CEN

WORKSHOP

AGREEMENT

CWA 18245

July 2025

ICS 35.030

English version

Trusted Data Transaction - Part 2: Trustworthiness requirements

This CEN Workshop Agreement was corrected and reissued by the CEN-CENELEC Management Centre on 16 July 2025.

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This CEN Workshop Agreement has been developed in accordance with the CEN/CENELEC Guide 29 “CEN and/or CENELEC Workshop Agreements - A rapid way to standardization” and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was approved by a Workshop of representatives of interested parties on 2025-06-13, the constitution of which was supported by CEN following the public call for participation made on 2023-02-10. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2025-06-27.

The following organizations and individuals developed and approved this CEN Workshop Agreement:

- AIRBUS – Arnaud Cauchy
- BIG DATA VALUE ASSOCIATION (BDVA) – Daniel Alonso and Ana Garcia
- DATA SPACES SUPPORT CENTRE – Boris Otto
- DAWEX – Fabrice Tocco
- EDF – Mazen Samaan
- FIWARE - Chandra Challagonda
- FRAUNHOFER ISST – Jan Jürjens and Tobias Guggenberger
- GAIA-X – Giuditta Del Buono and Pierre Gronlier
- HUB ONE DATA TRUST – Romain Rollet
- INTERNATIONAL DATA SPACES ASSOCATION (IDSA) – Silvia Castellvi
- MICROSOFT – Eric Samson
- PROMETHEUS-X – Matthias De Bièvre
- STICHTING ISHARE FOUNDATION - Rajiv Rajani
- TNO – Simon Dalmolen and Matthijs Punter

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CEN policy on patent rights is described in CEN-CENELEC Guide 8 “Guidelines for Implementation of the Common IPR Policy on Patent”. CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk. The CEN Workshop Agreement should not be construed as legal advice authoritatively endorsed by CEN.

Introduction

Sharing of data can have significant commercial, financial, privacy and other impacts on all stakeholders involved. Therefore, it is important to identify the requirements for trustworthiness of data transactions.

Data transactions can take place in many different organisational set-ups, requiring an interplay between data rights holders, data providers, data users and any involved data intermediaries facilitating the sharing of data, through technical, legal or other means.

Agreements between these actors are established in data usage contracts, containing policies, terms and conditions for the sharing of data between two or more participants. Data usage contracts can be bound by commonly established technical and legal agreements (i.e. policies, semantic models, protocols and processes). In data spaces, such agreements are managed by a Data Space Governance Authority (DSGA) and documented in the data space rulebook, providing the common trust context and supporting services for data sharing.

CWA 18125:2024 (Trusted Data Transaction – Part 1) provides the terminology, concepts and mechanisms for trusted data transactions. This CWA (Trusted Data Transaction – Part 2) defines the trustworthiness requirements for trusted data transactions.

1 Scope

This document provides trustworthiness requirements and guidance for participants in support of trusted data transactions.

Specifically, it defines a set of foundational principles for trusted data transactions, and establishes general requirements and guidance that apply to all phases of a trusted data transaction, and specific requirements for each phase of a trusted data transaction.

This document applies to all types of participants, regardless of their type or size.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CWA 18125:2024, *Trusted Data Transaction*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in CWA 18125:2024 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1 General

3.1.1
principle
fundamental truth, proposition or assumption that serves as foundation for a set of beliefs or behaviours or for a chain of reasoning

3.2 Trust

3.2.1
claim
statement of something to be true including associated conditions and limitations

3.2.2
evidence
information supporting a claim

3.2.3
policy
set of rules related to a particular purpose

Note 1 to entry: A rule can be expressed as an obligation, an authorization, a permission or a prohibition.

Note 2 to entry: Policies enable the structured evaluation of claims.

3.2.4
reconciliation
process of evaluating and demonstrating that policies are fulfilled by the claims and evidence to a sufficient degree

3.2.5
trust
decision that an entity of interest can be relied upon

Note 1 to entry: Trust comes often with a certain level of risk acceptance.

Note 2 to entry: Trust is associated to a defined context of use for a given entity of interest.

Note 3 to entry: Trust can be based on evidence.

3.2.6
trustworthiness claim
claim about a set of trustworthiness characteristics, processes, behaviours, events or facts related to the trustworthiness of an entity of interest

3.2.7
trust framework
set of requirements, rules, roles, responsibilities and assessment mechanisms in support of trust

3.2.8
trust service
enabling service that offers assurances within a data transaction

[SOURCE CWA 18125:2024, 4.13]

3.2.9
trust anchor
well-defined, shared authority that creates assurances

[SOURCE CWA 18125:2024, 4.14]

3.2.10
content integrity
property that content has not been altered or deleted by unauthorised parties

[SOURCE: ISO 7498-2:1989, 3.3.21, modified: data replaced by content]

3.3 Data sharing

3.3.1
participant
natural or legal person that engages in a data transaction

Note 1 to entry: Participants can be represented by a software instance.

3.3.2
interoperability
ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged

[SOURCE ISO/IEC 22123-1:2023]

3.3.3
data space rulebook
documentation of the data space governance framework for operational use

[SOURCE DSSC Data Spaces Blueprint v2.0]

3.3.4
data space governance framework
structured set of principles, processes, standards, protocols, rules and practices that guide and regulate the governance, management and operations within a data space to ensure effective and responsible leadership, control, and oversight

[SOURCE DSSC Data Spaces Blueprint v2.0]

3.3.5
data quality
degree to which a set of inherent characteristics of data fulfils requirements

[SOURCE: ISO 8000-2:2022, 3.8.1, modified: Note to entry removed]

3.3.6
observability
ability to monitor and verify the state and behaviour of a trusted data transaction

3.3.7
traceability
ability to log and track a trusted data transaction throughout its lifecycle

Note 1 to entry: Traceability enables compliance, accountability, dispute resolution, and proof of execution.

Note 2 to entry: Traceability ensures compliance with legal and ethical standards, allowing stakeholders to follow the flow of data transactions while preserving trust and security.

3.3.8
data lineage
description of the entire history of data, including its creation, transformation, and the processes it undergoes

Note 1 to entry: Data lineage provides a comprehensive map of how data evolves during its lifecycle.

3.3.9
data provenance
information on the place and time of origin, derivation or generation of data, proof of authenticity of the data, or a record of past and present ownership of the data

[SOURCE: ISO/IEC 5259-1:2024, 3.16 with modification, data set replaced by data]

4 Principles for trusted data transactions

4.1 Introduction

The objective of this clause is to define the overarching principles that serve as foundation for the detailed requirements in Clause 5.

4.2 Phases of a data transaction

Trust shall be established during all phases of a trusted data transaction, involving all relevant participants, each with defined roles specific to the phase.

4.3 Data rights

Data rights holders should have sufficient control over how their data is accessed and used through technical or legal means, in accordance with agreed data usage policies and in compliance with relevant regulations.

4.4 Data products

The concept of data product is at the core of trusted data transactions, since it bundles all the elements needed to make the data findable, shareable, and usable.

Data rights holders and data providers should rely on data governance processes and systems to manage their data products (and data and metadata therein) along the lifecycle of the data product.

4.5 Data quality

Data quality is a multi-dimensional concept relating to aspects such as accuracy, integrity, completeness, and the provenance of the data. If data is not tailored to its intended purpose, it can fail to generate meaningful outcomes, regardless of its inherent quality. Data quality can be managed through technical means and appropriate data governance processes.

The quality of a data product is critical to ensuring trust in the transaction. The data quality of a data product should be accurately described using metadata, enabling to verify that the data is suited to the purpose or application in which the data will be used.

NOTE Regulations or data spaces can impose rules for the expected quality of certain types of data products.

4.6 Data provenance and data lineage

Data provenance captures details about who created the data, when and how, including the context of data generation (e.g., environmental conditions, tools, and methodologies used). It also documents certifications, licenses, and regulatory attributes to ensure compliance with legal and ethical standards. A tamper-resistant provenance scheme enhances trust and auditability, allowing stakeholders to verify the authenticity, integrity, and legitimacy of data sources across trusted transactions.

Data lineage involves tracking transformations, merges, and derivations, establishing a relationship between raw data and processed outputs. A comprehensive data lineage framework ensures that data usage stays aligned with regulatory requirements and quality and transparency standards.

Parties involved in trusted data transactions should implement robust data governance processes to ensure that metadata within the data product includes all necessary information to guarantee accurate data provenance (origin and historical record) and data lineage (lifecycle and transformations).

4.7 Observability and traceability of data transactions

Observability ensures that data transactions can be monitored and diagnosed, providing insights into system behaviour, performance, security threats and potential failures by continuously collecting and analysing relevant signals.

It ensures that data sharing systems are working correctly, in compliance with shared values, enhancing confidence among stakeholders.

Key functions include, without being limited to:

- anomaly detection,
- root cause analysis when issues occur, and
- real-time insights into data transaction performance.

Traceability ensures that data transactions can be tracked, logged, monitored, and verified throughout their lifecycle, providing an audit trail for accountability, compliance, and dispute resolution.

Traceability provides transparency, helping participants and regulators ensure that data usage aligns with policies, ethical guidelines, and contractual agreements.

Key functions include, without being limited to:

- ensuring accountability by tracking who performed what action and when,
- providing a complete audit trail for compliance,
- enabling verification of contractual and regulatory adherence, and
- supporting non-repudiation, ensuring data transactions cannot be denied.

By incorporating traceability functions, participants can ensure accountable and secure data transactions.

NOTE Traceability can be applied to transactions within a data space as well as to transactions across different data spaces.

Participants involved in data transactions should rely on data governance processes and systems to ensure their data transactions are observable and traceable.

4.8 Data spaces

Data spaces are not giant data warehouses or data lakes hosted in a shared, centralised storage. Metadata and claims are being exchanged during the negotiation process. If and how the data is physically transferred depends on the agreement between individual parties.

Participants of a data space adhere to a common governance framework, documented in a data space rulebook. The governance framework defines all policies and services which apply and defines the relevant trust framework for each of them.

Trusted data transactions can be facilitated by data spaces: When parties are participants of the same data space, implying adherence to the common data space rulebook, this facilitates trusted data transactions.

4.9 Interoperability across data spaces

Parties can choose to adhere to the rulebooks of multiple different data spaces when they wish to share data across different domains or contexts. Data space governance authorities can facilitate this by defining interoperable policies, services and associated trust frameworks.

Interoperability across data spaces can be achieved by using common terminologies for expressing policies, adopting common protocols and services as well as associated trust frameworks. Interoperable data space rulebooks can facilitate connections between participants and services across different data spaces.

NOTE Added interoperability can be achieved by creating multiple specific instantiations of an overarching rulebook or by creating explicit links between multiple rulebooks.

4.10 Trust frameworks

Trust frameworks provide a way to establish trust between participants in a data transaction. In defining a trust framework, the following elements are specified:

- the rules a participant in a data transaction must comply with,
- the semantic models of the trust information exchanged, and
- the processes and technical standards adopted to perform and possibly automate compliance checks.

A data space shall rely on one or more trust frameworks.

A data space may combine and/or extend trust frameworks to fit their needs, or alternatively define its own trust framework, as long as the result complies with the requirements for trust frameworks in Clause 5.

The use of interoperable trust frameworks can help to create synergy effects across different domains, enabling connections across data spaces.

4.11 Trust policy dimensions

Trusted data transactions are inherently complex, as they encompass a wide variety of use cases, business models, IT architectures while adhering to laws and regulations across multiple jurisdictions.

Trust policies for data transactions should address three dimensions: Legal, operational and technical. While the three dimensions rely on one another, separation of these three dimensions helps to enable reuse and interoperability in different contexts.

5 Trustworthiness requirements

5.1 Introduction

The primary objective of this section is to define a comprehensive set of trustworthiness requirements for trusted data transactions, taking the principles discussed in section 4 as a basis.

To this end, the section is structured around the six phases of a data transaction identified in Part 1:

i) Grant rights,

ii) Publication,

iii) Discovery,

iv) Negotiation,

v) Data exchange / sharing, and

vi) Access and usage.

5.2 General requirements

5.2.1 Overview

This section covers general trustworthiness requirements that apply to all phases of a trusted data transaction, addressing the role of trust frameworks and data space governance authorities.

5.2.2 Identification of participants

5.2.2.1 General

Verification of the identity of participants is a critical process in establishing trust, ensuring that all participants in a data transaction are known to each other. Automated verification relies on digital evidence of the participant's identity.

5.2.2.2 Digital identity

Participants shall possess a valid digital identifier issued by a recognised identity provider.

NOTE Identity providers can be recognised by participants, the data space governance authority, or any other competent authority.

5.2.2.3 Evidence of digital identity

The evidence provided by identity providers shall:

1) be provided to other participants in a machine-readable format;

2) include a reference to the identity provider;

3) include an identifier of the participant that is unique within the domain of the identity provider.

5.2.3 Policies, claims and evidence

5.2.3.1 General

Claims, policies and evidence work together to establish trust. Automated resolution of policies, claims and evidence is based on semantic alignment of the metadata.

5.2.3.2 Issuer of policies, claims and evidence

The issuer of each policy, claim and evidence shall be identifiable.

NOTE For example, by including metadata in a claim with a resolvable identifier pointing to the issuer's information.

5.2.3.3 Identification of policies, claims and evidence

Each policy, claim and evidence shall be identified with a unique identifier in the context of the issuer.

5.2.3.4 Identification of objects of policies, claims and evidence

The object(s) of policies, claims and evidence shall be identified with a unique identifier in the context of the issuer of the identifier.

EXAMPLE Machine referenced in a policy. The machine ID is unique within the domain of the issuer of the identifier.

5.2.3.5 Verification of content integrity of polices, claims and evidence

The content integrity of each policy, claim and evidence shall be verifiable by other participants. Mechanisms for the verification of content integrity of policies, claims and evidence shall be documented, and this documentation shall be made available to all participants.

NOTE For example, using a cryptographic signature.

5.2.3.6 Authentication of party to which polices, claims and evidence are issued

The party to which the policy, claim or evidence has been issued shall be authenticable.

NOTE For example, with key-binding during claim issuance.

5.2.3.7 Verification of validity of polices, claims and evidence

The validity of a policy, claim and evidence shall be verifiable by other participants. Mechanisms for the verification of the validity of a policy, claim and evidence shall be documented, and this documentation shall be made available to all participants.

NOTE For example, by including validity dates and revocation status.

5.2.3.8 Presentation of evidence

Evidence shall be presented in a manner that enables both manual and automatic validation.

5.2.3.9 Presentation of claims

Claims should be presented in a machine-readable form.

5.2.4 Operational and legal aspects of policies, claims and evidence

5.2.4.1 General

The acceptance of the trusted data transaction occurs when policies, claims and evidence have been compiled and reconciled to a level of trust accepted by all signing parties.

The legal certainty of trusted data transactions relies on the validity and enforceability of policies, claims and evidence in the jurisdiction(s) where the transaction takes place.

5.2.4.2 Reconciliation of policies, claims and evidence

Participants involved in trusted data transactions shall reconcile the policies, claims and evidence.

NOTE Trusted data transactions are between a single data provider and a single data user. Agreements between multiple data providers and data users can be decomposed into multiple trusted data transactions.

5.2.4.3 Legal enforceability of policies, claims and evidence

Participants in trusted data transactions shall ensure that policies, claims and evidence are legally valid and enforceable.

5.2.4.4 Reconciliation of policies, claims and evidence of data intermediaries

When data intermediaries are involved, participants shall reconcile the policies, claims and evidence of involved data intermediaries, to the extent these policies, claims and evidence are relevant to the data transaction.

EXAMPLE 1 The data intermediary receives a fee based on the transaction being established.

EXAMPLE 2 Regulations require a data intermediary to be involved in the transaction.

5.2.5 Trust frameworks

5.2.5.1 General

A trust framework provides pre-defined methods and processes to collect, organise and compile policies, claims and evidence, for participants to perform their risk assessment before deciding to participate in a trusted data transaction.

The trust framework supports the decision-making process of the participants involved in the transaction, whereas the participants remain responsible for the ultimate trust decision.

5.2.5.2 Trust framework requirements

The trust framework shall define:

1) the allowed methods to identify policies, claims and evidence;

2) the allowed methods to identify the object(s) of policies, claims and evidence;

3) the allowed methods to identify the issuer of policies, claims and evidence;

4) a taxonomy to describe the different types of policies, claims and evidence;

5) the semantic model(s) used to describe the policies, claims and evidence.

5.2.6 Data spaces

Data sharing within data spaces relies on the verification of membership.

Before membership credentials are issued, each participant provides its recognised identifier along with any additional information or certifications required by the data space governance authority (DSGA). Participation in a data space implies the acceptance of the data space rulebook, acceptance of these common rules is an important aspect of trustworthiness.

In support of the execution of data transactions, the data space governance authority helps to ensure trust and accountability among participants by providing the means to verify whether a given participant is member of a given data space.

The data space governance authority shall:

1) ensure validation of all claims referenced in the data spaces rulebook, during onboarding of a new member;

   NOTE 1 Execution of the validation can be delegated to trusted third parties.

   NOTE 2 This includes re-validation during the full membership lifecycle.

2) define a mechanism to verify the membership of a data space participant;

   NOTE The data space governance authority can provide additional information about the participant.

3) define a mechanism to validate other claims referenced in the data space rulebook;

4) define a mechanism to validate claims of other data spaces for which agreements have been established.

5.3 Grant rights

5.3.1 Overview

The objective of the grant rights phase is to ensure that participants have clear, verifiable, and enforceable rights to publish, share, access, and use data according to agreed terms and legal requirements. In case the data rights holder and data provider are different parties, establishing evidence of granted data rights is paramount in the context of data transactions.

5.3.2 Evidence of granted data rights

If the data rights holder and data provider are different parties, evidence of granted data rights shall include:

1) traceable records of delegation, including any legal documentation;

   NOTE Traceable records provide information on the specific purposes for which the data rights holder has granted rights to the data provider.

2) metadata that defines the data products to which the granted data rights apply, including purpose of use and any use restrictions or explicitly prohibited uses of the data (e.g., no redistribution, no commercial use);

3) metadata that defines the allowed kinds of data users to which the granted data rights apply;

   NOTE Metadata can for example specify the entities or roles (e.g., researchers, analysts, third-party vendors) allowed to access and use the data.

4) any applicable information on the data provenance and data lineage;

5) insofar as personal or sensitive data are the object of the transaction, any applicable information about the consent or permission for data sharing and usage.

5.4 Publication

5.4.1 Overview

The objective of the publication phase is to make the data product visible to potential data users. Main involved elements are the data product and the data catalogue(s) where the data product will be published.

The data catalogue can be operated by the data provider or by a data intermediary.

5.4.2 Verification of publication rights

The rights granted to the data provider can include the right to publish the data product under specific terms (see clause 5.3).

In case the data catalogue is operated by a data intermediary, the data provider should be able to show evidence of the publication rights, and the data intermediary should be able to verify this.

The party that operates the data catalogue shall ensure that it only publishes data products for which the data provider has the appropriate rights.

5.4.3 Catalogue metadata of the data product

The catalogue metadata of the data product is the subset of the metadata that enables to make the data product visible and discoverable for potential users. The information about the data product serves to enable other parties to easily find the data product (further addressed in the Discovery section) and

assess its trustworthiness, applicability, quality and relevance. This information also includes the rights or limitations for the use of the data product for specific purposes, as well as specific conditions in the case of personal data.

The catalogue metadata of a data product shall:

1) provide a description of the data product that enables the user to distinguish between the different data products and make an informed decision about the fitness for its intended use;

2) be up-to-date;

   NOTE Reflecting the current status of the data product.

3) be provided in a machine-readable format;

   NOTE For example, the format as agreed by the data space participants.

4) at minimum, contain the required metadata;

   NOTE For example based on the required fields according to agreed-upon standard(s) between participants or agreed minimum requirements of a data space.

5) describe the policies regarding the visibility of the product metadata;

   NOTE For example, in case visibility of the data product metadata is limited to certain organisations.

6) provide information on the data access methods that are supported by the data product;

7) describe the use restrictions and licence terms that apply to the data product;

   NOTE This includes any legal restrictions and requirements that apply.

8) where applicable, reference the data collection methodology;

   NOTE The exact requirements will depend on the intended domain and context in which the data product will be used.

9) describe the data provenance and data lineage;

   NOTE In case the data product includes anonymized or pseudonymized data, data lineage includes information about the applied anonymization or pseudonymization method.

10) where applicable, reference the data quality methodology that was applied, including information on related data quality dimensions and metrics.

    NOTE 1 For example using agreed-upon quality standards such as the ISO 8000 series or domain-specific quality frameworks.

    NOTE 2 The exact data quality requirements will depend on the intended domain and context in which the data product will be used.

5.4.4 Data catalogue requirements

Parties operating a data catalogue need to ensure the trustworthy publication of the catalogue metadata of data products.

The data catalogue shall:

1) support the agreed machine-readable formats for the publication of catalogue metadata;

2) be able to process all agreed catalogue metadata attributes;

3) ensure that only authorised users can publish or modify metadata in the catalogue.

NOTE This includes mechanisms to control access to metadata and the data product itself, audit records of publication and access control changes.

5.5 Discovery

5.5.1 Overview

The objective of the discovery phase is to enable potential data users to discover data products and make an informed decision on their appropriateness for the intended purpose, before engaging in a trusted data transaction.

Data discovery services can be offered by data providers and by data intermediaries.

Metadata accessed via a discovery service should be easily accessible by potential data users. This ensures a seamless user experience, facilitating the discovery of the most relevant data products and providing all necessary information for informed decision-making.

5.5.2 Verification of rights and access control

Discovery services enable access to relevant data products to potential data users, for example participants of data space(s). A discovery service manages access on multiple levels: 1. Access to the discovery service, 2. Access to general attributes of data products 3. Access to the full metadata of a data product.

The discovery service shall:

1) ensure that it only makes data products discoverable from data catalogues for which it has access rights;

2) incorporate mechanisms to manage access to specific data products to groups of authorised users.

NOTE For example, access is limited to parties that are member of the data space in which the product is intended to be offered.

5.5.3 Discovery service requirements

The primary goal of discovery services is to provide potential data users with all the necessary information to make informed decisions about whether to engage in a data transaction for a data product.

The discovery service shall:

1) present query results in a way that enables potential data users to assess the relevance and suitability of the data product;

NOTE 1 For example, through summaries specifying the dataset's purpose, scope, and intended use cases, with preview or samples of data, or any other mechanism.

NOTE 2 This includes data quality and provenance indicators to support decision-making.

NOTE 3 This can include multi-lingual and localisation capabilities.

2) provide information about data access conditions, rights, and licence terms of the data product.

5.5.4 Discovery service recommended features

Discovery services can play an important role in establishing data transactions, enabling data users to get in touch with data providers, enter in negotiations, and provide feedback.

The discovery service should:

1) support automated access;

   NOTE For example via an API.

2) help interested users to initiate negotiations or transactions;

   NOTE For example, mechanisms that allow to request additional information about a specific data product.

3) incorporate mechanisms to provide feedback to the data provider about the data product.

5.6 Negotiation

5.6.1 Overview

The objective of the negotiation phase is to formally record the agreed data usage contract in a machine-readable form.

NOTE The formally recorded contract will transcribe the terms in the legal contract as well as the authorisation given by the data rights holder.

5.6.2 Verification of rights

The data provider shall be able to provide evidence that it has the right to authorise usage of the data product.

5.6.3 Recording of the data usage contract

The data usage contract must be recorded in such a way that it cannot be disputed and can serve as legal foundation in case problems arise.

The recorded data usage contract shall:

1) include all mandatory contractual elements;

2) be registered in a way that ensures availability to all involved participants (data provider, data user, other involved parties);

3) include an unambiguous reference to the data product(s);

   NOTE This implies access to the metadata of the data product(s) at the time of signing the contract.

4) specify the terms of usage, including any applicable data usage permissions and data usage consent;

5) follow a commonly agreed standard.

   NOTE For example the agreed-upon standard within a data space.

5.7 Data sharing/exchange

5.7.1 Overview

The data sharing/exchange phase involves at a minimum the data user and data provider but can also involve data intermediaries and other service providers.

5.7.2 Identification, authentication and authorisation

Before the sharing/exchange of data, the data provider shall:

1) verify the identity of the data user;

2) evaluate the authorisations of the data user;

3) insofar as personal or sensitive data are the object of the transaction, verify the validity of any related data usage consents or permissions.

5.7.3 Observability of data transactions

Trusted data transactions can be monitored as per agreed conditions set in the contract or to comply with regulations. A trusted third party can assist in observing and logging the transactions.

Participants shall comply with the agreed mechanisms for observability of data transactions.

NOTE 1 For example requirements on the observability as defined in the data space rulebook.

NOTE 2 These mechanisms can be implemented by the data provider and the data user, potentially assisted by a third party.

5.8 Data access and usage

5.8.1 Overview

This phase covers the access and use of the data by the data user for a particular use case or application.

5.8.2 Verification of access rights

Data access rights need to be verified each time the data is accessed, since these can have expired or been revoked.

The data provider shall:

1) verify the authorisations each time before providing access to the data to the data user;

2) have the means and right to stop providing the data in case the data user does not respect the data usage contract.

NOTE The data provider may represent multiple data producers that rely on this capability.

5.8.3 Usage of data

The conditions agreed during contract negotiation need to be respected. Applicable data usage consent and data usage permissions need to be verified each time the data is used, since these can have expired.

The data user shall:

1) verify beforehand whether the data usage permissions and data usage consent are in line with what was agreed in the data usage contract;

2) verify validity of data usage permissions and data usage consent before using the data.

5.8.4 Observability

Data access and usage can be monitored as per agreed conditions set in the contract or to comply with regulations. A trusted third party can assist in observing and logging the transactions.

Participants shall comply with the agreed mechanisms to support observability of data transactions.

Annex A
(informative)

Trust frameworks

A.1 Introduction

Trust frameworks help to establish trust between participants and so facilitate trusted data transactions. They provide assurance of the identity of participants and the validity of claims about them, as well as of the services and data products they provide, in accordance with agreed-upon standards and principles.

A trust framework achieves this by:

- linking trust to specific, well-defined criteria, such as technical standards, security measures, integrity, traceability, and other quality attributes;
- defining a reliable process for enforcing the trust based on these criteria.

The scope and rules covered by a trust framework can be specific or generic:

1) Specific trust framework: A framework that defines rules and standards to achieve a specific purpose or is commonly used in a specific ecosystem.

2) Generic trust framework: A framework that defines rules and standards which can be applied across many different digital ecosystems.

A.2 Trust mechanisms

In establishing trust in data transactions, the policies from each participant are matched with claims from the other participant. This process, called “policies to claims reconciliation”, is the primary means of building trust, enabling participants to feel comfortable in trusting the other party – and the data that is being shared. The process, often supported by technology, enables to validate that the agreed requirements and criteria are met.

NOTE For example, where a policy requires that the “participant is based in Europe”, the participant would provide a claim that provides evidence of that policy being met.

At the technical level, participants are represented by software components or software agents. This simplifies and enhances interoperability between trusted data sharing solutions. The process is executed by asking participants for attestations or claims regarding their compliance and validating these with internal or external services.

Trust anchors serve as the ultimate point of trust from which an entity begins its validation process. The trustworthiness of trust anchors is based on the recognized authority of the organisation, which can be established by governmental bodies (e.g., for identity verification) and other entities (e.g., recognized compliance verification or accreditation bodies).

This basic trust creation mechanism is flexible enough to cover various conditions, constraints and requirements.

A.3 Elements of trust frameworks

While trust mechanisms are the specific processes and technologies used to establish and verify trust, trust frameworks provide the overarching structure and guidelines within which these mechanisms operate.

A trust framework comprises two core dimensions:

1) governance dimension: The set of requirements and criteria which apply to participants and the transactions they engage in. These requirements and criteria can relate to all conceptual layers (legislative, economic, technical).

2) process/technical dimension: The process to implement and operationalise the governance dimension, including the technical means (e.g. software) to actually perform and possibly automate validation and verification of the criteria defined in point 1.

Governance dimension

Requirements and criteria for the governance dimension of the trust framework can stem from different sources:

1) legal frameworks;

2) individual policies of participants in the transaction;

3) wider agreements between two or more parties.

Requirements and criteria can be mutually linked and there can be dependencies between them, creating the specific set of rules which need to be met for a specific transaction in a specific context.

The criteria can be related to identities and other elements specifically relevant in the context of data transactions and can reflect and build on top of existing regulations.

NOTE Different levels of trustworthiness may be defined by referring to different sets of criteria or to different trust anchors for the different levels.

Process and technical dimension

To operationalise the governance dimension, the process and technical dimension of the trust framework defines the following elements:

- format of the claims or attestations to be validated and verified,
- the trust anchors and trust service providers accredited to issue attestations for each claim,
- mechanisms to collect claims,
- means to digitalise the criteria,
- semantic models and ontologies,
- protocols used to exchange attestations,
- means and technical standards used to validate and verify attestations,
- means to revoke/suspend the attestations.

NOTE As part of the trust framework, means for rights or trust delegation and consent management may also be specified, together with the computation of indexes providing interoperability metrics and information on the potential trustworthiness of an entity/element in the criteria.

A.4 Trust frameworks and data spaces

On a domain- or ecosystem-level, participants can agree on a set of requirements and criteria that applies to all participants and their transactions, forming a specific trust framework. Knowing that a participant is adhering to the dataspace rulebook can greatly facilitate trusted data transactions between large groups of participants.

In data spaces such a trust framework is captured as part of the dataspace rulebook, managed by the Dataspace Governance Authority (DSGA). In addition, the Dataspace Governance Authority can take on the role of trust anchor in the data space.

Re-using an already existing trust framework for establishing a trust-enforcing environment for trusted data transactions can be beneficial in terms of interoperability with and among relevant other initiatives committed to enhancing trust in data exchanges.

Bibliography

[1] European Commission, European Strategy for Data, 2020

[2] European Commission, Staff Working Document on Common European Data Spaces, 2022

[3] European Commission, Second Staff Working Document on Common European Data Spaces, 2024

[4] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[6] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)