Thought Leadership:

Smart Data in the Age of AI: Why APIs Remain the Foundation of Innovation

RAIDIAM

Introduction:
Smart Data Meets Next-Gen Technology

The world is experiencing a seismic shift in how data is created, shared, and consumed. The global open data movement - once the domain of financial services and government transparency - is now intersecting with a wave of transformative technologies: artificial intelligence (AI), tokenisation, blockchain, digital wallets, digital identity, agentic AI, and large language models (LLMs). These innovations promise to unlock new value, drive efficiency, and empower consumers and businesses alike.

As these technologies mature, important questions are being raised:

- Is the foundational API and standards-based approach that underpins today's data ecosystems still the most appropriate solution for supporting the next generation of digital services?
- Or do we need a new paradigm to support the next generation of digital services?

The Global Smart Data Movement: A New Era of Opportunity

Across the world, governments and industry leaders are launching ambitious smart data initiatives to unlock the value of data for individuals, businesses, and society.

The UK's Data Use and Access Act, for example, is set to provide a legal and regulatory framework for smart data schemes across sectors - enabling consumers to securely share their data and access innovative services in finance, energy, telecoms, and beyond. Similar efforts are underway in the EU, Australia, Brazil, and other markets, all aiming to create interoperable, consumer-centric data ecosystems that drive competition, unlock growth and stimulate innovation.

These initiatives are not just about compliance - they are about building the infrastructure for a digital economy where data can flow securely and efficiently, empowering new business models, delivering tangible benefits to end users, and creating value for the providers who make it happen.

The Core Question: Can APIs Keep Up with AI and Blockchain?

With the emergence of agentic AI - autonomous systems acting on behalf of users - alongside innovations like tokenised assets and blockchain-based solutions, some in the industry are beginning to question whether APIs and existing standards can keep pace, and whether a new approach is needed to enable secure, scalable, and interoperable data exchange. This concern is understandable: as the diversity and complexity of data consumers increase, so too do the demands placed on the infrastructure that underpins consent-driven data sharing.

This question is not just theoretical. It reflects real uncertainty among financial services leaders, policymakers, and technology strategists. As organisations look to harness the power of AI, tokenisation, and digital identity, they must decide whether to build on the proven foundations of APIs and trust frameworks - or to pursue entirely new architectures.

The Enduring Value of APIs and Trust Frameworks in a Disruptive Era

Despite the rapid evolution of technology, the core challenge of smart data remains unchanged: enabling secure, open standards-based, consent-driven access to data, regardless of who - or what - is consuming it. Whether the consumer is a banking app, an AI agent, a digital wallet, or a technology yet to be imagined, the need for robust, scalable, and interoperable data sharing infrastructure is universal.

Why APIs and Standards Still Matter

APIs remain the most appropriate and reliable mechanism for enabling secure, scalable data exchange between organisations, sectors, and technologies.

Far from being outdated, APIs - when paired with robust trust frameworks and security protocols - continue to offer the most effective means of transferring data between parties with transparency, consent, and confidence.

> *The future of smart data isn’t about replacing what works - it’s about building on proven standards, frameworks and patterns that provide secure foundations to unlock new value for everyone, from AI agents to tokenised assets.*

Why APIs Work:

Separation of Concerns

APIs provide a clear structure for defining how systems interact - separating concerns between data format (e.g. JSON/XML), interaction methods (e.g. REST/GraphQL), and transport. This makes them inherently modular and easier to govern across complex, multi-party ecosystems.

Ubiquity of Consumption

APIs enable a consistent method of data exchange that can power a wide range of end points and user journeys - mobile apps, web applications, digital wallets, kiosks, embedded systems in cars or smart devices, and even agentic AI interfaces. This ubiquity makes APIs essential for omnichannel digital experiences.

Use Case Flexibility

APIs are inherently extensible, making them capable of supporting a wide array of use cases - ranging from open finance and digital ID to cross-sectoral smart data scenarios involving health, energy, and telecoms. They allow innovation without redesigning the foundations.

Security and Trust Controls

When implemented within a trust framework and governed by security standards such as OAuth 2.0 and OpenID Connect, APIs deliver controlled access, robust identity assurance, permissions, and auditability. These controls are critical for maintaining trust between data providers and consumers.

Support for Distributed and Centralised Models

APIs are agnostic to deployment architecture. They can support centralised hubs, decentralised peer-to-peer models, or hybrid federated networks - making them especially well-suited for global smart data environments where governance, resilience and scalability must coexist.

Accountability and Governance

APIs support traceability and operational control - ensuring clear lines of accountability when things go wrong. Consistent logging, version control, and permission scaffolding help detect misuse or data breaches and speed up resolution.

In short, APIs have proven to be the best tool not only for standardising and structuring how data is shared, but also for sustaining a uniform, secure flow of information across highly complex ecosystems. Their continued relevance in the face of disruptive technologies like AI, tokenisation and blockchain is a testament to their adaptability and enduring design principles.

Enabling the Next Generation of Smart Data

As organisations navigate the opportunities and challenges of AI, tokenisation, and digital identity, the need for secure, scalable, and interoperable data sharing has never been more pressing. Leading platforms, like **Raidiam Connect**, are evolving to meet these demands by providing:

Centralised Trust and Access

Raidiam Connect powers some of the world's leading open data networks. In Brazil, it underpins the Open Finance infrastructure connecting over 940 institutions and securing over 100 billion API calls annually.

Self-Service Onboarding and Automation

Raidiam Connect's intuitive tooling helps participants integrate rapidly. In New Zealand, this model delivered 95% banking market coverage across the payments sector in just six months.

Financial-Grade Security

Raidiam Connect implements layered security - including asymmetric authentication, certificate-based workflows, and rapid revocation systems - aligned with the FAPI 2.0 baseline, ensuring participants can isolate threats and respond in real time.

Shared Identity and Trust

Raidiam Connect enables major institutions to share verified identity attributes across participants, supporting real-time authorisation, consent enforcement, and seamless end-to-end journeys - including a live national digital identity exchange powered by major banks.

What does 'Financial-Grade Security' mean - and why does it matter?

'Financial-grade security' refers to protections defined by the **Financial-grade API (FAPI)** standard developed by the OpenID Foundation. FAPI is internationally recognised as the most robust API security profile - originally designed for financial services but now applied anywhere high-risk data is exchanged. It builds on secure authentication, authorisation, and consent management using advanced standards such as OAuth 2.0 and OpenID Connect, ensuring privacy, integrity, and rapid incident response across diverse sectors.

Interoperability and Federation: Building the Global Smart Data Network

Historically, open finance and smart data ecosystems have evolved as market-specific networks, designed to address domestic regulatory and industry needs. But the next major shift is already underway: connecting these ecosystems across borders through secure, standards-based federation.

Federation allows interoperability between previously separate schemes - financial networks, digital ID systems, sectoral smart data platforms - by enabling trust exchange based on common protocols and mutual recognition of accreditation, identity, and authorisation.

This vision is being realised using standards like OpenID Federation, which lets decentralised participants discover, authenticate, and connect across trust boundaries. This means that data providers and consumers - no matter where they operate - can interact securely using a federated trust and consent framework.

Raidiam is already supporting this future: its infrastructure enables cross-ecosystem collaboration within and across jurisdictions. Whether it's banks offering federated identity services, or fintechs connecting to multiple national open finance frameworks through a single set of credentials, these models demonstrate how federation translates from theory into operational readiness.

Why This Matters:

For individuals:
It enables truly seamless digital services across borders or sectors - no repeated onboarding, no new credentials for every service.

For institutions:
It reduces integration friction, enabling a single institution to serve multiple ecosystems with unified interfaces.

For regulators:
It ensures transparency, auditability, and compliance in distributed networks - while respecting local governance models.

> *Interoperability is no longer optional. It's the connective tissue of tomorrow's digital economy.*

Smart Data: Building on APIs for the AI and Tokenisation Era

The experience gained from open data initiatives provides a powerful blueprint for the future of smart data across sectors. The frameworks and standards that underpin today's financial data sharing ecosystems are not static; they are designed to be extended and adapted to support new use cases and technologies.

AI and LLMs:

The same API patterns and trust frameworks that enable secure data sharing for banking apps are now being adopted by cutting-edge AI companies. The Model Context Protocol, for example, allows AI agents to access external data using the standards pioneered for open banking - demonstrating that the infrastructure is ready for the next wave of innovation.

Tokenisation and Blockchain

APIs provide the bridge between traditional data systems and blockchain-based assets, enabling secure, consent-driven access to tokenised data.

Digital Identity and Wallet Ecosystems

APIs play a central role in enabling the issuance and presentation of digital credentials, such as mobile driver's licenses and digital IDs. Standards like OpenID for Verifiable Credentials (OpenID4VC) and OpenID for Verifiable Presentations (OpenID4VP) define interoperable protocols and APIs for credential issuance and presentation. These standards support global interoperability and secure credential exchange, laying the foundation for trusted, cross-border digital identity systems.

Addressing the Future: Interoperability, Security, and Innovation

As organisations look to the future, three priorities stand out: interoperability, security, and innovation.

Interoperability

API-based approaches support seamless data sharing across sectors and geographies, enabling organisations to participate in expanding digital federations and collaborative marketplaces.

Security

By leveraging asymmetric authenticated, centralised controls, and dynamic consent management, APIs and trust frameworks provide a resilient defence against emerging threats.

Innovation

The flexibility and extensibility of API standards mean that organisations can rapidly adopt new technologies - AI, tokenisation, digital identity - without having to rebuild their infrastructure from scratch.

Conclusion: APIs as the Foundation in a Tech-Driven World

The question is no longer whether open protocols and APIs will power tomorrow's digital infrastructure - they already do. The real challenge is whether organisations will build on nearly a decade of proven experience or risk repeating the expensive mistakes of the past.

A standards-based, API-driven approach - powered by trusted technology partners like Raidiam - remains the foundation for a secure, innovative, and inclusive smart data economy, even as AI, tokenisation, and blockchain reshape the landscape.

The infrastructure is ready. The standards are proven. The only question is: are you?

Frequently Asked Questions (FAQs)

Why are APIs still relevant in the age of AI, tokenisation, and blockchain?

APIs provide a universal, secure, and flexible way to enable data sharing and service access, regardless of the technology consuming the data. Their agnostic design and adherence to proven standards make them adaptable to new use cases - including AI agents, tokenised assets, and digital wallets - without requiring fundamental changes to the underlying infrastructure.

How do trust frameworks enhance the security of open data ecosystems?

Trust frameworks, built on protocols like OAuth 2.0 and OpenID Connect, ensure strong authentication, authorisation, and consent management. They allow organisations to control access to sensitive data, comply with regulatory requirements, and protect user privacy at scale, even as new technologies and threats emerge.

Can APIs and existing standards support future technologies we haven't imagined yet?

Yes. The strength of robust API standards is their agnosticism - they don't care what's consuming the service. This future-proof approach means that as new technologies emerge, they can be integrated into existing ecosystems without the need for wholesale infrastructure changes.

What is the business case for investing in standards-based platforms like Raidiam Connect?

Organisations benefit from reduced implementation costs, future-proof infrastructure, proven scalability, and the ability to participate in multi-sectoral data sharing schemes. Governments and enterprises can accelerate innovation, maximise infrastructure investments, and ensure cross-sectoral and cross-border compatibility with emerging global standards.

How do APIs enable interoperability across sectors and geographies?

API-based approaches support seamless data sharing across sectors and geographies, enabling organisations to participate in expanding digital federations and multi-sectoral data sharing schemes. This interoperability is essential for building smart data ecosystems that can adapt to new business models and regulatory environments.

How does Raidiam support digital identity and consent management?

Raidiam provides and operates the enabling trust framework infrastructure for national digital identity schemes, working alongside other organisations to help define the standards that will govern digital credentials across multiple countries. Its solutions enable secure digital identity verification and dynamic consent management for a wide range of use cases.

Frequently Asked Questions (FAQs) - continued

What makes APIs and trust frameworks “proven at scale”?

APIs and trust frameworks are already enabling secure access for AI agents, LLMs, tokenised data, and digital wallets in some of the world’s largest and most complex data ecosystems. For example, platforms like Raidiam Connect power national open finance initiatives, connecting hundreds of institutions and managing billions of API calls annually.

What are the key priorities for organisations looking to future-proof their data infrastructure?

- Interoperability: Ensuring seamless data sharing across sectors and geographies.
- Security: Leveraging asymmetric authenticated, centralised controls, and dynamic consent management.
- Innovation: Adopting flexible, extensible API standards to rapidly integrate new technologies without rebuilding infrastructure.

Is a new paradigm needed, or can APIs evolve to meet future demands?

While technology will continue to evolve, the foundational principles of secure, consent-driven data access remain unchanged. APIs and trust frameworks are designed to be extended and adapted, making them well-suited to support the next generation of digital services - including those powered by AI, tokenisation, and blockchain.

How can organisations get started with future-proofing their smart data strategy?

Begin by evaluating your current data sharing infrastructure and identifying opportunities to adopt standards-based APIs and trust frameworks. Partner with experienced technology providers, like Raidiam, to leverage proven platforms that offer scalability, security, and interoperability - ensuring your organisation is ready for the next wave of digital innovation.

Begin by evaluating your current data sharing infrastructure and identifying opportunities to adopt standards-based APIs and trust frameworks. Partner with experienced technology providers, like Raidiam, to leverage proven platforms that offer scalability, security, and interoperability - ensuring your organisation is ready for the next wave of digital innovation.

Sources for *Smart Data in the Age of AI*

This article draws on a combination of publicly available materials, including standards documentation, and information about industry initiatives. Below is a representative list of sources and references used in researching and preparing the piece:

Primary Legislation and Government Initiatives

- UK Data Use and Access Act (draft and explanatory notes)
- European Union Digital Identity Framework and EU Digital Identity Wallet program
- Australian Consumer Data Right (CDR) legislation and implementation updates
- Brazil Open Finance national initiative documentation

Industry Standards and Technical Protocols

- OAuth 2.0 and OpenID Connect official specifications (OpenID Foundation)
- FAPI (Financial-grade API) and FAPI 2.0 working group publications (OpenID Foundation)
- OpenID for Verifiable Credentials (OpenID4VC) and OpenID for Verifiable Presentations (OpenID4VP) standards
- Model Context Protocol for AI agent access to external data

Market and Ecosystem Reports

- Raidiam Connect platform documentation, case studies, and public whitepapers
- Open Banking Implementation Entity (OBIE) UK reports and technical papers
- Reports and technical notes from New Zealand Payments NZ on open API ecosystem deployment
- Public statements and briefings from national digital ID schemes in the EU and other regions

Industry Analysis and Commentary

- "Global Open Finance Networks" article by Barry O'Donohoe, CEO of Raidiam, LinkedIn, 2024
- Consultancy and sector reports (e.g., Deloitte, McKinsey, OIX) on open data, smart data, and digital trust frameworks
- Industry blogs, public technical presentations, and webinars on emerging technologies (LLMs, agentic AI, secure multiparty computation, TEEs, blockchain integration)

Technical and Market Benchmarks

- OpenID Foundation technical interoperability test results
- PCI DSS 4.0 compliance information for secure API implementations
- Public metrics on API usage and participant onboarding in national open finance ecosystems

RAIDIAM

raidiam.com