



HAL
open science

D2.1 - Documentation of available building blocks and technologies

Raffaele Giaffreda, Davaadorj Battulga, Bernd Rauch, Raghad Matar, Piergiorgio Cipriano, Clement Jonquet, Bruno Salinier, Léonard Dallot

► **To cite this version:**

Raffaele Giaffreda, Davaadorj Battulga, Bernd Rauch, Raghad Matar, Piergiorgio Cipriano, et al.. D2.1 - Documentation of available building blocks and technologies. D2.1, CEADS. 2025, 39p. <hal-05506413>

HAL Id: hal-05506413

<https://hal.science/hal-05506413v1>

Submitted on 12 Feb 2026

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons CC BY-ND 4.0 - Attribution - No Derivative Works - International License



DELIVERABLE 2.1

DOCUMENTATION OF AVAILABLE BUILDING BLOCKS AND TECHNOLOGIES



Project title	Deploying and operating an European framework for the secure and trusted data space for agriculture		
Project acronym	CEADS		
Call topic	DIGITAL-2024-CLOUD-DATA-AI-06-AGRISPACE		
Type of action	DIGITAL-SIMPLE		
Coordinator	EIGEN VERMOGEN VAN HET INSTITUUT VOOR LANDBOUW- EN VISSE-RIJONDERZOEK - EV ILVO		
Project number	101195295		
Project start date	1 April 2025	Duration	36 months
URL	https://ceads.eu/		

D2.1 - Documentation of available building blocks and technologies

Due date	31/08/2025	Delivery date	29/08/2025
Work package	WP2		
Responsible Author(s)	R. Giaffreda, D. Battulga (FBK)		
Contributor(s)	B. Rauch, R. Matar (IESE), P. Cipriano (DEDA), C. Jonquet (INRAE), B. Salinier, L. Dallot (Orange)		
Reviewer(s)	A. Moerenhout (EV-ILVO), S. Bosch (VO-ILVO)		
Version	v1.0		
Dissemination level	Public		

DISCLAIMER

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CEADS consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CEADS Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CEADS Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

COPYRIGHT MESSAGE

© CEADS Consortium, 2025-2028. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgment of previously published material and of the work of others has been made through appropriate citation, quotation, or both. Reproduction is authorised provided the source is acknowledged.

Version and amendments history

Version	Date (MM/DD/YYYY)	Created /Amended by	Changes
V0.1	01/07/2025	R. Giaffreda (FBK)	First draft produced
V0.5	22/08/2025	B. Rauch, R. Matar (IESE)	Related DS initiatives contribution
V1.0	28/08/2025	R. Giaffreda (FBK)	Finalised version following interactions and Partners' contributions

Table of Content

- List of Abbreviations 6
- Executive summary 8
- 1 Introduction 9
 - 1.1 Objective 9
 - 1.2 Methodology..... 9
 - 1.3 Link to other tasks and WPs..... 11
 - 1.4 Structure of the Deliverable 11
- 2 CEADS Building Blocks 12
 - 2.1 Canonical Building Blocks 12
 - 2.2 CEADS Onboarding Path and Building Block Mapping 13
 - 2.2.1 Control and Data Planes within CEADS Onboarding Path..... 13
 - 2.2.2 Building Block Mapping 15
 - 2.3 Trust identity framework..... 16
 - 2.3.1 Identity Assurance 16
 - 2.3.2 Trust Anchors 16
 - 2.3.3 Credential Management 16
 - 2.3.4 Policy Enforcement 17
 - 2.3.5 Decentralized vs. Centralized Identity Models and CEADS implementation..... 17
 - 2.3.6 Real-World Examples and Standards..... 17
 - 2.3.7 Challenges and considerations 18
 - 2.4 Catalogues and Metadata 18
 - 2.4.1 Methods of Metadata Enrichment 19
 - 2.4.2 Metadata Standards and Controlled Vocabularies 19
 - 2.4.3 Provenance & Traceability..... 21
 - 2.5 Consent and permission management..... 21
 - 2.6 Interoperability..... 22
 - 2.6.1 Data Interoperability Standards..... 23
 - 2.7 Data Exchange and Monetization 25
 - 2.7.1 Data monetisation 25
 - 2.7.2 Value Creation Services 26
 - 2.8 Data Privacy preservation 26
 - 2.8.1 Compute-to-Data 26
 - 2.8.2 Anonymisation 27
- 3 Reference Architectures and Implementations 28
 - 3.1 Key Initiatives (mapped to CEADS framing) 28

- 3.1.1 SIMPL (Smart Middleware Platform for Cloud-to-Edge Federations)..... 30
- 3.1.2 IDS / Dataspace Protocol 30
- 3.1.3 Gaia-X Trust Framework 31
- 3.1.4 Eclipse Dataspace Components (EDC)..... 32
- 3.1.5 FIWARE Data Space Stack 32
- 3.1.6 Pontus-X 33
- 3.2 Other relevant initiatives..... 34
- 3.3 Summary and Implications for CEADS..... 36
- 4 Conclusions..... 37

LIST OF FIGURES

Figure 1 – First draft of CEADS building blocks 10
Figure 2 – Framework for selecting relevant competences 11
Figure 3 – The DSSC Building Blocks from the Blueprint 2.0 12
Figure 4 – CEADS onboarding path 14

LIST OF TABLES

Table 1 – Building block mapping 15
Table 2 – Mapping related key initiatives 29

List of Abbreviations

Abbreviation	Full term
AI	Artificial Intelligence
API(s)	Application Programming Interface(s)
CEADS	Common European Agriculture Data Space
CKAN	Comprehensive Knowledge Archive Network
CSV	Comma-Separated Values
DCAT	Data Catalog Vocabulary
DCAT-AP	DCAT Application Profile
DLT	Distributed Ledger Technologies
DRM	Digital Rights Management
DSI / DSIs	Data Space Initiative(s)
DSP	Dataspace Protocol
DSSC	Data Spaces Support Centre
EC / EU	European Commission / European Union
EDC	Eclipse Dataspace Components
eIDAS 2.0	electronic IDentification, Authentication and trust Services (EU Regulation 2.0)
ELK (stack)	Elasticsearch, Logstash, Kibana
ETSI	European Telecommunications Standards Institute
EUDI Wallet	EU Digital Identity Wallet
FAO	Food and Agriculture Organization of the United Nations
FHE	Fully Homomorphic Encryption
GDPR	General Data Protection Regulation
GEMET	General Multilingual Environmental Thesaurus
GeoDCAT-AP	Geospatial DCAT-AP
GODAN	Global Open Data for Agriculture and Nutrition
IDS (Connector)	International Data Spaces (Connector)
IDSA	International Data Spaces Association
IoT	Internet of Things
IP	Intellectual Property
JSON	JavaScript Object Notation

MFA	Multi-Factor Authentication
ML	Machine Learning
MPC	Secure Multi-Party Computation
NGSI-LD	Next Generation Service Interfaces – Linked Data
NLP	Natural Language Processing
O&M	Observations and Measurements
ODRL	Open Digital Rights Language
OGC	Open Geospatial Consortium
OPA	Open Policy Agent
RDF	Resource Description Framework
SAREF	Smart Applications REFerence ontology
SensorML	Sensor Model Language
SSI	Self-Sovereign Identity
SSO	Single Sign-On
Tx.x	Task x.x
TF	Trust Framework
UI	User Interface
URI	Uniform Resource Identifier
W3C	World Wide Web Consortium
WP	Work Package
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
ZK Proofs	Zero-Knowledge Proofs

Executive summary

This deliverable illustrates the key building blocks that have been identified as part of the Common European Agriculture Data Space Architecture (CEADS) implementation. Given the extensive work done in other related projects, such as the DSSC and AgriDataSpace, this deliverable is the result of the analysis of potential application domains for dataspace in agriculture; it introduces the building blocks that will create value while ensuring backward compatibility towards those results already achieved and it also includes specific functionality elements that have been identified as characterising the agricultural sector.

While separating the functionality amongst the building blocks, the overall results here shed some light on what incremental integration steps could be to be considered for progressively onboarding functionality and features that make generic DSIs compliant with the expected rules and characteristics of a dataspace.

The document is to be considered as a starting point rather than an exhaustive list, and we expect the boundaries and functionality of each of the proposed building blocks to evolve over time, based on requirements elicited from other project activities, especially those related to the implementation of use-cases.

1 Introduction

1.1 Objective

The objective of this document is to kickstart the process of bringing together a diverse set of Partners and competences to focus on activities to be executed in the project, starting from a high-level set of building blocks that also provide onboarding anchor points and paths for integration that will allow existing DSIs or different organisations' provided datasets to become part of CEADS. Additionally the document sheds some light on existing initiatives that have already produced results in data space domain which will be leveraged to avoid reinventing the wheel and maximise the use of existing standards and implementations for trust and sovereignty management, metadata and catalogues, data models, semantic models and vocabularies and other building blocks that are specific for the agricultural sector.

The reader will therefore find the description of a collection of building blocks rather than a full design (that will come later with Task 2.3), which is to be considered as an ongoing draft architectural canvas giving Partners opportunities for aggregating competences and focusing then their implementation activities without ignoring the wealth of existing initiatives and assets produced to bring dataspace and data economy vision closer to reality.

1.2 Methodology

The methodology used to validate the contents of this deliverable against existing work and Project Partners' expertise is described in this section hereafter.

Starting points were the outcome and project deliverables of the project AgriDataSpace, as well as DSSC Blueprint v. 2.0. The intersection between these two activities was deemed to be a good starting point from a requirements perspective. It is envisaged that there will be an onboarding procedure for DSIs and Organizations that will integrate their data assets into the CEADS and these considerations have guided us in separating functionality between envisaged building blocks. This document will therefore serve as a reference document to understand at what level additional DSIs and Organizations will need to be integrated, according to the assessment of the level of overlap and interoperability between equivalent building blocks.

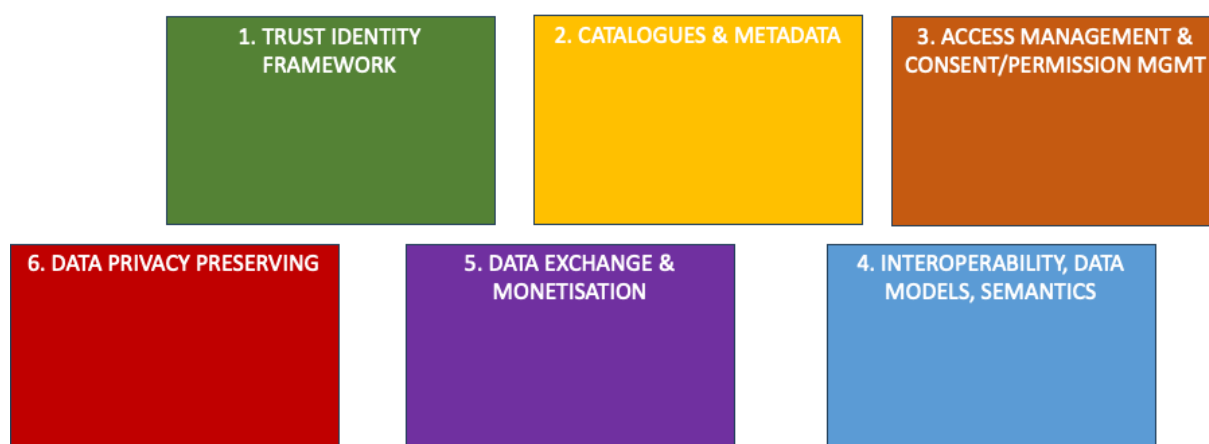


Figure 1 – First draft of CEADS building blocks

As a result of this bootstrapping activity a first draft of building blocks has been proposed (see Figure 1, more details will be provided later in dedicated sections of the document) and feedback requested where all WP2 Partners interested in such project activities provided their input and knowledge to the following leading questions:

1. Which building blocks are you familiar with and have already tackled in previous activities?
2. Which building blocks can you help develop?
3. Are there any other assets not mentioned or related to proposed building blocks that you deem relevant to integrate?

Processing such feedback led to bilateral discussions that took place to validate and refine, with the most appropriate experts, the proposed Building Blocks, involving many of the technology partner of the project. The results reported in this deliverable are the fruit of these preliminary interactions.

Validation and building block assessment didn't uniquely identify the implementation path ahead (this will be further elaborated after requirements elicitation and assessment planned activities) and is therefore to be considered a stepping stone in understanding what assets and competences the Consortium Partners will contribute towards the CEADS implementation.

It is also worth mentioning here that this is a first collection of building blocks rather than a full architectural design (that will come later with Task 2.3); further work will be aimed at refining these results continuing the interactions with Partners and gaining support from Partners based on the framework and questions illustrated below in Figure 2.

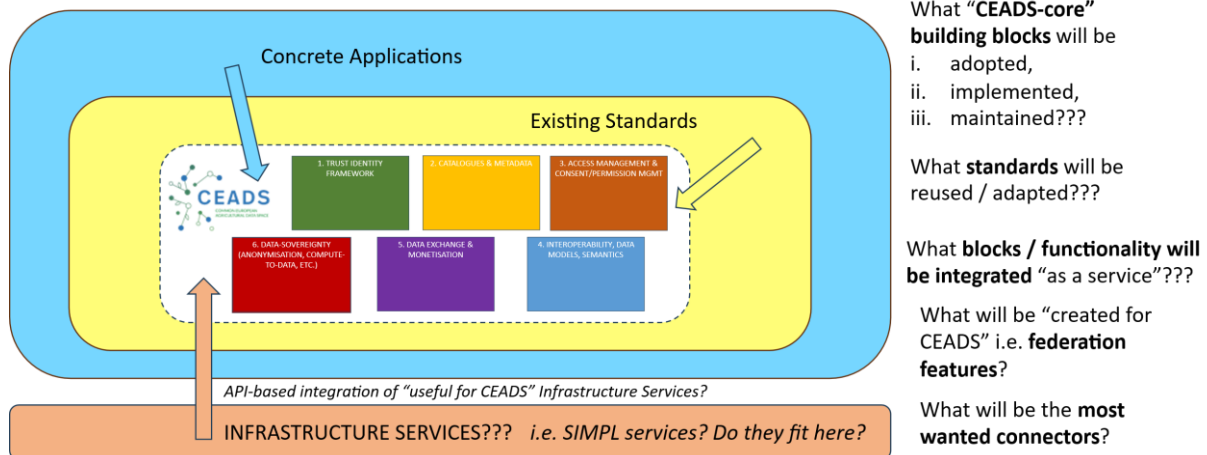


Figure 2 – Framework for selecting relevant competences

1.3 Link to other tasks and WPs

This Deliverable constitutes the foundations of the activities that WP2 will execute, further detailing the overall architecture of the CEADS (expected activities in Task T2.3). It is linked to the activities being executed in the use-cases work-package (WP1) and it supports the execution of other tasks in WP2 expected to do requirements elicitation (Task 2.2), design and implementation of CEADS services (Task 2.3) and help produce the right guidance for onboarding and integration of use case partners (Task 2.4).

1.4 Structure of the Deliverable

The deliverable is structured as follows: Chapter 2 introduces the six building blocks adding more explanation details and mentioning where possible the relevant standards that exist, to provide guidance for standard-based (for interoperability's sake) implementations. Chapter 3 illustrates in a nutshell the mapping towards relevant architectures and implementations from other existing initiatives.

2 CEADS Building Blocks

2.1 Canonical Building Blocks

In order to ground CEADS in the wider European context and to ensure coherence with ongoing initiatives, it is useful to recall the canonical set of technical building blocks as defined in the DSSC Blueprint v2.0. These building blocks are grouped into three functional clusters, each addressing a core capability required for data spaces.

DSSC Technical Building Blocks (Blueprint v2.0¹)

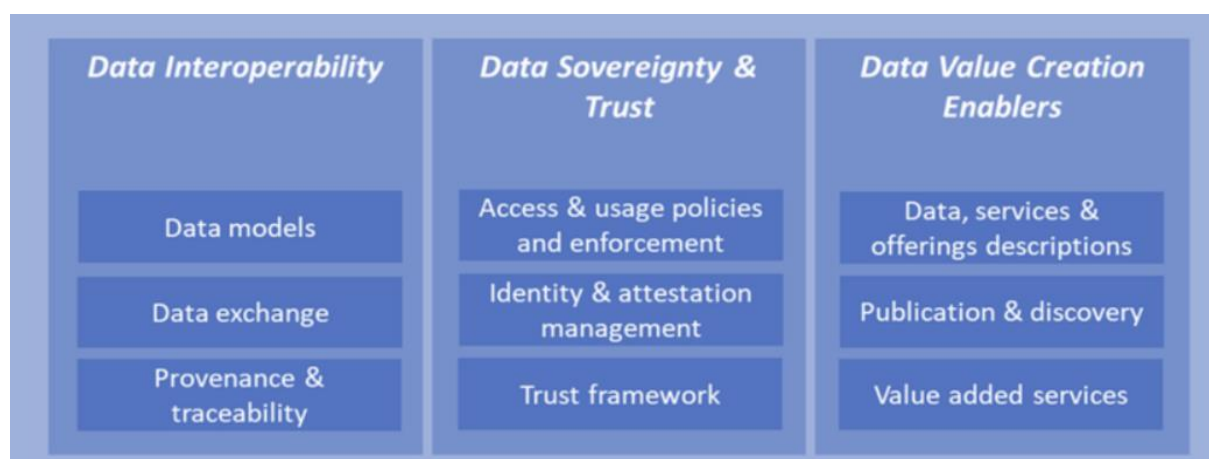


Figure 3 – The DSSC Building Blocks from the Blueprint 2.0

Data interoperability

- **Data models** – shared structures and vocabularies that allow participants to describe and interpret data consistently across organisations and domains.
- **Data exchange** – mechanisms and protocols that enable secure and reliable transfer of data between participants, e.g. via connectors or APIs.
- **Provenance & traceability** – capabilities to record and verify the origin, lineage, and processing history of data to ensure accountability and trust.

Data sovereignty & trust

- **Identity & attestation management** – systems to establish, verify, and manage the identities of participants and their attributes, ensuring authenticity in the data space.
- **Trust framework** – common rules, certification, and conformance mechanisms that allow participants to rely on each other's compliance and behaviour.

¹ <https://dssc.eu/space/BVE2/1071251457/Data+Spaces+Blueprint+v2.0+-+Home>

- **Access & usage policies enforcement** – tools to define and enforce conditions under which data may be accessed and used, including obligations and restrictions.

Data value creation enablers

- **Data, services & offering descriptions** – metadata and cataloguing capabilities that allow providers to describe their datasets and services in a machine-readable way.
- **Publication & discovery** – functions that make datasets and services visible and searchable, enabling participants to find and access relevant resources.
- **Value creation services** – mechanisms and platforms that support transactions, marketplaces, and accounting, helping participants to realise economic or societal value from shared data.

In addition to these generic building blocks, the **AgriDataSpace** project has highlighted sector-specific extensions that are particularly relevant in the agricultural domain:

- **Consent & Permission Management**, including farmer-facing dashboards to keep data providers in control.
- **Anonymisation**, to protect sensitive information when aggregating or processing data.
- **Semantic Mapping & Backward Compatibility**, to bridge across heterogeneous ontologies and legacy data sharing infrastructures.
- **Compute-to-Data**, enabling algorithms to move to where data resides, thereby supporting sovereignty and scalability.

Together, these canonical and sector-specific building blocks provide the comprehensive reference catalogue against which CEADS can be positioned. The subsequent subsections (2.2 → 2.8) will align these building blocks with the CEADS-specific six-box framing introduced in Figure 1, ensuring that the CEADS design is both complete with respect to European reference initiatives and coherent with its own architecture.

2.2 CEADS Onboarding Path and Building Block Mapping

2.2.1 Control and Data Planes within CEADS Onboarding Path

To ensure consistency with mentioned previous work, here we position the identified blocks within a Data and Control plane, illustrating the envisaged CEADS Onboarding paths that other Data Sharing Initiatives can relate to, in order to assess their CEADS “integration readiness” level.

The **Control Plane** defines the organizational and legal frameworks necessary to build trust, sovereignty, and secure collaboration among stakeholders in data-sharing. Governance mechanisms rely on compliance services, certification, and identity frameworks to establish credibility and trust; while Identity and Access Management systems such as Single Sign-On, Multi-Factor Authentication, the EU Common Identity Framework, and self-sovereign identity enforce secure authentication and access control.

Data usage and access control policies enforce restrictions beyond initial access, attaching policies that monitor and limit use, processing, aggregation, and dissemination in real time to preserve sovereignty. These governance structures create the conditions for a trusted, compliant, and efficient agricultural data economy. It includes the Trust Identity Framework building block, the Catalogues and Metadata one and part of the Access and Permission management (see Figure 3). We expect the onboarding path to progressively build and enrich existing functionality starting from basic Control Plane features.

The **Data Plane** on the other end encompasses the technical foundations required for effective data sharing, covering data sources, ingestion, storage, processing, analytics, visualization, and reporting. Key challenges to address will span technical interfaces, standardized data models and formats, APIs for exchange, provenance and traceability, semantic consistency, organizational alignment, and legal frameworks, all working together to guarantee secure, sovereign, and efficient data exchange across the system. Such a plane includes interoperability services, data exchange and monetisation as well as data privacy preservation functionality, acting directly on the data-exchange flow.

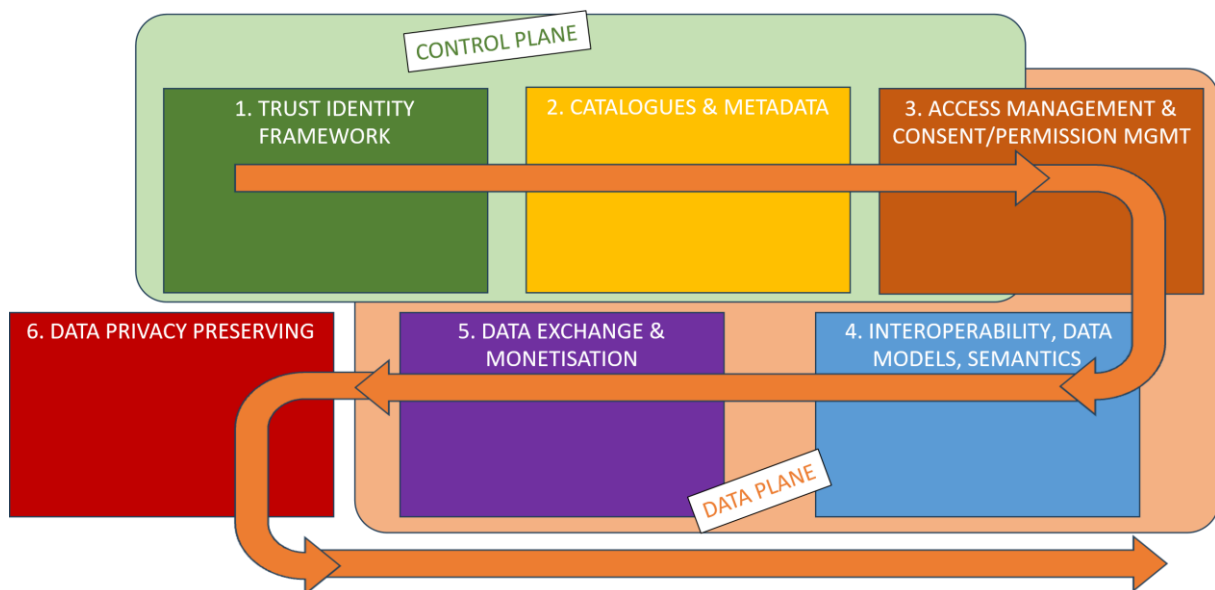


Figure 4 – CEADS onboarding path

2.2.2 Building Block Mapping

Table 1 provides an explicit alignment between the canonical building blocks from DSSC and AgriDataSpace, and the CEADS framing as illustrated in Figure 4. This shows that all reference building blocks can be coherently positioned within the CEADS architecture, ensuring that the deliverable maintains both completeness (with respect to European reference initiatives) and internal consistency (with respect to its own architectural structure). This framing reflects the common separation of control plane (identity, policy, catalogue, contracting) and data plane (transfer/processing), also seen in SIMPL and connector-based architectures.

Table 1 – Building block mapping

Canonical Building Block (DSSC / AgriDataSpace)	CEADS Frame (Figure 4)	Notes on Alignment
Identity & attestation management (DSSC) Trust framework (DSSC)	1. Trust Identity Framework	Covers participant onboarding, credential management, attestations, and trust anchors
Data, services & offering descriptions (DSSC) Publication & discovery (DSSC) Provenance & traceability (DSSC)	2. Catalogues & Metadata	Catalogues cover dataset/service descriptions and discovery; provenance is captured via metadata lineage
Access & usage policies enforcement (DSSC) Consent & Permission Management (AgriDataSpace) Consent Control Dashboard (AgriDataSpace)	3. Access Management & Consent/Permission Management	Combines generic usage control with sector-specific consent flows and user dashboards.
Data models (DSSC) Semantic Mapping & Backward Compatibility (AgriDataSpace)	4. Interoperability, Data Models, Semantics	Explicitly addresses common models, semantic mediation, and integration of legacy DSIs.
Data exchange (DSSC) Value creation services (DSSC)	5. Data Exchange & Monetisation	Includes secure technical data transfer as well as economic/transactional services (marketplaces, accounting).
Anonymisation (AgriDataSpace) Compute-to-Data (AgriDataSpace)	6. Data Privacy Preserving	Privacy-enhancing mechanisms, including anonymisation of shared

		datasets and federated computation models.
--	--	--

2.3 Trust identity framework

In the rapidly evolving ecosystem of data sharing and exchange, **trust** is a foundational principle. In a dataspace environment it is important to ensure participants are who they claim to be, behave in accordance with defined rules, and can be held accountable for what they share. For these reasons the **Trust Identity Framework** is one of the cornerstone building blocks also in CEADS.

A **Trust Identity Framework** defines a structured, standardized approach to digital identity management, verification, and trust assurance among participants in a data space and it is particularly important given the need to support sovereignty in data management, one of the pillars underpinning data economy. The framework is essential for preventing unauthorized access, ensuring data sovereignty, and enabling legal and regulatory compliance.

The following sections describe the key components in a Trust Identity Framework.

2.3.1 Identity Assurance

Ensuring that all participants (organizations, systems, or users) are verified and authenticated; given the multi-country reach of CEADS it is plausible that a federated approach amongst existing Identity Providers and the use of i.e. eIDAS 2.0 regulation for CEADS will provide such a feature. Identity Providers are the organizations that issue and manage digital identities. They ensure that identity attributes are accurate, up-to-date, and verifiable.

2.3.2 Trust Anchors

Independent authorities or mechanisms that vouch for identities could become an essential enabler for the federation aspects to be handled by the above-mentioned Identity Assurance. Neutral entities that evaluate and certify the trustworthiness of participants. They can be certification bodies, federated governance authorities, or decentralized ledgers.

2.3.3 Credential Management

Federation of Identity Providers for the purposes of CEADS will also need to be integrated with a proper and continued system for managing the issuance, validation, and revocation of identity credentials (e.g., digital certificates, verifiable credentials etc.). Verifiable Credentials are digitally signed claims that prove a participant's identity or authorization status by using standards like W3C Verifiable Credentials and X.509 certificates.

2.3.4 Policy Enforcement

The Trust Identity Framework will have to fulfil the need for setting the policies and make sure that all actors adhere to common governance and usage rules. This is to be managed by a Policy Enforcement layer within the Dataspace, defining the rules of engagement, including roles, trust levels, credential types, liability frameworks; and dispute resolution mechanisms.

2.3.5 Decentralized vs. Centralized Identity Models and CEADS implementation

Modern Trust Identity Frameworks increasingly favour **decentralized identity models**, such as **Self-Sovereign Identity (SSI)** which allows users and organizations control their own identity credentials; and the **Distributed Ledger Technologies (DLT)**, where trust anchors and verifiers can operate on decentralized infrastructure for increased transparency and resilience. DLT are not mandatory for SSI but can eventually be used to build the trust framework.

These models support the **data sovereignty principle**, where participants can decide how their data and identity information are used. Such an approach is particularly suited for the handling of many datasets of different nature and originated in many different contexts exposed by Digital Agriculture.

The implementation of a Trust Identity Framework will have to handle steps such as **defining the Trust Model**: what entities are to be trusted, under what conditions, and who governs the overall CEADS Trust Identity Framework Model. The project will have to specify what are the CEADS **onboarding procedures** explaining how existing Identity Providers are to be integrated / federated shedding some light on how the participants are to be verified and enrolled within CEADS, what types of credentials are supported, and how are they issued, revoked and verified. The proposed federative model will have to embed support for **interoperability** ensuring therefore compatibility amongst identity systems and standards.

2.3.6 Real-World Examples and Standards

Several initiatives and standards bodies are already shaping the Trust Identity Framework landscape and will have to be assessed:

- **EUDI Wallet (EU Digital Identity Wallet)**: Enables EU citizens and businesses to prove identity and attributes across borders.
- **GAIA-X Trust Framework**: Provides an interoperable trust model for data spaces in Europe.
- **IDSA (International Data Spaces Association)**: Defines connectors and identity mechanisms for secure data exchange.

- **ISO/IEC 29115:** Framework for identity assurance levels.
- **iSHARE Trust Framework:** Enables secure, controlled data exchange between organisations by defining uniform processes for identification, authentication, and authorisation across different sectors and data spaces.

2.3.7 Challenges and considerations

Implementing a robust Trust Identity Framework currently brings many challenges that will need to be considered and tackled. Balancing Trust and Usability is one of the main ones: high-assurance identity processes can add friction, and farmers are not the ideal technology advance adopters. At European level, CEADS will need to ensure Cross-border Recognition, bringing its legal and technical harmonization across jurisdictions challenges. Scalability and Performance will have to be robust, given CEADS expected wide reach, identity systems and their federation must handle high volumes without compromising security and privacy, avoiding unnecessary exposure of identity attributes.

Trust in Data Spaces in general is not an abstract ideal but a concrete, enforceable principle given existing and upcoming technologies that can be used in implementing the Trust Identity Framework. By defining how identities are managed, verified, and governed, the framework lays the foundation for secure, sovereign, and scalable data sharing. As CEADS implementation will evolve, it will be of paramount importance to ensure a robust and interoperable Trust Identity Framework is part of it.

2.4 Catalogues and Metadata

The next level of aggregation and interoperability that has been identified is a building block essential in creating a Data Space, especially when starting from the wide and fragmented situation we currently have in the agricultural sector.

Metadata enrichment is essential for transforming raw datasets into valuable, shareable, and trusted assets. Whether applied manually, semi-automatically, or fully automated, it unlocks the true potential of data in open platforms, enterprise systems, and federated data spaces.

Like all Data Spaces, the main rationale for CEADS existence is the possibility of creating rich agricultural data catalogues, underpinned by commonly agreed metadata or mapping systems that ensure a good level of interoperability at the level of bridging different catalogues.

Metadata is "data about data" and it provides descriptive, structural, and administrative information about a dataset. Common metadata elements describing datasets may include parameters such as Title, Description, Creator/Publisher, Rights Owner, Format and size, Date of creation/modification, rules for use and access policies, Keywords or subject tags. Metadata

helps users and applications understand, find, access and use datasets appropriately. In the lack of such a feature, CEADS could propose and implement **automatic annotation**, using AI or NLP to extract metadata from the dataset itself or related documents. To promote automated applications **semantic enhancement** might become important, linking metadata elements to external resources (e.g., connecting a location to its URI in a geospatial database).

A proper implementation of catalogues with well organised metadata structures greatly improves discoverability. Enriching datasets with metadata in fact helps these to show up more accurately in search engines, catalogues, or data portals, due to the aligning with common terminologies.

To promote and facilitate **better interoperability** standardized metadata schemas (like DCAT, Dublin Core, Schema.org) might be considered. These enable datasets to be exchanged and integrated across platforms and domains as this is amongst the strong requirements for CEADS. Furthermore, adding metadata such as data lineage, source, or quality metrics increases transparency and user confidence (providing support for **data enhanced trust and provenance**).

2.4.1 Methods of Metadata Enrichment

Metadata enrichment can be obtained in a number of different ways, using for example **manual curation**, where human experts edit and supplement metadata for accuracy and domain relevance or **automated tools**, through the use of NLP, machine learning, or scripts to extract metadata from raw data, filenames, or related documents. Additional, more advanced ways of labelling data with corresponding metadata correspond to ‘**ontology mapping**’ or ‘**semantic annotation**’, aligning terms with controlled vocabularies e.g., AGROVOC or other semantic artefacts such as the ones harvested in AgroPortal (<https://agroportal.eu>), which plays the role of reference ontology repository for agri-food). Next to manual curation with human experts, **crowdsourcing** through community or user-driven improvements is also used in open data platforms.

Challenges to be addressed include **data sensitivity** (enrichment must respect privacy or proprietary limits), **automation accuracy** (acknowledging that machine-generated metadata can introduce errors and ensuring adequate control for critical applications) and **standards compatibility** (choosing the right schema or vocabulary for the agricultural domain or sub-sector).

2.4.2 Metadata Standards and Controlled Vocabularies

To ensure wide discoverability and interoperability it will be important to ensure that descriptive metadata use common and standardised formats so that data assets, access conditions and

provenance can be properly described. Here we give an overview of existing standards according to their current purpose.

We start from one of the most developed ones, **DCAT** (Data Catalogue Vocabulary), published by W3C as a general RDF-based vocabulary to describe datasets and data catalogues. Its goal is to make datasets discoverable and interoperable on the web (especially for linking open data). DCAT is often used by governments, research organizations, and data providers to describe datasets and expose them in catalogues (e.g., using SPARQL endpoints or as part of CKAN/Drupal metadata).

There is a closely related standard **DCAT-AP** (DCAT Application Profile), a customized profile of DCAT, adapted for European public sector data portals meant to ensure interoperability across EU open data portals. There is also a variant of DCAT-AP customized for describing High Value Datasets, which may be relevant to consider. EU-funded digital agriculture platforms and data portals (e.g. SmartAgriHubs, INSPIRE²) use this standard and it will be worth considering its adoption.

INSPIRE Metadata Implementing Rules used in Europe as a geospatial metadata standard based on ISO 19115 and ISO/TS 19139, especially for agricultural datasets with a spatial component (e.g., land use, crop maps, soil zones). ISO 19115 / ISO 19139, published by ISO as international standard for geospatial metadata, provide exhaustive set of metadata elements (more than 400) including spatial resolution, bounding box, coordinate reference system, distribution info, online resources, licenses. It's used in precision agriculture, satellite imagery metadata, soil/geospatial databases. ISO 19115 is also mapped towards GeoDCAT-AP while ISO19119 is the taxonomy used for geospatial services³

SensorML / O&M is another standard for metadata but also for Observations and Measurements published by OGC, the Open Geospatial Consortium, particularly focused on describing sensors and their outputs and suited for managing IoT data in agriculture produced by devices such as soil moisture sensors, weather stations, drone imagery, etc.

SensorThings API provides an open, geospatial-enabled and unified way to interconnect the Internet of Things (IoT) devices, data, and applications over the Web. It is crucial also for agricultural sector as it is a worldwide used standard implementing also SensorML and O&M.

² https://knowledge-base.inspire.ec.europa.eu/evolution/good-practice-library/geodcat-ap_en

³ https://knowledge-base.inspire.ec.europa.eu/publications/inspire-metadata-implementing-rules-technical-guidelines-based-en-iso-19115-and-en-iso-19119_en

Schema.org (with agriculture-specific extensions) Semantic markup for web content. Increasingly used in web-based agricultural data catalogues to improve search engine discoverability.

GS1 Standards (for supply chain traceability) Metadata for products, locations, and logistics events in agri-food value chains. Farm-to-fork traceability systems, food provenance platforms.

At a different level we find **AGROVOC** is a controlled vocabulary / multilingual thesaurus managed by FAO that supports semantic annotation of datasets, improves search and classification of crop types, pests, farming techniques, soil types. It is used in AGRIS, GODAN, CGSpace, and other global agri-knowledge platforms.

Other standard vocabularies include GEMET⁴, CORE vocabularies⁵ and controlled vocabularies⁶ (i.e. AGRIPROD).

2.4.3 Provenance & Traceability

Provenance and traceability functions ensure that the origin and lineage of data assets can be verified. By recording how data was produced, processed, and exchanged, these functions provide transparency, accountability, and reproducibility. They also contribute to compliance with regulatory requirements and strengthen trust among participants. Provenance information can be captured as part of metadata enrichment and catalogues, for example by applying standards such as W3C PROV-O.

2.5 Consent and permission management

In the agricultural sector the issue of ensuring righteous access to data has been under scrutiny for many years, to regulate the frequent situation where tech providers (agricultural machinery manufacturers, but also emerging agritech software solution providers) collect data from farms and use it for their business purposes. This causes concerns that farmers would be negatively impacted, at business level, by the fact that data about their own farms would be stored in siloed cloud platforms. EU Code of Conduct was the first expression of such concerns that led to the establishment of some ethics and a voluntary alignment with those from manufacturers in primis. The Data Governance Act and the Data Act came later with a stronger objective of protecting farmers rights in terms of having access to data collected within their own farms, paving the ground for compulsory rules to be observed.

⁴ <https://www.eionet.europa.eu/gemet/en/about/>

⁵ <https://op.europa.eu/en/web/eu-vocabularies/corevocs>

⁶ <https://op.europa.eu/en/web/eu-vocabularies/controlled-vocabularies>

Having said that, Consent and Permission Management in agricultural dataspace is not just a legal compliance issue, but a trust-building mechanism and a technical foundation for data sovereignty. Without it, farmers and cooperatives are unlikely to share data, and the vision of interoperable, fair, and innovation-friendly agri-dataspace collapses. For these reasons this building block is one of the essential features for guaranteeing trust (intended in this context as a safe place for sharing data in a sovereign way) in agricultural dataspace. It's possible to empower farmers with control on who gets to use their data for what purpose, while enabling innovation for technology companies that can more easily exploit such responsible data sharing. Implementing such systems requires careful integration of some of the relevant features introduced earlier such as identity management, and data-policy enforcement, as well as specific features such as consent handling and transparency tools, all designed with the data provider rights in mind. Design choices include making sure data is annotated or divided with the correct (farm) identifiers in order to apply the consent, either by not sharing any data or resulting in the correct data filtering within the dataflow. It might be that data providers and data consumers use different identifiers. In this case a mapping service is needed to be able to complete the data flow specifying the correct farm identifiers in the data request. A data access request should be consented first by the data provider. Only when a data provider consents, the data access request should be presented to the farmer(s). It is also important that the purpose of the data request is clearly explained and binding, meaning that any changes to the purpose of the data request should result in another consent request. As data is not stored at the farmer side, consent is usually given via an appropriate UI outside of the typical connectors used in data sharing initiatives, being an app (Agronod) or a webportal (DjustConnect). When it comes to the requirements for such building block it must be clear the trade-off between the scope of intervention (size of the considered dataset) and the frequency for access permission, must be duly balanced to prevent farmers been swamped with continuous requests.

As data continues to shape the future of agriculture, permission management systems will not only protect data rights but also foster the trust needed for collaboration and growth.

2.6 Interoperability

This building block will be needed to address **Data Interoperability** issues given the need for CEADS-related different systems, organizations, and applications to **understand, exchange, and make use of data in a meaningful and consistent way**, even when the data originates from different sources or is used in different contexts. Especially in CEADS, expected to bring together multiple independent data providers and consumers, interoperability is foundational rather than optional.

There are four types of interoperability that shall be supported, according to different status of DSIs or organisations willing to become part of CEADS and exposing their datasets visibility and different opportunities for integration according to the different levels of what is often referred to as the **interoperability stack** (here we envisage a “two-systems” situation where on one side we have CEADS and on the other existing DSIs of Organisations that would be part of data exchange – without necessarily being yet aligned or compliant with what will be required for becoming an integrated subset of CEADS):

- **Technical Interoperability:** Can systems connect and exchange data (e.g., are APIs available? Are the rules and protocols for data-exchange well defined? Etc.)?
- **Syntactic Interoperability:** Once systems can interface through “connecting pipes” and are technically interoperable, are they equipped to parse and understand the data format (e.g. data to be exchanged can be formatted according to JSON, XML, CSV)?
- **Semantic Interoperability:** This one is also about metadata interoperability between systems as data interpretation in particular must be done on the basis of common semantic grounding (e.g., “yield” should be understood / used in the same way across platforms)?
- **Organizational Interoperability:** This interoperability level belongs more in the “control plane” as it relates to policies, workflows, and governance rules that promote or prevent cooperation.

These different data interoperability levels require substantial coding effort and therefore need to provide concrete advantages and returns for involved stakeholders that we expect will be driven by the compelling needs to implement the many proposed use cases. The advantages relate to lowering data-silo barriers, enriching data-value, increasing automation and collaboration opportunities, federation and cross-platform analytics that are more and more needed to support demanding AI applications.

What is illustrated in this chapter relates more to the issues of producing data-catalogues that can be easily parsed by automated systems and used to search for relevant data according to various conditions and search boundaries.

2.6.1 Data Interoperability Standards

To ensure interoperability, besides ensuring common understanding between different systems at metadata level as seen in previous paragraph dedicated to Catalogues and Metadata, CEADS implementation will need **Common Data Models**, highlighting shared structures that define how data should be organized and labelled; relevant examples are AgGateway ADAPT

(the world's only standard to support a broad range of farm data implemented by leading farm management information systems) as well as SAREF (an ETSI promoted suite of ontologies that forms a shared model of consensus intended to enable semantic interoperability between solutions from different providers and among various activity sectors in the IoT, including agriculture).

Very often in agriculture we will be dealing with data that acquire additional value when tied to a specific location. For geo-located (georeferred or georeferencable) datasets, there are standards from ISO 19100 series and OGC (<https://www.ogc.org/standards/>) that are already widely adopted at both, server and client levels⁷. Further open standard specs should be taken into consideration (and related to data models, semantic and also format encoding)⁸.

Besides these popular widely ones, also other common data models and terms specific to the agricultural sector can be found through Agroportal, a website dedicated to ontologies and semantic artefacts in agri-food and related domains. We already mentioned AGROVOC and GS1 amongst the ones that provide also support for standardised metadata, to ensure different types of interoperability – also at the level of catalogues.

Within such building block we will also find Data Transformation Services, intended as middleware or adapters that can map or convert data from one format/model to another and often implemented as “connectors” or “wrappers” in wider data space architectures.

Ripening the advantages of data interoperability in Agricultural Dataspaces can for example mean that farm machinery vendors that use different terms for “soil type” or “fertilizer use” can, through data interoperability efforts (e.g., harmonized vocabularies and transformation logic), integrate datasets, enabling tools like precision farming platforms to combine them and deliver value. IDSA connectors use semantic mediation to bridge vocabulary gaps.

To conclude this section, we can see how Data Interoperability is the building block that allows dataspace to function across organizational and technical boundaries. It will be therefore key to align shared models, semantics, and protocols so that the CEADS can turn fragmented data

⁷ <https://www.ogc.org/standards/ogcapi-maps/>, <https://www.ogc.org/standards/ogcapi-features/>, <https://www.ogc.org/standards/sensorthings/>, <https://www.ogc.org/standards/wms/> (ISO19128, required by INSPIRE Directive), <https://www.ogc.org/standards/wfs/> (ISO19128, required by INSPIRE)

⁸ https://knowledge-base.inspire.ec.europa.eu/data-specifications-technical-guidelines_en, <https://www.ogc.org/standards/geopackage/>, <https://www.ogc.org/standards/ogc-cloud-optimized-geotiff/>, <https://www.ogc.org/standards/eo-geojson/>

assets into a usable, trusted, and powerful ecosystem – one where participants can extract value without sacrificing control.

2.7 Data Exchange and Monetization

With metadata and data interoperability at catalogue level tackled through commonly agreed standards, interfaces and data transformation services, the focus can now shift towards data-plane functionality. To enable data exchange it is appropriate to consider **Data Exchange Connectors** or **Gateways** that are there to secure and govern data transfer between participants. Depending on data types such functionality can be activated via API-based or file-based exchanges, with policy enforcement activated before data leaves the system.

For this purpose we find different standards promoted by different organizations such as, for example the IDS Connector (International Data Spaces) and the Eclipse Dataspace Connector.

It is important to consider that such a building block must provide support for **Data Usage Control & Policy Enforcement**, to ensure that data usage complies with policies even after access is granted. For this purpose we foresee the implementation of usage contracts (e.g., "no further sharing", "use only for research" clauses), dynamic policy evaluation, sticky policies and DRM-like controls with tools such as ODRL, Rego (Open Policy Agent), XACML, IDS Policy Enforcement Point

2.7.1 Data monetisation

The vision behind dataspace wants to make sure they can support and fuel a growing data economy. Within CEADS there will be the need to envisage tools that can enable commercial models where data sharing also leads to monetization and, more generically, to valorisation of data assets. Besides the design of adequate pricing models (subscription, pay-per-access, usage-based), CEADS will have to efficiently tackle the granularity of exchanged datasets and strike the right balance between size and frequency of exchange. That means supporting the dataspace with the right instruments that support the data exchange process also when automated micro-payments are needed. Such functionality will include smart contracts or digital rights management (DRM) engines and other forms of electronic contract framework (e.g. policy-based), as well as the integration of payment systems (Stripe, PayPal, crypto if applicable). Amongst the elements fostering monetization we also find roles for intermediaries that might be introducing platforms for licensing marketplaces and technologies for tokenized data access that can log micro transactions. Examples related to such aspects include the use of blockchains as promoted by the Ocean Protocol in PONTUS-X, and commercial service Dawex that adds data monetization modules in their data platforms.

These tools enable also **Data Provenance & Auditing** to track who accessed or modified data and when, through immutable audit trails and tamper-proof logs (related tools are Hyperledger, ELK stack, Audit log APIs, Gaia-X Self-Descriptions).

2.7.2 Value Creation Services

Value creation services provide the mechanisms through which participants in a data space can realise economic or societal benefit from shared data. These services go beyond the mere exchange of datasets by enabling functionalities such as contracting, settlement, and usage accounting. They may underpin marketplace environments but also support non-commercial value exchanges, e.g. in research or sustainability reporting. In CEADS, such services are expected to complement the technical data exchange layer by creating incentives for sustained participation.

2.8 Data Privacy preservation

This building block relates to ensuring the right to privacy when it comes to data usage. Besides having policies that travel with datasets when expecting users to observe them or having means to enforce them, there might be situations where data itself cannot be disclosed. This is amongst the less stringent requirements for CEADS, given its implementation complexity and the fact that in the agricultural sector applications are not considered mission critical to justify the additional effort. It will be often enough to ensure appropriate data-anonymization techniques are applied to prevent the association between data and parcels (and then farmers) represented by specific data.

Stronger but more expensive techniques include Secure Multiparty Computation (MPC), (Fully) Homomorphic Encryption, Differential Privacy and Zero Knowledge Proofs (ZK Proofs) and there must be strong security motivations for justifying the additional effort needed for implementing these systematically.

2.8.1 Compute-to-Data

Compute-to-Data approaches allow algorithms to be moved to the location of the data rather than transferring the data itself. This enables privacy and data sovereignty by design, since providers retain full control over their datasets, which remain in secure environments to minimize data exposure risks. This reduces risks related to data movement, supports compliance with usage policies, and enables collaboration even where raw data cannot leave its source environment. However, Compute-to-Data also requires coordination between data owners and algorithm providers (computation requests), secure communication channels and execution environments. Algorithm providers must ensure compatibility with the data providers' formats, while infrastructure providers need mechanisms such as Trusted Execution Environments or

isolated computing environments. Examples include federated learning or secure multi-party computation. In agricultural dataspace, this approach may be particularly useful for sensitive or large-scale datasets such as genomic data or satellite imagery.

2.8.2 Anonymisation

Anonymisation mechanisms enable the removal or masking of sensitive information from datasets before sharing or aggregation. This function is particularly important in the agricultural domain, where farm-level or personal data may raise privacy and competition concerns. Techniques can include data generalisation, aggregation, pseudonymisation, or differential privacy. Anonymisation complements other privacy-preserving mechanisms such as consent management and Compute-to-Data.

3 Reference Architectures and Implementations

To complement the canonical building blocks introduced in Chapter 2, this chapter documents major reference initiatives and implementations that are relevant for CEADS. The purpose is not to provide an exhaustive review but to highlight key frameworks and tools that can be considered in Task 2.3 when concrete CEADS services are designed.

3.1 Key Initiatives (*mapped to CEADS framing*)

Table 2 positions the most widely adopted initiatives against the CEADS six-box building block frame. This illustrates which parts of the CEADS architecture can already be supported by existing assets, and where gaps remain.

Table 2 – Mapping related key initiatives

Initiative	1. Trust Identity Framework	2. Catalogues & Metadata	3. Access Management & Consent	4. Interoperability (Data Models, Semantics)	5. Data Exchange & Monetisation	6. Data Privacy Preserving
SIMPL	Central identity services, partial central trust	Ontology repositories, catalogues	Hooks for policy enforcement	Abstracts infrastructure, vocab libraries	Generic data transfer middleware	Not covered (future add-ons possible)
IDS / Dataspace Protocol	Identity brokering, IDS certificates	Broker, self-descriptions	Policy enforcement point (usage control)	Semantic mediation concepts	IDS Connector, contract negotiation	Not directly covered
Gaia-X Trust Framework	Self-descriptions, conformance, labels	Service descriptions	Baseline for usage policies	Ontology registries (planned)	Data connector specs	Not covered
Eclipse Dataspace Components (EDC)	Integrates with VCs / identity providers	Catalogue API	Policy engine (ODRL/Rego)	Can integrate semantic adapters	Connector for DSP-based exchange	Not core; extensions exist
FIWARE Data Space Stack	Federated identity (Keyrock)	Context Broker as metadata hub	Basic role/consent features	NGSI-LD models, mapping tools	Connector + APIs for exchange	Not core
Pontus-X	Federated identity	Self-descriptions	Smart-contracts, role-based and policy-based access	Self-descriptions, standard data formats, semantic adapters	Blockchain and smart-contracts	Not covered

3.1.1 SIMPL (Smart Middleware Platform for Cloud-to-Edge Federations)

SIMPL is the European Commission's open-source middleware initiative intended to provide common technical foundations for European data spaces. It is conceived as an agent-based, decentralised but partially centralised platform that abstracts infrastructure, offers catalogue and ontology repositories, and includes basic capabilities for data transfer and policy hooks. Its modular design allows it to interoperate with existing data space solutions rather than replacing them.

For CEADS, SIMPL is important for two reasons. First, as a Commission-backed platform, it represents the expected baseline for cross-data space interoperability and alignment with other EC-funded initiatives. Second, it provides potential building blocks that CEADS can adopt directly, such as catalogue services and identity functions, thereby reducing development effort and ensuring compliance with the broader European strategy. However, SIMPL does not cover sector-specific functions or advanced governance features; CEADS will need to complement it with agricultural extensions (e.g. consent dashboards, semantic mapping) and domain-specific services.

CEADS Building Block Coverage

- **1. Trust Identity Framework:** (central identity services, partial federation)
- **2. Catalogues & Metadata:** (ontology repository, catalogue services)
- **3. Access Management & Consent:** (partial, hooks for policy enforcement only)
- **4. Interoperability (Data Models & Semantics):** (abstraction layer, vocabularies)
- **5. Data Exchange & Monetisation:** (generic data transfer functions)
- **6. Data Privacy Preserving:** (not currently addressed)

References: European Commission SIMPL architecture & clarifications.

3.1.2 IDS / Dataspace Protocol

The International Data Spaces (IDS) initiative and its Dataspace Protocol (DSP) provide the conceptual and technical reference model for trusted data spaces in Europe. IDS defines the architecture (RAM) with roles and connectors, and DSP specifies interoperability at the protocol level, including contract negotiation, metadata exchange, and policy enforcement.

For CEADS, IDS/DSP are relevant as the baseline reference model that many implementations build upon (e.g. EDC). They bring a mature conceptual framework for trust, usage control, and semantic interoperability. CEADS does not need to reimplement IDS but can rely on existing

connector implementations that adhere to DSP, ensuring compatibility with other European data spaces.

CEADS Building Block Coverage

- **1. Trust Identity Framework:** (IDS certificates, identity brokering)
- **2. Catalogues & Metadata:** (IDS Broker, self-descriptions)
- **3. Access Management & Consent:** (policy enforcement point, usage control)
- **4. Interoperability (Data Models & Semantics):** (semantic mediation concepts)
- **5. Data Exchange & Monetisation:** (IDS Connector, DSP contract negotiation)
- **6. Data Privacy Preserving:** (not directly covered)

3.1.3 Gaia-X Trust Framework

The Gaia-X Trust Framework defines the rules for federation and trust in European data spaces. It introduces self-descriptions for participants and services, conformance testing, and trust labels that ensure compliance with baseline requirements. Although Gaia-X is not itself a connector, it provides the compliance layer that can be applied across data spaces.

For CEADS, the Gaia-X Trust Framework is important for political alignment and interoperability. Using its conformity assessment and trust labels will allow CEADS to integrate with the wider European dataspace landscape. However, Gaia-X does not provide technical data exchange functions, so it must be combined with connectors (e.g. EDC) and domain-specific services.

CEADS Building Block Coverage

- **1. Trust Identity Framework:** (self-descriptions, conformance, labels)
- **2. Catalogues & Metadata:** (service descriptions in self-descriptions)
- **3. Access Management & Consent:** (baseline rules for policies, not detailed enforcement)
- **4. Interoperability (Data Models & Semantics):** (partial, alignment via registries)
- **5. Data Exchange & Monetisation:** (indirect, supports connector conformance)
- **6. Data Privacy Preserving:** (not addressed)

3.1.4 Eclipse Dataspace Components (EDC)

EDC is the most widely used open-source connector implementing the Dataspace Protocol. It provides APIs for catalogue discovery, secure data transfer, and policy enforcement based on ODRL/Rego. EDC is designed to integrate with existing identity providers and can be extended with semantic adapters.

For CEADS, EDC represents a practical and mature building block for implementing data exchange and catalogue functions. It is already used in many European pilots and has strong community support. CEADS can leverage EDC to avoid building connectors from scratch, while still extending it for agricultural specifics such as consent dashboards or domain ontologies.

CEADS Building Block Coverage

- **1. Trust Identity Framework:** (integration with verifiable credentials, identity providers)
- **2. Catalogues & Metadata:** (Catalogue API)
- **3. Access Management & Consent:** (policy engine with ODRL/Rego)
- **4. Interoperability (Data Models & Semantics):** (partial, via adapters)
- **5. Data Exchange & Monetisation:** (DSP-based secure exchange)
- **6. Data Privacy Preserving:** (extensions possible, not core)

3.1.5 FIWARE Data Space Stack

FIWARE extends its NGSI-LD context broker ecosystem to data spaces. The stack includes identity services (Keyrock), catalogue and discovery functions, semantic interoperability via NGSI-LD models, and connectors for data exchange. FIWARE has strong uptake in IoT and smart agriculture projects, making it especially relevant for CEADS.

For CEADS, FIWARE is attractive because it combines data models, exchange, and catalogue functions with a proven presence in the agriculture sector. Its semantic grounding in NGSI-LD and its practical tooling make it a candidate for integration into CEADS use cases, complementing or interfacing with other connectors such as EDC.

CEADS Building Block Coverage

- **1. Trust Identity Framework:** (Keyrock for federated identity)
- **2. Catalogues & Metadata:** (Context Broker as metadata hub)
- **3. Access Management & Consent:** (basic role-based and consent features)

- **4. Interoperability (Data Models & Semantics):** (NGSI-LD models, mapping tools)
- **5. Data Exchange & Monetisation:** (connector + APIs for exchange)
- **6. Data Privacy Preserving:** (not core)

3.1.6 Pontus-X

Pontus-X is a decentralized digital ecosystem. It enables companies and institutions to consume, offer and monetize data, software and infrastructure services within a trusted and transparent environment. Pontus-X is built on Gaia-X principles and Ocean Enterprise technology, emphasizing decentralization and data sovereignty. It facilitates technically enforced data-sovereign data sharing and digital service monetization, all while adhering to the rules of the Gaia-X Trust Framework. It allows companies and institutions to consume and offer AI, software, data and infrastructure services in the Pontus-X ecosystem while remaining in control of their IP and sensitive data, thus meeting GDPR and IT security requirements. The Pontus-X portals provide a place to publish, discover, select, and consume digital service offerings, providing a user interface to interact with federation and other ecosystem services. Besides the portals, all services can be managed and consumed programmatically through libraries such as Nautilus.

While CEADS will not adopt blockchain-based architectures, Pontus-X is significantly important for discovering agricultural datasets and algorithms AI/ML models. Exploring interoperability between Pontus-X and EDC based datasets is an interesting topic to cover.

CEADS Building Block Coverage

- **1. Trust Identity Framework:** (Federated identity)
- **2. Catalogues & Metadata:** (service descriptions in self-descriptions)
- **3. Access Management & Consent:** (Smart-contracts, role-based and policy-based access)
- **4. Interoperability (Data Models & Semantics):** (Self-descriptions, standard data formats, semantic adapters)
- **5. Data Exchange & Monetisation:** (Blockchain and smart-contracts)
- **6. Data Privacy Preserving:** (not addressed)

3.2 Other relevant initiatives

iSHARE

iSHARE is a trust scheme originally developed in the Netherlands and now applied in several European pilots. It provides a uniform set of agreements, processes, and technical specifications for identification, authentication, and authorisation of participants in data sharing. Rather than offering a connector, iSHARE defines how organisations can delegate rights securely across sectors.

Relevance for CEADS: iSHARE complements the Trust Identity Framework (Box 1) and Access & Consent (Box 3) within the control plane (see Figure 4) by providing ready-to-use patterns for delegation and trust, which could reduce governance overhead in cross-border or cross-sector contexts.

Ocean Protocol

Ocean Protocol is an open-source framework that combines decentralised registries, smart contracts, and compute-to-data functions. It enables data owners to publish assets on a blockchain-based marketplace and allows algorithms to run where the data resides.

Relevance for CEADS: Ocean is significant for Data Exchange & Monetisation (Box 5) and Data Privacy Preserving (Box 6) as part of the data plane (see Figure 4). While CEADS will not adopt blockchain-based architectures wholesale, the compute-to-data model and marketplace concepts offer inspiration for privacy-preserving analytics and incentivisation mechanisms.

AgriDataSpace project outputs

AgriDataSpace builds directly on DSSC but adds agriculture-specific extensions such as consent dashboards, anonymisation, and semantic mapping across farm management systems. These outputs are highly aligned with CEADS objectives, providing tested patterns and community validation in the agri-food sector.

Relevance for CEADS: Strongest contributions are to Access & Consent (Box 3), Interoperability (Box 4), and Privacy (Box 6) within the CEADS envisaged building blocks (see Figure 4). These outputs provide a sector-tailored complement to generic frameworks like SIMPL and IDS.

GS1 Standards

GS1 develops globally adopted standards for product identifiers, logistics events, and traceability across supply chains. In agriculture and food, GS1 identifiers are widely used for farm-to-fork traceability, logistics, and market transparency.

Relevance for CEADS: GS1 contributes to Catalogues & Metadata (Box 2) and Interoperability (Box 4). It provides a mature standardisation backbone that CEADS can integrate for supply-chain related use cases.

INSPIRE / ISO 19100 / OGC Standards

These geospatial standards are widely implemented across Europe and globally. INSPIRE defines EU-level rules for spatial data infrastructures, ISO 19100 standards specify metadata and geospatial data models, and OGC standards enable interoperability of geospatial services and sensor data.

Relevance for CEADS: These standards are directly relevant to Interoperability (Box 4) and Catalogues & Metadata (Box 2), especially for agricultural datasets with spatial dimensions such as land use, soil data, or satellite imagery.

AgroPortal / AGROVOC

AgroPortal is a repository of ontologies for the agri-food domain, while AGROVOC is FAO's multilingual thesaurus for agriculture. Together, they provide a rich semantic backbone for annotation, discovery, and integration of agricultural datasets.

Relevance for CEADS: These resources strengthen Catalogues & Metadata (Box 2) and Interoperability (Box 4). They can serve as controlled vocabularies and semantic hubs to ensure CEADS data assets are consistently annotated and discoverable.

Commercial platforms (e.g., Dawex)

Dawex and similar platforms offer commercial data exchange solutions with built-in marketplace and monetisation modules. They provide contractual frameworks, payment integration, and compliance features in a turnkey solution.

Relevance for CEADS: These platforms illustrate mature implementations of Value Creation Services (Box 5 – Figure 4). While CEADS may not adopt them directly, they provide useful benchmarks for business models and operational capabilities.

3.3 Summary and Implications for CEADS

The landscape of initiatives and implementations around European data spaces is diverse and rapidly evolving. This chapter has shown that several major frameworks (SIMPL, IDS/DSP, Gaia-X Trust Framework, EDC, FIWARE) already cover significant parts of the CEADS building block frame. Their relevance lies in providing tested and widely recognised solutions for trust, catalogues, interoperability, and data exchange.

In addition, a range of other initiatives and sectoral assets (such as iSHARE, Ocean Protocol, AgriDataSpace outputs, GS1, INSPIRE/OGC standards, AgroPortal/AGROVOC, and commercial offerings) complement these frameworks. They do not replace the major initiatives but provide valuable extensions, patterns, or domain-specific assets that CEADS can draw upon.

For CEADS, the implication is clear: there is no need to build all building blocks from scratch. Instead, CEADS should selectively combine and adapt existing initiatives, focusing its own innovation effort on sector-specific requirements such as agricultural semantics, consent and permission management, and privacy-preserving functions. This ensures that CEADS remains consistent with the wider European dataspace ecosystem while addressing the unique needs of the agricultural domain.

4 Conclusions

This deliverable provides a first consolidated overview of building blocks relevant for CEADS, drawing from the DSSC Blueprint v2.0, AgriDataSpace outputs, and other European and sectoral initiatives. The CEADS six-box framing ensures that all canonical building blocks can be positioned coherently, giving a clear architectural anchor for subsequent work.

A range of reference architectures and implementations (e.g. SIMPL, IDS/DSP, Gaia-X TF, EDC, FIWARE) were identified as major initiatives that CEADS can build upon, complemented by additional sector-specific standards and tools.

The document is not a final design, but a guiding reference: it will be used throughout the project to inform decisions in Task 2.3 (service design) and related work packages. The building blocks and initiative landscape are dynamic; this deliverable captures the status at project month 4, but will be updated during the project to reflect evolving standards, implementations, and project experience.

The overview supports CEADS partners by avoiding duplication of existing solutions, identifying gaps and weakly supported areas (e.g. consent dashboards, agricultural semantics, privacy-preserving services). Furthermore it ensures alignment with European policy context (Gaia-X, SIMPL, DSSC).

As CEADS progresses, this document will serve as a living reference and baseline for design decisions, helping WP2 and other work packages to remain consistent, interoperable, and relevant for the European data economy.