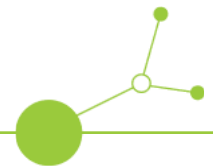




D.2.3.5: Development of GAIA-X Use Case



INFORDATA with other Interreg CE ReBuilt
partners

Version 1.0

May 2026





INTERREG CENTRAL EUROPE 2021-2027

CE0100390 - ReBuilt

Work Package	WP2 - Developing and testing innovative solutions for circular and digital construction
Activity	Activity 2.3 - Tool for digitalisation of circular value chains with material passports and digital market for circular construction
Deliverable Number	D.2.3.5
Version	1.0
Lead Partner	INFORDATA (PP5) - Italy
Contributing Partners	IIC (PP11), CZGBC(PP13), Opencontent (PP4)
Reporting Period	Period 7
Delivery Date	26.05.2026
Status	Final
Dissemination Level	Public

This document has been produced in the context of the Interreg Central Europe Programme, co-funded by the European Regional Development Fund (ERDF).



Table of Content

Contents

1. INTRODUCTION	5
2. BASIC INFORMATION ABOUT THE DIGITAL SOLUTION	6
2.1. Objectives:	6
2.2. Core components:	6
3. USE CASE SCENARIO	7
4. SYSTEM ARCHITECTURE	8
4.1 Overview	8
4.2 DID Document and Identity Layer	8
4.3 Participant Credential and Clearing House Layer	8
4.4 Digital Product Passport Signing Architecture	9
4.5 Federated Data Sharing Endpoints	9
4.6 Key Management and Certificate Infrastructure	10
5. INTEGRATION WITH EXTERNAL SYSTEMS (BIM, GAIA-X, CINDEROSS, MARKETPLACES)	11
5.1 Integration with BIM (Building Information Modelling)	11
5.2 Gaia-X Federated Infrastructure Integration	11
5.2.1 Identity and Trust Infrastructure	11
5.2.2 Data Federation and Sharing	13
5.2.3 Operational Implementation	13
5.2.4 Gaia-X Compliance Achievement	15
5.2.5 JSON-LD Product Passport Signing	17
5.2.6 Compliance and Interoperability Considerations	22
5.3 Integration with CinderOSS Platform	23
6. DATABASE SCHEMA DESCRIPTION	24
7. CHALLENGES AND LESSONS LEARNED	25
7.1 Technical Implementation Challenges	25
7.2 Operational and Organisational Challenges	25
7.3 Lessons Learned	26
8. CONCLUSIONS AND NEXT STEPS	26
8.1 Summary of Achievements	26
8.2 Contribution to ReBuilt Objectives	26
8.3 Next Steps and Recommendations	27



Summary

D2.3.5 delivers the Gaia-X use case for the ReBuilt project – the concrete implementation of European federated data sovereignty within a real circular construction workflow. Where D2.3.1 documented the material traceability platform, this deliverable focuses entirely on what happens when that platform joins the Gaia-X ecosystem: how construction materials receive cryptographically verifiable Digital Product Passports, how the platform establishes a trusted identity through Decentralised Identifiers, and how this creates the foundation for cross-border circular economy data exchange in Central Europe. The use case is live, validated at the NIGRAD demonstration site in Slovenia, and fully aligned with the W3C Verifiable Credentials standard, the UN/CEFACT DPP 0.6.0 vocabulary, and the Gaia-X Trust Framework.



1. Introduction

D2.3.5 is the Gaia-X use case deliverable for the ReBuilt project. It does not repeat what D2.3.1 covered – the architecture, platform functionality, and database schema. Instead, it focuses on a single, precise question: what does it take to make a circular construction platform a trusted participant in Europe’s federated data infrastructure?

The answer required implementing three interconnected Gaia-X components: a did:web Decentralised Identifier that gives the platform a verifiable identity on the open web; a Gaia-X Participant Credential that anchors that identity within the European trust framework; and a JsonWebSignature2020-signed Digital Product Passport that makes every material record independently verifiable by any third party, anywhere in Europe, without calling back to a central authority.

This deliverable documents exactly how those three components were built, configured, and validated – including the live DID document, the signed DPP structure, and the lessons learned when connecting a real construction pilot to Gaia-X Clearing Houses.



2. Basic Information about the Digital Solution

This section provides the minimum context needed to understand the Gaia-X use case. For full platform documentation, see D2.3.1. The components below are those directly involved in the Gaia-X implementation.

2.1. Objectives:

- **Establish a verifiable digital identity** for the ReBuilt platform within Gaia-X using did:web – making the platform a recognised, trusted participant in European federated data infrastructure.
- **Issue cryptographically signed Digital Product Passports** as W3C Verifiable Credentials that any third party can verify independently, without calling back to a central authority.
- **Achieve Gaia-X Participant Credential status** through the official onboarding wizard and Clearing House validation, demonstrating compliance with the Gaia-X Trust Framework.
- **Enable cross-border material data exchange** between construction stakeholders across Central Europe, under EU data sovereignty principles.

2.2. Core components:

- **did:web Decentralised Identifier (DID):** W3C-compliant DID document published at <https://rebuilt.infordata.eu/.well-known/did.json>, establishing a cryptographically verifiable identity on the open web.
- **Gaia-X Participant Credential:** Verifiable Credential issued through the official Gaia-X onboarding wizard, anchoring the platform within the Gaia-X Trust Framework and enabling Clearing House participation.
- **JsonWebSignature2020 Signing Service:** Every Digital Product Passport is signed using the platform's RSA private key (RS256), producing a self-certifying JSON-LD Verifiable Credential verifiable against the published DID.
- **Federated Data Endpoints:** REST APIs expose signed DPP data and material metadata in formats compatible with Gaia-X Catalogue discovery and cross-border circular economy workflows.
- **Gaia-X Compliance Credential:** The platform is a confirmed Gaia-X Legal Participant. The gx:compliance credential (issued 28 July 2025, valid through 26 October 2025) was obtained by submitting signed credentials to the Gaia-X Compliance Service and validates all three identity documents against the Trust Framework v22.10.



3. Use Case Scenario

The Gaia-X use case is grounded in a specific, real workflow at the NIGRAD demonstration centre in Slovenia. A concrete block – product ID 7, "Concrete block C25/30" – recovered from a demolition site goes through the following sequence:

- **Material registration:** The block is catalogued in the ReBuilt portal with waste type, dimensions, weight, and origin location. A unique product ID is assigned.
- **DPP generation:** The portal assembles a Digital Product Passport in JSON-LD following the UN/CEFACT DPP 0.6.0 vocabulary, including product metadata, recycling events, and issuer identity.
- **Cryptographic signing:** The DPP is signed using the platform's RSA private key (RS256), producing a JsonWebSignature2020 proof block referencing `did:web:rebuilt.infordata.eu#key-1`.
- **Independent verification:** Any third party retrieves the DID document, extracts the public key, and verifies the JWS signature – no API call to the ReBuilt platform required. The passport is self-certifying.
- **Gaia-X discovery:** The signed DPP and material metadata are published through Gaia-X-compliant interfaces. Because the platform holds a valid `gx:compliance` credential, any Gaia-X Catalogue participant can discover the material and independently verify both the data integrity and the issuer's trusted status – without contacting the ReBuilt platform.



4. System Architecture

The platform architecture relevant to this deliverable is the Gaia-X trust layer – the components that sit above the core web application and give it a verifiable identity within federated European data infrastructure. The underlying platform (Yii2 / MySQL / REST API) is documented in D2.3.1. This section focuses exclusively on the Gaia-X-specific architecture.

4.1 Overview

The Gaia-X architecture layer comprises three components that together create a complete trust chain: a DID Document for identity, a Participant Credential for ecosystem membership, and a signed DPP for individual material data integrity.

4.2 DID Document and Identity Layer

The DID document is the anchor of the entire trust chain. Published at <https://rebuilt.infordata.eu/.well-known/did.json>, it is a publicly accessible JSON document that declares: "This is the ReBuilt platform, and here is its public key for verifying any credential it issues."

- **Method: did:web** – the simplest and most interoperable DID method, leveraging HTTPS for document hosting. No blockchain, no special infrastructure required.
- **Verification method: JsonWebKey2020** with RSA-2048 public key (kty: RSA, alg: RS256). The corresponding private key signs every DPP issued by the platform.
- **x5u certificate link:** Points to an eIDAS-aligned certificate at

<https://rebuilt.infordata.eu/.well-known/did-cert.pem>

providing additional trust anchoring via European digital identity infrastructure.

4.3 Participant Credential and Clearing House Layer

The Gaia-X Participant Credential (VC) declares the platform's membership in the Gaia-X ecosystem. It was created using the official Gaia-X onboarding wizard and signed by a Gaia-X-recognised notary. Any Gaia-X Clearing House can verify it, making the platform a trusted node in federated data spaces.

- **Credential format:** JSON-LD Verifiable Credential following the Gaia-X Trust Framework schema – including `legalRegistrationNumber`, `headquarterAddress`, and `gaiaXTermsAndConditions` claims.



- **Issuer:** `did:web:rebuilt.infordata.eu` – the platform’s own DID, creating a self-referential trust chain where identity and credentials share the same cryptographic anchor.
- **Clearing House validation:** Submitted to Gaia-X Clearing Houses v1 (production). A successful response confirms compliance with the Gaia-X Trust Framework.
- **Terms and Conditions:** Published at <https://rebuilt.infordata.eu/.well-known/gx-terms-and-cs.json> – the legally binding usage policies governing how shared data may be consumed by Gaia-X participants.

4.4 Digital Product Passport Signing Architecture

When a product is finalised in the ReBuilt portal, the signing service generates a W3C Verifiable Credential wrapping the material data. The signing process applies JSON-LD canonicalization (URDNA2015) to ensure the signature is deterministic and reproducible by independent verifiers.

- **Input:** Product metadata serialised as JSON-LD using the UN/CEFACT DPP 0.6.0 vocabulary, with @context referencing <https://www.w3.org/ns/credentials/v2> and the UNTP DPP namespace.
- **Signing algorithm:** `JsonWebSignature2020 / RS256`. The `proof.jws` field carries the base64url-encoded detached JWS; `proof.proofPurpose` is `assertionMethod`.
- **Verification method reference:** `did:web:rebuilt.infordata.eu#key-1` – pointing to the RSA public key in the DID document. The verification path is embedded in the credential itself; no additional lookup needed.
- **Storage:** Each signed DPP version is saved in `product_dpp_sign` with its hash, full JSON-LD, optional `blockchain_id`, and timestamps for a complete audit trail.

4.5 Federated Data Sharing Endpoints

The platform exposes material data through endpoints designed for both direct API access and Gaia-X federated discovery – the output of the signing pipeline, consumable by external systems without any special client.

- **GET /product/{id}/dpp:** Returns the full signed DPP as a JSON-LD Verifiable Credential, including the complete proof block for independent verification.
- **GET /product/{id}/dpp/download:** Downloads the DPP as a machine-readable JSON-LD file for offline verification or submission to regulatory systems.
- **GET /.well-known/did.json:** The DID document endpoint – called by verifiers resolving the platform’s identity before checking DPP signatures.



- **GET /.well-known/participant.json:** The Gaia-X Participant Credential — used by Catalogues and Clearing Houses to confirm ecosystem membership.
- **GET /.well-known/gx-terms-and-cs.json:** The Terms and Conditions document referenced in the Participant Credential.

4.6 Key Management and Certificate Infrastructure

The RSA private key used for DPP signing is stored securely on the server and never exposed through any API. Certificate and key lifecycle management ensures uninterrupted Gaia-X compliance.

- **eIDAS certificate:** The x5u certificate referenced in the DID document was obtained through the Gaia-X onboarding process, aligned with eIDAS trust service requirements for institutional trust anchoring.
- **Certificate renewal:** Expiry is monitored and renewal is integrated into the platform's operational calendar, with DID document updates triggered automatically on rotation.



5. Integration with External Systems (BIM, Gaia-X, CinderOss, Marketplaces)

This section documents the three external system integrations that form the Gaia-X use case: BIM (for interoperable material data export), Gaia-X (the primary focus of this deliverable, detailed in 5.2), and CinderOSS (the circular economy marketplace where signed DPPs are published). Together they demonstrate an end-to-end trusted data flow from physical material to European federated infrastructure.

5.1 Integration with BIM (Building Information Modelling)

The system is designed with compatibility toward **BIM environments**, allowing materials tracked and catalogued through the web platform to be referenced or embedded in architectural and engineering workflows.

IFC Data Structure Compatibility: The backend database schema is designed to export relevant metadata (e.g., material ID, classification, location, lifecycle status) into IFC-compatible formats.

This integration facilitates compliance with green procurement, construction material reuse targets, and life-cycle analysis in building projects.

5.2 Gaia-X Federated Infrastructure Integration

Gaia-X integration positions the platform within European federated data infrastructure while ensuring data sovereignty, security, and interoperability across construction industry digital ecosystems.

5.2.1 Identity and Trust Infrastructure

The platform implements a fully Gaia-X-compliant Decentralized Identifier (DID) infrastructure using the **did:web** method, enabling verifiable organizational identity and cryptographically secure interactions within federated ecosystems. The DID document published at <https://rebuilt.infordata.eu/.well-known/did.json> exposes the platform's public verification materials in accordance with W3C DID Core and Gaia-X Trust Framework requirements. Below shown DID file that used on portal

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:web:rebuilt.infordata.eu",
  "verificationMethod": [
    {
      "id": "did:web:rebuilt.infordata.eu#key-1",
      "type": "JsonWebKey2020",
      "controller": "did:web:rebuilt.infordata.eu",
      "publicKeyJwk": {
```



```
    "kty": "RSA",
    "n":
"xh2OCizU_oTypojyK7Y35cHhPoD_R0GUOeFb2HorQju_W8Mo07bgWKJfINclzC1i2LwUKi40VbNW-XTFr-
CX-ct_mvGj-9SnLQEqUkVA2oyEiC_7rfINTn4GXvx9ASRtEC0cp95CxdE7eAMN7-
6tIjPcc3kKaVuEhHZVAXHVRUQcUf7YDK6ev6waHwQ-
rrLEDzfs2QgOSOIGs3hQRt_7DnsLIY7bsZLsoO5m_GhvjaeDUgA16kLh7OJnh5DxUueuuA19S3tieVHcUIW
SO7iGj9iIYc-eqGiDzBq7LHs4U1xUnfPWUly1O3vn4hmjM5K-XZ-hDUBA7MKQNYzIiAkQ
",
    "e": "AQAB",
    "alg": "RS256",
    "kid": "did:web:rebuilt.infordata.eu#key-1",
    "x5u": "https://rebuilt.infordata.eu/.well-known/cert7.pem"
  }
],
"authentication": [
  "did:web:rebuilt.infordata.eu#key-1"
]
}
```

The DID document includes a **JsonWebKey2020** verification method that provides an RSA-based public key in JWK format. This key is referenced through the fragment identifier **#key-1** and is used for authentication, signature verification, and validation of all Gaia-X-related artifacts. The **x5u** field links to an **eIDAS-aligned** certificate, enabling additional trust anchoring through external certificate chains. Below show key fields of the DID document:

Table 1: Key fields of the DID document

Parameter	Description
id	The globally unique decentralized identifier (did:web:rebuilt.infordata.eu) representing the organization within Gaia-X federated networks.
verificationMethod	Defines cryptographic material used for signature verification. The platform uses the JsonWebKey2020 type, which is required for Gaia-X JsonWebSignature2020-based credentials
publicKeyJwk	RSA public key parameters (kty, n, e) used for verifying signatures on Verifiable Credentials and signed product passports
alg	Specifies the signing algorithm (RS256) ensuring compatibility with Gaia-X trust services
x5u	URL pointing to the certificate used during Gaia-X onboarding and compliance validation.
authentication	Declares which verification method is authorized for DID authentication operations.



Verifiable Credentials generated through official Gaia-X onboarding procedures establish trusted organizational identity that enables secure data sharing across federated networks. Credential verification processes ensure authentic participant identification while supporting automated trust establishment for cross-border collaborations. To establish trusted organizational identity within Gaia-X, Participant Verifiable Credentials were created using the official [Gaia-X onboarding wizard](#) as shown in Table 2:

Cryptographic Security implementation utilizes eIDAS-compliant key generation and JsonWebSignature2020 signing algorithms that ensure data integrity and authenticity verification for all federated data exchanges. Private key protection and certificate management procedures maintain security while enabling automated verification processes. The certificate referenced via x5u follows eIDAS trust service requirements, enabling alignment with European digital identity regulations.

5.2.2 Data Federation and Sharing

Gaia-X compliance enables secure material data sharing across European construction networks while maintaining data sovereignty and privacy requirements. Federated query capabilities allow authorized participants to discover available materials and services without exposing sensitive organizational information or compromising competitive advantages.

Metadata Standardization follows Gaia-X ontology requirements that ensure consistent data discovery and interoperability across diverse organizational systems and national jurisdictions. Material data publishing includes appropriate classification, access controls, and usage policies that protect intellectual property while enabling circular economy collaboration.

Cross-Border Compliance implementation addresses varying national regulations and data protection requirements while maintaining seamless data access for authorized participants. Legal framework documentation and terms of service agreements ensure regulatory compliance while enabling practical data sharing operations.

5.2.3 Operational Implementation

Gaia-X compliance was achieved through a structured four-stage onboarding process documented internally by INFORDATA. The process began with a review of the Gaia-X Trust Framework (v22.10) to confirm the platform's role as a Data Provider and Legal Participant. It concluded with a successful compliance submission that produced a signed gx:compliance credential from the Gaia-X Compliance Service, valid from 28 July 2025 through 26 October 2025.

The four onboarding stages were: (1) DID creation – generating an eIDAS-compatible cryptographic key pair and publishing the DID document at <https://rebuilt.infordata.eu/.well-known/did.json> using the did-web-generator tool; (2) Verifiable Credential creation – using the Gaia-X Wizard (wizard.lab.gaia-x.eu/onboarding) to generate the Participant VC, Terms and Conditions VC, and Legal Registration Number VC, all issued under the rebuilt.infordata.eu domain; (3) Compliance submission – calling the Gaia-X Compliance API (compliance.gaia-x.eu) with the signed credentials to obtain the gx:compliance credential; (4) Publishing – saving the compliance output as the platform's self-description file.



Table 2: Gaia-X DID and Verifiable Credential Configuration

Parameter	Value	Description
DID Method	did:web	Gaia-X-compliant method for decentralized identifiers
DID	did:web:rebuilt.infordata.eu	Root DID representing the platform
Verification Method	did:web:rebuilt.infordata.eu#key-1	Reference to public key fragment inside the DID document
DID Document Location	https://rebuilt.infordata.eu/.well-known/did.json	Publicly accessible DID document
Issuer	https://rebuilt.infordata.eu	Platform base URL used as issuer identifier in the VC
Verifiable Credential ID	https://rebuilt.infordata.eu/.well-known/participant.json	URL under which the VC is published
Credential Subject ID	https://rebuilt.infordata.eu/.well-known/participant.json#subject	Subject identifier embedded in the VC
Terms and Conditions URL	https://rebuilt.infordata.eu/.well-known/gx-terms-and-cs.json	JSON document defining legal terms and Gaia-X conditions
Terms and Conditions Subject ID	https://rebuilt.infordata.eu/.well-known/gx-terms-and-cs.json#subject	Identifier inside the terms document



VC Creation Method	wizard.lab.gaia-x.eu / API endpoint	Used for generating and validating VCs
Gaia-X Environment	Clearing Houses v1 (production) / Gaia-X dev	Depending on target environment: production or test

5.2.4 Gaia-X Compliance Achievement

The Gaia-X Compliance Service validated the ReBuilt platform's credentials and issued a signed `gx:compliance` Verifiable Credential on 28 July 2025, confirming the platform as a recognised Gaia-X Legal Participant. The credential covers three submitted documents: the Participant VC (`participant.json`), the Terms and Conditions VC (`gx-terms-and-cs.json`), and the Legal Registration Number VC (`lrn.json`). Compliance is valid through 26 October 2025.

Onboarding Steps Executed

- **Role identification:** Reviewed the Gaia-X Trust Framework v22.10 and confirmed the platform's role as a Data Provider and Legal Participant under the rebuilt.infordata.eu domain.
- **DID creation:** Generated an eIDAS-compatible RSA key pair using the `gaia-x/did-web-generator` tool. Published the DID document at `https://rebuilt.infordata.eu/.well-known/did.json` with a `JsonWebKey2020` verification method.
- **Verifiable Credential creation:** Used the Gaia-X Wizard (`wizard.lab.gaia-x.eu/onboarding`) with Environment set to "Clearing Houses v1 (production)" and "I'll use my own DID solution". Generated three VCs: Legal Participant, Terms and Conditions, and Legal Registration Number.
- **Compliance submission:** Submitted the signed VC bundle to the Gaia-X Compliance API (`compliance.gaia-x.eu`). Received the signed `gx:compliance` credential confirming all three documents passed integrity checks using `RFC8785:JCS` normalisation and `gx:version 22.10`.
- **Self-description publishing:** Saved the `gx:compliance` credential output as the platform's self-description file, completing the Gaia-X onboarding cycle.

Compliance Credential Output (condensed)

The following shows the structure of the `gx:compliance` Verifiable Credential returned by the Gaia-X Compliance Service, confirming the platform's compliance status:

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/security/suites/jws-2020/v1",
```



```
"https://registry.lab.gaia-x.eu/development/api/trusted-shape-
registry/v1/shapes/jsonld/trustframework#"
],
"type": [
  "VerifiableCredential"
],
"id": "https://wizard.lab.gaia-x.eu/api/credentials/2d37wbGvQzbAQ84yRouh2m2vBkN8s5AfH9Q75HZRCUQmJW7yAVSNKzjJj6gcjE2mDNDUHCichXWdMH3S2c8AaDLm3kXmf5R8DWCDUCfZxgGR5x15hJJkfQffpvp6HTfAGG2BC4b447bLVG496CpSrSZ7P4LNMKqJ9fu8KJbtoCXFpijk6LFQM8zUon1YFe71R8Y5LQK9h6gQafBC5hJiQHZ6H3yZvf7mXPau8q7E6drffW292pPB5894CVld8mviLSrRCyVoHyTvyK2GuV8hvPxLPdJLGCutjTkRvTnbib3HxBBUdpYbPVK5bfcADcQKu2ZXfi3pR7tPPUnRPWzh3JUCS1s1tboZpZjLod2xTM54XxsXEGKxZ3zBLZAS7SBxt5t3JdZPDGcEW3G77q8ZuQEY3j8re4zW3q5qDdDe94lvzRPdro3ELeS8cR2aKVyKxwSuUn7UEepqmiU8R4fDW6PSqiKeTzLF8wDPCXj5ux1j2ar7Stz14XGpDilnEpKks7zLjjYmwSw6u6wuZMqRWbvXaAue4Q3zQmc3HD4KRKfCziXovHChhTY9NS3N9h8zdovkQ2dJCSTHzoLvnbQGb3HztbZK7iKXuz2KE?uid=43285747-5465-427a-9aae-e9cda29ae095",
"issuer": "did:web:compliance.lab.gaia-x.eu:v1-staging",
"issuanceDate": "2026-01-28T15:14:04.300Z",
"expirationDate": "2026-04-28T15:14:04.300Z",
"credentialSubject": [
  {
    "type": "gx:compliance",
    "id": "https://rebuilt.infordata.eu/.well-known/participant.json",
    "gx:integrity": "088fcef8a1547b19dfa03d1b8a684387cf8da02e0ea68bc8340657376a4a9e5e",
    "gx:integrityNormalization": "RFC8785:JCS",
    "gx:version": "22.10",
    "gx:type": "gx:LegalParticipant"
  },
  {
    "type": "gx:compliance",
    "id": "https://rebuilt.infordata.eu/.well-known/gx-terms-and-cs.json",
    "gx:integrity": "c1f1a13bdc083320875fcb9eb8da9ccf0c81068fee48cdfde6f7aa53ee8fb70d",
    "gx:integrityNormalization": "RFC8785:JCS",
    "gx:version": "22.10",
    "gx:type": "gx:GaiaXTermsAndConditions"
  },
  {
    "type": "gx:compliance",
    "id": "https://rebuilt.infordata.eu/.well-known/lrn.json",
    "gx:integrity": "3bf56f479232154662939221c436d15369ddb39b4c92ca4a5cb50b2192367d81",
    "gx:integrityNormalization": "RFC8785:JCS",
    "gx:version": "22.10",
    "gx:type": "gx:legalRegistrationNumber"
  }
],
"proof": {
  "type": "JsonWebSignature2020",
  "created": "2026-01-28T15:14:04.312Z",
  "proofPurpose": "assertionMethod",
  "verificationMethod": "did:web:compliance.lab.gaia-x.eu:v1-staging#X509-JWK2020",
  "jws": "eyJhbGciOiJIUzI1NiIsImI2NCI6ZmFsc2UsImNyYXQiOiJ0IiwiaWF0Ij0119..kyuBbfU_8sMXBILbAuq3Pt8maiPnXI0DWEpg0HItYuJIAvU2BlrDmpxdttIEZUahAzwni28K_XCwSvMv4WtwJfBnk5oMgDO9VqXZBA7I37rhVguBfO5D2zcVDxVZbdfj_QzfGw72ne8rPzT05UGsspFV4s0fKBdwSSA43XbBcYLcUpLezjxpJgG78sZ5MoIHt0RgQqJ_SCH3ASOSv2hNZB1TdVzAik1QDRxz7W7Eidrow8N0o7U2zAeD_a4Vn8DQ2sfZ015ecI3nq5Vd50x5UN-R0inzC3VXTLZzmFIPEgSqxe4WYRYxgGRx-v9p9qKNDy-Jedj5PdWe3DKEtkldg"
}
```

The issuer `did:web:compliance.lab.gaia-x.eu:v1-staging` is the Gaia-X Compliance Service itself, signing the credential with its own `JsonWebSignature2020` proof. This creates an independently



verifiable chain: the platform's DPPs are signed by the platform's DID, and the platform's identity is endorsed by the Gaia-X Compliance Service. Any verifier following this chain can confirm both the material data integrity and the issuer's standing as a compliant Gaia-X participant.

5.2.5 JSON-LD Product Passport Signing

The platform implements a fully verifiable Digital Product Passport (DPP) using W3C Verifiable Credentials and Gaia-X trust components. Each passport is issued as a Verifiable Credential and signed using the JsonWebSignature2020 algorithm, ensuring cryptographic integrity, authenticity, and interoperability across federated data spaces.

The DPP includes a proof section containing a JWS signature generated with the private key corresponding to the public verification method published in the platform's DID document (did:web:rebuilt.infordata.eu). This enables any external verifier to validate the passport by:

1. Retrieving the DID document from .well-known/did.json
2. Extracting the JsonWebKey2020 public key (#key-1)
3. Verifying the JWS signature over the JSON-LD payload.

This decentralized verification workflow aligns with the Gaia-X Trust Framework and ensures that product data can be validated without relying on centralized authorities.

The Digital Product Passport follows the UN/CEFACT DPP 0.6.0 vocabulary, providing structured information on product characteristics, material composition, recycling events, certifications, and regulatory compliance. The passport is linked to the organization's Gaia-X Participant Verifiable Credentials, obtained through the official Gaia-X onboarding wizard, ensuring trusted organizational identity and enabling automated compliance checks through Gaia-X Clearing Houses.

This implementation provides a fully interoperable, verifiable, and Gaia-X-compliant mechanism for product data exchange, supporting circular economy processes and cross-border collaboration within European digital ecosystems.

Below shown example signed DPP product in format Json-LD

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://test.uncefact.org/vocabulary/untpl/dpp/0.6.0/"
  ],
  "type": [
    "VerifiableCredential",
    "DigitalProductPassport"
  ],
  "id": "https://rebuilt.infordata.eu/credentials/7",
  "issuer": {
    "id": "did:web:rebuilt.infordata.eu",
    "name": "Infodata"
  },
  "validFrom": "2025-11-10T18:16:12+00:00",
  "validUntil": "2035-11-10T18:16:12+00:00",
  "credentialSubject": {
    "id": "https://rebuilt.infordata.eu/product?id=7",
```



```
"type": [
  "ProductPassport"
],
"granularityLevel": "batch",
"product": {
  "id": "https:\\\\rebuilt.infordata.eu\\product?id=7",
  "type": [
    "Product"
  ],
  "name": "Concrete block C25\\30",
  "category": "Recycling",
  "colour": "#d9d9d9",
  "weight": {
    "value": 20,
    "unit": "KGM"
  },
  "dimensions": {
    "depth": {
      "value": 400,
      "unit": "MMT"
    },
    "height": {
      "value": 200,
      "unit": "MMT"
    }
  },
  "serialNumber": "3c7e6d39-3eaf-404d-b668-8c41bb03e4cc",
  "producedByParty": {
    "id": "did:web:rebuilt.infordata.eu#org-1",
    "name": "Infodata",
    "address": "str. per Vienna, 55\\1, 34151 Trieste TS, Italia"
  },
  "materialContent": [
    {
      "name": "Concrete",
      "quantity": {
        "value": 11,
        "unit": "t"
      },
      "disposals": [
        {
          "batchId": "BATCH-2025-01",
          "wasteCode": "17 01 06",
          "quantity": {
            "value": 5,
            "unit": "t"
          },
          "disposal_date": "2025-01-05T12:00:00+00:00",
          "supplier": {
            "name": "Gradbeništvo Novak d.o.o."
          },
          "demolitionCompany": {
            "name": "Gradbeništvo Novak d.o.o."
          },
          "events": [
            {
              "type": [
                "Event"
              ],
              "processing_id": "P 1",
              "processor_permit_issued_at": "2025-09-10",
              "processor_permit_no": "35407-164\\2006-10",
              "transport_evidence_sheet": "EVID-2025-0045",
              "consumed_transport_event_id": "T1",
              "departure_time": "2025-06-04T12:00:00+00:00",
              "arrival_time": "2025-06-04T21:00:00+00:00",
            }
          ]
        }
      ]
    }
  ]
}
```



```
        "vehicle_type": "dump truck",
        "treated_mass": {
            "value": 15,
            "unit": "t"
        },
        "transport_organisation": {
            "name": "2FAST4U, TRANSPORT IN LOGISTIKA,
D.O.O."
        },
        "recycling_organisation": {
            "name": "ABRASIV MUTA PROIZVODNJA, TRGOVINA IN
STORITVE D.O.O."
        },
        "storage_location": "IZOLA - INDUSTRIJSKA CESTA 8A,
6310 IZOLA - ISOLA",
        "treatment_location": "IZOLA - INDUSTRIJSKA CESTA
8A, 6310 IZOLA - ISOLA",
        "location_departure": "Dunajska cesta 200, 1000
Ljubljana",
        "location_destination": "Celovška cesta 300, 1000
Ljubljana",
        "hazardous": "Not hazardous - meets non-hazardous
classification",
        "treatment_type": "R_12"
    }
}
]
}
],
"image":
"https://\rebuild.infordata.eu/uploads/product_attachments/7/Non-Bearing-Wall-
Partition-Building-Material-AAC-Block.webp",
"additionalProperty": [
    {
        "name": "Product Type",
        "value": "Precast concrete element"
    },
    {
        "name": "Manufacturer Organization",
        "value": "ABC Concrete d.o.o."
    },
    {
        "name": "Manufacturer Address",
        "value": "Ljubljana, Slovenia"
    },
    {
        "name": "Unique Product ID",
        "value": "ABC-CB-C2530-001"
    },
    {
        "name": "Intended Use",
        "value": "Load-bearing wall component"
    },
    {
        "name": "Harmonised Standard",
        "value": "EN 771-3"
    },
    {
        "name": "Dop Reference Number",
        "value": "DOP-2025-001"
    },
    {
        "name": "DOP Date",
        "value": "23\07\2025"
    },
]
```



```
{
  "name": "System Assessment",
  "value": "System 2+"
},
{
  "name": "Certification Body",
  "value": "TÜV Slovenia"
},
{
  "name": "Certification Number",
  "value": "NB1234"
},
{
  "name": "Compressive Strength (MPa)",
  "value": "25.0"
},
{
  "name": "Density (kg\m³)",
  "value": "2200.0"
},
{
  "name": "Fire Resistance Class",
  "value": "REI 90"
},
{
  "name": "Thermal Conductivity (W\mK)",
  "value": "0.350"
},
{
  "name": "Safety Instructions Attached",
  "value": "Yes"
},
{
  "name": "GHG Emissions (kg CO2-eq\unit)",
  "value": "174.000000"
},
{
  "name": "Recyclability Rate (%)",
  "value": "20"
},
{
  "name": "Recycled Content (%)",
  "value": "30"
},
{
  "name": "Digital Carrier Type",
  "value": "QR code"
},
{
  "name": "Carrier Location",
  "value": "Printed on product packaging"
},
{
  "name": "Data Access Url",
  "value": "https:\\\\rebuilt.infordata.eu\\product?id=7"
},
{
  "name": "Linked Eu Legislation",
  "value": "REACH, CLP"
},
{
  "name": "Safety Data Sheet Available",
  "value": "Yes"
},
{
  "name": "Technical File Reference",
```



```
      "value": "TECH-DOC-2025-01"
    },
    {
      "name": "Dpp Create By",
      "value": "Elazem Abdelhamid"
    },
    {
      "name": "Dpp Creation Date",
      "value": "22\07\2025"
    },
    {
      "name": "Dpp Last Updated",
      "value": "23\07\2025"
    },
    {
      "name": "Dpp Backup Location",
      "value": "Internal Server \\/ DPP provider"
    },
    {
      "name": "Dpp Version Number",
      "value": "1.0"
    }
  ]
},
"proof": {
  "type": "JsonWebSignature2020",
  "created": "2025-11-10T18:16:12Z",
  "proofPurpose": "assertionMethod",
  "verificationMethod": "did:web:rebuilt.infordata.eu#key-1",
  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..OrY1rFPJVi0-RoYGaKrx6ICuf94r_ltVSGuyiHz84m-nvZG1-IJ1k2SNgZq6XKl5BV9-YI2q4NOGkeQkfd8tKq2YvEGgvWKyMyf3ojq34aNLnS98qOsO9LdmS4_dnobxvIO3OuMp4ZlTz-EoDkgM6lW2ZWAccF41JefYEXOCxFRqz0fSPfTws4ZZb_O5_0-ssCUJ2rsiVQlJ5GJKziiAbl2RnbiGBdh-FfO57F7XfHpJXcrt6_D_krExLaz0bQbstQYz_JIfYYHsixrQhkRkpZplx9V4-TRiaqYjP6m4eS8U_WhCgHfg8qN7ehe_H1KIdj1w-Xkbb3qu36c-fMRprQ"
}
```

Table 3: Key Fields of the Digital Product Passport Verifiable Credential

Field	Value Type	Description
@context	Array of URIs	Defines semantic vocabularies (W3C VC + UN/CEFACT DPP).
type	Array	Indicates the document is a Verifiable Credential and a Digital Product Passport.
id	url	Unique identifier of the credential.
issuer.id	DID	Decentralized Identifier of the issuing organization.



issuer.name	String	Human readable name of the issuer.
validFrom / validUntil	DateTime	Credential validity period.
credentialSubject.id	URL	Identifier of the product or batch described by the passport.
credentialSubject.type	Array	Declares the subject as a Product Passport.
granularityLevel	String	Defines whether the passport applies to a unit, batch, or product family.
Product.type, product.name etc	String	Product fields
proof.type	String	Signature type (JsonWebSignature2020).
proof.created	DateTime	Timestamp of signature creation.
proof.proofPurpose	String	Purpose of the signature (assertionMethod).
proof.verificationMethod	DID URL	Reference to the public key in the DID document.
proof.jws	String	JWS encoded cryptographic signature of the VC.

5.2.6 Compliance and Interoperability Considerations

The implemented identity and signing architecture follows the Gaia-X Trust Framework, W3C Verifiable Credentials Data Model, and UN/CEFACT DPP specifications. The use of JsonWebSignature2020, JsonWebKey2020, and did:web ensures full interoperability with Gaia-X Clearing Houses, conformity assessment services, and federated catalogues. The platform applies JSON-LD canonicalization (URDNA2015) prior to signing, enabling deterministic and verifiable signatures across independent verification tools. The inclusion of eIDAS-aligned certificates further strengthens trust anchoring and supports future integration with European digital identity services.



5.3 Integration with CinderOSS Platform

The upgraded **CinderOSS platform**, managed by Open Content, serves as a **transnational circular economy platform** for sharing knowledge, tools, and materials.

Through API-level integration, the system supports:

- **Publishing of Digital Product Passports** for identified materials and components
- **Exposure of DPP records via CinderOSS frontend**
- **Linking legislative frameworks** and EoW criteria to relevant material types
- **Uploading reusable technologies and green business model templates**

This integration ensures visibility of pilot outcomes across Central Europe and contributes to the scalability of the solution.

These external integrations transform the digital pilot into an **interoperable and extensible ecosystem**, supporting real-world circular economy objectives while complying with EU digital infrastructure frameworks.



6. Database Schema Description

The complete database schema for the ReBuilt platform is documented in D2.3.1. This section covers only the table directly introduced by this deliverable: `product_dpp_sign`, which stores every signed version of a Digital Product Passport.

`product\_dpp\_sign` database table

This table stores signed versions of a product's Digital Product Passport (DPP) after each modification. It includes a hash of the signed data, the full JSON-LD Verifiable Credential, and an optional `blockchain_id` for external verification. Each row represents one signed version – a complete audit trail of DPP evolution.

F ie ld	Type	Comment
i d	int(11) NOT NULL	
p ro du ct _i d	int(11) NOT NULL	Foreign key to product
h as h	text NOT NULL	SHA hash of the signed JSON payload
j so n	JSON NOT NULL	Full JSON-LD Verifiable Credential
b lo ck ch ai n_ id	varchar(64) NULL	Optional distributed ledger reference
c re at ed _a t	int(11) NULL	



F ield	Type	Comment
updated _at	int(11) NULL	

7. Challenges and Lessons Learned

7.1 Technical Implementation Challenges

The development and integration of Gaia-X infrastructure within the ReBuilt platform presented several notable technical challenges. Establishing a fully compliant Decentralised Identifier (DID) using the did:web method required careful alignment with W3C DID Core specifications and the Gaia-X Trust Framework. Generating eIDAS-aligned certificates and managing the corresponding private keys securely while enabling automated signing of Digital Product Passports demanded a robust key management process that balanced security with operational continuity.

Integration with the Gaia-X Clearing Houses for automated compliance verification proved more complex than anticipated. The clearing house APIs were subject to versioning changes during the project period, requiring adaptive implementation to maintain compatibility with both the production (Clearing Houses v1) and development environments. Fallback procedures were implemented to ensure platform functionality during periods of external system unavailability.

Aligning the Digital Product Passport data model with both the UN/CEFACT DPP 0.6.0 vocabulary and the Gaia-X ontology requirements necessitated iterative schema development. The JSON-LD canonicalization process (URDNA2015) required validation across multiple independent verification tools to confirm deterministic signature generation.

7.2 Operational and Organisational Challenges

Raising awareness and understanding of Gaia-X concepts among construction sector stakeholders proved challenging. The technical complexity of federated identity, verifiable credentials, and decentralised data sharing is unfamiliar to most construction industry professionals. Significant effort was invested in translating these concepts into practical, value-oriented demonstrations at the NIGRAD pilot site.

Cross-border data sharing under varying national interpretations of data sovereignty and GDPR required consultation with legal experts across partner countries. Defining clear



terms of service and data usage policies that satisfied both Gaia-X compliance requirements and national regulatory frameworks added complexity to the operational implementation.

7.3 Lessons Learned

The most important lesson learned is that Gaia-X compliance is not a binary state but a continuous alignment process. As the Trust Framework and Clearing House specifications evolved during the project, the platform architecture benefited greatly from its modular design, which allowed targeted updates without disrupting core functionality. Future implementations should plan for regulatory and specification evolution from the outset, building in configuration flexibility rather than hard-coded compliance parameters.

Practical demonstration of Gaia-X value – through signed Digital Product Passports that can be verified by any external party without relying on a central authority – proved to be the most effective way to communicate the benefits of the approach to non-technical stakeholders. Concrete use cases grounded in material traceability were far more persuasive than abstract descriptions of federated infrastructure.

Finally, the eIDAS certificate chain proved to be a critical trust anchor that significantly strengthened stakeholder confidence in the solution. Ensuring that certificate procurement and renewal processes are integrated into platform operations is essential for long-term sustainability of the Gaia-X use case.

8. Conclusions and Next Steps

8.1 Summary of Achievements

Deliverable 2.3.5 successfully demonstrates the development of a GAIA-X use case within the ReBuilt project, building directly on the digital material traceability platform described in D2.3.1. The implementation establishes INFORDATA's platform as a Gaia-X compliant participant through a fully operational Decentralised Identifier (`did:web:rebuilt.infordata.eu`), Verifiable Credentials generated via the official Gaia-X onboarding wizard, and cryptographically signed Digital Product Passports using `JsonWebSignature2020`. These achievements position the ReBuilt solution as a reference implementation for Gaia-X-aligned circular construction data infrastructure in Central Europe.

The use case demonstrates end-to-end verifiability: any external party can retrieve the DID document, extract the public key, and independently verify the authenticity of any signed DPP without relying on a centralised authority. This realises the core Gaia-X principle of data sovereignty while enabling practical circular economy workflows across organisational and national boundaries.

8.2 Contribution to ReBuilt Objectives

The GAIA-X use case directly supports the ReBuilt project's goal of delivering interoperable digital solutions for circular construction in Central Europe. By embedding



Gaia-X compliance into the material passport and data-sharing infrastructure, the platform enables the kind of trusted cross-border collaboration that is essential for scaling circular construction material flows beyond single pilot sites. The solution contributes to D2.3.4 (Summary report on testing of digital tools) by providing empirical evidence of Gaia-X feasibility in a real construction sector context, and to the broader output O2.2 (Circular construction digital pilots) by serving as the Gaia-X case study referenced in the Grant Agreement.

8.3 Next Steps and Recommendations

In the short term, the priority is completing the connection between the platform's Gaia-X Participant Verifiable Credentials and the Clearing House validation workflow in the production environment. Automated credential renewal processes should be established to ensure continuity of Gaia-X participation beyond the project period.

In the medium term, the platform should pursue alignment with the evolving EU Digital Product Passport regulation, leveraging the existing Gaia-X and UN/CEFACT DPP 0.6.0 foundations as a basis for regulatory compliance. Expanding the DID ecosystem to cover partner organisations within the ReBuilt consortium would further demonstrate the federated potential of the approach.

Long term, the GAIA-X use case developed in ReBuilt provides a replicable template for other construction sector platforms seeking to participate in European data spaces. The modular architecture, open standards alignment, and practical demonstration at NIGRAD collectively form a knowledge asset that can support technology transfer to additional Central European regions and construction value chain actors.