Once-Only Technical System High Level Architecture

Single Digital Gateway (SDG) High Level Architecture Version 1.00

Purpose of the document

The following table summarises the objectives, target audience and main outputs of this document:

Objective(s)	• Introduce and position the Once-Only Technical System in the context of the SDG Regulation and OOTS Implementing Act. • Provide a high-level overview of the main components in the system and the functionality they provide. • Provide a description of the evidence exchange process.
Audience	• 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.
Output	• Functional description of components in Once-Only Technical System. • Identification of roles and responsibilities of the European Commission and the Member States in Once-Only. • 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
DS	Data Service
EB	Evidence Broker
EC	European Commission
ISA²	Interoperability solutions for public administrations, businesses and citizens
ISO	International Organization for Standardization
LSP	Large Scale Pilot
MS	Member State
OASIS	Organization for the Advancement of Structured Information Standards
OOP	Once-Only Principle
OOTS	Once-Only Technical System
SDG	Single Digital Gateway

Acronym	Description
TOOP	The Once-Only Principle

References

Ref.	Document	Content outline
[REF1]	ebXML Messaging Protocol Binding for RegRep Version 1.0	The OASIS ebXML Messaging Protocol Binding for RegRep Version 1.0 specifies a messaging protocol binding for the Registry Services of the OASIS ebXML RegRep Version 4.0 OASIS Standard. This binding is compatible with both the versions 2.0 and 3.0 of ebMS as well as the AS4 profile and complements the existing protocol bindings specified in OASIS RegRep Version 4.0. It is compatible with eDelivery AS4 [REF13].
[REF2]	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.
[REF3]	CEF Digital	CEF Digital including the eID and eDelivery Building Blocks.
[REF6]	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 Infrastructures (DSIs) and broadband networks.
[REF7]	DE4A	Digital Europe for All (DE4A) Large Scale Pilot

Ref.	Document	Content outline
[REF8]	Data Service Directory (DSD) - OOTS	Data Service Directory design documentation
[REF9]	Evidence Broker (EB) - OOTS - API Variant	Evidence Broker design documentation
[REF10]	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.
[REF11]	eDelivery	eDelivery is a building block that provides technical specifications and standards, software and ancillary services to allow projects to create a network of nodes for secure digital data exchange. By building with eDelivery, public and private organisations from different sectors can easily create a safe and interoperable channel to transfer documents and data among each other over a public or private network.
[REF12]	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.
[REF13]	eDelivery AS4	eDelivery AS4 Specification, profiling the ISO 15000 international standards ebMS3 [REF26] and AS4 [REF25].

Ref.	Document	Content outline
[REF14]	eDelivery Security Controls	The CEF 'Security Controls' guidance document addresses the security controls and recommendations applicable to CEF eDelivery's message exchange Use Case. As the message exchange Use Case is closely linked to the Electronic Registered Delivery Service (ERDS), a trust service under the eIDAS regulation, this document maps the Qualified ERDS (QERDS) requirements to the security controls of eDelivery.
[REF15]	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.
[REF16]	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.
[REF17]	eID Homepage	eID is a set of services provided by the European Commission to enable the mutual recognition of national electronic identification schemes (eID) across borders. It allows European citizens to use their national eIDs when accessing online services from other European countries.
[REF18]	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.
[REF19]	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.

Ref.	Document	Content outline
[REF20]	Evidence Exchange - OOTS	Draft design document describing use of open technical specifications and ISA vocabularies for evidence requests and responses.
[REF21]	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 95/46/EC (General Data Protection Regulation).
[REF22]	IMI	Internal Market Information system (IMI).
[REF23]	ISA²	ISA². Interoperability solutions for public administrations, businesses and citizens
[REF24]	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.
[REF25]	ISO 15000-2:2021	ISO 15000-2:2021. Electronic business eXtensible Markup Language (ebXML) — Part 2: Applicability Statement (AS) profile of ebXML messaging service
[REF26]	ISO 15000-1:2021	ISO 15000-1:2021. Electronic business eXtensible Markup Language (ebXML) — Part 1: Messaging service core specification
[REF27]	OASIS ebXML registry and repository version 4.0	Electronic business eXtensible Markup Language (ebXML). Registry and repository. Under submission to ISO TC 154 for inclusion in the ISO 15000 series of International Standards as ISO 15000-3.
[REF28]	Semantic Repository (SR) - OOTS	OOP Semantic Repository design documentation
[REF29]	SEMIC	Semantic Interoperability Community (SEMIC).

Ref.	Document	Content outline
[REF30]	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.).
[REF31]	Single Digital Gateway Coordination Group	The Single Digital Gateway Coordination Group is based on the SDG Regulation [REF30]. The coordination group will have approximately 6 meetings per year and has a high need of exchange of information and content in between.
[REF32]	Single Digital Gateway Regulation Implementation Guidelines	Guidelines for the implementation of the single digital gateway Regulation 2019-2020 work programme. Commission notice. (2019/C 257/01).
[REF33]	TOGAF	TOGAF Standard, a specification of The Open Group, is a proven Enterprise Architecture methodology and framework used by the world's leading organizations to improve business efficiency.
[REF34]	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.
[REF35]	TOOP D23	The Once-Only Principle Project (TOOP) Generic Federated OOP Architecture (3rd version).
[REF36]	ISO 25010	ISO/IEC 25010:2011. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models
[REF37]	UX Guidance - OOTS	Once-Only User Experience.

Ref.	Document	Content outline
[REF38]	OOTS Implementing Act	Draft Commission Implementing Regulation EU ... XXX on the technical and operational specifications of the technical system for the cross-border exchange of evidence and application of the "once only" principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council.
[REF39]	SIP	Barros, Alistair P. and Dumas, Marlon and ter Hofstede, Arthur H.M. (2005) Service Interaction Patterns. In Proceedings 3rd International Conference on Business Process Management 3649, pages pp. 302-318, Nancy, France.
[REF40]	CCCEV	Core Criterion and Core Evidence Vocabulary (CCCEV) - Version 2.00.

1. Introduction

1.1. Once-Only Technical System

Article 14 of the Single Digital Gateway Regulation [REF30] 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. The Once-Only Implementing Act [REF38], which the Commission shall adopt by 11 June 2021, further sets out the technical and operational specifications of the technical system necessary for the implementation of this Article.

This document complements the Implementing Act by providing a high-level architecture. This high level architecture is complemented by, and serves as an introduction to, further technical and operational design documents. References to preliminary versions of this documentation are provided in this document. Together, these documents and the interface documentation they provide deliver the interoperability necessary to support the implementation and interconnection of the distributed components that constitute the Once-Only Technical System. These documents will reach a stable version by 11 June 2021, at which date the Commission shall adopt the Implementing Act. Further evolution of these documents is subject to the governance as specified in Chapter VI of the Implementing Act.

All content of this draft version of this draft architecture is preliminary, subject to agreement in the legislative process and other feedback.

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”.
- The "Evidence Exchange" topic in Work Package 6, "Functionality".

The Once-Only technical system serves primarily as an integration mechanism for existing systems in Member States and is therefore primarily concerned with establishing interoperability by providing interface documentation. Interoperability is defined in the European Interoperability Framework (EIF, [REF19]).

This document also provides an initial introduction to outputs from the following Work Packages and topic:

- WP2, “User Centricity”, which addresses user journeys and use cases for Once-Only. This Work Package adds a User perspective.
- WP4, “Data Semantics, Formats and Quality”, which covers content aspects of evidence exchange. Its main focus is Semantic Interoperability.
- The "User Identification" topic in Work Package 6, "Functionality".

1.3. Input

This document is based on the following main inputs:

- Single Digital Gateway Regulation, in particular Art 14 [REF30];
- OOTS Implementing Act [REF38].

Other inputs include:

- Deliverables and other input from the TOOP Large Scale Pilot [REF34];
- Initial feedback from the DE4A Large Scale Pilot [REF7];
- The “OOP Blueprint” [REF1] created by the preparatory action on Once-Only. That action, which was started in 2019, intends to pave the way for 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 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"; WP2, "User Centricity"; WP4, "Semantics", and WP6, "Functionality";
- Input from policy and subject matter experts in the Commission and from other Commission actions, in particular the ISA^2 action and the CEF Building Blocks at DIGIT and the relevant units at DG GROW and DG CNECT.

1.4. Scope

This document covers the Once-Only Technical System specified in article 14 of the SDG Regulation [REF30] and the draft Implementing Act [REF38]. The scoping is preliminary, subject to agreement in the legislative process and other feedback.

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.

The current version of the architecture does not support representation, in accordance with recital (17) of the Implementing Act [REF38].

Other types of evidence handling, not in the scope of 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;
- Once-Only functionality that uses different mechanisms for the exchange of evidences, as stated in Art 14.10.

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

1.5. Extensibility

While Article 14 of the SDG Regulation [REF30] and the Implementing Act [REF38] set a clear functional scope, the intended applicability of the OOP Technical System is broader. The system, or selected subsets of it, support and enable other data sharing requirements. In particular, the system is intended to not be limited to the procedures described in Article 14.1 but to also support other electronic procedures.

A key consideration is to make sure that additional functionality, if needed in the future, can be added in an incremental way to avoid a major redesign of the initial system. Incremental extensions in the future 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 of the SDG Regulation. This 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.

A future version of the OOP Technical System may also incorporate, at design level, other implementation technologies to implement existing elements, or add additional optional elements.

1.6 Structure of this document

The remainder of this document is structured as follows:

- Section 2, Requirements: gives an overview of the requirements on which the architecture is based.
- Section 3, 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 4, Evidence Requester Side Architecture Elements: covers Requester-side systems;
- Section 5, Evidence Providing Side Architecture Elements: covers Provider-side elements;
- Section 6, Once-Only Common Services that support the system;
- Section 7, Evidence Exchange and eDelivery: explains evidence exchange protocol supported by the eDelivery Building Block;
- Section 8, Identification and Representation: covers identification of natural and legal persons as well as representation;
- Section 9, System Operation: covers general operational constraints for the technical system;
- Section 10, Sample Once-Only Flows: describes in some detail sample flows involving the Once-Only Technical System.

2. Requirements

The High Level Architecture is closely aligned with the activities and outputs of the User Centricity Work Package. That Work Package is in the process of defining a set of Functional Requirements that the Once-Only Technical System must support [REF37].

The following table complements these functional requirements by providing a more general overview of the key architectural requirements that the Once-Only Technical System addresses. The table classifies these requirements using the ISO 25010 quality attributes framework [REF36]. It also provides the source, in most cases the relevant section of the SDG Regulation (label "SDG.*"), the Implementing Act (label "IA.*"), and/or the applicable principle from the European Interoperability Framework (label "EIF.*") [REF19]. To support traceability, the table indicates the architectural element (or elements) in which each requirement is addressed.

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
1	Functional Suitability	Completeness, correctness and appropriateness of coverage of tasks and user objectives	Member States shall ensure that, where a procedure [..] can be accessed and completed online by non-cross-border users, it can also be accessed and completed online by cross-border users [..].	SDG.Art.13.1	Portal	Context, not about Once-Only per se.
2	Functional Suitability		Users are able to access the instructions for completing the procedure in an official language of the Union [..].	SDG.Art.13.2.a; EIF.P.9	Portal	Context, not about Once-Only per se.
3	Functional Suitability		Cross-border users are able to submit the required information, including where the structure of such information differs from similar information in the Member State where the user is undertaking the procedure.	SDG.Art.13.2.b	Portal, Evidence Broker	The Evidence Broker helps find evidence types that have "the required information" even if "the structure of such information" is different.
4	Functional Suitability		Cross-border users shall identify and authenticate themselves electronically.	SDG.Art.13.2.c; eIDAS	Portal, eID	SDG does not mandate eID (it says users "are able to") . But for OOP it is essential (an uploaded scanned identity document does not provide any validated identity attributes). So Art 13.3 seems not to be sufficient/relevant for OOP.

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
5	Functional Suitability		Cross-border users are able to provide evidence of compliance with applicable requirements in all cases where this is also possible for non-crossborder users.	SDG.Art.13.2.d	Portal	Article also mentions "to receive the outcome of the procedures in electronic format" but that is out of scope for OOP.
6	Functional Suitability		A technical system for the automated exchange of evidence between competent authorities in different Member States ('the Technical System') shall be established by the Commission in cooperation with the Member States.	SDG.Art.14.1; EIF.P.6	All	
7	Functional Suitability		The system supports the exchange of evidence for the online procedures listed in Annex II to the SDG Regulation and the procedures provided for in Directives 2005/36/EC, 2006/123/EC, 2014/24/EU and 2014/25/EU.	SDG.Art.14.1; EIF.P.6	All	
8	Functional Suitability		Where competent authorities lawfully issue, in their own Member State and in an electronic format that allows automated exchange, evidence that is relevant for the online procedures referred to in SDG.Art.14.1, they shall also make such evidence available to requesting competent authorities from other Member States in an electronic format that allows automated exchange.	SDG.Art.14.2; EIF.P.6	Data Service	Allowing for automated exchange means that the data in electronic format must be structured in such a way that it allows for machine-to-machine exchange of the data, or automated processing, based on a request from a user, through a competent authority in another Member State. This includes both structured and unstructured evidence. Evidence issued in paper format only falls outside the scope of the Article 14 exchange.

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
9	Performance Efficiency	Time behaviour	If the requested evidence is available, the issuing authority shall return it instantly to the requesting authority so that the procedure can be completed without making the user wait. If this is not possible (e.g. because the evidence is not yet in a digital format or otherwise needs more time to be created), the provider shall return a response informing the requester of this.	EIF.P.6	Data Service	Requirement added to reflect that the system does not have a Deferred response feature.
10	Performance Efficiency	Resource Utilization	A requesting competent authority shall only request evidences that are relevant for the user in the context of the procedure, and shall only request these from issuing competent authorities in the specified Member State that issue that type of evidence.		Portal; Data Service Directory	
11	Compatibility	Co-Existence	The user shall be permitted to submit evidence by means other than the technical system and directly to the requesting competent authority.	SDG.Art.14.4; EIF.P.6	N/A	Context, scope.
12	Compatibility	Co-Existence	The system shall not apply to procedures established at Union level which provide for different mechanisms for the exchange of evidence, unless the technical system necessary for the implementation of this Article is integrated into those procedures in accordance with the rules of the Union acts that establish those procedures.	SDG.Art.14.10	Related Systems	

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
13	Compatibility	Co-Existence	Where the technical system, or other systems for the exchange or verification of evidence between Member States, are not available or are not applicable, or where the user does not request the use of the technical system, competent authorities shall cooperate through the Internal Market Information System (IMI).	SDG.Art.15; EIF.P.4	Related Systems	Context, scope.
14	Compatibility	Interoperability	Components in the system interact following common interface specifications that are based on open standards and technical specifications.	EIF.P.2	All	
15	Compatibility	Interoperability	The technical system shall reuse existing standards.	EIF.P.4	Portal, Data Service, Evidence Broker	
16	Compatibility	Interoperability	Evidence exchange shall be enabled for evidences that are in a format that allows for automated exchange.	SDG.Art.14.2; EIF.P.4	Portal, Data Service, Evidence Broker	
17	Compatibility	Interoperability	Evidence formats and metadata structures shall be based on agreed standards and technical specifications.	EIF.P.2	Portal, Data Service, Evidence Broker	

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
18	Compatibility	Interoperability	Competent authorities shall be identified using an agreed party-identifier format.	EIF.P.4.	eDelivery, Data Service Directory, Evidence Broker	
19	Compatibility	Co-Existence	The identifier format shall be able to leverage existing identifier systems in Member States.	EIF.P.1	eDelivery, Data Service Directory, Evidence Broker	
20	Compatibility	Interoperability	The message packaging format for evidence exchange shall be based on open standards and technical specifications.	EIF.P.2	eDelivery Message Exchange	
21	Compatibility	Interoperability	The interfaces of common services shall be based on open standards and technical specifications.	EIF.P.2	Data Service Directory, Evidence Broker	

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
24	Usability	Operability	The system makes it easy for the user to determine what (kind of) evidence is needed, and where to get it.	EIF.P.6; SDG.Art.14.3.a; SDG.Art.14.3.f; IA.Art.5; IA.Art.6; IA.Art.11;	Portal, Evidence Broker, Data Service Directory	
25	Usability	User error protection	Evidence requesters shall ensure that their procedure portals contain an explanation about the possibility to use the OOTS and its features.	EIF.P.6; IA.Art.10	Portal	
26	Usability	User error protection	Evidence requesters shall give users the possibility to select and request the types of evidence.	EIF.P.6; IA.Art.11	Portal, Evidence Broker, Data Service Directory	
27	Usability	User error protection	The user is provided with information about name of evidence provider and evidence type for confirmation, before any request is made.	EIF.P.6; IA.Art.13	Portal	The user does not have to provide the name him/herself.

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
28	Usability	User error protection	The user has the ability to preview evidence and can control whether or not it is used.	EIF.P.6; SDG.Art.14.3.f; IA.15	Preview Space	In case an evidence was selected by mistake, or an evidence that has some issue, it can be discarded.
29	Usability	Accessibility	Accessibility refers to the degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use.	EIF.P.7	Portal	
30	Reliability	Maturity	The solution reuses mature, proven eID and eDelivery Building Blocks developed under the Connecting Europe Facility.	EIF.P.4	eDelivery, eID	
31	Reliability	Availability	Member States and the European Commission shall ensure the availability of components up to agreed Service Levels.	EIF.P.6	All	
32	Reliability	Fault Tolerance	Exchange of evidence shall provide mechanisms to recover from temporary transmission failures.	EIF.P.6	eDelivery Message Exchange	
33	Security	Confidentiality	The system shall ensure the confidentiality of the evidence. Evidences cannot be read/viewed while in transit between requester and provider.	SDG.Art.14.3.e; EIF.P.8	eDelivery Message Exchange	

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
34	Security	Integrity	The system shall ensure the integrity of the evidence. Evidences cannot be modified while in transit between requester and provider.	SDG.Art.14.3.e; EIF.P.8	eDelivery Message Exchange	
35	Security	Integrity	The Evidence Provider shall ensure the integrity of the evidence between the Data Source (Base Registry) and its Access Point.	EIF.P.8; IA.18	Data Service, Access Point	See section 5.3. Same security requirements on messaging within a Member State as on eDelivery messaging.
36	Security	Integrity	The evidence requester shall ensure the integrity of the evidence request between Portal and its Access Point,	EIF.P.8	Portal, Access Point.	See section 4.3. Same security requirements on messaging within a Member State as on eDelivery messaging.
37	Security	Non-Repudiation of Receipt	A competent authority cannot repudiate its receipt of an evidence through the technical system, as it sends a signed eDelivery receipt that includes the digest of the received message.	EIF.P.8	eDelivery Message Exchange	
38	Security	Non-Repudiation of Origin	A competent authority cannot repudiate its issuing of an evidence through the technical system, as evidences are exchanged in signed messages.	EIF.P.8	eDelivery Message Exchange	
39	Security	Non-Repudiation of Origin	A competent authority cannot repudiate having requested an evidence through the technical system, as evidence requests are exchanged in signed messages.	EIF.P.8	eDelivery Message Exchange	

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
40	Security	Authenticity	The evidence exchanged through the technical system shall, for the purposes of the requesting competent authority, be deemed to be authentic.	SDG.Art.14.8; EIF.P.8	eDelivery Message Exchange, Data Service.	
41	Security	User Identification	The identification of users, the provision of information and supporting evidence, signature and final submission can all be carried out electronically at a distance, through a service channel which enables users to fulfil the requirements related to the procedure in a user-friendly and structured way.	SDG.Art.6.2.a; EIF.P.6 ;EIF.P.8	Portal, eID	
42	Security	User Identification	Evidence Providers shall indicate for Evidence Types the required Level of Assurance of identification attributes.	IA.Art.12.1	eID, Data Service Directory	
43	Security	User Identification	Evidence Requesters shall ensure that users are authenticated at the Level of Assurance required to request evidence of a type from an Evidence Provider.	IA.Art.12.3	eID, Portal	
44	Security	User Identification	Evidence Requesters shall obtain values for additional disambiguating attributes from the user if specified by the Provider	IA.Art.12.5	Portal, Data Service Directory	See section 7.4.
45	Security	User Identification	Evidence Providers shall use additional attributes to disambiguate if no unique match is found based on the attributes provided via eID	IA.Art.12.5; IA.Art.17	Data Service	See section 7.4.

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
46	Security	User Identification	Evidence Providers shall not return an evidence if there is no unique match for the user based on his or her attibutes but instead return an error	IA.Art.17	Date Service	
47	Security	Accountability	Requesting and issuing competent authorities shall log all exchanges of (requests for) evidence and associated metadata and non-repudiation data.	EIF.P.3; EIF.P.8	Portal, Data Service, eDelivery	
48	Maintainability	Modularity	The technical system is a distributed system consisting of systems supporting the evidence requester, the evidence provider and supporting common services.	EIF.P.1	All	
49	Maintainability	Modularity	Components are placed where possible and, if preferred by a MS, in the MS rather than at central EU level.	EIF.P.1	All	
50	Maintainability	Modularity	The components in the system communicate based on agreed interfaces. Beyond these interfaces and SLAs, no implementation constraints apply.	EIF.P.2; EIF.P.5	All	Components can be implemented in any programming language or framework, run on any operating system, hardware or cloud, as long as the interfaces are correctly implemented.
51	Maintainability	Modifiability	The system will not be hard-wired to particular types of evidence requirements and evidence types. Evidence Requesters may use a registry to dynamically discover evidence types to use. Evidence Providers may register evidence types in the registry.	EIF.P.2; EIF.P.4; EIF.P.12	Evidence Broker	

ID	Quality Attribute	Quality Sub-Attribute	Requirement	Source	Applies to Architectural Element(s)	Comments
52	Maintainability	Modifiability	The system will not be hard-wired to particular data services for particular evidence types. Evidence requester may use a registry to dynamically discover data services that can be used. Evidence Providers may register (and change registrations for) Data Services.	EIF.P.2; EIF.P.4; EIF.P.12	Data Service Directory	
53	Maintainability	Modifiability	The system is designed to enable future enhancements to support types of exchange beyond Article 14 requirements, such as subscriptions or deferred responses.	EIF.P.2;EIF.P.4; EIF.P.12	Portal, Data Service, Data Service Directory	
54	Maintainability	Reusability	Elements of the system should be reusable for data sharing beyond the scope of the SDG Regulation.	EIF.P.2;EIF.P.4	All	
55	Portability	Adaptability, Replaceability	Elements in the system can transferred from one hardware, software or other operational or usage environment to another.	EIF.P.5	All	The focus of the architecture is on interfaces; implementations can be changed.

3. Once-Only Technical System Architecture

3.1. Context

The Single Digital Gateway Regulation [REF30] aims to make it easier for a user to initiate and execute, subject to specified constraints, a set of procedures online where:

- the user is using an Online Procedure Portal of a public administration in a Member State;
- the procedure requires evidence from a different Member State than the Member State hosting the Online Procedure Portal.

While carrying out a cross-border online procedure, evidence relating to a citizen or a represented business may be required. The Once-Only Technical System allows the governmental Portal to request, following 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. This means that this system aims at enabling cross-border data-sharing between competent authorities at all administrative levels (local, regional and national).

Note that:

- Under ECJ case law competent authorities can also be non-governmental entities with a formal task in the public remit.
- The competent authority that *issues* the evidence acts, in terms commonly used in other contexts (including the former TOOP large scale pilot [REF34]), as a Data Provider. The competent authority that *requests* the provided evidence acts as a Data Consumer.

This document provides a high-level architecture for the Once-Only Technical System. Its aim is to link the SDG Regulation [REF30] and Implementing Act [REF38] to the more detailed technical design documents and to provide a summary overview.

3.2. Approach

The OOP Technical System establishes a general purpose data exchange ecosystem for the public sector in Europe. The system enables trusted cross-border data sharing between competent authorities in a distributed environment involving many data providers and many data consumers.

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 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 context of the SDG Regulation.

To allow the 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 interfaces. They are designed to minimise the impact on existing systems in Member States and to maximise 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 common services to provide comprehensive support for Once-Only. The interfaces may be implemented in multiple independent software implementations or services, including software products or services from third party solution providers.

3.3. Overview

Figure 1 provides a High Level view of the Once-Only Technical System.[1] The system as shown includes a “Once-Only evidence exchange” business process that establishes a transition between two business events, associated to a cross-border administrative procedure:

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 one or more other Member 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 request of the user and the acceptance for use in the procedure.

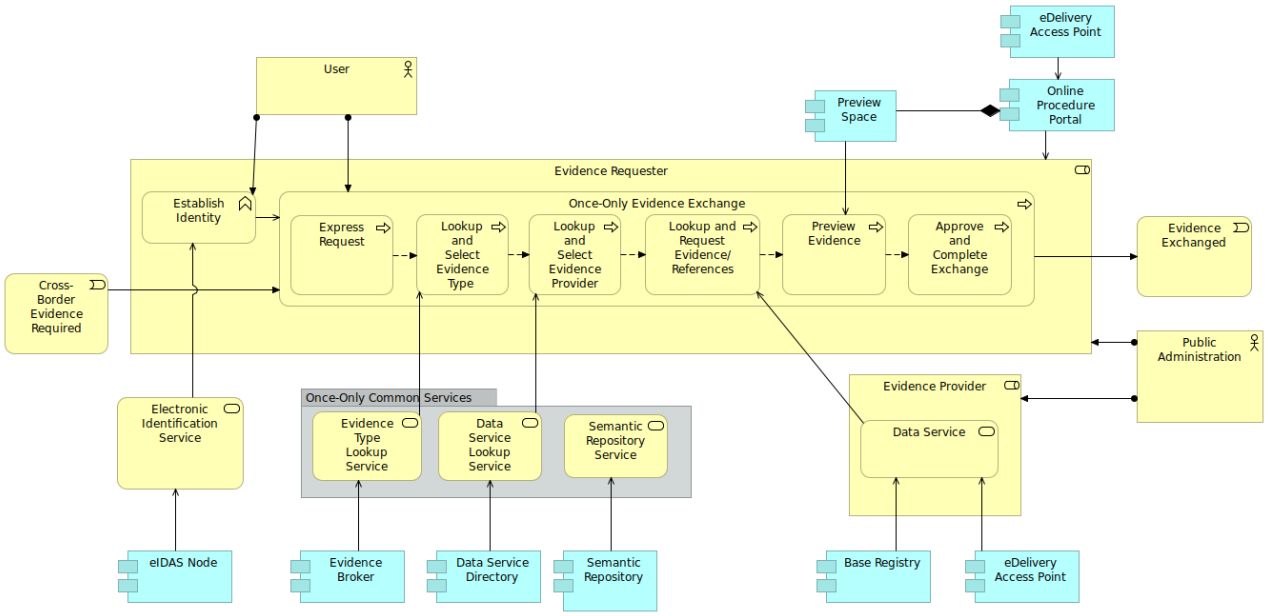

Figure 1 High Level View of the Once-Only Technical System

Both of these events relate to the competent authority that requests the evidence(s). They are connected by the business process that involves interactions with:

- the user;
- the Data Service of the competent authority that provides the evidence;
- Once-Only common services that support the operational uses of the Once-Only Technical System.

The flow of the business process follows the steps described in Article 14(3) of the SDG Regulation [REF30].

As Article 14(7) of the SDG Regulation and Article 12 of the Implementing Act explain, an 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 from the eID Building Block [REF17] or by other components (not shown in the diagram), such as a notified electronic 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 only for evidence exchange, it is not modeled as a step in the exchange business process but as a business function that serves it.

The “Once-Only evidence exchange” process consists of the following steps, all initiated from an Online Procedure Portal (see section 4.2):

1. "Express Request" is a step in which the user is asked to express explicitly whether he or she wants to use the Once-Only Technical System.
2. “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 an Evidence Broker component (see section 6.2).
3. “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 6.3).
4. “Lookup and Request Evidence” is a step in which a request for available evidences is made to a “Data Service” (see section 5.2). This service is provided by a “Base Registry” component owned by a competent authority that is an “Evidence Provider”.

5. “Preview Exchange” is a step in which the user previews the evidence to determine if he of she wants to use it in the context of the procedure. As explained in Article 14(5) of the SDG Regulation, this step shall not be required for procedures where the automated cross-border data exchange without such preview is allowed under applicable Union or national law.
6. “Approve and Complete Exchange” is a step in which the user confirms that the evidence can be used in the procedure.

Of these six steps, the second, third and fourth involve interaction between IT systems in different Member States. The Once-Only Technical System is based on detailed technical design documentation that provide interoperability between these systems. The last two steps only involve the User and the Online Procedure Portal.

The three services “Evidence Type Lookup Service”, “Data Service Lookup Service” and “Semantic Repository Service” together comprise a group of Once-Only common services. These platforms do not handle requests for evidences and their issuance directly but provides supporting services.

Section 4 will discuss the architectural elements relating to the competent authority that requests the evidence. Section 5 will do the same for the evidence-issuing competent authority. Section 6 discusses the Once-Only common services. Section 7 and 8 cover eDelivery, evidence change and identification and authentication in the Once-Only Technical System.

3.4. 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.

Other elements of the architecture are extension elements, as their functionality is not always needed. For example:

- The user may authenticate to the Online Procedure Portal of a public administration in a Member State using a notified national eID of that Member State, thus obviating the need to use eIDAS nodes.
- In procedures in which Member States have agreed to all use the same evidence types, there is no need for Evidence Broker functionality to determine evidence types to select. In that case, an Online Procedure Portal can directly look up Data Services in the Data Service Directory without having to first look up a rule for a particular requirement.

3.5. Governance

Chapter VI of the Implementing Act [REF38] defines the governance of the once only technical system.

3.6. Roles and Responsibilities

The Once-Only Technical System is a collection of interacting technical systems of the Member States and the Commission. According to Article 14(11) of the SDG Regulation, 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. Chapter VI of the Implementing Act [REF38] defines these responsibilities.

4. Evidence Requester Architecture Elements

4.1. Introduction

The interaction in the Once-Only Technical System is an interaction between competent authorities. This section covers architectural elements involving systems of competent authorities that 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 online 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. Using the Once-Only Technical System, the candidate can provide the university or public administration with proof of any relevant existing qualifications he or she obtained from institutions in other Member State(s), and other relevant documentation such as information on social situation and level of income.

4.2. 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. The Once-Only Technical System is 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 "Once-Only evidence exchange" business process as shown in Figure 1.

The functionality of an Online Procedure Portal can be considered along two dimensions, which relate to the two axes in Figure 2:

- Front end functionality versus back end functionality. This is reflected in the vertical axis of the diagram. A front end components can be implemented, for example, as a website that supports access using a Web browser or as a mobile application.
- Different types of functionality. This is reflected in the horizontal axis of the diagram. Eight components and related sets of functions are defined.

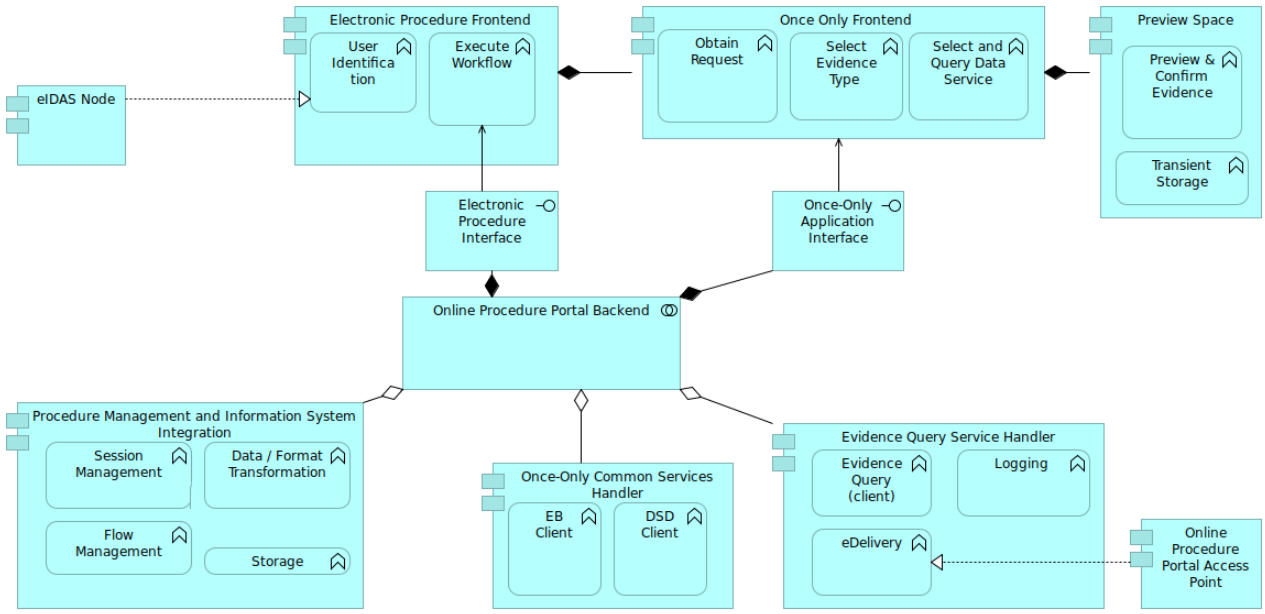

Figure 2 Online Procedure Portal Application View

Together, the front end components and the back end components include functions to allow the user to execute the actions in the "Once-Only evidence exchange" business process, as well as any preceding actions that are preconditions:

- Identify himself/herself ("Establish Identity");
- Explicitly request to use the system for exchange of evidence ("Express Request");
- Select evidence types ("Lookup and Select Evidence Type");
- Select data services ("Lookup and Select Evidence Provider");
- Select evidences ("Lookup and Request Evidence");
- Preview the evidence ("Preview Evidence");
- Confirm whether or not a selected (and possibly previewed) evidence can be used in the procedure ("Approve and Complete Exchange");

This architecture only specifies at a high level the interfaces provided by back-end components to front-end components. It does not constrain them at more detailed technical level because they are only used internally in Member State systems.

Article 14 of the Implementing Act requires a separate component for preview from the general functionality of a procedure portal. It requires giving the user access to a **Preview Space**, a component separate from the procedure portal. In particular, this component is required to have its own separate storage. The Preview Space component can be a fully separate special-purpose component, or it can be combined with other Once-Only functionality. The former is illustrated in the sample flow in section 10.2. The latter in the sample flow in section 10.1. The sample flow presented in section 10.1. uses the term **Once-Only Staging Area** for the combination of Once Only Front end, Preview Space, the Once Only Common Services Handler, the Evidence Query Service Handler and the (interface to) the Online Procedure Portal Access Point. Such an area could be used as a complete generic sub-system on the evidence requester side to connect a portal to the Once-Only technical system

The Once-Only technical system, including the preview functionality, is about exchange of "read-only" evidences. The user can decide to not use the evidence but cannot modify its content in any way. 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. If the user does not confirm the use of the evidence, the evidence is permanently deleted.

Figure 2 classifies back end functions in three groups:

- Procedure management and information systems integration. This is common functionality that is needed in an Online Procedure Portal that does not relate to Once-Only technical system. It is mentioned for context.
- Once-Only Common Services handler functions that interface to the Once-Only common services described in section 6. These functions include client interfaces to the **Evidence Broker** and the **Data Service Directory**.
- Evidence query service handler functions that control the exchange of evidence requests and correlated evidence responses (or error messages) from a **Data Service** using the functionality described in section 7.

Article 9 of the Implementing Act [REF38] requires the Online Procedure Portal to explain the possibility to use the Once-Only technical system and its features to users. Article 10(1) requires involving the user in the selection of evidence types and data services. Article 11, user authentication, is addressed in section 8. Article 12 shows information that must be provided to the user before evidence is requested.

An Online Procedure Portal Back-end needs to cover general electronic procedure functionality, such as procedure management functionality, to manage a user's session and flow through the procedure, and information system integration, which includes any permanent storage of procedure data and submitted evidences. These functionalities include:

- Procedure and session state management: 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 end-user that issued the query for those evidences. In addition, user input to the procedure, and evidences retrieved to support it, may be provided over time, and possibly interrupted/resumed;
- Integration with information systems and/or databases and any required data or format transformation. This may involve transformation between different structured formats, or from structured (data-oriented) to unstructured (presentation-oriented) formats.

Since the Once-Only Common Services Handler and Evidence Query Service Handler relate to systems in different Member States, and to systems provided by the European Commission, their external interfaces are specified in design documentation of the Once-Only Technical System in order to achieve interoperability. Their internal interfaces to the front end components are not standardized as they are used within a Member State.

The functionality for evidence exchange includes functionality to:

- 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;
- Handover of received evidences to the **Preview Space** for preview by the user;
- Logging of evidence exchange information including date and time and unique identifiers of evidence request, evidence response, user, data service and evidence type.

Article 13, content of evidence request, and Article 15, the response to evidence requests, are addressed in section 7.3.

4.3. Online Procedure Portal Access Point

The Evidence Query Service Handler application component of an Online Procedure Portal uses an eDelivery **Access Point** to request the evidence from the evidence provider and receive the evidence in response. This may be a dedicated Access Point for that specific Portal, or a more general communication component that is also used by other portals and systems. By sharing an Access Point, competent authorities can reduce the cost and complexity of implementation. For further discussion and references, see section 7.2.

Since this Access Point is the entry point into the Once-Only Technical System, it is essential that the competent authority on behalf of which the Access Point makes such a request has an appropriate legal basis to make such a request, such as Directive 2005/36/EC, 2006/123/EC, 2014/24/EU or 2014/25/EU or, for the procedures listed in Annex II of the SDG Regulation, other applicable Union or national law as stated in recital 45 of the SDG Regulation.

Member States are responsible for securing the evidence request as it is transmitted from an Online Procedure Portal to the Access Point.

4.4. eIDAS Node of Evidence Requesting Member State

To use the Once-Only system, the user needs to be identified and authenticated. If the user is registered in the Evidence Requesting Member State, a notified eID system of the Member State may be used. If the user is from a different Member State and has an eID from that Member State, the **eIDAS Nodes** of the two Member States can be used for cross-border authentication. The attributes obtained from the user are included in evidence requests to the Data Services. The eID functionality will be accessed from the front-end part of the Online Procedure Portal as it involves interaction with the user. For more on eIDAS nodes, see section 7.

5. Evidence Provider Architecture Elements

5.1. Introduction

The interaction in the Once-Only Technical System is an interaction between competent authorities. A competent authority that *issues* evidences in response to evidence requests provides a **Data Service** as specified in section 5.2. The transmission of requests and evidences uses an **eDelivery Access Point** as specified in section 5.3. This section covers architectural elements involving systems of competent authorities that issue evidences.

5.2. Data Service

Competent authorities in Member States operate **Data Services** to issue evidences, in response to requests from requesting competent authorities and users executing procedures in Online Procedure Portals. The legal base for this service is provided in article 15 and 16 of the Implementing Act.

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 a common “Evidence Query Service”. In support of this 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”;
- Perform evidence request validation;
- Perform identity matching, to determine which (if any) evidences in storage relate to the user (see section 8.5);
- Apply, if requested, a transformation on the evidence, from a predefined set of transformations;
- Return evidence responses (including possibly errors) and submit them to an eDelivery Access Point for transmission to the requesting Online Procedure Portal.

A Data Service may respond to requests by providing pre-existing evidences or by creating or assembling evidences from data dynamically. Such assembling may involve operations such as selection, filtering or transformation.

The generic format for evidence requests and responses is based on exchange data model design documentation based on open standards and technical specifications introduced in section 7.

A data service may not be directly connected to an information system. Instead, middleware or other integration solutions may be used. A data service may also connect to a national OOP layer.

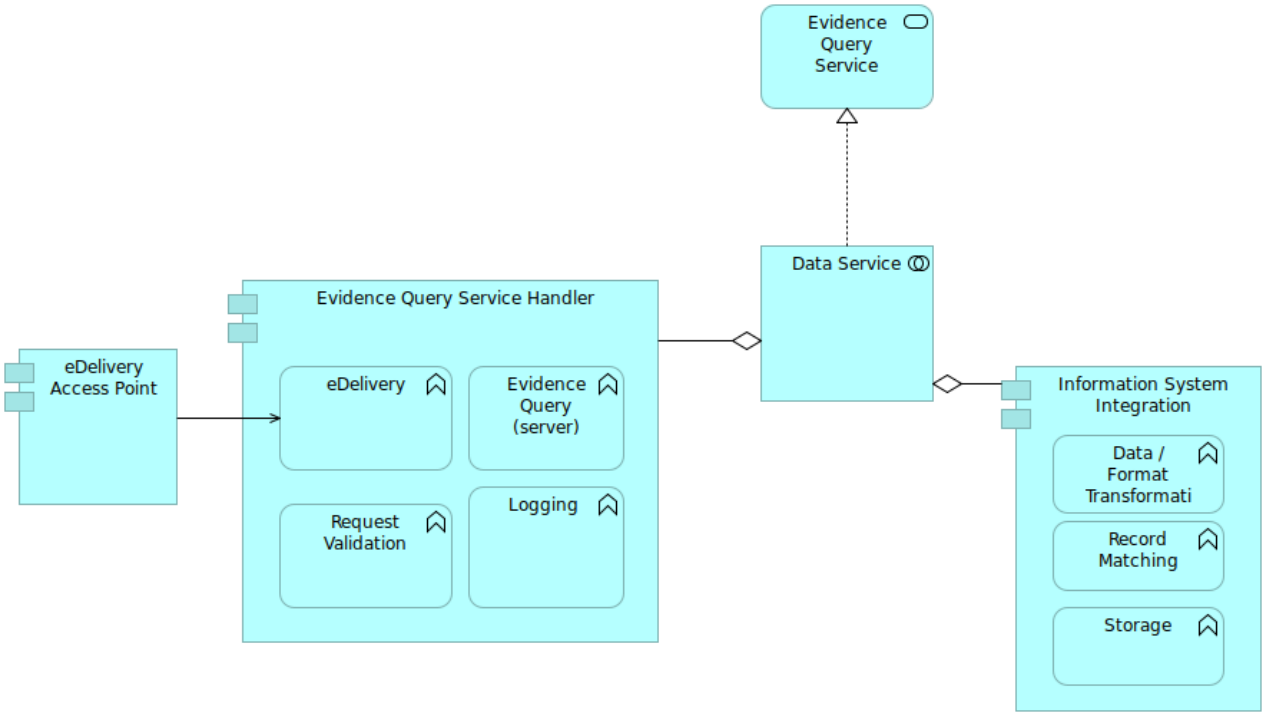

Figure 3 Data Service Application View

5.3. 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 may be a dedicated Access Point for that specific Data Service. It can also be a more general communication component that is also used by other applications. An Access Point may be shared by multiple competent authorities, to reduce the cost and complexity of implementation. For further discussion and references, see section 7.2.

Member States are responsible for securing the evidence as it is transmitted from a Base Registry to the Access Point, as required in Article 17 of the Implementing Act.

5.4. eIDAS Node of Evidence Issuing Member State

As mentioned in section 4.6, 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.

6. Once-Only Common Services

6.1. Introduction

To support the exchange of evidences between **Data Services** and **Online Procedure Portals**, the Once-Only Technical System uses Once-Only supporting services. The draft Implementing Act [REF38] refers to these services as the Common Services. The Common Services do not process data about citizens or businesses. Instead they contain and serve operational data parameters that support the operation of the Once-Only technical system. The Common Services are:

- Evidence Broker (see section 6.2);
- Data Service Directory (see section 6.3);
- Semantic Repository (see section 6.4).

Each of these services will provide a life-cycle management interface (see section 6.5) to maintain the data it serves as this data is subject to change over time. The Once-Only technical system follows a hybrid deployment model (see section 6.6).

6.2. Evidence Broker

The Once-Only Technical System supports situations in which an Online Procedure Portal, when performing an online procedure, requests an evidence from a data service in a different Member State. The evidence relates to a requirement to obtain information on a citizen or business or to prove that certain claims about the citizen or business are true. Its legal base is Article 6 of the Implementing Act.

If for a particular procedure, for a particular requirement, a harmonized evidence type (and associated schema) is defined and agreed by the Member States, all Member States know in advance which evidence type needs to be requested. However, the Once-Only Technical System also supports situations in which there is no 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 another Member State. 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 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 that 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 States, but also because the rules underlying the equivalence may change over time. Therefore, the Once-Only Technical System provides a common service, the **Evidence Broker**, 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. Its legal base is Article 6 of the Implementing Act.

The Evidence Broker has a defined interface. It responds to requests that contain the following information:

- The Member State from which evidence is to be retrieved;
- An identifier of the requirement for which evidence is requested (information needed, criteria that need to be met);
- The context in which the request is made (life event, procedure, applicable Directive);
- Optionally, the geographic area code for the Member State in which the competent authority that lawfully issues the evidence is based.

It will return, in response, the following information:

- A (possibly empty) list of the following information item pairs:
    - An identifier of an evidence type that satisfies the information requirement;
    - Optionally, for structured evidences, an identifier of a transformation that may be applied, if requested, to the evidence by the Evidence Provider.

The ability to specify transformations that may be applied to evidences supports the data minimization requirement of the GDPR [REF21]. The provider can use a transformation to provide an evidence that more narrowly matches the relevant requirement, by removing unnecessary substructures and/or aggregating information. However, this functionality is optional. If the competent authority providing the requested evidence can only provide digitalised documents, instead of data, it is possible that the requesting authority receives more personal data than strictly needed. However, this situation is no different from those in which such evidence is submitted by the user. The SDGR does not aim to harmonise the format in which evidence is provided by the different competent authorities in the Member States. Until all administrations move to a system based on data instead of documents, the once-only system will be able to accommodate both.

This Evidence Broker service is based on rule content, provided by the Member States themselves. It provides an online mechanism for Member States to align and query their evidence requirements and evidence type sets. This obviates the need for full EU-level harmonisation of evidences types. The Evidence Broker allows Member States to manage and share information about rules relating to evidence types. As noted, 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 are defined in the Core Criterion and Core Evidence Vocabulary (CCCEV, [REF40]), provided by the ISA^2 SEMIC team [REF29]. Additional design documentation is available for the Evidence Broker [REF9].

In case where there are multiple options (multiple evidence types) for a particular requirement, the Online Procedure Portal may ask the User to select which (if any) option will be used, putting the user in control of the execution of the procedure.

Note that use of the Evidence Broker is not needed and its use is not required in situations where the evidence requester already has obtained the response information mentioned above.

6.3. Data Service Directory

To request electronically available evidence 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 Technical System includes a **Data Service Directory** which allows Member States to manage and share this information in a structured format. Its legal base is Article 5 of the Implementing Act.

The Data Service Directory has a defined interface. It responds to requests that contain the following information:

- An identifier of the Evidence Type;
- The Member State in which Data Services for the identified Evidence Type are being looked up;
- Optionally, the geographic area code for the Member State in which the competent authority that lawfully issues the evidence is based.

It will return, in response, the following information:

- A (possibly empty) list of tuples providing the following information:
    - The identifier and identifier type of the Evidence Provider served by the Data Service;
    - The identifier and identifier type of the authority that operates the Data Service Access Point used by the Data Service;
    - Whether the user needs to be identified as a natural person or as a legal person;
    - A list of required identification attributes, their formats, and required Levels of Assurance for each of them.

The Once-Only technical situation supports situations in which there is more than one Evidence Provider for an Evidence Type in a Member State. In these cases, the user may help decide which (if any) of them will be queried, as he or she may know from which Data Service(s) relevant evidence(s) can be obtained. For example, in an educational procedure the user could select the university that he or she knows issued an educational evidence type for him/her from a list of universities, if universities in the relevant Member State use different Data Services.

Additional design documentation is available for the Data Service Directory [REF8]. This work is based on open technical specifications and ISA^2 specifications.

On the support of the Data Service Directory for identification and authentication, see section 8 below.

6.4. 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. Its legal base is Article 7 of the Implementing Act. This Repository is not used in the run-time exchange of evidences. Its purpose is only to support the Member States as they design and implement systems consuming or providing evidences.

The Semantic Repository contains:

- Visual class diagrams;
- Data models and definitions;
- Data elements and definitions;
- Distributions in XML schema (XSD) or equivalent formats;
- Code lists of information requirements;
- Code lists of evidence types;
- Other code lists, or references to code lists, used in the system;
- A methodology for developing new data models for structured evidence types.

Additional design documentation is available for the semantic repository [REF28].

The Semantic Repository will include a generic metamodel that can be used for the exchange of arbitrary unstructured evidences.

6.5. Life Cycle Management

The instances of the Evidence Broker and the Data Service Directory provided by the European Commission will provide an interface that allows Member States to maintain (add, change, delete) content regarding evidence types available from them and data services that provide them. Candidates for this interface are:

- A user-interface that can be used by Member State representatives to interactively manage content;
- An automated interface that allows Member States to synchronise content in the EC provided instances to their national registries.

PLANNED FUTURE UPDATE: there is not yet a decision on the technical design for the automated interface.

6.6. Deployment Options

The deployment of the Once-Only common services Data Service Directory and Evidence Broker follows a hybrid model, in which:

- The European Commission operates an EU-wide central service instance for the Member States. This instance contains metadata for (some, but possibly not all) Member States. This instance allows metadata from these Member States to be searched by all participants in the Once-Only Technical System. Member States using this instance still need to provide and help maintain the metadata in the central service as discussed in section 6.5.
- A Member State that wants to do so can operate and provide access to its own instance of the service. To search metadata related to this Member State, this instance is used and there is no need to provide data to the EU-wide central service instance.

The legal base for this deployment model is Article 8 of the Implementing Act. The model is illustrated for the Data Service Directory in the following diagram. It shows a situation in which Member State 1 uses the EC central Data Service Directory but Member State 2 provides its own. For queries relating to Data Services in Evidence Providing Member State 1, Evidence Requesters query the EU central data service directory. For Evidence Providing Member State 2, they query the MS-specific instance of the service.

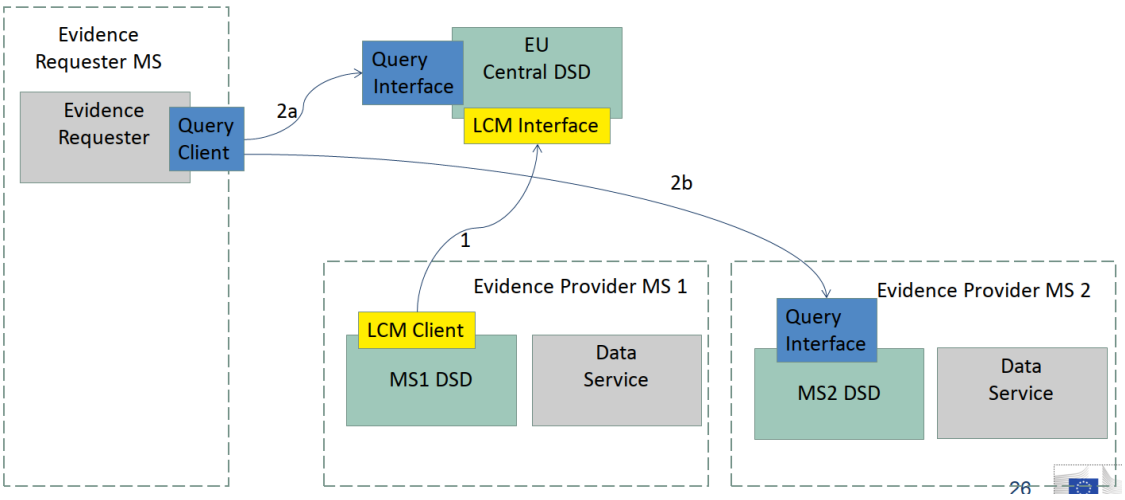

Figure 4 Hybrid deployment model for common services

Note that there shall be no more than one instance of a common service for a given Member State. Therefore, a given Member State either has no service instance of its own, like MS 1 in Figure 4, or a single service instance, as is the case for MS 2. No Member State shall have two or more instances.

The lookup interface design documentation to be used for a service instance shall be the same for the European Commission-operated service instance and for any service instance operated by a Member State, following Article 8 of the Implementing Act [REF38]. The life cycle management interface is covered in section 6.5 above.

7. Evidence Exchange and eDelivery

7.1. Introduction

Evidence exchange in the Once-Only Technical System is based on bilateral exchange between competent authorities. An exchange is always a pair of two correlated messages:

- An evidence request message generated by an Online Procedure Portal in a Member State, supporting a competent authority in the “Evidence Requester” role;
- A corresponding evidence response message generated by a Data Service in one or several other Member States, supporting a competent authority in the “Evidence Provider” role.

For interoperability, the Once-Only Technical System defines in detail the structure and content and message exchange parameters.

7.2. Integration Patterns

The Once-Only Technical System is based on a number of common patterns identified in technical literature such as Enterprise Integration Patterns [REF18] or Service Interaction Patterns [REF39].

The OOP Technical System uses the **Request-Reply** integration pattern. The exchange of evidences takes place between competent authorities, but never in isolation or spontaneously, always in response to explicit requests:

- Evidence requests are made by Online Procedure Portals in a Member State in the "Evidence Requester" role;
- Corresponding evidence responses are provided by Data Services in one or several other Member States in the "Evidence Provider" role.

The use of message-based communication components called Access Points in eDelivery is an instance of the **Messaging Gateway** pattern. A gateway is a component that is responsible for the implementation of messaging functionality according to the agreed interoperability design. Reusable Access Points make it easy to enable the use of eDelivery in Online Procedure Portals and Data Services by competent authorities and their service providers.

Access Points also instantiate the **Messaging Bridge** integration. The communication between the Online Procedure Portal and its Access Point and the communication between the Data Service and its Access Point may use different communication protocols and formats, which the Access Point helps bridge.

In a particular step in a procedure, an Online Procedure Portal may issue multiple requests to different Data Services and collect the responses in parallel. This follows the **Scatter-Gather** with **Distribution List** pattern.

7.3. Evidence Request Response

The evidence request response exchange legs use generic structures based on a specified profile of the RegRep4 open technical specifications [REF27] and ISA vocabularies. The structures support transport, routing, packaging and correlation.

The request structure includes, following Article 13 of the Implementing Act:

- a unique identification of the evidence request;
- the evidence type that is requested;
- date and time when the request was made;
- identification of the procedure for which the evidence is required;
- name of the evidence requester and intermediary platform, where applicable;
- name of the evidence provider;
- the personal identification data of the user;
- the level of assurance of the electronic identification means used by the user;
- any additional attributes provided by the user for the purpose of the request of evidence;
- optionally, for structured evidences, an identifier of a transformation operation to be applied by the Data Service to the evidence before it is issued to the evidence requester.

The response structure (if the response is not an error) includes, following Article 15(2) of the Implementing Act:

- a unique identification of the evidence response;
- the identifier of the evidence request to which the response relates, to support correlation;
- date and time at which the response is created;
- identifier of the evidence requester and intermediary platform, where applicable;

- identifier of the evidence provider and intermediary platform, where applicable.
- For each evidence included in the response, the response includes:
    - evidence metadata as defined in CCCEV [REF40]:
        - Title; distribution; issuer; issue date; language; validity period.
    - an indication of the transformation applied, if any;
    - the evidence in electronic form;

NB: if the evidence request requested application of a transformation, the attached evidence is the output of the application of the transformation to the evidence;

The syntax and semantic of evidence requests and evidence response is covered in the technical design documents [REF20].

The technical system supports a one-step process:

1. The request for evidence specifies that evidences are requested.
2. The response includes any matching evidences.

Note that in error situations, a error message will be returned instead of the content responses, following Article 15(3) of the Implementing Act. This shall include:

- a unique identifier of the error;
- the identifier of the evidence request to which the response relates, to support correlation;
- date and time at which the error was generated;
- a description of the error that occurred.

The optional requested transformation allows the requester to receive a more tailored version of the evidence, as explained above in section 6.2. Since this transformation is applied by the Data Service of the Evidence Provider, it is the output of the transformation that is exchanged as the authentic evidence in the Once-Only technical system. It is protected by the integration and non-repudiation features of eDelivery.

7.4. eDelivery

The Once-Only Technical System reuses the eDelivery Building Blocking [REF11] and uses its Acccess Point [REF12] specification. See Figure 5 for an overview of its functions.

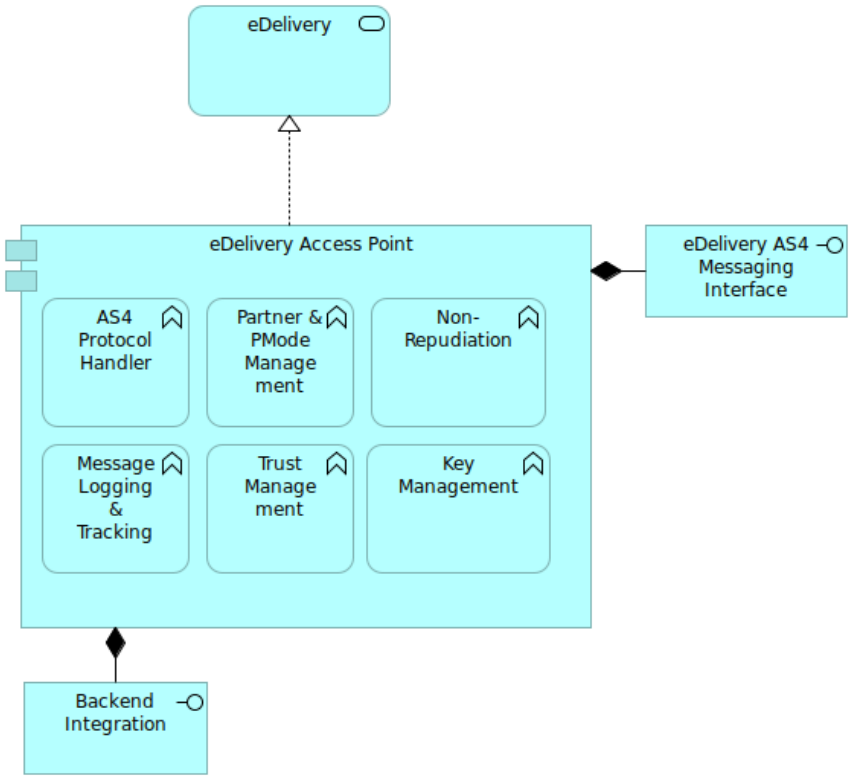

Figure 5 Access Point Application View

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 [REF14].

As noted above in section 4.3, the competent authority that operates an Online Procedure Portal Access Point has a responsibility to make sure that it only issues evidence requests on behalf of requesting competent authorities that have an appropriate legal basis to make such requests, as required in recital 45 of the SDG Regulation [REF30].

7.5. Configuration of eDelivery

Evidence exchange uses eDelivery Access Points as provided by the CEF eDelivery Building Block. It uses the ISO 15000 ebMS3 [REF26] and AS4 [REF25] standards profiled as eDelivery AS4 using the so-called four-corner topology profile enhancement [REF13]. The packaging of RegRep4 in AS4 and the values of key AS4 processing mode parameters and associated headers are specified in a separate open technical specification [REF1]. The four-corner topology applies to both the flow of the request from the Online Procedure Portal to the Data Service and the reverse flow from the Data Service to the Online Procedure Portal.

As the four corner topology profile enhancement is used, for an evidence request:

1. The competent authority on whose behalf the evidence request is made is identified as *original sender* (Corner 1).
2. The competent authority that operates the Access point is identified as the sender (the "From" party) of the AS4 message (Corner 2).
3. The competent authority that operates the Access Point for the Data Service is the receiver (the "To" party) of the AS4 message (Corner 3).

4. The competent authority that provides the evidence is the *final recipient* of the message (Corner 4).

Routing of eDelivery messages is handled as follows:

- The Data Service Directory provides both the identifiers of the evidence provider and of its Access Point provider. Therefore any evidence request message can be routed appropriately, for any identified Data Service.
- Evidence response messages shall be routed in reverse order, i.e. the final recipient value of the response is set to the value of the original sender in the request (*C1 → C4*), the response original sender value is set to the request final recipient value (*C4 → C1*), and the sender and receiver values are swapped *(C2 → C3*; *C3 → C2*).

A single Access Point may serve any number of evidence requesters and/or evidence providers. If a competent authority operates its own Access Point, then:

- Corner 1 and 2 are the same for outbound messages. The value of the AS4 sender header ("*eb:From"*) shall be the same as the value of the *original sender* message property.
- Corner 3 and 4 are the same for inbound messages. The value of the AS4 receiver *("eb:To")* shall be the same as the value *final recipient* message property.

All Access Points that are part of the Once-Only Technical System are statically configured to make evidence requests to, and respond to evidence requests from, all other Access Points. This configuration includes networking (e.g. firewall settings), transport layer security, message layer security (including certificates used for signing and encryption) and all AS4 processing mode configurations including endpoint URIs.

The following diagram shows the integration of eDelivery in the exchange between an Online Procedure Portal and a Data Service. The Data Service Directory provides corner 3 and 4 routing identifier information for the request message. The Data Service reverse routes the response message to the Online Procedure Portal.

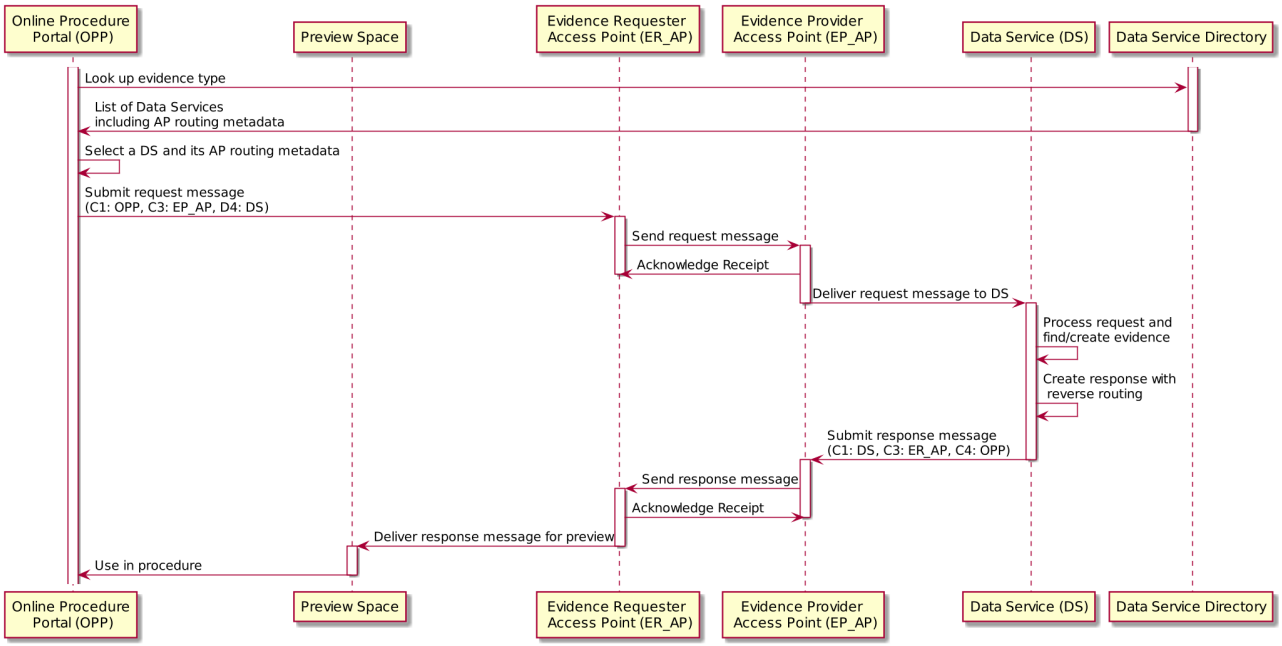

Figure 6 Message exchange and routing using eDelivery Access Points and Data Service Directory

As discussed in section 4.2, evidences retrieved via the technical system are delivered to the Preview Space to support preview by the user.

The Once-Only Technical System does not provide end-to-end security:

- Evidence requests and evidence responses are trusted based on the message signature applied by the sending Access Point. The OPP (for requests) and the DS (for responses) do not sign the content that they submit to the Access Point with an expectation that the DS (for requests) and the OPP (for responses) verify the signature. This obviates the need for sharing of signing certificates and agreement on trusted Certification Authorities between competent authorities that use the Once-Only technical system.
- Evidence requests and responses are encrypted when they packaged and transmitted as eDelivery messages. The OPP (for requests) and the DS (for responses) do not encrypt the content that they submit to the Access Point with an expectation that the DS (for requests) and the OPP (for responses) decrypt the content. This obviates the need for sharing of encryption certificates and agreement on trusted Certification Authorities between competent authorities that use the Once-Only technical system.

Member States are responsible for providing equivalent or better protection of evidence requests and responses in the exchange between Online Procedure Portals, Data Services and their respective Access Points (i.e. between C1 and C2 and between C3 and C4).

Exchange of eDelivery messages between Access Points shall use the public Internet. As specified in the eDelivery AS4 specification, eDelivery is secured at both the transport layer and the message layer. This provides integrity, authentication, confidentiality and non-repudiation of origin and non-repudiation of receipt at a level of protection comparable to the use of a private network.

A Member State may 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 potentially having specialised Access Points for specific domains.

7.6. Use in complex scenarios

The Once-Only Technical System does not provide any specific functionality beyond the exchange of pairs of evidence requests and responses. There are no mechanisms to link different subsequent uses of the system by the same user. This does not mean that it is not possible or useful to use the system in situations where one procedure is dependent on another procedure.

For example, the system can be used for procedures involving registration and related de-registration. An example of this is shown in the following figure. Here, the user performs a registration procedure in Member State A. The output of this procedure is created as an output of this procedure in a registry in Member State A. The Once-Only Technical System can be used as an input in a separate de-registration procedure in Member State B.

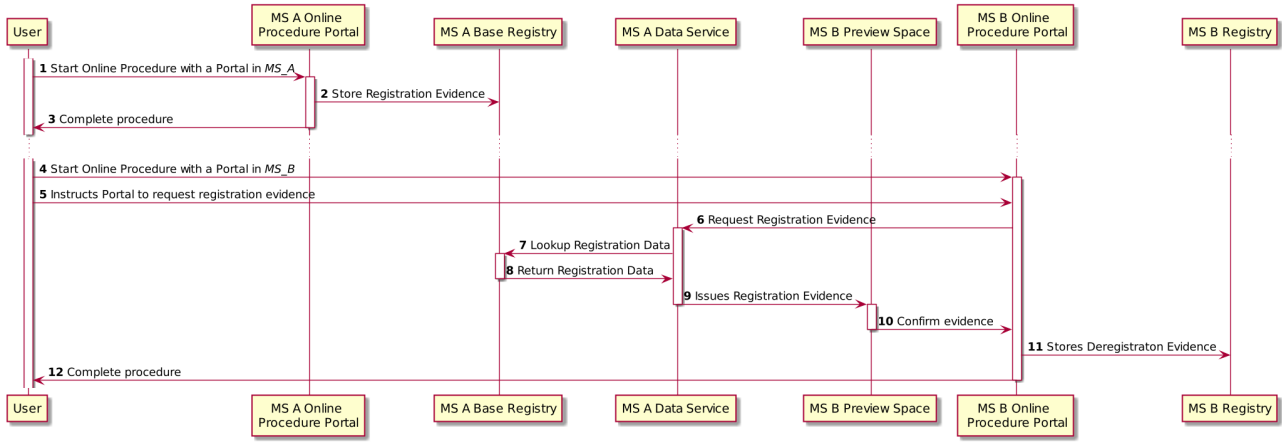

Figure 7 Once-Only technical system supporting registration and Deregistration

Note that this example assumes that the registration evidence is input to the subsequent de-registration procedure. In other situations the registration procedure may use output from a prior de-registration procedure.

7.7. Intermediary Platform

In some Member States, some evidences are not provided directly by individual competent authorities but by dedicated entities that provide such evidences in a delegated capacity. For example, there may be a dedicated service organisation in a Member State that stores and makes available, on request, educational evidences on behalf of many educational institutions, such as universities. The Implementing Act, Article 1(6), refers to these organisations as Intermediary Platforms.

Use of such a platform may simplify the use of the Once-Only Technical System on the Evidence Provider side:

- Only the Intermediary Platform needs to implement a Data Service for the type of evidences that it provides;
- Only the Intermediary Platform needs to implement (or connect to) an Access Point and needs to be integrated in the Once-Only Technical System;
- The evidence providing competent authorities that use the Intermediary Platform do not have to join the Once-Only Technical System directly themselves;
- Evidence requesters that look up the provided evidence type in the Data Service Directory will find only one provider in the Member State. This means that there is no need to determine which Data Service(s) (potentially among many) to send the evidence request(s) to, and therefore no need to consult the user to select a Data Service.
- Implementation, testing, configuration, maintenance, etc. are all simplified.

An Intermediary Platform may also simplify the use of the Once-Only Technical System on the Evidence Requester side:

- It could provide the functionality of the Once-Only Staging Area to Online Procedure Portals and the competent authorities served by those portals;
- Online Procedure Portals that use the platform do not need to operate client interfaces to the Common Services themselves;
- The platform could implement eDelivery for the Online Procedure Portals by providing (or connecting to) an Access Point.

Whether or not a Member State uses a (or some) Intermediary Platform(s), and which competent authorities should use the (or a particular) Intermediary Platform, is at the Member State's discretion.

An Intermediary Platform also instantiates the **Messaging Gateway** and **Messaging Bridge** integration patterns. In addition to bridging messaging protocols (e.g. eDelivery AS4 to other protocols used within the Member State), functionality provided may include:

- Mapping between national party identifier systems and cross-border identifier systems;
- Mapping between data formats, schemas, code lists;
- Mapping between synchronous and asynchronous communication;
- Service Bus connections;
- Aggregation services (e.g. combine information from multiple Base Registries).

The concept of an Intermediary Platform is also sometimes known as a "Single Window" or as a "Data Aggregator".

8. Identification and Authentication

8.1. Introduction

The architecture of the Once-Only Technical System reuses the eID building block.

8.2. eIDAS Node

The use of eIDAS nodes is discussed in sections 4.4 and 5.4. The purpose, use and specifications of eIDAS Nodes are specified in the existing, separate eID Building Block [REF17]. They are reused in the Once-Only context.

Note that in some procedures, for some users, a national eID that has been notified may be used without the need to use the eIDAS Node. This is the case for a user that executes a procedure in Member State A, has a national eID for MS A but wants to use evidence from MS B. This is an option irrespective of the nationality of the user. To be used, the national eID for MS A must be a notified eID according to Article 11(1) of the Implementing Act .

Note that notified eIDs may differ in Level-of Assurance. To use the Once-Only Technical System, the user should be authenticated using a level of assurance that is at least as high as the level expected by the Data Service as explained in Article 11(4) of the draft Implementing Act [REF38].

The Once-Only Technical System distinguishes the identity and authentication of natural persons and legal persons, if supported by the eID service used.

8.3. Identification and authentication

In the execution of an electronic procedure, there are two situations in which the user can be identified and authenticated:

- to use the procedure;
- to use the once-only technical system to retrieve a particular evidence.

The allowed means of identification and the required level of assurance may differ for these situations. As explained in Article 11(4) of the Implementing Act [REF38], this could result in situations where the user needs to re-authenticate to use the Once-Only technical system. The use of the Once-Only technical system requires the user to use electronic identification. The Online Procedure Portal should help the user avoid unnecessary re-authentication by encouraging the user to:

- Use electronic identification to authenticate when he or she starts the procedure, even if the procedure itself does not require identification or authentication or also accepts digitalised copies of non-electronic evidence of identity, such as identity cards or passports. Such digitalised copies are not sufficient to use the Once-Only technical system.
- Use the appropriate type of eID. If a service is only accessible to legal person, the representative user should not authenticate as a natural person to the service or vice versa.
- Use a means of identification that provides a "High" level of assurance, if the user has a choice between more than one means of electronic identification, and one of these provides a "High" level of assurance. If the Data Service requires the user to authenticate with a "High" level of assurance and the user used an eID with a "Substantial" level of assurance to authenticate to the procedure, the user would have re-authenticate as explained in Article 11(4) of the Implementing Act.

8.4. Additional Attributes

If the Data Service has an ability to use the mechanism of user-provided attributes that are not included in the required eIDAS attribute set, but which can serve to disambiguate in the process of record matching as mentioned in recital (15) and Article 11(1)(h) of the Implementing Act [REF38], it shall publish this ability by adding these attributes to the list of identification attributes for the evidence type in the Data Service Directory as stated in Article 5(3)(b). The Data Service Directory shall set the level of assurance to "N/A" (as they will be user-provided and therefore unverified) and specify the required format. The Online Procedure Portal shall use this information and prompt the user to supply values for these attributes for inclusion in the evidence request.

The evidence request shall never store or use these user-provided attributes outside the Preview Area and after the end of the user's session with the portal.

For example, a Data Service could indicate that it can use the last four digits of the citizen identification number of the user as additional user-provided attribute, if those four digits are sufficient to always uniquely identify users, even users that have the same values for the mandatory eIDAS attributes as other citizens.

8.5 Identity Matching

As part of user identification and authentication, a relying party commonly wants to know whether that the user has previously accessed that service and/or the user's history with other public services. In the use of electronic procedures, such identity matching may be needed at two points in time:

1. When the user authenticates in order to interact with the Online Procedure Portal. This authentication may involve use of the eIDAS nodes or use a notified eID in the evidence requester Member State. This step is typically needed for any interaction with an electronic procedure, including interactions that do not involve the use of the Once-Only Technical System.
2. As part of the processing of an evidence request by a Data Service in the context of the Once-Only Technical System. In this case the evidence request contains the identity attributes that have been provided using eID and any additional attributes provided by the user as described in section 8.4. These attributes are used to select evidences for a specific user.

Note that the eIDAS Minimum Data Set may not be enough to properly identify a foreign user according to national rules. Therefore, the ability to request additional attributes should be used to make sure sufficient disambiguating information is available.

The identity matching functionality needed for authenticating the user to the online service may be part of the functionality of an interactive service or it may be provided by a dedicated (typically centralized) **Matching Service**. In the latter case, this service could be repurposed to also support identity matching for a Data Service in the context of the Once-Only technical system. Note however that in the case of the Once-Only technical system, there is no direct interaction of the user with the Data Service. All information that is needed for identity matching should therefore be provided and included in the evidence request.

8.6. Representation

This version of the architecture supports situations in which the user wants to use the system to retrieve a piece of evidence that relates to him or herself, i.e. situations in which the "data subject" is the same as the user. It also enables transferring information about representation and mandates where the evidence provider is able to check the authenticity of those rights or roles of the person.

The user can be authenticated in one of two ways:

- Using a notified national eID in the evidence requester Member State.
- Using another notified eID and the eIDAS nodes.

Where the evidence request is made by the authenticated user on behalf of another natural or legal person, the following scenarios may apply:

1. The evidence provider is able to verify or requires verification of the representation of powers or mandate.

This may happen when, for example, the evidence requester did not make/needed any validation or the validation is not legally recognized/provide legally valid proof. The evidence provider can request the use additional attributes provided by the user to identify and validate the powers of representation if these are accessible for the evidence provider (e.g. held by it or in the same MS or otherwise accessible and legally recognised).

2. The evidence provider relies on a representation power or mandate being verified by the evidence requester because the validation process is legally recognised.

If the powers of representation are not already automatically accessible for the evidence provider (e.g. located in another Member State), there is a need to introduce a method of conveying this information to the evidence provider. Since it concerns access to potentially confidential and sensitive data, there is a need to establish legal, organizational and semantic interoperability aside of technical interoperability.

Below three examples, how the power of representation can be obtained by the evidence requester:

a. The evidence requester itself already has information about power of representation

b. Validation of power of representation is obtained from another organization in the evidence requester Member State, e.g. in the context of user authentication with the national notified eID. This is visualized in Figure 1 below as the flow that includes the green box.

c. Validation of the powers of representation is obtained from another Member State, e.g. during user authentication via notified eID such as the NL eHerkenning. This is visualized in that same diagram below as flow that includes the red box.

Notified eID-s, where they represent a power of representation already have a legal basis by virtue of the eIDAS notification process. All other scenarios typically lack legal harmonization of such powers and mandates. For the scenarios where the evidence provider does not already have automatic access to power of mandates, the following alternatives are relevant:

d. Where eIDAS was used for user authentication, the SEMPER project results are being studied;

e. Where notified eID means were used for user authentication without eIDAS nodes, EC is studying how SEMPER results could be modified for use outside of eIDAS interoperability framework.

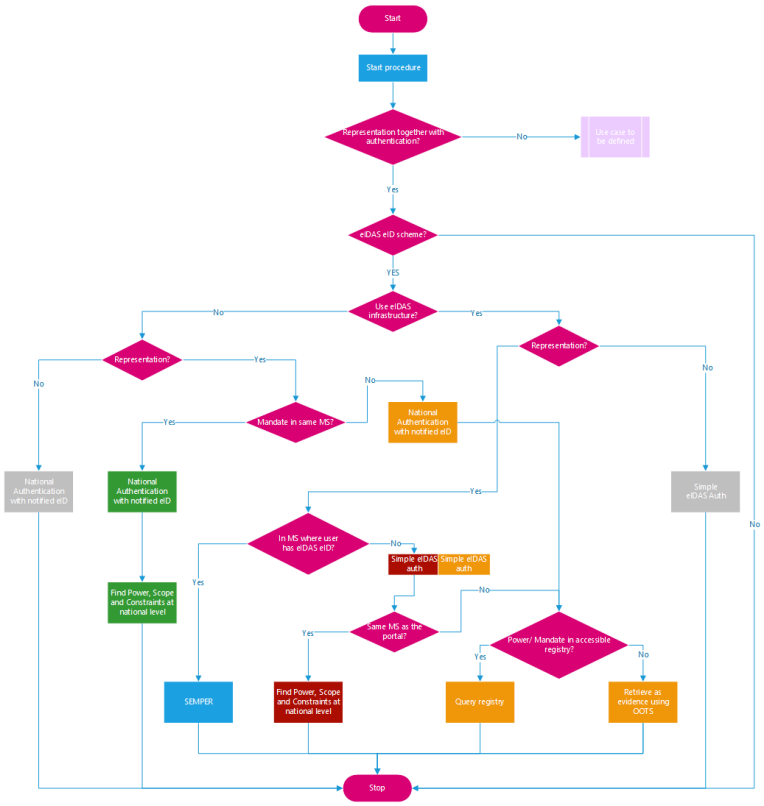

Figure 8 Power and mandates in OOTS, evidence requester representation validation

For the case where the user specifies after the authentication that there is a case of representation, re-authentication may be required.

9. System Operation

9.1 Introduction

To support the operation of the technical system, additional constraints need to be adhered to.

9.2 Log System

The legal base for logging in the technical system is provided in Article 18 of the draft Implementing Act.

The approach to logging in the technical system reflects its distributed nature. Actors perform logging

- Member States as evidence requesters and providers
- Commission (and some Member States) as provider of common services

The information to be logged is:

- Evidence request metadata
- Evidence response or error metadata
- eDelivery event data (message sent, received, acknowledged, acknowledgment received, any errors)
- Use of common services

Confidentiality, integrity and availability of the logs need to be applied. Note, however, only evidence request metadata includes personal information.

10. Sample Once-Only Flows

10.1. Sample Flow

The sequence diagram in Figure 9 shows a sample execution flow of a procedure where the user involved uses the Once-Only Technical System. It is provided as an illustrative example only.[2] The diagram assumes "Once-Only"-specific functionality is handled by a separate **Once-Only Staging Area** sub-portal, which includes the **Preview Space**. The diagram shows a single successful flow. At many stages there is more than one potential next step, including error situations, which are not shown in the diagram - the diagram shows only ideal user progress through the system. Furthermore, the use of eDelivery (using Access Points) is omitted from the diagram. Refer to chapter 7 to see how use of eDelivery Access Points can be represented.

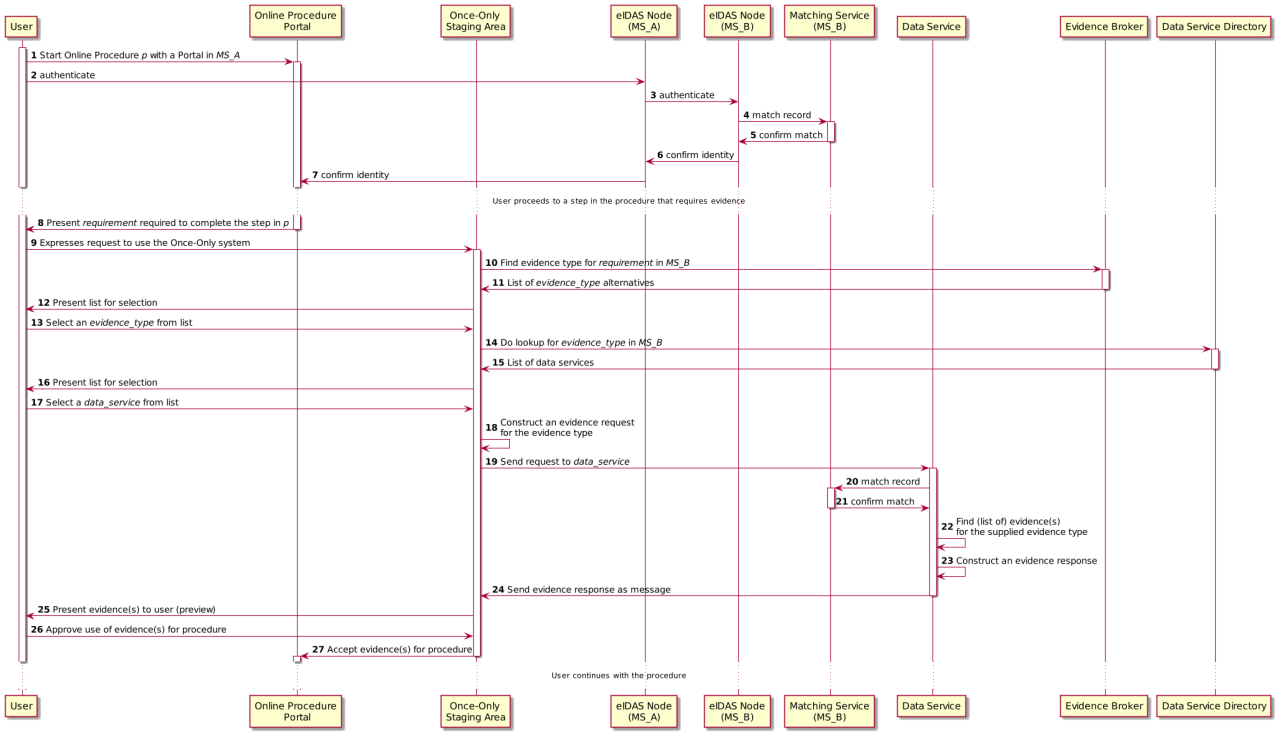

Figure 9 Once-Only Technical System Flow

The diagram shows an approach that maximises interaction with the User. This goes beyond the strict requirements of Article 14, which only mandates the preview feature, but it follows the principle of giving the user full control of their evidence when interacting with the Once-Only Technical System.

The following table provides more in-depth explanations of each step in the sequence.

Step	Description	Notes
1	Unless otherwise provided for under Union or national law, any Once-Only operation only starts when a user 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 branching, loops, etc.	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.
2-7	The User is authenticated, as such authentication is a pre-condition to the use of the Once-Only Technical System. In this example, the User is from another Member State, Member State B, is authenticated using the eIDAS nodes.	If the user has a notified eID from Member State A, in which the requesting competent authority is based, the user could also use that eID. The example assumes a separate "Matching Service" that is integrated with the eIDAS node of Member State B.

Step	Description	Notes
8	In the execution of the procedure, the User may arrive at a point where evidences need to be provided to fulfil certain information requirements or to prove that certain conditions have been 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 requirement. The Portal may support multiple ways to provide this evidence. For evidence that is available using the Once-Only Technical System, the Portal may ask the User to indicate in which (if any) other Member State(s) such evidence can be found.	Step (8) – (27) could be repeated for each of the points in the procedure at which evidence is to be provided.
9	The User makes an explicit request to use the Once-Only Technical System to have evidence retrieved from Member State B.	This flow assumes the interaction of the user with the Once-Only Technical System is handled by a separate Once-Only Staging Area sub-portal. The user is directed to this sub-portal to complete the evidence exchange. The sample Portal asks the user to specify from which Member State the 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.
10	The Once-Only Staging Area, with this User-provided information, proceeds to consult the Evidence Broker to check which types of evidence should be selected from the specified Member State.	The sample flow assumes the portal is designed to use the Evidence Broker. For some procedures and/or evidence types, Member States may have agreed on a predefined set of harmonized evidence types. In that case, no interaction is needed with the Evidence Broker.

Step	Description	Notes
11	In response, the Evidence Broker indicates that in Member State B, from which evidence is being requested, the information requirement can be met using either evidence type *ET1* or evidence type *ET2.* For example, a structured electronic diploma based on the EDCI data model [REF10] or another evidence type.	
12	The Once-Only Staging Area displays the results of its interaction with the Evidence Broker and asks which (if any) of the 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 *ET1* and/or *ET2,* without asking for user input, skipping steps (10) and (11).
13	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.
14	Now that (pairs of) the evidence type to be requested and the Member State holding it has been 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 where a User may have relevant evidence is likely to be small, so this would create a large amount of unnecessary message traffic.
15	The Data Service Directory returns a list of Providers of the selected evidence type.	
16-17	Similarly to (12)-(13), the Portal may allow the User to select one or a subset of items from 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.

Step	Description	Notes
18	For the selected Data Service(s) in the selected Member State(s), a request is constructed using the evidence exchange data model and format [REF20]. This request is subsequently sent to the Data Service.	Steps (18)-(27) need to be repeated for each selected provider of each selected evidence type. The diagram omits the use of Access Points and the details of the use of eDelivery.
19, 24	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.
20-21	In order to process the request and approve the exchange of evidences, the Data Service interacts with the Matching Service to uniquely identify the user.	
22-23	In case of a successful match, the Data Service will find any evidences for the specified evidence type for the user and constructs the response using the OOTS packaging [REF20].	
25, 26	The Once-Only Staging Area shows the evidence(s) that have been retrieved to the User. The User determines which (if any) evidence(s) he or she wants to approve for use in the procedure.	Note that at this stage the evidence has been transmitted to the Portal, but it has not been formally accepted and is therefore not “exchanged” in the sense understood in Article 14.3.f.
27	With the approval of the User, the Once-Only Area transfers the approved evidences to the Online Procedure Portal. This concludes the use of the Once-Only Technical System.	The evidence is now formally “exchanged” and available for the procedure.

10.2. Simplified Flow

Another example flow is shown in Figure 10. This flow is much simpler than the one in Figure 9.

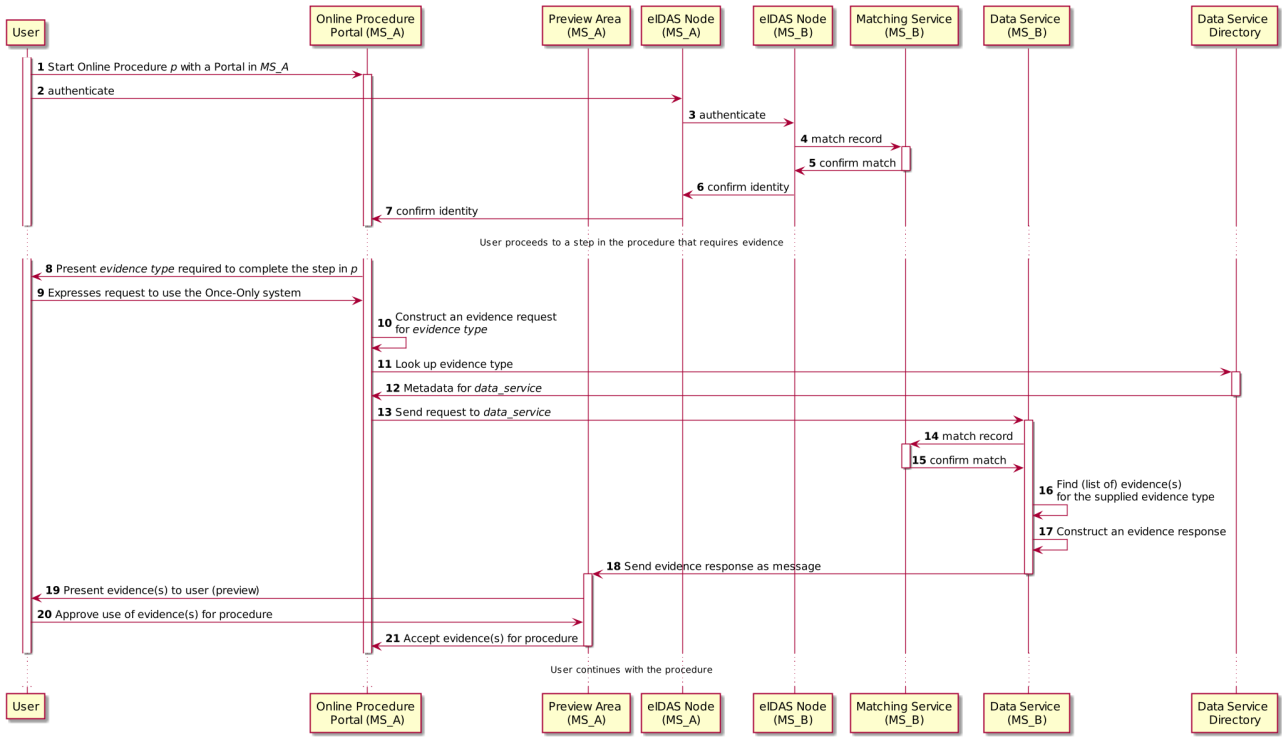

Figure 10 Simplified Once-Only Technical System Flow

Step	Description	Notes
1-7	The first seven steps are the same as in the previous sample: the User starts a procedure in an Online Procedure Portal and authenticates him or herself.	
8	This step differs in that a specific evidence type is needed at a step in the procedure.	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.
9	As before, the User explicitly requests to use the Once-Only Technical System.	This flow assumes the Online Procedure Portal includes the functionality to interact with the Once-Only Technical system. There is no separate Once-Only Area.

Step	Description	Notes
10-17	The request is processed similarly to steps (18) - (23) in the previous flow,the response is sent to the portal, and then previewed and decided on as in steps (25) to (27).	The steps (10)-(17) from the previous diagram are omitted, as we assume that MS_A knows which evidence type to request for the requirement from MS_B.
18	The returned evidence is routed to the Preview Space	In this simplified scenario, only preview is handled in an component that is separate from the Online Procedure Portal. The other Once-Only related interactions with the user are handled by the Online Procedure Portal
19-20	The user previews the evidence in the preview space and approves its use.	This step is like steps (25)-(26) in the other scenario.
21	The approved evidence is transferred to the Online Procedure Portal.	

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

- The Evidence Broker is not needed, due to the assumption that harmonized evidence types are used.
- The Data Service Directory returns just a single data service for that evidence type in MS B, so no choice is needed.
- 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 and to support selection of data services.
- The number of steps is much smaller than the number of steps in the more complex flow.
- The User is involved in far fewer steps, and less input is required from him or her.

[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.

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