



Fraunhofer Cluster of Excellence
Cognitive Internet Technologies CCIT

Verifiable Credentials-Based Decentralized Master Data Management in Data Spaces

Enabling Trusted Master Data Exchange Across Organizational Boundaries

Management Summary

The importance of trustworthy, interoperable data spaces has become a strategic priority for business, administration, and research. Efficient master data management is a key prerequisite for their successful operation. However, increasing connectivity of heterogeneous actors, regulatory requirements, and high demands on data quality, data sovereignty, and transparency are pushing existing, centralized master data management approaches to their structural limits.

In federated data ecosystems in particular, redundant data storage, manual verification processes, and a lack of trust mechanisms lead to increased effort, limited scalability, and reduced interoperability. Against this background, the use of verifiable, cryptographically secured credentials is becoming increasingly important in order to establish trust between organizations without central data pooling or unnecessary disclosure of sensitive master data.

The project Verifiable Credentials for Master Data Sovereignty (VC4MDS) addresses these challenges by introducing a verifiable credential-based approach to decentralized master data management in data spaces. Building on self-sovereign identity standards, VC4MDS enables the exchange of master data attributes as verifiable credentials, ensuring data quality, timeliness, and validity while supporting data sovereignty and selective disclosure. The following report provides a systematic overview of the conceptual, technical, and economic potential of this approach and demonstrates how VC4MDS can be integrated into existing data space architectures and operated sustainably. It highlights both utilization models as well as governance and adoption aspects in order to demonstrate the potential of VC-based master data management as a key component of future, trustworthy data ecosystems.

Contents

1. Master Data Management in Data Spaces	4
1.1. Identification of legal entities	7
1.2. Analysis of Master Data Management in Data Spaces	8
1.3. VC-Based MDM in Data Spaces – Field Research	9
1.4. Current State and Requirements of MDM in Data Spaces	12
2. Decentralized Identities	13
2.1. Decentralized Identifiers	14
2.2. Issuer-Holder-Verifier Model	16
2.3. Verifiable Credentials and Verifiable Presentations	16
2.4. Credential Status Update	18
3. Trust Architecture	19
3.1. Core Principles of the Trust Architecture	20
3.2. Components of the Trust Architecture for MDM in Data Spaces	21
3.2.1. Participant Layer	21
3.2.2. Data Space Layer	21
3.2.3. Data Space Authority Layer	22
3.2.4. Trust Anchor Layer	22
3.2.5. Services Layer	22
4. Security Aspects of Decentralized MDM in Data Spaces	23
4.1. Verification and Linking	24
4.2. Issuance & Output	24
4.3. Organizational Requirements	25
4.4. Cryptographic Security	25
4.5. Lifetime & Validation Procedures	26
4.6. Revocation & Blocking Mechanisms	26
5. Verifiable Credentials-based MDM in Data Spaces	27
5.1. A Simple Example for Master Data Exchange with SSI Presentation	28
5.2. Complete Process of Master Data Exchange	30
5.3. Credential Revocation	31
5.4. Integration with the Data Space Components & Trust Architecture	32
6. Business Model and Utilization Plan	34
6.1. Scope and Objectives of the Business Model	35
6.2. Market Context and Stakeholder Landscape	35
6.2.1. Stakeholders in VC4MDS-enabled Data Spaces	35
6.2.2. Market Environment and External Influences	35
6.3. Value Proposition of VC-based Decentralized Master Data Management	36
6.3.1. Core Value Proposition	36
6.3.2. Status Quo	36
6.4. Utilization Models and Value Creation	37
6.5. Sustainability and Adoption Challenges	38
7. Further Research	39
8. References	41



1 Master Data Management in Data Spaces

The increasing importance of data-driven value creation in business, science, and administration is leading to a steadily growing demand for reliable, interoperable, and high-quality data. Efficient and consistent management of master data plays a central role, especially in distributed data ecosystems that are supported by a large number of independent actors. Master data—such as information on products, organizations, people, or geographical units—forms the basis for transactional and analytical processes. It is particularly well suited to serve as a common frame of reference between organizations.

In practice, however, master data management in data ecosystems presents specific challenges. Different data models, heterogeneous standards, and divergent governance structures lead to inconsistencies and make it difficult to use data sustainably across organizational boundaries. In addition, the exchange of sensitive or competitively relevant master data in data space is subject to special requirements in terms of data protection, data sovereignty, and trustworthiness. This problem is further exacerbated by the increasing dynamics in data ecosystems – for example, due to new partners, regulatory changes, or technological innovations.

The central problem is therefore to design master data management concepts and methods in such a way that they take into account the individual requirements of individual actors on the one hand, and enable the collaborative, interoperable, and sustainable use of master data in data space on the other. Without suitable approaches, there is a risk of fragmentation of the database, which significantly reduces the added value of data ecosystems and limits their scalability and innovation potential.

Master data management in data ecosystems is embedded in a complex, multidimensional context that is shaped by

technological, organizational, and regulatory conditions. Data spaces do not arise in isolation, but rather as part of overarching digitization strategies that are driven by both political and economic forces. Examples of this include Common European data spaces in the areas of mobility, health, or Industry 4.0. These developments illustrate that the ability to manage master data in a consistent, trustworthy, and interoperable manner is becoming a key prerequisite for the functionality of such data spaces.

The landscape of actors in data ecosystems is typically heterogeneous and comprises different roles with diverging interests and responsibilities:

- **Data providers** supply master data that they generate or maintain within their organization. They are responsible for the quality, completeness, and timeliness of this data.
- **Data users** access the master data provided in order to use it for their own business processes, analyses, or innovations. For them, the reliability and semantic comprehensibility of the data are particularly important.
- **Intermediaries and platform operators** create the technical and organizational infrastructures that enable the exchange and management of master data. These include interfaces, identity and access management, and data quality assurance services.
- **Regulatory bodies and standardization organizations** define legal frameworks, compliance requirements, and technical standards that significantly determine how master data may be exchanged and used.
- **Governance and community organizations**—such as consortia or industry initiatives—take on a coordinating role by developing common rules for data sovereignty, access rights, and interoperability.

The context is also characterized by a tension between **cooperation and competition**. On the one hand, the establishment of shared data spaces requires close cooperation between the players in order to establish standards and interfaces. On the other hand, there are often competing economic interests that can limit the scope and depth of data exchange. Master data management must therefore not only provide technological solutions, but also address socio-economic and institutional aspects in order to create acceptance and trust.

The success of master data management in data ecosystems depends largely on how successfully the different roles of the stakeholders and their interests can be embedded in a coherent framework that ensures both technical interoperability and organizational governance.

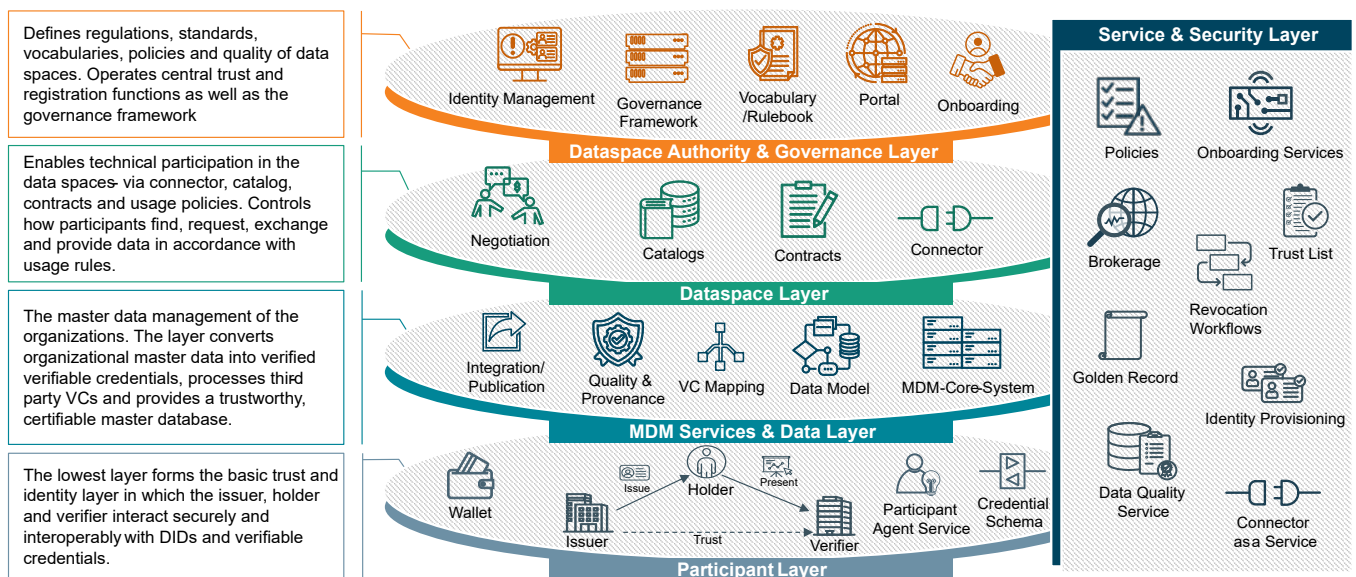


Figure 1: Layer Diagram of VC-based Master Data Management in Data Spaces

1.1. Identification of legal entities

The unambiguous identification of legal entities is a foundational requirement for legal certainty, regulatory compliance, and transparency in national and transnational economic activities. A range of complementary identification systems has emerged to address different regulatory, administrative, and market-driven needs, each providing standardized, machine-readable identifiers that support trust, interoperability, and efficiency in digital and physical transactions. While traditional numbering schemes remain central, newer models—particularly those grounded in electronic identities and trust services—reflect the growing importance of secure, verifiable, and cross-border digital interactions.

One of the most widely recognized identifiers is the Legal Entity Identifier (LEI), a 20-character alphanumeric code standardized by ISO 17442. Designed primarily for the global financial system, the LEI enables the unique, persistent identification of organizations engaged in financial transactions and reporting. With approximately 2.8 million active registrations worldwide and especially rapid growth in emerging markets such as India, the LEI has become essential for regulatory reporting, risk management, and transparency in ownership structures. Its tripartite structure—issuer prefix, entity-specific code, and verification checksum—ensures uniqueness and global interoperability while supporting annual renewal cycles that maintain data accuracy¹.

A second major system is the Data Universal Numbering System (D-U-N-S® number), a nine-digit identifier issued by Dun & Bradstreet. It is used by roughly 240 million entities across the public and private sectors, particularly for supply-chain visibility, compliance checks, international trade, and public procurement. Because the numerical sequence is randomly generated and semantically neutral, duplication is virtually impossible. The D-U-N-S® number enhances transparency in global commerce by linking organizations to one of the world's largest corporate databases, thereby improving data quality and enabling more reliable risk assessments².

In the context of customs and cross-border logistics within the European Union, the Economic Operators Registration and Identification (EORI) number provides uniform identification for all actors involved in customs procedures. By combining a member-state country code with a national reference number, the EORI facilitates streamlined import–export processes, secure information exchange, and harmonized communication with customs authorities. Participation in any customs-related activity within the EU requires possession of an EORI number, underscoring its regulatory centrality³.

Traditional national corporate registers also play a critical role. In Germany, the Handelsregisternummer assigns a unique identifier to companies upon entry into the commercial register, offering verifiable legal and economic transparency for contractual relations, disclosures, and business legitimacy. Complementing these national identifiers, the European Unique Identifier (EUID), introduced in 2017, connects national registers across the EU via the Business Registers Interconnection System (BRIS). Its structured format—consisting of a country code, register code, and national company number—supports accurate, cross-border reconciliation of company data and avoids duplication, thereby contributing to a unified European digital registry infrastructure⁴.

Other identifiers fulfill specialized regulatory or administrative functions. The Value Added Tax Identification Number (VAT ID or USt-ID) enables the correct treatment of cross-border goods and services within the EU's internal market, supporting tax compliance, reverse-charge procedures, and rapid verification of business status. The Wirtschafts-Identifikationsnummer (W-IdNr.), issued by the German Federal Central Tax Office, aims to provide a nationwide, uniform identifier for all economically active entities, facilitating digital public-sector processes and enabling once-only data exchange across registers⁵.

Furthermore, the Global Location Number (GLN), part of the GS1 system, provides a standardized method for identifying companies and their physical locations worldwide. By assigning unique 13-digit codes to sites such as headquarters, warehouses, or distribution centers, the GLN supports high-quality master data exchange and interoperable supply-chain operations. Its use in frameworks such as Peppol for electronic invoicing demonstrates its significance for automated, cross-organizational communication⁶.

Beyond numeric identifiers, the EU's eIDAS regulation establishes a comprehensive legal framework for electronic identification, authentication, and trust services. eIDAS enables secure, legally recognized digital transactions across member states by defining interoperable electronic IDs, qualified signatures, seals, and timestamps. This enhances security, reduces administrative friction, strengthens consumer and business trust, and allows organizations to scale digital services across the European Single Market. With its emphasis on cross-border recognition, integrity, and automation, eIDAS represents a pivotal step toward a unified European digital identity ecosystem.

Collectively, these identification systems form a multilayered infrastructure that supports regulatory oversight, risk mitigation, administrative efficiency, and trustworthy digital interaction in increasingly networked economic environments.

1.2. Analysis of Master Data Management in Data Spaces

Desk research and field research were conducted to assess the current status of master data management in data spaces and to identify requirements. The desk research involved analyzing scientific and gray literature on data spaces for requirements and information on master data management. The field research involved conducting interviews with experts from the data spaces. The results of the desk research can be found in this subchapter, and the results of the field research in the following subchapter.

The analysis of contemporary data space initiatives reveals a diverse landscape of domain-specific ecosystems that seek to enable secure, sovereign, and interoperable data exchange across industries. A prominent example is **Catena-X**, a data space tailored to the automotive sector and operated in cooperation with **Cofinity-X**, which provides an integrated framework for managing business-partner master data and exchanging certificates. Central to Catena-X is the **Business Partner Data Management (BPDM)** system, a distributed, service-based architecture built upon a shared central data pool adhering to Catena-X design principles. This pool is made available to participants in the form of a **Golden Record**, a harmonized, high-quality master-data representation intended to improve data quality, reduce rework, and lower overall operational costs. Companies can autonomously maintain their Golden Records, while Catena-X ensures standardized formats and trust mechanisms so that partner firms across the network can consume the shared data. Updates—such as changes in bank details—are propagated automatically to relevant parties while preserving anonymity, thereby eliminating the need for complex ERP integrations.

To enable members to upload, enrich, and distribute master data, Catena-X provides the **Business Partner Gate**, a standardized API that supports platform functionality through governance mechanisms addressing data consistency, data sovereignty, data quality, and interoperability. The API requires JSON over HTTP and enforces registration of records with the main service provider—for instance, via the type “cx-taxo:BPDMPool”—which grants controlled access to legally relevant entities, locations, and addresses. Only Catena-X members can access this pool, as external calls are not permitted.

Quality assurance and governance rules are integral to the Golden Record. To obtain a **Business Partner Number (BPN)**—a globally scalable identifier used across applications—datasets must conform to a standardized structure. Catena-X distinguishes among three partner types: legal entities (**BPNL**), sites (**BPNS**), and addresses (**BPNA**). The BPN structure consists of a prefix, a type character (L, S, or A), a ten-character alphanumeric entity identifier, and a two-character checksum, as illustrated by the example “BPNL 0000 0000 IF61.” The

underlying data model prescribes strict relational rules: each legal entity has at least one legal address; each site belongs to exactly one legal entity and must be associated with at least one address; each address is linked to exactly one legal entity and zero or one site; and multiple addresses or sites may be assigned to a single legal entity. Additional quality principles specify that each record must be classified as L, S, or A; that location-related information may only be defined by its owner; that modification histories must remain traceable; and that original inputs, proposed changes, and data sources must be preserved to guarantee transparency.

Beyond master data, Catena-X – through the **Eclipse Data Space Connector (EDC)**—supports certificate management and standardized certificate exchange (e.g., ISO, IATF, environmental certifications). These services reduce administrative and integration burdens, providing value to both SMEs and OEMs. SAP contributes an integration package that connects Catena-X BPDM with SAP Master Data Governance, enabling bidirectional data exchange during onboarding and ongoing operations. This integration also permits the aggregation of customer and supplier data outside the Catena-X network where appropriate consent exists.

Expanding beyond Catena-X, the **Manufacturing-X** initiative, funded by the German Federal Ministry for Economic Affairs and the European Union, aims to build federated data ecosystems across industries to enhance efficiency, strengthen supply-chain resilience, and preserve value creation. Manufacturing-X comprises multiple domain-specific projects, some of which strongly emphasize **Business Data Management**, while others address it only marginally or not at all. Projects with strong BDM components include Aerospace-X, Chem-X, CX-NEXT, Semiconductor-X, GrowING, and Wind-X; those that treat BDM only partially include Decide4Eco, Factory-X, HealthTrack-X, and HealthTrack-X’s use cases illustrate the practical relevance of standardized master data. Its objectives include: (1) optimizing business processes via automated provision of digital delivery documentation; (2) establishing shared standards for CO₂ accounting to support sustainability assessments across supply chains; and (3) enabling early prediction of supply bottlenecks through digitally connected logistics data.

Within the **Telekom Data Intelligence Hub (DIH)**, the **Digital.ID** component provides identity verification and identity management and functions as a verification node for Gaia-X compliance. Operated by T-Systems, Digital.ID integrates external conformity assessment bodies, authenticates master data by converting them into tamper-resistant W3C-compliant verifiable formats, supports unique identification for authentication and transactions, and ensures secure storage and processing of sensitive identity attributes.

The **European Health Data Space (EHDS)** constitutes a sector-specific ecosystem designed to improve individuals' control over their electronic health data while fostering research, innovation, and public-health applications. Although no explicit master-data management mechanisms are publicly defined, successful implementation depends on structured, consistent data and adherence to standardized documentation practices by healthcare providers, enabling high-quality analytics and cross-system interoperability.

Similarly, **sphin-X** seeks to build a secure, trustworthy data space for the healthcare sector, aiming to strengthen collaboration among stakeholders and promote responsible data use. While explicit master-data management services are not detailed, shared master data is identified as a central use case within project development.

In contrast, for several other emerging European data spaces—including the **Mobility Data Space**, **AgriDataSpace**, **Tourism Data Space**, and **Health-X dataLOFT**—no specific information regarding master-data management is currently available.

Overall, the analysed initiatives illustrate the increasing strategic relevance of standardized, high-quality master data within federated data ecosystems, as well as the variety of governance frameworks, technical architectures, and sectoral priorities shaping their implementation.

1.3. VC-Based MDM in Data Spaces – Field Research

To validate the theoretical insights obtained through desk research and to complement them with practical perspectives, a qualitative field study was conducted. The objective of this empirical component was to develop a deeper understanding of the current state, challenges, and future developments of master data management in data spaces based on verifiable credential (VC) technologies. The approach follows established principles of information systems research by emphasizing contextual depth and interpretive insight. All interview participants remain anonymized.

Methodology of the Field Research

The field research was conducted in the form of qualitative, semi-structured expert interviews. This methodology made it possible to address predefined thematic areas through targeted questions while simultaneously allowing room for open and in-depth discussion. As a result, individual experiences, assessments, and best practices could be captured that go beyond purely theoretical knowledge.

Three experts from different organizations and projects in the data space environment were interviewed. The experts are involved in data space initiatives in the automotive industry, mechanical engineering, and the healthcare sector. Participants were deliberately selected based on their professional expertise and active involvement in the development or implementation of data-space-related infrastructures.

The interviews were based on a guideline structured along six core analytical dimensions: (1) currently offered services and methods for master data management, (2) data models, (3) ensuring data quality and trustworthiness, (4) interoperability and connectivity, (5) future outlook, and (6) security-related aspects.

The combination of structured guidance and open response formats enabled both cross-interview comparability and the capture of individual perspectives and detailed domain knowledge. Particularly in the dynamic and innovative field of data spaces, this qualitative approach provides valuable insights into practical challenges, technical solution approaches, and strategic developments that are only partially reflected in the existing literature.

Interview Results I: Golden Record Service – Services and Methods for Master Data Management

The first interview describes the Golden Record Service as a core component of an industrial data space. It serves as a central instance for managing, verifying, and ensuring the quality of master data without requiring participating companies to disclose sensitive supply chain information. As the expert states, "The Golden Record Service gives participants the opportunity to provide their master data [...] as input data without disclosing their own supply chain to other data space participants." This approach addresses a fundamental tension in federated data ecosystems: balancing data sharing with data sovereignty. Data ownership remains with the respective data owners, while a shared, high-quality dataset is established at the ecosystem level.

Data Quality, Trustworthiness, and Security

Data quality is ensured through a multi-stage process that includes plausibility checks, external verification, and correlations across multiple sources. A key methodological principle is the so-called "intelligence of the crowd," where the frequency of consistent data entries serves as an indicator of correctness.

As the expert explains, “If, for example, six large OEMs regularly use the same address in their supply chain, the probability is high that it is correct – even if it is not the official legal address.”

Trust is thus generated through decentralized, repeated confirmation rather than centralized control. A major challenge identified is the activation of participants and the establishment of trust. According to the expert, “The whole approach only works if data space participants share their data. [...] As long as there are only one or two large participants, this is difficult.” This highlights the relevance of network effects, as the value of the service increases significantly with the number of participating actors.

Data quality assurance is implemented at several levels. Technically, all data transfers are secured via the Eclipse Data Connector, which handles authentication and authorization: “Every data transfer runs through the Eclipse Data Connector. It ensures exactly that: everyone who participates is authenticated and registered.” In addition, data are continuously validated and enriched using external sources: “We verify legal addresses via external data sources. [...] These data sets are validated by us as the Golden Record Service.” An anonymized quality indicator is used to assess correctness based on the frequency of matching entries: “If the same address is reported by ten members, the probability is high that it is correct. We label this with an anonymized quality indicator.” Data freshness is ensured through a hybrid model combining self-maintenance by data owners, collective change detection, and periodic revalidation by the operating entity: “Ideally, a data space participant maintains their data themselves quickly and correctly. [...] We also check the data ourselves at regular intervals – about twice a year.” Identity validation is handled separately via a Gaia-X-compliant clearing house: “Technically, we do not handle this ourselves. That is done by a Gaia-X clearing house.” Identity management and master data management are therefore “technically completely separated, but conceptually complementary.”

Data Model, Interoperability, and Outlook

The underlying data model follows a standardized structure with the three-level Business Partner Number classification described above: Legal Entity, Site, and Address. Official identifiers such as VAT IDs are considered indispensable: “For this, official identifiers are indispensable, for example a VAT ID or a commercial register entry. [...] This is comparable to a social security number.” Regarding interoperability, the service is described as fundamentally agnostic toward other data spaces: “The master data management of Catena-X is per se agnostic with regard to other data spaces.” However, a structural tension remains between federated governance and the necessity of a minimal central reference: “It is indispensable that there is a central ‘golden’ record somewhere. [...] The only thing we can do is ensure that the central part is as small as possible, but as large as necessary.” Looking ahead, the expert emphasizes that technological

excellence alone is insufficient. Participant activation and communication of ecosystem value are decisive: “Every master data project must ask itself: How do I activate participants? How do I communicate the added value of the ecosystem so that everyone understands it – and accepts the initial additional effort?” In particular, small and medium-sized enterprises could benefit significantly from shared master data services.

Interview Results II: TrustED Data Space in the Healthcare Context – Services, Data Models, and Trust Concepts

The second interview focuses on the TrustED project, which explores the management and controlled release of personal data based on self-sovereign identity (SSI) and verifiable credentials. Master data are framed as dynamic rather than static: “Data are not ‘immutable’. Their correctness can change over time.” A central principle is the use of verifiable presentations instead of full data disclosure. This allows an entity to confirm specific attributes without revealing the underlying data: “I do not want to disclose my data set, but I can confirm that I fall within a certain age or weight category. [...] This is possible via verifiable presentations.” Trusted issuers such as hospitals or public authorities act as trust anchors: “The hospital or a registration authority acts as a trusted issuer.” Data models are domain- and context-specific, particularly in healthcare. Relevant master data attributes depend on the use case: “Which master data are relevant always depends on the context.” Interoperability is achieved through established standards such as HL7 FHIR: “Harmonization is important here – for example via standards such as HL7 FHIR version 4B.”

Data Quality, Interoperability, and Security

Data quality is assessed through provenance and process transparency. The expert distinguishes between error quality and manipulation risk: “Is the value self-measured, recorded by a nurse, by a physician, or automatically determined? The accuracy depends on that.” Manipulation risks are also explicitly addressed: “There is the possibility of deliberately providing false information, for example to fraudulently obtain benefits from a health insurance provider.” Interoperability is described as a governance issue rather than a purely technical one: “For catalogs or metadata formats, it is the task of governance: anyone who wants to participate must comply with certain specifications.” Global standardization is viewed skeptically: “People will never fully agree on standards – at least not globally.” Instead, translation mechanisms between standards are considered unavoidable.

Security discussions focus on manipulation protection and the contextual definition of trusted authorities: “One could say: the government. But which government?” Current solutions rely on federated trust frameworks such as eIDAS and OID4VC, while many security mechanisms are still implemented in a use-case-specific manner.

Interview Results III: Decentralized Identity in Manufacturing-X – VC-Based Identity and Master Data Abstraction

The third interview adopts a strong SSI/VC perspective and explicitly differentiates it from classical master data management. The focus shifts from centralized registers to issuer-based, verifiable proofs. In this context, the BPN credential serves as a link between decentralized identifiers (DIDs) and the logical identification of a legal entity: “There is the BPN credential, in which you map the DID to a logical identification ID – [...] an ID issued by the operator.” The credential itself is intentionally minimalistic: “The credential actually contains only the BPN.” All further master data are managed externally and linked through subsequent resolution mechanisms.

Data Quality, Interoperability, and Future Vision

Data quality is ensured through issuer trust, cryptographic signatures, and credential lifecycle mechanisms such as refresh and revocation. The expert illustrates this using a banking example: “The bank confirms to the company that it is the holder of account number ABC. [...] If the bank revokes the credential, I see it immediately on the revocation list.” VC-based credentials are viewed as fundamentally data-space-independent and integrable into existing master data governance systems: “I do not even think that you necessarily need a data space for this. For master data governance, I would see this independently of the data space.”

Looking ahead, the expert anticipates a shift toward state- or EU-issued organizational identities: “As soon as there is an identity issued by the state, [...] I no longer need the operator. [...] The identity has to come from a state.” This is expected to result in significant efficiency gains, higher data quality, and reduced fraud.

Synthesis and Interpretation

The three expert interviews provide a consolidated view of the current state and future directions of VC-based master data management in data spaces. They represent perspectives from industrial practice, applied research, and technical architecture design. Despite these different viewpoints, consistent patterns emerge with regard to trust, governance, interoperability, and technological design.

Services and Methods

Across all interviews, master data management is understood as a socio-technical challenge rather than a purely technical task. Catena-X relies on a Golden Record service that ensures data quality through collective validation and shared reference data. The TrustED project follows a data-minimising, self-sovereign approach based on verifiable presentations, enabling

trust without data disclosure. The third interview introduces a decentralised identity layer via BPN credentials, reducing master data management to the verifiability of identities and attributes. Although conceptually different, all approaches shift trust away from central institutions toward verifiable, rule-based mechanisms.

Data Models and Harmonisation

The interviews reveal differing data-model strategies combined with a shared demand for standardisation. Catena-X applies a structured, industry-wide BPN model to ensure interoperability within its data space. In healthcare, data harmonisation is achieved through domain standards such as HL7 FHIR and remains strongly context-dependent. The decentralised-identity perspective decouples identity from domain data by keeping credentials intentionally minimal. This creates a tension between semantic richness and cross-domain interoperability, which can only be addressed through translation and mapping mechanisms.

Data Quality and Trustworthiness

Complementary trust mechanisms emerge across the interviews. Catena-X applies collective quality assurance based on convergence across participants and external validations. The TrustED project evaluates quality through provenance and measurement processes. The decentralised-identity approach relies on issuer-based credentials with cryptographic lifecycle control. Together, these approaches form a layered trust model combining network validation, source-based assessment, and technically enforced validity.

Interoperability and Connectivity

All experts emphasise that interoperability depends on governance as much as on technology. While Catena-X enforces interoperability through mandatory models and connectors, TrustED highlights governance rules as participation requirements. VC-based credentials, as described in the third interview, enable platform- and data-space-independent integration, indicating a shift from data-space-internal interoperability toward cross-data-space structures.

Future Outlook and Security

Future success is expected to depend primarily on trust, participant activation, and governance. Global standardisation is considered unrealistic; instead, translation between standards and public or state-backed trust infrastructures are seen as key enablers. Security is addressed on two levels: technical trust infrastructures (DIDs, signatures, revocation) and institutional trust anchors (clearing houses, governance). Coordinating both is essential to balance federated principles with the need for reliable reference points.

Overall, the interviews indicate a paradigm shift in master data management within data spaces, from central data repositories toward verifiable, context-sensitive proofs. Classical master data functions are increasingly complemented by cryptographic and

institutional trust mechanisms. The central challenge lies not in technological maturity, but in institutionalisation, governance, and economic incentives. Only when these dimensions are aligned can the full potential of VC-based master data management in data spaces be realised.

1.4. Current State and Requirements of MDM in Data Spaces

The combined analysis of desk research and field research provides a comprehensive understanding of the current state, challenges, and requirements of master data management in data spaces, particularly in relation to VC technologies. While the desk research offers a broad, systematic view of existing initiatives, architectures, and standards, the field research enriches these findings with practical insights from ongoing implementations and expert experience. Together, both perspectives reveal converging patterns and highlight key requirements for sustainable, scalable MDM in federated data ecosystems.

A key convergence lies in the importance of standardized identifiers and data models. Desk research highlights the role of the Business Partner Number (BPN) in Catena-X as a globally scalable identifier that enables interoperability across applications and organizations. The interviews confirm the practical relevance of such identifiers while also exposing architectural trade-offs. Industrial practice favors semantically rich, standardized data models to enable immediate reuse within a data space, whereas VC- and SSI-oriented approaches advocate intentionally minimal credentials that separate identity from domain-specific master data. This tension between semantic depth and abstraction emerges as a fundamental design challenge, implying a requirement for translation mechanisms, mappings, and layered architectures that can support both domain specificity and cross-data-space interoperability.

Both desk and field research emphasize that data quality and trustworthiness are central value drivers of MDM in data spaces. Desk research illustrates how initiatives like Catena-X institutionalize quality through governance rules, standardized schemas, and shared Golden Records. Field research complements this by revealing multiple, coexisting trust mechanisms: collective validation through network effects, provenance- and process-based quality assessment, and issuer-centric, cryptographically secured credentials with lifecycle management (revocation and refresh). The synthesis indicates that no single mechanism is sufficient; instead, robust MDM requires a multi-layered trust model combining technical enforcement with social and institutional validation.

Interoperability emerges as another core requirement, consistently framed as a governance issue rather than a purely technical one. While desk research documents diverse sectoral data spaces with heterogeneous priorities and maturity levels, the interviews clarify that interoperability is achieved only when participation is tied to binding rules, standards, and certification mechanisms. At the same time, VC-based approaches introduce the prospect of data-space-independent interoperability, enabling identities and attributes to be reused across platforms and ecosystems. This suggests a structural evolution from isolated, domain-specific data spaces toward inter-federated ecosystems connected by shared trust and identity layers.

Finally, both research streams converge on future-oriented requirements. Trust, participant activation, and incentives are identified as decisive success factors. Desk research points to the strategic relevance of MDM for efficiency, resilience, and sustainability, while field research highlights the difficulty of achieving critical mass and the limitations of purely voluntary participation. There is broad agreement that global standardization is unrealistic; instead, modular standards, translation capabilities, and—potentially—state- or EU-backed trust infrastructures will be necessary. Security is consistently addressed on two levels: technical trust infrastructures (e.g., DIDs, signatures, revocation mechanisms) and institutional trust anchors (e.g., clearing houses, governance bodies), both of which must be aligned.

In summary, the synthesis of desk and field research indicates a paradigm shift in master data management within data spaces. Traditional centralized MDM approaches are increasingly complemented or replaced by federated, trust-based mechanisms relying on verifiable credentials, governance frameworks, and standardized identifiers. The most critical requirements are not technological feasibility, but institutional embedding, governance design, and economic incentives. Only when these dimensions are coherently integrated can VC-based master data management unfold its full potential as a foundational capability of future data spaces.



2 Decentralized Identities

From a technical perspective, we build our architecture on the W3C standards for Verifiable Credentials¹⁸ and Decentralized Identifiers¹⁹ (DID). The VC standard defines the data model for Verifiable Credentials and how these can be secured and exchanged. The DID standard defines a way to provide identity information for individuals, organizations and objects without being dependent on a central authority. Both standards are often used in conjunction as a common basis for SSI architectures.

2.1. Decentralized Identifiers

DIDs are strings used to define where a DID-document containing identity information in a structured format can be found. „**Figure 2: Components of a Decentralized Identifier.**“ shows the schematic structure of a DID, containing besides the “did”-prefix, information about the did method and the method-specific identifier, used to resolve the DID-document by providing an example. In this example, the did method “example” would define how the identifier “123456789abcdefghi” can be resolved to the DID-Document of the respective holder.

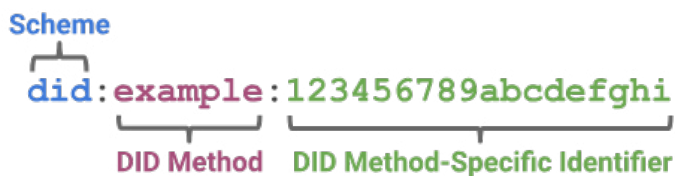


Figure 2: Components of a Decentralized Identifier.

DID Documents provide identity information in a structured format, potentially containing verification methods, service endpoints and information about the entity controlling the DID. „**Figure 3: A Simple DID-Document Example**“ shows an example of a simple DID-Document only containing public key material used for the verification of the document.

EXAMPLE 1: A simple DID document

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMnam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Figure 3: A Simple DID-Document Example⁸

The creation process of a DID is visualized in „**Figure 4: Creation Process of a DID and the corresponding DID-Documents**“⁸. Firstly, the entity controlling the DID creates a DID-Documents using a predefined DID-method. Both, the DID itself and the DID-Documents are stored inside a Verifiable Data Registry (VDR), which is publicly accessible. The “subject” refers to entity to be identified, the “controller” is the entity that created the DID and can update it afterwards. After the DID is created, the DID subject can be identified in a decentralized way through the DID-resolution via the VDR.

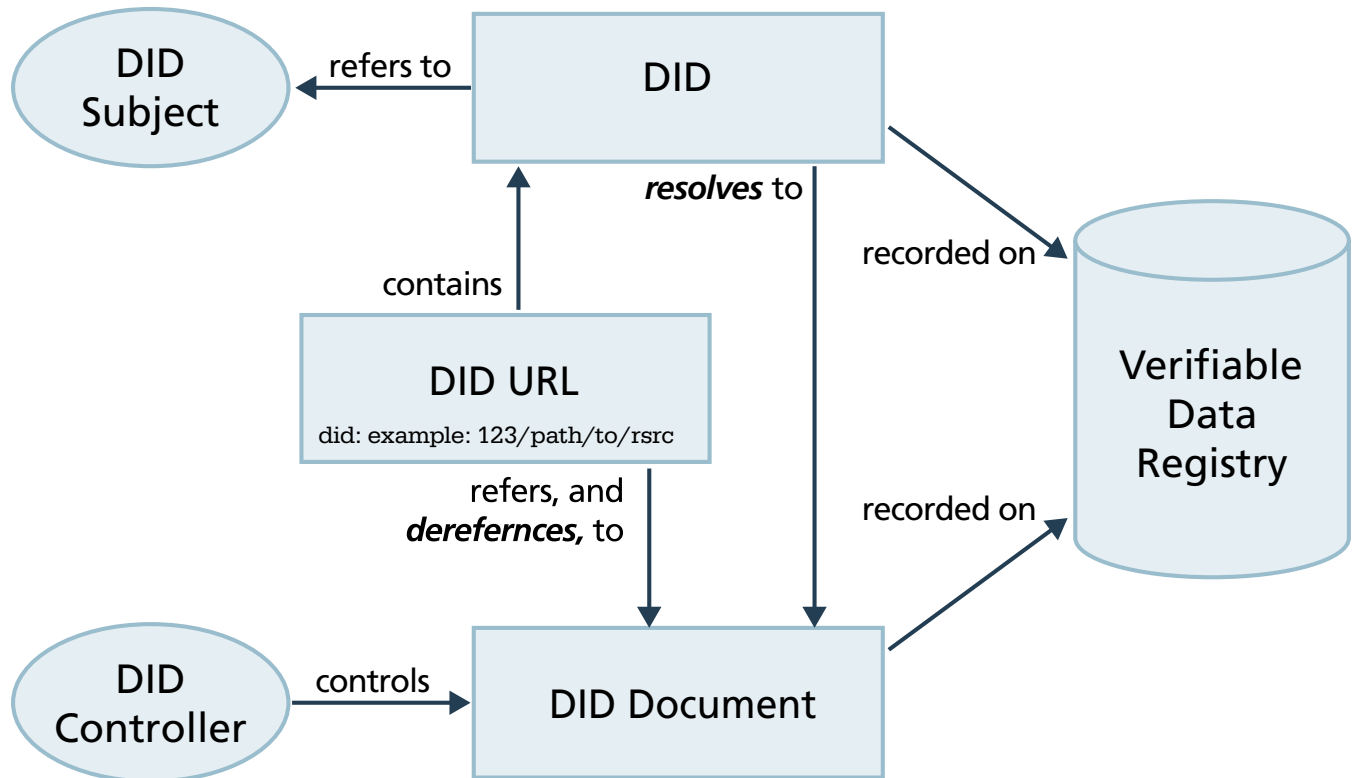


Figure 4: Creation Process of a DID and the Corresponding DID-Documents⁸

Security Note

Due to its convenience and well-known technological basis, did:web has become the predominant de facto standard in many reference implementations and architectures, including various Data Space applications.

The use of did:web is not insecure per se, but its security relies on the PKI properties of the underlying TLS-based communication, a fact that often goes unnoticed. When increased security, e.g. independence from TLS infrastructure, is a design goal, it is therefore strongly recommended to evaluate alternative, e.g. blockchain-based, options for DIDs. See also [Section 4](#) for further information.

2.2. Issuer-Holder-Verifier Model

VCs offer the possibility to assert tamperproof, technically verifiable claims about a subject. The identification process for VCs is separated in two flows. The preceding credential issuance is used to attest properties by trusted sources. The credential presentation from the credential holder to the verifier, which is used for the actual identification process, e.g. to access a service. This way, the holder can present their credentials independently of the issuer to potential verifiers. Similarly to DIDs, all identifiers, credentials schemas and registries for the status updates of credentials are stored in an underlying publicly accessible VDR. „**Figure 5: The Issuer-Holder-Verifier Model**“⁸ shows the Issuer-Holder-Verifier Model presented in the W3C VC standard.

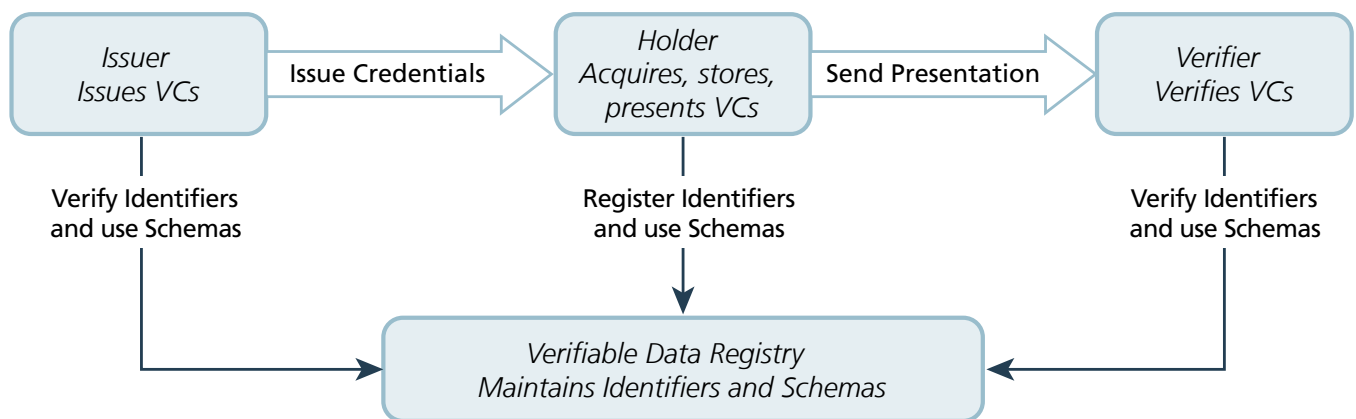


Figure 5: The Issuer-Holder-Verifier Model⁸

2.3. Verifiable Credentials and Verifiable Presentations

Verifiable Credentials consist of three components: credential metadata, the claims itself presented as a knowledge graph, and the proofs used for verification. The claims presented inside a VC are represented as a knowledge graph, dependent on the credential schema stored in the VDR. The metadata belonging to a VC may contain information about the issuer, the expiry date and validity period, a representative image, verification material status information, and potentially additional information⁸. The presentation flow considers Verifiable Presentation (VP) instead of credentials, which contain embedded credentials or proof derived of their contained claims. The creation of VPs enables the credential holder to generate a set of verifiable properties based on their possessed credentials. Additional mechanisms for selective disclosure and zero-knowledge proofs ensure that the holder can reduce the transmitted information to a minimum. The example in „**Figure 6: Structure of a Verifiable Presentation containing a Verifiable Credential**“ contains a VC that contains an exemplary claim about the subject “Pat”, which attests them an alumni membership of a “Example University”. Additionally, the embedded proof of the credential is also presented as a knowledge graph. In this simple example, the described VC is directly encapsulated inside a VP without deriving any proofs from it.

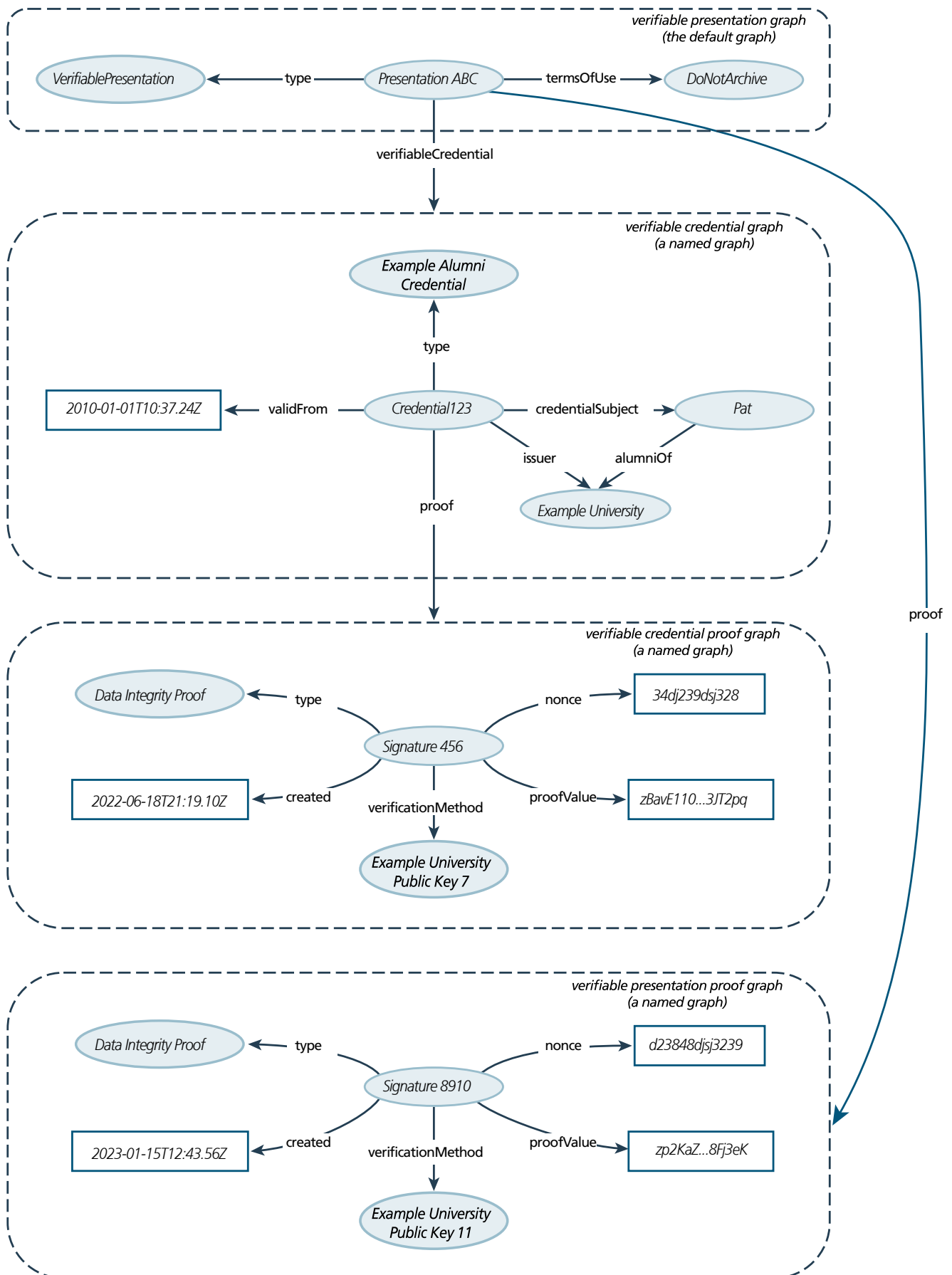


Figure 6: Structure of a Verifiable Presentation containing a Verifiable Credential

2.4. Credential Status Update

The W3C standard for VCs also allows to publish status updates. Available status keys are “refresh”, “revocation”, “suspension” or “message”. The status “refresh” signals that a new version of the credential is available, but the original one still remains valid. Status codes for “suspension” and “revocation” make the credential invalid, whereas “suspension” suppresses the validity of the credential only temporarily. The credential status property need to be checked by the at the time of validation to ensure the information inside a credential can still be trusted. In the W3C standard, this is accomplished in a scalable and privacy-preserving way with Bitstring Status Lists⁹, which are hosted by the issuer. A bit position in the list is assigned for every credential of the respective issuer, whereby a bit in the list represents a status update. As the complete list containing the bits for all issued credentials must be sent for each status request of verifiers, the potential for usage tracking of the VCs is limited.

Security Note

In order to allow for reliable revocation or suspension of credentials in case of compromise or supersession, it is of utmost importance that every issuer has implemented and tested the corresponding mechanisms thoroughly. If any credential does not include credential status information as explained, it might be accepted indefinitely.

It is therefore advisable to **reject** any credential that does not contain this information, unless the content of the credential is absolutely considered uncritical (whereas it must be sure that this consideration is never going to change) or has a very short lifetime, in which case this precaution may not be necessary.

See [Section 4](#) for more information.



3 Trust Architecture

A trust infrastructure for Master Data Management (MDM) in data spaces is essential to guarantee secure, transparent, and reliable handling of master data across diverse organizations and domains. This infrastructure provides the necessary mechanisms for the identification, authentication, and continuous certification of all participants, as well as the protection and controlled sharing of sensitive data assets. The following core principles were inspired from the (Acev et al., 2025) although decentralization of data governance and identity management was not given importance in the article but as these are some of the core principles of data spaces we regard it as essential to consider decentralization characteristics as part of our trust infrastructure as well.

3.1. Core Principles of the Trust Architecture

■ Decentralized Data Governance

This principle distributes decision-making authority over data management across participants, avoiding centralized control to enhance sovereignty and flexibility in MDM processes. In data spaces, it allows organizations (data-providers) to define and enforce their own rules and policies for master data handling (e.g., consolidation workflows, authentication mechanisms or quality standards) while collaborating via shared governance models, such as those in the Gaia-X Trust Framework, which promote peer-to-peer agreements without a single authority. For MDM, this means data stewards can maintain a “single source of truth” for entities like suppliers or assets in a hybrid landscape, reducing silos and ensuring compliance with regulations like the EU Data Governance Act.

■ Decentralized Identity & Access Management

Decentralized Identity & Access Management (IAM) empowers users and organizations with self-sovereign identities, using technologies like decentralized identifiers (DIDs), to control access without relying on central authorities. In the context of MDM in data spaces, this principle secures access to master data by verifying participant (consumer) identities through federated systems or Gaia-X Trust Frameworks (e.g., IDSA's identity providers, Gaia-X Participant Credential), preventing unauthorized modifications and enabling granular permissions for data sharing.

■ Data Provenance

Data provenance tracks the origin, history, and transformations of master data, providing a verifiable audit trail to ensure integrity and trustworthiness in shared environments. It also helps to detect inconsistencies or tampering during cross-organizational exchanges. It enhances MDM reliability by allowing consumers to validate data quality – such as confirming the source of product master records – aligning with EU standards for transparent data flows.

■ Transparency

Transparency ensures all participants have clear visibility into data processes, policies, and interactions, building accountability and reducing risks in decentralized systems. For MDM in data spaces, this means openly documenting data flows, usage conditions, and governance decisions (e.g., via machine-readable trust lists), allowing stakeholders to understand how master data is consolidated or shared.

■ Audit & Compliance

Audit & compliance focuses on ensuring that data management practices adhere to established regulations, standards, and organizational policies. In the context of MDM in data spaces, this principle involves regular audits of data handling processes and governance frameworks to verify compliance with legal requirements such as the GDPR, and industry standards. It also entails implementing mechanisms for reporting and addressing non-compliance issues, thereby promoting trust among participants. This can include automated compliance checks, documentation of data usage, and adherence to established protocols for data sharing and protection.

■ Interoperability Standards

Interoperability standards are essential for enabling seamless data exchange and collaboration across diverse systems and platforms in decentralized environments. In MDM, this principle ensures that different data formats, protocols, and technologies can communicate effectively, facilitating integration and collaboration among various stakeholders. By adhering to established interoperability standards (such as Credential Formats, APIs, data schemas, and communication protocols), organizations can enhance data accessibility, reduce integration costs, and improve the overall efficiency of master data management across disparate systems. This standardization fosters a more connected data ecosystem, promoting innovation and reducing friction in data sharing initiatives.

3.2. Components of the Trust Architecture for MDM in Data Spaces

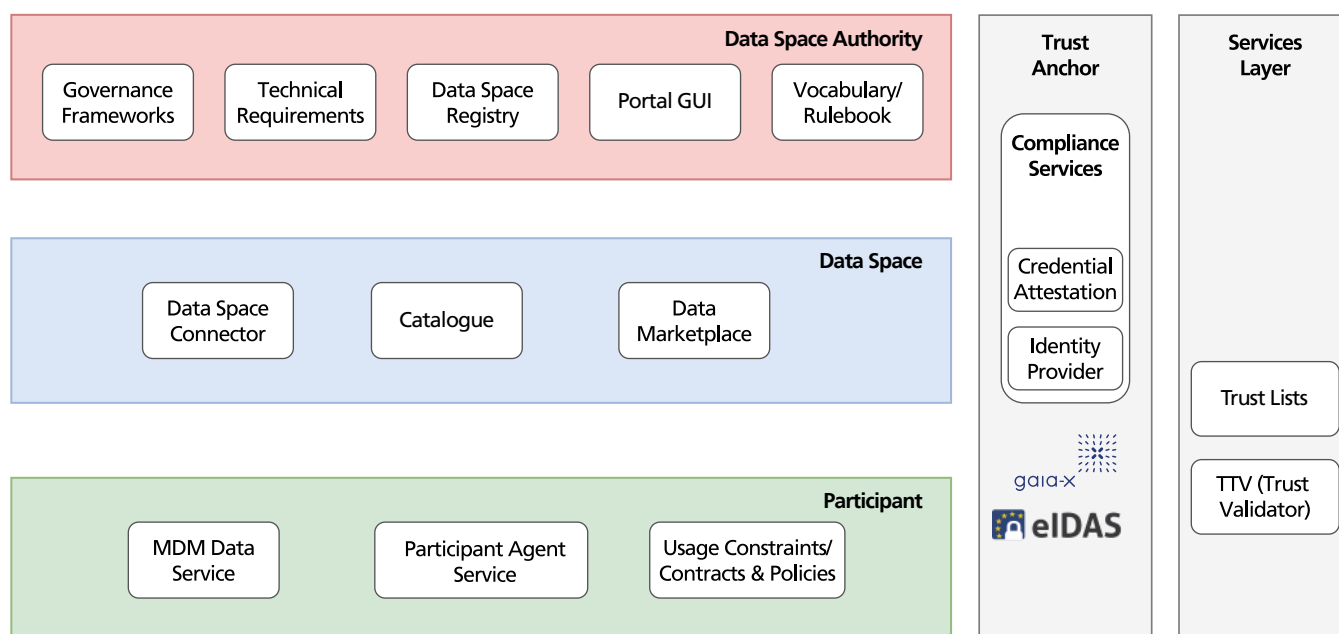


Figure 7: High Level Trust Architecture for MDM in Data Spaces

3.2.1. Participant Layer

Participant Agent Service: plays a critical role in managing identities and credentials for participants, ensuring they can securely issue, store, and verify their credentials while maintaining decentralized control over their identity.

MDM Data Source: At the core of the participant's operations, the MDM provides clean, consistent, and authoritative master data in W3C VCDM2.0 data model, ensuring that the data attributes can be shared selectively within the data space participants or across organizations based on policies and governance rules by the participant agent service.

3.2.2. Data Space Layer

Data Space Connector facilitates seamless MDM data exchange and integration among participants by providing standardized interfaces for connecting diverse systems (wallets, consumer) to the data space ecosystem. It handles secure data routing, and compliance checks to ensure that data flows adhere to shared governance while enabling efficient interoperability across heterogeneous environments.

Usage Constraints/Contracts & Policies define the enforceable rules and agreements that govern data usage, access, and

sharing of MDM Data within the data space. These components manage dynamic contracts between participants, specifying permissions, obligations, and restrictions to protect sensitive information, selectively disclose information and promote fair collaboration, with automated enforcement through policy engines integrated with the Data Space Connector.

Catalogue serves as a repository for discovering and describing available data assets, metadata, and services within the data space. It indexes MDM data sources (Provider Wallet Information) and other resources, allowing participants (consumer) to query and locate relevant MDM Dataset while ensuring discoverability aligns with privacy policies and trust validations from TTV.

Data Marketplace enables the buying, selling, and trading of data products and services in a regulated environment. It supports monetization models, negotiation of contracts, and secure transactions, leveraging trust lists and usage policies to verify participants and ensure that all exchanges comply with data space governance and selective sharing rules. But in the context of MDM Data sharing we don't see a requirement to publish MDM Data in marketplace rather it is planned to be stored in the wallet of provider. But if the provider wishes to disclose their MDM data via marketplace, they could publish the MDM Data as verifiable credentials in a well-known location linked to Marketplace.

3.2.3. Data Space Authority Layer

Governance Frameworks: establish the overarching rules, standards, and processes that guide the operation and evolution of the data space. They define participation criteria, definition of their own trust anchor or support of existing one (eiDAS) of and compliance obligations, integrating with other trust anchors to enforce consistent behavior across all layers and participants.

Technical Requirements: outline the mandatory specifications for interoperability, security, and performance within the data space, including protocols for data formats like W3C VCDM2.0 and integration with components such as the data space connector. These requirements ensure that all systems meet baseline standards for reliable and trustworthy data sharing.

Data Space Registry: maintains a comprehensive record of all registered participants, connectors, and data assets in the data space. It acts as a lookup service for verification and onboarding, cross-referencing with trust lists and TTV to validate entities and support seamless credential interoperability.

Portal GUI: provides a user-friendly web interface for participants and authorities to manage data space interactions, such as registering MDM Data, attesting MDM Data with a trust anchor, monitoring life cycle of data, and accessing catalogues. It simplifies administrative tasks while incorporating identity verification from the participant agent service for secure access.

Vocabulary/Rulebook: standardizes terminology, ontologies, and rule definitions to ensure consistent communication and interpretation across the data space. It includes semantic models aligned with MDM data models, schema definitions, facilitating policy enforcement and data mapping in contracts and governance frameworks.

3.2.4. Trust Anchor Layer

The Trust Anchor layer is a foundational component in digital ecosystems, ensuring secure credential attestation and identity verification for participants or data spaces. Trust anchors are entities or frameworks that establish trust by adhering to specific standards and protocols for identity management and credential issuance.

This layer, which spans vertically across all horizontal layers (participant, data space, and data space authority) in „[Figure 7: High Level Trust Architecture for MDM in Data Spaces](#)“, enables the horizontal layers to individually leverage one or more trust anchors based on governance, jurisdiction, or compliance requirements. For example, a participant in a European data space might use eIDAS 2.0 (Electronic Identification, Authentication, and Trust Services) for legal and regulatory compliance, while another participant might rely on Gaia-X for decentralized and federated identity management. Similarly, EBSI (European Blockchain Services Infrastructure) could be used for blockchain-based credential verification. The flexibility of the Trust Anchor layer ensures interoperability and inclusiveness, allowing participants to choose trust anchors that align with their operational or regional standards. This adaptability fosters collaboration across diverse ecosystems while maintaining security, sovereignty, and trust in credential attestation processes.


3.2.5. Services Layer

The services layer, similar to the trust anchor layer, spans vertically in „[Figure 7: High Level Trust Architecture for MDM in Data Spaces](#)“, enabling the horizontal layers (participants, data spaces, and the data space authority) to independently utilize the services provided in this layer. The functionalities of trust lists and TTV services are explained in detail below.

Trust Lists: Trust Lists can be used by participants or data spaces for different purposes. To establish trust among participants, trust lists act as registries of verified entities, allowing participants to confirm the authenticity of credential issuers and other entities in the data space. For example: Trust lists can be used by providers to verify the authenticity of the credentials of the consumer.

TTV (Trustworthiness Validation): TTV is the component of TRAIN infrastructure that can ensure that credentials and their issuers meet the trust requirements of the participant or data space, enabling seamless interoperability of MDM credentials issued across different trust anchors and even outside data spaces.

Later in [Section 5.4](#) of this document the detailed sequence diagram of the data spaces components with trust architecture is discussed in detail.



4 Security Aspects of Decentralized MDM in Data Spaces

One project goal is the secure implementation of both technical systems and governance standards. To align well-known best practices of IT security with the demands of Data Spaces, it has been tried to gain insights about security needs and expectations during three expert interviews.

Whilst conducting and analyzing the expert interviews, we found the available information about hard IT security requirements and expectations to be very limited. Therefore, the primary focus of this chapter lies on implementing IT security best practices applicable to the presented architecture, augmenting and adapting our approach using information from our expert interviews wherever possible.

Our analysis consists of 6 selected categories covering relevant security aspects of the system's architecture. These categories and our findings and recommendations for each of them are described in this chapter.

Some aspects of previous reports have been omitted because they have a significant overlap with trust-related aspects covered in other parts of this document.

4.1. Verification and Linking

As outlined in previous chapters, our architecture makes heavy use of Verifiable Credentials (VCs) and Verifiable Presentations (VPs), which have evolved to the de-facto standard of Data Spaces for representation of identity information and other critical peer properties. The platform must support DIDs with at least did:web, although DID methods that do not depend on TLS PKIs (e.g., ledger/anchor-based methods such as did:ion or did:ebasi) are strongly recommended to reduce the DNS/TLS attack surfaces. Linking decisions must be fully auditable via an immutable audit trail (e.g., WORM/append-only with cryptographic chaining and RFC 3161 timestamps) that records all evidence, verification steps, decisive attributes (including legal form, register number, address, and BPN mappings), and responsible roles, with long-term retention (at least ten years) and revision-safe versioning.

4.2. Issuance & Output

Issuance operations must implement clearly defined roles – Requester, Approver, and Issuer – with effective segregation of duties, and critical steps must follow a four-eyes principle supported by mandatory checklists covering identity proofs, data quality, validity periods, and status checks.

Issuance must be audit-proof, with records that include the Issuer DID, the subject identifier (e.g., BPN), the credential type and schema reference, the algorithms and key IDs used, issuance and expiry timestamps with synchronized time, status endpoints and references to verification results; these records must be stored immutably under a defined retention and deletion policy.

4.3. Organizational Requirements

Issuers must employ vetted and trained personnel, including role-appropriate background checks and onboarding plus periodic refresher training. Onboarding (identity verification and trust establishment) and operations (data maintenance and issuance) must be separated organizationally and personnel-wise. Formal change and incident response processes must be established, covering planning, approvals, rollback, forensic preservation, internal and external communications, and lessons learned, while periodic role and permission reviews must enforce least privilege. Depending on criticality, a two-person or four-person rule must govern sensitive steps, including key operations, schema changes, and bulk revocations.

4.4. Cryptographic Security

All cryptographic mechanisms must follow current NIST/BSI recommendations, using modern, well-parameterized primitives such as Ed25519 or ECDSA P-256/P-384 for signatures, SHA-256/384 for hashing (for password hashing: Argon2i or similar), AES-256-GCM for encryption, and HKDF for key derivation. That list represents examples which are considered sufficiently secure at the time of writing. It is neither complete, nor will it be up to date in the near future.

A post-quantum cryptography roadmap must be defined; where feasible, hybrid approaches should be employed – e.g., classical algorithms plus CRYSTALS-Dilithium for signatures and Kyber-based KEMs for key establishment – together with a clear migration strategy and timelines.

Signing and key operations must run on hardened systems, whereas it is strongly recommended that private keys be generated, stored, and used exclusively within certified HSMs (e.g., FIPS 140-3 Level 3 or Common Criteria EAL4+ or higher). Access must be tightly controlled with measures like MFA, RBAC, and M-of-N quorum policies.

Key management must define fixed rotation intervals (for example, annual rotation for issuer keys, shorter for higher risk) and event-driven rotation upon suspicion or compromise. The issuer keys must be derived from root keys that are handled entirely offline, i.e., on air-gapped systems. The general recommendations above, regarding HSM usage, apply accordingly. Encrypted backups must be maintained offline/offsite, validated through regular restore tests, and documented across their entire lifecycle.

4.5. Lifetime & Validation Procedures

Credential lifetimes must align with protection needs and operational cadence, with typical validity between six and twelve months, while VPs must be short-lived (from minutes to hours) and context-bound. Validation must verify signatures, current revocation/status, and integrity; VP-only scenarios must include integrity bindings via referenced content hashes or embedded digests. Both online status checks (status lists or OCSP-equivalents) and robust offline validation paths (signed status objects with defined refresh intervals and expirations) must be supported, with explicit, secure fallback logic. Renewal and update procedures must be clearly defined and preferably automated – providing advance expiry notifications, streamlined re-issuance, version tracking – and must be fully logged with notifications to affected parties.

4.6. Revocation & Blocking Mechanisms

Any VCs issued externally (i.e., VCs that are not created with the holder’s own signature) must contain valid “credentialStatus” properties¹⁰ with an entry containing the “statusPurpose” with value “revocation”, and accordingly use the W3C VC Bitstring Status List mechanism¹¹ to allow for later revocation. Status lists must be reliably available and updated promptly. Verifiers must check status on every VP verification.

The revocation decision policy must be explicit and cover at minimum key compromise, changes in legal status (e.g., mergers, liquidation, representation rights), detected data errors, policy violations, and end of operational validity, with defined responsibilities and approval steps. Revocation information must propagate quickly and reliably to downstream systems under defined SLAs (e.g., publication within minutes), with enforced maximum client cache TTLs, monitoring and alerting on fetch or validation failures, and forensic traceability of all revocation operations.



5 Verifiable Credentials- based MDM in Data Spaces

In this section we describe the way master data is exchanged with the help of VCs on a technical level. Section 5.1 describes the process of generating verifiable presentations based on self- and externally attested claims. Section 5.2 describes the holistic process of master data exchange considering the “happy path” in which no credential is revoked. Lastly, Section 5.3 defines how the process for master data verification fails due to a credential revocation and shows how this case can be handled.

5.1. A Simple Example for Master Data Exchange with SSI Presentation

Before any master data exchange, certain properties need to be attested by a third party. These so-called "trust anchors" can either be participating inside the data space or be an external issuer outside the data space. In our example in „**Figure 8: Attestation process of master data by trust anchors**“, "Trust Anchor A" is located inside the data space and "Trust Anchor B" is located outside the data space. Both trust anchors attest claims about the data provider in the form of issuing a VC to the provider's wallet. Hereby, the issued VCs can contain multiple claims, in this example this is the case for the "Data Space Membership Credential", which contains the claim for the provider's address and a claim about the active data membership status of the provider. All credentials are bound to a Decentralized Identifier Document¹² (for short: DID-Documents), containing the provider's key material.

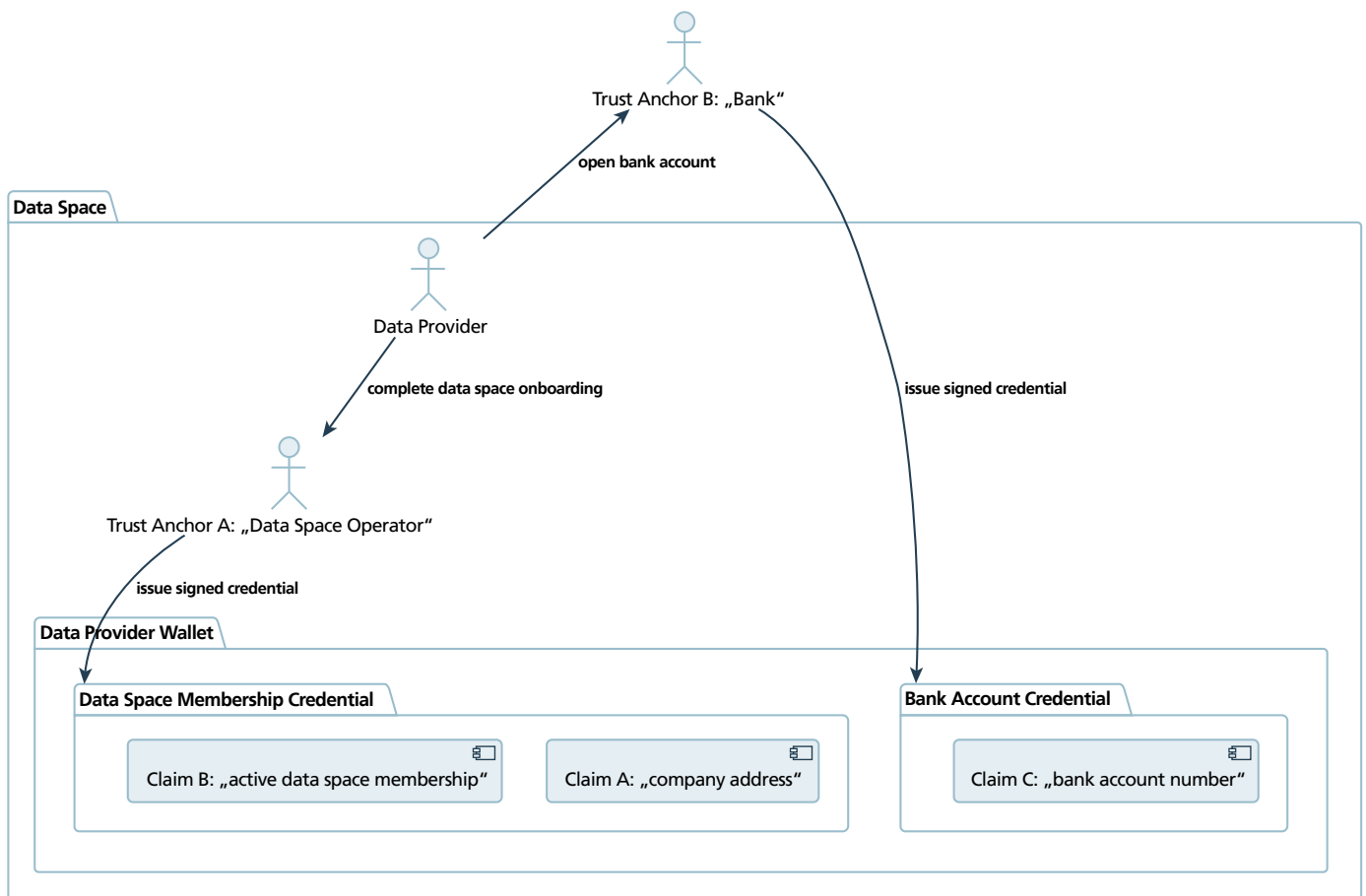


Figure 8: Attestation Process of Master Data by Trust Anchors

For the next step, we assume a data consumer requests the master data information in form of “company name”, “company address” and “bank account number” from the provider. For each requested property the provider needs to decide which of the requested information he wants to share with the consumer. Based on this, the provider needs to generate its Verifiable Presentation (VP) which is returned to the consumer, as visualized in „**Figure 9: Creation of a Verifiable Presentation based on the Data Provider’s Verifiable Credentials.**“. In our example, we assume that access to all requested properties should be included. We assume that the property “company name” does not have to be attested by an external trust anchor, thus the Provider embeds it into a self-asserted VC. As the “bank account number” exists in the “Bank Account Credential” without any other claim that contains information that should not be shared with the Consumer, it can be directly embedded into the VP. Similarly, the just created “Company Name Credential” can also be directly embedded into the VP. For the “company address” claim inside the “Data Space Membership Credential” we need to derive a proof with a technology that supports selective disclosure (e.g. SD-JWT¹³). The direct embedding for the VC would also include the claim for “active data space membership”, which is neither requested nor might it be shared by the Data Provider. Additionally, selective disclosure could be used to derive claims that further reduce or obscure the information in a claim, here this might be a claim that a bank account at a specific bank exists, but not the which bank account number. However, for this project selective disclosure is just considered for the simple case.

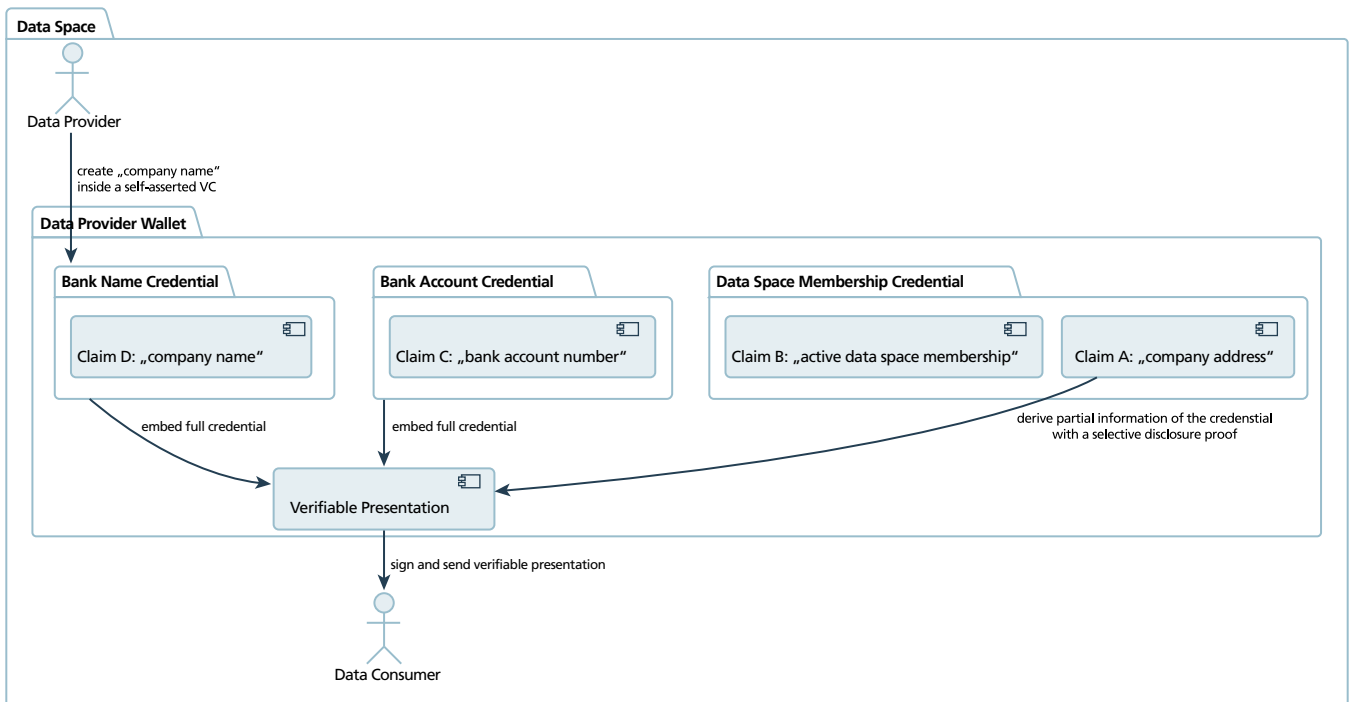


Figure 9: Creation of a Verifiable Presentation based on the Data Provider’s Verifiable Credentials

5.2. Complete Process of Master Data Exchange

In „Figure 10: Complete process of attestation, presentation and verification of the master data.“ the complete process from master data request to presentation is shown. In this case, we assume that no credential revocation occurs and thus, the verification of the master data succeeds. In [Section 5.3](#) the case for credential revocation is considered. First, the provider queries an attestation of certain master data claims at the trust anchor as described in „Figure 7: High Level Trust Architecture for MDM in Data Spaces“. These attestations come in the form of VCs, potentially containing multiple claims per credential. After the master data is requested by the consumer, the provider goes ahead and creates a VP as shown in „Figure 8: Attestation process of master data by trust anchors“. After the consumer has successfully verified the signature of the presentation and has confirmed the non-revocation, the contained master data claims can be securely used.

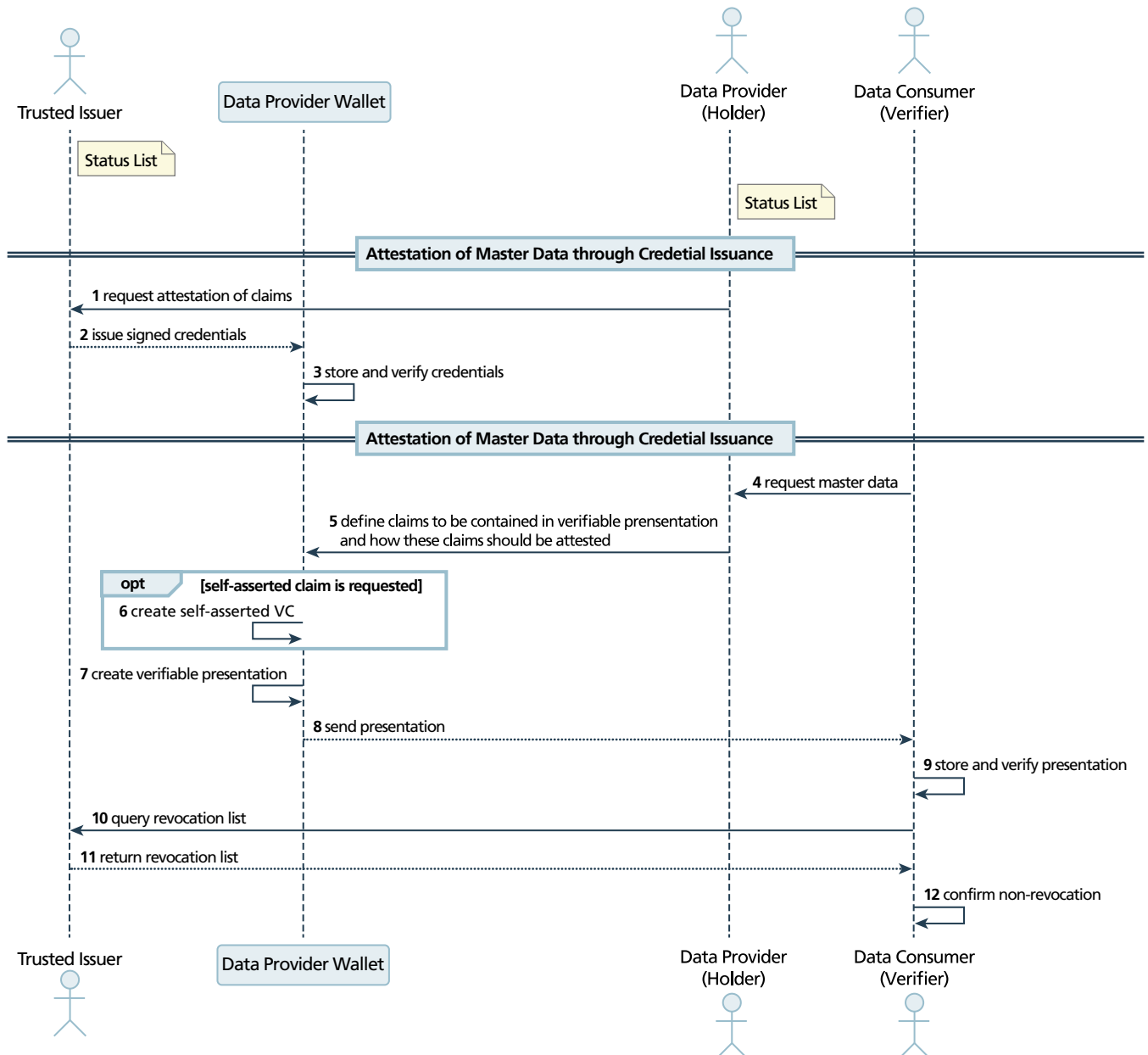


Figure 10: Complete Process of Attestation, Presentation and Verification of the Master Data

5.3. Credential Revocation

The W3C Verifiable Credential Data Model ensures that credentials can be revoked through status lists, as already mentioned in [Section 2.4](#). In our model, this revocation can either affect the credential issued by a trusted issuer or a self-asserted credential. The presentation might include the creation of self-asserted claims, some of which the Provider might need to retract later. This can either be accomplished by hosting a revocation list at the Provider, in which case these credentials must have the corresponding credential status elements for revocation, or through short expiry dates. [Section 4](#) elaborates further on the securing of VCs, especially with respect to revocation. „**Figure 11: Failed verification of a presentation containing a revoked credential.**“ shows a case in which some of the proofs or embedded credentials are invalid, because some of the credentials used to create presentations have been revoked. In this case, the Consumer can simply request a new presentation of the invalid properties at the Provider.

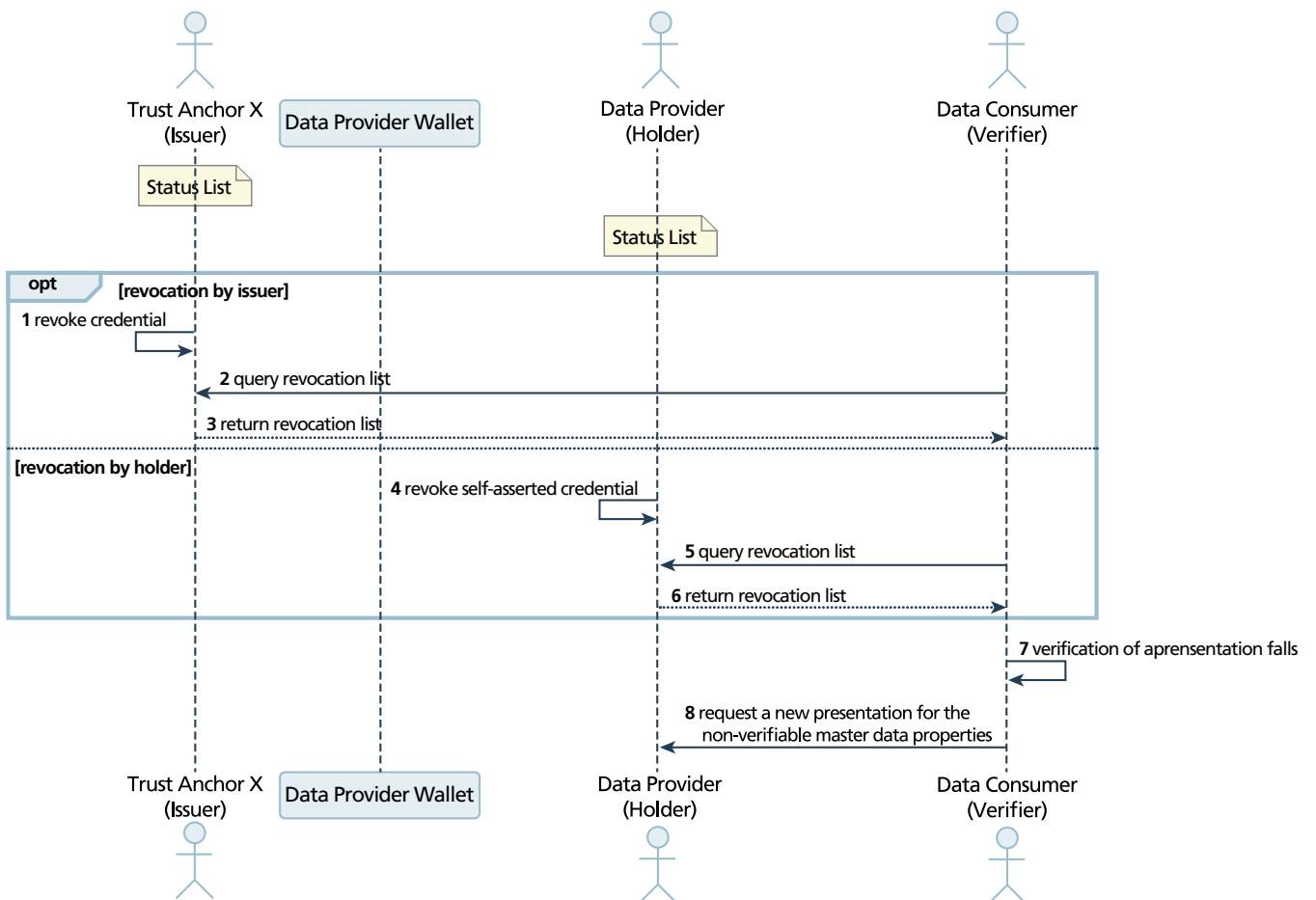


Figure 11: Failed Verification of a Presentation Containing a Revoked Credential

5.4. Integration with the Data Space Components & Trust Architecture

In this section, the process of Master Data Exchange with Self-Sovereign Identity (SSI), as discussed in [Section 5.1](#) and [Section 5.2](#), will be further extended by incorporating data space components and the trust architecture outlined in [Section 3](#). The data space connector serves as the entry point for data exchange between the provider and the consumer, facilitating secure and efficient communication.

The Participant Agent Service plays a crucial role in managing credential storage and performing credential verification, ensuring that participants can securely interact within the data space. Additionally, Trust Lists and Trusted Timestamp Verification (TTV) are employed to enhance the overall trustworthiness of the system. Trust Lists are used to register and maintain metadata about credential issuers, ensuring that only verified and trusted entities are included. TTV, on the other hand, validates credentials issued by various trust anchors, ensuring compliance with established standards and protocols. The detailed sequence diagram can be found on **„Figure 12: Complete Process including trustworthiness validation using Data space Components“**.

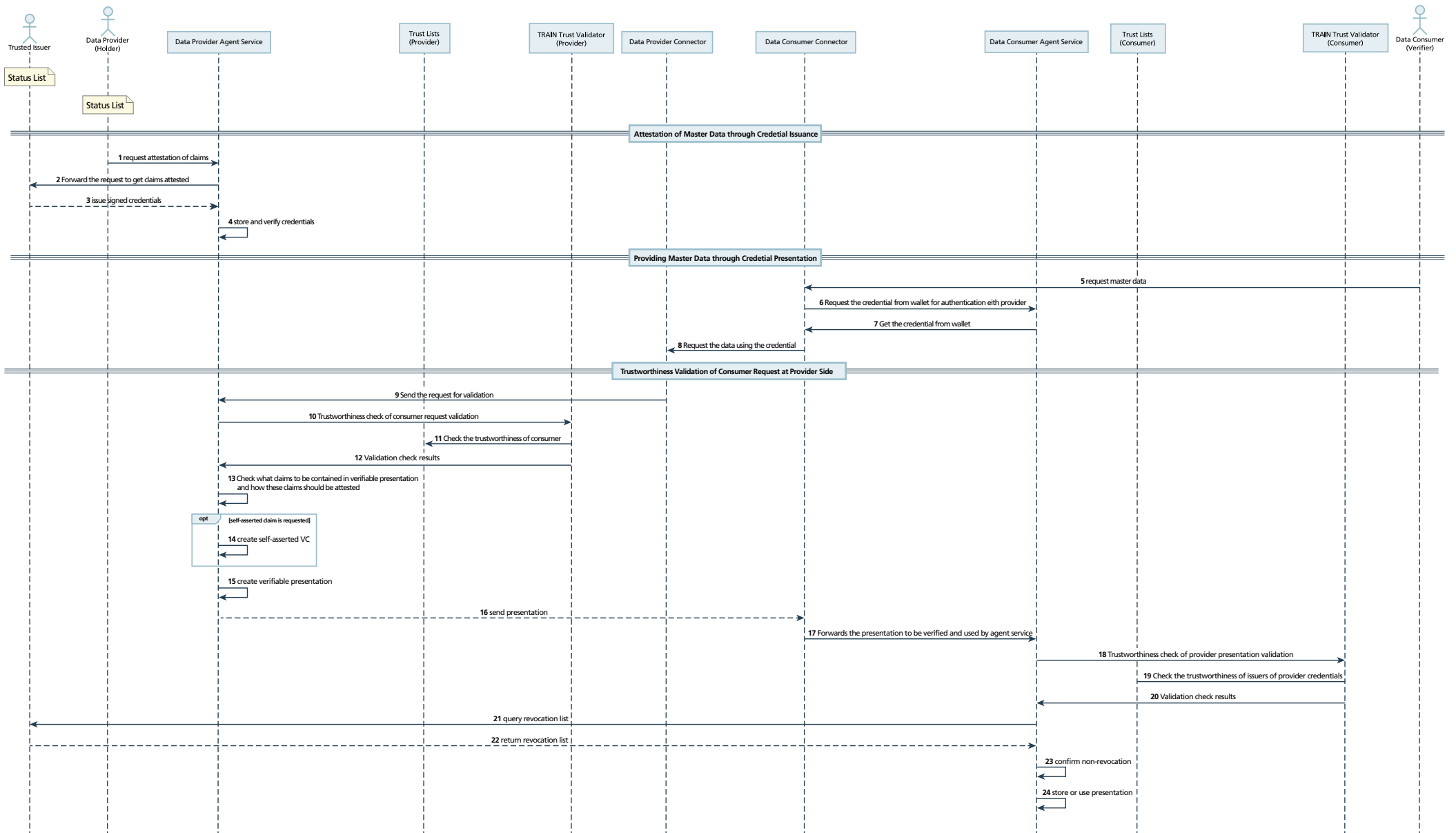


Figure 12: Complete Process Including Trustworthiness Validation Using Data Space Components



6 Business Model and Utilization Plan

6.1. Scope and Objectives of the Business Model

This chapter develops a business model and utilization plan for VC4MDS. Unlike traditional master data management solutions, which rely on centralized repositories or tightly coupled system integrations, VC4MDS introduces a federated, trust-based approach in which master data attributes are exchanged as cryptographically verifiable proofs rather than shared databases.

The objective of this chapter is twofold. First, it analyzes how economic value can be created, delivered, and captured through VC-based decentralized MDM in data spaces. Second, it identifies viable utilization and monetization models that ensure long-term operation under the regulatory, organizational, and technological conditions of European data spaces. In line with Teece (2010), the business model is understood as the architecture of value creation, value delivery, and value capture. Rather than presenting business-model theory exhaustively, established concepts are applied selectively to structure and analyze VC4MDS as a concrete socio-technical solution. It was originally used to illustrate procedural processes (Fibitz 2022). Osterwalder et al. (2005) define a business model as follows: *“A business model is a conceptual tool containing a set of*

objects, concepts and their relationships with the objective to express the business logic of a specific firm. Therefore we must consider which concepts and relationships allow a simplified description and representation of what value is provided to customers, how this is done and with which financial consequences.” Another important concept is the V4 business model from Al-Debei and Fitzgerald (2010), which represents a hierarchical taxonomy of a business model concept and includes the four dimensions value proposition, value architecture, value network and value finance. According to Massa et al. (2017), business models can be categorized into the following three types cognitive/linguistic model, formal conceptual representations like Business Model Canvas according to Osterwalder and Pigneur (2011) and attributes of real companies. Technological innovations do not automatically guarantee business success; they must be combined with a suitable business model and a strategy for market launch and value creation (Teece 2010). However, the terms ‘business model’ and ‘corporate strategy’ are often not clearly distinguished from one another (Rüger et al. 2018). While business models represent the fundamental logic of a company and are customer-oriented, corporate strategy defines how competitive advantages can be gained and a better market position achieved.

6.2. Market Context and Stakeholder Landscape

6.2.1. Stakeholders in VC4MDS-enabled Data Spaces

Federated data spaces are characterized by heterogeneous actors with distinct roles and incentives. In the context of VC4MDS, three primary stakeholder groups can be identified:

- **Data Space Operators / Intermediaries:** These actors provide and govern the technical and organizational infrastructure of the data space. They are responsible for onboarding participants, enforcing governance rules, and ensuring compliance with standards and regulations.
- **Data Providers:** Data providers maintain and issue master data attributes about themselves or their assets. In VC4MDS, they remain sovereign over their data and decide which attributes are disclosed, to whom, and under which conditions.
- **Data Users:** Data users consume master data attributes for operational, analytical, or compliance-related purposes. Their primary interest lies in the reliability, verifiability, and semantic clarity of the data.

- VC4MDS addresses the needs of all three groups by decoupling trust establishment from centralized data storage and enabling verifiable attribute exchange across organizational boundaries.

6.2.2. Market Environment and External Influences

The macro-environment of VC4MDS is shaped by political, legal, technological, social, and ecological factors. European initiatives such as the Data Governance Act and the Data Act emphasize secure, interoperable, and sovereign data sharing. At the same time, regulations such as the GDPR impose strict requirements on the handling of personal data, which is particularly relevant when master data contains identifiers such as names, addresses, or organizational affiliations.

From a technological perspective, increasing heterogeneity of systems and standards reinforces the need for interoperable trust mechanisms. Socially, the success of decentralized MDM depends on trust, cooperation, and participant activation, confirming that MDM in data spaces is fundamentally a socio-technical integration problem rather than a purely technical one.

6.3. Value Proposition of VC-based Decentralized Master Data Management

6.3.1. Core Value Proposition

The central question of the value proposition is: Which concrete problems does VC4MDS solve compared to existing MDM approaches?

VC4MDS provides value primarily through:

1. Trust without central data pooling: Master data attributes are exchanged as verifiable credentials or verifiable presentations, eliminating the need for shared central databases while preserving trust.
2. Data sovereignty and selective disclosure: Data providers disclose only the attributes required for a given context, reducing data exposure and supporting compliance with data-protection regulations.
3. Improved data quality and verifiability: Cryptographic signatures, issuer trust, and revocation mechanisms ensure that data authenticity, integrity, and validity can be verified at any time.
4. Interoperability across data spaces: VC-based credentials are not bound to a single platform or data space, enabling reuse across ecosystems and reducing integration costs.
5. Reduced operational and onboarding costs: Automated verification and standardized trust mechanisms lower manual verification efforts and accelerate onboarding processes.

6.3.2. Status Quo

Besides this desk and field research, relevant influencing factors of the macro-environment for the solution and to derive the challenges and needs from the perspective of the customers can be identified with a PESTEL-analysis.

- **Economical:** The global MDM market was estimated at USD 16.07 billion in 2024. According to forecasts, the market will grow from USD 18.63 billion in 2025 to USD 57.02 billion in 2032, representing a compound annual growth rate of 17.33% during the forecast period¹⁴. Moreover, MDM makes a significant contribution to the overall success of a company. Effective data management is a prerequisite for digitalization and an important competitive factor. This shows the economical influences and potential of trustful and secure MDM in companies and how it can have an impact in the competitiveness of a company¹⁵.
- **Social:** The interviews conducted show that MDM in data spaces is not purely a technical problem, but rather a socio-technical integration problem. The various approaches show that trust is no longer centrally controlled. Instead, it is created through traceable evidence and shared rules, which requires social interactions and agreements between the actors. The success of MDM depends heavily on the cooperation and social dynamics of the organizations and individuals involved. That is why it is necessary for actors to talk to each other and establish standards in order to build trust between them. In addition, encouraging participation in data spaces remains a social challenge, which is why highlighting the added value of participating in data spaces continues to be relevant. In particular, this added value is created by the trusted architecture for MDM in data spaces.
- **Technological:** The previous SLR has shown that interoperability and standards are important factors for successful MDM within data spaces. In addition, support from VC and VP is necessary for attribute confirmation, if necessary without disclosure of raw data. SSI is considered a key technology for strengthening data protection, trust, and user control in digital ecosystems. It plays a crucial role in ensuring the integrity and traceability of transactions, especially in blockchain-based architectures (Costagliola et al., 2025). VCs and VPs are used to confirm feature checks without disclosing raw data, while SSI is based on W3C standards and forms verifiable credentials and decentralized identifiers as well as OIDC protocols. Furthermore, it is a fundamental trust factor for data spaces.
- **Ecological:** In view of the ecological dimension, it can be noted that resource conservation is becoming increasingly important in data management. AI and cloud computing require many data centers and consume a lot of energy, which is why resource-efficient data management is

important¹⁶. Green IT and Green Cloud Computing, as well as Green Software Engineering, are becoming increasingly relevant topics in this context. The aspect of sustainability is therefore also important to mention the awareness of these topics in this context of MDM.

- **Legal:** With the Data Act, the EU is establishing regulations for interorganizational data sharing. The law is intended to strengthen the EU's data economy and regulate increased data availability. This also includes regulations that affect participants in data spaces and establish standards and specifications.

In addition, master data may also contain personal data, such as name, age, or address. When handling master data, it is important to ensure that data is handled in accordance with the GDPR. Data may only be used for the original purpose for which it was collected.¹⁷

The PESTEL-Analysis shows that the challenges in MDM in data spaces require an integrative approach that takes technical and social aspects into account in order to ensure trust and interoperability. It is important that the solutions are suited to the dynamic environment and regulatory landscape so that a successful business model can be guaranteed.

6.4. Utilization Models and Value Creation

The economic utilization of VC4MDS can be systematically analyzed using the Magic Triangle („**Figure 13: Business Model magic triangle according to Gassmann et al. (2013)**“) according to Gassmann, Frankenberger, and Csik (2013), which structures business models along the dimensions Who, What, How, and Value. This framework is particularly suitable for decentralized data-space solutions, as it allows different operational constellations to be compared while maintaining a consistent analytical perspective.

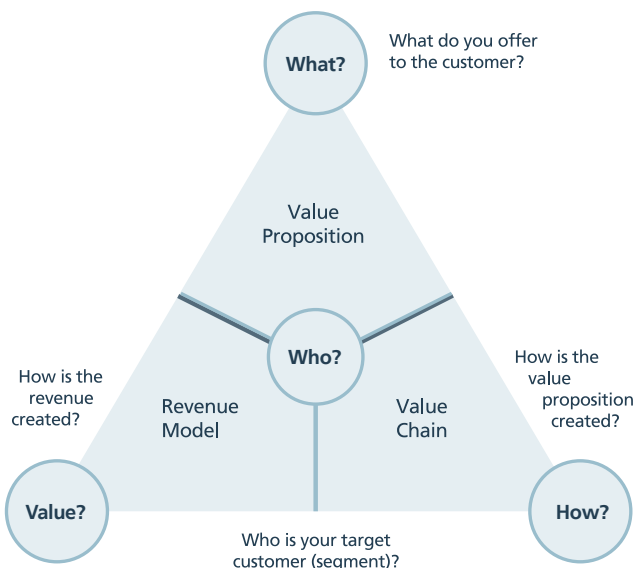


Figure 13: Business Model Magic Triangle According to Gassmann et al.

Across all utilization models, VC4MDS provides a shared technological and governance foundation for trustworthy master data exchange. The differences lie primarily in operational responsibility, governance intensity, and revenue mechanisms.

In the first utilization scenario, VC4MDS is operated directly by the data space operator. In this configuration, the operator offers the VC-based master data management functionality as an integral part of the data space infrastructure. The target customers are data providers and data users participating in the data space, who benefit from a standardized, trustworthy, and interoperable solution. The value proposition consists of seamless integration with existing data-space components, compliance with Gaia-X and IDS principles, and centralized governance for onboarding, certification, and auditing. Value creation is achieved through the operation of the technical infrastructure, the enforcement of governance rules, and the integration of complementary services such as identity management and data-quality mechanisms. Economic value is captured through platform-related revenue streams, such as membership fees, platform usage fees, or pay-per-use pricing for specific verification or credential-related services. This model aligns well with platform-oriented data spaces and emphasizes ecosystem stability and trust.

A second utilization model involves operation by a trusted third-party provider. In this case, the data space operator does not directly manage master data services; instead, an external provider offers VC4MDS as a federated MDM-as-a-Service solution. This model targets multiple data spaces or organizations seeking a standardized and interoperable master data service without operating their own infrastructure. The value proposition lies in specialization and scalability: third-party providers can leverage domain-independent expertise, reuse components across ecosystems, and continuously enhance functionality. Value creation is driven by service integration, interoperability with existing data spaces via Gaia-X-compliant interfaces, and the incorporation of best practices from established MDM and identity-management vendors. Revenue generation typically follows subscription-based models, transaction-based fees, or service-level agreements, allowing predictable and scalable monetization.

In a third scenario, VC4MDS is operated directly by data providers or data users for their own organizational purposes or within bilateral or small multilateral constellations. Here, the focus shifts from platform monetization to internal efficiency gains. Organizations manage and issue their own credentials, integrate VC-based verification into existing master data governance systems, and automate administrative processes. The value proposition consists of increased data quality, reduced manual effort, and improved decision-making based on verifiable master data.

Although direct revenue generation may be limited in this model, economic value is realized indirectly through cost reduction, process acceleration, and risk mitigation. This utilization pathway is particularly attractive for organizations with high internal compliance requirements or complex partner networks.

Taken together, the utilization models demonstrate that VC4MDS is not bound to a single operational or economic logic. Instead, it provides a flexible foundation that can be embedded into platform-centric, service-oriented, or organization-centric value creation structures.

6.5. Sustainability and Adoption Challenges

Ensuring the long-term sustainability of VC4MDS requires a combination of robust monetization mechanisms, strategic partnerships, and effective governance. A central prerequisite for economic viability is compliance with established data-space standards and trust frameworks, such as Gaia-X, IDS, and related European initiatives. Adherence to these frameworks not only ensures interoperability and regulatory compliance but also increases market acceptance and reduces adoption barriers.

Monetization approaches for VC4MDS can be derived from existing models used in data spaces and digital platforms. These include subscription-based access to master data verification services, pay-per-use pricing for credential issuance or validation, and platform-level fees for participation in trusted data ecosystems. In early phases, hybrid funding models that combine public funding with market-based revenues may be particularly relevant, reflecting the strategic importance of trustworthy data infrastructures for the European data economy.

Strategic partnerships play a crucial role in scaling and sustaining VC4MDS. Collaboration with technology providers, such as established MDM or ERP vendors, enables integration into existing enterprise landscapes and facilitates adoption. At the same time, partnerships with trust-service providers and certification bodies strengthen the credibility of issuer roles and validation mechanisms. These partnerships contribute to a layered trust model that combines technical verification with institutional legitimacy, consistent with the socio-technical nature of data spaces.

Despite its economic potential, VC4MDS faces several adoption challenges. One major dependency is the achievement of critical mass: the value of verifiable master data increases significantly with the number of participating actors, making early-stage adoption particularly challenging. Furthermore, governance acceptance is essential, as organizations must trust not only the technology but also the rules defining issuer roles, revocation procedures, and liability. Another challenge lies in standard fragmentation. As global uniformity of standards is unlikely, translation and mapping mechanisms between schemas and governance regimes will remain necessary.

Finally, organizational change represents a non-negligible barrier. Introducing VC-based master data management requires adjustments to established processes, responsibilities, and mindsets. These transformation costs must be offset by clearly communicated benefits, such as reduced verification effort, improved data quality, and enhanced interoperability.

In summary, the economic success of VC4MDS depends less on technological maturity—which is already well advanced—and more on institutional embedding, governance alignment, and incentive structures. Only if monetization strategies, partnerships, and trust frameworks are coherently aligned can VC-based decentralized master data management unfold its full potential within and across data spaces.



7 Further Research

This work has examined master data management in federated data spaces with a particular focus on the role of verifiable credentials (VCs) as an enabling trust technology. Based on a combination of desk research and qualitative field research, the study has shown that traditional centralized approaches to master data management reach structural limits in data-space environments characterized by organizational autonomy, heterogeneous systems, and strict data-sovereignty requirements. The results indicate that VC-based decentralized master data management (VC4MDS) represents a promising paradigm shift, enabling trustworthy master data exchange without the need for central data pools. Core contributions of this work include the identification of key trust mechanisms, governance requirements, and viable utilization models for VC4MDS, as well as the articulation of its economic and organizational implications. Despite these contributions, the findings also highlight that VC4MDS is still at an early stage of maturity and raises a number of open research questions. Future research should therefore focus on deepening, validating, and operationalizing the conceptual insights developed in this study.

A first avenue for further research concerns the empirical evaluation of VC4MDS in real-world deployments. While this work draws on expert interviews and existing initiatives, longitudinal case studies and pilot implementations are required to assess how VC-based master data management performs under operational conditions. Such studies should analyze adoption dynamics, governance effectiveness, and measurable impacts on data quality, onboarding effort, and process efficiency. In particular, research is needed to understand how network effects evolve over time and how critical mass can be achieved in early-stage data spaces.

Second, governance and trust frameworks require further investigation. This study has shown that trust in VC4MDS emerges from a combination of technical mechanisms (e.g., signatures, revocation, credential lifecycles) and institutional arrangements (e.g., issuer roles, certification bodies, clearing houses). Future research should explore how these elements can be systematically combined into reference governance models that are adaptable across domains while remaining compliant with regulatory requirements. Comparative studies across sectors—such as manufacturing and healthcare—would be particularly valuable in identifying transferable governance patterns and domain-specific constraints.

A third research direction relates to standardization and interoperability. Although global uniformity of standards appears unrealistic, further work is needed on translation mechanisms, semantic mappings, and layered architectures that enable interoperability between different data spaces and master data schemas. From a technical perspective, this includes research on integrating VC-based approaches with existing master data governance systems and enterprise platforms. From an organizational perspective, it involves studying how standards are negotiated, adopted, and enforced within federated ecosystems.

In addition, economic and incentive-related aspects warrant deeper analysis. This study has outlined potential utilization and monetization models, but further research is required to quantify costs, benefits, and risks for different stakeholder groups. Economic modeling and simulation could support the design of sustainable incentive structures that encourage participation, data quality maintenance, and long-term commitment to VC4MDS-based solutions.

Beyond academic research, several practical steps are necessary to establish VC4MDS as a viable approach in practice. These include the development of reference architectures and open-source building blocks, the execution of cross-data-space pilot projects, and the involvement of public institutions as trust anchors to increase legitimacy and adoption. Clear communication of value propositions—particularly for small and medium-sized enterprises—will be essential to overcome initial adoption barriers.

VC4MDS offers a vision for the future of master data management in data spaces, aligning technological trust mechanisms with principles of data sovereignty and interoperability. However, realizing this vision requires sustained interdisciplinary research and coordinated action among researchers, practitioners, standardization bodies, and policymakers. Future work should therefore focus not only on technical refinement, but also on governance design, economic viability, and ecosystem-building to fully unlock the potential of verifiable-credential-based master data management.

8. References

- 1 <https://www.gleif.org/en/lei-data/access-and-use-lei-data>
- 2 D&B D-U-N-S®-Identifikationsnummern - Dun & Bradstreet
- 3 https://taxation-customs.ec.europa.eu/customs/customs-procedures-import-and-export/customs-operations/economic-operators-registration-and-identification-number-eori_de
- 4 <https://www.lexware.de/wissen/unternehmerlexikon/handelsregisternummer/>
- 5 <https://blog.northdata.com/european-unique-identifier>
- 6 <https://www.gs1-germany.de/standards/identifikation/unternehmen-gln/>
- 7 <https://www.w3.org/TR/did-1.0/>
- 8 <https://www.w3.org/TR/vc-data-model-2.0/>
- 9 <https://www.w3.org/TR/vc-bitstring-status-list/>
- 10 <https://www.w3.org/TR/vc-data-model-2.0/#status>
- 11 <https://www.w3.org/TR/vc-bitstring-status-list/>
- 12 <https://www.w3.org/TR/did-1.0/>
- 13 <https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/22/>
- 14 <https://www.fortunebusinessinsights.com/master-data-management-market-114277>
- 15 <https://www.pwc.de/de/digitale-transformation/pwc-studie-master-data-management-im-handel-und-in-der-konsumgueterindustrie-2018.pdf>
- 16 <https://www.pwc.de/de/nachhaltigkeit/interview-wie-datenzentren-energieeffizienter-und-nachhaltiger-werden.html>
- 17 <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>
- 18 <https://www.w3.org/TR/vc-data-model-2.0/>
- 19 <https://www.w3.org/TR/did-1.0/>

- Acev, D., Biyani, S., Rieder, F., Aldenhoff, T. T., Blazevic, M., Riehle, D. M., & Wimmer, M. A. (2025). Systematic analysis of data governance frameworks and their relevance to data trusts. *Management Review Quarterly*. Advance online publication. <https://doi.org/10.1007/s11301-025-00545-1>
- Al-Debei, M. M [M. M.], & Fitzgerald, G. (2010). The design of innovative mobile artifacts: How to develop powerful value networks? In 2010 IEEE International Conference on Management of Innovation & Technology: Icmitt 2010 ; Singapore, 2 - 5 June 2010 (pp. 129–134). IEEE. <https://doi.org/10.1109/ICMIT.2010.5492826>
- Al-Debei, M. M [Mutaz M.], & Avison, D. (2010). Developing a unified framework of the business model concept. *European Journal of Information Systems*, 19(3), 359–376. <https://doi.org/10.1057/ejis.2010.21>
- Fibitz, A. (2022). Grundlagen. In A. Fibitz (Ed.), *Research. Auswirkungen der Digitalisierung auf unternehmerische Geschäftsmodelle*. Dissertation (pp. 27–120). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-39206-2_2
- Gassmann, O., Frankenberger, K., & Csik, M. (2013). *The St. Gallen Business Model Navigator*. <https://www.alexandria.unisg.ch/bitstreams/d71e2821-d8f8-4cc1-a1ee-97baff7d9e48/download>
- Lukas, T. (2017). *Business Model Canvas – Geschäftsmodellentwicklung im digitalen Zeitalter*. In S. Grote & R. Goyk (Eds.), *Führungsinstrumente aus dem Silicon Valley: Konzepte und Kompetenzen* (1. Aufl. 2018, pp. 143–159). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-54885-1_9
- Osterwalder, A., & Pigneur, Y. (2011). *Business Model Generation: Ein Handbuch für Visionäre, Spielveränderer und Herausforderer* (J. T. A. Wegberg, Trans.) (1. Auflage). Campus Verlag. <https://nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-3246145>
- Osterwalder, A., Pigneur, Y., & Tucci, C. L. (2005). Clarifying Business Models: Origins, Present, and Future of the Concept. *Communications of the Association for Information Systems*, 16. <https://doi.org/10.17705/1CAIS.01601>
- Rüger, M., Fischer, D., & Nägele, R. (2018). *Strategieorientierte Geschäftsmodellentwicklung*. <https://doi.org/10.24406/PUBLICA-FHG-255403>
- Schallmo, D. (2013a). *Geschäftsmodelle erfolgreich entwickeln und implementieren: Mit Aufgaben und Kontrollfragen*; [Lehrbuch. Lehrbuch. Springer Gabler. <https://doi.org/10.1007/978-3-642-37994-9>
- Schallmo, D. (2013b). *Geschäftsmodell-Innovation: Grundlagen, bestehende Ansätze, methodisches Vorgehen und B2B-Geschäftsmodelle*. Zugl.: Ulm, Univ., Diss., 2012. Research. Springer Gabler. <https://doi.org/10.1007/978-3-658-00245-9>
- Teece, D. J. (2010). Business Models, Business Strategy and Innovation. *Long Range Planning*, 43(2-3), 172–194. <https://doi.org/10.1016/j.lrp.2009.07.003>



Authors

Inan Gür

Fraunhofer ISST
inan.guer@isst.fraunhofer.de

Niklas Schulte

Fraunhofer ISST
niklas.schulte@isst.fraunhofer.de

Isaac Henderson Johnson Jeyakumar

Fraunhofer IAO
isaac-henderson.johnson-jeyakumar@iao.fraunhofer.de

Michael Lux

Fraunhofer AISEC
michael.lux@aisec.fraunhofer.de

Michael Kubach

Fraunhofer IAO
michael.kubach@iao.fraunhofer.de

Contact

Inan Guer

Research Associate
IT Service Providers

Tel. +49 231 9 76 77-418
inan.guer@isst.fraunhofer.de

www.isst.fraunhofer.de

Image Credits

©anyaberkut – iStock, title

©S and V Design – AdobeStock, pp.4,12,18,22,26,32,37