European Commission

Synergies between the

Once-Only Technical System

and the

EUDI Wallet

INTERIM REPORT

MARCH 2024

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Executive summary

The Once-Only Technical System and the EU Digital Identity Wallet are two EU initiatives designed to facilitate the interactions of citizens and businesses with EU public administrations.

The Once-Only Technical System, established as part of the Regulation (EU) 2018/1724, aims to allow citizens and businesses to reuse information (evidence) already kept by relevant authorities in any Member State, when carrying out an online procedure in a cross-border context, e.g. registering an address or vehicle in another Member State. When using the Once-Only Technical System, citizens and businesses are not required to manually upload the information necessary to carry out a cross-border online procedure, if the same information was already provided to another public administration in the EU.

The EU Digital Identity Wallet stems from the revision of the eIDAS Regulation. The original regulation already provided the mechanisms to access highly secure electronic identity solutions in a cross-border context. The revision of the eIDAS Regulation introduces, the concept of EU Digital Identity Wallet, among other innovations. The EU Digital Identity Wallet will enable citizens and businesses to store identity data, credentials linked to their identity and other data issued by trusted sources. In addition, the EU Digital Identity Wallet will allow citizens and businesses to provide data to relying parties on request, to use their data for (1) online and offline authentication, and (2) for the provision of data to digital services. Member States are expected to implement the EU Digital Identity Wallet at the national level.

The Commission recognised the need for cooperation, interoperability and complementarity of the two initiatives. In February 2022, the Commission — supported by the Member States — decided to establish a group of experts (henceforth referred to as the Contact Group) to analyse and define an implementation strategy for several synergies between the Once-Only Technical System and the EU Digital Identity Wallet. A synergy between the OOTS and the EU Digital Identity Wallet entails that one system reuses the capabilities of the other system either in its entirety or a component thereof. The analysed synergies are categorised in two different groups　:

1. **User experience synergies.** These entail the reuse of the EU Digital Identity Wallet by the Once-Only Technical System to facilitate and enrich the user experience of citizens and businesses when carrying out an online procedure in a cross-border context.
2. **Investment synergies.** These entail the reuse of OOTS general-purpose building blocks in the EU Digital Identity Wallet ecosystem. The reuse of building blocks is expected to optimise IT investments for the European Commission, Member States and the private sector, as it prevents the proliferation of competing technical infrastructures and their parallel operations and maintenance. Furthermore, the reuse of already tested building blocks aims to help minimise the risks for the roll out of EU Digital Identity Wallets.

In addition to helping identify opportunities to improve the user experience and optimise investments, the analysis of the synergies allowed the Contact Group to better position and define the functional boundaries between the Once-Only Technical System and the EU Digital Identity Wallet. In concrete terms, the Once-Only Technical System could be used to facilitate the issuance of electronic attestations of attributes by trust service providers to business and citizens. As an example, citizens could use the Once-Only Technical System to request the issuance of a European Health Insurance Card (EHIC) to have access to healthcare treatments during a temporary stay in any EU country. If the EHIC is issued as an Electronic Attestation of Attributes, citizens could use their EU Digital Identity Wallet to present it to healthcare providers for verification.

Figure 1 provides an overview of the synergies analysed by the Contact Group so far.

User experience synergies		
Synergy 1	**Synergy 2** Status: *Under investigation*	**Synergy 3** Status: *Agreed*
The EUDI Wallet provides an additional way for citizens and businesses for authentication and identification purposes when using the Once-Only Technical System. **Variant 1** Status: *Agreed* Identification and authentication of natural persons acting on their own behalf[1] **Variant 2** Status: *Under investigation* Identification and authentication with representation[2]	The preview area may offer the option for the user to start the process of issuance of the evidence in the EUDI format. Upon finalisation of the procedure, competent authorities can offer the option to issue the output of the procedure in the EUDI format.	Citizens and businesses can combine evidence uploaded from the EUDI Wallet with evidence retrieved through the Once-Only Technical System.

Investment synergies	
Synergy 4 Status: *Under investigation*	**Synergy 5** Status: *Under investigation*
Qualified Trust Service Providers (QTSPs[3]) could use the Common Services of the Once-Only Technical System to discover the authentic sources of evidence. The QTSPs could also use the Once-Only technical system message exchange protocol and operational framework to request the attributes from the authentic data source.	Citizens and businesses could use the Common Services of the Once-Only Technical System to discover the authentic sources able to provide QEAA and EAA.

Figure 1: Overview of the synergies analysed by the Contact Group

For the synergies marked as agreed in the figure above, the Contact Group reached a consensus on their relevance and implementation. Technical and legal analysis activities need to be carried out to determine how and when the synergies can be implemented. For synergies under investigation, the Contact Group acknowledged their potential, but additional discussions are needed to create more concrete proposals.

Note that in some cases the implementation of the identified synergies depend on the eIDAS legislative process. As a result, the timelines and milestones of the future work of the Contact Group must be aligned with the timelines of the EU Digital Identity Wallet legislative process. As such, after the adoption of the revised eIDAS Regulation, work will start on the drafting and adoption of relevant Implementing Acts. During this process, the eIDAS stakeholders will consider and analyse the synergies identified by the Contact Group. At the same time, the Contact Group may further detail the value proposition of the Once-Only Technical System, including its Common Services to be presented to the

---

[1] This variant refers to electronic **identification and authentication** through eID means that have been issued under an electronic identification scheme that has been notified in accordance with Regulation (EU) No 910/2014 to authenticate **the users acting on their own behalf.**

[2] This synergy refers to electronic **identification and authentication** through eID means that have been issued under an electronic identification scheme that has been notified in accordance with Regulation (EU) No 910/2014 to authenticate **the users acting on behalf of a natural or legal person.**

[3] It is important to highlight that a QTSP mayis not be the authentic source of evidence. In this context, a QTSP is a third party (natural or legal person), who provides a trust service for the issuance of (Q)EAAs.

eIDAS actors in the context of synergy 4 and 5. Before the adoption of the relevant Implementing Acts, the Contact Group may also identify and analyse additional potential synergies between the Once-Only Technical System and the EU Digital Identity Wallet. Finally, once the revised eIDAS Regulation and its Implementing Acts are adopted, the Contact Group may assess the technical impact of the implementation of the agreed synergies on both the Once-Only Technical System and the EU Digital Identity Wallet.

Herbert **Leitold**

Director General A-SIT

Role in the contact group
- ■ Member
- ☐ Observer

Member of
- ■ SDG Coordination group
- ■ eIDAS Expert group

OOTS and the EUDI Wallet are the major initiatives to ease services for European citizens and businesses. In first working on the most obvious synergies between these the contact group only started learning how this leads to even better user experience. With the EUDI Wallet increasingly taking shape continuing the work in the contact group can dig deeper and is expected to identify further elements where OOTS and EUDI can cross-fertilise to improve services and make better use of the infrastructure investments.

The need to have a solid, clear, cross border, definition of powers and mandates is key for the functioning of SDGR Annex II Procedure #16, therefore, we believe that the Contact Group is vital for the definition of the future operation of the OOTS. Without these synergies between eIDAS and SDGR/OOTS these procedures will hardly be fully provided via Technical System.

Jorge **Sousa**

Portuguese national coordinator for European Single Digital Gateway, Administrative Modernization Agency (AMA)

Role in the contact group
- ■ Member
- ☐ Observer

Member of
- ■ SDG Coordination group
- ☐ eIDAS Expert group

Michal **Ohrablo**

Ministry of Investments, regional development and informatization of the Slovak Republic

Role in the contact group
- ■ Member
- ☐ Observer

Member of
- ■ SDG Coordination group
- ■ eIDAS Expert group

Experts in the group clearly see a window of opportunity provided by the two new initiatives. We can tackle some recurring issues in the area of identification and sharing of data with and within public administration. We see the needs and viable solutions, now we need to use momentum and carry out actions

I firmly believe that it is utmost important to work further on this synergy. As both areas are still under preparation, it is necessary that the work on this synergy continues. Even more, I believe that the Contact group will gain the importance in the upcoming months, years to reach user-centric solutions for citizens and companies to boost the digital single market.

Alenka **Zuzek Nemec**

Slovenian Ministry of Public Administration

Role in the contact group
- ■ Member
- ☐ Observer

Member of
- ■ SDG Coordination group
- ■ eIDAS Expert group

Key definitions

Throughout this document, the terms below are defined as follows:[4]

Table 1: Key definitions

Term	Definition
Authentic source	'Authentic source' means a repository or system, held under the responsibility of a public sector body or private entity, that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in national law.
Authentication	'Authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.
Data Service Directory	'Data service directory' means a registry containing the list of evidence providers and the evidence types they issue together with the relevant accompanying information.
Electronic Identification	'Electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
Electronic identification means	'Electronic identification means' means a material and/or immaterial unit containing person identification data, and which is used for authentication for an online service.
Electronic identification scheme	'Electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons.
European Digital Identity Wallet	'European Digital Identity Wallet' means a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service, and to create qualified electronic signatures and seals.
Evidence	'Evidence' means any document or data, including text or sound, visual or audio-visual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements.
Evidence Broker	'Evidence broker' means a service allowing an evidence requester to determine which evidence type from another Member State satisfies the evidence requirement for the purposes of a national procedure.
Evidence Provider	'Evidence provider' means a competent authority [...] that lawfully issues structured or unstructured evidence;
Evidence Requester	'Evidence requester' means a competent authority responsible for one or more of the procedures

---

[4] The definitions have been inspired by the Commission Implementing Regulation (EU) 2022/1463 and the Proposal for amending the eIDAS regulation (EU) No 910/2014

Mandate Management System	A mandate management system is an IT system that allows the definition of electronic powers of representation and mandates. Mandate management systems are usually seamlessly integrated with identity management systems to empower users to act on behalf of a third party, e.g. a natural or legal person.
Once-Only Technical System	'Once-only technical system' ('OOTS') means the technical system for the cross-border automated exchange of evidence referred to in Article 14(1)[5] of Regulation (EU) 2018/1724, i.e. Single Digital Gateway Regulation.
Online procedure	'Online procedure' means a sequence of actions that must be taken by users to satisfy the requirements, or to obtain from a competent authority a decision, in order to be able to exercise their rights.
Procedure portal	'Procedure portal' means a webpage or a mobile application where a user can access and complete an online procedure.
Preview space	'Preview space' means a functionality that enables the user to preview the requested evidence before exchanging it with the data requester.
(Qualified) Electronic Attestation of Attributes - (Q)EEA	'(Qualified) Electronic Attestation of Attributes' means an attestation in electronic form that allows the authentication of attributes, which is issued by a qualified trust service provider.
Qualified Trust Service	'Qualified trust service' means a trust service that meets the applicable requirements laid down in the eIDAS Regulation.
(Qualified) Trust Service Provider – (Q)TSP	'Qualified trust service provider' means a natural or a legal person who provides one or more qualified trust services.
Trust Service	A 'trust service' means an electronic service normally provided against payment which consists of […] the creation, verification, and validation of […] electronic attestation of attributes.

---

[5] For the purpose of the exchange of evidence for the online procedures listed in Annex II [of the Single Digital Gateway Regulation] and the procedures provided for in Directives 2005/36/EC, 2006/123/EC, 2014/24/EU and 2014/25/EU, 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.

1. Introduction

1.1 Background

The eGovernment Action Plan 2016-2020 envisioned that public administrations should ensure that citizens and businesses should only supply the same information once by reusing data already provided by users. It also launched cross-border pilots, notably the Once-Only Principle Project (TOOP), which explored and demonstrated the possible implementation path of the "Once-Only" principle (OOP) through multiple sustainable pilots.

Regulation (EU) 2018/1724, establishing a single digital gateway, requires that the Commission, in cooperation with Member States, creates and implements a technical system for a cross-border automated exchange of evidence (the Once-Only Technical System - OOTS). This system will substantially facilitate the use of agreed online procedures[6], as citizens and businesses will not have to manually upload cross-border evidence, which is already kept by the relevant competent authorities in any Member State. The OOTS will securely connect the authentic sources of EU Member States public authorities, so that they can exchange official documents and data (evidence), at the request of citizens and businesses as part of cross-border administrative procedures, e.g. when registering an address or vehicle in another Member State. This innovative system will help eliminate the burden on citizens and businesses to manually search, map, fetch and provide pieces of evidence in different Member States. In addition, it will facilitate the exchange of information between Member State´s Competent Authorities.

In parallel, as part of the eIDAS revision, in June 2021, the Commission proposed to introduce the EU Digital Identity Wallet. The current eIDAS Regulation[7] already provides the instruments for the cross-border use of highly secure and trustworthy electronic identity solutions. The EU Digital Identity Wallet will complement the existing electronic identity solutions. It will be provided as a service by the Member States to allow citizens and businesses to store identity data, credentials and attributes linked to their identity, to provide them to relying parties on request, to use them for authentication, online and offline, for a service, and to create qualified electronic signatures and seals. The EU Digital Identity Wallet common technical standards interfaces will be defined in upcoming implementing acts, once the regulation is adopted.

In parallel to the EU Digital Identity legislative process, the Commission is working with Member States on the technical implementation of the European Digital Identity framework. The Commission Recommendation accompanying the June 2021 eIDAS revision Proposal provides that Member States and the Commission develop a Toolbox, including a comprehensive technical architecture and reference framework, common standards and technical references and guidelines and best practices for the European Digital Identity, including EU Digital Identity Wallet.

The Commission acknowledged the need for interoperability between the EU Digital Identity Wallet and OOTS initiatives, and reinforced the importance of their complementarity and synergies (understanding synergies as the reuse of capabilities of the systems involved) that could add value for businesses and citizens, while optimising investments on both projects.

During the February 2022 Council Internal Market Working Group meeting, the Commission presented an overview of potential synergies between the OOTS and EU Digital Identity Wallet initiatives. In 2023, the Commission, supported by the Member States, created the informal group of experts "OOTS and EU DIGITAL IDENTITY Wallet Synergies and Interoperability Contact Group" (henceforth referred to as the "Contact Group") to ensure that the synergies presented during the Council meeting are taken up

---

[6] The procedures falling in the scope of the Once-Only Technical System are the ones specified in Art. 14 and Annex II of the SDG Regulation

[7] 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 (eIDAS)

by both initiatives, and that they agree to implement them. The synergies that were presented are categorised in two groups:

1. **User experience synergies**. These entail reuse of the EU Digital Identity Wallet to facilitate and enhance the experience of citizens and businesses when carrying out cross-border administrative procedures using the Once-Only Technical System.
2. **Investment synergies**. These seek to reduce investments by reusing common building blocks relevant for both initiatives. The reuse of common building blocks aims to help avoid the creation of parallel components with similar functionalities, which would need to be maintained and operated, thus leading to growing costs for the European Commission and the Member States.

The Contact Group is composed of experts coming from two Commission Expert Groups supporting the successful implementation of the Once-Only Technical System and the EU Digital Identity Wallet initiatives, respectively:

1. The Single Digital Gateway Coordination Group (abbreviation "SDG Coordination Group") mandated by the Regulation (EU) No 2018/1724 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services.

2. The eIDAS Expert Group mandated by the Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the 'eIDAS regulation') (adopted on 23 July 2014).

The Contact Group reflects a balanced representation from Member State experts from the SDG coordination group and the eIDAS expert group. It also includes representatives from the European Commission, namely DG GROW, as policy owner of the SDG, DG CNECT, as policy owner of eIDAS, and DIGIT, as the solution provider.

The figure below presents the current composition of the Contact Group (members, observers and Secretariat).

Figure 2: Contact Group members and observers

The difference between Members and Observers is that Observers and their representatives may be permitted to take part in the discussions of the group and provide expertise. However, they shall not have voting rights and shall not participate in the formulation of recommendations or advice of the group.

To date, the Contact Group held five meetings after its inauguration in 2023. Figure 3 on the next page presents the timeline of these meetings.
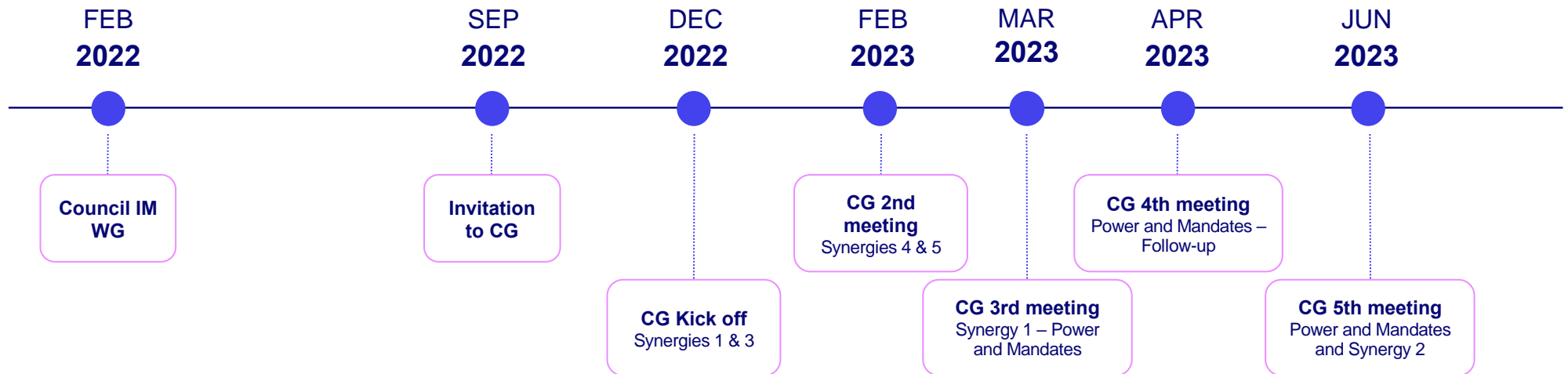
Figure 3: Meetings held by the Contract Group

Note that during the period when the Contact Group held their meetings, the Once-Only Technical System and EU Digital Identity initiatives were in very different stages of development. The Once-Only Technical System   already has an adopted legal basis with the Single Digital Gateway Regulation, and Implementing Regulation, which also mandates the reuse of eIDAS. Furthermore, Member States were already working on the implementation of the Once-Only Technical System at the national level. While the EU Digital Identity legal basis was still under discussion by the Parliament and Council, in the so-called trilogue process. As a result, EU Digital Identity did not have a stable legal basis, and the Implementing Regulations will only be drafted in the coming months   after the regulation is adopted.

1.2 Purpose

This is an interim report that marks the end of the first round of discussions of the Contact Group. The content of the report is based on the extensive minutes of Contact Group meetings.

This report aims to provide a summary of the work and of the analysis that has been carried out by the Contact Group, as well as the conclusions that have been reached. This includes the identification of synergies between the Once-Only Technical System and the EU Digital Identity Wallet initiatives, a summary of the discussions held within the Contact Group and the agreements reached by the Member States, the key results and way forward.

This information shall serve to raise awareness of the work being done by the Contact Group providing understanding of its activities and their status to a broader audience (technical and non-technical), including members of the SDG coordination group and the eIDAS Expert group that are not part of the Contact Group.

This report also highlights the importance and the future scope of the continued work of the Contact Group and encourages continuous support by all stakeholders from both expert groups and the European Commission in this important initiative.

2. Synergies between the Once-Only Technical System and the EU Digital Identity Wallet

The Contact Group discussed and analysed five synergies between the EU Digital Identity Wallet and the Once-Only Technical System, as presented by the Commission during the February 2022 Council Internal Market Working Group meeting.

A synergy emerges when one system reuses the other system either in its entirety or in its components, to fulfil a legal requirement. In some cases, a synergy has several variants, corresponding to different real-life scenarios, e.g. synergy 1 has two variants: (1) use of the EU Digital Identity Wallet to authenticate natural or legal persons acting on their own behalf, and (2) use of the EU Digital Identity Wallet to authenticate natural persons representing and acting on behalf of another natural or legal person.

Table 2 below shows an overview of the synergies discussed by the Contact Group.

Table 2: Overview of the synergies between the Once-Only Technical System and the EU Digital Identity Wallet

User experience synergies		
Synergy 1 Status: **Agreed**	**Synergy 2** Status: **Under investigation**	**Synergy 3** Status: **Agreed**
The EUDI Wallet will provide an additional way for citizens and businesses for authentication and identification purposes when using the Once-Only Technical System. **Variant 1** Status: **Agreed** Identification and authentication of natural persons acting on their own behalf[8] **Variant 2** Status: **Under investigation** Identification and authentication with representation[9]	The preview area may offer the option for the user to start the process of issuance of the evidence in the EUDI format. Upon finalisation of the procedure, competent authorities may offer the option to issue the output of the procedure in the EUDI format.	Citizens and businesses can combine evidence uploaded from the EUDI Wallet with evidence retrieved through the Once-Only Technical System.

Investment synergies	
Synergy 4 Status: **Under investigation**	**Synergy 5** Status: **Under investigation**
Qualified Trust Service Providers (QTSPs[10]) could use the Common Services of the Once-Only Technical System to discover the authentic sources of evidence. The QTSPs could also use the Once-Only technical system message exchange protocol and operational framework to request the attributes from the authentic data source.	Citizens and businesses could use the Common Services of the Once-Only Technical System to discover the authentic sources able to provide QEAA and EAA.

---

[8] This variant refers to electronic **identification and authentication** through eID means that have been issued under an electronic identification scheme that has been notified in accordance with Regulation (EU) No 910/2014 to authenticate **the users acting on their own behalf.**

[9] This synergy refers to electronic **identification and authentication** through eID means that have been issued under an electronic identification scheme that has been notified in accordance with Regulation (EU) No 910/2014 to authenticate **the users acting on behalf of a natural or legal person.**

[10] It is important to highlight that a QTSP may not be the authentic source of evidence. In this context, a QTSP is a third party (natural or legal person), who provides a trust service for the issuance of (Q)EAAs.

The analysis of the defined synergies helped the Contact Group better position and clearly define the boundaries between the Once-Only Technical System and the EU Digital Identity Wallet. From the outset, the Once-Only Technical System has been conceived to issue documents to citizens and businesses in a cross-border context. In addition, upon the finalisation of an administrative procedure, the output of the procedure is delivered to the end-users, e.g. European Health Insurance Card (EHIC), for future use. If EHIC is issued as an Electronic Attestation of Attributes, citizens could use their EU Digital Identity Wallet to present it to verifiers.

Based on the above, both the Once-Only Technical System and the EU Digital Identity Wallet are about making the issuance of documents easier for business and citizens. The EU Digital Identity Wallet additionally facilitates the verification of those documents by both public authorities and private entities.

The table below presents an overview of how each synergy is described in this report.

Table 3: Overview of fields used to detail each synergy

Field	Description
Visual representation	High-level overview of how the EU Digital Identity Wallet and the Once-Only Technical System interact in a cross-border context.
Requirement	Legal requirement that the synergy aims to address.
Description	Detailed description explaining how the Once-Only Technical System and the EU Digital Identity Wallet interact once the synergy is implemented.
What's being reused	Information whether the EU Digital Identity Wallet reuses the Once-Only Technical System (or components thereof), or vice versa[11].
Step in the user journey	Information about at which step of the user journey the end-user benefits from the synergy. The steps refer to the <u>Once-Only Technical System user journey</u> as described in the Once-Only hub collaborative space[12] [13].
Benefits	Information about the advantages that the implementation of the synergy would bring in the implementation of the (legal) requirement. There are four types of benefits: **Improved user experience:** the synergy improves the experience of citizens and businesses by making the user journey easier or richer. **Optimised investments:** the synergy helps achieve investment gains through, for instance, the reuse of <u>building blocks</u>[14]. **Faster time to market:** the synergy accelerates the implementation of the services offered by the Once-Only Technical System or the EU Digital Identity Wallet. **Minimised risks:** the synergy minimises risks through the adoption of building blocks already used in real life systems.

---

[11] The Once-Only Technical System will use eIDAS from the outset as mandated by the Commission Implementing Regulation (EU) 2022/1463 (Article 3). The evolution of eIDAS from its current version to the wallet will be taken up as soon as the procedure portals of the Member States will support it.

[12] Key steps in the once only journey https://ec.europa.eu/digital-building-blocks/wikis/display/OOTS/User+Journey+-+Step+1+Authentication

[13] The step in the user journey field will only be described for the synergies affecting the OOTS user journey. The EU Digital Identity Wallet does not have a user journey defined and published.

[14] It is important to highlight that investments do not derive exclusively from the creation of a new IT system. More importantly, investments are required for the maintenance and operations of the new IT system after its creation.

Field	Description
Status	Information about the level of consensus of the Contact Group on the synergy. The synergy can be either: • **Agreed:** The Contact Group agrees about the relevance of the synergy and on its implementation. Technical or legal analysis activities shall be carried out. The report also provides a tentative timeline of the actions that need to be undertaken for the agreed synergy to be implemented; or • **Under investigation:** The Contact Group did not reach a common position on the relevance of the synergy and its implementation. Additional discussions with relevant stakeholders must take place to either reach consensus (agreed synergy) or disregard the synergy (rejected synergy); or • **Rejected:** The Contact Group decided to disregard the synergy, which will not be implemented.
Challenges and actions agreed by the Contact Group	For synergies under investigation, information about the challenges that prevented an agreement from being reached.
Alternatives	For synergies under investigation, alternative approaches to implement the synergy, should they be needed.
Timeline and actions for implementation	For agreed synergies, information about the potential timeline, as well as the actions that need to be undertaken for the implementation of the synergy.

2.1 User experience synergies

This section describes a set of synergies aiming to facilitate and enrich the user experience of citizens and businesses carrying out cross-border administrative procedures and choosing to use the Once-Only Technical System instead of manually uploading the evidence requested by public administrations. The user experience will be improved, first, using eIDAS in its current implementation, and afterwards using the EU Digital Identity Wallet. In its current and future implementation, eIDAS will improve the OOTS user experience by making the SDG online procedures accessible from a distance using notified eID schemes.

The EU Digital Identity Wallet may be used in different steps of the Once-Only Technical System user journey as depicted in Figure 4 below.
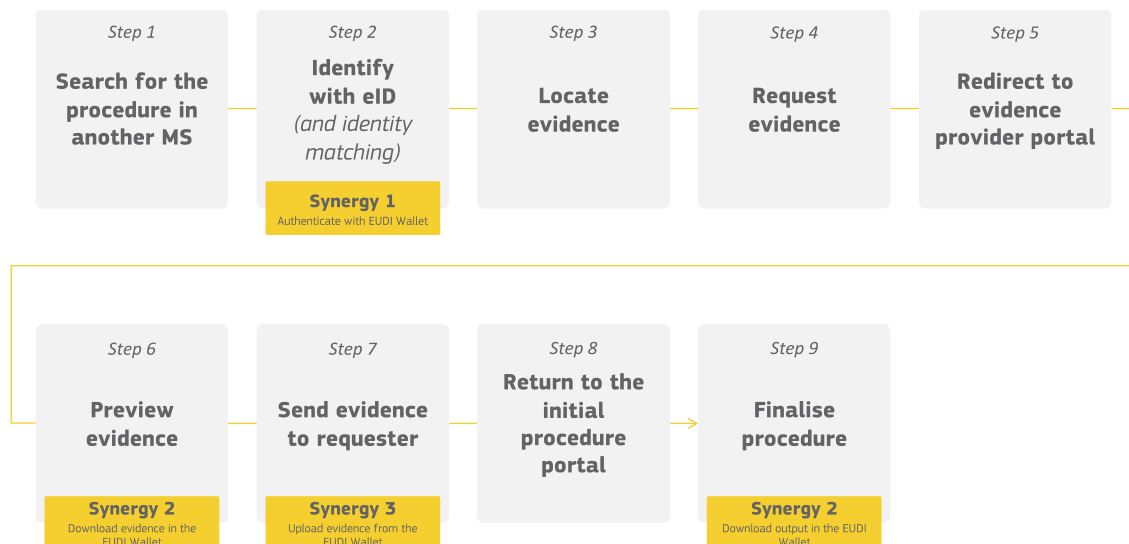

Figure 4: Once-only technical system user journey

The OOTS user journey starts when an end-user from one Member State accesses an administrative procedure in another Member State, e.g. if a user wishes to request a change of address after moving in another Member State. The user is requested to identify with a notified eID means[15], before being able to carry out the procedure. At this step, the solution becomes more accessible by enabling the end-user to identify with her/his EU Digital Identity Wallet (**synergy 1**).

As next step, the end-user may be requested to provide some evidence, e.g. a proof of residence, to finalise the online procedure. The user can choose to provide the evidence by manually uploading it (default mechanism), e.g. from his/her computer, requesting it using a national data exchange solution, providing the evidence as an electronic attestation of attributes from his/her EU Digital Identity Wallet (**synergy 3**), or to request its automatic retrieval directly from the authentic data source in another Member State through the Once-Only Technical System. If the user decides to retrieve the evidence through the Once-Only Technical System, she/he will be redirected to the evidence provider portal to preview the evidence before sharing it with the original national portal providing the online procedure. At this step, the competent authority (evidence provider) may issue the evidence as a (Q)EAA in a format compatible with the EU Digital Identity Wallet (**synergy 2**).

It is worth noting that evidence is not standardised across Member States. One advantage of using the Once-Only Technical System is that it automatically maps the requirements of an administrative procedure, in terms of documents to be provided, to different types of evidence in the Member States. For example, to prove a citizen's residence, different Member States may provide different types of evidence. This automatic mapping is crucial for a smooth user journey, which otherwise would require end-users to identify manually whether the available type of evidence meets the procedure portal's requirements or not.

Once all necessary pieces of evidence are provided, the end-user will be able to finalise the online procedure in the national portal. At this step, the competent authority providing the online procedure may issue the output of the procedure, e.g. confirmation of registration at the new address, as a QEAA compatible with the format required by the EU Digital Identity Wallet (**synergy 2**).

The remainder of this section provides a more detailed description of the synergies mentioned above.

---

[15] To date, users can already authenticate using the eID means, which have been notified by almost every Member State under the current implementation of eIDAS.

SYNERGY 1.

The **EUDI Wallet** provides an additional way for citizens and businesses for authentication and identification purposes when using the Once-Only Technical System

Variant 1

identification and authentication of natural persons acting on their own behalf

Member State A

Member State B

Data Requester

" *I want to change my address to Member State A.*

My country of origin provides the evidence.

Data Provider

"

eGov Portal

Cross-border **Authentication**

OOTS

Authentic Data Source

MY OPTIONS

EUDI
tomorrow

Notified eID means
today

Synergy 1: The EUDI Wallet provides an additional way for citizens and businesses for authentication and identification purposes when using the Once-Only Technical System.

Variant 1: identification and authentication of natural persons acting on their own behalf

Requirement

In line with Article 3.1 of the Commission Implementing Regulation (EU) 2022/1463[16], Member States shall ensure that **evidence requesters are connected to an eIDAS-node to enable user authentication** […], either directly or through an intermediary platform. Furthermore, according to Article 11 of the same Regulation, **evidence requesters shall rely on electronic identification means** that have been issued under an electronic identification scheme **that has been notified** in accordance with Regulation (EU) No 910/2014 **to authenticate the users acting on their own behalf** […].

What's being reused

OOTS reusing EU Digital Identity Wallet

Status

⊘ **Agreed**

Step in the user journey

Identify with eID > Select eID Means

(Step 2 of the user journey)

Benefits

☑ Improved user experience
☐ Optimised investments
☐ Faster time to market
☑ Minimised risks

Description

This synergy entails that the Once-Only Technical System reuses the EU Digital Identity Wallet to identify and authenticate natural persons as set out in the Commission Implementing Regulation (EU) 2022/1463. The EU Digital Identity Wallet becomes an additional identification and authentication mechanism complementary to the existing notified eID schemes.

In practice, end-users could use the EU Digital Identity Wallet to:

1. Identify and authenticate themselves to a national procedure portal in a cross-border context, for instance to request a change of address; and
2. Identify and authenticate themselves to the Once-Only Technical System preview area[17] when previewing evidence from national authentic sources[18].

Timeline and actions for implementation

The implementation of this synergy can be carried out once citizens are using EU Digital Identity Wallets, and OOTS Procedure Portals have implemented EU Digital Identity Wallet specific interfaces. Regarding the readiness of the once-only technical system, the Commission Implementing Regulation (EU) 2022/1463 already mandates the use of eIDAS, as well as of its evolution towards the EU Digital Identity Wallet, as an authentication mechanism. Therefore, no amendment on the Once-Only Technical System legal basis is foreseen. Similarly, from a technical standpoint, the architecture of national procedure portals should already accommodate the additional authentication means based on the EU Digital Identity Wallet. Therefore, the technical impact on the Once-Only Technical System should be limited   .

Based on the above considerations, the following actions need to be carried out before this synergy can be implemented:

Action	Responsible	When

---

[16] Commission Implementing Regulation setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1463

[17] The Once-Only Technical System Preview Space: exchanging evidences through Once-Only Technical System will happen at the request of the user. The user should remain free to submit evidence by other means outside the technical system and, crucially, the user should have the possibility to preview the evidence and the right to choose not to proceed with the exchange of evidence in cases where the user, after previewing the evidence to be exchanged, discovers that the information is inaccurate, out-of-date, or goes beyond what is necessary for the procedure in question.

[18] If the preview area is provided by an evidence provider located in the same country of origin of the end-user, then eIDAS is less relevant, and national identification and authentication schemes may apply.

Analyse and determine the changes to be made on national procedure portals to allow users to use the EU Digital Identity Wallets for identification and authentication purposes	Member States *(eIDAS)*	2025-2026 *(Provisional)*

SYNERGY 1.

The EUDI Wallet provides an additional way for citizens and businesses for authentication and identification purposes when using the Once-Only Technical System

Variant 2

identification and authentication with representation

Member State A

B Member State

Data Requester

" *I want to notify my business activity in Member State A.*

Data Provider

" *My country of origin provides the evidence.*

eGov Portal

Cross-border **Authentication**

OOTS

Authentic Data Source

User representing a legal person

MY OPTIONS

EUDI
tomorrow

Notified eID means
today

Synergy 1: The EUDI Wallet provides an additional way for citizens and businesses for authentication and identification purposes when using the Once-Only Technical System.

Variant 2: identification and authentication with representation

Requirement
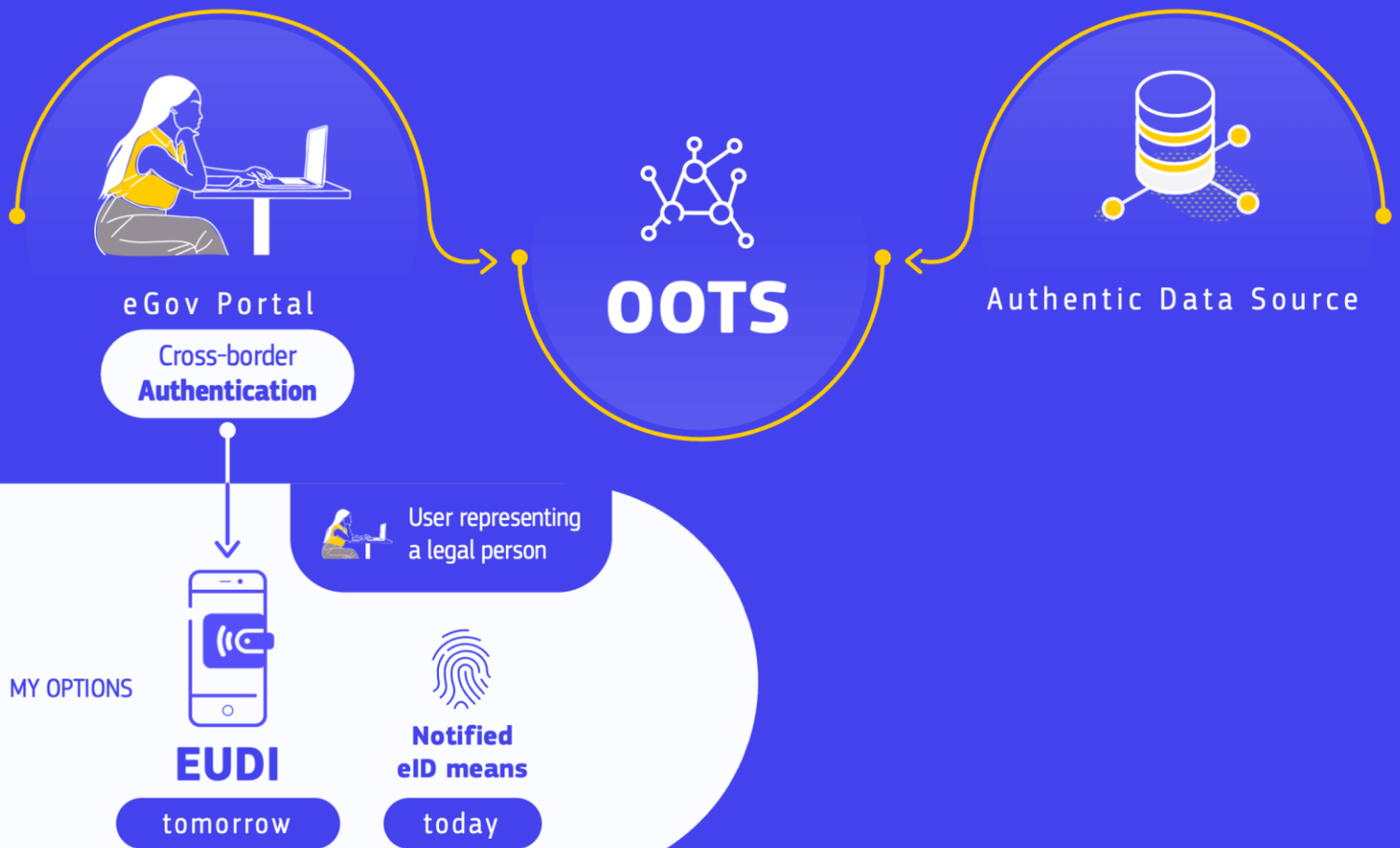
In line with Article 11 of the of the Commission Implementing Regulation (EU) 2022/1463[19], **evidence requesters shall rely on electronic identification means** that have been issued under an electronic identification scheme **that has been notified** […] **to authenticate users acting through a representative** […].

In practice, evidence requesters must support the identification and authentication of both natural and legal persons, as well as electronic powers of representation and mandates to allow natural persons to act on behalf of other natural or legal persons.

What's being reused

OOTS reusing EU Digital Identity Wallet

Status

⏳ **Under investigation**

Step in the user journey

Identify with eID > Select eID Means

(Step 2 of the user journey)

Benefits

- ☑ Improved user experience
- ☐ Optimised investments
- ☐ Faster time to market
- ☐ Minimised risks

Description

This synergy entails that the Once-Only Technical System reuses the EU Digital Identity Wallet to enable the identification and authentication of a natural person acting on behalf of another natural or a legal person. Like the previous variant, the EU Digital Identity Wallet becomes an additional identification and authentication mechanism complementary to existing notified eID schemes.

In the future, if natural persons using their EU Digital Identity Wallet are identified and authenticated as representing another natural or legal person, they could:

1. Access to a national procedure portal, for instance to pay corporate taxes on behalf of a company; and
2. Access the Once-Only Technical System preview area[20] when requesting evidence from the national authentic source[21].

It is important to highlight that the information about the representation of a natural or legal person must be provided along with the personal identification data of the EU Digital Identity Wallet, otherwise OOTS will not allow the request of evidence regarding the represented entity. For instance, an accountant or lawyer can only request evidence about a company in another Member State if the representation right is included in the electronic identity.

Challenges and actions agreed by the Contact Group

The biggest obstacle to this variant of the synergy is that OOTS enables the request of evidence about another person only if it stems from the eID means. eIDAS support for electronic powers and mandates is currently limited. There are three notified eID means out of twenty that support such a feature and even then, the scope of powers and mandates is not commonly defined in different Member States. Furthermore, the eIDAS Regulation does not harmonise mutual recognition of (1) scope of powers of a representative (it only supports 'full power'), nor (2) types of mandates. Discussions in the Contact Group revealed that Member State approaches to powers and mandates are quite different. In some cases, information about powers and mandates is a value-added service of the authentication service, in other cases it is a

---

[19] Commission Implementing Regulation setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1463

[20] The Once-Only Technical System Preview Space: exchanging evidences through Once-Only Technical System will happen at the request of the user. The user should remain free to submit evidence by other means outside the technical system and, crucially, the user should have the possibility to preview the evidence and the right to choose not to proceed with the exchange of evidence in cases where the user, after previewing the evidence to be exchanged, discovers that the information is inaccurate, out-of-date, or goes beyond what is necessary for the procedure in question.

[21] If the preview area is provided by an evidence provider located in the same country of origin of the end-user, then eIDAS is less relevant, and national identification and authentication schemes may apply

separate evidence type and in other cases the information about powers and mandates is not retrieved from elsewhere but kept within the procedure portal itself.

Before moving forward with this variant of the synergy, the Contact Group shall identify and analyse short and medium term solutions to allow users to represent and act on behalf of another natural person or a company with a defined set of representation powers. At the same time, DG CNECT will work on finding solutions for power and mandates in the context of eIDAS.

More specifically, the Contact Group recognised the following challenges and identified the following related actions:

Challenge	Action	Responsible
How to determine the powers authenticated users have when acting on behalf of a company? Currently eIDAS only supports 'full power'	**Short and medium term**	
	Enable the exchange of information on the scope of powers through eIDAS[22] based on the use of sectorial attributes already foreseen in the current eIDAS specifications. Nevertheless, the following two aspects must be analysed: • The impact of using sectorial attributes on the eIDAS nodes and national portals; and • The legal value of using eIDAS to exchange information about the scope of powers. Furthermore, it must be highlighted that the scope of sectorial attributes may be limited and may not cover all OOTS procedures.	Contact Group
	Define a controlled vocabulary to express the values of the powers of representation used in the context of the OOTS as a sector-specific attribute.	OOTS Team
	Perform a mapping to define the powers and mandate necessary in the OOTS procedures.	OOTS Team
How can end-users identify themselves and act on behalf of a company or of another natural person?	Currently, detailed work on preparing the implementing acts that define the person identification data of EU Digital Identity Wallet Users[23], including when they identified as representing another natural or legal person has not yet started. Once it does, DG CNECT shall consider the work of the Contact Group.	DG CNECT

Alternatives

The Contact Group analysed an alternative approach to support power of representation and mandates based on existing national Mandate Management Systems[24]. When a natural person needs to act on behalf of another natural or legal person, the national Mandate Management Systems could be used to exchange evidence, through the once-only technical system, to confirm the specific powers of the natural person. By doing so, the once-only technical system would be used as a data source to express powers and mandates, thus removing the dependency on the eIDAS framework.

Nevertheless, the Contact Group disregarded this alternative approach due to two reasons: (1) Not all Member States have a Mandate Management System in place, which may be connected to the once-only technical system. (2) Some Member States questioned the legal value of pieces of evidence retrieved from a Mandate Management System, as they do not fall under the eIDAS framework.

---

[22] In technical terms, the Contact Group should adopt an additional sector-specific attribute as part of the eIDAS data model for expressing the scope of power information. The legal value of such attribute must be determined.

[23]

[24] A mandate management system is an IT system that allows the definition of electronic powers of representation and mandates. Mandate management systems are usually seamlessly integrated with identity management systems to empower users to act on behalf of a third party, e.g. a natural or legal person.

SYNERGY 2.

The **preview area** may offer the option for the user to start the process of issuance of the evidence in the **EUDI format**. Upon finalisation of the procedure, competent authorities can offer the option to issue the output of the procedure in the **EUDI format**

Member State A

B Member State

Data Requester
" *I want to change my address to Member State A.*

Data Provider
" *My country of origin provides the evidence.*

eGov Portal

OOTS

Authentic Data Source

download official document → **EUDI** ← download evidence

Synergy 2: The preview area may offer the option for the user to start the process of issuance of the evidence in the EUDI format. Upon finalisation of the procedure, competent authorities may offer the option to issue the output of the procedure in the EUDI format.

Requirement

The revision of the Commission's proposal to revise the eIDAS Regulation states (Amended Article 6a/3a[25]) that *"the European Digital Identity Wallets shall enable the user to securely request and **obtain, store, select, combine and share**, in a manner that is transparent to and traceable by the user, the [...] **identification data and electronic attestation** of attributes to authenticate online and offline in order to use online public and private services"*.

What's being reused

EU Digital Identity Wallet reusing OOTS

Status

⏳ **Under investigation**

Step in the user journey

Preview evidence

(Step 6 of the user journey)

Finalise procedure

(Step 9 of the user journey)

Benefits

☑ Improved user experience

☐ Optimised investments

☐ Faster time to market

☐ Minimised risks

Description

The objective of this synergy is twofold. It aims to enrich the Once-Only Technical System Preview Area to allow Evidence Requesters to issue pieces of evidence as a QEAA to citizens and businesses in a format compatible with the EU Digital Identity Wallet. On the other hand, it will allow procedure portals to issue the output of the procedures, e.g. European Health Insurance Card, as a QEAA to citizens and businesses in a format compatible with the EU Digital Identity Wallet.

In practice, the Once-Only Technical System will help users identify the right evidence and/or issuing authority in another Member State in relation to a procedure. The retrieved evidence and the output of the procedure may be then optionally issued to the EU Digital Identity Wallet for later use.

By implementing this synergy, the Once-Only Technical System will facilitate the issuance of electronic attestation of attributes by Evidence Providers and OOTS Procedure Portals. The EU Digital Identity Wallet enables citizens to present (Q)EAAs to verifiers. For example, the Once-Only Technical System will help users complete the registration of their motor vehicle in another Member State, and users may use the EU Digital Identity Wallet to present that proof of registration later.

Challenges and actions agreed by the Contact Group

This synergy requires additional analysis and discussions before it can be agreed. The main obstacle is the relatively high security requirements of eIDAS Regulation for qualified electronic attestation of attributes issuers. The requirements for issuers of non-qualified electronic attestations of attributes are less strict but require additional analysis. DG CNECT will clarify the applicable requirements once the eIDAS legal text has been agreed upon. The OOTS team must identify the evidence and outputs of the Single Digital Gateway procedures that could be relevant to be issued as a QEAA in a format compatible with the EU Digital Identity Wallet.

---

[25] https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.02/DOC_1&format=PDF (Page 23)

More specifically, the Contact Group recognised the following challenges and identified the following related actions:

Challenge	Action	Responsible
What are the legal and technical requirements that apply to issuers and to the issuance process?	If applicable, present requirements for authentic sources to be able to issue QEAAs and EAAs to EU Digital Identity Wallet(s).	DG CNECT
	Present examples of (Q)TSPs willing to issue attestations that may be used in the context of the EU Digital Identity Wallet.	DG CNECT
Not all evidence and outputs of procedures are relevant for download into the EU Digital Identity Wallet.	Present a list of evidence collected through evidence mapping processes that serve as inputs to the Once-Only Technical System procedures. Present a list of the expected outputs of the procedure - e.g. Birth Certificate, EHIC - so that the Contact Group can consider if they could be interesting for the user to download to their EU Digital Identity Wallet (these are listed in ANNEX II of the Single Digital Gateway Regulation).	OOTS Team

Alternatives

The Contact Group identified two alternative implementations of this synergy:
1. **Redirections to the QTSP from the preview area**: instead of issuing the evidence as QEAAs from the preview area, the end-user may be redirected to the national QTSP allowed to issue the evidence as a QEAA compatible with the EU Digital Identity Wallet.
2. **Creation of a central QTSP at national level**: as a variant of the previous alternative, Member States may decide to create a central QTSP at the national level acting as a hub issuing QEAAs for all national authentic sources. The preview area may redirect end-users to the central QTSP to issue the evidence as QEAA compatible with the EU Digital Identity Wallets.

Both alternatives require assessing the impact on the Single Digital Gateway Regulation, as well as on the OOTS implementing act.

SYNERGY 3.

Citizens and businesses can combine evidence uploaded from the **EUDI Wallet** with evidence retrieved through the **Once-Only Technical System**
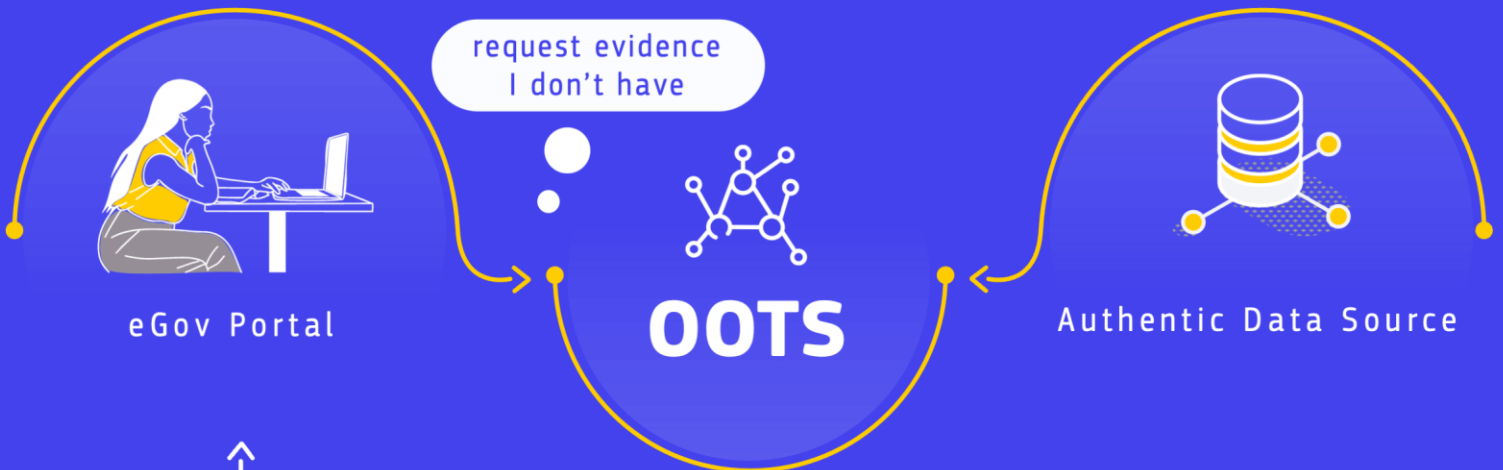
Member State **A**

B Member State

Data Requester
" *I want to change my address to Member State A.*

Data Provider
" *My country of origin provides the evidence.*

request evidence
I don't have

OOTS

eGov Portal

Authentic Data Source

upload evidence
I already have

or

EUDI

Synergy 3: Citizens and businesses can combine evidence uploaded from the EUDI Wallet with evidence retrieved through the Once-Only Technical System

Requirement

The Single Digital Gateway Regulation aims to improve citizens' and businesses' interactions with eGovernment processes in a cross-border context. It lays the foundation to carry out administrative procedures, e.g. cross-border change of address, fully online.

These online services should guide the users through the list of the requirements needed to fulfil the procedure, as well as to establish the channels that end-users may use to provide procedure portals with the supporting evidence, e.g. birth certificate, needed to carry out a procedure.

The Single Digital Gateway Regulation (Article 14) mandates the establishment of a technical system for the automatic retrieval of evidence from authentic sources, so that end-users do not have to manually upload the necessary evidence. Nevertheless, the use of the technical system is not mandatory. Its use is a choice of the end-user. End-users will always have the possibility to upload evidence manually through means other than the OOTS, e.g. upload from a folder on their own computer.

What's being reused

OOTS reusing EU Digital Identity Wallet

Status

◎ **Agreed**

Step in the user journey

Send evidence

(Step 7 of the user journey)

Benefits

- ☑ Improved user experience
- ☐ Optimised investments
- ☐ Faster time to market
- ☐ Minimised risks

Description

In line with the requirements set out in the Single Digital Gateway Regulation [26], the objective of this synergy is to reuse the EU Digital Identity Wallet as an additional source for end-users to provide procedure portals with the necessary evidence to carry out an online procedure. The choice of system to use is up to the end-user. As such, the Once-Only Technical System and the EU Digital Identity Wallet are intended to be complementary.

If a piece of evidence is not available on an EU Digital Identity Wallet, or the user simply does not want to use the EU Digital Identity Wallet, the Once-Only Technical System may allow users to retrieve the evidence from another Member State. If some evidence cannot be retrieved through the Once-Only Technical System, e.g. the authentic source is temporarily unavailable, then the EU Digital Identity Wallet may be used to present the evidence to the procedure portal.

Timeline and actions for implementation

Similarly to the first variant of synergy 1, the timeline for the implementation of this synergy depends on the legislative process and resulting implementation of the EU Digital Identity Wallet at the national level.

Regarding the readiness of the Once-Only Technical System, all procedure portals must implement interfaces to request the required evidence from EU Digital Identity Wallet. This means each procedure portal must configure appropriate attribute requests and integrate the received attributes in the appropriate business processes which requires development work.

Based on the above considerations, the following actions need to be carried out before this synergy can be implemented:

Action	Responsible	When
Analyse and determine the changes to be made on national procedure portals to allow users to use the EU Digital Identity Wallets for the provision of evidence.	Member States *(eIDAS)*	2023-2024 *(Estimated)*

---

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1724

2.2 Investment synergies

This section introduces a set of synergies relying on the **reuse of the Once-Only Technical System Common Services by the EU Digital Identity Wallet**. The OOTS Common Services consist of a set of reusable building blocks that, among other features, allow the automatic discovery of providers of evidence. The Commission Implementing Regulation (EU) 2022/1463[27] mandates the Commission, in cooperation with the Member States, to establish the following Common Services:

1. The **Data Service Directory** (Article 5): an online repository that Member States must populate with all evidence providers and evidence types that they issue and that are relevant for online procedures.
2. The **Evidence Broker** (Article 6): it provides mapping functionalities to allow evidence requesters to determine which evidence types issued in other Member States correspond to the document required in the context of an online procedure.
3. The **Semantic Repository** (Article 7): it provides access to the OOTS generic metadata model, which is designed to display metadata that uniquely identifies   the evidence and the evidence providers. Among other information, the Semantic Repository will contain (1) a representation of the data models used in OOTS, (2) distributions of XML schema definitions (XSDs), (3) code lists, and (4) a mechanism to generate the human readable format of the OOTS data entities.

The Common Services will be used to guide end-users step-by-step through the process of selection of providers of evidence necessary to carry out an online procedure.

(Q)TSPs may benefit from using OOTS to verify the person's attributes in (Q)EAA issuance (**synergy 4**), or to use the OOTS Common Services[28] [29] to publish the attestations they provide (**synergy 5**).

The reuse of the OOTS Common Services may provide several benefits. It aims to lead to investment gains, if EU Digital Identity Wallets relies on the existing OOTS infrastructure rather than creating a new one and if the features of the infrastructure are fit-for-purpose. On the other hand, the adoption of tested building blocks may accelerate the time to market if the user group's requirements do not require the building block to be updated. For these reasons the features of the building blocks need to be further studied in the course of the EU Digital Identity Wallet specifications development work.

The remainder of this section provides a more detailed description of the synergies mentioned above.

---

[27] Commission Implementing Regulation setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1463

[28] The Once-Only System Common Services - https://ec.europa.eu/digital-building-blocks/wikis/display/OOTS/Common+and+Supporting+services

[29] Article 4, 5, 6 and 7 of the Commission Implementing Regulation 2022/1463

SYNERGY **4**

Qualified Trust Service Providers (QTSPs) could use the Common Services of the **Once-Only Technical System** to discover the authentic sources of evidence. Afterwards, the **QTSPs** could also use the **Once-Only Technical System** message exchange protocol and operational framework to request the attributes from the authentic data source

Data Requester

" *I have a paper diploma. I want to add my diploma to my digital wallet.*
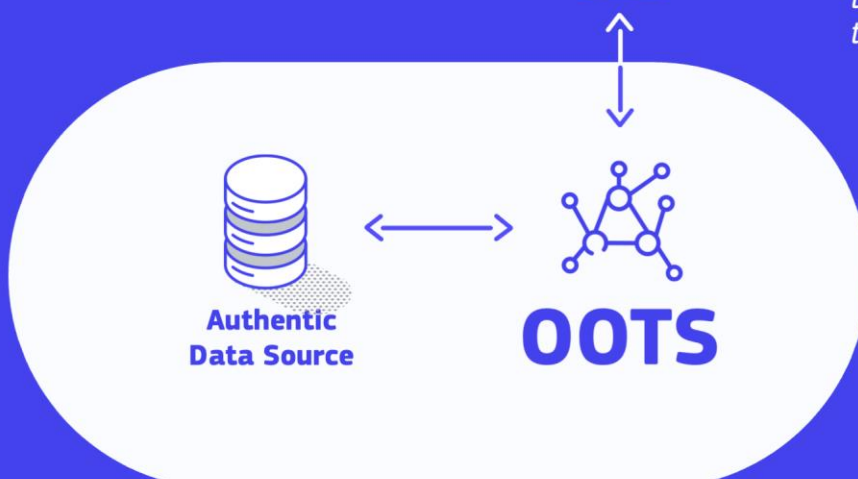
eGov Portal

Data Provider

" *QTSP can provide a legally recognised digital attestation of my diploma.*

QTSP
service

" *Upon my request, the QTSP accesses the authentic data source to verify the data of my diploma.*

Authentic Data Source

OOTS

Synergy 4: Qualified Trust Service Providers (QTSPs) could use the Common Services of the Once-Only Technical System to discover the authentic sources of evidence. The QTSPs could also use the Once-Only technical system message exchange protocol and operational framework to request the attributes from the authentic data source (as per requirement Article 45d of the eIDAS proposal).

Requirement

In line with Article 45d of the revision of the eIDAS Regulation, Member States shall ensure that, upon the request of the users, Qualified Trusted Service Providers (QTSPs) are able to verify the authenticity of the attributes they issue (at least the ones listed in Annex VI of the revision) directly against the authentic source at national level.

It is important to highlight that a QTSP may not be the authentic source of the evidence. In this case, a QTSP is a third party (natural or legal person), who provides a trust service for the issuance of QEAAs. QTSPs need to be connected to the authentic source for the validation of the attributes they issue.

What's being reused

EU Digital Identity Wallet using OOTS Common Services

Status

⧗ **Under investigation**

Benefits

☐ Improved user experience
☑ Optimised investments
☑ Faster time to market
☑ Minimised risks

Description

In order to fulfil this requirement, QTSPs need to know which authentic data source to contact for the validation of attributes (upon request of the citizens or businesses) that they attest.

The objective of this synergy is to assess whether it is feasible for QTSPs to reuse the Once-Only Technical System, in a role similar to a procedure portal, to discover the authentic sources for the verification of attributes. Afterwards, QTSPs may rely on the OOTS message exchange protocol and operational agreements to retrieve the evidence from the authentic source.

From a legal standpoint, QTSPs must be allowed access to the OOTS, although this is currently prevented by Article 4.3 of the Commission Implementing Regulation (EU) 2022/1463[30]. In practice, after amending the Commission Implementing Regulation 2022/1463, the OOTS may be reused by the QTSPs and do not need to be recreated by Member States, thus lowering costs and risks, while accelerating their availability to qualified providers of electronic attestations of attributes for verification purposes.

Challenges and actions agreed by the Contact Group

The Contact Group acknowledged that the use of the Once-Only Technical System for verifying the authenticity of attributes against the authentic sources would help avoid duplication of investments for the Commission and Member States in relation to the development and, most importantly, to the maintenance and operations of competing IT systems. Nonetheless, the synergy cannot be considered as agreed as eIDAS negotiations are still ongoing.

Furthermore, another obstacle to the reuse of the Common Services lies in the OOTS Implementing Regulation explicitly preventing QTSPs from using the OOTS Common Services.

As immediate next steps, the Commission shall assess whether any amendments to the Commission Implementing Regulation (EU) 2022/1463 and/or eIDAS Regulation are necessary to enable the reuse of OOTS from a legal standpoint. In addition, the Contact Group may present the opportunities for reuse of the OOTS in the context of the relevant work by the eIDAS Expert Group to further assess feasibility.

More specifically, the Contact Group recognised the following challenges and identified the following related actions:

Challenge	Action	Responsible
Knowledge sharing	OOTS team will be invited to present the benefits of the reuse of OOTS, when the eIDAS expert group starts to work on detailing the requirements for verification of attributes by QTSPs	DG GROW DG CNECT DIGIT eIDAS Expert Group
Unclear legal implications on the use of the Once-Only Technical System for the verification of attributes.	If eIDAS Expert Group is interested in reusing the Once-Only Technical System, the Commission shall analyse whether and how the Single Digital Gateway Regulation and Implementing Regulation (EU)	DG GROW Member States

---

[30] Article 4.3: Member States shall ensure that only evidence requesters are connected, directly or through intermediary platforms, to the common services and that only evidence requesters and evidence providers can use the OOTS. Member States shall check the functioning of the connections to the common services at regular intervals.

SYNERGY 5.

Citizens and businesses could use the Common Services of the **Once-Only Technical System** to discover the authentic sources able to provide **QEAA** and **EAA**

Data Requester

" *I want to know which documents I can download to my digital wallet.*

eGov Portal

EUDI

EUDI queries the Common services of OOTS to retrieve the Catalogue of authentic sources able to deliver official documents to EUDI wallets.

OOTS

Synergy 5: Citizens and businesses could use the Common Services of the Once-Only Technical System to discover the authentic sources able to provide QEAA and EAA.

Requirement

In order to facilitate (Q)EAA discovery, Article 45d of the revision of the eIDAS Regulation[31] mandates the Commission to set out the minimum technical specifications, standards and procedures with reference to a catalogue of attributes and schemes for the attestation of attributes [...], by means of an implementing act.

What's being reused

EU Digital Identity Wallet using OOTS Common Services

Status

⧗ **Under investigation**

Benefits

☐ Improved user experience
☑ Optimised investments
☑ Faster time to market
☑ Minimised risks

Description

This synergy entails that Once-Only Technical System Common Services are considered to play the role of catalogue of attributes and schemes for the attestation of attributes. This will enable citizens and businesses to discover the authentic sources able to issue (Q)EAAs. The reuse of the OOTS building blocks will be considered by eIDAS Expert Group when work starts on the relevant aspects of the EU Digital Identity Wallet ecosystem.

Challenges and actions agreed by the Contact Group

One obstacle to the reuse of the Common Services lies in the OOTS Implementing Regulation explicitly preventing the use of the OOTS Common Services to entities other than the OOTS procedure portals.

Therefore, as an immediate next step, the European Commission will analyse the legal and technical implications, as well as the potential need to amend the OOTS Implementing Regulation and/or eIDAS Regulation, to allow the EU Digital Identity Wallet to access the OOTS Common Services. The Contact Group will present the opportunities for reuse to the eIDAS Expert Group to obtain their agreement.

More specifically, the Contact Group recognised the following challenges and identified the following related actions:

Challenge	Action	Responsible
Knowledge sharing	The OOTS team will be invited to present the benefits of the reuse of relevant OOTS building blocks, when the eIDAS expert group starts to work on detailing the requirements for the catalogues of attributes and schemes for the attestation of attributes.	DG GROW DG CNECT DIGIT eIDAS Expert Group
Unclear legal implications on the use of the Once-Only Technical System building blocks for EU Digital Identity Wallet purposes.	If eIDAS Expert Group is interested in reusing the Once-Only Technical System building blocks, the Commission will analyse whether the Single Digital Gateway Regulation needs to be amended to enable the reuse of the Once-Only Technical System.	DG GROW DG CNECT

---

[31] Revision of the eIDAS Regulation, Article 45d https://eur-lex.europa.eu/resource.html?uri=cellar:5d88943a-c458-11eb-a925-01aa75ed71a1.0001.01/DOC_1&format=DOC

3. Way forward

The Contact Group made significant progress with the analysis of the potential synergies between the Once-Only Technical System and the EU Digital Identity Wallet, as described above. The Contact Group already agreed on the implementation of some synergies (mainly where the Once-Only Technical System reuses the EU Digital Identity Wallet), while discussions are still ongoing for the synergies where the EU Digital Identity Wallet reuses the Once-Only Technical System Common Services.

It is important to highlight that the timeline for the implementation of the identified synergies greatly depends on the legislative process and resulting implementation of the EU Digital Identity Wallet at the national level, and on the legal and technical changes on OOTS. As a result, the timelines and the milestones of the future work of Contact Group must be aligned with the timelines of the EU Digital Identity Wallet legislative process and OOTS.

A detailed proposal for the upcoming activities of the Contact Group is described in Figure 5 on the next page.

Activity	2023 Q4	2024 Q1	2024 Q2	2024 Q3	2024 Q4	2025 Q1	2025 Q2	2025 Q3	2025 Q4	2026 Q1	2026 Q2	2026 Q3	2026 Q4	2027 Q1	2027 Q2	2027 Q3	2027 Q4
eIDAS legislative process and implementation of the EUDI Wallet *(estimated timeline)*																	
Finalise eIDAS basic act to introduce the Digital Identity Wallet	▓																
Adopt Implementing Acts resulting from the revision of the eIDAS Regulation		DG CNECT															
Develop and roll-out EUDI Wallets at the national level								Member States (eIDAS)									
Synergy 1: The EUDI Wallet will provide an additional way for citizens and businesses for authentication and identification purposes.																	
Assess the impact of the roll-out of EUDI Wallets on national procedure portals					Member States (OOTS)												
Clarify approach to support electronic power of representation and mandates		DG CNECT															
Analyse use eIDAS sectorial attributes for powers of representation and mandates			Contact Group + DG GROW														
Define controlled vocabulary for powers of representation and mandates in OOTS			OOTS Team														
Synergy 2: The preview area may offer the option for the user to start the process of issuance of the evidence in the EUDI format. Upon finalisation of the procedure, competent authorities may offer the option to issue the output of the procedure in the EUDI format.																	
Present requirements for authentic sources to issue QEAAs to Contact Group		DG CNECT															
Present examples of QTSPs		DG CNECT															
Identify OOTS evidence and outputs relevant for download in the Wallet		OOTS Team															
Assess impact for the implementation of synergy 2					Member States (OOTS)												
Synergy 3: Citizens and businesses can combine evidence uploaded from the EUDI Wallet with evidence retrieved through the Once-Only Technical System.																	
Assess the impact of the roll-out of EUDI Wallets on national procedure portals					Member States (OOTS)												
Synergy 4: Qualified Trust Service Providers (QTSPs) could use the Common Services of the Once-Only Technical System to discover the authentic sources of evidence. The QTSPs could use the Once-Only technical system message exchange protocol and operational framework to request the attributes from the authentic data source.																	
Present OOTS to eIDAS Expert Group for agreement on reuse		Contact Group															
Assess legal implications of reusing the OOTS Common Services by QTSPs					DG CNECT + DG GROW												
Decide on reuse of OOTS for validation of attributes by QTSPs		DG CNECT															
Assess impact for the implementation of synergy 4			Member States (OOTS and eIDAS)														
Synergy 5: Citizens and businesses could use the Common Services of the Once-Only Technical System to discover the authentic sources able to provide QEAA and EAA.																	
Present OOTS to eIDAS Expert Group for agreement on reuse		Contact Group															
Assess legal implications of reusing the OOTS by EUDI Wallet					DG CNECT + DG GROW												
Decide on reuse of OOTS for validation of attributes by Wallets		DG CNECT															
Assess impact for the implementation of synergy 5			Member States (OOTS and eIDAS)														
Analysis of additional synergies between the Once-Only Technical System and the EUDI Wallet																	
Identify additional synergies between the OOTS and the EUDI Wallet	Contact Group																
Analyse additional synergies			Contact Group														

Figure 5: High-level roadmap of the actions for the implementation of the synergies

4. Conclusions

The Once-Only Technical System and the EU Digital Identity Wallet are two strategic initiatives that aim to facilitate the interactions of citizens and businesses with public administrations. Both initiatives aim to make the issuance process of (Q)EAAs easier and more efficient, while the EU Digital Identity Wallet will also allow end-users to store and present (Q)EAAs to public and private authorities for the verification of (Q)EAAs. In February 2022, the Internal Market Working Group emphasised the importance of ensuring interoperability and complementarity of the two initiatives. To this end, the Commission presented five potential synergies between the Once-Only Technical System and the EU Digital Identity Wallet that, if implemented, would (1) make the user experience of the Once-Only Technical System easier and richer for citizens and businesses, and would (2) optimise IT investments and minimise risks through the reuse of well-tested building blocks. Following the presentation of the synergies, the Commission established a group of experts (Contact Group) to ensure that the identified synergies are taken up by both initiatives and that they are implemented. The Contact Group held five meetings to discuss the synergies individually. Its members already agreed to implement some of the synergies, mainly where the Once-Only Technical System reuses the EU Digital Identity Wallet. The synergies entailing the reuse of the Once-Only Technical System building blocks by the EU Digital Identity Wallet are still under discussion, waiting for the negotiations of the revision of eIDAS to be finalised.

The work of the Contact Group confirmed the importance of ensuring interoperability and complementarity between the Once-Only Technical System and the EU Digital Identity Wallet. All identified synergies could rely on a wide consensus by the Contact Group on their relevance and importance. Furthermore, both the Contact Group member and the European Commission expressed the importance of continuing the work started. For the synergies whose implementation was already agreed, the Contact Group must assess the impacts on existing systems, e.g. procedure portals. For the synergies still under discussion, it becomes fundamental to liaise with the eIDAS actors working on the revision of the eIDAS Regulation, to ensure that the benefits of reusing the OOTS building blocks are clearly understood and considered. Finally, the Contact Group will identify and analyse potential new synergies to further strengthen the interoperability between the Once-Only Technical System and the EU Digital Identity Wallet.

This report marks the end of the first round of the work of the Contact Group. Work is still in progress, and it is important that all involved stakeholders build on the work done so far to make this important initiative a success.