D5.2 Final inventory of features for products/components

Document Identification			
Status	Final	Due Date	31/07/2022
Version	1.0	Submission Date	02/08/2022

Related WP	WP5	Document Reference	D5.2
Related Deliverable(s)	D2.5, D4.1, D4.5, D4.9, D5.1	Dissemination Level (*)	PU
Lead Participant	SGAD	Lead Author	Javier Ferrero Merchán (SGAD, ES)
Contributors	Ángel Palomares (ATOS)	Reviewers	Miguel Correia (INESC)
			Carl-Markus Piswanger (BMDW)

Keywords:
Feature, patterns, common, components

Document Information

List of Contributors	
Name	Partner
Javier Ferrero Merchán	MPTFP-SGAD (ES)
Ángel Palomares Pérez	ATOS

Document History			
Version	Date	Change editors	Changes
0.1	18/07/2022	Javier Ferrero (SGAD)	Initial version of document
0.2	22/07/2022	Ángel Palomares (ATOS)	SSI functionalities added
0.3	25/07/2022	Javier Ferrero (SGAD)	Version ready for formal review
0.3.1	26/07/2022	Javier Ferrero (SGAD)	Fixed a problem with references
0.4	29/07/2022	Javier Ferrero (SGAD)	Corrections resulting from the formal review.
0.5	01/08/2022	Julia Wells (ATOS)	Revision for submission
1.0	02/08/2022	Alberto Crespo (ATOS)	Final version for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Javier Ferrero Merchán (SGAD, ES)	29/07/2022
Quality manager	Julia Wells (ATOS)	01/08/2022
Project Coordinator	Alberto Crespo (for Ana Piñuela) (ATOS)	02/08/2022

Table of Contents

List of Acronyms

Abbreviation / acronym	Description
API	Application Programming Interface
AS4	Applicability Statement, 4
DE	Data Evaluator
DE4A	Digital Europe for All
DO	Data Owner
DR	Data Requestor
DT	Data Transferor
Dx.y	Deliverable number y, belonging to WP number x
EBSI	European Blockchain Services Infrastructure
ESL	Evidence Service Locator
ESSIF	European Self Sovereign Identity Framework
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAL	Issuing Authority Locator
IM	Intermediation (pattern)
LU	Lookup (pattern)
MOR	Multilingual Repository Ontology
PSA	Project Start Architecture
S&N	Subscription and Notification (pattern)
SSI	Self-Sovereign Identity
SMP	Service Metadata Publisher
USI	User-Supported Intermediation (pattern)
VC	Verifiable Credentials (pattern)
XML	Extensible Markup Language
WP	Work Package

Executive Summary

This deliverable describes the set of features necessary for the common specifications and components of the DE4A project to build a fully operational environment.

The inventory encompasses the following features:

▸ Transference of a request for evidence from the Data Evaluator (DE) to Data Owner (DO).
▸ Transference of a requested piece of evidence from the DO to the DE.
▸ Transference of an event notification referred to a previous subscription from the DO to the DE.
▸ The error handling necessary to inform other components about problems occurred when processing or exchanging a message.
▸ Identification of the Issuing Authority of a Canonical Evidence Type within a specific country.
▸ Location of the service endpoint of a required Issuing Authority.
▸ Label translation service for the e-procedure portals of DEs.
▸ Component management and operation via the corresponding interfaces.
▸ Issuance of Verifiable Credentials by Data Producers.
▸ Verification of Verifiable Presentations by Data Consumers (DC).
▸ Identity information management by students.
▸ Communication security.
▸ Traceability and auditory of the exchange messages.

These features have been implemented through the DE4A interfaces and common specifications, the DE4A common components and the components of the DE4A Self-Sovereign Identity Supporting Framework.

1 Introduction

1.1 Purpose of the document

The present document has been written in the context of **"WP5 Common Component Design & Development"** under the **Task T5.1 Consolidation of Features and Patterns**. The aim of this task is to analyse all the features required by the architecture framework, the semantic blocks and the pilots in order to obtain common needs for their implementation as common services and components for building a fully operational environment.

The scope of WP5 is the design and development of all new common software components, required for the pilot implementations, and according to the outputs of "WP2 Architecture vision and framework" and "WP3 Semantic Interoperability Solutions" on architecture and semantic components.

This deliverable defines an inventory of features required by the pilots, defined in "WP4 Cross-border Pilots for Citizens and Business and Evaluation" and implemented in the common components and the Self-Sovereign Identity (SSI) supporting framework.

This deliverable D5.2 is related to the following DE4A deliverables:

▸ D2.5 Project Start Architectures (PSA), second iteration
▸ D4.1 Studying Abroad pilot - Use Case Definition & Requirements
▸ D4.5 Doing Business Abroad - Use Case Definition & Requirements
▸ D4.9 Moving Abroad - Use Case Definition & Requirements
▸ D5.1 First inventory of features for products/components

1.2 Structure of the document

This document is structured into three chapters:

▸ Chapter 1 is the introduction to the document
▸ Chapter 2 set outs the catalogue of features
▸ Chapter 3 provides the conclusions

2 Inventory of Features

This section describes the main features required to build a fully operational environment.

2.1 Introduction and methodology

The inventory of features takes into consideration the following definitions:

▸ **Feature**: The IEEE 829 standard defines feature as "a distinguishing characteristic of a software item (e.g., performance, portability, or functionality)."
▸ **Component:**
  - A **software component** is basically a **software** unit with a well-**defined** interface and explicitly specified dependencies.
  - A **software component** can be as small as a block of reusable code, or it **can be as big as an entire application.**
▸ **Application Programming Interface (API)** is a software interface that serves as a means of data transfer between different applications or program functions.
▸ **A Service:** a function offered by an electronic device to another electronic device communicating via Web.
▸ A **Web service:** a service provided using web technologies, such as web servers, the HTTP/HTTPS protocols, XML, etc.

A feature can then be implemented via components, APIs or web services.

The inventory of features has been compiled considering the DE4A pilot use cases and the requirements described in the pilot deliverables [6][7][8] and the final version of the Project Start Architecture [4].

The following interaction patterns [4] have been considered:

▸ Intermediation (IM)
▸ User-Supported Intermediation (USI)
▸ Verifiable Credentials (VC)
▸ Subscription and Notification (S&N)
▸ Lookup (LU)

For the scope of this deliverable, only features of the **common components** are considered, for that is the scope defined in Annex 1 – Description of the action [1] of the Grant Agreement of DE4A. The common components developed and/or managed by WP5 are:

▸ DE4A Connector
▸ Central IAL
▸ SSI Authority Agent
▸ SSI User Agent
▸ eDelivery infrastructure: SML, SMP and AS4 Gateway

2.2 Main Features

2.2.1 Functional features

2.2.1.1 Transference of a request for evidence

The aim of the DE4A project is to enable the automatic exchange of verifiable evidence in a communication between two legal entities located in different Member States. The entity that needs the evidence lies on the Data Consumer (DC) side, while the entity the provides the evidence lies on the Data Provider (DP) side. The Data Consumer (DC) side is made up of the Data Evaluator (DE) and the Data

Requestor (DR), whereas the Data Provider side in turn consists of the Data Provider (DP) and the Data Transferor (DT) [2].

Therefore, one of the first key functionalities of the DE4A components is to allow a Data Evaluator (DE) to send a request for evidence to a Data Owner (DO). This functionality is mainly realised through the DE4A Connector, which takes the role of the Data Requestor (DR) and/or the Data Transferor (DT), and the eDelivery AS4 Gateway.

The DE4A Connector allows a Data Evaluator (DE) to send an evidence request message to the appropriate Data Owner (DO), delegating the routing of the message to the Data Requester (DR). The transferred message will handle the following information:

▸ The **identifier of the request message**.
▸ The identifier of the **DE4A specification version**.
▸ A **timestamp** of when the request message was created.
▸ The **SDG procedure**, which is the DE's administrative procedure whose processing requires the request, and that must include at least one category for the procedure according to the SDG regulation.
▸ The identifier of the DE4A participant that makes the request (**DE**).
▸ The identifier of the DE4A participant to whom the request is addressed (**DO**).
▸ The requested Canonical Evidence Type or the Event Catalogue.

It is possible to request multiple items (Canonical Evidence Types or Event Catalogues) according to the multi-evidence cases considered in the second iteration of the project [4]. In addition, the requested Canonical Evidence Type or Event Catalogue always refers to a Subject (natural or legal person) and the grounds for making the request are included in the message as well.

The exact information requested varies depending on the interaction pattern used [4]:

▸ Intermediation (IM)
  - The request allows to send some additional parameters, specifically requested by each DO in order to access to the corresponding evidence. This pattern is intended to exchange pieces of Canonical Evidence.
▸ User-Supported Intermediation (USI)
  - This pattern is also intended to exchange pieces of Canonical Evidence, while no additional parameters are needed since the User will have the opportunity to interact directly with system of the DO.
▸ Subscription and Notification (S&N)
  - Instead of evidence, a subscription message asks the DO to subscribe the DE to a Catalogue of Events in relation to the Subject of the request.
▸ Lookup (LU)
  - Very similar to the IM pattern, the request allows to send some additional parameters too, and also allows to exchange pieces of Canonical Evidence.

The DE4A Connector does not support the Verifiable Credentials pattern since this interaction pattern is implemented by the SSI components.

2.2.1.2 Transference of a requested piece of evidence

Once the request for evidence has successfully reached the Data Owner, the DO will analyse the request and prepare the response. Thus, the other key functionality of the DE4A components is to allow a Data Owner to send a piece of evidence to a Data Evaluator in response to a previous request. This functionality is mainly realised through the DE4A Connector, taking the role of the Data Requestor and/or the Data Transferor, and the eDelivery AS4 Gateway.

The routing of the response message is delegated to the DT by the DO. The transferred message will handle the following information:

▸ The **identifier of the request message** to which the response refers.

Document name:	D5.2 Final inventory of features for products/components				Page:	8 of 13
Reference:	D5.2	Dissemination:	PU	Version:	1.0	Status:	Final

‣ A **timestamp** of when the response message was created.
‣ The identifier of the DE4A participant that made the request (**DE**).
‣ The identifier of the DE4A participant that sends the response (**DO**).
‣ The requested piece of **Canonical Evidence**.
‣ Optionally, the **Domestic Evidence** that is regularly issued by the DO.

It is possible to send back multiple pieces of Canonical Evidence according to the multi-evidence cases considered in the second iteration of the project [4].

The exact information returned to the DE varies depending on the interaction pattern used [4]:

‣ Intermediation (IM)
  - The response includes one or multiple pieces of Canonical Evidence, besides the Domestic Evidence the DO might wish to add.
‣ User-Supported Intermediation (USI)
  - Additionally to the evidence response, in this interaction pattern there is a first response message for the DO to inform the DE about the URL of the evidence portal to where the User must be redirected to extract and preview the requested evidence.
‣ Subscription and Notification (S&N)
  - In this case, no evidence is exchanged, but a confirmation of the subscription is sent back from the DO to the DE.
‣ Lookup (LU)
  - As in the IM case, the response includes one or multiple pieces of Canonical Evidence, plus any Domestic Evidence the DO might want to add.

In the same way as in the case of requests, the DE4A Connector does not support the Verifiable Credentials pattern since this interaction pattern is implemented by the SSI components.

2.2.1.3   Transference of an event notification

The event notification is a unique type of message in DE4A. It is sent by initiative of the sender, instead of in response to a previous request message. The event notification is triggered by an event on the DP side, and thus, the DO sends a message notifying the DE about such an event affecting a previously requested subscription. This functionality is also realised through the DE4A Connector, which takes the role of the Data Requestor and/or the Data Transferor, and the eDelivery AS4 Gateway.

The routing of the event notification message is delegated to the DT by the DO as in the above transferences. The transferred message will handle the following information:

‣ The **identifier of the event notification message**.
‣ The identifier of the **DE4A specification version**.
‣ A **timestamp** of when the event notification message was created.
‣ The identifier of the DE4A participant that sends the event notification (**DO**).
‣ The identifier of the DE4A participant to whom the event notification is addressed (**DE**).
‣ The **event-related data**: event identifier, affected subject, Canonical Event Catalogue to which the event belongs, etc.

It is possible to notify about multiple events at the same time according to the multi-evidence cases considered in the second iteration of the project [4].

This type of message is part of the Subscription and Notification pattern.

2.2.1.4   Error handling

Sending back a piece of Canonical Evidence in response to a request is considered the end of a "happy flow". However, the DE4A components must be able to report errors, exceptions or undesired endings that prevent the DE from receiving the requested evidence.

Each major DE4A component is able to exchange a standardised set of error messages with the appropriate components informing about problems occurred when **processing** or **exchanging** a message. As with the request, response and event notification messages, the error messages are exchanged via the DE4A Connector and the eDelivery AS4 Gateway.

2.2.1.5   Issuing Authority Location

When a DE needs to send a request for evidence to a DO, the first step is to identify the DO. During the dialogue with the User in the e-procedure portal of the DE, the DE will establish which Canonical Evidence Types are needed for the ongoing online procedure and from which Country they must be requested. With that information (the Canonical Evidence Types and the country), the DE is able to identify the issuing authority able to return the desired evidence from the corresponding country, namely, the Data Owner.

The Issuing Authority Locator (IAL) functionality [5], defined by WP3 Semantic Interoperability Solutions, is realised by the Central IAL, and the DE4A Connector facilitates the communication with it.

2.2.1.6   Evidence Service Location

At the time of sending an evidence request, evidence response or event notification message, DEs and DOs delegate the routing of the message to the DE4A Connector.

The DE4A Connector is able to find the service endpoint of the other Connector to send the message to. To do so, the dynamic discovery functionality of the eDelivery components is used. It is a two-step process:

▸ The sending DE4A Connector queries the European Commission's SML/DNS for the identifier of the receiving participant (either a DE or a DO). The Connector receives in response the URL and the certificate of the SMP that the sender needs to query further (in general, this will be the SMP of the country where the other necessary information of the recipient is stored).
▸ The DE4A Connector then queries the aforementioned SMP with the identifier of the recipient participant and the Canonical Evidence Type to exchange (and some other data needed by the protocol). The Connector receives in response the URL and the certificate of the AS4 Gateway or the Connector to which it has to send the corresponding message.

At this point, the DE4A Connector is able to send the message as an AS4 message to the receiving Connector.

2.2.1.7   Label Translation

This functional feature allows DEs to request a translation of its e-procedure portals into the language requested by the User, provided that it is one of the official languages of the European Union.

The translation is requested by the DE to a component of the Multilingual Repository Ontology (MOR) functionality [5], defined by WP3, which, in turn, requests the translation to the MOR label repository located in the Central IAL.

2.2.1.8   Component management and operation

The components built in DE4A need to present a user interface for the operator to manage some configurable information.

In the case of the DE4A Connector, there are two sets of information that need to be managed:

▸ The configuration properties of the Connector, managed through a configuration file.
▸ The URLs of the service endpoints of the DEs and DOs that the DE4A Connectors serve. These URLs are used by Connectors to send messages to DEs and DOs when the Connector and the DE or the Connector and the DO belong to the same side of the communication, i.e. to the Data Consumer side or the Data Provider side, respectively. This information is managed through a JSON file loadable by the DE4A Connector.

Document name:	D5.2 Final inventory of features for products/components				Page:	10 of 13
Reference:	D5.2	Dissemination:	PU	Version:	1.0	Status:	Final

2.2.1.9 Data Producer: Issue Verifiable Credentials

This functionality allows:

▸ The creation of Verifiable Credentials (VC) (using the student's diploma data)
▸ Their signing by following the EBSI/ESSIF guidelines and services
▸ The delivery of the VC to the student's mobile application

2.2.1.10 Data Consumer: Verify Verifiable Presentation

This functionality allows:

▸ To obtain the student's diploma Verifiable Presentation from the mobile application.
▸ To verify the content of the Verifiable Presentation containing the diploma information. The verification process includes the validation of the subject, the schema, the issuer and the digital signature.

2.2.1.11 Students: Identity Information Management

This functionality is provided by a mobile application to the student. Such mobile application allows the student to manage their Identity Information following a Self-Sovereign Identity approach. The most significant functionalities allowed by the mobile application are as follows:

▸ Manage the connections with the stakeholder (Data Providers/Data Consumers)
▸ Manage the Verifiable Credentials (obtained from the Data Producers)
▸ Manage the Verifiable Presentations (presented to the Data Consumers)

2.2.2 Non-functional features

2.2.2.1 Communication security

The security protection of communications in DE4A takes into account the security properties of confidentially, integrity, authenticity and non-repudiation of the exchanges that take place between different components. This is achieved through the use of cryptographic methods to identify the components and participants involved in a communication and by properly encrypting the exchanged data. In short, a Trust Architecture [3] has been set up.

Some of the functionalities here involved are:

▸ Digital certificates management
▸ Creation, verification and validation of digital signatures
▸ Cryptographic protection of the information

2.2.2.2 Traceability and auditory

DE4A components are able to keep and show the trace of messages during their journey from their origin to their destination.

To do so, a standardised set of log messages has been defined so that each DE4A component records a certain number of actions during exchanges. These messages are stored in local log files, so that they can be collected and analysed to assess the performance of the DE4A pilots.

Messages are also sent to a Kafka server. The log messages received in this Kafka server may be viewed through a Kafka Tracker that displays the messages in real time. This is also useful during *Conectathons*, live sessions where participants test the correct exchange of messages and evidence.

3 Conclusions

The identified inventory of features, aligned with the Project Start Architecture (PSA), the Semantic Tools, and the Pilot requirements defined by work packages "WP2 Architecture vision and framework", "WP3 Semantic Interoperability Solutions", and "WP4 Cross-border Pilots for Citizens and Business and Evaluation", comprises a complete set of common functional and non-functional characteristics required to build a fully operational environment for the DE4A project.

These features have been implemented through:

▸ The DE4A interfaces and common specifications [10]
▸ The DE4A common components [11] and the components of the DE4A Self-Sovereign Identity Supporting Framework [12]

References

[1] DE4A Description of the Action

[2] DE4A D2.1 Architecture Framework (2020) retrieved via https://www.de4a.eu/project-deliverables

[3] DE4A D2.3 Final DE4A Trust Management Models and Self-Sovereign Identity Supporting Framework Design (2021) retrieved via https://www.de4a.eu/project-deliverables

[4] DE4A D2.5 Project Start Architecture (PSA), second iteration (2021) retrieved via https://www.de4a.eu/project-deliverables

[5] DE4A D3.6 Semantic Toolkit – Final Version (2022) retrieved via https://www.de4a.eu/project-deliverables

[6] DE4A D4.1 Studying Abroad - Use cases definition and requirements v1.0 (2020) retrieved via https://www.de4a.eu/project-deliverables

[7] DE4A D4.5 Doing Business Abroad - Use cases definition and requirements v1.0_Final (2020) retrieved via https://www.de4a.eu/project-deliverables

[8] DE4A D4.9 Moving Abroad - Use cases definition and requirements v1.0 (2020) retrieved via https://www.de4a.eu/project-deliverables

[9] D5.1 First inventory of features for products/components (2020)

[10] DE4A D5.3 First technical design of interfaces and common specifications (2021)

[11] DE4A D5.5 First Release DE4A Common Components (2021)

[12] DE4A D5.8 Final Release of DE4A Self-Sovereign Identity Supporting Framework (2022) retrieved via https://www.de4a.eu/project-deliverables