Date: 2025-04-1

prCWA XXXXX: XXXX

Secretariat: AFNOR

Trusted Data Transaction — Part 2: Trustworthiness requirements

ICS:

CCMC will prepare and attach the official title page.

This CEN Workshop Agreement is an agreement, developed and approved by an open independent workshop structure within the framework of the CEN-CENELEC system.

This CEN Workshop Agreement reflects the agreement of the registered participants responsible for its content, who decided to develop this document in accordance with the specific rules and practices available in CEN for the development and approval of CEN Workshop Agreements.

This CEN Workshop Agreement can in no way be held as being a European Standard (EN) developed by CEN, as it does not represent the wider level of consensus and transparency required for a European Standard (EN). Furthermore, it is not intended to support legislative requirements or to meet market needs where significant health and safety issues are to be addressed. For this reason, CEN cannot be held accountable for the technical content of this CEN Workshop Agreement, including in all cases of claims of compliance or conflict with standards or legislation.

The Workshop parties who drafted and approved this CEN Workshop Agreement, the names of which are indicated in the Foreword of this document, intend to offer market players a flexible and timely tool for achieving a technical agreement where there is no prevailing desire or support for a European Standard (EN) to be developed.

Contents

Page

European foreword

This CEN Workshop Agreement has been developed in accordance with the CEN/CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping 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 YYYY-MM-DD, the constitution of which was supported by CEN following the public call for participation made on YYYY-MM-DD. 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 YYYY-MM-DD.

Results incorporated in this CWA received funding from the [European Union's Horizon 2020 research and innovation programme] [Euratom research and training programme 2014-2018] under grant agreement No [Number].

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

- name organization/individual
- name organization/individual
- …

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 evolved. 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 intermediary services 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 "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 defines the requirements to establish trust in data transactions. It defines the foundational principles for trusted data transactions, general trustworthiness requirements that apply to all phases of a transaction and specific trustworthiness requirements for each individual phase.

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.

- CEN CWA 18125:2024, *Trusted Data Transaction - Part 1*

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

[SOURCE ISO 37000:2021, 3.2.1]

3.2 Trust

3.2.1

claim

statement of something to be true including associated conditions and limitations

[SOURCE: ISO/IEC 15026-1:2010, 2.4]

Note 1 to entry: In its entirety, a claim conforming to ISO/IEC 15026-2 is an unambiguous declaration of an assertion with any associated conditionality giving explicit details including limitations on values and uncertainty. It could be about the future, present, or past.

3.2.2

evidence

information supporting a claim or the occurrence of an event or action

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

property of an entity to meet specified requirements in a verifiable way

[SOURCE: ISO/IEC AWI 31303]

3.2.7

trustworthiness claim

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

[SOURCE: ISO/IEC AWI 31303]

3.2.8

trust framework

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

3.2.9

trust service

enabling service that offers assurances within a data transaction

[SOURCE CWA 18125:2024 4.13]

3.2.10

trust anchor

well-defined, shared authority that creates assurances

[SOURCE CWA 18125:2024 4.14]

3.2.11

content integrity

assurance the content has not been altered or deleted by unauthorized parties

3.3 Data sharing

3.3.1

participant

natural or legal person that wishes to share data with other participants or to use shared data from other participants

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

set of principles, standards, policies (rules/regulations), agreements and practices that apply to the governance, management, and operations (including business and technology aspects) of a data space as well as to the enforcement thereof, and the resolution of any conflicts

[SOURCE DSSC Data Spaces Blueprint v2.0]

3.3.5

data quality

degree to which the characteristics of data satisfy stated and implied needs when used under specified conditions

[SOURCE ISO/IEC 25012-1:2008]

3.3.6

data uncertainty

inherent lack of precision, accuracy, or reliability in a data product

Note 1 to entry: data uncertainty can arise at any stage of data product lifecycle

Note 2 to entry: data uncertainty is often quantified as a probability, confidence interval, or qualitative assessment, or a combination thereof

3.3.7

observability
<trusted data transaction>

ability to capture, monitor and analyse the state and behaviour of trusted data transactions

3.3.8

traceability
<trusted data transaction>

ability to track, log, monitor and verify a data transaction throughout its lifecycle

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

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

3.3.9

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 within a system

3.3.10

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 section is to define the principles that serve as foundation for the requirements in section 5. The principles are not requirements, but the assumptions and chain of reasoning on which the requirements are based.

4.2 Data rights

From CWA 18125:2024 (Trusted data transaction - Part 1) the following base principles can be derived:

Principle 1: Trust is established during every phase of a trusted data transaction, involving all relevant participants, each with defined roles specific to the phase.

To foster confidence in trusted data transactions, data rights holders retain a high degree of autonomy in the usage of their data.

Principle 2: Data rights holders 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.

NOTE Digital sovereignty and digital autonomy are important underlying factors that enable the rights of the data holder to be respected by all involved parties.

4.3 Data products and data quality

The concept of data product is at the core of trusted data transactions, since it bundles all the elements needed to make the data easily findable, shareable, and usable. The quality of a data product (considering both data quality and metadata accuracy) is critical to ensuring trust in the transaction.

NOTE In some cases, regulations and data spaces can impose rules for the expected quality of certain types of data products.

Data quality is enabled by the usage of technical means and by establishing appropriate data governance processes. Data providers rely on a robust internal data governance framework for the definition and management of their data products.

Principle 3: Data holders and data providers rely on data governance processes and systems to manage their data products (and data and metadata therein) along the lifecycle of the data product.

Data quality is a multi-dimensional concept relating to aspects such as accuracy, integrity, completeness, and the provenance of the data. Additionally, if data is not tailored to its intended purpose, it may fail to generate meaningful outcomes, regardless of its inherent quality. Data quality dimensions and metrics are described using metadata and reusable, standardized vocabularies.

Principle 4: Trusted data transactions rely on predictable data quality, accurately described using metadata, enabling to verify that the data is suited to the purpose or application in which the data will be used.

4.4 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.

Principle 5: Parties involved in data transactions 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).

4.5 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 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.

Principle 6: Parties involved in data transactions rely on data governance processes and systems to ensure their data transactions are observable and traceable.

4.6 Data spaces

Data spaces are not giant data warehouses or data lakes hosted in a shared, centralised storage. Only metadata and claims are being exchanged during the negotiation process. If and how 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 rulebook. The governance framework defines all policies and services which apply and defines the relevant trust framework for each of them.

If parties are able to determine that they are participant of the same data space, this assures adherence to the rulebook of that data space and so facilitates the creation of trusted data transactions.

Principle 7: Trusted data transactions can be facilitated by 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, services and associated trust frameworks.

Principle 8: Interoperable rulebooks facilitate connections between participants in a data space with services and participants in other 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.

4.7 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 to which the participants in the data transaction are required to be compliant,
- the semantic models of the trust information exchanged, and
- the processes and technical standards adopted to perform and possibly automate compliance checks.

Principle 9: A data space relies on one or more trust frameworks. A single trust framework can support multiple data spaces.

Principle 10: A data space can combine and / or extend trust frameworks to fit their needs, or define its own trust framework, as long as the result complies with the requirements for trust frameworks (see section 5).

Principle 11: The use of technically and semantically interoperable trust frameworks can help to create synergy effects across different domains, enabling connections across data spaces.

4.8 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 address three dimensions: Legal, operational and technical. Separation of these three dimensions helps to enable reuse and interoperability in different contexts.

The three dimensions rely on one another: the operational and legal dimensions often rely on the technical dimension for their implementation.

Principle 12: Trustworthiness requirements that are defined across technical, operational, and legal dimensions help to enhance reusability and interoperability.

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.

The requirements are identified by addressing two key questions:

- What actions must the involved stakeholders perform?
- What features or attributes must the involved components or services possess?

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

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.

5.2.2.1 Digital identity

Participants shall possess an active, digital identifier issued by a recognised identity provider.

NOTE 1 Identity providers can be recognized by participants, the data space rulebook, or any other competent authority.

NOTE 2 Identifiers can be recognized by participants, the data space rulebook, or any other competent authority.

5.2.2.2 Evidence of digital identity

The evidence provided by identity providers shall:

1) be provided to other participants in a machine-readable format, including a machine-readable mechanism for the validation of the evidence based on the current state of the technology.
2) include a reference to the identity provider
3) include the unique identifier of the participant

NOTE Unique within the domain of the identity provider.

5.2.3 Policies, claims and evidence

Claims, policies and evidence work together to establish trust. Automated resolution of policies, claims and evidence relies on technical requirements regarding the metadata.

5.2.3.1 Issuer of policies, claims and evidence

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

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

5.2.3.2 Identification of policies, claims and evidence

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

5.2.3.3 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.

5.2.3.4 Verification of content integrity of polices, claims and evidence

The content integrity of each policy, claim and evidence shall be verifiable.

EXAMPLE For example, using a cryptographic signature.

5.2.3.5 Verification of party to which polices, claims and evidence are issued

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

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

5.2.3.6 Verification of validity of polices, claims and evidence are issued

The validity of a policy, claim and evidence shall be verifiable.

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

5.2.3.7 Presentation of evidence

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

5.2.3.8 Presentation of claims

Claims should be presented in a machine-readable form according to the state of technology.

5.2.4 Operational and legal aspects of policies, claims and evidence

The acceptance of the trusted data transaction occurs when policies, claims and evidence have been compiled and reconciled to a level of risk assessment 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.

5.2.4.1 Reconciliation of policies, claims and evidence

Participants involved in trusted data transactions shall reconcile:

1) the policies, claims and evidence of the primary involved parties;

   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.

2) the policies, claims and evidence of any involved data intermediaries, to the extent these policies, claims and evidence are relevant to the data transaction.

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

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

5.2.4.2 Legal enforceability of policies, claims and evidence

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

5.2.5 Trust frameworks

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.

At the time of the realisation of the transaction, the trust framework supports the decision-making process of the participants involved in the transaction.

The participants remain responsible for the ultimate trust decision.

5.2.5.1 Trust framework requirements

The trust framework shall:

1) define the allowed methods to identify policies, claims and evidence;
2) define the allowed methods to identify the object(s) of policies, claim and evidence;
3) define the allowed methods to identify the issuer of a policy, claim or evidence;
4) provide a taxonomy to describe the different types of policies, claims and evidence

NOTE Claims can be declaration or 1st party assessment, evidence or 2nd party assessment, proofs or 3rd party assessment (reference to ISO/IEC 17000:2020).

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

5.2.5.2 Trust framework recommended features

The trust framework should provide policies, claims and evidence in support of the realisation of a trusted data transaction.

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 This also happens during 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.

5.3.2 Evidence of granted data rights

Establishing evidence of granted data rights is paramount in the context of data transactions. In case the data rights holder and data provider are different parties, it enables the data rights holder to provide evidence of the granted data rights to the data provider. The scope of the data on which rights are being granted is an important element, enabling it to be well-understood by all involved parties.

Evidence of granted data rights shall include:

1) delegation rights (traceable records of delegation);

2) legal documentation granting power of attorney to act on behalf of the data rights holder for specific purposes;

3) information on the data provenance and lineage, to ensure legitimate ownership and data sharing;

4) information about the explicit and informed consent for data sharing and usage, where personal or sensitive data are involved;

5) 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);

6) 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.

5.4 Publication

5.4.1 Overview

The requirements in this section build on the requirements in section 5.3 (Grant rights).

The objective of the publication phase is to make the data product visible to its potential users or participants, by including it in one or more data catalogues or through other agreed methods.

Involved actors in this stage are the data provider and possible data intermediaries providing a catalogue service. Main involved elements are the data product in general and its metadata description in particular, the catalogue service(s) where the data product might be published.

The catalogue service can be offered by an intermediary or by the data provider. An additional scenario is when the catalogue is composed of multiple individual catalogue services in a federated manner.

5.4.2 Verification of publication rights

The rights granted to the data provider will include the right to publish the data product under specific terms (publication rights). In case the catalogue service is provided by an intermediary, the data provider needs to be able to show evidence of the publication rights, and the intermediary needs to be able to verify these.

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

5.4.3 Data product metadata

The metadata about the data product 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 for specific purposes, as well as specific conditions in the case of personal data.

The data product metadata shall:

1) provide an accurate and specific description of the data product;

2) be consistent and up to date;

NOTE To ensure that data is well-documented, discoverable, and interpretable (metadata quality)

3) be provided in a machine-readable format;

4) be complete;

Note 1 For example based on the required fields according to agreed-upon standard(s)) or agreed minimum requirements of a data space.

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

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

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

NOTE This includes any legal restrictions and requirements, such as GDPR.

7) 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.

8) describe the data lineage;

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

9) describe the data provenance;

10) reference the data quality methodology that was applied.

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

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

5.4.4 Catalogue service requirements

For catalogue services provided by data intermediaries, specific requirements apply to ensure the trustworthy publication of the data product metadata.

The catalogue service shall:

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

2) be able to process all agreed data product metadata attributes;

3) ensure that only authorized 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 and manageable 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 for which it has the appropriate rights;
2) incorporate mechanisms to manage access to specific data products to groups of selected 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 under trustworthy conditions. Therefore, queries and query responses are structured in a way that maximizes usability, transparency, and relevance for discovery, evaluation, and trust-building.

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;

EXAMPLE 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 1 This includes data quality and provenance indicators to support decision-making.

NOTE 2 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;

EXAMPLE For example via an API.

2) help interested users to initiate transactions or negotiations;

EXAMPLE For example, mechanisms that allow to request additional information about 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 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 they have the right to authorise usage of the data product.

5.6.3 Recording of data usage contract

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

The data usage contract shall:

1) be in a legally valid form;

   NOTE This means that all mandatory contractual elements need to be present.

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 signing the contract.

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

5) be recorded using a commonly agreed standard.

   EXAMPLE 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 services providers.

5.7.2 Identification, authentication and authorisation

Before the data sharing/exchange can happen, the data provider verifies with whom it is sharing the data and performs the necessary authentications and validations of claims.

The data provider shall:

1) verify the identity of the data user before the sharing/exchange of data;

2) evaluate the authorisations of the action(s) requested by the data user before the sharing/exchange of data;

3) verify the validity of the related data usage consents, in case of personal data, before the sharing/exchange of data.

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 support and implement agreed mechanisms to support observability of data transactions.

EXAMPLE For example requirements of the observability as defined in the data space rulebook.

NOTE 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

The objective of the data access and usage phase is to access and use the data, in accordance with the agreed terms.

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 revoked.

The data provider shall:

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

2) shall 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. The data user shall verify the validity of data usage permissions before using the data.

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.

Annex A Trust frameworks
(informative)

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;
- providing a reliable process for enforcing the trust based on these criteria.

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.

EXAMPLE 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 possible 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 proving compliance with the set of criteria.

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

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 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.

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.

EXAMPLE Examples of generic trust frameworks are the Gaia-X tr and iSHARE trust frameworks.

Generic trust frameworks can provide a foundation for the definition of the governance and the technical/process dimensions (see section A.3). Generic trust frameworks establish requirements and criteria for identities, authorisation, and other important elements in the interaction between the entities involved in the data transaction process. In addition, generic trust frameworks define the processes and methods to operationalise the enforcement of the requirements and criteria, based on widely adopted technical standards and practices. Capitalizing on proven, already implemented and adopted trust frameworks can help data spaces increase their potential market impact and adoption speed.

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)