EUROPEAN COMMISSION

DIGIT
Connecting Europe Facility

Single Digital Gateway (SDG)

Once-Only Technical System High Level Architecture

Version [~~0.2~~0.3]

Status [draft]

Date: 13/08/2020

Document Approver(s):

Approver Name	Role
	SDG Coordination Group

Document Editor(s):

Editor Name	Role
Pim van der Eijk	DG DIGIT CEF OOP Preparatory Action

Document Contributor(s):

Contributor Name	Role

Summary of Changes:

Version	Date	Created by	Short Description of Changes
0.1	2020-04-20	Pim van der Eijk	First Draft Version for SDG CG WP7 Kick-Off Meeting
0.2	2020-05-28	Pim van der Eijk	Updated two diagrams to be consistent with the latest Archimate model
0.3	2020-08-13	Pim van der Eijk	Processed comments and feedback, updates to specifications: • Renamed Criterion and Evidence Type Rule Base to "Evidence Broker". • Completely rewritten the text for Evidence Broker. • Updated reference for AS4-RegRep4 OASIS specification. • Updated Archimate Diagrams

			• New section on Deployment Options of Once-Only Core Services. • Expanded the description of the exchange business process and main elements overview. • Explained benefits of two-step evidence retrieval. • Mention some potential future non Article 14 extensions. • Mention use of Internet/TESTA. • Added a second, simplified flow to section 9.

Formatte
0,25" + Ir

Table of Contents

Field Coc
Field Coc
Field Coc
Field Coc
Field Coc
Field Coc
Field Coc

PURPOSE OF THE DOCUMENT

The following figure summarises the objectives, target audience and main outputs of this document.

Introduce and position the Once-Only Technical System in the context of the SDG Regulation.

Provide ~~an~~a high-level overview of the main components in the system and the functionality they provide.

~~Relate the functionality to layers in the European Interoperability Framework.~~

Member State representatives in SDG Coordination Group and other designated experts.

Participants in Once-Only Large Scale Pilots.

European Commission DG CNECT and GROW policy units in the area of the Once Only Principle (OOP) and of the Single Digital Gateway (SDG).

European Commission Connecting Europe Facility (CEF) Building Blocks OOP Preparatory Action team.

~~Member State representatives preparing implementation of SDG regulation.~~

Functional description of components in Once-Only Technical System.

~~Overview of evidences in scope for Once-Only exchange.~~

Identification of roles and responsibilities of European Commission and Member States in Once-Only.

~~Explanation of the user-centricity concept.~~

Sample OOP flows.

ACRONYMS

Acronym	Description
AP	Access Point
AS4	Applicability Statement 4
CEF	Connecting Europe Facility
DSM	Digital Single Market
DE4A	Digital Europe for All
EC	European Commission
ISA²	Interoperability solutions for public administrations, businesses and citizens
ISO	International Organization for Standardization
LSP	Large Scale Pilot
MS	Member State
~~**MSH**~~	~~Message Service Handler~~
OASIS	Organization for the Advancement of Structured Information Standards
OOP	Once Only Principle
SDG	Single Digital Gateway
TOOP	The Once Only Principle

REFERENCES

Ref.	Document	Content outline
[REF1]	~~AS4 binding for RegRep4~~AS4 binding for RegRep4	~~Future~~Draft OASIS specification describing a standard protocol binding for OASIS RegRep4 for AS4 [REF27], compatible with eDelivery AS4 [REF15]. ~~Will be developed~~Developed based on input from TOOP, standardized in OASIS and used in piloting by TOOP [REF37].
~~[REF2]~~	~~Blueprint Readiness for SDG Procedures~~	~~Review of Readiness of the OOP Blueprint for SDG Procedures (EC internal).~~
~~[REF3]~~[RE	Breg-DCAT-AP	A draft of registry of registries (RoR) specification, definition of the main aspects and elements to be served for the creation of potential Registry of Registries at the European level in the future. The specification elaborates the Registry of Registries specification, namely BRegDCAT-AP, an extension of the DCAT application profile for data portals in Europe (DCAT-AP), aiming to facilitate MS work on creating their own Registry of Registries.
~~[REF4]~~[RE	CEF Digital	CEF Digital including the eID and eDelivery Building Blocks.
~~[REF5]~~[RE	CEF PKI	CEF Public Key Infrastructure (PKI) service.
~~[REF6]~~[RE	~~CEF SML~~CEF SML	CEF Metadata Service Location service.
~~[REF7]~~[RE	CEF Telecom	The Connecting Europe Facility (CEF) supports trans-European networks and infrastructures in the sectors of transport, telecommunications and energy. The European Commission has proposed a series of guidelines for telecommunications covering the objectives and priorities for Digital Service

Ref.	Document	Content outline
		Infrastructures (DSIs) and broadband networks.
~~[REF8]~~	~~Common Assessment Method for Standards and Specifications (CAMSS)~~	~~CAMSS is the European guide for assessing and selecting standards and specifications for an eGovernment project, a reference when building an architecture and an enabler for justifying the choice of standards and specifications in terms of interoperability needs and requirements.~~
~~[REF9][RE~~	DE4A	Digital Europe for All (DE4A) Large Scale Pilot
~~[REF10][R~~	Data Service Directory Interface Specification	Future specification describing use of OASIS ebXML RegRep4 registry services and ISA vocabularies to an interface format for the Data Service Directory. Initial development and piloting by the TOOP EU Large Scale Pilot [REF37]. A draft input specification is available at http://wiki.ds.unipi.gr/display/TOOP/Data+Services+Directory
[REF9]	Evidence Broker Specification	Future specification of the OOP Evidence Broker component and its interfaces. A draft input specification is available at: http://wiki.ds.unipi.gr/display/TOOP/Criterion+And+Evidence+Type+Rule+Base
~~[REF11][R~~	eCERTIS	eCertis is the information system that ~~helpsidentifying~~helps identifying different certificates requested in procurement procedures across the EU.
[REF11]	eCERTIS REST API	eCertis REST API.

Formatte

Ref.	Document	Content outline
[REF12]	EDCI Data Model	The European Commission is developing the Europass Digital Credentials Infrastructure (EDCI) – a set of tools, services and software to support the issuance of authentic, tamper-proof digital credentials (such as qualifications and other learning achievements) across Europe. The EDCI is being developed as part of ongoing work to implement the new Europass Framework for supporting transparency of skills and qualifications in Europe.
[REF13]	eDelivery Home Page	Entry point to documentation on eDelivery.
[REF14]	eDelivery Access Point	The eDelivery Access Point (AP) implements a standardized message exchange protocol that ensures interoperable, secure and reliable data exchange. An eDelivery AP is an implementation of the eDelivery AS4 Profile.
[REF15]	eDelivery AS4	eDelivery AS4 Specification, profiling the OASIS AS4 Specification [REF27].
[REF16]	eDelivery Security Controls	CEF Security Controls document.
[REF17]	eGovernment Action Plan 2016-2020	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government COM/2016/0179 final.
[REF18]	eIDAS Regulation	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[REF19]	eID Homepage	CEF eID Building Block home page.

Ref.	Document	Content outline
[REF20]	Enterprise Integration Patterns	A pattern language consisting of 65 integration patterns to establish a technology-independent vocabulary and a visual notation to design and document integration solutions.
~~**[REF21]**~~	~~EU Standardisation Regulation~~	~~REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.~~
~~**[REF22]**~~	~~EU Identification of ICT Specifications~~	~~The European Commission has developed a flexible approach to standardisation when identifying new ICT technical specifications. The European Commission can identify ICT technical specifications that are not national, European, or international standards, provided they meet precise requirements.~~
~~[REF23]~~[R	European Interoperability Framework	The European Interoperability Framework (EIF) is part of the Communication (COM(2017)134) from the European Commission adopted on 23 March 2017. The framework gives specific guidance on how to set up interoperable digital public services.
~~[REF24]~~[R	Evidence Exchange Data Model	Future specification describing use of OASIS ebXML RegRep4 registry services and ISA vocabularies for evidence requests and responses~~. Initial development and piloting by~~, based on input from the TOOP EU Large Scale Pilot [REF37]. In August 2020, input draft specifications are available at http://wiki.ds.unipi.gr/display/TOOP/.TOOP+Exchange+Data+Model+v2+v2.0.1.
~~[REF25]~~[R	General Data Protection Regulation	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

Formatte

Ref.	Document	Content outline
		95/46/EC (General Data Protection Regulation).
~~[REF26]~~[R	IMI	Internal Market Information system (IMI).
~~[REF27]~~[R	ISA²	ISA². Interoperability solutions for public administrations, businesses and citizens
~~[REF28]~~[R	ISA Core Vocabularies	The e-Government Core Vocabularies are simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral fashion.
~~[REF29]~~[R	OASIS AS4	AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard. 23 January 2013. Approved in 2020 as ISO 15000-2.
~~[REF30]~~[R	OASIS ebMS3 Core	OASIS ebXML Messaging Services 3 Version 3.0: Part 1, Core Features OASIS Standard 1 October 2007. Approved in 2020 as ISO 15000-1.
~~[REF31]~~[R	OASIS ebXML registry and repository version 4.0	OASIS standard for registry and repository.
[REF30]	Registry of Authorities	Future specification of the OOP Registry of Authorities and its interfaces. A draft input specification is available at: http://wiki.ds.unipi.gr/display/TOOP/Registry+of+Authorities
[REF31]	Semantic Repository	Future specification of the OOP Semantic Repository component and its interfaces. A draft input specification is available at: http://wiki.ds.unipi.gr/display/TOOP/Semantic+Repository

Ref.	Document	Content outline
[REF32]	SEMIC	Semantic Interoperability Community (SEMIC).
[REF33]	Single Digital Gateway Regulation	Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance.).
[REF34]	Single Digital Gateway Coordination Group	The Single Digital Gateway Coordination Group is based on the SDG Regulation [REF33]. The coordination group will have approximately 6 meetings per year and has a high need of exchange of information and content in between.
[REF35]	Single Digital Gateway Regulation ~~Implemenetation~~Implementation Guidelines	Guidelines for the implementation of the single digital gateway Regulation 2019-2020 work programme. Commission notice. (2019/C 257/01).
[REF36]	TOGAF	The TOGAF Standard, a standard of The Open Group, is a proven Enterprise Architecture methodology and framework used by the world's leading organizations to improve business efficiency.
[REF37]	TOOP	The Once-Only Principle Project (TOOP) is a Large Scale Pilot (LSP) that was launched by the European Commission in January 2017 as an initiative of about 51 organisations from 21 EU Member States and Associated Countries. ~~The main objective of TOOP is to explore and demonstrate the once-only principle across borders, focusing on data from businesses. Doing this, TOOP wants to enable better exchange of business related data or documents with and between public administrations and reduce administrative burden for both businesses and public administrations.~~
[REF38]	TOOP D23	The Once-Only Principle Project (TOOP) Generic Federated OOP Architecture (3rd version).

1. INTRODUCTION

1.1. Once-Only Technical System

Article 14 of the Single Digital Gateway regulation [REF33] states that the Commission, in cooperation with the Member States, shall establish a technical system for the cross-border automated exchange of evidences between competent authorities in different Member States.

For this system, which from this point we shall refer to as the *Once-Only Technical System*, this document provides a high-level architecture. This architecture is complemented by, and is an introduction to, further technical and operation specifications. References to preliminary versions of these further specifications are provided in this document. Together, these documents are necessary to support the implementation of Article 14. The final form of these documents will be reached by 12 June 2021, when the Commission shall adopt implementing acts for the Once-Only Technical System.

1.2. Context

Preparatory work for the entry into force of the Once-Only Technical System, which is set to be in place and ready for use by 12 December 2023, is organized into a number of Work Packages, operating under the SDG Coordination Group. This document is an output of Work Package 7, "Technical Design", which addresses a range of technical topics. The focus for this Work Package is Technical Interoperability, as defined in the European Interoperability Framework (EIF, [REF1]).

Related, complementary, work packages are:

- WP 2, "User Centricity", which addresses user journeys and use cases for Once-Only. This Work Package adds a User perspective.
- WP 4, "Data Semantics, Formats and Quality", which covers content aspects of evidence exchange. Its main focus is Semantic Interoperability.
- WP 6, "Functionality", which includes a topic "Evidence Exchange" that is closely related to this Work Package.

1.3. Inputs

This document is based on the following inputs:

- Deliverables and other input from the TOOP Large Scale Pilot [REF37].
- Initial feedback from the recently launched DE4A Large Scale Pilot [REF1].
- The "OOP Blueprint" [REF1] created by the preparatory action on once-only. That action, which was started in 2019, intends to pave the way to the creation of a dedicated 'once-only' principle (OOP) building block and the identification of potential new building blocks supporting cross-border interoperability.

- Input from Member State representatives in the SDG Coordination Group, provided during its periodic SDG plenary meetings.

- Input from Member ~~States~~State experts, provided during bilateral meetings scheduled with their representatives in the SDG Coordination Group, but also involving a broader range of experts.

- Input from Member State experts participating in the meetings and discussion item section of WP7, Technical Design.

- Input from policy and subject matter experts in the Commission and from other Commission actions, in particular the ISA² action and the CEF Building Blocks.

1.4. Requirements

Multiple requirements analyses of Once-Only are available and have been input to this document. Among these is the requirements analysis provided by the EU TOOP LSP [REF38].

Further requirements and analysis work is being done in the User Centricity Work Package. Work in this document is closely aligned with the activities and outputs of that Work Package.

1.5. Exchange Pattern

An essential principle of the Once-Only Technical System is to approach once-only using the Request-Reply integration pattern [REF20] from Enterprise Integration Patterns [REF20]:

- Evidence requests are made by Online Procedure Portals in a Member State in the "~~Data Consumer~~Evidence Requester" role;

- Corresponding evidence responses are provided by Data Services in one or several other Member States in the "~~Data Provider~~Evidence Issuer" role.

The actual exchange will happen through the eDelivery building blocks. The exchange itself will follow online interactive user sessions. Note that the acceptance ("exchange") of evidence that is transmitted for use in the context of the procedure is subject to approval of the user.

While other approaches to once-only are possible and are used in similar contexts, this exchange pattern is the pattern specified in Article 14. This will therefore become the default evidence exchange pattern of the OOP technical system.

1.6. Extensibility

~~1.6.1.1. Approach~~

While Article 14 sets a clear functional scope, in detailing the design of the OOP system some attention ~~will~~must be paid to functionality beyond what is strictly required by Article 14. A key objective is to make sure that such additional functionality, if needed in the future, can be added in an incremental way to avoid a major redesign of the initial system of systems. Examples of potential extensions, which are not supported in the current architecture but which could be added relatively easily, are:

- Deferred response option: allows a Data Service to indicate that a requested evidence is not immediately available, but will be available later. This can be useful in situations in which some manual work is needed to prepare the evidence for exchange.

- Subscription and notification option: allows a query to set a subscription and the Data Service to also return future additional evidences that become available as notifications.

- Coupon option: allows an evidence requester to include a code that proves that access to an evidence has been prepaid. This coupon would simply be an additional Slot in the RegRep4 request.

- Data Quality feedback option: if, after retrieval of the evidence, the User or the Requesting competent authority find the evidence is incorrect or incomplete, there should be a mechanism to report this back to the Data Service.

Incremental extensions in the future ~~will be~~are made easier by defining the OOP system, as much as possible, using profiled subsets of more comprehensive open standards. This will allow functionality to be added relatively easily by extending the profiled subsets beyond the requirements in Article 14. The approach of using profiled subsets of standards was used successfully in the eDelivery Building Block, which has been extended in response to new needs without disrupting existing users and deployments.

As of August 2020, the following open Discussion Items relating to the Extensibility are listed at the WP7 Discussion Item page:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-411, Deferred Responses.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-408, Pro-active services.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-406, Support evidence pre-payment using coupon model.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-317, policy for handling data discrepancy.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-305, Explain extensibility of initial architecture and specifications used (currently limited to Art 14) to include more patterns. Role DE4A?

1.7. Scope

This document covers the Once-Only technical system specified in article 14 of the SDG regulation.

This system will come as an addition to several existing systems for cooperation between Member States mentioned in recital (50) of the regulation, which are used to exchange evidence for exchanges that are in the scope of the SDG regulation. If these existing systems will continue to be used after 12 December 2023 for these exchanges, according to Article 14 paragraph 10 this document does not apply to these exchanges.

~~If these existing systems will continue to be used after 12 December 2023 for these exchanges, this document does not apply to these exchanges.~~

1.8. Structure of this Document

This remainder of this document is structured as follows:

- Section 2 Once-Only Technical System Architecture provides a high level overview of Business Layer and Application Layer views. It partitions the elements in the architecture in four groups, which are discussed in the four next sections.
- Section 3 Evidence Requester Architecture Elements covers Consumer-side systems.
- Section 4 Evidence Issuer Architecture Elements covers Producer-side elements.
- Section 5 Once-Only covers supporting infrastructure elements.
- Section 6 Reuse of Existing Building Blocks explains the reuse of some existing Building Blocks.
- Section 7 Core and Extension Architectural elements groups the elements using another perspective, of being a core or extension element.
- Section 8 Roles, responsibilities and organisational arrangements discusses the responsibilities of Member States and Commission regarding elements in the architecture and its overall governance.
- Section 9 Sample Once-Only Flows describes in some detail sample flows involving the Once-Only Technical System.

2. ONCE-ONLY TECHNICAL SYSTEM ARCHITECTURE

2.1. Context

The Single Digital Gateway Regulation [REF33] aims to make it easier for a user (a citizen or an individual representing a business) to initiate and execute a procedure online~~-~~:

- using an Online Procedure Portal of a public administration in another Member State, ~~or~~
- that requires evidence from another Member State.

While carrying out the electronic procedure, evidence relating to the citizen or the represented business may be required. The Once-Only technical system allows the Portal to request, at the explicit request of the user, the exchange of evidences from one or several competent authorities in (a) different Member State(s), for use in the context of the procedure. In the Once-Only technical system, the competent authority that *issues* the evidence acts as a Data Provider. The competent authority that ~~*(re)uses*~~*requests* the provided evidence acts as a Data Consumer. This document provides ~~an~~a high-level architecture for this system.

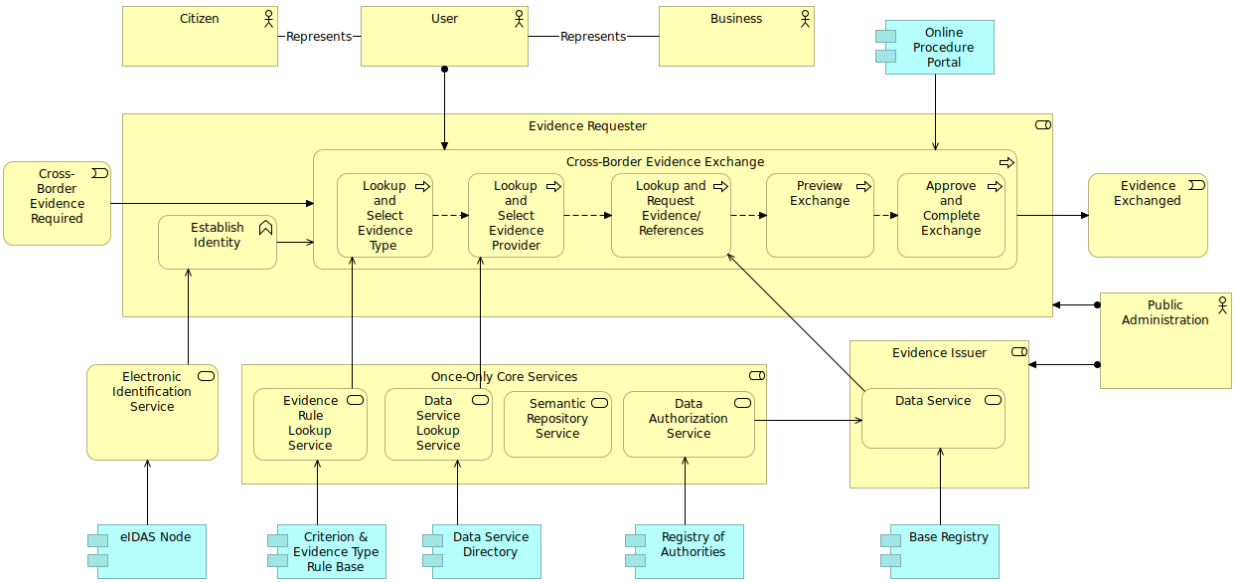
2.2. Approach

The Once-Only technical system is not a single monolithic system. Instead, it is a distributed collection of systems that, once interacting with one another, form a Once-Only technical "ecosystem". Rather than assuming a shared single central information system, the architecture takes a decentralized approach based on integration and interconnection of independent systems. Most of the systems that are part of the Once-Only technical system ~~will be~~are independently operated by Member States, and many of them are likely to be (evolutions of) existing systems that are already in use today, rather than new systems designed specifically for once-only in the SDG context.

To allow interconnection of existing systems in use in Member States, the architecture uses a loosely coupled interoperability layer based on the concept of common reusable "building blocks". Building Blocks provide agreed common interface specifications. They are designed to minimize the impact on existing systems in Member States and to maximize opportunities for reuse. The architecture includes interoperability enabling elements provided by existing building blocks of the Connecting Europe Facility (CEF) such as eID and eDelivery [REF3] and adds additional Once-Only support infrastructure services to provide comprehensive support for once-only.

2.3. Overview

Figure 1 provides a High Level view of the Once-Only technical system.



~~Figure 1 High Level View of the Once-Only Technical System~~

[1] The system as shown provides functionality to establish a transition from two business events:

1. A “Cross-Border Evidence Required” input event that indicates that (an action in) a procedure requires one or more evidences to be retrieved from ~~a~~one or more different Member ~~State~~States. (This will most likely be based on information supplied by the user).

2. An “Evidence Exchanged” output event that occurs when the required evidence(s) has/have been exchanged, where “exchange” implies not just the transmission of the evidence, but also the subsequent consent of the user and the acceptance for use in the procedure.

[1] The sources of all Archimate models in this document are publicly available at https://ec.europa.eu/cefdigital/code/projects/OOP/repos/hla/browse.

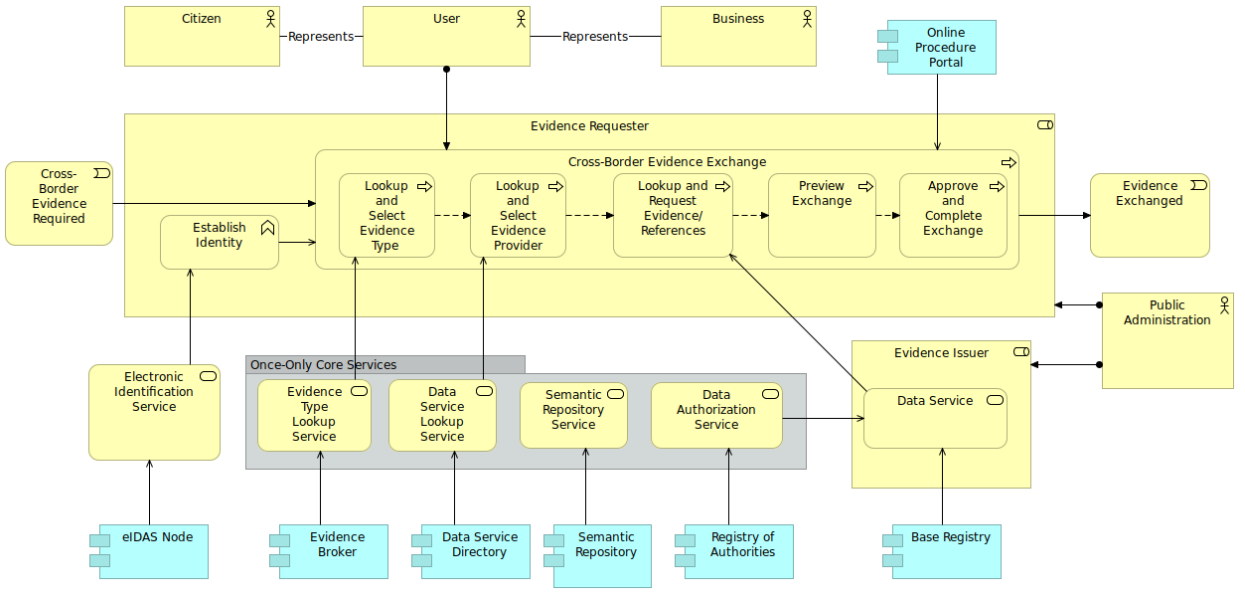


Figure 1 High Level View of the Once-Only Technical System

Formatte

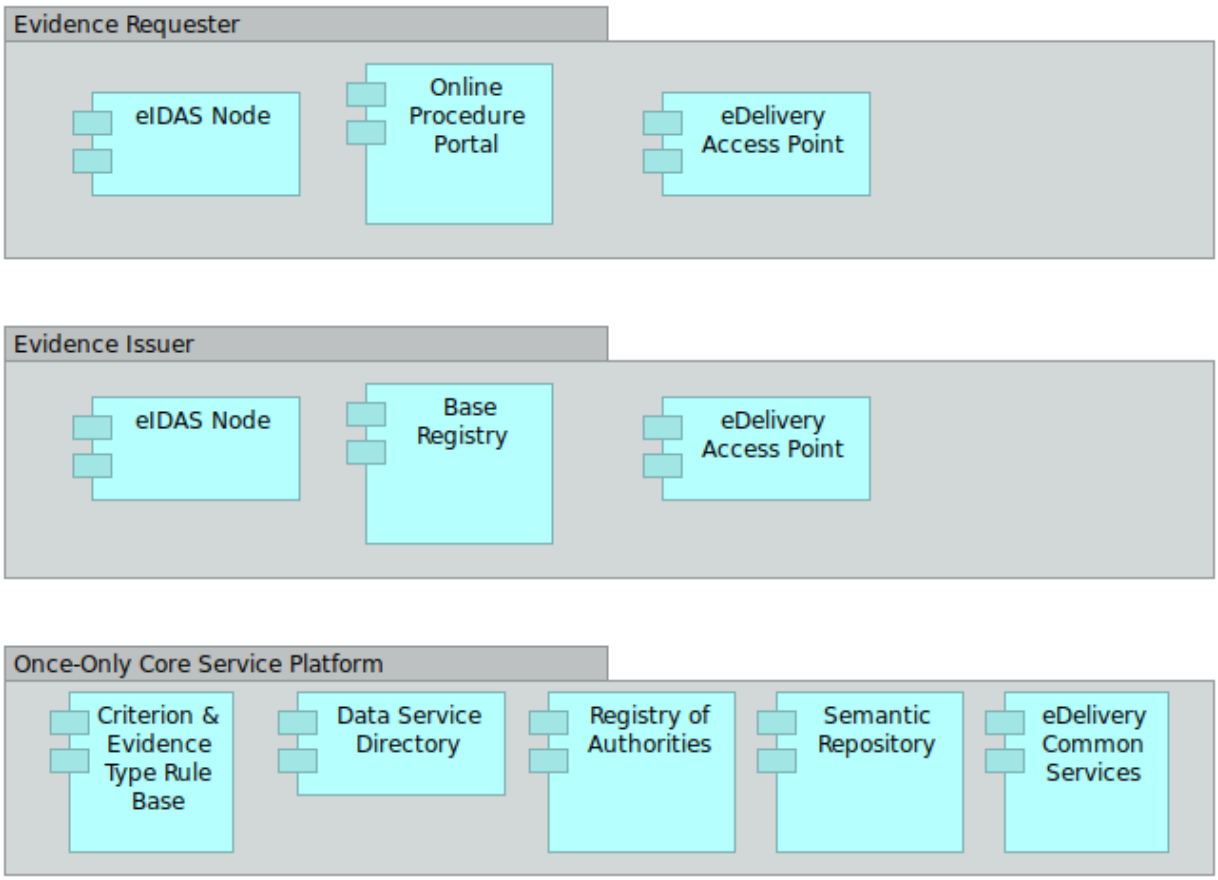
Formatte
Accent 1

Both of these events relate to the competent authority that ~~uses~~requests the evidence(s). They are connected by a business process "~~Apply~~ Cross-Border ~~Once-Only Principle~~Evidence Exchange" that involves multiple interactions with~~-~~:

- the user, ~~with~~
- the competent authority that issues the evidence, ~~and with infrastructure services~~
- Once-Only Core Services that support the operational uses of the ~~once-only technical system~~Once-Only Technical System.

Formatte
0,25" + Ir

~~The business functionality shown in Figure 1 is supported by a range of application components. These components are shown in Figure 2, grouped by whether they are operated for the Member State of the competent authority that *requests* the evidence, or the one that *issues* it, or by being part of the Once-Only support infrastructure.~~



~~**Figure 2 Application Layer Components in the Once-Only Technical System**~~

The business process implements the requirements of SDG Article 14 paragraph 3 and the flow it describes.

As SDG Article 14 paragraph 7 explains, the evidence request is issued by a competent authority but is subject to an explicit request given by the user. It therefore relies on authentication of the user. This is provided by the "Establish Identity" business function that is served by an "Electronic Identification Service". This service may be provided by the eIDAS Node component or by other components (not shown in the diagram), such as the national identification service of the Member State in which the requesting authority is based. Since identification is typically a general requirement for electronic procedures and not for evidence exchange only, it is not modelled as a step in the exchange business process but as a business function that serves it.

The "Cross-Border Evidence Exchange" process consists of the following steps, all initiated from an Online Procedure Portal (see section 3.2):

1. "Lookup and Select Evidence Type" is an optional step in which an "Evidence Type Lookup Service" is used to determine the type of evidence to be retrieved. This service is implemented in a Evidence Broker component (see section 5.2).

2. "Lookup and Select Evidence Provider" is a step in which a "Data Service Lookup Service" is used to determine the competent authority to which the evidence request is made. This is implemented in a Data Service Directory component (see section 5.3).

3. "Lookup and Request Evidence/References" is a step in which a request for available evidences, or references to such evidences, are made to a "Data Service" (see section 4.2). This service is provided by a "Base Registry" component owned by a competent authority that is an "Evidence Issuer". The "Data Service" uses a "Data Authorization Service" to determine if the request is approved. That service is provided by a "Registry of Authorities" component (see section 5.4).

4. "Preview Exchange" is a step in which the user previews the evidence to determine if it can be used in the context of the procedure.

5. "Approve and Complete Exchange" is a step in which the user confirms that the evidence can be used in the procedure.

Of these five steps, the first three involve interaction between IT systems in different Member States. The Once-Only Technical System is based on detailed technical specifications that provide interoperability between these systems. The last two steps only involve the User and the Online Procedure Portal.

The four services "Evidence Type Lookup Service", "Data Service Lookup Service", "Semantic Repository Service" and "Data Authorization Service" together comprise a "Once-Only Core Services Platform". This platform does not handle requests for evidences and their issuance directly but provides foundational supporting services.

Section 3 will discuss the architectural elements relating to the competent authority that ~~uses~~requests the evidence~~, and the Member State it is based in.~~ . Section 4 will similarly do this for the evidence issuing competent authority. Section 5 ~~discuss~~discusses the Once-Only ~~Support Infrastructure~~Core Services and section 6 the existing Building Blocks that are reused in the Once-Only Technical System.

It should be noted that every Member State has its own landscape of frontend systems, backend systems, access points and authentic sources (commonly known as base registries), which will be integrated using the Once-Only Technical System. A "backend system" or "data service", "components" should be understood as potentially including be a collection of different systems, integrated using integration middleware, enterprise service buses, application programming interfaces, different national eDelivery systems etc. It is up to each Member State to consider its own particular set of systems (their number, level of readiness, maturity, etc.) when analysing the impact of integrating them into the Once-Only Technical System.

3. EVIDENCE ~~USE SIDE~~REQUESTER ARCHITECTURE ELEMENTS

3.1. Introduction

A competent authority in a Member State that ~~*uses*~~*requests* evidence operates (or uses a third party to operate on their behalf) an Online Procedure Portal that uses the Once-Only ~~technical system.~~Technical System. This section covers architectural elements involving systems of competent authorities that ~~use~~request evidences.

As an example, a university, or another public administration in the education domain, could provide an Online Procedure Portal to help candidates apply on-line for a tertiary education study financing. A prospective student that previously studied in a different Member State, or even in multiple different Member States, could use this portal to apply and, using the ~~'once-only' technical system~~Once-Only Technical System, provide the university or public administration in the Member State with proof of any relevant existing qualifications s/he obtained from institutions in the other Member State(s).

3.2. Online Procedure Portal

An **Online Procedure Portal** is an online system of a public administration in a Member State that allows users, including cross-border users from other Member States, to execute a procedure of the public administration. This architecture is only concerned with the subset of functionality of an Online Procedure Portal that relates to the cross-border automated exchange of evidence between competent authorities in different Member States and application of the 'once-only' principle as defined in Article 14 of the SDG Regulation. This functionality is provided by the "~~Apply~~ Cross-Border ~~Once-Only Principle~~Evidence Exchange" business process as shown in Figure 1.

Other types of Once-Only evidence exchange, not in scope for this document, include:

- Once-Only functionality that does not involve any cross-border border exchange.
- Cross-border exchange involving private sector sources.
- Evidences directly uploaded by the user.

Requirements of SDG Regulation other than functionality covered by Article 14 are also out of scope.

An Online Procedure Portal typically consists of a separate frontend part handling the user interaction and backend parts implementing the business logic. This is illustrated in Figure 2.

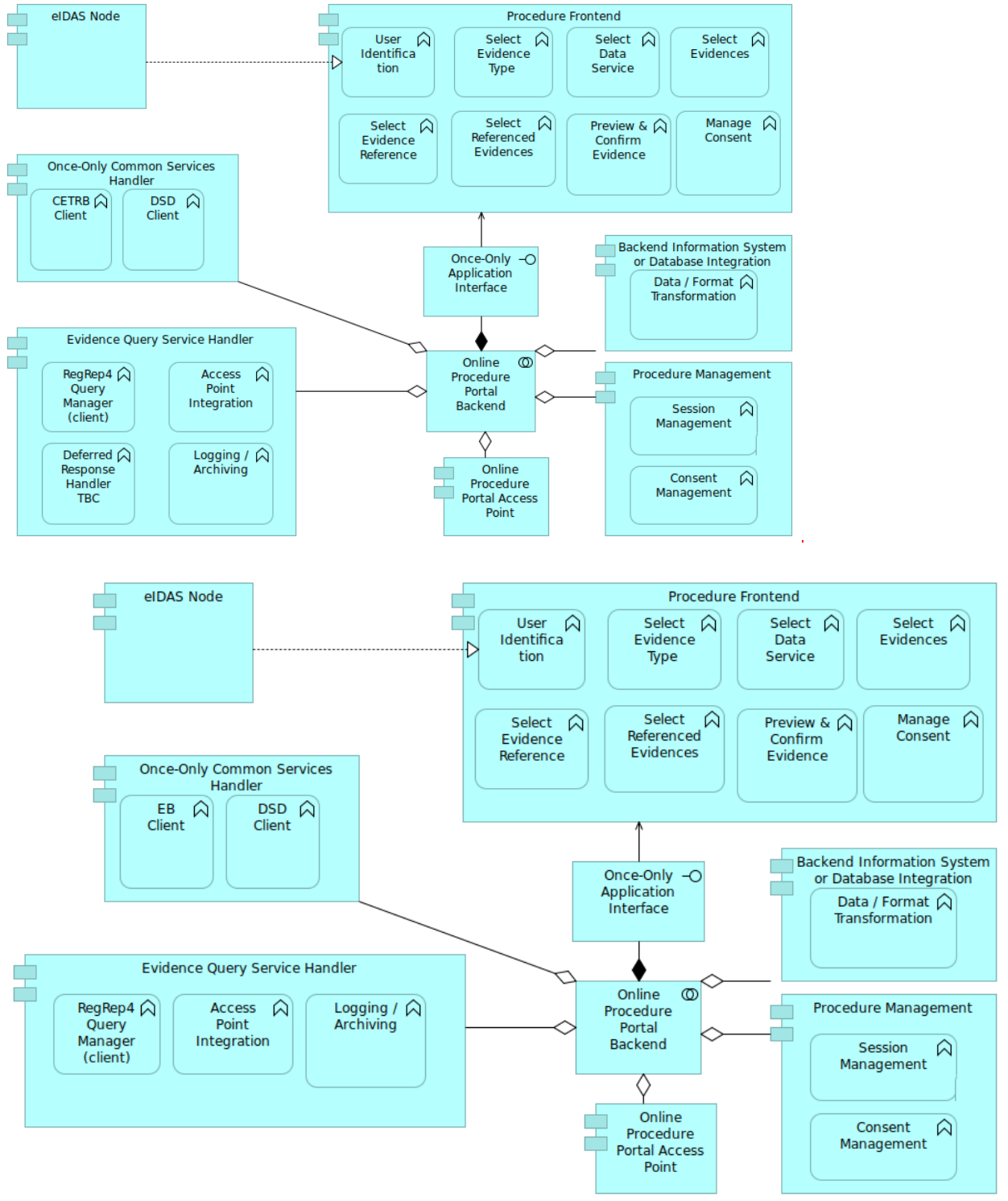


Figure 2 Online Procedure Portal Application View

The Procedure Frontend (for example, a Website supporting a browser or a mobile application) needs to include functions to:

- Identify the user, possibly by making ~~uses~~use of **eIDAS Nodes**.

- Make selections for options among different evidence types (provided by ~~a **Criterion and**~~an Evidence ~~**Type Rule Base**~~Broker), data services (provided by a **Data Service Directory**), evidences or evidence references (provided by a **Data Service**). These selections are further illustrated in the sample flows in chapter 9 and ~~will be further~~are addressed in WP2 "OOP User Centricity".

- Manage consent, e.g. allowing a user to withdraw previously provided consent.

The Online Procedure Portal Backend needs to include functionality to:

- Manage procedure and session state. At a particular point in time, multiple users may be interacting with the system and using the once-only technical system. Any evidences that are returned in response are made available to the specific procedure and user that issued the query for those evidences. Also, user input to the procedure, and evidences retrieved to support it, may be provided over time, and possibly interrupted/resumed.

- Integrate with information systems and/or database and perform any required data or format transformation. This may involve transformation between different structured formats, or from structured (data-oriented) to unstructured (presentation-oriented) formats.

- Create evidence requests and submit them to the **Online Procedure Portal Access Point** for transmission to a Data Service.

- Receive evidence responses, delivered by the eDelivery Access Point, and (after user preview and approval) accept them for use in the procedure.

- Interface with the Central Services ~~**Criterion and**~~ **Evidence** ~~**Type Rule Base**~~**Broker** (if used) and **Data Service Directory**.

- As an alternative to requesting evidences, an evidence reference may be requested. An evidence reference is a structure that provides a unique identifier and some metadata (e.g. a short description). It allows the user to decide if the evidence should be retrieved, without actually retrieving the full content of that actual evidence. This feature can help avoid the transfer of evidences that the User will discard during the preview step.

- The evidence can subsequently be retrieved (if needed) using its unique identifier, following the Claim Check pattern [REF20].

The generic format for evidence requests and response ~~will be~~is based on an Exchange Data Model specification [REF22] based on ~~open standards~~the OASIS RegRep4 specification ~~[REF31]~~[REF29]. The use of RegRep4 with eDelivery AS4 will follow the eDelivery AS4 specification [REF15] and a special-purpose RegRep4 protocol binding specification under development at OASIS [REF1].

In August 2020, input draft specifications are available at http://wiki.ds.unipi.gr/display/TOOP/.TOOP+Exchange+Data+Model+v2+v2.0.1.

Discussion items common to Online Procedure Portal and Data Service are listed in section 4.2.

Specific discussion items relating to the Online Procedure Portal include:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-419, Delivery of result of the procedure.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-307, National Messaging Infrastructure integration, such as XROAD in Estonia etc.

Article 14 requires that the user has the option to preview any retrieved evidence and is to be requested to explicitly confirm whether the previewed evidence is used for the procedure, allowing the user to be in control on the execution of the procedure. User confirmation to use evidence in the context of a particular procedure does not constitute a blanket authorization to use the provided evidence in other contexts or for other purposes.[2]

3.3. Online Procedure Access Point

An Online Procedure Portal uses an eDelivery **Access Point** to request the evidence from the evidence ~~source~~issuer and receive the evidence in response. This Access Point may be dedicated for the specific Portal, or a more general communication component that is also used by other applications. For further discussion, see section 6.2.

3.4. eIDAS Node of Evidence Using Member State

Services of public administrations in the Member State of the competent authority that uses evidence may allow use of the national eID infrastructure for identification of users who possess an eID in a different Member State. If the user is a citizen or business representative from a different Member State and has an eID from that Member State, the **eIDAS Node** of the two Member States can be used for cross-border authentication.

This functionality will be accessed from the frontend part of the Online Procedure Portal as it involves interaction with the user. All other interactions with the Once-Only ecosystem are handled by the backend parts of the portal. Essentially however, at various steps in the exchange the user must be involved, for example to select among multiple options, to preview evidences that are retrieved, and to approve (or not to approve) their use in the context of the procedure. For more on eIDAS nodes, see section 6.3.

[2] The topic will be further explored in the topic “Explicit Request” in the context of Work Package 6 on OOP Functionality.

4. EVIDENCE ~~ISSUING SIDE~~ISSUER ARCHITECTURE ELEMENTS

4.1. Introduction

A competent authority that *issues* evidences in ~~request~~response to evidence ~~responses~~requests provides **Data Services** as specified in section 4.2. The transmission of requests and evidences uses eDelivery Access Points as specified in section ~~0.~~4.3. This section covers architectural elements involving systems of competent authorities that issue evidences.

4.2. Data Service

Competent authorities in Member States operate **Data Services** to issue evidences, in response to requests from Online Procedure Portals. For example, the Ministry of Education in one Member State may offer a service that provides evidences concerning diplomas, certificates or other proof of studies or courses obtained in that Member State that can be shared with other Member States through the OOP system.

A Data Service must implement two standardized once-only application services, an "Evidence Query Service" and an "Evidence Retrieve by Id Service". These services are based on the OASIS RegRep4 standard [REF29]. In support of these services, a Data Service includes functionality to:

- Receive evidence requests, delivered by an eDelivery Access Point, and interpret them. These requests are the input to the "Evidence Query Service".
- Interface with the Registry of Authorities (see section 5.4) to authorize evidence requests.
- Subject to successful authorization, retrieve any evidences (or evidence references) matching the request.
- Return evidence responses (including possibly errors) and submit them to an eDelivery Access Point for transmission to the requesting Online Procedure Portal.
- If an evidence reference is requested (instead of an evidence), the response includes evidence identifiers instead of actual references. This relates to the "Evidence Retrieve by Id Service".
- The Data Consumer may follow up on this by requesting the evidence using the provided identifier.

The generic format for evidence requests and response will be based on an Exchange Data Model specification [REF22] based on open standards.

The generic format for evidence requests and responses is based on an Exchange Data Model specification [REF22] based on the OASIS RegRep4 specification [REF29]. The use of RegRep4 with eDelivery AS4 will follow the eDelivery AS4 specification [REF15] and a RegRep4 protocol binding specification under development at OASIS [REF1].

A draft specification for Evidence Exchange is available from the TOOP LSP [REF22]. This work is based on the OASIS RegRep4 open standard and ISA specifications.

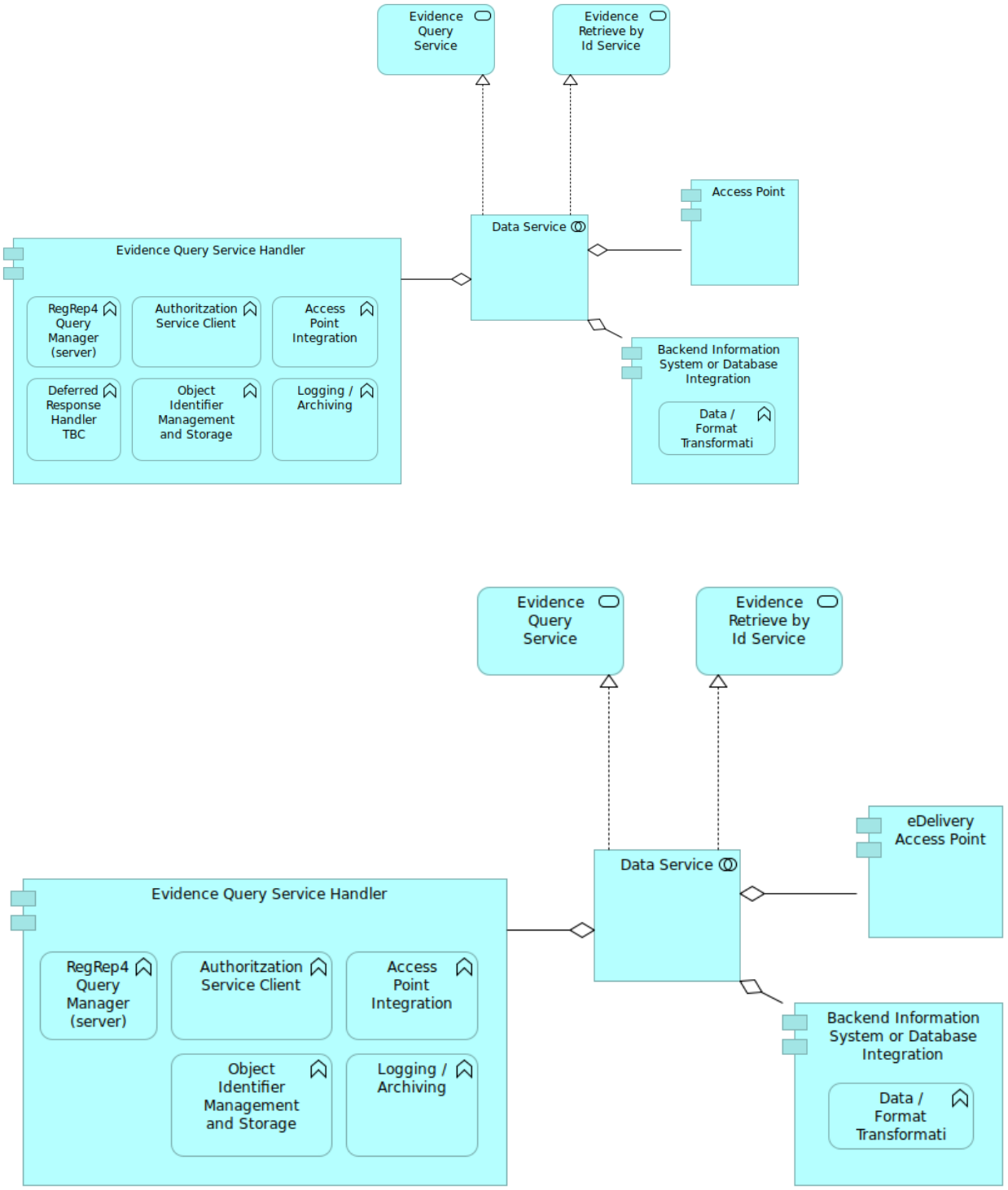


Figure 3 Data Service Application View

Formatte

As of August 2020, the following open Discussion Items relating to the Data Service and its interaction with the Online Procedure Portal using Evidence Exchange are listed at the WP7 Discussion Item page:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-405, Mechanism to encode user consent in evidence requests
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-313, Legal entitlement of the authority request data - where will it be recorded? Who will validate it? Maintain?

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-412, Include Data Provider as Slot in RegRep4 evidence request messages.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-468, Mandates, how to represent them, where to validate them.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-417, Code List of Evidence Types.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-410, Code List for Request Purpose.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-420, Use "Evidence Service Directory" instead of DSD and "Evidence Service" instead of "Data Service"?
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-307, National Messaging Infrastructure integration. For example, XROAD in Estonia etc.

4.3. Data Service Access Point

The requests to a Data Service and the responses to those requests are exchanged securely and reliably using eDelivery. The Data Service must therefore also be accessible via an eDelivery **Access Point**. This Access Point may be dedicated for the specific Data Service, or a more general communication component that is also used by other applications. For further discussion, see section 6.2.

4.4. eIDAS Node of Evidence Issuing Member State

As mentioned in section 3.4, the eIDAS Node of the Member States from which evidences are requested may be used to authenticate the user. This is initiated via the eIDAS Node and Online Procedure Portal from which the evidence is requested. For more on eIDAS nodes, see section 6.3.

5. ONCE-ONLY ~~SUPPORT INFRASTRUCTURE ARCHITECTURAL ELEMENTS~~CORE SERVICES

5.1. Introduction

To support the exchange of evidences between **Data Services** and **Online Procedure Portals**, five sets of supporting ~~infrastructure services~~Once-Only Core Services are provided. In addition to one existing set of **eDelivery Common Services**, four of these are specific to Once-Only exchange.

~~Criterion and~~ As of August 2020, several open Discussion Items relating to the Data Service Directory are listed at the WP7 Discussion Item page. The ones for specific services are included in the following subsections.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-421, API to synchronize data with central services (data management/LCM)
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-403, Multiple instances of a Core Service per MS?
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-402, DNS-based discovery mechanism for Core Services.

5.2. Evidence ~~Type Rule Base~~Broker

~~When~~The Once-Only Technical System supports situations in which an Online Procedure Portal, when performing an online procedure, ~~the Online Procedure Portal may need~~requests an evidence ~~that proves that a specific criterion is met by~~ from a data service in a different Member State. The evidence relates to a requirement to obtain information on a citizen or ~~by a~~ business~~. In some domains, or in the context of some procedures~~ or to prove that certain claims about the citizen or business are true.

If, for a particular situation, for a particular requirement, a harmonized ~~set of~~ evidence ~~types~~type (and associated ~~schemas) may be~~ schema) is defined and agreed ~~for use among~~ by the Member States~~. This approach is similar to the one used in many successful existing cross-border data exchange systems in the EU and is therefore preferred wherever possible.~~, it is known to all which evidence type is to be requested. For this situation, the choice of evidence type can be “hard-wired” in the implementation of an Online Procedure Portal and is independent of the specific Member State that provides the evidence. The Portal can use the Data Service Directory (see section 5.3) directly to retrieve the list of issuers of this evidence type in the other Member State.

However, ~~in other situations, for a given criterion it may not be possible for Member States to agree on a single harmonized evidence type, as the rules that express which evidence (or combination of evidence or evidence alternatives) applies to a particular criterion, and in which formats it is available, differ among different Member States.~~

~~The OOP system~~ the Once-Only Technical System also supports situations in which there is no ~~use of harmonized evidence types by providing a~~single agreed evidence type that is harmonized across the EU and that all Member States can provide. The type of evidence that is used in the Member State that requests the evidence may not exist in other Member States. However, that Member State may be able to provide an "equivalent" evidence type, or even multiple "equivalent" types. Here, "equivalence" is used in the informal sense as expressing that the other type(s) can be used to prove the same claim about the citizen or business, or that the evidence type provides the same required information, as the evidence type used in the Member State from which the request is made. In this case, the procedure can be executed using the alternative evidence type(s).

It is impractical to assume an Online Procedure Portal in a Member State knows in advance which type of evidence to request, not just because this may differ for each of the many other source Member State but also because the rules underlying the equivalence may change over time. Therefore, the Once-Only Technical System provides a service, the Evidence Broker service, which allows an Online Procedure Portal in a Member State to determine which evidence type it may request from another Member State, for a particular purpose in a particular context.

This Evidence Broker service is based on rule content, provided by the Member States themselves, and provides an on-line mechanism for Member States to align and query their information requirements and evidence ~~and criteria~~type sets, obviating the need for full EU-level harmonisation of procedures or evidences. ~~This mechanism is expected to be provided by an updated version of the Core Criterion and Core Evidence Vocabulary, launched by ISA2 SEMIC team [REF32], appropriately adapted to meet OOP needs.~~

~~The resulting **Criterion & Evidence Type Rule Base** system will allow~~ The Evidence Broker allows Member States to manage and share information about rules relating evidence types ~~to criteria~~ in Member States, in particular for standardised types of evidence ~~(e.g. birth certificates)~~ that do not require a detailed substantial assessment. ~~The~~Note that, for any evidence type, equivalence is relative to the purpose for which, and context in which, it is used.

The data model and concepts used in the Evidence Broker is defined in the Core Criterion and Core Evidence Vocabulary (CCCEV), provided by the ISA2 SEMIC team [REF32]. A future updated version of the eCertis system [REF10] is under consideration as a basis for the Evidence Broker implementation. This system has an API that can be used to query the rule content [REF11]. The Evidence Broker system should also provide a management interface to allow Member State representatives to create and update rules relating criteria to evidences interactively.

In case ~~a rule states that~~where there are multiple alternative options ~~that meet~~for a particular ~~criterion~~requirement, the ~~user~~Online Procedure Portal may ask the User to help decide to select which (if any) alternative option will be used, allowing the user to be in control on the execution of the procedure.

A draft specification for the Evidence Broker is available from TOOP [REF9].

As of August 2020, the following open Discussion Items relating to the Evidence Broker are listed at the WP7 Discussion Item page:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-278, Define who /how to take care of the rules of criteria and evidence type rule.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-410, Code List for Request Purpose.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-417, Code List of Evidence Types.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-466, EB, allow parameters to narrow search

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-467, Granularity and variations of Evidence Types in DSD and EB

5.3. Data Service Directory

To request evidence electronically available from a Data Service in a different Member State, the portal of a public administration in a Member State needs data about the Data Service (such as the relevant eDelivery routing identifier) in the other Member State that may provide the evidence. The OOP system ~~will include~~includes a **Data Service Directory** system which ~~will allow~~allows Member States to manage and share this information in a structured format.

~~Interface format specifications for the Data Service Directory are under development in collaboration with the TOOP LSP [REF10]. This work is based on the OASIS RegRep4 open standard and ISA specifications.~~

In case the Data Service Directory indicates that multiple Data Services may provide the specified evidence type, the user may help decide to select which (if any) of them will be queried, allowing the user to be in control on the execution of the procedure.

A draft specification for the Data Service Directory is available from the TOOP LSP [REF8]. This work is based on the OASIS RegRep4 open standard and ISA specifications.

As of August 2020, the following open Discussion Items relating to the Data Service Directory are listed at the WP7 Discussion Item page:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-279, Identification of the authorities - a central register? What data? Integration with SDG data model.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-404, For DSD, use selection parameters in request to limit result set.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-409, DSD, should it indicate which user/data subject attributes are needed in queries?

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-413, Should DSD and ROA be combined into a single component?

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-414, Should DSD consult ROA before returning its list of data services?

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-417, Code List of Evidence Types.

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-421, API to synchronize data with central services (data management/LCM).

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-467, Granularity and variations of Evidence Types in DSD and EB.

5.4. Registry of Authorities

To comply with the EU General Data Protection Regulation [REF23], Data Services in Member States are required to determine whether a particular public administration in another Member State is allowed to ask for a certain requested type of evidence in a particular context. This is facilitated by a central **Registry of Authorities** that lists, for public administrations in EU Member States, the procedures for which these administrations are authorized to request which types of evidence. The Registry of Authorities can complement, and provides a context for, but is not a replacement of, the explicit request/input of the user.

~~The~~Parts of the functionality of this component may be provided by a future version of the existing IMI system [REF24].

A draft specification for the Registry of Authorities is available from the TOOP LSP [REF30].

As of August 2020, the following open Discussion Items relating to the Registry of Authorities are listed at the WP7 Discussion Item page:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-279, Identification of the authorities - a central register? What data? Integration with SDG data model.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-293, What is the link from OOP to IMI as fallback or complementary system? Can parts of IMI be reused?
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-413, Should DSD and ROA be combined into a single component?
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-414, Should DSD consult ROA before returning its list of data services?
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-415, ROA, what mechanism/logic is used to structure authorization information.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-416, ROA, for structured evidences/concepts, is authorization per evidence type or per attribute?
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-417, Code List of Evidence Types.
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-420, Use "Evidence Service Directory" instead of DSD and "Evidence Service" instead of "Data Service"?

5.5. Semantic Repository

In order to achieve semantic interoperability, Member States need to make detailed agreements on the semantics of evidence types that are to be exchanged using the OOP Technical System. The **Semantic Repository** supports this by storing and sharing definitions of names, definitions and data types of data elements associated with specific evidence types. This Repository is not used in the run-time exchange of evidences. Its purpose is only to support design and implementation by Member States of systems consuming or providing evidences.

At the time of writing the architectural specification of the Semantic Repository is in an initial state. A draft specification for the Evidence Broker is available from TOOP [REF31].

The following open Discussion Items relating to the Registry of Authorities are listed at the WP7 Discussion Item page:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-469, Semantic Repository.

5.6. eDelivery Common Services

Depending on the chosen topology, the eDelivery Building Block can be configured using a static set of configuration parameters or using dynamic discovery. Static configuration is well-suited to situations in which a relatively small and static number of competent authorities are interconnected using the OOP system.

If eDelivery is configured using dynamic discovery, it is recommended to use the **eDelivery Common Services** to locate the metadata service of the Access Point of receivers [REF5].

Furthermore, the Public Key Infrastructure (PKI) common service may be used to secure the eDelivery exchanges [REF4].

Formatte

5.7. Deployment Options

The Once-Only Core Services as described in this section can be deployed in various ways, including:

- The European Commission could operate a single EU-wide central service for the Member States, containing data for all Member States (*centralized*).
- Each Member States operates one instance of the service for its data (*decentralized*).
- A combination of the two, in which some Member States choose to operate an instance of the service and the EC operates an instance for the other Member States (*hybrid*).

Member State representatives have been asked to form their views on these options. A discussion document with more information has been provided to Member States via the Collaborative Space, https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=225544634, as input to support them in making their impact assessment.

6. Reuse of Existing Building Blocks

6.1. Introduction

The architecture of the Once-Only Technical System reuses the eDelivery and eID building blocks.

6.2. eDelivery

The Once-Only technical system reuses the eDelivery Building Blocking [REF13] and uses its Acccess Point [REF14] specification. See Figure 4 for an overview of its functions.

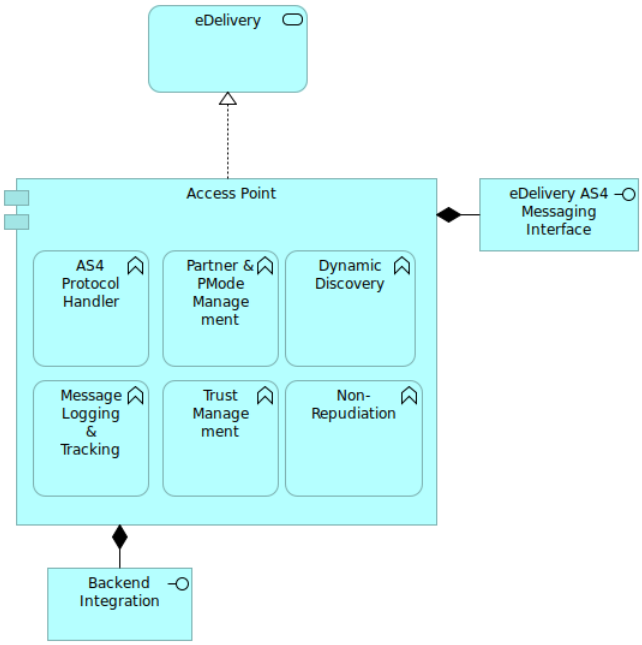


Figure 4 Access Point Application View

An Access Point in the Once-Only Technical System performs key security and reliability functions. It signs and encrypts messages and, in a delegated role, provides integrity, confidentiality, authenticity and non-repudiation of origin and receipt as explained in the CEF Security Controls guidance document [REF16].

The eDelivery AS4 interface specification is based on the eDelivery AS4 Profile [REF15] specification which profiles OASIS AS4 [REF27], which is a profile of OASIS ebMS3 [REF28]. The specifications of the content of evidence request and response payloads are provided [REF22], [REF29] and were already mentioned in sections 3.2 and 4.2. A specification on using these data formats with AS4 will be provided and is intended to be standardized [REF1]. Finally, specific configuration parameters for use of eDelivery AS4 will be provided. These specification parameters reflect decisions on use of any Profile Enhancements (e.g. the Four Corner Typology) and whether static configurations or dynamic discovery will be used.

At the time of writing, no specific constraints have been defined on the topology of eDelivery nodes for use in the context of the OOP technical system. This means that, unless a further decision is made by the Single Digital Gateway (SDG) Coordination Group according to the appropriate governance arrangements, Member States are free to decide to have one or several eDelivery Access Points. A Member State may therefore deploy a single Access Point covering all OOP related eDelivery messaging. Alternatively, it may deploy multiple Access Points at any hierarchical or geographic level of the public administration, in addition to possibly being specialized for specific domains. These considerations apply both in the context of Online Procedure Portals and of Data Services.

Message exchange using eDelivery can use either the Internet or private networks like TESTA. The OOP system can use the public Internet as eDelivery secures OOP messages at both transport layer and message layer, and provides integrity, authentication, confidentiality and non-repudiation of origin and non-repudiation of receipt. This level of protection is comparable to the use of a private network. Choice of communication network is a deployment issue, to be decided between competent authorities. Potentially different decisions are made for different domains and/or evidence types, and are not an intrinsic aspect of the overall architecture.

As of August 2020, the following open Discussion Items relating to eDelivery are listed at the WP7 Discussion Item page:

- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-292, Will OOP use the TESTA or other private networks, or the Internet?
- https://ec.europa.eu/cefdigital/tracker/browse/SDGOO-311, How to guarantee that the needed data was transferred?

6.3. eIDAS Node

Use of eIDAS nodes is discussed in sections 3.4 and 4.4. The purpose, use and specifications of eIDAS Nodes are specified in the existing, separate eID Building Block [REF19]. They are simply reused in the once-only context.

Note that the User Authentication Work Package is also looking in cases in which the national authentication system may be used instead of the eIDAS Node.

7. CORE AND EXTENSION ARCHITECTURAL ELEMENTS

The following elements are core elements as they are used for all once-only exchanges:

- Online Procedure Portal
- Data Service
- Data Service Directory
- eDelivery Access Points
- Registry of Authorities

Other elements of the architecture are extension elements, as their functionality is not always needed, or can be integrated in some another element.

- The user may authenticate to the Online Procedure Portal of a public administration in a Member State using an authentication mechanism of that Member State, thus obviating the need to use eIDAS nodes.
- In some procedures, ~~no Rule Base may be needed~~there is no need for Evidence Broker functionality to determine evidence types to select. This is the case for a procedure in which Member States have agreed to all use the same evidence types. In that case, an Online Procedure Portal can directly ~~request an evidence from a~~look up Data Services in the Data Service Directory without having to first look up a rule for a particular criterion.

A third group concerns recommendations made in this current proposal. These elements are still subject to discussion and approval as, in principle, the same functionality could also be provided by alternative means.

- The Semantic Repository provides a central service for sharing semantic assets. These assets support system design only and are not used for run-time exchange. These assets can also be shared among stakeholders in other ways, not requiring a common repository.
- When using static configuration for eDelivery, some of the eDelivery Common Services are not needed.

8. ROLES, RESPONSIBILITIES AND ORGANISATIONAL ARRANGEMENTS

The Once-Only Technical System is a collection of interacting technical systems of the Member States and the Commission. , According to SDG Article 14 paragraph 11, the Commission and each of the Member States shall be responsible for the development, availability, maintenance, supervision, monitoring and security management of their respective parts of the technical system.

Different entities are responsible for different parts of the overall system. Once final, this chapter will contribute to a future version of the guidelines for the implementation of the single digital gateway Regulation [REF35]. The roles, responsibilities and organisational arrangements of public administrations in Member States and the Commission are in the process of being defined and will be elaborated in the course of further joint preparatory work.

Stakeholders in EU Member States, supported by the Commission, are expected to contribute as follows:

- Provision and integration of technical systems in EU Member States:
    - Operation of an eIDAS Node, in order to allow users from other Member States to authenticate.
    - Deployment, operation and configuration of one or more eDelivery Access Points for national Online Procedure Portals and Data Services and integrating them to the central eDelivery services (if used). All configurations shall be based on agreed technical specifications.
    - Design, development, operation and maintenance of national Online Procedure Portals, providing once-only integration to the eIDAS Node, to eDelivery Access Points and to the central services Criterion and Evidence Type Rule Base and Data Service Directory for procedures specified in the SDG regulation. All integrations shall be based on agreed technical specifications, and will align with semantic assets stored in the Semantic Repository.
    - Design, development, operation and maintenance of national Data Services, providing once-only integration to eDelivery Access Points and to the central service Registry of Authorities, for evidences that may be requested in the context of procedures specified in the SDG regulation. All integrations shall be based on agreed technical specifications.
- Data Provision to Central Services:
    - Provision of data relating to competent authorities in their Member State to the central services Criterion and Evidence Type Rule Base, Data Service Directory, Registry of Authorities and (if used) Semantic Repository.
- OOP System Lifecycle Management:
    - Contribution to the definition and maintenance of OOP technical specifications, according to agreed governance procedures.
- Stakeholder community participation:

  - Participation in all relevant required joint activities with stakeholders in other Member States and with the Commission, including but not limited to planning, testing, evaluation, preparation, promotion.

- Compliance:
  - Ensuring compliance with all applicable regulations relating to the exchange and use of evidences, including but not limited to data protection and security.

The Commission, in collaboration with stakeholders in Member States, is expected to contribute as follows:

- Provision of Central Services:
  - Design, development, operation and maintenance of the central services Criterion and Evidence Type Rule Base, Data Service Directory and the Registry of Authorities, which Member States will access using agreed interface specifications.
  - Design, development, operation and maintenance of the Semantic Repository service that may be used by public administrations in Member States in the design of operational elements in the OOP System.
- eDelivery:
  - Design, development, operation and maintenance of central services for eDelivery, if used, considering conformance testing as well (the ISA^2 testbed experience could contribute to this potential future activity).
- OOP System Lifecycle Management:
  - Definition and maintenance of OOP technical specifications as well as specifications for reusable Building Blocks including eID and eDelivery, according to agreed governance procedures. Considering Conformance testing should be offered as well to ensure correct implementation (the ISA^2 testbed experience could contribute to this potential future activity).
- Stakeholder community support:
  - Participation in all relevant required joint activities with stakeholders in Member States.
  - Provision of support to stakeholders in Member States for implementing the OOP technical system. NB: exact nature and degree of support is yet to be determined.

9. SAMPLE ONCE-ONLY FLOWS

9.1. Sample Flow

The sequence diagram in Figure 5 shows a sample execution flow of a procedure by a user that involves the use of the Once-Only technical system. It is provided as an illustrative example only.[3]

For expository purposes, the diagram shows a single successful flow. At many stages there is more than one potential next step, including error situations. Only one next step, which is not an error, is shown in the diagram. Furthermore, the use of eID (using eIDAS nodes) and eDelivery (using Access Points) is omitted from the diagram. Refer to chapter 9.3 to see how use of eDelivery Access Points can be represented.

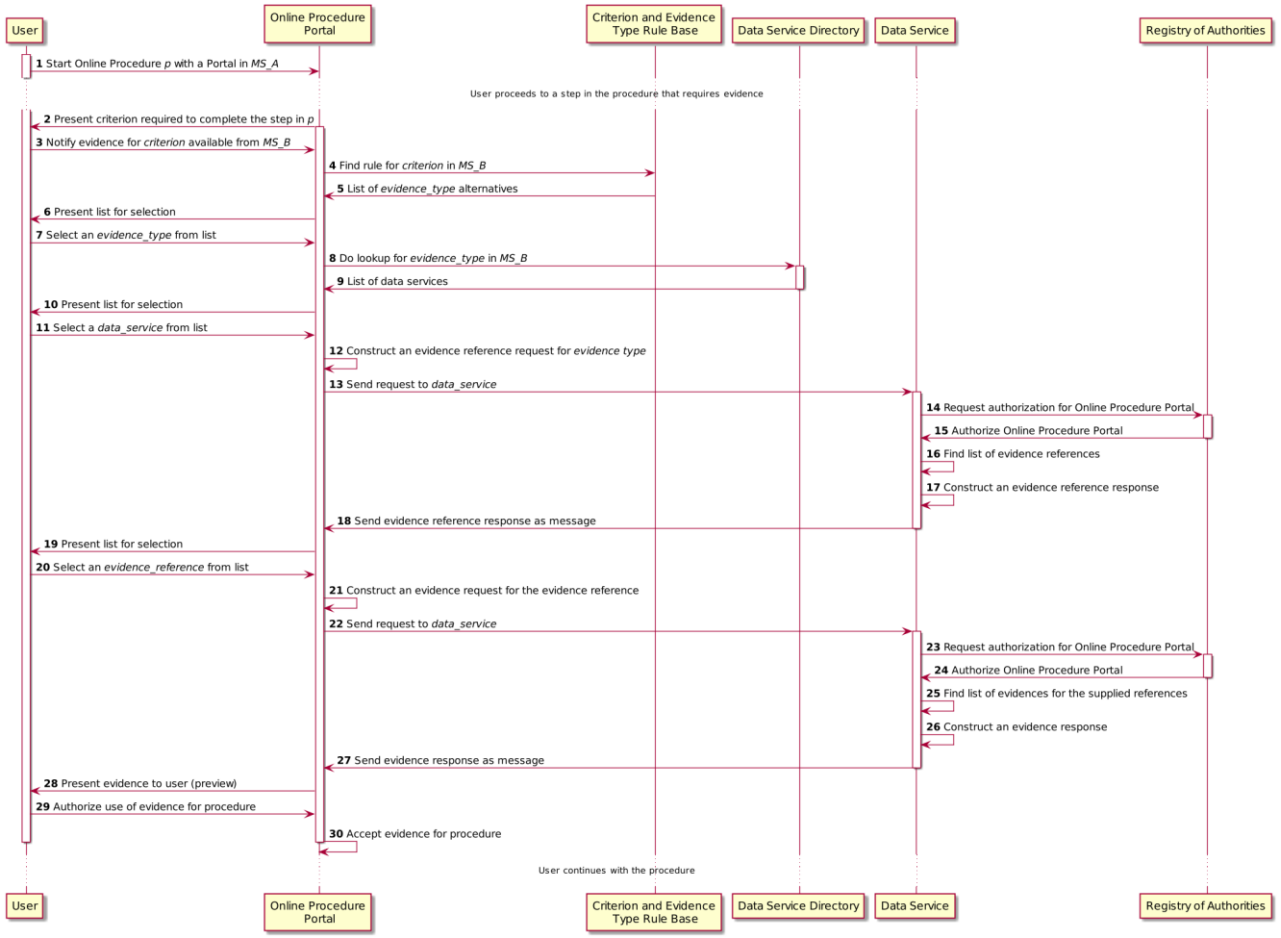
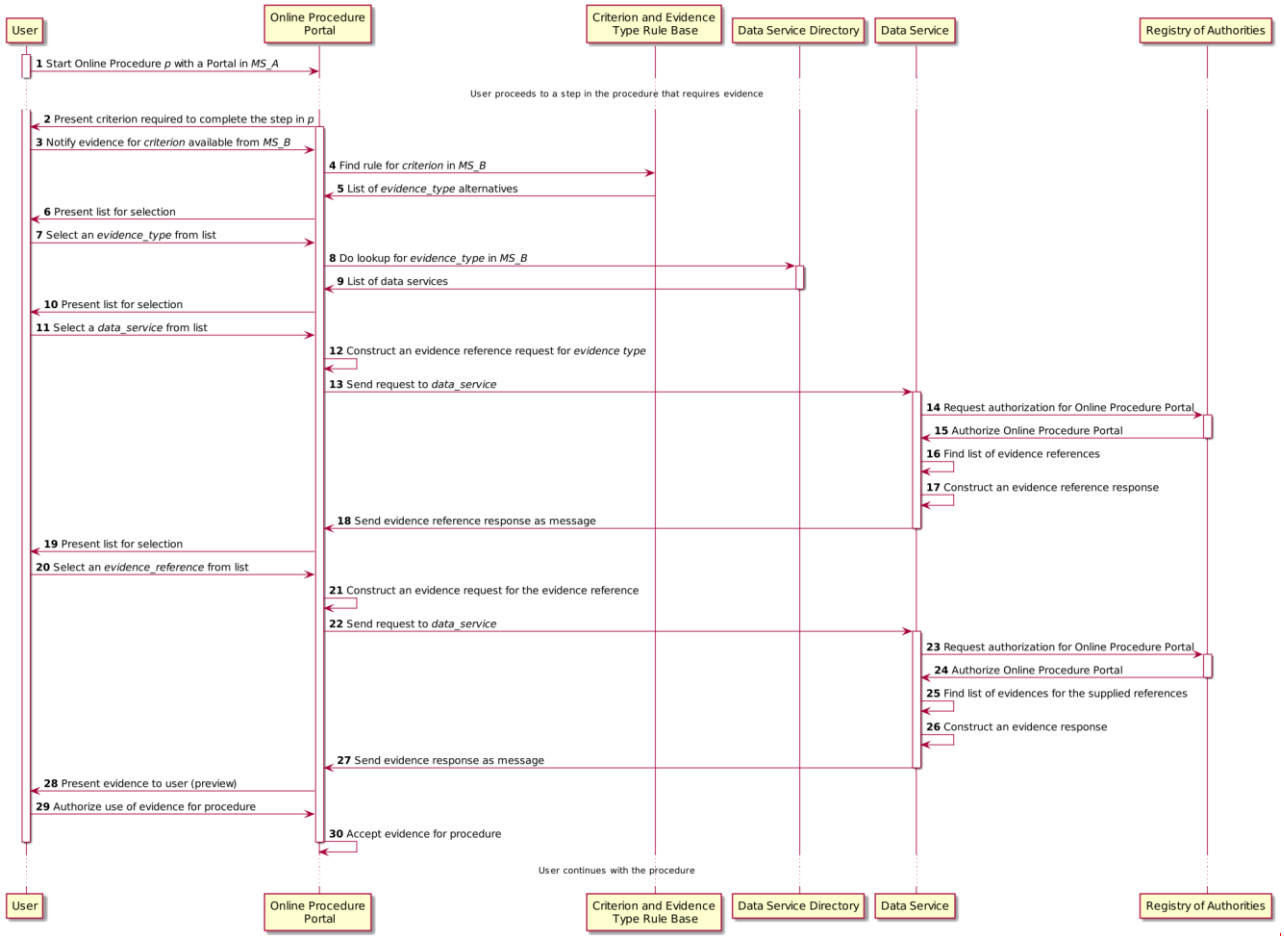


Figure 5 Once-Only Technical System Flow

[3] The sources of all UML models in this document are publicly available at https://ec.europa.eu/cefdigital/code/projects/OOP/repos/hla/browse.

The diagram shows an approach that maximizes interaction with the User. This goes beyond the strict requirement of Article 14, which only mandates the preview feature, but ~~is arguably desirable with the overall aim of user centricity~~it follows the principle of giving the user full control how the Once-Only Technical System operates.[4]

~~The diagram includes the Criterion and Evidence Type Rule Base, which may not be used in a specific case as explained in section 7.~~



~~**Figure 6 Once-Only Technical System Flow**~~

The following table provides a bit more explanation about the steps in the sequence.

Step	Description	Notes
1	Unless otherwise provided under Union or national law, any Once-Only operation starts by a User who initiates an electronic procedure provided by an Online Procedure Portal in a Member State. The procedure may involve many different steps, and a complex logic potentially involving conditional	The User may have found the Portal via the "Your Europe" portal, or some other way. It is not important for the functioning of the Once-Only Technical System.

[4] Work Package 2 "User Centricity" will further elaborate on the role of the User in the Once-Only technical system.

Step	Description	Notes
	branching, loops etc.	
2	In the execution of the procedure, the User may arrive at a point at which ~~one or more criteria~~evidences are to be provided to provide required information or to prove that certain conditions are met. For example, the procedure "*apply on-line for a tertiary education study financing*" may require "*proof of any existing qualifications for tertiary education*". At this point, the portal may interact with the User to obtain evidence that proves the requested criterion. The Portal may support multiple ways to provide this evidence. For evidence that is available using the Once-Only system, the Portal may ask the User to indicate in which (if any) other Member State(s) such evidence can be found.	Step (2) – (30) could be repeated for each of the points in the procedure at which evidence is to be provided.
3	In this sample flow, the User indicates that the relevant evidence ~~proving the criterion~~ can be retrieved from another Member State.	The sample Portal asks the user for the Member State from which evidence is to be requested. Alternatively, the Portal may query all Member States, but this is not recommended as it would result in a large amount of unnecessary queries.
4	The Portal, with this User-provided information, proceeds to consult the ~~Criterion and~~ Evidence ~~Type Rule Base~~Broker to check ~~if there is a rule defining evidences that relate to this criterion in~~which types of evidence should be selected from the specified Member State.	The sample Portal is assumed to be designed to ~~distinguish criteria and evidence~~use the Evidence Broker. For some procedures and/or evidences, Member States may have agreed on a predefined set of harmonized evidence types. In that case, steps (4), (5), (6) and (7) can be omitted, and the Portal can directly go to step (8).
5	In response, the ~~Criterion and~~ Evidence ~~Type Rule Base~~Broker indicates that in the Member State from which evidence is requested the ~~criterion~~information requirement can be met using either evidence type *ET1* or evidence type *ET2*. For example, a structured electronic diploma	

Step	Description	Notes
	based on the EDCI data model [REF12] or a PDF scan of a paper diploma with minimal metadata.	
6	The Portal displays the results of its interaction with the ~~Criterion and~~ Evidence ~~Type Rule Base~~Broker and ~~ask~~asks which (if any) of the ~~evidences~~evidence types should be requested.	The portal takes advantage of the fact that the User may know which evidences are or aren't available. This may avoid some unnecessary queries. The Portal may also simply query ~~both~~ *ET1* and/or *ET2,* without asking user input, skipping steps (6) and (7).
7	In this sample flow, the User knows that only type *ET2* is available and therefore indicates that evidence type *ET1* does not have to be requested.	Note that the user may still select more than one option.
8	Now that (pairs of) evidence type and Member State to be requested are identified, the Portal can consult the Data Service Directory to determine which competent authorities in the Member State provide this type of evidence.	If the Member State is not known, the Portal may also search for Data Services in any Member State. However, in practice the number of Member States a User may have relevant evidence in is likely to be small, so this would create a large amount of unnecessary message traffic.
9	The Data Service Directory returns a list of Providers of the selected evidence type.	
10-11	Similarly to (2)-(3) and (6)-(7), the Portal may allow the User to select one or a subset of items of the list. For example, if individual educational institutions in a Member State are separate Data Services, the list could be quite long, and the User could indicate which of them may hold evidence.	If there is only one Data Service for the evidence type in the Member State, the check with the User may be omitted. It is still possible to query all Data Services, but, as before, it could result in many unnecessary requests.
12	For the selected Data Service(s) in the selected Member State(s), a request is constructed using the evidence exchange data model and format [REF22]. This request is subsequently sent to the Data Service.	Steps (12)-(20) need to be repeated for each selected provider of each selected evidence type. The diagram omits the use of Access Points

Step	Description	Notes
	As discussed in ~~section 2.2.1 and~~ [REF22], the Once-Only system offers as an option a two-step retrieval, in which in a first step evidence identifier references and some short description are requested. Then, in a second step, (some of) the evidences can be requested using their identifier references, following the Claim Check pattern [REF20]. This option is used in this flow.	and the details of the use of eDelivery.
13, 18	The request and response messages are exchanged using eDelivery.	The diagram omits the use of Access Points and the details of the use of eDelivery.
14-15	The Data Service verifies that the requesting Portal is authorized to make the request using the Registry of Authorities.	
16-17	The Data Service finds any matching evidences for the request. As the request is for evidence references, only the identifier and some metadata are returned, using the evidence exchange data model and format [REF22].	
19-20	Similar to (2)-(3), (6)-(7) and (10)-(11), the Portal may allow the User to select one or a subset of items of the list. To allow the user to make the choice, sufficient descriptive metadata must be sent alongside the references.	If, instead of evidence references, the actual evidences are requested as supported in the evidence exchange model, steps 19-27 can be omitted.
21-22, 27	The Online Procedure Portal queries and receives in response the selected evidences.	This is similar to (12)-(13), except that here the actual evidences are requested instead of the evidence identifiers. The diagram omits the use of Access Points and the details of the use of eDelivery.
23-26	Just as in the evidence reference request (14-17), the evidence request needs to be authorized using the Registry of Authorities.	
28, 29	The Online Procedure Portal shows the evidence(s) that have been retrieved to the	Note that at this stage the evidence has been transmitted to the Portal, but it has not been

Step	Description	Notes
	user.	formally accepted and is therefore not "exchanged" in the sense of Article 14.3.f.
30	The user indicates her/his approval of the exchange the evidences. This ends the use of the once-only system.	The evidence is now formally "exchanged" and available for the procedure.

9.2. Simplified Flow

Another example flow is shown in Figure 7. This flow is much simpler than the one in Figure 5.

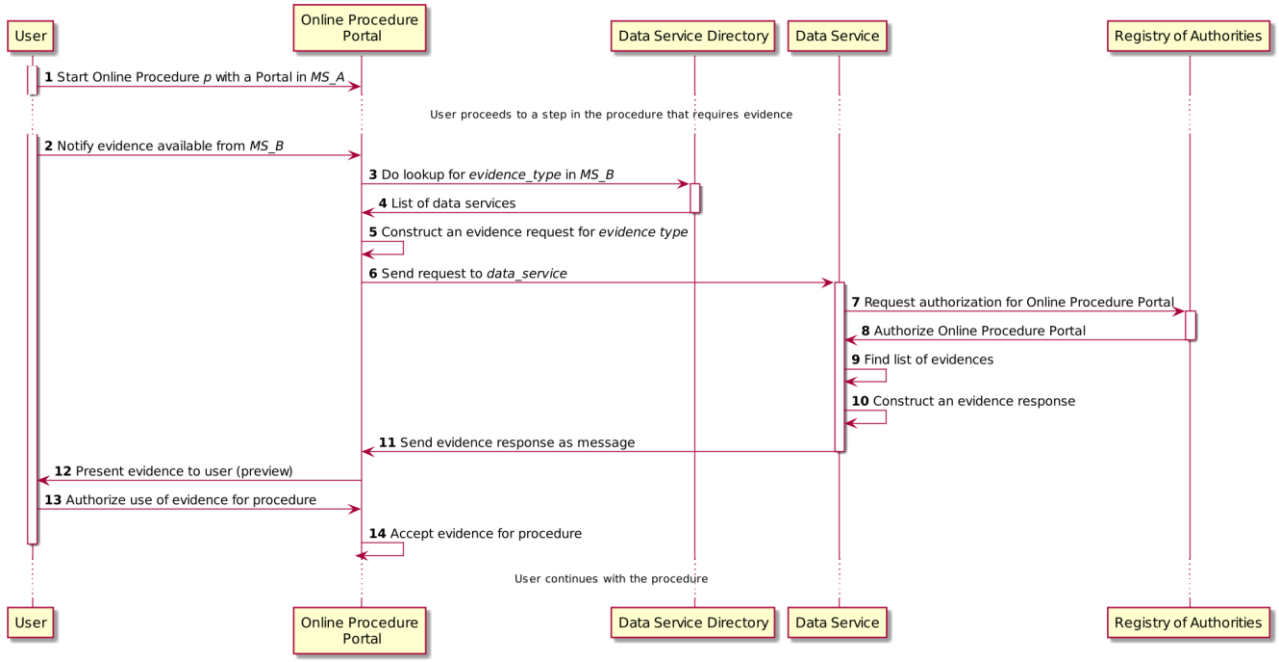


Figure 6 Simplified Once-Only Technical System Flow

Step	Description	Notes
1	This step is as in the previous sample: the User starts a procedure on an Online Procedure Portal.	
2	This step is also as in the previous sample: the procedure requires evidence, and the User indicates this evidence is available from	

Step	Description	Notes
	a different Member State.	
3	In this step, the Online Procedure Portal looks up the data services for a specific evidence type for the indicated Member State in the Data Service Directory.	This flow assumes a harmonized evidence type has been defined. Therefore, there is no need to use the Evidence Broker to determine which evidence type is to be selected.
4	The Data Service Directory indicates which data service provides the selected evidence type.	This flow assumes that there is a single data service for the evidence type in the member state. (This might be a Single Window data service that actually connects to multiple data services, and hides the complexity internal to the Member State from authorities in other Member States).
5	The Online Procedure Portal constructs a request for the evidence for the selected data service.	As there is only one data service, there is no need to consult the User.
6	The request is sent to data service.	In this example, instead of a request for evidence references, a request is directly made for evidences.
7-8	The request is authorized as in the previous flow.	
9-11	A search is done for matching evidences, these are packaged into a response that is then sent back to the Online Procedure Portal.	The step of presenting the list of evidence references with descriptions to the user is skipped, as the Portal asked for evidences instead of evidence references.
12	The evidence (or evidences) are presented to the user, as before.	As the user did not select evidences from an evidence reference list, it is more likely that some of the evidences are irrelevant or otherwise unwanted.
13-14	The user confirms the evidence and the exchange is completed as in the previous step	

When comparing this flow to the previous flow, the following comments can be made:

- The Evidence Broker is not needed, due to the assumption that harmonized evidence types are used.
- This also greatly simplifies the implementation effort for the Online Procedure Portal, as it does not need to support more than one type of evidence.
- The number of steps is about half the number of steps in the more complex flow.
- The User is only involved in four instead of eleven steps.

~~9.2.~~9.3. eDelivery

The following diagram shows the integration of eDelivery in the exchange between an Online Procedure Portal and a Data Service. It is a simplification that assumes static configuration of the AS4 endpoints. For dynamic configuration, additional BDXL and SMP services would need to be added. It is provided as an illustrative example only.

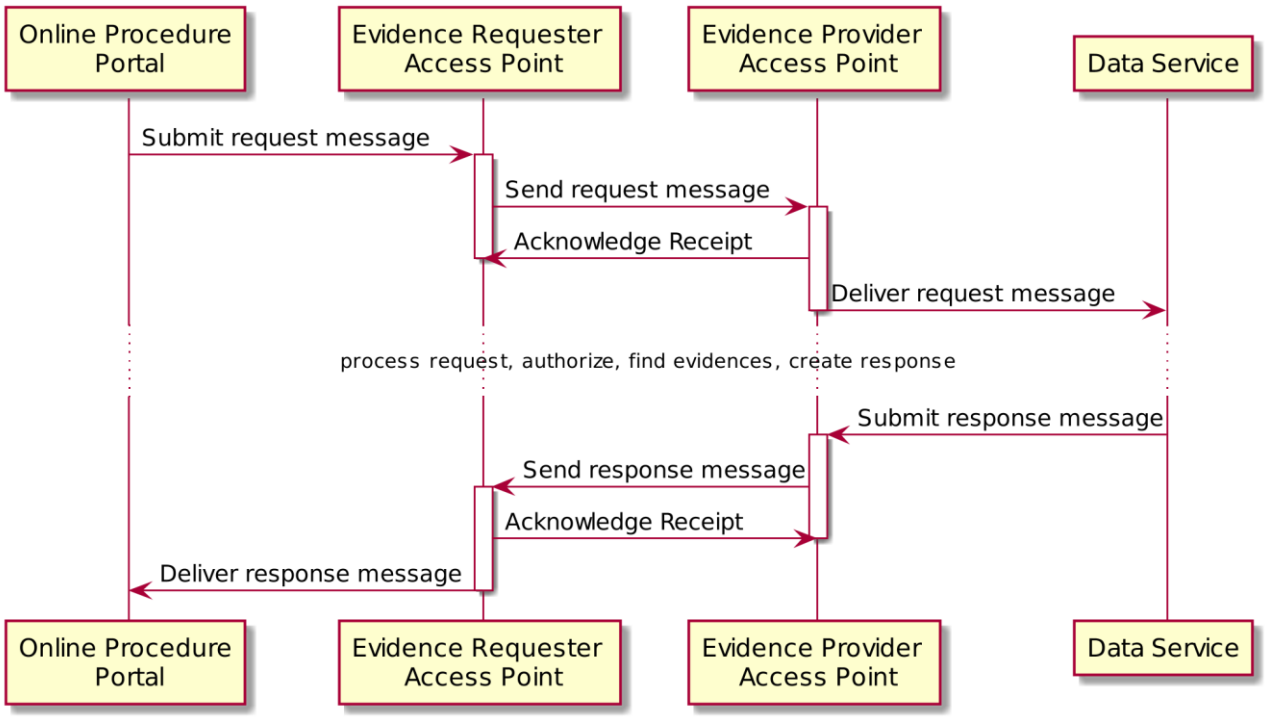


Figure 7 Flowing including eDelivery Access Points