's Consumer Data Right (CDR), the European Union's PSD2 regime and the United Arab Emirates' open finance model to understand what lessons can be learnt for the UK. The research points out that no existing international model provides a transferable blueprint for the UK, but the analysis surfaces real-world implementation opportunities and constraints that can inform UK infrastructure design. It recognises that there are many examples worldwide that can provide useful insights, and the four used in this research are just reference points. The international examples also help illustrate the three infrastructure model families considered in the report: the UAE is most relevant to the centralised model, Australia and Brazil are most relevant to the hybrid model, and the EU's PSD2 regime is most relevant to the decentralised or federated model.

Country/regime	Model family	Lesson for the UK
UAE	Centralised	Strong central coordination reduces fragmentation but raises questions about concentration risk and scalability.
Australia (CDR)	Hybrid	High-assurance accreditation and central coordination work well but can create onboarding burdens for smaller firms.
Brazil	Hybrid	Phased, standardised expansion under strong central governance avoids siloed development as scope grows.
EU (PSD2)	Decentralised/federated	A legal right to data access does not guarantee consistent, interoperable implementation without stronger coordinating standards.

The research identifies that strong standardisation matters early. Technical co-ordination is just as important as policy decisions, as legal rights to access data do not, on their own, create interoperability. Brazil highlights the value of standardisation through a phased technical expansion strategy that began with open data about businesses before expanding to consumer data sharing, enabled payment initiation and, finally, specialised data such as investments and insurance. The system relies on standardised API structures conforming to the Central Bank of Brazil's specification, helping avoid the siloed development the UK will need to manage as open finance expands.

This makes Brazil an important hybrid comparator, as it combines strong central co-ordination and common standards with distributed implementation by ecosystem participants. The EU's PSD2 experience reinforces the importance of standardisation from the opposite direction. PSD2 created a legal framework for account information and payment initiation access, but did not mandate a single technical API standard. Multiple standards emerged, including Berlin Group and STET, with varied implementation across national markets and account providers.

This demonstrates that legal openness is insufficient where implementation is fragmented, as third-party providers can face high integration costs, inconsistent user journeys and uneven API performance. For this reason, PSD2 provides the clearest comparator for the decentralised or federated model, showing both the flexibility of a legal access framework and the risks of weaker interoperability when technical implementation is not sufficiently co-ordinated.

The research further highlights that trust and governance architectures are interdependent, as the chosen architecture will decide who holds power to grant, monitor and withdraw participation in the ecosystem. Australia's CDR illustrates this through central co-ordination, accreditation arrangements, a participant register and Public Key Infrastructure[xxiii]. If a participant's accreditation is revoked, that status can propagate through the ecosystem and terminate access. This highlights that the technical trust anchor must be designed with the governance framework, so technical controls can support accreditation, enforcement, monitoring and revocation in practice.

Australia is therefore best understood as a hybrid comparator, because it combines central assurance functions with distributed execution by accredited participants. Shifting from open banking to open finance and smart data increases the governance and interoperability demands. As data sharing expands to new products, asset classes and sectors, more effort is required to ensure interoperability, consistent assurance and cross-sector governance.

The UAE designed its open finance model with a broad financial scope from the outset, covering banking, insurance, investments and service initiation through a centralised trust framework, API hub and common infrastructure services. This makes the UAE the clearest comparator for the centralised model. It highlights how strong co-ordination and common infrastructure can reduce implementation friction, whilst also raising questions about concentration risk, scalability and UK institutional fit.

Additionally, the research suggests that co-ordination improves assurance but has associated operational costs. Strong accreditation, common registers and rigorous security controls can improve trust and resilience but also increase cost and complexity. Australia's CDR provides a clear example: its security-first design, rigorous accreditation, Public Key Infrastructure requirements and use of mutual Transport Layer Security support high assurance but can create onboarding burdens for smaller fintechs and mid-sized participants.

The research suggests that, for the UK, we need to consider how to balance the robustness of assurance and protection of the ecosystem with proportionality and barriers to entry. No existing international model is fully replicable for the UK, as each comparator reflects different institutional conditions, market structures and regulatory traditions. Brazil demonstrates the benefits of broad scope, phased expansion and strong

governance co-ordination; Australia shows the value and cost of high-assurance accreditation within a hybrid ecosystem; PSD2 highlights the risks of fragmented implementation in a decentralised or federated model; and the UAE highlights the strengths and limitations of a centralised hub model. None fully replicate the current UK ecosystem. The research highlights that the UK should recognise the lessons from other jurisdictions without replicating them, and should build future-proofed infrastructure that is flexible enough to account for evolving requirements.

Glossary of terms

[i] Trust Metadata is machine-readable information about a participant's identity, status, capabilities, authority, or assurance level that allows other participants to decide whether and how to rely on it.

[ii] Consent is a person's informed and freely given agreement to a specified use or sharing of their data. Consent records the individual's choice but does not, by itself, determine whether every resulting action is technically or legally permitted.

[iii] OAuth 2.0 is a framework that enables a user to authorise a third party to access specified resources without sharing the user's login credentials with that third party

[iv] OpenID Connect is an identity layer used with OAuth2.0 that enables a system to authenticate an end user and receive standardised information about that user.

[v] Financial-grade API (FAPI) is a security profile based on established standards including OAuth 2.0 and OpenID Connect, designed to provide stronger protection for high-risk or sensitive API interactions.

[vi] Common assurance is a shared set of standards, controls, and evidence used to confirm that participants and their systems meet the ecosystem's technical, security, and operational requirements.

[vii] Monitoring is the ongoing observation of participants, systems, and services to identify performance, security, compliance or operational issues.

[viii] Revocation is the process of withdrawing a participant's credential, status, permission, or access so that it can no longer be relied upon within the ecosystem. Consent revocation is the process through which a person withdraws previously given consent for their data to be accessed, used or shared. Once revoked, the relevant access or data-sharing activity should cease, subject to any applicable legal or regulatory requirements.

[ix] Strong Customer Authentication (SCA) means authentication based on the use of two or more elements that are independent, in that the breach of one element does not compromise the reliability of any other element, and designed in such a way as to protect the confidentiality of the authentication data, with the elements falling into two or more of the following categories— (a) something known only by the payment service user ("knowledge"); (b) something held only by the payment service user ("possession"); (c) something inherent to the payment service user ("inherence");

[x] Token protections are the security controls used to prevent access tokens from being intercepted, altered, stolen or used by an unauthorised party. These controls help ensure that a token is accepted only for its intended recipient, purpose and period of validity.

[xi] Cryptographic agility is the ability of infrastructure to replace or update cryptographic methods, keys and certificates without causing significant disruption or undermining interoperability.

[xii] Quantum resilience is the capacity of infrastructure to adapt to or withstand security risks arising from advances in quantum computing

[xiii] Signing keys are cryptographic keys used to create digital signatures that confirm the authenticity and integrity of data, messages, or credentials.

[xiv] Secure Transport Mechanisms are technical controls that protect data whilst it is transmitted between systems, helping to prevent unauthorised access, interception, or alteration.

[xv] Versioned keys are cryptographic keys assigned a version identifier so that systems can distinguish between current and previous keys and manage updates without disrupting interoperability.

[xvi] Planned migration paths are predefined arrangements for moving from one cryptographic method, key, or technical standard to another whilst maintaining security, continuity and interoperability.

[xvii] Rollback processes are procedures for returning to a previous stable key, cryptographic method, or system configuration if a change causes security, operational, or interoperability problems.

[xviii] A trust anchor is an authoritative entity, credential or source of information that provides the starting point from which trust in other participants or information can be established.

[xix] Access discovery is the process through which an authorised participant identifies the data, services, and APIs available within an ecosystem, where they are located and how they can be accessed.

[xx] Conformance expectations are the agreed technical, security, and operational requirements that participants and their implementation are expected to meet. These may include compliance with common API specifications, security profiles, testing requirements, and ecosystem rules.

[xxi] Trust portability is the ability for evidence of identity, status, accreditation, or authority to be recognised and relied upon across different organisations, schemes, or sectors.

[xxii] OpenID Federation is a framework that enables separate trust domains to exchange and verify information about participants, their roles, and their authority through federated trust arrangements.

[xxiii] Public Key Infrastructure is a framework of digital certificates, cryptographic keys, policies, and processes used to establish identity and secure communications.

12 Endeavour Square, London, E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk