iSHARE + EDC/IDSA Managed Services: A Commercial Opportunity for Cross-Silo Data Sharing

Executive Summary

Data spaces are rapidly emerging across Europe as the foundation for trusted data exchange in every sector—from energy and mobility to healthcare, logistics, and manufacturing. Yet, each sector today still builds its own siloed infrastructure for onboarding, authorization, and credential management. This fragmentation creates duplicated costs, inconsistent governance, and slower adoption.

Managed Service Providers (MSPs) such as **KPN**, **T-Systems**, **Orange Business**, or similar infrastructure providers are in a prime position to change this dynamic. By combining the **iSHARE Trust Framework** with the **Eclipse Dataspace Connector (EDC)** and the **International Data Spaces Association (IDSA)** standards — including the **Data Space Protocol (DSP)** and **Decentralized Claims Protocol (DCP)** — MSPs can deliver a **harmonised managed service** that serves all data spaces through a single, interoperable trust and data exchange layer.

This aligns directly with the **iSHARE Foundation's Mission Partner initiative**, which invites major infrastructure and technology providers to champion interoperable, secure, and ethical data sharing across borders. MSPs operating such managed services will be both enablers of sovereignty and commercial beneficiaries of the growing data economy.

1. Why a Cross-Silo Managed Service Matters

Today’s landscape of data spaces is fragmented: - Each initiative (Gaia-X, Catena-X, Mobility Data Space, Smart City, Energy, Agri-Food, etc.) builds its own onboarding and trust infrastructure. - Participants must register separately, maintain multiple credentials, and comply with different trust rules. - This raises entry barriers for SMEs and delays interoperability between domains.

A **cross-silo managed trust and connectivity service** solves this by providing: 1. **One unified trust layer** — built on iSHARE legal and technical standards. 2. **Interoperable data connectors (EDC)** — implementing IDSA’s DSP and DCP protocols for secure, credential-aware data exchange. 3. **Credential portability** — using iSHARE v3.0 Verifiable Credentials (Participant and Delegation Rights Credentials) that can be reused across domains. 4. **Legal assurance** — governed by iSHARE certification and Terms of Use, providing liability and audit assurance across ecosystems.

This approach enables a European “trust fabric” operated by neutral managed service providers that already excel in secure infrastructure and identity management.

2. The Mission Partner Opportunity

According to the iSHARE Foundation, **Mission Partners** are infrastructure and technology providers that connect organisations across sectors and borders through trusted data sharing. They drive the harmonisation of standards and governance across ecosystems, promote interoperability, and co-develop flagship cross-sector use cases that enable SMEs to participate in the digital economy.

For MSPs such as **KPN**, becoming an iSHARE Mission Partner means: - Taking a leadership role in **building the backbone of Europe's trusted data economy**. - Helping **standardise the onboarding and credential management process** for all data spaces. - Demonstrating **cross-sector interoperability** through managed trust infrastructure. - Co-developing use cases that scale impact and adoption across industries.

3. Technical Foundation: iSHARE + IDSA Integration

iSHARE: The Trust Framework

- Defines roles, legal agreements, and APIs for **Participant Registries (PR)** and **Authorization Registries (AR)**.
- Provides a cross-domain **legal trust framework** for data rights and participant validation.
- Uses **Hyperledger Fabric** as the governance ledger for immutable issuance records and non-repudiation.
- Evolving from OAuth 2.0 / JWT-based credentials to **DID- and VC-based credentials** (v3.0) under did.ishare.eu.

IDSA Data Space Protocol (DSP)

- Handles the **data exchange layer**, ensuring policy-compliant transfer between data connectors.
- The **Eclipse Dataspace Connector (EDC)** is the open-source reference implementation of DSP.
- It validates access control through policies linked to iSHARE Delegation Credentials.

IDSA Decentralized Claims Protocol (DCP)

- Provides the **identity and credential exchange layer**, enabling connectors to present and verify Verifiable Credentials.
- iSHARE v3.0 integrates with DCP to provide **Participant Credentials** and **Delegation Rights Credentials**, giving data connectors verifiable, interoperable proofs of identity and authorization.

Combined iSHARE–IDSA Stack

Layer	Standard	Implementation
Trust & Governance	iSHARE Framework	Participant & Authorization Registries (Hyperledger Fabric anchored)
Identity & Credentialing	IDSA DCP + iSHARE DID/VC	Participant & Delegation Rights Credentials
Data Exchange	IDSA DSP	EDC data plane + policy enforcement

This alignment delivers a **complete and harmonised technical and legal stack** that MSPs can operate as a single managed service offering.

4. Starting with the Core: Data Rights Holders First

The immediate opportunity for MSPs is to focus on **data rights holders** — the central actors in the **European Data Act** and **Data Governance Act**. These entities need trusted mechanisms to: - Prove ownership and control over data. - Delegate access and usage rights securely. - Ensure compliance with cross-border and sectoral governance frameworks.

iSHARE's **Authorization Registry (AR)** directly addresses these needs by managing **Delegation Rights Credentials** that record who is entitled to use which datasets, under what conditions, and for how long. Combined with the **Participant Registry (PR)** for organisational assurance, this provides a full trust layer aligned with the Data Act's legal obligations.

This rights-first approach allows MSPs to: - Start generating revenue immediately from credential issuance and delegation management. - Onboard data holders and consumers from any data space under a common governance model. - Build momentum and ecosystem trust before extending into infrastructure-level credentials or Gaia-X alignment.

5. Optional Future Integration: Gaia-X Clearinghouse Services

Once the data rights layer is operational, MSPs can expand into **infrastructure-level assurance** using **Gaia-X Clearinghouse Services**. These issue **Gaia-X Level Credentials** that attest to the compliance of infrastructure or service providers with Gaia-X’s security and sovereignty standards.

These credentials can later be used **as access conditions in iSHARE Delegation Rights Credentials**, for example: > “Access is granted only if the requesting infrastructure holds a valid Gaia-X Infrastructure Credential.”

This integration ensures that iSHARE Delegation Credentials not only govern **who may access data** but also **where and under what certified infrastructure conditions** it may be processed. However, it remains an **optional future enhancement**, enabling MSPs to phase adoption without dependency on Gaia-X from the start.

6. Legal Foundation of the iSHARE Ecosystem

The **iSHARE Trust Framework** is more than a technical standard—it is a legally binding ecosystem designed to ensure that every data transaction and delegation carries enforceable legal weight.

Legal Assurance and Non-Repudiation

- Each credential issued under iSHARE (Participant or Delegation Rights) is **digitally signed** and **anchored on Hyperledger Fabric**, providing immutable evidence of its origin, validity, and scope.
- Every transaction between participants using these credentials is **cryptographically verifiable**, ensuring **non-repudiation**—no party can deny having issued, received, or acted on a credential.
- The **Authorization Registry (AR)** acts as a legally accountable **Data Rights Credential Issuer**, maintaining a verifiable record of all delegations and their legal context.

Legal Coverage for Data Rights Holders

- The **iSHARE Terms of Use** and Certification Scheme provide a recognised **contractual and liability framework** for all participants.
- Data Rights Holders issuing or managing Delegation Rights Credentials gain **explicit legal protection**, as the iSHARE credential acts as an **enforceable declaration of rights and permissions**.
- Transactions recorded through the AR and verified via PR are **legally admissible** as proof of compliance with the **European Data Act** and **Data Governance Act**.
- This ensures that every actor in the ecosystem — from data provider to processor — operates under a transparent, auditable, and legally covered model.

In practice, this means that when an organisation issues a Delegation Rights Credential via an iSHARE-certified AR: 1. The delegation is logged immutably on the ledger. 2. The credential is signed under iSHARE legal authority. 3. Any use of that data can be validated, audited, and legally defended.

Through this structure, **iSHARE transforms technical authorisations into legally binding transactions**, creating the necessary legal backbone for compliant, cross-border, and cross-sector data sharing.

7. Commercial Opportunity for MSPs

Participant Registry (PR) Services

- **Annual Credential Subscription:** Yearly fees per registered organisation (e.g., €250–€500 per credential/year).
- **Compliance Packages:** KYC/KYB verification, SLA-backed services, and onboarding automation.
- **Ledger Anchoring Fees:** Micro-fees for credential anchoring transactions on Hyperledger Fabric.

Authorization Registry (AR) Services

- **Delegation Credential Issuance:** Charge per issued or verified Delegation Rights Credential (e.g., €0.05–€0.25 per event).
- **Subscription Tiers:** Bulk and enterprise plans for frequent delegators.
- **Governance Dashboards:** Optional premium audit and policy configuration tools.

Managed EDC Hosting

- Operate EDC nodes for participants unwilling to host their own connectors.
- Monthly fees (€50–€250 per node) covering maintenance, SLA, and credential processing.
- Optional per-transaction credential validation pricing.

Combined Data Space Packages

Offer bundled trust and exchange solutions combining PR, AR, and EDC hosting for: - **SMEs** (affordable compliance onboarding) - **Large enterprises** (dedicated managed connectors) - **Data space consortia** (turnkey governance + infrastructure stack)

8. Why MSPs Like KPN Are Best Positioned

MSPs already operate the backbone infrastructure that data spaces depend on: - Proven expertise in **network, identity, and cloud infrastructure management**. - Neutral governance position — ideal for multi-sector trust operations. - Strong regulatory, audit, and operational frameworks. - Alignment with **iSHARE’s Mission Partner values**: collaboration, interoperability, and ethical data sharing.

By adopting this model, **KPN** and similar providers can become the **European trust operators** that enable federated data exchange across all sectors.

9. Strategic Benefits

1. **Accelerates interoperability** across sectors via a unified trust and data exchange layer.
2. **Creates recurring revenue** through credential subscriptions, delegation fees, and hosting services.
3. **Reinforces EU digital sovereignty** through compliant, verifiable trust infrastructure.
4. **Reduces duplication and onboarding costs** across data spaces.
5. **Provides enforceable legal assurance** and non-repudiation for all data rights transactions.
6. **Enables phased evolution** — start with data rights and governance (iSHARE/IDSA) and expand later to infrastructure credentials (Gaia-X).

10. Recommended Next Steps

1. **Become an iSHARE Mission Partner** — formalise certification and alignment with the Foundation.
2. **Launch a Data Rights Pilot** — deploy managed PR/AR + EDC integration for data rights holders under the European Data Act.
3. **Develop a Commercial Catalog** — define subscription tiers and managed service offerings.
4. **Engage with iSHARE, IDSA, and Gaia-X** — coordinate phased interoperability and certification.
5. **Scale via Federation** — connect multiple PR/ARs through Hyperledger Fabric for a pan-European trust fabric.

11. Conclusion

The combination of the **iSHARE Trust Framework**, **IDSA Data Space Protocol**, and **Decentralized Claims Protocol** establishes a solid technical and legal foundation for interoperable data sharing across domains. Starting from the **data rights holder side**, MSPs can immediately deliver high-value, compliant trust services aligned with the **European Data Act** and **Data Governance Act**.

By embedding **legal assurance and non-repudiation** into every credential and transaction, iSHARE ensures that data rights holders operate under full legal protection — with verifiable, enforceable proof of who used what data, under which legal conditions. This creates a transparent, auditable environment for lawful data exchange across Europe.

In later stages, integration with **Gaia-X Clearinghouse credentials** will extend this legal trust model to include infrastructure-level assurance, resulting in a complete ecosystem of technical, operational, and legal trust.

This phased, standards-based approach creates a scalable business opportunity for Managed Service Providers like **KPN**, enabling them to become the backbone operators of Europe's trusted data economy — supporting every data space with verifiable, ethical, and legally covered managed services.