# Participant onboarding

## What is it.

Data space onboarding includes the administrative, technological, and governance processes that an entity undergoes when joining the data space.

The entity must provide the necessary registration information for the data space governance body to evaluate its application and, depending on the outcome of the evaluation, trigger the certification mechanisms that make the entity a registered, findable, and trustable participant of the data space.

Participating entities can request further attestations from data providers or data intermediaries, so that they can consume/deliver services requiring a further level of trust or certification.

## Detailed overview

### Graphical representation

A diagram of a company

Description automatically generated

### Actors

|  |  |  |
| --- | --- | --- |
| Actor | Description | Notes |
| Requestor | The legal entity that wants to join the EMDS data space and qualify as Participant |  |
| Data space authorit(ies) | A Data Space (Governance) Authority develops and maintains the  governance framework, where the rules to be part of the data space are defined. If EMDS regroups existing, or local, data spaces, their respective Authorities define the governances within their local domains | The DS Authority Trust Anchor might release credentials or delegate the release to a third party Trust Anchor. |
| Participant | Stakeholder in the EMDS data space; every Participant is assigned a unique identity by the Data Space Governance Authority ~~EMDS authority~~. | Participants can assume different roles (e.g., consumer, producer, intermediary, etc.) |
| Trust anchor(s) | Trust Anchors, which can be either the direct controller of the Trusted Data Source or a Notary, are entities that have been approved by a recognised authority like Gaia-X. | Often notary services are also trust anchors. |

### Customer journey: Registration

|  |  |  |  |
| --- | --- | --- | --- |
| Sub-customer journeys | Description | Examples of ISO 25010 Qualities | Review/tests |
| Gather information (on EMDS and onboarding) | Requestors are anyone/any entity can find out the offering of the data space, and how the onboarding process works, on the EMDS portal / interactive forum. | 1. Functional suitability [completeness]: The EMDS project provides an online resource center, covering onboarding information and data space governance. 2. Maintainability [reusability]: e.g., The EMDS online resource center records the questions and answers to create new FAQs. 3. Maintainability [Modularity]: The EMDS online resource center supports multi-lingual forums and FAQs covering as many EU languages as possible and without disclosing users’ data. | **1: Assessment: The system provides the means to build an online resource centre and its onboarding documentation.**  2: Test: If the FAQ recording feature is available, rank it by amount of administrative workload and information organization.  3: Assessment: amount of work to implement an automated translation feature that has its model trained and running in the EU. |
| Sign-Up | Requestors can create an account to gain access to community resources (e.g., interactive forums) and, optionally, engage in a participant application (Evaluation). | 1. Security: e.g., The sign-up process implements user verification measures. 2. Compatibility [Co-existence] Users of national mobility data spaces are federated in the community user base. | 1: Assessment: evaluate online validation features and, if any, the integration with external services that filter automated bots.  2: Assessment or test: If an IAM + IDP are present, test federation via a common protocol, like OAUTH. |
| Create a profile (and participate to forums) | Requestors describe themselves so they can better engage in discussions with the EMDS community of data space participants and experts. | 1. Security [Accountability]: The EMDS resource center protects users and forum systems from online abuse. 2. Security [integrity] Requestors’ profiles are accessible only for resource center working, for any other reason the consent of the Requestor is required. 3. Functional suitability [appropriateness] Profiles contain personal information that is strictly useful for EMDS functioning, and nothing more. | **1, 2,3: Assessment: This should be part of a general ISO 2700x assessment. The specific item follows subsets of ISO 27701 controls.** |
| Fed. Access via (regional) intermediary | An existing data initiative chooses to provide its users automatic registration to EMDS portal | 1. Interoperability: The system provides technical mechanisms to integrate industry standard IAMs to federate EMDS user profiles? | **1: Assessment and test: federate identities of a mock IDP via Oauth if this is supported.** |

### Customer journey: Evaluation

|  |  |  |  |
| --- | --- | --- | --- |
| Sub-customer journeys | Description | Examples of ISO 25010 Qualities | Review/Tests |
| Self-assessment | Requestors provide information on the nature and role of their participation (e.g., data provider), and submit the results of the evaluation framework results. The portal informs them on the completeness of their application. | 1. A self-assessment process exists with well-defined inputs and outputs standardised information that will be a relevant part of the profile of the aspiring participant. 2. Reliability [recoverability] can a self-assessment be interrupted or put on hold and restart from the breaking point? | **1: Assessment: if an onboarding online facility is provided, evaluate the level of customisation required to input participants’ metadata.**  2: Smoke test: test session interruption and recovery. |
| Proof of identity | Aspiring participants must prove their real-world identity, either as natural or legal entities. | 1. Security [authenticity] The system provides trustable proof of identity. 2. Performance [scalability] Does the mechanism support organizational and individual identities that operate under the same attestation context? | **1: Assessment: assess how the data space could validate requestors’ real-world identities from national identity providers.**  **2: Assessment: verify that the identity provider supports the notion of organization, and test that it can be used programmatically.** |
| Run and pass evaluation framework tests | Aspiring participants run standardised tests to ensure their technical and security maturity are adequate to integrate and use the EMDS connector. | 1. Functional suitability [completeness] A set of technical and compliance tests help requestors with the technical integration of their environment with EMDS. 2. Compatibility [interoperability] The evaluation framework’s tests are generic enough to be run on most IT environments. 3. Maintainability [reusability] The evaluation framework is always available to reassess participant’s IT compatibility with EMDS components. 4. Security [confidentiality] The tests don’t disclose participants’ critical data or configurations. | 1,2,3,4: Not testable because part of the deployment phase. |
| Assurance level evaluation | In a more nuanced variation of the above sub-journey, aspiring participants provide proof of the security and maturity levels that are needed for the role they intend to play. | 1. Dependent on data space standard. Current EMDS’ requirements do not foresee an autochthonous (i.e., data space driven) assurance level. | Assessment: verify that the stack is supported by a compliance verification framework, like IDSA certification. Rank the advantages that such certification cand de  liver to EMDS. |

### Customer journey: Certification

|  |  |  |  |
| --- | --- | --- | --- |
| Sub-customer journeys | Description | Examples of ISO 25010 Qualities | Review/Tests |
| Identity and credentials issuance | The newly assessed data space participant will receive data-space wide credentials that she can use to prove her identity. These credentials are recognised by all EMDS participants. The credentials will be interoperable with EU initiatives. | 1. Functional suitability [completeness]. The credential framework supports attestations and (multiple?) trust anchors. 2. Functional suitability [completeness] The credential framework supports EMDS-required LoAs[[1]](#footnote-2) 3. Compatibility [co-existence and interop]: The issuance service supports legacy schemes AND/OR supports recommended frameworks like eIDAS or GAIA-X Identity Framework. 4. Maintainability [modifiability] The credential issuance stack will require modifications to abide to changing EU’s claims standards without affecting the data sharing components? 5. Security [integrity] The credential issuance/verification services implements integrity controls manage the issuance and renewal/revoking of credentials and certificates. | **1: Test: prove that the stack uses a credential framework that is compatible with any of these inititatives: Gaia-X, eIDAS, EBSI.**  2: Test and Document which LoAs level is supported by the framework.  3: Test: create a mock GAIA-X self-descriptor and test that the issuer service can issue it. Nice to have: issue and validate on GAIA-X compliance framework.  Test or assess that the issuance service can integrate OpenID for VC or SIOP flows.  4: To be defined when SIMPL will deliver a reference design.  **5: Assessment / test: Prove that a full credential lifecycle is supported: request, issuance, validation, renewal, revocation.**  1: Assessment: This should be part of a general ISO 2700x assessment. |
| Certificates issuance | Depending on their role in the data space, participants are issued one or multiple certificates to operate securely. | 1. Security [integrity] Certificates and cryptographic material are managed securely. |
| Comply with domain trust anchors | Participants apply for issuance of attestations that they comply with additional governance | 1. Security [confidentiality] The credentials framework has mechanisms to protect confidential data and attestations from data leaks (principle of selective disclosure or only need to know) 2. Security [integrity] The IAM and credential frameworks have mechanisms to guarantee attestations cannot be tampered. 3. Security [non-repudiation] The framework has mechanisms to prove that a trust anchor issued an attestation. | 1,2,3: Assessment: This should be part of a general ISO 2700x assessment.  NIST 800-53 controls represent a valid alternative to ISO assessment. |

### Customer journey: Profile management

|  |  |  |  |
| --- | --- | --- | --- |
| Sub-customer journeys | Description | Examples of ISO 25010 Qualities |  |
| Manage profile on data space directory | New participants can improve their visibility on the data space directory by adding/modifying their profiles. | Skipped development |  |

1. Level of Assurance, as defined in eIDAS : <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS+Levels+of+Assurance> [↑](#footnote-ref-2)