DATASPACE 4HEALTH LUXEMBOURG

POC Demonstration Report: Interconnect Data Provider and Data User

Document ID: DS4H_WP5_D5.5

Hee Kim and Maximilian Fünfgeld

Luxembourg Institute of Health (LIH)

Date: 06/02/2026

Funding

This project has received funding from the Ministry of the Economy of Grand Duchy of Luxembourg under Grant agreement no 20230505RDI170010392869.

Disclaimer

The documents published by the consortium are intended solely for informational purposes and reflect the views and opinions of the consortium members at the time of publication and within the scope of the Dataspace4Health project (DS4H).

The ideas expressed herein do not necessarily reflect the official policy or position of the funding entity.

Efforts have been made to achieve the relevance of the content; however, the consortium does not make any representation regarding its completeness and accuracy.

This document may be subject to further revision.

This document is intended to be published on the Dataspace4Health website.

Table of Versions

Version n°	Issue Date	Reason for change
0.0	21/01/2025	First draft.
0.1	29/01/2025	The project context is provided in Section 1, while Section 3 is enriched with the details. This version has been internally validated.
1.0	30/01/2025	Final version has been sent to the coordinator.

TABLE OF CONTENTS

Glossary

Abbreviation	Expression
DS4H	Dataspace4Health
POC	Proof of Concept
WP5	Work Package 5
IAM	Identity and Access Management
VC	Verifiable Credential
VP	Verifiable Presentation
OIDC	OpenID Connect
OIDC4CI	OpenID for Verifiable Credential Issuance
OIDC4VP	OpenID for Verifiable Presentations
RBAC	Role-Based Access Control
LD Proof	Linked Data Proof
JSON-LD	JavaScript Object Notation for Linked Data
DUA	Data Usage Agreement
SPE	Secure Processing Environment
HSM	Hardware Security Module
IRB	Institutional Review Board
GDPR	General Data Protection Regulation

1. INTRODUCTION

The Dataspace4Health (DS4H) project aims to establish a sovereign health data space in Luxembourg for two use cases: diabetes and oncology use cases. This document, conducted under the second use case, is a validation report for the technical feasibility of interconnecting a Data Provider and a Data User through the Proof of Concept (POC) data space infrastructure. The demonstration has been conducted through two separate handover workshops held on October 21st, 2025 and January 20th, 2026.

To validate the technical feasibility, a single synthetic patient record of colorectal cancer was used as a Data Offering. This record was structured based on the OncoBox data model to ensure that the data format is the same as that of real-world patient data. For detailed information regarding the data structure and the harmonized variables, please refer to the document [1].

Note that the scope of this POC is limited to a technical feasibility demonstration. It operates under the assumption that no real patient records or live production systems are involved, and performance or scalability aspects are out of scope. Furthermore, as of this writing, the POC system is not yet available at HRS. This meant that there were many assumptions in the demonstration scenario. For instance, the LIH admin role was performed by NTT, and the HRS role was performed by LIH. Once the system is live at both HRS and LIH, HRS will publish its metadata to the catalogue, and LIH will identify the data of interest in the catalogue and download the service offering VP.

2. TECHNICAL BASELINE

The tested infrastructure is aligned with the Gaia-X Tagus (v22.10) [3, 5] ontology, which provides the technical compliance, data sovereignty, and interoperability standards for the ecosystem. Based on the Tagus Ontology, the tested infrastructure is built on top of the following technical components:

- **Keycloak-based Identity and Access Management (IAM)** is used in DS4H.
- User identity and access management are distributed across two-layered IAM systems.
    - **Legal participant IAM** is responsible for identity by managing (create, update, and remove) user accounts for natural person affiliated with the legal entity.
    - **Federator IAM** centrally manages role assignment in the **Federated Catalogue**. Roles are not self-assigned, but are granted.
- **Federated Catalogue** is a metadata registry for publishing and discovering datasets/services without storing actual data.
- To interact with these services, users are required to use a **Verifiable Presentation (VP)** [9]. A VP is a bundle of multiple **Verifiable Credential (VC)** [2, 6, 7], which is a digital attestation. All components in the dataspace exchange data in the form of VPs.
- **Wallet** is a digital container for holding and presenting **VC** to prove identity/affiliation/roles in DS4H services (e.g., the Federated Catalogue).

3. DEMONSTRATION SCENARIO AND RESULTS

The demonstration executed during handover workshops aims to validate the workflow of interconnecting Data Provider and Data User. Table 1 is the list of steps executed during the workshop. All steps were carried out successfully, with all technical components performing as expected. Note that it is assumed that the participating legal entity has completed the onboarding process before the demonstration.

Table 1. The steps for the handover workshops listed in chronological order.

#	Step	Test Date	Result
1	Create a User for Legal Participant (Section 3.1)	21/10/2025	Pass
2	VC Issuance for Natural Person (Section 3.2)	21/10/2025	Pass
3	Mobile Wallet Integration (Section 3.3)	21/10/2025	Pass
4	Cryptographic Signature (Section 3.4)	20/01/2026	Pass
5	Publish Data Offering (Section 3.5)	20/01/2026	Pass

3.1. CREATE A USER FOR LEGAL PARTICIPANT

This stage involved creating user account for individuals affiliated with the Legal Participant.

- **Subject:** Legal Participant Admin (NTT acted on behalf of the LIH admin)
- **Service:** https://lih.dataspace4health.lu/iam
- **Execution:**
  - The admin logged in to the LIH IAM system.
  - The admin determined the user type: “ds4h” realm for regular users and “master” realm for admin users.
  - The admin created user accounts via “Users - Add user”.
  - Mandatory fields were filled.
  - A temporary password was set in the “Credentials tab”, allowing change at first login.
- **Outcome:** Two regular users (Hee Kim and Mary Roszel) were created.

3.2. VERIFIABLE CREDENTIAL (VC) ISSUANCE FOR NATURAL PERSON

This stage covered issuing digital identity credentials to individual users.

- **Subject:** Legal Participant Admin (NTT acted on behalf of the LIH admin)
- **Service:** https://lih.dataspace4health.lu/iam/admin/ds4h/console
- **Execution:**
  - The admin logged in to the LIH admin console.
  - The Keycloak dashboard was opened via “Manage account”.
  - Under “Verifiable credentials”, “Natural Person VC” was selected.
  - The admin issued the credential via “Initiate Credential-Issuance (OIDC4CI)”.
- **Outcome:** A digital attestation was generated and displayed in a QR code via the OIDC4CI [4, 8] protocol.

3.3. MOBILE WALLET INTEGRATION

This step involved users storing their credentials (Natural Person VC) in their mobile wallet.

- **Subject:** Individual user (Hee Kim and Mary Roszel)
- **Service:** https://lih.dataspace4health.lu/wallet/ui
- **Execution:**
  - The user opened the Wallet service on their smart device.

  - The user signed in via “Connect with OIDC”.
  - The user credentials were entered.
  - The wallet dashboard was opened.
  - The user scanned the generated QR code via “Scan to receive or present credential”.
- **Outcome:** The Natural Person VC was successfully transferred and stored in the mobile wallet.

3.4. CRYPTOGRAPHIC SIGNATURE (MANUAL)

The Data Provider cryptographically signed the VP. The VP is a bundle of four VCs: Legal Participant, Terms and Conditions, Service Offering, and Legal Registration.

- **Subject:** Individual user (NTT acted on behalf of Hee Kim)
- **Service:** Offline executable (.exe) tool
- **Execution:**
  - Four VCs were prepared in advance.
    - Three VCs (Legal Participant, Terms and Conditions, Service Offering) were self-signed by LIH.
    - One VC (Legal Registration) was signed by the Gaia-X Registry.
  - The VP was signed using a dedicated offline executable tool.
- **Outcome:** A manually signed VP was created

3.5. PUBLISH DATA OFFERING

The signed VP was registered in the Federated Catalogue. The prerequisite of the VP publication, the federator administrator must grant publishing permission to the user. Note that the default permissions is limited to read permission (data discovery) only.

- **Subject:** Individual user (Hee Kim)
- **Service:** https://portal.dataspace4health.lu/catalogue/ui
- **Execution:**
  - The user logged in via “Login with SSI” by presenting the VC stored in their wallet.
  - After successful authentication, the catalogue was accessed.
  - The user submitted the Service Offering VP for the OncoBox colorectal cancer data [1].
- **Outcome:** The service offering became discoverable in the Federated Catalogue.

4. NEXT STEPS

This workshop did not cover the process of signing a Data Sharing Agreement (DSA), which must be initiated by Data User. To proceed with a DSA, Data User needs to download the service offering VP in Federated Catalogue, which serves as the basis for the DSA. Data User then needs to sign the VP using their organization’s cryptographic material, package it into a new VP, and uploads it back to the catalogue for verification. Once validated by the Federator, Data User receives a VP containing three signatures (Data Provider, Data User, and Federator) and stores the signed Service Offering in their Wallet for future use.

Beyond this POC, several critical actions are required for a production-ready environment. Production systems will need to replace temporary workarounds, particularly for the manual signature step. This involves incorporating signing functionalities directly into the web portal GUI to improve user experience.

It should also integrate interfacing with a Secure Processing Environment (SPE) to facilitate the transition from synthetic to real healthcare data access.

Finally, system must undergo validation for scalability and the security features, such as a real-time user revocation. It must also account for complex institutional IT policies, such as firewalls and network isolation, which were not present in this feasibility study.

5. CONCLUSION

This POC successfully proves the feasibility of basic technical interconnection between a Data Provider and a Data User. Dataspace concepts such as controlled access and data catalogue were validated at a conceptual level. This demonstration supports further development toward more advanced and production-ready dataspace implementations.

REFERENCES

1. DS4H, "Interoperable Harmonized Data Model for Colorectal and Lung Cancers," Project Document, ID: DS4H_WP5_D5.2, 2025.
2. W3C, "Verifiable Credentials Data Model v1.1," W3C Recommendation, 2022.
3. Gaia-X, "Gaia-X Architecture Document (Tagus Release v22.10)," Gaia-X Framework, 2022.
4. OpenID Foundation, "OpenID for Verifiable Credential Issuance (OIDC4CI)," Technical Specification, 2023.
5. Gaia-X, "Gaia-X Tagus ontology v22.10," Ontology Specification, 2022.
6. W3C, "Verifiable Credential Data Model v1.1," Data Model Standard, 2022.
7. JSON-LD, "JSON-LD Verifiable Credential with LD Proof," Technical Specification, 2023.
8. OpenID Foundation, "OpenID for Verifiable Credential Issuance - Draft 13," Protocol Specification, 2023.
9. OpenID Foundation, "OpenID for Verifiable Presentations - Draft 22," Protocol Specification, 2023.