



MAMI Framework

Minimal Agreements for Maximal Interoperability

V1.0, January 2026

MAMI Framework - Table of Contents

[Management summary](#)

[Authors' gratitude to contributors](#)

Introduction

- [Goals & purpose](#) | How MAMI contributes to accelerating sovereign data exchanges
- [Usefulness in practice](#) | How MAMI lets you win
- [Possible applications](#) | How to start using MAMI effectively based on your goals

North Star

- [Navigating the North Star](#)
- [Current trends](#) | From Fragmentation to Federation
- [Emerging ecosystems](#) | From Pilots to Production
- [Future trends](#) | Exploring 3 complementary scenarios
- [Strategic implications](#) | Ways to be future-ready

MAMI core contents 2025

- [Navigating recommendations](#)
- [High level recommendations](#)
- [Specific Recommendations](#)
- [List of common standards, protocols & trust anchors](#)

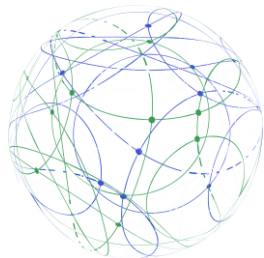
Reflections

- [Lessons learned & next steps](#) | Reflections on prioritization & usefulness of MAMI Recommendations

Appendix

- [Methodology](#)
- [Terminology](#)
- [Bibliography](#)

Management Summary



Welcome to the MAMI framework, which stands for **Minimal Agreements for Maximum Interoperability**. It is a concise list of co-created and broadly agreed-upon recommendations for data sharing that foster cross-sectoral and cross-border interoperability.

This document provides an overview of major trends and developments on the European level ([North Star](#)), followed by [recommendations](#) for data sharing initiatives (DSIs) and data spaces in the Netherlands to become more interoperable with one another and over time better aligned with the EU direction. The recommendations are split between (1) [high level recommendations](#) for making design choices explicitly human and (to an extent) machine readable, and (2) more [specific recommendations](#) across interoperability topics (i.e., Trust & Data Sovereignty, Semantics, Discoverability, Connectivity).

Next steps: as part of ongoing MAMI research, the next aim is to plot standards and protocols introduced in recommendations to show which are (a) currently adopted by major Dutch DSIs, (b) will be adopted within the next 1-2 years, and (c) foreseen to become obsolete due to e.g., sector specific dynamics. By doing so, MAMI sets the direction for other data sharing initiatives and service providers to follow and converge into a more interoperable future of data sharing.

MAMI framework provides insights for 3 different audiences

Data Sharing Initiatives



Who: Any organised group of various parties engaged in data sharing activities under common infrastructure and trust agreements

Why use MAMI: To progress interoperability of your solutions in order to:

- Meet your participants' needs
- Enable cross-domain collaborations

Service providers



Who: Any organisation that provides services to help define, manage and/or operationalise a data sharing initiative (or a data space), typically coming with a service agreement

Why use MAMI: To design future products and services in order to:

- Meet your clients' needs
- Unlock reach across-domains

Policy makers



Who: Government officials, international bodies, industry associations who influence & create policies related to data sharing

Why use MAMI: To design regulation and propel developments that:

- Stimulate adoption
- Remove barriers for cross-domain exchange

Involved parties in MAMI – *Authors' gratitude to contributors*

The following team of authors has worked on guiding the process and creating this document

Organisation

Name

INNOPY
A business of Oliver Wyman

Pieter Verhagen, Yekaterina Travkina

TNO

Gijs van Houwelingen, Kristiina Sau

Authors would like to express their gratitude to all contributors for their efforts, ideas and reviewing support during the writing process of 2025



Special thanks to the expert group

Davinci
CONCLUSION

Leon Roseleur, Joost Wisselink

INNOPY
A business of Oliver Wyman

Denise Hoppenbrouwer

UIES

Barend Mons

NimbleNova

Ewout Bouwman, Fabian Haijenga

TNO

Michiel Stornebrink, Bernadette Farias Loscio, Matthijs Punter, Harrie Bastiaansen



Special thanks to the Steering Committee of NL Data Sharing Initiatives & their architects

bdi

Sjoerd Boot, Steven Schouten, Ewout Bouwman

health RI
enabling data driven health & life sciences

Ruben Kok, Niels Bolding

HeNormo
duidelijke afspraken • veilige emergedata

Klaas Hommes, Richard Beekhuis, Gerard Huis in 't Veld

REALISATIE IBDS (FDS)

Ronald Slomp, Mike Dell, Danny Greefhorst

sc sn
expert communities
supporting
networks

John Blankendaal, Adriaan van Kalker, Guido Budziak (TNO), Maarten Kollenstart (TNO)

Introduction

- Goals & purpose | How MAMI contributes to accelerating sovereign data exchanges
- Usefulness in practice | How MAMI lets you win
- Possible applications | How to start using MAMI effectively based on your goals

With MAMI, CoE-DSC aims to contribute to interoperability, defragmentation and acceleration for sovereign data exchanges

The ecosystem for sovereign data exchange is maturing...



Sectoral data sharing initiatives (DSIs) are growing and maturing. CoE-DSC identified over 50 initiatives in the Netherlands.

Data space technology and approach are evolving and converging, due to EU R&D, standardisation and regulation.

Service providers start offering data space components “as a service”.

In a changing geopolitical landscape, EU society is rapidly discovering a concrete need for digital sovereignty

...but there are adoption, tech and interoperability challenges



However, data sharing initiatives and its participants struggle to:

Organise interoperability on various levels (semantic, technical, business & legal) required for data sharing within and between sectors

Make future-proof architecture choices for interoperable data sharing

This leads to a fragmented, not interoperable landscape, where participants struggle to find real-world business value, slowing adoption.

MAMI supports data sharing initiatives, service providers and policymakers to plot a joint, no-regret path forward



Together with leading Dutch DSIs and a team of various topic experts, CoE-DSC drives an iterative process to assemble and structurally update a basic set of minimal, no-regret recommendations, and gradually plot DSI's on it.

Single DSI's (or their participants) can use MAMI to plot themselves and granularly determine where they can improve to be more generically interoperable, and incorporate this into their architecture and roadmaps.

When creating specific cross-sectoral use-cases, multiple DSI's (or their participants) can compare their MAMI plots to quickly identify matches and blind spots to create 1-on-1 interoperability between them.

Service providers can use MAMI and the plots from DSI's to tune their products to suit generic and specific interoperability demands.

Policy makers can use MAMI to form policy, and as input for tenders or subsidy programs to create defragmentation instead of reinventing the wheel.

MAMI is a set of recommendations intended to help initiatives to reflect on design choices & become more interoperable

What is MAMI in a nutshell?

A set of recommendations

A set of recommendations listing “no-regret” best practices on various dimensions that together constitute a minimal set to approach interoperability discussions.

A list of protocols supporting recommendations

Each recommendation comes with an example list of protocols, from which any initiative can get inspiration for their design choices and/or add to the list

A plotted position of individual data sharing initiatives

Each DSI can plot itself (with support from CoE-DSC) on the MAMI framework:

- What recommendations does it support now, will it support in 1-2 years, and will it not support due to sectoral peculiarities
- What protocols does it support, and how generic are those within their sector.

Co-created & updated iteratively

What is the intended use?

The MAMI framework is intended to help any initiative to assess and further improve:

- **Human readability and actionability**, i.e. explicit publication of all relevant information to become a participant, share data and create valuable use cases within or across sectors, needed to promote adoption and growth.
- **Machine readability and actionability**, needed to facilitate automated interactions between participant and/or 3rd parties.
- **Clarity regarding chosen trust anchors** for the provision of key services in the initiative, needed to build trust among participants and/or 3rd parties.

How can it help achieve DSI's goals?

- **MAMI serves as a litmus test to discover potential blind spots** in architecture design & helps reflect on the way towards maturation and future-proof design choices.
- **MAMI makes your architectural choices explicit:** easier for new participants and service providers to interact with your initiative, which supports your “adoption/growth” KPIs.
- **MAMI structures discussion on approaches for cross-domain interoperability (e.g., harmonisation/proxy models):** step-by-step way to find similarities and differences on framework- and protocol-level between initiatives from different domains

MAMI can be used step-by-step to cover various needs

			
Individual initiatives wanting to boost generic interoperability	Two (or more) initiatives wanting to arrange cross-domain interoperability	Service providers (incl. trust anchors) in a field related to certain recommendations	Policy makers in a field related to certain recommendations
1 Individually go through the MAMI recommendations and compare to your current situation and roadmap. 2 Plot what recommendations you: • Already follow • Will follow in 1-2 years • Will not follow, including reasons why 3 Plot what protocols are common in your sector, and which you support or will support 4 Compare your plot with plots from other sectors for inspiration on the direction forward 5 Update your roadmap and strategy accordingly, and execute 6 Publish your plot via CoE-DSC	Follow steps 1 2 3 & continue here: 4 Compare the plots of both initiatives • Identify common areas, conflicts and blind spots on recommendations and protocols 5 Decide on interoperability method per topic*: • <i>Harmonisation</i>: create a roadmap to harmonize both initiatives to become similar on selected topics • <i>Proxy</i>: create a proxy model that is able to translate between both initiatives on selected topics 6 Update both roadmaps and strategies accordingly, and execute 7 Publish your plots via CoE-DSC <i>*Pay special attention to topics where recommendations are not followed, due to sector specific reasons</i>	1 Go through recommendations to see where your services can be relevant to data sharing initiatives 2 Compare your service offering to plots by DSI's 3 Identify gaps in your service offering on relevant topics with relevant sectors 4 Update your roadmap and strategy accordingly 5 Publish your plot via CoE-DSC <i>Steps 2-3 are only relevant when sufficient plots are available</i>	1 Go through recommendations & common lists of protocols. 2 Go through plots of relevant sector initiatives and service providers 3 Assess where your policies can help solidify the use best practices and (de facto) standards among initiatives in applicable sectors 3 Build guides for tender and subsidy provision to incentivise initiatives and service providers to follow interoperable solutions and/or avoid reinventing the wheel <i>Steps 2 is only relevant when sufficient plots are available</i>
Reach out to the authors if you need support to plot your initiative, have feedback or what to join our efforts in 2026			

North Star

- Navigating the North Star
- Current trends | From Fragmentation to Federation
- Emerging ecosystems | From Pilots to Production
- Future trends | Exploring 3 complementary scenarios
- Strategic implications | Ways to be future-ready

Alongside MAMI Framework, North Star was written to provide insights on trends & developments beyond the span of 1-2 years

What is in a North Star in a nutshell?



Current Trends

Examines the foundational developments reshaping data sharing: interoperability standards that reduce fragmentation, trust frameworks that enable sovereignty, and infrastructure that scales connectivity. These are not abstract concepts but building blocks already operational in production environments.



Emerging Ecosystems

Maps the consolidation happening across national, domain-specific, and cross-sector initiatives, showing how regulatory mandates are transforming voluntary pilots into required infrastructure.



Future Trends

looks ahead to the shifts we foresee in the future, exploring perspectives to reveal where the ecosystem is heading and what readiness looks like:

- Decentralized trust architectures,
- Data visiting models that eliminate the need to move sensitive datasets,
- Personal data spaces that extend federated principles to individual agency.

Read full North Star Document [here*](#)

*Please note, links to the full North Star Document will be added to this page after publication on the CoE-DSC website

10 January 2026. Centre of Excellence for Data Sharing and Cloud. All rights reserved.

What is the intended use of the North Star?

- North Star serves as an accompanying document to the MAMI Framework.
- While MAMI recommendations present a practical guidance that is focused on getting your initiative more mature in regard to interoperability in a span of upcoming 1-2 years, North Star aims to look forward and explore future trends.
- North Star sets the foundation for the detailed recommendations that follow, connecting today's developments to tomorrow's opportunities and ensuring your organization and/or data sharing initiative can move confidently in a complex, evolving environment.
- Next pages provide key insights from the North Star content. The full North Star document can be found [here*](#) at the CoE-DSC website.

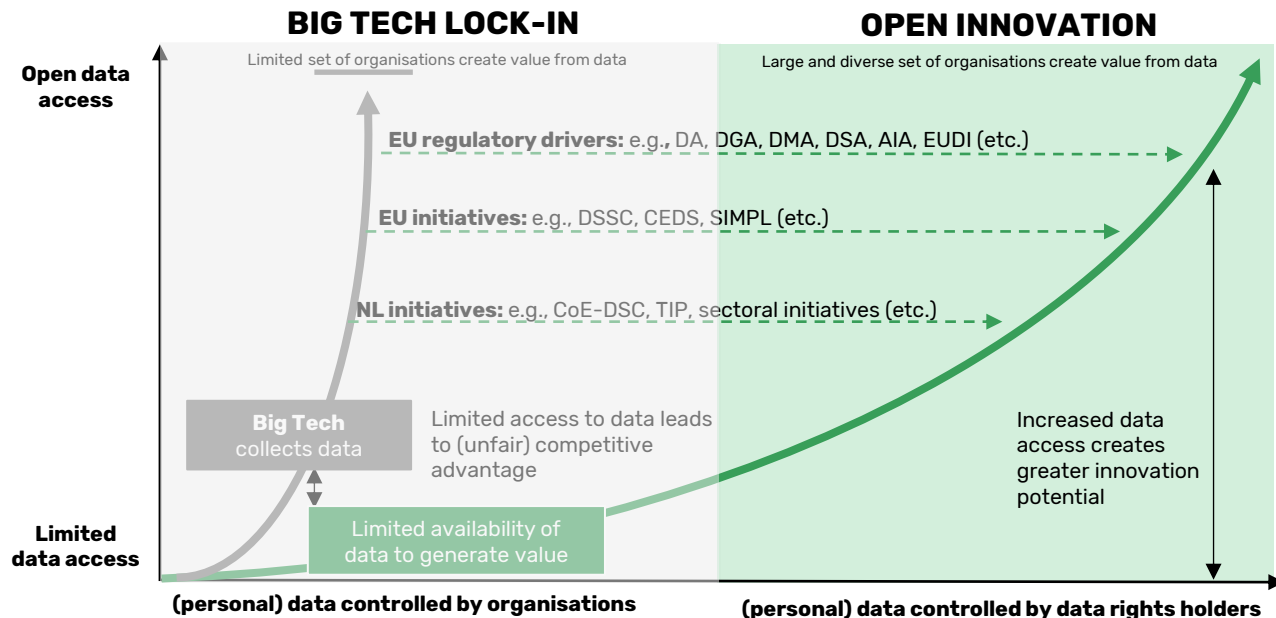


North Star: Current trends - *From Fragmentation to Federation*

1/4

Key insights

- Data sharing initiatives struggle with the same challenges: proprietary connectors, duplicated integration work, & trust barriers slowing ecosystem growth. Each new partnership requires custom technical work, legal negotiations, and identity verification - making data spaces difficult to scale.
- Now, at least three foundational developments are currently shifting data spaces from vision to operational reality: interoperability standards, verifiable trust frameworks, and shared infrastructure on local and EU scale.



Explanation of trend arrows

- ➔ Control over personal data lies in the hands of a few large Big Tech corporations. Neither the generators of the personal data nor data owners have an equal shot to reap the benefits of data sharing
- ➔ EU regulatory drivers, public and private initiatives contribute to the safe and reliable access and portability of data under the control of the entitled party. These drivers reduce data monopolisation, initiate data exchange and lower barriers for market parties and individuals to share data under EU values
- ➔ As a result, data sharing stimulates innovation and economic returns from data which are distributed more fairly among various market parties and individuals

Source: IMEC, Universiteit Gent, INNOPAY and TNO analysis

North Star: Emerging Ecosystems - *From Pilots to Production*

2/4

Key insights

Across Europe, data sharing ecosystems are evolving from pilot projects toward production infrastructure, though the path to operational maturity varies significantly. While regulatory mandates in various sectors (stick) are beginning to transform participation from optional to required, most data spaces are still refining their value propositions and building sustainable adoption with various tools emerging to assist new value capture (carrot).

Tools & Support



Data spaces Support Centre (DSSC),
Data Spaces Business Alliance (DSBA):
IDSA, Gaia-X, Fiware, BDVA

European Data Innovation Board
(part of Data Governance Act)

European Interoperability Framework (EIF)

Rolling Plan for IT Standardisation

SIMPL (Labs, Open, Live)

Data spaces development



EU Level:

Common European Data Spaces:

- European data space for agriculture
- European data space for cultural heritage
- European data space for energy
- European data space for finance
- European Green Deal data space incl. smart cities
- European data space for health
- European data space for research & innovation
- European data space for language
- European data space for manufacturing
- European data space for media
- European data space for mobility
- European data space for public administration
- European data space for skills
- European data space for tourism

Local level:

- Public & private data sharing initiatives (on a member state level)

Regulatory frameworks



Non-exhaustive

Universal:

- Data Act
- Data Governance Act
- Interoperable Europe Act
- AI Act
- Digital Services Act
- Digital Markets Act
- GDPR

Sector Specific:

- FIDA
- PSD&PSR
- eFTI
- EHDS
- Open Data Directive

Facilitation of interop. tools:

- EUDI regulation (eIDAS2)
- DPPs via ESPR



Carrot



Stick

North Star: Future Trends- *Exploring 3 complementary scenarios*

3/4

Key insights

The future of data spaces offers three distinct yet complementary scenarios. The convergence of 3 scenario's (federated trust, data visiting, and personal data spaces) may create a fundamentally different data economy, though the pace and pattern of adoption will vary by sector and context.

3 Scenarios – Federated Trust, Data Visiting, Personal Data Spaces

Scenario

What does it entail



Federated Trust

- **Participant-driven trust**, (e.g., by negotiating via Data Space Protocol (DSP))
- **Community-driven trust** (e.g., arranged by communities via rulebooks & agreements frameworks)
- **Market-driven trust** (e.g., via Cross-sectoral certification bodies, reputation systems, common carrier infrastructure)

Decentralized trust frameworks – layered models where trust emerges from participants, communities, and markets rather than being imposed top-down



Data Visiting

- **FAIR data trains – driven trust** (Data objects are made FAIR (findable, accessible, interoperable & reusable) with strict governance controls, allowing algorithms (trains) to “visit datasets”)
- **Privacy enhancing technologies (PETs)-driven trust** (The computation happens securely at the source and only results are shared)

Decentralized trust is achieved by ensuring sensitive data stays at a source, and is not directly shared. “Data stations” run queries with strict access & usage controls.



Personal Data Spaces

- **Self-sovereign implementations – driven trust** (e.g., personal data wallets and vaults, like introduced by EUDI regulation (eIDAS), and Solid implementations)

Decentralised trust is achieved by allowing individuals to store, manage, & selectively share data across services on their own terms.

Strategic implications & how to be prepared

Strategic implications:

- **Multi-layered trust may become the norm:**
Organizations must navigate participant, community, and market trust mechanisms simultaneously. Single-authority models won't scale.
- **Data mobility may coexist with data access:**
Infrastructure investments shift from secure data transfer only to also supporting secure computation environments and queryable interfaces
- **Consent becomes competitive enabler:** Individual data rights move from compliance burden to competitive advantage for organizations that design for consent-based models early.

How to be prepared:

The organizations that thrive in federated data sharing will be those that prepare not for a single trust model, data pattern, or participant type, but for the messy, multi-layered reality of decentralized ecosystems (read more in the full [North Star*](#)).

MAMI's value lies in providing navigational clarity through this complexity, ensuring readiness across the dimensions that matter: semantics, discoverability, trust, and connectivity.

*Please note, links to the full North Star Document will be added to this page after publication on the CoE-DSC website

North Star: Strategic implications - *Ways to be future-ready*

4/4

Key insights

Interoperability is a shared responsibility. It can only be achieved through an intense collaboration between all stakeholders (DSIs, SPs, and policy makers). Each of the three has distinct roles to stimulate development, collaboration, support & awareness and compliance.

Role in:

Development

Collaboration

Awareness & Support

Compliance

Data Sharing Initiatives



Discovery of user needs for cross-domain use cases and interoperability solutions grounded in practical reality

Stimulation of interactions leading to discovery of needs within a bigger relevant audience

Create an environment where participants can generate and share knowledge

Monitoring of relevant changes in **regulatory landscape** for involved stakeholders

Service providers



Creating great products addressing the demand for interoperable, scalable solutions

Co-creating technical and business solutions, standards and implementations together with the field

Supporting clients in creation & exchange of insights

Aiding clients to achieve compliance

Policy makers



Creating favourable conditions for a market for interoperability, stimulating demand & supply

Involving stakeholders in shaping policy instruments

Promoting awareness and understanding of standards, regulation and best practices

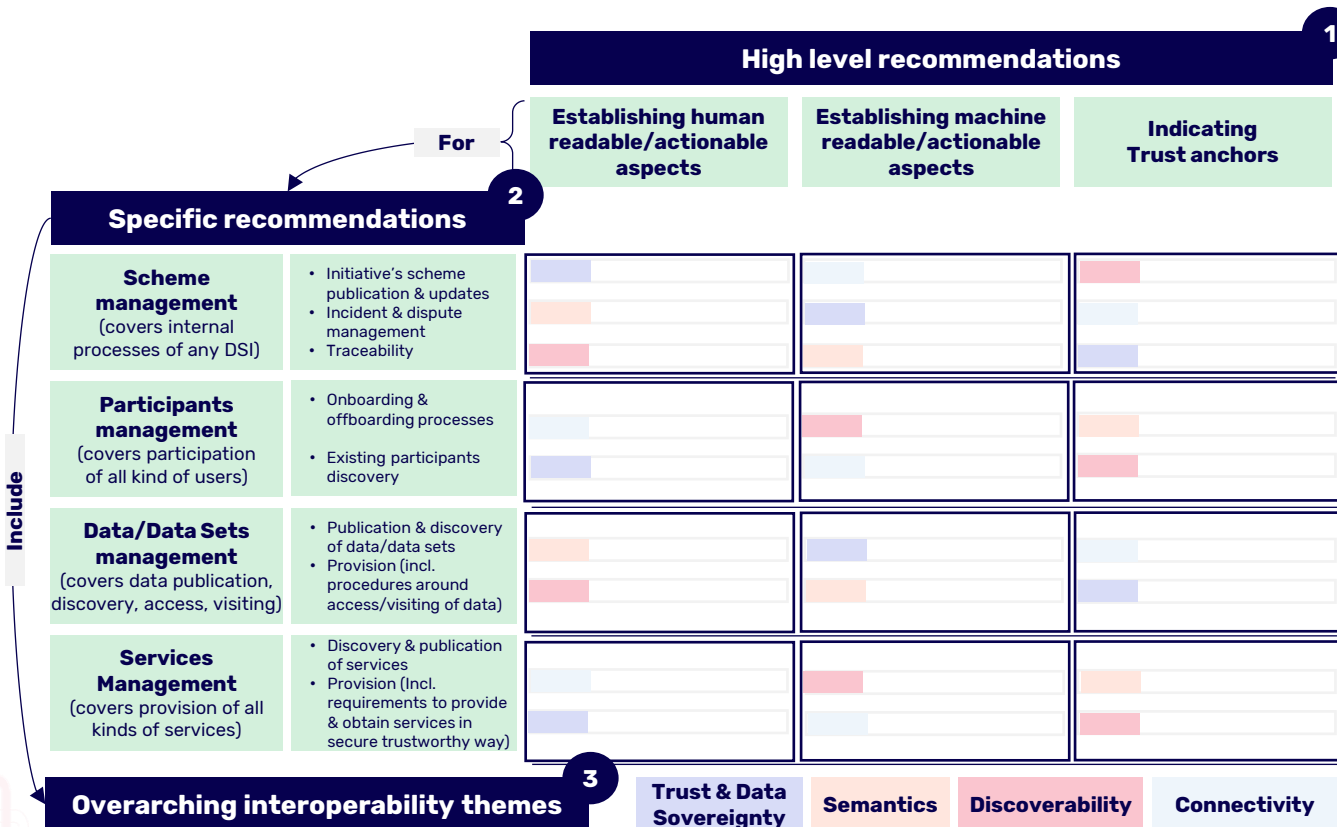
Enforcing regulation

Source: Source: CoE-DSC analysis (desk research & interviews), additionally see [DSIC 2024](#)

MAMI Core Contents 2026

- [Navigating recommendations](#)
- [High level recommendations](#)
- [Specific Recommendations](#)
- [List of common standards, protocols, & trust anchors](#)

Navigating MAMI framework in 4x3 matrix from a birds-eye view

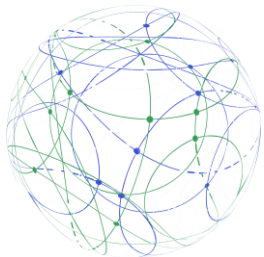


Content navigation

Here is a schematic representation of what you will see during your review of MAMI recommendations.

- 3 high level recommendations** of MAMI, contain descriptions on how any DSI can ensure that what they provide to their participants (& any potential 3rd parties) in terms of content/support is:
 - Human readable & actionable
 - Machine readable & actionable
 - Includes accepted trust anchors for their participants & 3rd parties to rely on
- Specific recommendations** dive deeper into how exactly human & machine readable/actionable support can be established, and what trust anchors can be considered for certain processes
- Each specific recommendation falls under an **overarching interoperability topic/theme**, (as indicated by colour coding). This would allow MAMI readers to sort for a specific category of their interest. In the future more categories may be added (& references to DSSC Building Blocks are also being made)

High level & Specific Recommendations repository with links



Navigation note:

High level recommendations are meant to provide overarching insights.

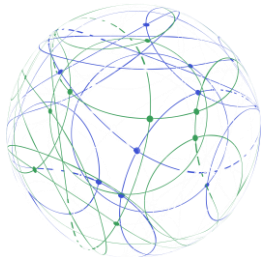
More practical information and actionable pointers* to enhance interoperability are covered in specific recommendations below on how to approach design choices and protocols per specific topic

- For human readability/actionability
- For machine readability/actionability
- For deciding on relevant trust anchors

*For actionability, recommendations are written in MOSCOW approach (according to [RFC2119](#) and ISO), that is each recommendation has an action indicator MUST, SHOULD, COULD, WON'T

			Human readable/ actionable	Machine readable/ actionable	Trust Anchors
			R-HRA-0	R-MRA-0	R-TA-0
Specific recommendations			Codes linking to recommendations		
Category	#	Title			
Scheme Management	1.1	Scheme publication & updates	S-HRA-1.1	S-MRA-1.1	S-TA-1.1
	1.2	Incidents & dispute management	S-HRA-1.2	S-MRA-1.2	S-TA-1.2
	1.3	Traceability	S-HRA-1.3	S-MRA-1.3	S-TA-1.3
Participants management	2.1	On(off)-boarding	PP-HRA-2.1	PP-MRA-2.1	PP-TA-2.1
	2.2	Participants discovery	PP-HRA-2.2	PP-MRA-2.2	PP-TA-2.2
Data/data sets management	3.1	Publication & discovery	D-HRA-3.1	D-MRA-3.1	D-TA-3.1
	3.2	Provisions	D-HRA-3.2	D-MRA-3.2	D-TA-3.2
Services management	4.1	Publications & discovery	SER-HRA-4.1	SER-MRA-4.1	SER-TA-4.1
	4.2	Provisions	SER-HRA-4.2	SER-MRA-4.2	SER-TA-4.2

Contents of the high-level recommendations



High level recommendations

Human readable/actionable

Machine readable/actionable

Trust Anchors

R-HRA-0

To enhance interoperability, DSIs MUST provide explicit human readable(1) and actionable (2) descriptions regarding their scheme agreements, participants, data, and services.

- 1 Human readable means that the information provided MUST be made accessible for a human (i.e. clear readable text*)
 - Note: To ensure broader accessibility to individuals with disabilities, DSIs COULD consult EU Accessibility Act to improve their webpages. (In certain cases, websites are subjected to EU Accessibility Act, please consult footnotes to determine if that is the case in the context of your DSI)
- 2 Human actionable means that the information provided MUST be current, unambiguous and includes instructions that a trained specialist is able to follow & fulfil.

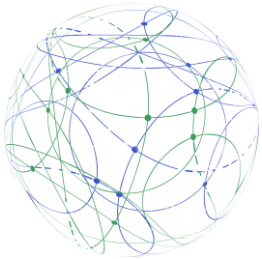
***Extra footnote regarding EU Accessibility Act:**

Organisations with 10 or more Full-Time Employees (FTEs) or an annual turnover exceeding €2 million MUST ensure compliance with WCAG 2.2. Level AA accessibility standards set forth by the EU Accessibility Act . This includes, but is not limited to:

- *Providing text alternatives for non-text content (e.g., images, charts).*
- *Ensuring sufficient colour contrast between text & background.*
- *Designing navigable interfaces that can be accessed via keyboard and compatible with assistive technologies.*

Organisations with fewer than 10 FTEs or an annual turnover below €2 million SHOULD consider adopting Level AA accessibility standards voluntarily. This proactive approach not only enhances usability for individuals with disabilities but also positions the organization as a socially responsible leader in the digital space.

Contents of the high-level recommendations



High level recommendations

Human readable/actionable

Machine readable/actionable

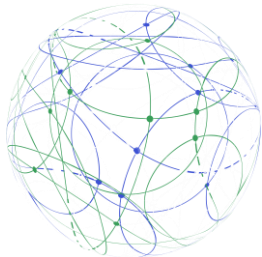
Trust Anchors

R-MRA-0

To enhance interoperability, DSIs SHOULD provide explicit machine readable (1) and actionable (2) descriptions regarding their scheme agreements, participants, data, and services

- 1 Machine readable means that the information provided MUST be accessible for a machine/algorithm:
 - Human-readable digital medium that is marked up* so that it can also be read by machines (e.g. microformats, RDFa, HTML)
 - Data file formats intended principally for processing by machines (e.g., CSV, RDF, XML, JSON).
 - *(*)Please note: Machine-readable content can be automatically transformed for human-readability but, generally speaking, the reverse is not true.*
- 2 Machine actionable means that the information provided MUST include instructions/code that a properly programmed machine/server/algorithm is able to read and execute:
 - To be machine actionable a content MUST have an executable code that can handle basic commands, known as CRUD operations: POST, GET, PUT, PATCH, DELETE
 - Usage of standardized protocols that have significant real-world adoption relevant to the DSI sectoral context is highly encouraged. Chosen protocols by a DSI MUST be explicitly indicated, to ensure parties are able to interact within and between DSI's.
 - Usage of APIs (Application Programming Interface) is highly encouraged to allow servers/ software systems to interact with each other. (e.g., RESTful APIs) to allow:
 - (1) Scalability: Statelessness allows easy scaling of services.
 - (2) Flexibility: Can be used with any programming language or platform.
 - (3) Simplicity: Easy to understand and implement due to its reliance on standard HTTP methods

Contents of the high-level recommendations



High level recommendations

Human readable/actionable

Machine readable/actionable

Trust Anchors

R-TA-0

To enhance interoperability, DSI's MUST specify the Trust Anchors (1) with regards to key provisions within their schemes (2)

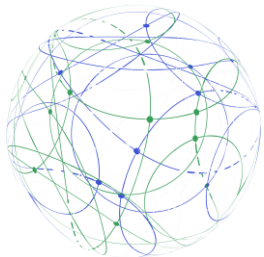
1 Trust anchors MUST be accepted by a DSI in relation to a specific scope of attestation(*)

- As defined in line with DSSC Glossary, Trust anchors are - "bodies, parties, i.e., Conformity Assessment Bodies or technical means accredited by the data space governance authority to be parties eligible to issue attestations about specific claims."
- (*) [DSSC Glossary reference to ISO/IEC 17000:2020\(en\)](#)

2 DSIs MUST specify for the provisions within their schemes which Trust Anchors are used respectively

- In their scheme management (e.g., for publication & updating the scheme, for incident & dispute management)
- For participation related provisions (e.g., issuance of identities, credentials, certificates, mandates etc.)
- For data related provisions (e.g., specifications on metadata, and any other relevant aspects like data quality, usability, provenance, etc.)
- For service related provisions (e.g., security of the exchange protocols, applications, services etc.)

High level & Specific Recommendations repository with links



Navigation note:

High level recommendations are meant to provide overarching insights.

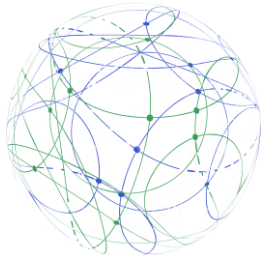
More practical information and actionable pointers* to enhance interoperability are covered in specific recommendations below on how to approach design choices and protocols per specific topic

- For human readability/actionability
- For machine readability/actionability
- For deciding on relevant trust anchors

*For actionability, recommendations are written in MOSCOW approach (according to [RFC2119](#) and ISO), that is each recommendation has an action indicator MUST, SHOULD, COULD, WON'T

			Human readable/ actionable	Machine readable/ actionable	Trust Anchors
			R-HRA-0	R-MRA-0	R-TA-0
Specific recommendations			Codes linking to recommendations		
Category	#	Title			
Scheme Management	1.1	Scheme publication & updates	S-HRA-1.1	S-MRA-1.1	S-TA-1.1
	1.2	Incidents & dispute management	S-HRA-1.2	S-MRA-1.2	S-TA-1.2
	1.3	Traceability	S-HRA-1.3	S-MRA-1.3	S-TA-1.3
Participants management	2.1	On(off)-boarding	PP-HRA-2.1	PP-MRA-2.1	PP-TA-2.1
	2.2	Participants discovery	PP-HRA-2.2	PP-MRA-2.2	PP-TA-2.2
Data/data sets management	3.1	Publication & discovery	D-HRA-3.1	D-MRA-3.1	D-TA-3.1
	3.2	Provisions	D-HRA-3.2	D-MRA-3.2	D-TA-3.2
Services management	4.1	Publications & discovery	SER-HRA-4.1	SER-MRA-4.1	SER-TA-4.1
	4.2	Provisions	SER-HRA-4.2	SER-MRA-4.2	SER-TA-4.2

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

S-HRA-1.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs MUST publish their schemes in a way that is human readable and actionable with a clear version management (notably, published material doesn't have to be open access, depending on sensitivity of the content) (1,2)

- 1 The extent of access to the published scheme depends on the sensitivity of the content:
 - Unless highly sensitive, scheme agreements MUST be made publicly available
 - In case of highly sensitive content, explicit descriptions MUST be provided about conditions under which a party is allowed to access published scheme agreements
- 2 DSIs MUST regularly (re)determine the extent of sensitivity for openly publishing their scheme agreements. To do so they can use the following factors:
 - commercial implications
 - regulatory & legal implications

Overarching interoperability themes in scope of this recommendation are marked in bold:

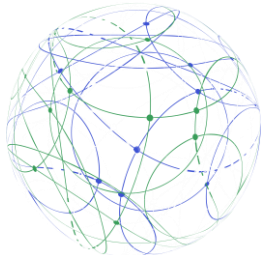
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

S-MRA-1.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs SHOULD publish their schemes in a way that is machine readable and actionable (to the extent that is permitted by sensitivity & privacy conditions) 1,2,3

- 1 A scheme SHOULD be published in a machine-readable format
 - e.g., HTML
- 2 A scheme SHOULD include machine-actionable instructions in the form of a code/APIs for a certain set of provisions that are crucial for interacting with a scheme as a participant (or a developer on behalf of a participant). Code instructions/APIs can be positioned:
 - Throughout the scheme
 - In a dedicated adjacent testbed
- 3 In case scheme content is sensitive:
 - Access management controls MUST be in place for schemes that hold sensitive information
 - Clear conditions MUST be included under which a party (participant, 3rd party, and or server/algorithm of a participant/3rd party) can have access to the scheme contents.

Overarching interoperability themes in scope of this recommendation are marked in bold:

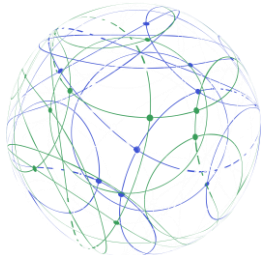
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



S-TA-1.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs MUST specify which Trust Anchors are used in their scheme management (for the process of publication & updating the scheme) 1,2

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 MUST specify the actor (also known as a governance/scheme authority) which is responsible for publishing and updating the scheme.
 - Indicate which party/organisation fulfils that role at the moment
 - If applicable specify any procedures relevant to change & re-application to fulfil the role of the scheme authority.
- 2 MUST specify allowed procedures/actions that the scheme authority can conduct for updating and publishing the scheme

Overarching interoperability themes in scope of this recommendation are marked in bold:

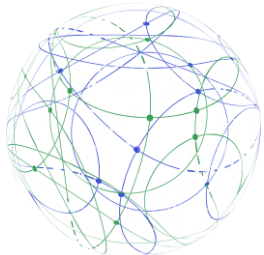
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



S-HRA-1.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs MUST provide legal clarity for dispute handling in a human readable/actionable way (1,2)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- DSIs SHOULD include conditions in the scheme agreement/contract via various clauses, which can be:
 - Settlement clauses (conditions in case parties prefer to resolve disputes without resorting to litigation)
 - Liability clauses (conditions behind liability claims/penalties for certain types of damages and/or losses)
 - Any force majeure clauses (if and where applicable)
- DSIs COULD facilitate a dedicated place to reach out for support, and/or to flag issues brought up by participants or aspiring participants
 - This could be in a form of a “complaint/ support bureau” via hotline/email/website.

Overarching interoperability themes in scope of this recommendation are marked in bold:

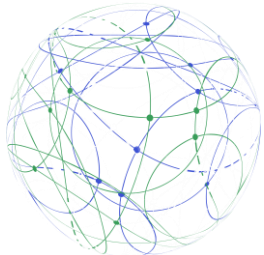
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



S-MRA-1.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs COULD provide machine readable/actionable mechanisms for facilitating the processes behind (1) automatic flagging of incidents & (2) progress tracking of dispute management.

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 A DSI COULD support an automatic way for flagging incidents (e.g., in a form of dashboards to signal issues with onboarding, data leaks, data mis-use, any other scheme breaches etc)
 - If that is put in place, the Scheme Authority MUST have clear instructions on how to interpret & react to incidents
- 2 A DSI COULD support an automatic way to track progress of the started disputes (e.g., in a form of a dashboard, and/or a dedicated portal).

Overarching interoperability themes in scope of this recommendation are marked in bold:

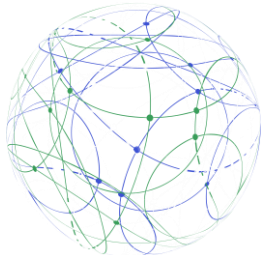
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



S-TA-1.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs MUST indicate what are the trust anchor(s) that parties can go to for dispute management (1,2,3)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 This COULD be a litigation via court:
 - If so, specifying under which jurisdiction(s) certain disputes fall, will provide clarity to the participants & 3rd parties during dispute management.
- 2 This COULD be via boards of arbitration:
 - If so, specifying which party(s) are trusted and credible to be the arbiter, will provide clarity to the participants & 3rd parties during dispute management.
 - This includes indicating to what extent this is the responsibility of the Scheme Authority.
- 3 This COULD be via mediation:
 - If so, specifying which party(s) are trusted and credible to fulfill that role, will provide clarity to the participants & 3rd parties during dispute management.
 - This includes indicating to what extent this is the responsibility of the Scheme Authority.

Overarching interoperability themes in scope of this recommendation are marked in bold:

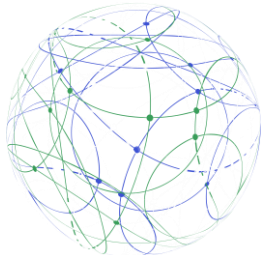
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



S-HRA-1.3

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, any traceability tools provided by a DSI **MUST** generate a human readable/actionable record that can be used to achieve legal clarity for any subsequent dispute handling. (1)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- Traceability tools (e.g., ledgers, audit trails, logs etc.) **MUST** be set up in a way that:
 - Allows to record and trace occurred machine-to-machine (M2M) and/or human-to-machine (H2M) transactions between various participants and/or 3rd parties interacting under the scope of DSI's scheme.
 - Produces a record that is tamper-proof, with immutability guarantees (e.g., qualified electronic ledger trust service under eIDAS 2.0).
 - Produces a record that is human readable/actionable for a legal professional to use during dispute management (e.g., in court, board of arbitration, and/or mediation)

Overarching interoperability themes in scope of this recommendation are marked in bold:

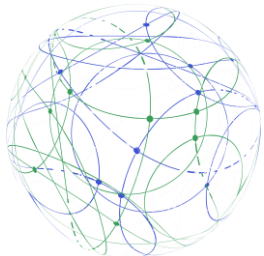
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



S-MRA-1.3

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, any traceability tools provided by a DSI SHOULD generate a machine readable/actionable record that can be used to achieve automatic flagging of incidents, and aid in subsequent dispute handling (1)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- Traceability tools (e.g., ledgers, audit trails, logs etc.) MUST be set up in a way that
 - Allows to record and trace occurred machine-to-machine (M2M) and/or human-to-machine (H2M) transactions between various participants and/or 3rd parties interacting under the scope of DSI's scheme
 - Produces a record that is tamper-proof, with immutability guarantees (e.g., qualified electronic ledger trust service under eIDAS 2.0).
 - Produces a record that is machine readable/actionable so that a machine/algorithm responsible for flagging incidents can act upon it (e.g., automatically signaling via an incident dashboard)

Overarching interoperability themes in scope of this recommendation are marked in bold:

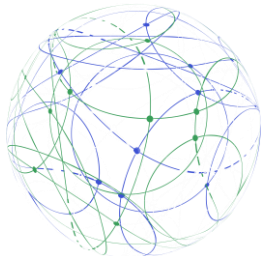
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



S-TA-1.3

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance trust, credibility and transparency DSIs **SHOULD** specify (1) what are the Trust Anchors responsible for the operation/provision of the traceability tools in a tamper-proof & immutable manner, and (2) what is being traced in line with the scope of their schemes.

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 A DSI **SHOULD** specify a Trust Anchor responsible for the operation/provision of the traceability tools. That is:
 - Specify which licenses/ certifications/ credentials a party must have in order to provide traceability tools under the scheme
 - For example (non-exhaustive):
 - ISO/IEC 27001 (security)
 - ISO/IEC 27701 (privacy)
 - ISO 9001 (quality)
 - ISO/IEC 20000-1 (IT services))
 - EIDAS 2.0 (qualified) electronic ledger trust service
- 2 A DSI **SHOULD** specify what is being traced in accordance with the scope of their scheme, to ensure clarity and transparency for the interacting participants and/or 3rd parties joining the scheme.
 - For example (non-exhaustive):
 - Log of authorised occurred visiting/accessing of data sets
 - Log of authorised computations conducted via queries on data sets
 - Log of any other occurrences where actions with data and/or provision of other services has occurred (e.g., issue of credentials, certificates etc.)
 - Log of monetary transactions as part of services provision

Overarching interoperability themes in scope of this recommendation are marked in bold:

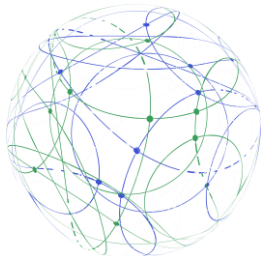
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

PP-HRA-2.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSI's MUST provide human readable/actionable information regarding their scheme participation, which includes onboarding and offboarding procedures (to the extent allowed by privacy & sensitivity conditions) (1,2,3)

- 1 The extent of public disclosure of the scheme participation procedures depend on the sensitivity of the content (e.g., due to business/legal reasons):
 - Unless the scheme content is sensitive, it MUST be made publicly available
 - In case of sensitive scheme content, explicit descriptions MUST be provided about conditions under which a party is allowed to access this information
- 2 As part of the onboarding procedures DSI's:
 - a) MUST specify digital identity means that a participant needs to obtain and that are fit-for-purpose & satisfy scheme conditions in 4 ways. That is:
 - Fit for required Levels of Assurance (LoA) to participate under the DSI scheme
 - Fit for uniquely identifying participants
 - Fit for establishing right mandates for role-based permissions & signage
 - Fit for establishing a clear way to authenticate and authorize a participant
 - b) MUST provide legal clarity via contracts at the time of onboarding regarding conditions/clauses that fall under the scheme; and timely specify any legal effect caused by changes & updates in the scheme.
 - Such contract MUST have clauses to ensure binding effect between participants (i.e., derdenwerking) within a dataspace/initiative
 - MUST be signed by the natural person acting on behalf of the legal entity with the suitable mandate
 - DSI's MUST update contract(s) and communicate changes accordingly in a timely manner
 - c) MUST detail any technical procedures & tests for a participant to run and adhere to prior to joining the scheme in accordance with scheme agreements.
- 3 As part of the offboarding procedures DSI's:
 - a) MUST provide procedural & legal clarity for the contract termination
 - b) SHOULD specify procedures for facilitating closure & proper exit of a participant, e.g.:
 - Any processes to follow at a Scheme Authority
 - Any processes to follow with service providers (like deregistration, node/connection de-activation etc.)
 - Any system tests to ensure proper offboarding has been completed.

Overarching interoperability themes in scope of this recommendation are marked in bold:

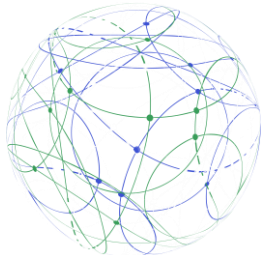
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



PP-MRA-2.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSI's SHOULD provide machine readable/actionable information necessary for scheme participation (1,2,3)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- For onboarding/offboarding procedures DSIs COULD provide code/APIs and/or adjacent testbeds to technically support procedures like:
 - For onboarding:
 - Obtainment of the digital identity certificates and/or any required credentials, attestations
 - Activation of the end-points (could be computational nodes, end-points of an ERP system/server/database)
 - Any automated security tests that a participant's system should run and adhere to in accordance with scheme agreements
 - For offboarding:
 - Automatic procedure facilitating closure & proper exit of a participant (e.g., removal from registries, deactivation of node/connection services etc.)
 - Any automated tests that allow the participant to confirm they were properly offboarded
- The extent of public disclosure of the scheme participation/on(off)boarding procedures and (open) access to testbeds MUST depend on the scheme conditions (e.g., business, privacy sensitivity).
- In case of sensitive/classified content:
 - MUST have access management controls in place for the sensitive content
 - MUST include clear conditions under which a party (participant, 3rd party, and or server/algorithm of a participant/3rd party) can have access to the scheme contents (e.g., signed NDA)

Overarching interoperability themes in scope of this recommendation are marked in bold:

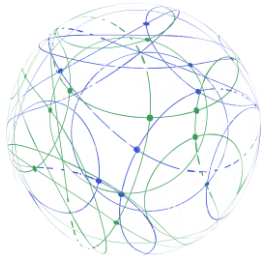
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

PP-TA-2.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability DSI's MUST specify trust anchors for onboarding & offboarding procedures (1,2)

- 1 For onboarding:
 - a) For accepted/trusted Digital Identity:
 - MUST specify who is trusted to provide identifiers for participants E.g., Chamber of Commerce (KvK) – where KvK number is further used for EORI identifier
 - MUST specify who is trusted to provide Digital Identity related certificates E.g., eIDAS QTSPs (Qualified Trust Service Providers)
 - MUST specify who is trusted to provide digital identity related attributes in a form of credentials/attestations E.g., eIDAS QTSPs, Gaia-X Certified Clearing Houses, etc.
 - MUST specify who is trusted to establish mandates for the right of signage on behalf of the legal entity E.g., QTSPs under eHerkenning digital identity scheme
 - b) For legal clarity:
 - MUST specify who is trusted to establish binding effect through the onboarding contracts in a role of the Scheme Authority (i.e., which organisation fulfils a role of Scheme Authority)
- 2 For offboarding:
 - MUST specify who is trusted to bring procedural & legal clarity when facilitating contract termination on behalf of the Scheme Authority (i.e., which organisation fulfils a role of Scheme Authority)

Overarching interoperability themes in scope of this recommendation are marked in bold:

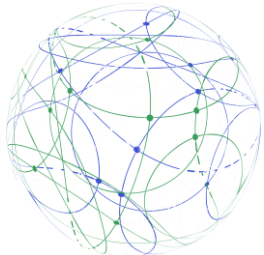
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



PP-HRA-2.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability DSI's MUST provide information about existing participants of the scheme via a registry, (wherein access to specific information is allowed to the extent permitted by sensitivity conditions of the scheme, e.g., due to business/legal reasons) (1,2,3)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 A registry that is put in place, could be fulfilled in various ways and formats depending on the fit-for-purpose (e.g., centralized/ distributed, as database(s), table(s), or list(s)), as long as it is interpretable by a human.
- 2 The registry needs to be properly managed & updated with procedures in place to have a properly updated participant's related information (e.g., membership status and any relevant credentials and respective permissions etc.)
- 3 In case the participant specific information is sensitive/classified, explicit descriptions MUST be provided about conditions under which a party is allowed to access this information.

Overarching interoperability themes in scope of this recommendation are marked in bold:

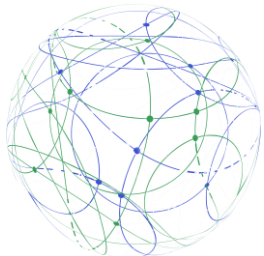
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

PP-MRA-2.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSI's SHOULD provide a machine readable/ actionable registry of participant endpoints (1,2)

- Such a registry can be in any form as long as it is machine readable & actionable and is fit-for-purpose (e.g., via APIs, blockchain ledger, etc.) with clear participant end-points containing relevant credentials, and (any) access permissions.
- The extent of open accessibility to the scheme registry depends on the scheme conditions (business, privacy sensitivity). In case of sensitive/classified content:
 - MUST have access management controls in place for registries with sensitive information
 - MUST include clear conditions under which a party (participant, 3rd party, and or server/algorithm of a participant/3rd party) can have access to the registry

Overarching interoperability themes in scope of this recommendation are marked in bold:

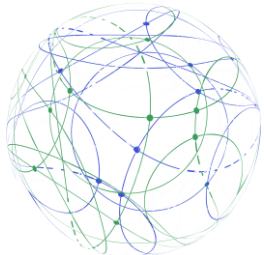
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



PP-TA-2.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability DSIs MUST specify Trust Anchors for registry services provision (1)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 A DSI MUST specify a Trust Anchor responsible for the operation/provision of the registry tools.
 - That is, specify which licences/certifications/credentials a party must have in order to provide registry tools under the scheme; E.g.:
 - ISO/IEC 27001 (security),
 - ISO/IEC 27701 (privacy),
 - ISO 9001 (quality), and
 - ISO/IEC 20000-1 (IT services))
 - eIDAS 2.0 qualified trust services certification
 - GAIA-X clearing house license for service providers
 - iSHARE Satellite credentials

Overarching interoperability themes in scope of this recommendation are marked in bold:

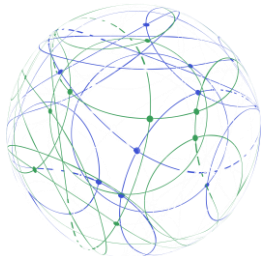
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

D-HRA-3.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSI's MUST provide (at least general) information regarding data sets available to scheme participants (and/or 3rd parties) to discover, understand, access and/or visit said data to the extent permitted by sensitivity & privacy conditions (1,2)

- 1 In case the information around data sets (including metadata) is sensitive/classified, explicit descriptions MUST be provided about conditions under which a party is allowed to access this information.
- 2 The descriptions around available data sets and respective access & usage conditions MUST be sufficiently detailed & SHOULD follow FAIR principles (Findable, Accessible, Interoperable, Reusable)* to enable effective interactivity for the scheme participants (and if applicable 3rd parties).
 - (*) If your initiative falls under EHDS (European Health Data Space) regulation, complying to the FAIR principles is a MUST.
 - [Follow this link to learn more about FAIR](#)

Overarching interoperability themes in scope of this recommendation are marked in bold:

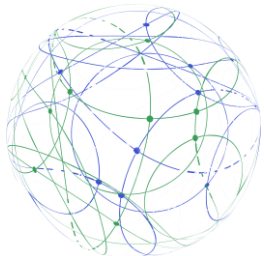
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



D-MRA-3.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs MUST ensure their members provide information about data/data sets in a machine readable/actionable way to give ability to other participants (and/or 3rd parties) to discover, understand, access and/or visit said data to the extent permitted by sensitivity & privacy conditions (1,2,3,4)

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- Generally, DSI participants SHOULD follow FAIR principles* (Findable, Accessible, Interoperable, Reusable) when configuring the metadata for their data sets;
 - (*) If your initiative falls under EHDS (European Health Data Space) regulation, complying to FAIR is a MUST.
 - [Follow this link to learn more about FAIR](#)
- DSI participants COULD provide 3 categories of metadata as fit for their context
 - (1) descriptive – for resource identification & retrieval
 - (2) structural – for relations with other objects/resources
 - (3) administrative – for management & preservation
- DSIs MUST specify metadata standards to be used by their participants for describing data models:
 - For that DSI's SHOULD use common internationally accepted standards (and/or their sector recognized standards). Those COULD be e.g.:
 - RDF Schema and SHACL for RDF (Resource Description Framework).
 - OWL (Web Ontology Language) also for RDF.
 - SKOS (Simple Knowledge Organization System).
 - JSON Schema • XML Schema (XSD), Schematron for XML-oriented data models.
 - CSVW for CSV-oriented tabular data.
 - XSLT, R2RML, RML, and CSVW for data transformation specification.
- DSIs MUST specify which standards can be used by their participants to describe access conditions in their metadata
 - For that DSI's SHOULD use common internationally accepted standards (and/or their sector recognized standards).
 - Those COULD be e.g.: DCAT and ODRL for data publication, discovery, and access/visiting conditions.

Overarching interoperability themes in scope of this recommendation are marked in bold:

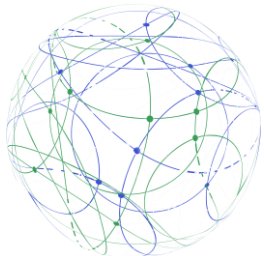
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



D-TA-3.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability DSIs (1) **MUST** specify trust anchors used for metadata standards, and (2) **COULD** specify trust anchors/ credibility means for assurance in data characteristics relevant in the context

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 DSIs **MUST** specify trust anchors for metadata standards (i.e., specify which are trusted/recognised organisations to follow for metadata standards in the applicable context)

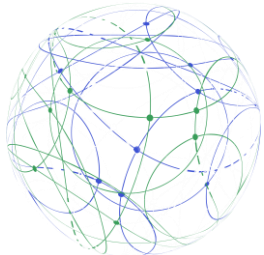
E.g.:

- W3C (World Wide Web Consortium)
- ISO (International Organization for Standardization)
- NISO (National Information Standards Organization)
- Dublin Core Metadata Initiative (DCMI)
- IEEE (Institute of Electrical and Electronics Engineers)
- OASIS (Organization for the Advancement of Structured Information Standards)
- EU Controlled vocabularies,
- GoFAIR Foundation

See footnote for more information on these organisations

- 2 DSIs **COULD** specify Trust Anchors/ credibility means for assurance in data characteristics based on what is expected in the context:
 - E.g., immutability and provenance proofs, data quality reports etc.

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

D-HRA-3.2

Human readable/actionable

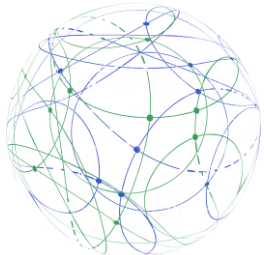
Machine readable/actionable

Trust Anchors

DSI's and/or DSI participants **MUST NOT** provide actual data **UNLESS** the specified access & usage conditions are met, (which **MUST** be documented in a human readable/actionable form) (1,2)

- 1 Actual data **MUST NOT** be accessed **UNLESS** all the applicable access & usage conditions are met by the scheme participants and/or 3rd parties requesting access to the said data.
 - In certain use cases data may never leave the source, and thus only data visiting may be permitted; if this applies, it **MUST** be described under the access & usage policies.
- 2 DSIs **SHOULD** encourage their participants to have access & usage policies and conditions documented in a human readable/actionable form*
 - (*)Since these can be then stored as part of audit trails (i.e., logs of occurred exchanges) for any future incident & dispute management (as already covered in recommendation S-HRA-1.3, [click here to go there](#)).

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

D-MRA-3.2

Human readable/actionable

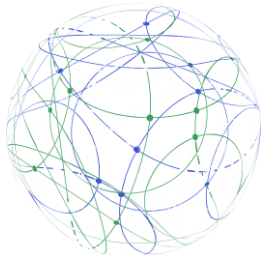
Machine readable/actionable

Trust Anchors

DSI's and/or DSI participants MUST NOT provide actual data UNLESS (1) the specified access & usage conditions are met and (2) during a request for data access/visiting an automatic (machine readable/actionable) procedure of authentication & authorization has been properly complete.

- Actual data MUST NOT be accessed UNLESS all the applicable access & usage conditions are met by the scheme participants and/or 3rd parties requesting access to the said data.
 - In certain use cases data may never leave the source, and thus only data visiting may be permitted; if this applies, it MUST be reflected in the access & usage policies in a machine readable/actionable form.
- DSIs MUST ensure that during digital requests participants can be properly authenticated with a trusted digital identity accepted as part of the scheme.
 - For more on that you can refer to participation & participants management recommendations
 - Click here to navigate to [Participation & Participants recommendations](#)

Contents of the specific-level recommendations



D-TA-3.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs MUST specify the Scheme Authority and/or governance mechanisms/procedures as a trust anchor to ensure participants have obtained trusted digital identity means for relying parties to use for authenticating & authorizing to provide data access

Navigation tab

[Click here to go back to overview](#)

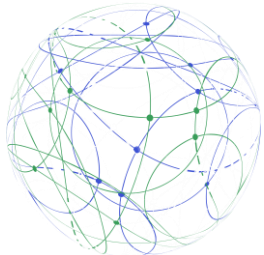
Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

1

Since access & usage policies are typically up to participants who are providing/exposing/allowing visiting to their data, therefore DSIs can only assist in ensuring that other participants have been properly onboarded into the scheme and have trusted digital identity means.

- For more on that you can refer to participation & participants management recommendations
- Click here to navigate to [Participation & Participants recommendations](#)

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

SER-HRA-4.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSI's MUST provide (at least general) information regarding services available to the scheme participants and/or 3rd parties (to the extent permitted by sensitivity & privacy conditions) 1,2

- 1 In case the information around services is sensitive/classified, explicit descriptions MUST be provided about conditions under which a party is allowed to access this information.
- 2 The descriptions around available services and their provision conditions MUST be sufficiently detailed, to enable effective interactivity for the onboarded & potential scheme participants (and if applicable 3rd parties).

These services COULD include:

For core provisions under the scheme; E.g.:

- Digital identity provisions
- Participants registry provisions
- Legal contracting
- Semantics support: vocabularies, taxonomies, metadata creation support etc.
- Traceability
- Connectivity for data provisions (e.g., for data access/visiting)

For additional value creation provisions under the scheme; E.g.:

- Any data analytics & data enrichment provisions (e.g., AI algorithms, Privacy Enhancing Technologies (PETs) provisions)
- Any applications and infrastructural services (e.g., digital twins, digital product passports)
- For more details refer to DSSC

Overarching interoperability themes in scope of this recommendation are marked in bold:

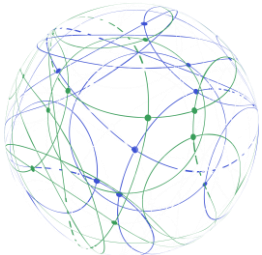
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

SER-MRA-4.1

Human readable/actionable

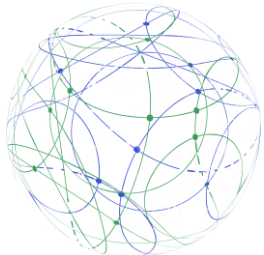
Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs SHOULD ensure they themselves and/or their members provide (at least general) information regarding services available to other participants and/or 3rd parties in a machine readable/actionable way (to the extent permitted by sensitivity & privacy conditions) 1,2,3

- 1 Besides the human readable descriptions of available services, DSI's SHOULD provide actionable code/APIs, and/or adjacent testbeds (where applicable). So that participants and/or 3rd parties can interact with those services.
- 2 The provided code/APIs/instructions SHOULD be sufficiently detailed to access, test & run a service
- 3 In case the information around services is highly sensitive/classified, explicit machine readable/actionable descriptions MUST be provided about conditions under which a party is allowed to access this information (e.g., via an API, access token).

Contents of the specific-level recommendations



SER-TA-4.1

Human readable/actionable

Machine readable/actionable

Trust Anchors

To enhance interoperability, DSIs MUST specify Trust Anchors per service which is provided under the scheme (see possible service lists below *, **) 1

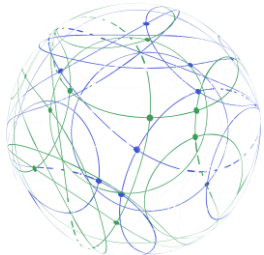
Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

- 1 For each service DSI MUST specify who can be responsible for the operation/provision of that specific service. That is:
 - Parties declared by Scheme authority as a trusted service providers
 - And/or parties complying to the list of recognised licences/ certifications/ credentials that one must obtain in order to be a trusted service provider under the scheme
 - E.g.: ISO/IEC 27001 (security), ISO/IEC 27701 (privacy), ISO 9001 (quality), ISO/IEC 20000-1 (IT services), EIDAS 2.0 qualified trust service provider license
- * Examples of services for which DSIs MUST specify Trust Anchors:
 - For core services/provisions under the scheme:
E.g.: For Digital identity provisions • For participants registry provisions • For legal contracting • For semantics: vocabularies, taxonomies, metadata support etc. • For data provisions (access/visiting) • For traceability
 - *For more details refer to [DSSC](#)*
- ** Example of services for which DSIs COULD specify Trust anchors:
 - For additional value creation services/provisions under the scheme:
E.g.:
 - For any data analytics & data enrichment provisions (e.g., AI algorithms, Privacy Enhancing Technologies (PETs) provisions)
 - For any applications and infrastructural services (e.g., digital twins, digital product passports)
 - *For more details refer to [DSSC](#)*

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

SER-HRA-4.2

Human readable/actionable

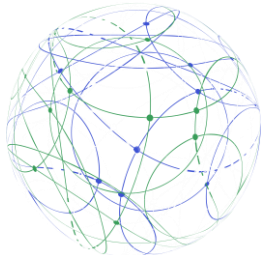
Machine readable/actionable

Trust Anchors

DSIs/DSI participants **MUST NOT** provide actual services **UNLESS** the specified provision conditions are met (such conditions **MUST** be made human readable/actionable) 1

- 1 Actual services **MUST** be delivered only after all conditions for the provision are met. Those conditions can include
 - Any valid registration(s)/ credential(s)/ certification(s) for a service provider to deliver certain services within a scheme
 - Any contract(s) signed and/or payment(s) fulfilled by a party requesting a service
- 2 DSIs **SHOULD** encourage service providers to have provision conditions documented in a human readable/actionable form*
 - (*)Since these can be then stored as part of audit trails (i.e., logs of occurred exchanges) for any future incident & dispute management (as already covered in recommendation S-HRA-1.3)
 - Click here to go to recommendation [S-HRA-1.3](#)

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

SER-MRA-4.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

DSIs/DSI participants **MUST NOT** provide actual services **UNLESS** the specified provision conditions are met, and any automatic checks to authorize the provision of service are completed (1)

- 1 Actual services **MUST NOT** be delivered **UNLESS** all conditions for the provision are met. Those conditions can include:
 - Any valid registration(s)/ credential(s)/ certification(s) for a service provider to deliver certain services within a scheme, (which **COULD** be checked/proven automatically via a scheme authority/registry)
 - Any contract(s) signed and/or payment(s) fulfilled by a party requesting a service (which **COULD** be proven automatically to initiate a service - e.g., automatic payment completion from a bank, etc.)

Overarching interoperability themes in scope of this recommendation are marked in bold:

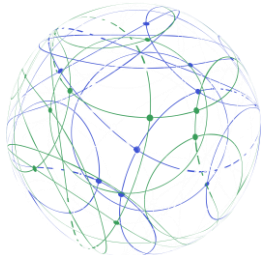
Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Contents of the specific-level recommendations



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

SER-TA-4.2

Human readable/actionable

Machine readable/actionable

Trust Anchors

To ensure credibility for secure provision of services DSIs **MUST** establish Scheme Authority and/or governance mechanisms & procedures to ensure that trusted service providers (for core and value adding services) adhere to the scheme conditions 1,2,3

- For core services where applicable (*), DSIs **MUST** validate and overtime audit that trusted providers have right credentials/ certification/ attestations for provision of services and adhere to security measures established in scheme agreements.
 - (*) Extra audits & checks by DSIs are not needed in case a Trusted Service Provider is recognised as a trust anchor with proper attestations from a higher-level scheme (e.g., Trusted Service providers officially recognised under EU regulation/legislation and/or laws on a Member State level. If that is the case, then a higher-level scheme assures trust).
 - For example: Qualified Trust Service Providers (QTSPs) under eIDAS 2.0 (EUDI Regulation).
- For non-core value-added services DSIs **COULD** validate and overtime audit that trusted providers have right credentials/certification/attestations for provision of services and (if applicable adhere to security measures established in scheme agreements)

Overarching interoperability themes in scope of this recommendation are marked in bold:

Trust & Data Sovereignty

Semantics

Discoverability

Connectivity

Accompanying list of common standards, protocols & trust anchors



The section below covers lists of standards, protocols and trust anchors that form a practical implementation base for the recommendations provided earlier (i.e., for (1) [scheme management](#), (2) [participation management](#), (3) [data](#) and (4) [services management](#)).

Provided are non-exhaustive examples of most commonly used protocols and standards, that are generally suitable for most cross-domain contexts. However, there is no one-size fits all, therefore for specific contexts we encourage MAMI readers to see these lists as an inspiration material and to reach out to the CoE-DSC team for further guidance, and in case of questions.

Accompanying list of common standards, protocols & trust anchors



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

Listed protocols & standards are a collection of non-exhaustive examples, suitability depends on the context

Human readable/actionable

Machine readable/actionable

Trust Anchors

1.1 Scheme Publication & updates

For publishing textual content:

- HTML
- PDF
- Markdown (in Gitlab repositories)

For testbeds/sandboxes:

- APIs (e.g., Rest APIs, OpenAPIs)
- HTTP methods (CRUD commands)

For establishing trust:

- Governance/scheme authority/data space authority responsible for publishing and updating the scheme.

1.2 Incidents & dispute management

For flagging incidents:

- HTTP Webpage (e.g., with a chatbot, contact form)
- Email-address (e.g., info@)
- Phonenumber
- Ticketing system (e.g., Jira Service Management)

For tracking incidents/disputes:

- API calls
- HTTP methods (CRUD commands)

For establishing trust:

- Governance/scheme authority/data space authority to aid with dispute management (if applicable)

1.3 Traceability

For converting logs into textual (human readable) content:

- CSV
- TXT

For registering logs (audit trails):

- JSON
- XML
- Common Event Format (CEF)
- Log Event Extended Format (LEEF)
- Blockchain-based audit trails
- Transactions log portal
- Logboek Dataverwerkingen, PROV

For establishing trust:

- (Certified) service provider(s)/brokers recognised for operation/provision of the traceability tools

Accompanying list of common standards, protocols & trust anchors



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

Listed protocols & standards are a collection of non-exhaustive examples, suitability depends on the context

Human readable/actionable

Machine readable/actionable

Trust Anchors

2.1 On(off)-boarding

For identifying participants:

- GLN - GS1 ID
- EORI (based on KvK number in NL)
- W3C DIDs

NL specific:

- BSN (DIGID)
- KvK number
- UZI pas
- Self-issued Energy Data Link

For authenticating/authorising:

- PKI X.509
- JWT
- SAML
- OAuth2.0
- OpenID Connect (e.g., via IDS Dynamic Attribute Provisioning Service)
- OpenID4VC (OpenID4VCI & OpenID4VP)
- Verifiable Credentials/Presentations
- Decentralized Claims Protocol

NL specific:

- eHerkenning
- DigiD
- PKI-Overheid in NL

For establishing trust:

- Governance/scheme authority/data space authority responsible for establish binding effect through the onboarding contracts
- Various (Certified/qualified) trusted service providers to issue:
 - identifiers to participants
 - digital identity related certificates (e.g., eIDAS QTSPs)
 - attributes in a form of credentials/ attestations/ mandates (E.g., eIDAS QTSPs, Gaia-X Certified Clearing Houses, QTSPs under eHerkenning scheme etc.)

2.2 Participants discovery

For human readable registry:

- HTML
- SQL (for database queries)

For machine readable registry:

- APIs (for end-points)
- Database configurations/engines
- DLT (distributed ledger technology)

For establishing trust:

- (Certified/qualified) trusted service providers responsible for the operation/provision of the registry tools

Accompanying list of common standards, protocols & trust anchors

Listed protocols & standards are a collection of non-exhaustive examples, suitability depends on the context

Human readable/actionable

Machine readable/actionable

Trust Anchors

3.1 Data Publication & discovery

For human readable metadata

- PDF
- HTML (Semantic Treehouse web-based representation of the data models)
- Additionally, mostly the same as the machine readable list (e.g. JSON, XML can produce human readable entries)

For machine readable metadata

- RDF Schema and SHACL for RDF
- OWL (Web Ontology Language) also for RDF.
- SKOS (Simple Knowledge Organization System).
- JSON Schema.
- XML Schema (XSD), Schematron
- CSVW for CSV-oriented tabular data.
- XSLT, R2RML, RML, and CSVW
- ISO 19115 (Geographic Information Metadata)
- NISO Z39.87 (Data Dictionary for Libraries)
- Dublin Core Metadata Terms
- IEEE 1484.12.x (Learning Object Metadata)
- OASIS Context Server Business Standards
- SODA 2.0 (for open data services)
- MEDFORD metadata language
- OpenAPI
- MIM
- DCAT (e.g., DCAT-AP-NL 3.0)
- NL-SBB
- Asset Administration Shell
- Digital Product Passports (DPPs)

For establishing trust:

- Trusted/recognised organisations to follow for metadata standards in the applicable context) e.g.,:
 - W3C (World Wide Web Consortium);
 - ISO (International Organization for Standardization);
 - NISO (National Information Standards Organization);
 - Dublin Core Metadata Initiative (DCMI);
 - IEEE (Institute of Electrical and Electronics Engineers);
 - OASIS (Organization for the Advancement of Structured Information Standards);
 - EU Controlled vocabularies;
 - GoFAIR Foundation

3.2 Data Provisions

For human readable usage policies

- DCAT
- ODRL

For Machine readable usage policies

- DCAT (e.g., DCAT-AP-NL 3.0)
- ODRL
- XACML
- SPARQL
- REGO policy language
- ISO/IEC TS 27560:2023
- IDS Usage Control specifications RAM 4.0
- Gaia-X Policy Reasoning Engine
- Aster X verification & compliance deployment
- Prometheus X verification & compliance deployment
- iSHARE Delegation policy information point.

For establishing trust:

- Governance/scheme authority/data space authority to aid/guide participants in establishing access & usage policies for their datasets



Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

Accompanying list of common standards, protocols & trust anchors



Listed protocols & standards are a collection of non-exhaustive examples, suitability depends on the context

Human readable/actionable

Machine readable/actionable

Trust Anchors

Navigation tab

[Click here to go back to overview](#)

Category	#	Title
Scheme Management	1.1	Scheme publication & updates
	1.2	Incidents & dispute management
	1.3	Traceability
Participants management	2.1	On(off)-boarding
	2.2	Participants discovery
Data/data sets management	3.1	Publication & discovery
	3.2	Provisions
Services management	4.1	Publications & discovery
	4.2	Provisions

4.1 Services Publications & discovery

For human readable services catalogue:

- HTML (e.g., for a developer portal)
- PDF
- DCAT (e.g., DCAT-AP-NL 3.0)
- OAS (via API Design Rules)

For machine readable services catalogue:

- APIs (e.g., OpenAPI; SODA 2.0 for open data services; OAS (via API Design Rules)
- Database configurations (for services catalogue)
- DCAT (e.g., DCAT-AP-NL 3.0)
- DLT (distributed ledger, if applicable)

For establishing trust:

- (Certified/qualified) trusted service providers:
 - (a) for core services/provisions under the scheme
 - (b) for additional value creation services/provisions under the scheme

Rf. Recommendation SER-TA-4.1

4.2 Services Provisions

For human readable service provision conditions:

- HTML
- PDF

For machine readable service provision conditions:

- APIs
- IDS Contract Negotiations (CN) protocol
- Gaia-X Contract Negotiations protocol
- Proof of payment protocol (e.g., SWIFT MT103)

For establishing trust:

- Governance/scheme authority/data space authority to validate and overtime audit that trusted providers have right credentials/certification/ attestations for provision of services and adhere to security measures established in scheme agreements

Lessons learned, reflections & next steps

- [Lessons learned & next steps for authors](#) | Reflections on prioritisation & usefulness of MAMI recommendations

We learned 7 main lessons, which we will act upon in the 2026 CoE-DSC program

In 2025 we learned:		In 2026 we will:	
1	MAMI recommendations can be formulated in a 4x3 matrix, which strikes the balance between sufficient detail without losing overview.	1	Not add too much detail on recommendations, but try to streamline and shorten rather than expand. Also try to give prioritization on which recommendation is most important. Focus will also be more on protocols.
2	We confirmed that the selected MAMI recommendations resonate with DSI architects	2	Approach Service Providers and Policy Makers to validate MAMI also resonates with them, or should be adapted
3	We found that plotting of protocols is most meaningful when considered in the context of an individual sector(s)	3	Create a sector specific plotting mechanism for protocols, based on the Data Sharing Strategy Model (DSSM)
4	Self-plotting by DSI's proved to be complex since: a) Some initiatives are more in design phase and not fully in implementing phase b) Some initiatives cover several sub-initiatives with specific features, making it hard to come to 1 plot c) Some initiatives only cover a part of all building blocks by design	4	Practically support DSI to plot themselves: a) provide support for individual DSI's to plot themselves b) create and publish a website with sector-specific plots to get the ball rolling c) Include the option "does not apply" in the "comply or explain" list and provide mapping support
5	DSI expressed a strong need to see plots of other initiatives for inspiration and coordination	5	Involve MAMI as an integral part of the CoE-DSC acceleration and defragmentation approach, and the CoE-DSC architect community to create a funnel of MAMI-plots
6	MAMI acts as a litmus test to see common issues, blind spots and conflicts for interoperability	6	Use MAMI as a tool to prioritize the CoE-DSC backlog for tools creation and deployment
7	We identified international interest in MAMI	7	Reach out to IDSA and DSSC to promote MAMI internationally

Appendix

Methodology

- [Guiding principles](#)
- [Scope](#)
- [Process](#)

Terminology

- [Glossary](#)
- [Syntax of recommendations](#)

Bibliography

- [Resources & reference material](#)
- [Footnotes to MAMI recommendations](#)

In creating the framework, experts agreed on & followed 7 guiding principles for recommendations

1



Minimal agreements for maximal interoperability

- We don't overengineer
- We don't reinvent the wheel, take what is there, and consider existing open standards
- We target for a large subset, but may not provide 100% coverage

2



Implementable in a production environment

- Within 1-2 years;
- By a competent software engineer

3



Inclusivity: Supporting interoperability in a variety of use-cases

- We stay domain agnostic (inclusivity for cross-border & cross-sector);
- We consider different data types & exchange patterns:
 - (1) primary/secondary use of data
 - (2) direct exchange/streaming/messaging/event-based/algorithm visiting etc.

4



Vendor agnostic, can be solution specific

- We support healthy competition in the market among vendors providing various services to data sharing initiatives and users

5



Future-proof but not "unattainably futuristic"

- We aim to reduce unattainable futurism in the proposed recommendations (in Dutch "toekomstmuziek")
- Supporting EU regulation roadmap & EC developments (i.e. pointing in the same direction; e.g., Simpl, eIDAS, FAIR, EHDS, etc.)

6



Real-life proof

- In line with international standardization
- Backed by adoption
- Executable for different end-user groups (in Dutch "achterban"), including for example SMEs

7

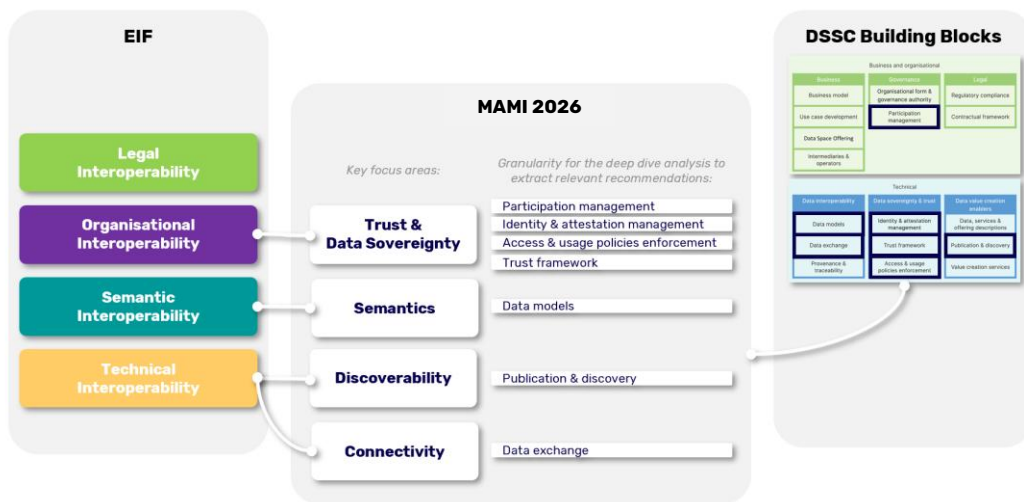


Built on consensus

- Recommendations need to be backed by consensus between data sharing experts, by management and architects of data sharing initiatives, and supported by vendors and policy makers

MAMI recommendations focus on core interoperability topics, and can be plotted simultaneously on EIF and DSSC frameworks

MAMI recommendations can be plotted on the EIF and the DSSC framework simultaneously



We scoped MAMI to encompass core interoperability topics

We give high level recommendations first, followed by the specific recommendations arranged across focus areas in line with the EIF¹ (European Interoperability Framework) and DSSC (Data Spaces Support Center) Blueprint² v2.0.

We structure the order of our focus areas according to EIF, and to detail recommendations inside each focus area we have done the deep-dive analysis using DSSC building blocks that are related to the chosen areas.

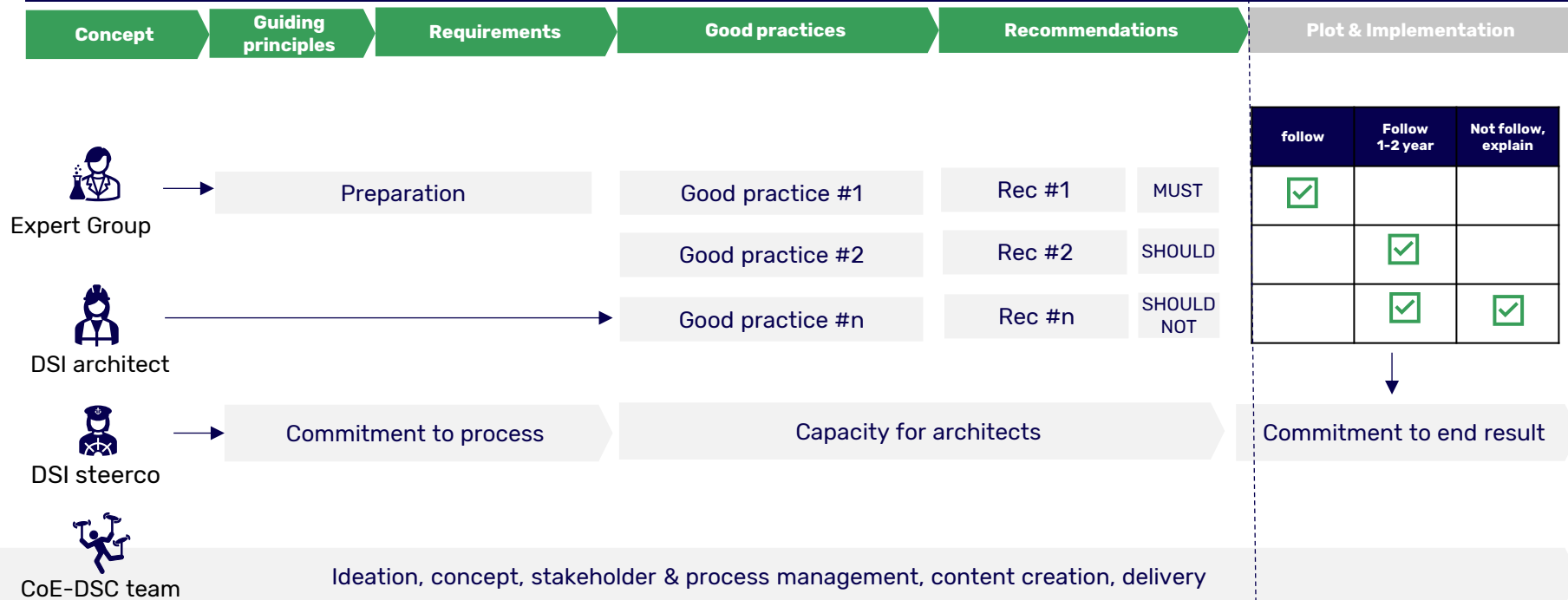
Notably, in our scoping, for MAMI 1.0 we have omitted legal, and business areas, since these are usually arranged on the level of individual use-cases/transactions between end-users of a data sharing initiative. From the governance side we pack topics around participation management into the trust and data sovereignty area. The rest of the governance decisions around organisational form and authorities are typically rather specific and differ per use case for establishing cross-domain interoperability and, thus, are not addressed in this version .

1. <https://ec.europa.eu/isa2/eifen/>

2. <https://dssc.eu/space/BVE2/1071252426/Building+Block+Overview>

We used a structured co-creation approach with experts, DSI architects and steering committee to come to 1st version of MAMI

Co-creation process to arrive at MAMI framework



Glossary

Non-exhaustive

Overview of key terminology* used in report

Terminology used	Definition	Source
Cross-domain Interoperability	The extent to which participants of different data spaces across domains, (including cross-sector & cross-border) are able to share data and discover each other's services, data sources, participants	CoE-DSC, based on DSSC Blueprint
Data Space	A data space is an infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. A data space should be generic enough to support the implementation of multiple use cases.	DSSC
 Data Sharing Initiative (DSI)	Is the sum of all its participants utilising a common infrastructure for trustworthy data sharing, based on commonly agreed principles	CoE-DSC
Maturity	Status of the data space/data sharing initiative's developmental progression (rf. IDSA Maturity stages, also rf. DSSC maturity model)	IDSA/DSSC
Service provider (SP)	A data space service provider – hereafter referred to as 'SP' – is an organisation that provides services to help define, manage and/or operationalise a data space, typically governed by a service agreement.	CoE-DSC
Trust Anchor	A specific kind of service provider that is a root, verifiable source of trust that all participants rely on to establish secure and trustworthy interactions	CoE-DSC

*Please note, for other general Data Spaces terms MAMI Framework referred to [DSSC Glossary](#)

Glossary

Non-exhaustive

Overview of abbreviations used in MAMI



General:

- AI – Artificial Intelligence
- DSIC – Data Spaces Interoperability Compass
- DSIs – Data Sharing Initiatives
- EC – European Commission
- EU – European Union
- FoFs – Federation-of-federations
- LE – Legal Entity
- MVP – Minimal Viable Product
- SMART – specific, measurable, achievable, relevant, time bound goals
- SPs – Service Providers
- PoC – Proof of concept

Related to regulations:

Acts:

- AIA – Artificial Intelligence Act
- DA – Data Act
- DGA – Data Governance Act
- DMA – Data Markets Act
- DSA – Data Services Act
- IEA – Interoperable Europe Act

Directives:

- AMLD/CFT – Anti-money laundering & counter terrorism financing directives
- ODD – Open Data Directive
- PSD3 – Payment Services Directive 3

Regulations:

- eIDAS – electronic Identification, Authentication and Trust Services Regulation
- eFTI – electronic Freight Transport Information regulation
- EHDS – Regulation to establish European Health Data Space
- ESPR – Eco-design for Sustainable Products Regulation
- EUDI – European Digital Identity Regulation
- FIDA – Framework for Financial Data Access

Regulation

- GDPR – General Data Protection Regulation
- PSR – Payment Services Regulation

Dutch regulations:

- GUE – Gegevens Uitwisselings Entiteit
- EPD – Elektronisch patiëntendossier wet
- WGBO – Wet op de geneeskundige behandelingsovereenkomst
- IBDS – Interbestuurlijke Datastrategie

Related to EU level initiatives/bodies:

- BDVA – Big Data Value Association
- CEDS – Common European Data Spaces
- DSBA – Data Spaces Business Alliance
- DSSC – Data Spaces Support Centre
- EIF – European Interoperability Framework
- FIWARE Foundation
- IDSA – International Data Spaces Association
- OpenDEI – EU Project on “Aligning Reference Architectures, Open Platforms and Large Scale Pilots in Digitising European Industry”
- SIMPL – open source, smart and secure middleware platform

Related to Dutch Data Sharing Landscape:

- BDI – Basis Data Infrastructuur
- CoE-DSC – Centre of Excellence for Data Sharing & Cloud
- DIL – Digitale Infrastructuur Logistiek
- DITM – Digital Infrastructure for Futureproof Mobility
- DMI – Dutch Metropolitan Innovations ecosystem
- DSGO – Digitaalstelsel Gebouw Omgeving
- FDS – Federatief Datastelsel
- FSC – Federatieve Service Connectiviteit
- MFFBAS – Marktfaciliteringsforum (MFF) en het Beheerder Afsprakenstelsel (BAS)
- NLAIC – NL AI Coalition

- PDOK – platform voor hoogwaardige geodata
- TIP – Trusted Information Partners
- TNO – Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek

Related to Trust:

Digital identity related (general concepts)

- DI – Digital Identity
- IAA – Identification, Authentication, Authorisation processes
- LOA – Levels of Assurance

Digital identity related (services)

- 365MS – 365 Microsoft Services
- AWS – Amazon Web Services
- eH – eHerkenning
- EUDIW – European Digital Identity Wallet
- IdP – Identity Provider
- JWT – JSON Web Token
- OAuth – Open Authorisation
- PKI – Public Key Infrastructure
- QEAA – Qualified Electronic Attestations
- QEA – Qualified Electronic Archiving
- QELedger – Qualified Electronic Ledger
- QERDS – Qualified Electronic Registered Delivery Service
- QESeal – Qualified Electronic Seal
- QESig – Qualified Electronic Signature
- QETimestamp – Qualified Electronic Timestamp
- QTSP – Qualified Trusted Service Provider (under eIDAS 2.0)
- QWAC – Qualified Website Authentication Certificate
- SSO – Single Sign On
- UZI – Unieke Zorgverlener Identificatie

Privacy related

- PETs – Privacy Enhancing Technologies
- F(M)L – Federated (Machine) Learning
- HE – Homomorphic Encryption
- MPC – Multiparty computation
- SS – Secret Sharing
- API – Application Programming Interface
- LDAP – Lightweight Directory Access Protocol
- ODRL – Open Digital Rights Language
- PAP – Policy Administration Point
- PDP – Policy Decision Point
- PEP – Policy Enforcement Point
- PIP – Policy Information Point
- SAML – Security Assertion Markup Language

Traceability related

- REGO – Renewable Energy Guarantees of Origin
- DPPs – Digital Product Passports

Related to Discoverability:

- CKAN – Comprehensive Knowledge Archive Network
- DCAT – Data Catalogue Vocabulary
- DMS – Document Management System
- DOI – Digital Object Identifier
- GraphQL – Graph Query Language
- ISO standards – International Standards Organisation
- iXBRL – Inline Extensible Business Reporting Language
- LDES – Linked Data Event Stream
- LLM – Large Language Models
- OGC standards – Open Geospatial Consortium
- XAML – Extensible Application Markup Language
- XBRL – Extensible Business Reporting Language

All recommendations were structured according to a logical syntax

Category of recommendations			
Tag for easier navigation	Human readable/actionable	Machine readable/actionable	Trust anchors
	R-HRA-0	R-MRA-0	R-TC-0
	To enhance interoperability, DSIs MUST provide explicit human readable(1) and actionable (2) descriptions regarding their scheme agreements, participants, data, and services.	To enhance interoperability, DSIs SHOULD provide explicit machine readable (1) and actionable (2) descriptions regarding their scheme agreements, participants, data, and services	To enhance interoperability, DSI's MUST specify the Trust Anchors (1) with regards to key provisions within their schemes (2)
	1. Human readable means that the information provided MUST be made accessible for a human (i.e. clear readable text*) *Note: To ensure broader accessibility to individuals with disabilities, DSIs COULD consult EU Accessibility Act to improve their webpages. (In certain cases, websites are subjected to EU Accessibility Act, please consult footnotes to determine if that is the case in the context of your DSI).	1. Machine readable means that the information provided MUST be accessible for a machine/algorithm: - Human-readable digital medium that is marked up* so that it can also be read by machines (e.g. microformats, RDFa, HTML) - Data file formats intended principally for processing by machines (e.g., CSV, RDF, XML, JSON).	1. Trust anchors MUST be accepted by a DSI in relation to a specific scope of attestation. As defined in line with DSSC Glossary, Trust anchors are - "bodies, parties, i.e., Conformity Assessment Bodies or technical means accredited by the data space governance authority to be parties eligible to issue attestations about specific claims."
	2. Human actionable means that the information provided MUST be current, unambiguous and includes instructions that a trained specialist is able to follow & fulfil.	2. Machine actionable means that the information provided MUST include instructions/code that a properly programmed machine/server/algorithm is able to read and execute: - To be machine actionable a content needs an executable code that can handle basic commands, known as CRUD operations: POST, GET, PUT, PATCH, DELETE - Usage of standardized protocols that have significant real-world adoption relevant to the DSI sectoral context is highly encouraged. Chosen protocols by a DSI MUST be explicitly indicated, to ensure parties are able to interact within a DSI. - Usage of APIs (Application Programming Interface) is highly encouraged to allow servers/ software systems to interact with each other. (e.g., RESTful APIs)	2. DSIs MUST specify for the provisions within their schemes which Trust Anchors are used respectively - In their own scheme management (e.g., for publication & updating the scheme, for incident & dispute management) - For participation related provisions (e.g., issuance of identities, credentials, certificates, mandates etc.) - For data related provisions (e.g., specifications on data quality, data usability, provenance, etc.) - For service-related provisions (e.g., security of the exchange protocols, applications, services etc.)
	Any additions, with examples of good practices		
	E.g., lists with protocols/standards commonly recognised in various sectors/ contexts		

For creating MAMI recommendations, we relied on a broad set of published materials as background for our thinking

List of recourses & materials

Organisation/Institution	Recourses/materials used	Link(s)
European Commission	CEDs: Information on Common European Data Spaces	Common European data spaces Shaping Europe's digital future European Health Data Space Regulation (EHDS) - Public Health The New European Interoperability Framework ISA²
	EIF: European Interoperability Framework	EU's Digital Product Passport: Advancing transparency and sustainability data.europa.eu
	DPPs: Information on Digital Product Passports	eIDAS Dashboard
	EUDI (eIDAS) regulation: Information on EU Digital Identity	Data Spaces Blueprint v2.0 - Home - Blueprint - Data Spaces Support Centre
DSSC	DSSC Blueprint 2.0	DSSC Maturity Model.pdf
DSSC	DSSC Maturity Model	Home Simpl Programme
SIMPL	Information about SIMPL (Labs, Open, Live)	Introduction IDSA Rulebook IDS Knowledge Base
IDSA	IDSA Rulebook	README IDS-RAM 4 IDS Knowledge Base
IDSA	IDSA Assets (incl. RAM4.0)	Trust Framework architecture - Gaia-X Architecture Document - 25.05 Release
Gaia-X	Gaia-X Trust Framework	FAIR Principles - GO FAIR
GoFAIR Foundation	Information on FAIR principles	iSHARE Trust Framework
iShare	iShare Trust Framework	Data on the Web Best Practices
W3C	W3C Recommendation - Data on the Web Best Practices	BOMOS aanvullende modules: Stelsels Logius Wat is BOMOS?
Logius	BOMOS	EU Datatienetwerk: Position paper 'Sturen op Datawaarde' - Realisatie IBDS
IBDS	Position Paper: EU Datatienetwerk 'Sturen op Datawaarde'	Inventarisatie Architectuur Data Ecosystemen t.b.v. CDO IenW
Geonovum	Report: Inventarisatie Architectuur Data Ecosystemen	Advies Digitale Infrastructuur Logistiek (DIL) Adviescollege ICT-toetsing
ICT-toetsing	ICT Auditing Report - Digitale Infrastructuur Logistiek	data-sharing-canvas.pdf
CoE-DSC materials	Data Sharing Canvas	DSIC-Living-Document-2024-initial-public-first-version.pdf
	DSIC (Data Spaces Interoperability Compass)	Trust Frameworks - Centre of Excellence for Data Sharing & Cloud
	Trust Frameworks research	CoE-DSC-Towards-Scalable-Data-Space-Interoperability-and-Federation.pdf
	Discussion Paper: Towards Scalable Data Space Interoperability and Federation	CoE-DSC-eIDAS-impact-on-data-spaces.pdf
	eIDAS whitepaper	CoE-DSC-Whitepaper-PETs.pdf
	PETs whitepaper	

MAMI Recommendations Footnotes – additional material

Recommendations Footnote related to Data/datasets management - Trust Anchors

<i>Organisation</i>	<i>Focus</i>	<i>Standards</i>
W3C (World Wide Web Consortium)	Develops web standards, including those for semantic web technologies.	RDF, OWL, SKOS
ISO (International Organization for Standardization)	Develops international standards in various fields, including data and metadata.	ISO 19115 (Geographic Information Metadata)
NISO (National Information Standards Organization)	Focuses on standards for information services, libraries, and related sectors.	NISO Z39.87 (Data Dictionary for Libraries)
DCMI (Dublin Core Metadata Initiative)	Focuses on the development of simple yet effective metadata solutions.	Dublin Core Metadata Terms
IEEE (Institute of Electrical and Electronics Engineers)	Develops standards for a broad range of technologies including metadata.	IEEE 1484.12.x (Learning Object Metadata)
OASIS (Organization for the Advancement of Structured Information Standards)	Focuses on data and metadata standards for e-business and web services.	OASIS Context Server Business Standards



Interested to learn more or to get involved,
Reach out to us at info@coe-dsc.nl