CENTRE OF EXCELLENCE
DATA SHARING & CLOUD

Trustworthy Claims and Credentials across Data Spaces

Towards Cross-Cutting Trust Frameworks for Data Sovereignty

Concept ICDS 2026 Conference Paper

August 2026

www.coe-dsc.nl
info@coe-dsc.nl

Title:	Trustworthy Claims and Credentials across Data Spaces: Towards Cross-Cutting Trust Frameworks for Data Sovereignty	
Author(s):	H. Bastiaansen, B. Farias Loscio	TNO
	A. van den Wall Bake, M. Punter	TNO
Date:	August 2026	
Number of pages:	16	

www.coe-dsc.nl
info@coe-dsc.nl

Summary

This concept paper has been submitted to the 3rd International Conference on Digital Sovereignty 2026 (ICDS 2026), to be held from November 25th until November 27th, in Oslo (Norway).

The goal of this paper is to disseminate the results of the CoE-DSC work on the role of (governance of) verifiable credentials and claims within the bigger perspective of cross-cutting trust frameworks to support data sharing initiatives and data spaces in enabling cross-community use cases. As such, it is closely related to the development, deployment and adoption of the combination of the community-driven and participation-driven data sharing models, together with a Common Carrier Layer as enabler for large-scale interoperability harmonization and reuse of facilities. The participation-driven model based on a Common Carrier Layer may become a key success factor for broad adoption of data space architectures and concepts and realizing the EU ambition of the Common European Data Spaces, as expressed in the EU Data Strategy.

The audience of the paper, therefore, is the broader (applied) community of data sharing governance authorities, policymakers and architects, aiming to foster the discussion on policymaking for the development and deployment of interoperable and harmonized cross-cutting trust frameworks.

Abstract of the ICDS 2026 paper

Data sovereignty and trust are central to Europe's data economy and the development of Common European Data Spaces (CEDS). As technical architectures, standards, and building blocks mature, key deployment and adoption challenges increasingly shift to governance and policy. This is particularly relevant for claims and credentials, which are foundational to federated data-sharing architectures under the European Data Strategy. Their issuing, verification, and validation therefore require suitable governance mechanisms to support large-scale adoption. In the context of the EU Data Strategy, CEDS architectures, and cross-cutting trust frameworks, this paper identifies and addresses the main governance topics for claims and credentials.

Keywords

European Data Strategy, Data Spaces, Verifiable Credentials, Claims, Trust Anchors, Community-Driven, Participant-Driven, eIDAS 2.0, Digital Identity.

www.coe-dsc.nl
info@coe-dsc.nl

1 Introduction

Data spaces are a core element of Europe's Data Strategy [1], which aims to establish Common European Data Spaces [2] and create a single market for data. Data sovereignty and trust are central to this ambition: data sovereignty enables data holders to define and enforce sharing conditions, while trust assures participants that data is accurate, used as agreed, and protected through appropriate governance, legal, and technical mechanisms.

The data-sharing landscape is expanding rapidly, including Common European Data Spaces and other Data Sharing Initiatives (DSIs) and communities [3]. However, many initiatives remain organizationally and technically fragmented, limiting interoperability and reuse. Increasingly, use cases extend beyond a single data space, for example in Digital Product Passports under the ESPR Regulation [4], collaborative Digital Twins [5], and Privacy Enhancing Technologies (PETs) [6]. Such applications combine data, services, and actors across sectors and therefore require trust mechanisms that operate across communities.

Enabling cross-community data sharing requires harmonized trust frameworks and their coordinated adoption toward a common overarching objective. However, currently, trust frameworks are still largely siloed within individual data spaces. Each data space may define its own onboarding processes, legal agreements, credentials, and trust anchors. Robust cross-cutting trust frameworks are therefore needed to provide a shared trust foundation for data sharing across the boundaries of individual data spaces.

Within these frameworks, claims and credentials provide assurance about participants, rights, capabilities, certifications, and compliance with data-space rules. Although a limited set of credentials is legally harmonized at EU level, such as Person Identification Data [7] and the Mobile Driver's License [8], and other initiatives are also being developed, such as the Large Scale Pilot WeBuild [9], broader governance is still needed to enable the reuse of credential schemas, issuer roles, and trust anchors across data spaces and participant-driven data sharing relationships.

This paper addresses this governance gap by identifying categories of cross-cutting trust frameworks and discussing trust models for credential issuance. Together with maturing technologies for verifiable credentials, trusted data transactions, and electronic signatures, these frameworks and models provide important foundations for trusted data sharing across data-space boundaries.

Nevertheless, technology and trust models alone do not solve the governance challenge. A sustainable policy and governance model is still required to determine how credential schemas are harmonized, how issuer roles and trust anchors are recognized, and how responsibilities, liabilities, and cross-community trust decisions are allocated. The paper therefore discusses the key challenges that must be addressed to develop such a model and to enable harmonized, scalable, and trusted data sharing across data sharing communities.

This paper is structured as follows. Section 2 introduces key concepts of claims and credentials for trusted data sharing. Section 3 describes cross-cutting trust architectures, while Sections 4 and 5 discuss models for issuing and verifying trustworthy claims and credentials and the related governance challenges. Section 6 concludes the paper.

www.coe-dsc.nl
info@coe-dsc.nl

2 Fundamental concepts for trusted data sharing

This section introduces the core concepts to enable trusted data sharing and it explains how these elements support verification, policy enforcement, contract negotiation, and scalable trust across data spaces. In the remainder of this section, consider the definitions in Table 1.

2.1 Claims and credentials

Within the trust framework, claims and credentials play a foundational role in assuring trustworthiness of various types of entities, e.g. participants, rights, capabilities, certifications, and compliance conditions. They enable data to be shared in a trustworthy manner. Claims and credentials may provide a standardized way to cryptographically verify the assurances during onboarding, discovery, contract negotiation, policy enforcement, and audit processes. As a result, they help translate abstract trust requirements into operational assurances: participants can demonstrate who they are, which roles or permissions they hold, whether they meet specific legal, organizational, or technical requirements, and under which conditions they may provide or consume data. The role of claims and credentials is especially important for cross-cutting data-sharing use cases that span multiple communities, sectors, or jurisdictions, where participants cannot rely on a single centralized authority or a single data space-specific trust framework. Hence, claims and credentials, together with their verification and validation, are key to enabling data sovereignty and trust in scalable architectures for cross-community data sharing as part of the emerging European data economy.

Table 1. Definitions of core concepts for trusted data sharing[1].

Claim: An assertion made about a subject.
Credential: A set of one or more claims made by an issuer. The claims in a credential can be about different subjects. [2]
Verifiable Credential: A tamper-evident credential whose authorship can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verifiable.
Validation: The assurance that a claim from a specific issuer satisfies the business requirements of a verifier for a particular use. This specification defines how verifiers verify verifiable credentials and verifiable presentations. It also specifies that verifiers validate claims in verifiable credentials before relying on them. Verifiers trust certain issuers for certain claims and apply their own rules to determine which claims in which credentials are suitable for use by their systems.
Verification The evaluation of whether a verifiable credential or verifiable presentation is an authentic and current statement of the issuer or presenter, respectively. This includes checking that the credential or presentation conforms to the specification, the securing mechanism is satisfied, and, if present, the status check succeeds. Verification of a credential does not imply evaluation of the truth of claims encoded in the credential.

[1] Most definitions are taken from W3C (https://www.w3.org/TR/vc-data-model-2.0/#dfn-credential). The concept Trust Anchor is defined by the IETF (https://www.rfc-editor.org/info/rfc5914).

[2] Although with these definitions of “claim” and “credential”, the former is formally included in the definition of the latter as well. However, for reasons of common use of (the combination of) both terms, they will both be used alongside each other in this paper.

Verifier: A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation for processing. Other specifications might refer to this concept as a relying party.
Issuer: A role an entity can perform by asserting claims about one or more subjects, creating a (verifiable) credential from these claims, and transmitting the (verifiable) credential to a holder.
Trust Anchor: An authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information or actions for which the trust anchor is authoritative

For these fundamental concepts of trusted data sharing, claims and credentials provide important trust capabilities. Standards and protocols play a key role in making claims and credentials interoperable across data-sharing contexts. Within the European Digital Identity Framework [10] technical interoperability is converging around a limited set of credential formats and exchange protocols, including ISO/IEC 18013-5 mdoc, SD-JWT VC, OpenID4VCI and OpenID4VP [11]. This provides a baseline for issuing, presenting and verifying credentials. Yet for data sharing, standardization must also address the meaning and assurance of claims: which credential types are recognized, which attributes they contain, which issuers may provide them, and under which governance arrangements they can be relied upon.

2.2 Participant agents and the Data Space Protocol

To establish trusted data sharing transactions, the participants have a data space participant agent (or “connector”), consisting of a Control Plane that manages discoverability, trust, and contracts, and a Data Plane that handles the actual movement and exchange by means of traditional, well-known protocols (ex: HTTPS, MQTT, Kafka). Various open-source implementations of the data space participant agent are (becoming) available, e.g. as provided by the Eclipse Data Space Components (EDC) framework [12] and the Simpl-open initiative [13]. The Control Plane implements the Data Space Protocol (DSP) [14] for establishing trusted data sharing transactions. The DSP includes a contract negotiation protocol and the machine readable ODRL language [15] for defining usage policies, together with the DCAT protocol [16] for registering and discoverability of data sharing assets. Fig. 1 depicts these fundamental concepts for trusted data sharing.

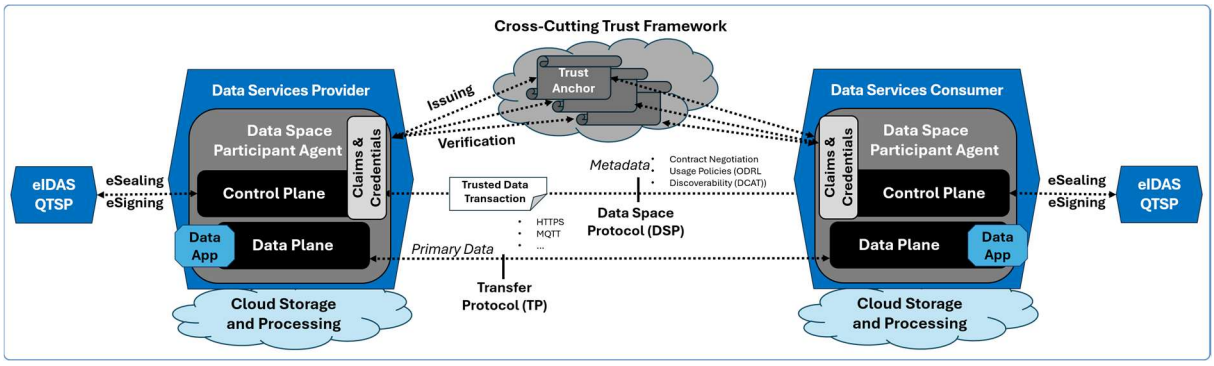


Fig. 1. Data sharing between participant agents enabled by the Data Space Protocol (DSP), the Trusted Data Transaction standards, and qualified electronic signatures.

2.3 Trusted Data Transactions

In addition, CEN/CENELEC is currently developing the Trusted Data Transaction standards [17]. They define the requirements on a common structure for data sharing transactions. This format allows claims and credentials to be included within the data product definition, alongside permissions, prohibitions, and obligations, where obligations may reference applicable claims and credentials. Although other types of claims can be included as well, the CEN/CENELEC Trusted Data Transaction standards distinguish three basic types of claims: (i) identity claims, (ii) data rights claims, and (iii) data space participation claims. Various technical standards and protocols are available for formatting and verifying

these claims. For executing a trustworthy data transaction, the claims and credentials that are bilaterally negotiated between participants need verification and validation. The use of Verifiable Credentials (VCs), in combination with the issuing trust anchor, therefore, provides additional assurances.

Using the combination of the DSPs negotiation protocol, the Trusted Data Transaction standards for claims and credentials and the ODRL protocol of usage policies enables the dynamical establishment of technical data sharing agreements between participants. However, from a legal perspective, these are not yet legally binding. This requires qualified electronic signatures, e.g. as implemented by means of the electronic seals (eSeals) and signatures (eSignatures) as mandated by the EU eIDAS regulation [18]. Qualified eIDAS eSeals and eSignatures service offerings are already becoming broadly available in EU member states, provided by eIDAS Qualified Trust Service Providers (QTSPs).

2.4 Community-driven and participant-driven approaches for data sharing

Data spaces are commonly organized according to a community-driven approach. In this model, a group of stakeholders establishes a data sharing environment around a shared domain, sector, region, or use case. The data space governance authority defines the common rules, onboarding procedures, trust mechanisms, semantic agreements, and technical requirements that apply to the community. Claims and credentials are therefore typically issued, interpreted, and trusted within the boundaries of that specific community. This approach is effective when participants have similar requirements and when data sharing mainly takes place within a well-defined ecosystem.

However, community-driven approaches become more difficult to scale when data sharing use cases cross the boundaries of individual data spaces. Participants that need to interact with multiple communities may have to complete several onboarding processes, comply with different governance frameworks, and manage different trust and credential mechanisms. Similarly, data spaces that want to federate with each other must align agreements across legal, organizational, semantic, and technical levels. As the number of data spaces grows, this creates complexity for both participants and governance authorities.

The participant-driven approach [19] addresses this limitation by enabling individual participants to establish trusted data sharing relationships directly with one another, independently of membership in the same data space. In this model, trust is created at the level of the bilateral interaction between a data provider and a data consumer, supported by interoperable claims, credentials, identity services, contract negotiation mechanisms, and legally binding data transaction contracts. Rather than relying solely on community-specific trust frameworks, participants can present and verify claims and credentials as part of the data sharing process itself.

For the topic of trustworthy claims and credentials, the distinction between these two approaches is important. In a community-driven model, credentials mainly express membership, accreditation, or compliance within a specific data space. In a participant-driven model, credentials must be usable across data space boundaries and support dynamic verification between parties that may not share the same governance authority. A trustworthy claims and credentials framework for data spaces should therefore support both models: community-specific assurance where needed, and cross-community verification where participants need to establish trust beyond the boundaries of a single data space.

www.coe-dsc.nl
info@coe-dsc.nl

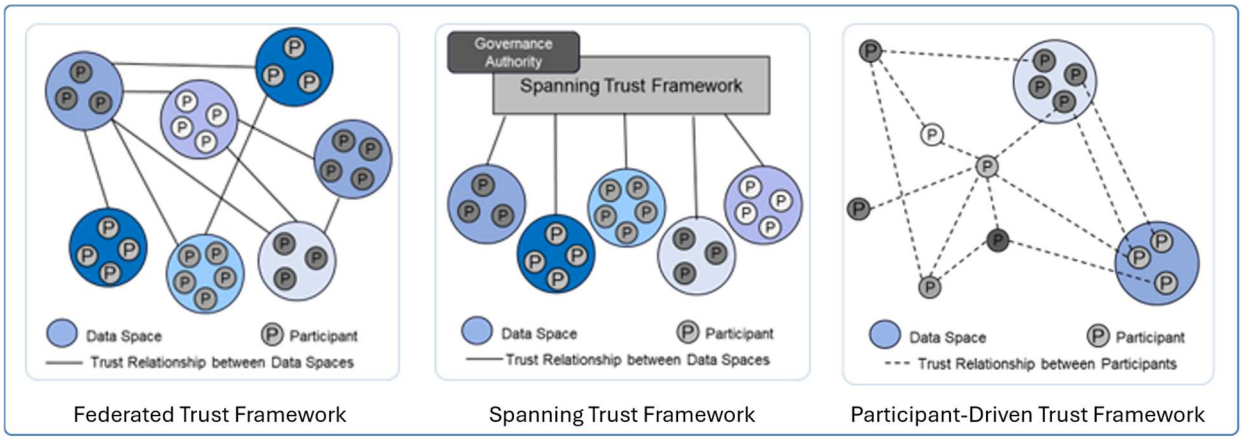
3 Cross-cutting trust framework topologies

This section distinguishes two main categories of cross-cutting trust frameworks: *community-driven* and *participant-driven*. Each category addresses a different governance need in enabling trust across data sharing communities and participants. These types are explained below and illustrated in Fig. 2.

In *community-driven trust frameworks*, Data Space Governance Authorities (DSGAs) define cross-community legal, organizational, semantic, and technical trust conditions on behalf of participants. Two types are distinguished: *federated* and *spanning trust frameworks*. In federated frameworks, data spaces recognize each other's memberships, rules, policies, and credentials, while agreeing on additional legal and technical conditions for cross-data-space use cases. Spanning frameworks provide shared trust capabilities—such as legal conditions, identification services, and attestation processes—governed by a separate body that manages onboarding and trust services for participating data spaces. Each data space must be onboard to the spanning trust framework.

In *participant-driven trust frameworks*, individual participants, such as data service providers and consumers, manage their own trusted data sharing relationships. They can dynamically establish bilateral or multilateral legally binding trust relationships at run time, even when they belong to different data sharing communities or data spaces. This can be done through direct contract negotiation, without prior design-time legal agreements. Such contracts may include usage and access conditions, intellectual property rights, liability terms, and dispute resolution mechanisms, for example.

Fig. 2. Cross-cutting trust frameworks.



www.coe-dsc.nl
info@coe-dsc.nl

4 Trust models for credential issuance

Cryptographic verification proves that a credential was issued by a specific entity and has not been altered, but it does not establish whether the issuer is competent, the claim is correct, or the credential is fit for a particular decision. Governance must therefore define how issuers become trusted. As depicted in Table 3, three ideal-typical approaches are relevant.

Table 3. Trust models for credential issuance: advantages and disadvantages.

Fully decentralized identity	**Regulated or authoritative issuance**	**Accredited issuance**
In this model, any entity may technically issue a credential, while the relying party decides which issuers, credential types, evidence, and assurance levels it accepts. Trust may rely on existing relationships, reputation, community endorsement, trust registries, or credentials issued to the issuer itself.	In this model, legislation or another binding public framework authorizes specific entities to issue credentials, such as passports, civil-register extracts, or professional licenses. Trust mainly derives from the issuer's legal mandate and authentic source. [3]	The accreditation model sits between open reliance and public designation. A scheme owner defines requirements for governance, evidence, security, competence, auditability, and revocation. Organizations that meet these requirements may issue credentials within a defined scope, with recurring assessment maintaining confidence over time.
Advantages		
High flexibility: new issuers and credential types can emerge without prior regulatory approval. *Low central bureaucracy*: trust policies can be adapted to a relying party's risk appetite and use case. *Pluralism and innovation*: communities can establish alternative forms of authority and reputation rather than depending on established institutions.	*High legal certainty*: relying parties can rely on a clearly defined issuer mandate and statutory legal effects. *Uniform assurance*: common issuance and verification rules facilitate large-scale and cross-border acceptance. *Public accountability*: democratic oversight, administrative law, and formal complaint mechanisms can protect credential holders.	*Balance between openness and assurance*: multiple issuers can participate while maintaining a common quality level. *Scalability*: new issuers can enter by satisfying published criteria rather than requiring individual legislative designation. *Shared responsibility*: relying parties can refer to an established assurance scheme when demonstrating due diligence

[3] Under the European Digital Identity Framework, such attestations have defined legal effects within a regulated trust framework.

www.coe-dsc.nl
info@coe-dsc.nl

Fully decentralized identity	Regulated or authoritative issuance	Accredited issuance
Disadvantages		
Liability: relying parties must justify issuer trust and may bear legal and operational responsibility if credentials prove unreliable. *Fragmentation*: different relying parties may assess the same credential differently, reducing interoperability and predictability. *Platform dominance*: trust may concentrate around well-known actors, making recognition harder for smaller or less visible issuers.	*High bureaucracy*: changing credential definitions, adding issuers, or adopting new technologies may require lengthy legislative or administrative procedures. *Limited flexibility*: a small set of authoritative issuers can become a bottleneck and may not address specialized or emerging use cases. *State dependency*: reliance on state-issued credentials becomes risky if public authorities become unreliable, captured, or exclusionary.	*Governance overhead*: accreditation requires scheme management, audits, monitoring, complaints procedures, and mechanisms for suspension or withdrawal. *Risk of formalistic compliance*: successful auditing does not necessarily guarantee that every underlying credential claim is correct. *Barriers to entry*: accreditation costs may favor large incumbents and exclude smaller organizations or community-based issuers.

These three approaches form a continuum. Low-risk credentials may rely on verifier-defined trust, high-impact public credentials may require authoritative issuance, and professional or sector-specific credentials may benefit from accreditation. The appropriate model depends on how discretion, liability, and societal authority are distributed among issuers, relying parties, scheme operators, and public institutions.

www.coe-dsc.nl
info@coe-dsc.nl

5 Governance of claims and credentials for data sharing: challenges, discussion and future directions

As architecture, standards, and protocols for cross-cutting trust frameworks mature, the main challenge increasingly lies in governance. Although some credentials are being harmonized at EU level or developed through public and private initiatives, the landscape remains fragmented. Broader governance is therefore needed to align reusable claim and credential schemas, issuer frameworks, and trust anchors across data-sharing communities. Additionally, some are being developed as private initiatives by European organizations to support the emerging data spaces landscape, such as GAIA-X [20] for infrastructural services and iSHARE [21] for data sharing rights.

These individual initiatives will help future harmonization. However, a broader governance effort is needed toward aligned, accepted and reusable claim and credential schemas, issuer frameworks and trust anchors to support the broader range of emerging cross-cutting trust frameworks as described in the previous sections. This governance effort should address the following main challenges in claims and credentials:

- *Ensuring reliable issuing and verification:* Trust depends on credentials to be managed (issued and verified) by mandated, accredited and recognized, trust anchors, preferably implemented as *verifiable credentials*. This must be supported by transparent criteria, described by the appropriate trust model.
- *Supporting multiple cross-cutting trust framework topologies:* Different data sharing relationships require multiple coexisting trust framework topologies, supported by an associated set of claims and credentials. Specifically, this requires both claims and credentials that (i) describe participation in specific data sharing initiatives or data spaces (e.g. the data space participation claims as standardized by CEN/CENELEC), and (ii) address specific topics at the individual participant (organization) level, such as legal identity, financial credibility, or ISO certification.
- *Standardizing claim definitions and profiles:* Claims must be easily and uniquely interpretable and reusable by both data sharing initiatives and individual participants. A wildly expanding proliferation of new, overlapping and non-interoperable set of claims and credentials should be prevented. This may require harmonized and agreed definitions, profiles, and semantics.

As future direction, a set of orchestration principles for trust frameworks, claims and credentials may be required, as discussed in the following.

Governance for the harmonization of claims and credentials needs to be addressed across the two types of approaches for cross-cutting data sharing use cases: the community-driven approach and the participant-driven approach. The active development of claims and credentials on specific topics needs to be pursued in alignment with the goals and ambition of the EU Data Strategy. Neutral orchestrators must provide leadership and stewardship in developing, deploying, and adopting cross-cutting trust frameworks, rather than relying solely on market initiatives. Cross-community trust decisions must be made with joint awareness of both community and participant perspectives, while the market supplies conformant services. Existing communities should therefore be used as springboards for trust framework harmonization, rather than developing new ad hoc trust frameworks.

www.coe-dsc.nl
info@coe-dsc.nl

6 Conclusions

As described in this paper, claims and credentials are an important component for enabling cross-cutting trust frameworks to support cross-community data sharing use cases. They are fundamental for realizing the data economy and EU's ambition of the Common European Data Spaces. Currently, a diverse set of actors is shaping, guiding, and aligning the development and deployment of trust frameworks. These public and private actors — spanning governance, technical, and operational roles — must work together to move from today's fragmented landscape of siloed data sharing initiatives towards a harmonized, consistent, scalable, and interoperable trust foundation for cross-community data sharing use cases. This needs orchestration, with a requirement for (neutral) orchestrators to take the lead in development, deployment and adoption of harmonized trust frameworks and their associated and required claims and credentials.

At the same time, existing communities can serve as springboards to initiate the governance approach towards the development and deployment of such a harmonized and overarching trust framework, claims and credential strategy. In the context of the common European Mobility Data Space (EMDS), the European Commission (EC) has already reacted to the fragmented and siloed landscape of data sharing initiatives by proposing an Interlinking Layer [22] as a core part of the EMDS to enable cross-data space data discovery by collecting metadata in a federated catalogue. By extending this foundation from discoverability to interoperable trust, the EMDS Interlinking Layer can serve as a practical springboard for harmonizing trust frameworks, claims, and credentials across European data spaces.

www.coe-dsc.nl
info@coe-dsc.nl

Acknowledgement

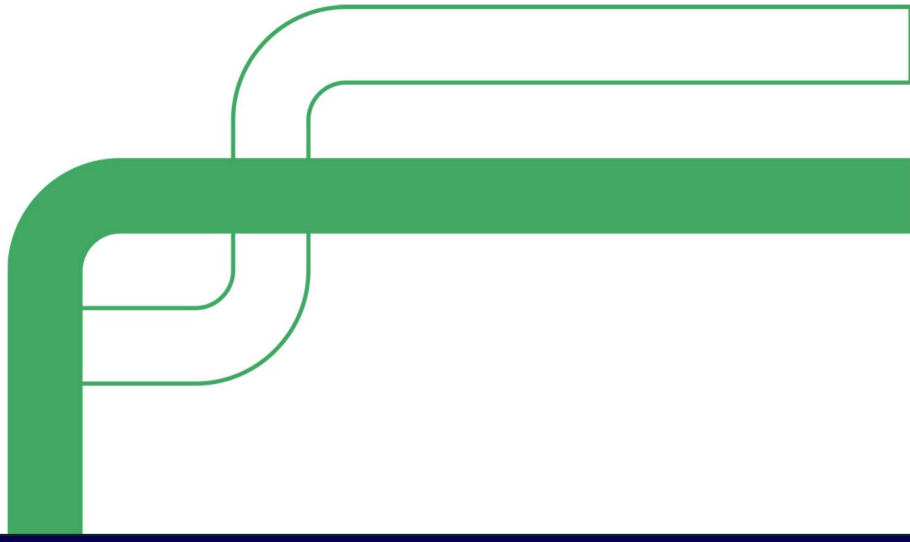
The work presented in this paper was conducted under the umbrella of the Dutch Centre of Excellence for Data Sharing and Cloud (CoE DSC, www.coe-dsc.nl).

www.coe-dsc.nl
info@coe-dsc.nl

References

1. European Commission Homepage, https://digital-strategy.ec.europa.eu/en/policies/ strategy-data, last accessed 2026/03/19.
2. European Union, https://eur-lex.europa.eu/eli/reg/2023/2854/oj/, last accessed 2026/03/19.
3. Oliveira, S., et al.. Investigations into data ecosystems: a systematic mapping study. *Knowledge and information systems*, 61, 589-630 (2019).
4. European Commission Homepage, https://eur-lex.europa.eu/eli/reg/2024/1781/oj, last accessed 2026/03/19.
5. TNO. 'Reliable and Real-Time Digital Twin Systems'. https://www.tno.nl/en/digital/digital-innovations/data sharing/reliable-real-time-digital-twin-systems, last accessed 2026/06/29.
6. OECD: Emerging privacy-enhancing technologies: current regulatory and policy approaches. OECD Digital Economy Papers, No. 351. OECD Publishing, Paris (2023).
7. Regulation (EU) 2024/1183 establishing the European Digital Identity Framework, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183 (2024)
8. European Commission rules on electronic attestations of attributes, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C%282025%295046 (2025)
9. GitHub. https://github.com/webuild-consortium, last accessed 2026/08/31.
10. European Union. Regulation 2024/1183. 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng, last accessed 2026/08/31.
11. European Union. Architecture and Reference framework https://eudi.dev/latest/about/#the-architecture-and-reference-framework, last accessed 2026/08/31.
12. Eclipse Foundation, https://projects.eclipse.org/projects/technology.edc, last accessed 2026/03/19.
13. European Commission. Simpl-Open. https://simpl-programme.ec.europa.eu/dashboard/simpl-open, last accessed 2026/08/27.
14. International Data Spaces Association, https://internationaldataspaces.org/offers/dataspace-protocol, last accessed 2026/03/10.
15. W3C. https://www.w3.org/TR/odrl-model, last accessed 2026/03/19.
16. W3C. https://www.w3.org/TR/vocab-dcat-2, last accessed 2026/03/19.
17. TDT. Trusted Data Transaction towards standardization. https://www.trusted-data-transaction.org/trusted-data-transaction-towards-standardization, last accessed 2026/08/30.
18. European Commission. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation, last accessed 2026/03/19.
19. Pretzsch, S. et al.. Towards a Common Carrier Layer - A First Step for a Participant-Driven Data Sharing Approach for Data Spaces. Accepted as a chapter for the DSSC book (Q4 2026). Concept available: https://coe-dsc.nl/wp-content/uploads/2025/12/coe-dsc-a-participant-driven-data-sharing-model-for-data-spaces.pdf.
20. Gaia-X. A Federated Secure Data Infrastructure. https://gaia-x.eu, last accessed 2026/08/27.
21. ISHARE. Trust Framework for Data Rights. https://ishare.eu, last accessed 2026/08/27.
22. European Commission. https://transport.ec.europa.eu/transport-themes/smart-mobility/creating-common-european-mobility-data-space_en, last accessed 2026/03/10.

www.coe-dsc.nl
info@coe-dsc.nl



Colophon

This concept paper is a result of the work of the Dutch Centre of Excellence for Data Sharing and Cloud (CoE-DSC, www.coe-dsc.nl), specifically its work on on the role of (governance of) verifiable credentials and claims within the bigger perspective of cross-cutting trust frameworks to support data sharing initiatives and data spaces in enabling cross-community use cases. It has been submitted to ICDS 2026) conference, to be held from November 25th until November 27th, in Oslo (Norway).

The goal of this concept is to disseminate the results of the CoE-DSC to the broader (applied) community of data sharing governance authorities, policymakers and architects, aiming to foster the discussion on policymaking for the development and deployment of interoperable and harmonized cross-cutting trust frameworks.

Authors

- H. Bastiaansen, B. Farias Loscio, G. Kruithof TNO
- A. van den Wall Bake, M. Punter TNO

Contact

- Centre of Excellence for Data Sharing and Cloud (CoE-DSC)
- E-mail — info@coe-dsc.nl
- Website — www.coe-dsc.nl

August 2026

CoE DSC

www.coe-dsc.nl
info@coe-dsc.nl