# OLYMPUS PROJECT

## OBLIVIOUS IDENTITY MANAGEMENT FOR PRIVATE USER-FRIENDLY SERVICES

## D6.1 Use cases description

| PROJECT NUMBER | PROJECT ACRONYM |
|---|---|
| 786725 | OLYMPUS |
| **CONTACT** | **WEBSITE** |
| contact@olympus-project.eu | http://www.olympus-project.eu/ |

Due date of deliverable: 28-2-2019
Actual submission date: 15-03-2019

| Dissemination Level | |
|---|---|
| PU = Public, fully open, e.g. web | ✓ |
| CO = Confidential, restricted under conditions set out in Model Grant Agreement | |
| CI = Classified, information as referred to in Commission Decision 2001/844/EC. | |
| Int = Internal Working Document | |

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

OLYMPUS

# REVISION HISTORY

The following table describes the main changes done in the document since created.

| Revision | Date | Description | Author (Organization) |
|---|---|---|---|
| V0.1 | 31/01/2019 | First draft. Included Use cases table of contents and the concrete uses cases first approach for credit file and driver license. | Rafael Torres Moreno, Jorge Bernal Bernabé, Antonio Skarmeta (UMU) |
| V0.2 | 13/02/2019 | Use Case mobile Drivers License Updates | Evangelos Sakkopoulos, Stavros Dounias, Mersini Paschou, Emmanouil Viennas, Zafeiria-Marina Ioannou Konstantinos Papaxanthis (SCY) |
| V0.3 | 22/02/2019 | Use Case mobile Drivers License Updates | Evangelos Sakkopoulos, Stavros Dounias, Mersini Paschou (SCY) |
| V0.4 | 25/02/2019 | Use Case mobile Drivers License Updates | Nuno Ponte, Nuno Marques, Mauro Almeida, Nuno Martins (MUL), Evangelos Sakkopoulos, Stavros Dounias, Mersini Paschou (SCY) |
| V0.5 | 25/02/2019 | Credit File use case updates | Noelia Martínez, Felix Esteban (LOG) |
| V0.6 | 26/02/2019 | Template update | Rafael Torres Moreno, Jorge Bernal Bernabé, Antonio Skarmeta (UMU) |
| V0.7 | 04/03/2019 | Revisions and comments | Tore Kasper Frederiksen, Michael Stausholm (ALX) |
| V0.8 | 08/03/2019 | Use Case mobile Drivers License Updates | Nuno Ponte, Nuno Marques, Mauro Almeida, Nuno Martins (MUL), Evangelos Sakkopoulos, Stavros Dounias, Mersini Paschou (SCY) |
| V0.9 | 12/03/2019 | Credit File use case updates | Noelia Martínez, Felix Esteban (LOG) |
| V1.0 | 14/03/2019 | Document revision and updates | Rafael Torres Moreno, Jorge Bernal Bernabé, Antonio Skarmeta (UMU) |
| V1.1 | 18/06/2020 | Addressed review recommendations | Noelia Martínez (LOG) |

*TABLE **1**: REVISION HISTORY*

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

# INDEX



This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

# TABLE OF FIGURES



This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725



OLYMPUS

# OBLIVIOUS IDENTITY MANAGEMENT FOR PRIVATE AND USER-FRIENDLY SERVICES


## ABSTRACT

The aim for WP6 is to work on the validation of the OLYMPUS solution within the use cases and possible considering a wider deployment using OLYMPUS technologies developed in WP3-5 and integrated in WP6 for future business solutions.

The focus is on working on the use case, providing with real pilots, evaluating these prototypes and evaluating them with other stakeholders to identify a wider deployment for business development and exploitation.



## KEYWORDS

Risk management, Risk mitigation, Key Performance Indicators (KPIs) monitoring and Quality Assurance, Use cases



## AUTHORS (ORGANIZATION)

Rafael Torres (UMU), Jorge Bernal (UMU), Antonio Skarmeta (UMU), Noelia Martinez (LOG), Felix Esteban (LOG), Nuno Ponte (MUL), Nuno Marques (MUL), Mauro Almeida (MUL), Nuno Martins (MUL), Vangelis Sakkopoulos (SCY) Stavros Dounias (SCY), Mersini Paschou (SCY), Emmanouil Viennas (SCY), Zafeiria-Marina Ioannou (SCY), Konstantinos Papaxanthis (SCY), Tore Kasper Frederiksen (ALX), Michael Stausholm (ALX).



## DISCLAIMER

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725, but this document only reflects the consortium's view. The European Commission is not responsible for any use that may be made of the information it contains.

# 1. EXECUTIVE SUMMARY

To truly test the usability of OLYMPUS technologies, they need to be tested in real end-user driven use-cases. This document focuses on the use cases detailed definition and business opportunities that the OLYMPUS technologies unlock.

This document will provide a list of unified requirements specific from the use cases, with special focus on privacy and security analysis and a requirement mapping aims.

The main objective is to develop a set of requirements based on the set of use cases defined in the proposal provided on the business logic defined by MUL and LOG, and that will support the development of the architecture blueprint and the design of prototypes, their evaluation and eventual scaling.

To achieve this, this document involves mainly use case providers with different technical and cultural backgrounds, part of both the business exploitation and use-cases sides. Different kinds of requirements are elucidated: business, functional and non-functional (e.g. security, privacy and interoperability).

This document analyses and regroup the requirements to help mapping what are the impacts of those requirements upon the overall architecture.

The document is structured as follows: A first introductory section to the nomenclature of use cases. Next, section two deals with the "Credit File" use case, section three on the "Mobile driver license" use case, followed by a section four of conclusions and ending with references and annexes.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

# 2. USE CASE DESCRIPTION APPROACH

## 2.1. USE CASES DESCRIPTION FORMAT

According to the structure presented in the annex, each use case description contains the following elements: A description of the use case, the actors involved, a series of requirements and preconditions. Use cases define priority for their requirements and describe the frequency of use of the case as well as the normal course of events. Finally, sequence diagrams associated with the case, possible exceptions and assumptions are presented.

Next, the nomenclature for the use cases is defined.

## 2.2. USE CASE ID

According to the nomenclature of the project, the cases will be identified in the following way.

- UC of User Case.

And a sequential number that will identify the concrete use case.

- For example: UC1.

If the use case includes different use cases, a point is added and another sequential number that identifies it univocally.

- UC1.1, UC1.2, etc.

## 2.3. USE CASE NAME

In addition, a name will be given to each of the identified cases of use, which identifies it univocally and provides a simple functional description, for example “Credit identity scenario”.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 786725

# 3. UC1 - CREDIT FILE

The cFAPP is designed to serve the purpose of easing the contractual process for some financial services and products for both the financial entities and their customers.

LOG to provide details of the interfaces, APIs flows of the use case to have a more detailed information about the development environment IdP used and credit file retrieval (cFAPP).

## 3.1. DESCRIPTION

The objective of this use case is to create an online platform where SMEs, self-employed and legal or natural individuals can create and manage their credit file and their standardized rating for financial entities. All of it is based on several new regulations:

The Law 5/2015 of April 27 on promoting corporate financing has as one of its objectives to foster and promote the financing of SMEs and self-employed people, making bank finance more flexible and accessible. The Law establishes that extensive information on the financial situation and payment history will have to be provided in a document called "Financial Information-SME".

The World Bank's ICCR (International Committee of Credit Reporting), is proposing several initiatives to facilitate access to credit for individuals and small and medium-sized enterprises.

The new EU general data protection regulation 2016/679 (GDPR) [1] took effect on May 25th, 2018. The Law establishes that, if an entity requires personal information from a customer, they will need the express consent to use their personal data and these consents have to be stored by the entity. Penalties in case this standard is not met are high.

Currently, when a customer needs financing, the financial entity requires: his or her identification, access to external databases to collect and validate customer data, a credit risk evaluation, and, if it is granted, establishing a contractual credit relationship. As for the new EU general data protection regulation it is required for the client to give consent for providing his or her personal data and to sign one or more documents and for the financial entity to keep the consent and the personal data for several years. And, at this point, neither the financial entity nor the customer knows if the contractual relationship will be performed.

Within this project, we want to ease this process for both the financial entity and the customer, in a way that allows them to exchange the minimal required information, for the entity to save and for the user to provide, until the financial entity grants the service.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

Instead of providing the customer's identification and the financial information related to a specific service at the first step of the relationship, the financial entity will receive an anonymous credit file containing the minimal amount of required financial information, bound to a pseudonym, that allows them to evaluate the user's suitability for that specific product of service [2][3]. At this point in time, the bank must produce a binding response based solely on the financial information in the credit file, hence the bank cannot discriminate on name, area code or other non-relevant information. If the bank decides that the user's information is suitable for producing an offer/contract, the customer can use the pseudonym to reveal his or her identity to the financial entity and start a contractual relationship.

Thanks to the Oblivious authentication [4][5], the client is protected against the tracking that in current scenarios can be done in the IdP putting the user privacy under risk.

Since the financial entity and credit file platform does not communicate directly, all data is passed through the customer, hence we focus on the interfaces:

1. Between the financial entity and the customer.

2. Between the customer and the credit file platform.

The access to the interface between the financial entity and the customer can be performed from any computer. Similarly, any computer could in principle be used to access the interface between the customer and the credit file platform, however in order to make a good user experience, the process is started by scanning a QR code, hence this interface must be accessed using a mobile device, using a custom application.

## 3.2. ACTORS

The target audience would be SMEs, self-employed and individuals interested in obtaining their "credit file" certificates to facilitate their funding.

## 3.3. REQUIREMENTS

| ID | Type | Description | Rationale | Fit Criterion | Originator | Priority | Conflicts | History |
|---|---|---|---|---|---|---|---|---|
| **cF.RQ.1** | F | Initial Website | To provide an initial point for the user to access to the the Credit File functionality. | | LOG | H | | |
| **cF.RQ.2** | F | Credit File Mobile App | To guide the user in the process of getting his financial information and | | LOG | H | | |

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | providing it to the bank | | | | | |
| **cF.RQ.3** | F | Service selection | To allow the user to select between several different user profiles. | Several different profiles have to be displayed for the user to select | LOG | M | | |
| **cF.RQ.4** | F | User confirmation | To let the user know and confirm which information will be accessed and provided to the financial entity | A list of required information is displayed. | LOG | M | | |
| **cF.RQ.5** | F | QR Code generation | To generate a QR code with the purpose of identifying the operation using all the information that identifies the transaction: financial entity name, selected service and required information. | A QR code is generated and stored in our systems. | LOG | H | | |
| **cF.RQ.6** | F | Operation selection | To allow the user to choose between scanning a new QR code or navigating through the existing requests. | Both of the options are displayed and eligible. | LOG | L | | |
| **cF.RQ.7** | F | QR Code scan | To scan a previously generated QR code for creating a new request and start the Credit File process. | The QR code scanner is open and ready to scan it. Some information is stored in the device in order to be able to identify the operation later. | LOG | H | | |
| **cF.RQ.8** | F | User identification | To check if the user has an actual qualified identification in our system using an external app. | The user is identified properly. | LOG | H | | |

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **cF.RQ.9** | F | Financial information request | To request the user's financial information from the Credit File platform. | A message is displayed indicating that a request is sent to the platform. | LOG | H | | |
| **cF.RQ.10** | F | Consents fulfilment | If it is necessary to fulfil some additional consents for the platform to perform the financial information report, they are displayed in the app for the user to accept them. | A list of unfulfilled consents is displayed and they are eligible to be accepted. | LOG | M | | |
| **cF.RQ.11** | F | Financial information shipment | To send the financial information anonymously to the financial entity. | A message is displayed indicating that the information was sent. | LOG | H | | |
| **cF.RQ.12** | F | Financial information receiving | To receive the financial information with the actual identity related from the Credit File platform. | | LOG | H | | |
| **cF.RQ.13** | F | Anonymous credential request | To request to create an anonymous financial file. | | LOG | H | | |
| **cF.RQ.14** | F | Financial entity response shipment | The financial entity receives the financial information and evaluates it. When a response is performed, a push notification is sent to the mobile device | The response is stored in the database and the push notification sent. | LOG | H | | |
| **cF.RQ.15** | F | Financial entity response receiving | A push notification from the financial entity is received. | | LOG | M | | |
| **cF.RQ.16** | F | Navigation through the existing requests. | To allow the user to select one of the ready requests in order to check its status. | A list with the existing requests is displayed divided by its status: with the bank's response or not. Only the ready | LOG | M | | |

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | requests are eligible | | | | |
| **cF.RQ.17** | F | Access to the push notification | To display a summary of the related information after checking if the user has an actual qualified identification in our system using an external app. | The financial entity's response is displayed among a summary of information related to the request. | LOG | M | | |
| **cF.RQ.18** | F | Select a ready request | To display a summary of the related information after checking if the user has an actual qualified identification in our system using an external app. | The financial entity's response is displayed among a summary of information related to the request. | LOG | M | | |
| **cF.RQ.19** | F | Authorize to reveal the user identity | If the bank's response is positive, the user can decide to reveal his or her identity using an external app. | The user identification is performed and his or her data sent to the financial entity. | LOG | H | | |

## 3.4. PRECONDITIONS

The user must have previously a qualified digital identity registered in the credit file platform and have the cFAPP mobile device app installed.

## 3.5. PRIORITY

cF.RQ 1, 2, 5, 7, 8, 9, 11, 12, 13, 14 and 19 are High priority.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

## 3.6. FREQUENCY OF USE

An end user could use this use case when he wants to finance an operation such as the purchase of a house, a car or any other valuable asset, between 3 and 5 times every 5 years.

In the case of a company, it will increase the frequency of use up to several times a year, for the renewal of its lines of credit or additional financing.

## 3.7. NORMAL COURSE OF EVENTS

First, the customer should access to the financial entity website and to its Credit File section. There, he or she selects the product or service in which he or she is interested, and the platform will generate a QR code that identifies the requested service and the related financial entity. Then, the customer will use his or her mobile device and the cFAPP to scan this code and to perform the request to the credit file platform.

The process goes as follows:

a. From the initial financial entity website:

   1. The user navigates to the Credit File section.

   2. The user selects a specific profile, defining what types of request are available.

   3. The platform displays a list of the minimum required information needed to make a financial evaluation for the requested profile.

   4. If the user validates this information list to be provided, a QR code, containing a machine-readable description of the data that the credit file platform will need to provide, will be generated.


*Figure 1 - Financial entity and customer interaction*

b. From the cFAPP (customer's mobile device app) the user has two choices:

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

1. The user selects to scan a new QR code.

   a) The user scans the QR code displayed in the financial entity website.

   b) The user uses an external app to authenticate against an external, traditional IdP and obtains an access token *myToken*.

   c) The access token *myToken* and the information from the QR code are sent to a proxy containing an OLYMPUS based virtual IdP[1]. The proxy forwards *myToken* to the credit file platform and obtains the financial report on behalf of the user.

   d) If the credit file platform does not have the needed data to fulfill the financial evaluation and produce the financial report on its own, it may request the cFAPP for consent to access external data sources.

   e) The proxy extracts the relevant information from the financial report and processes it according to the requirements of the financial entity. This allows the proxy to create an anonymized credit file and sign this digitally. This anonymized credit file is then sent to the cFAPP.

   f) In addition to the anonymized credit file, the proxy also signs a message that allows the user to bind his or her identity to the anonymized credit file. This message may either be stored in the cFAPP or at the proxy, to be retrieved by the cFAPP at a later point in time,

   g) The cFAPP can now send the anonymized credit file to the financial entity for it to evaluate if the requirements are met.

   h) When the information is evaluated by the financial entity, and the corresponding response is received by the cFAPP, a push notification is sent to the user's mobile device to let him or her know that the response is ready to be read.

***Figure 2 - User and credit file interaction***

1 In a real setting, the OLYMPUS virtual IdP would be integrated as part of the credit file platform, which would be responsible for anonymizing the credit file data rather than using a proxy.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

2. The user selects to check an existing request.

    a) The user navigates through the requests that are ready for checking their responses or accesses them from the push notification.

    b) The user checks the financial entity's response.

    c) If the financial entity's response confirms the user suitability to the requested profile, the user sends the signed message binding his or her identity to the credit file to the financial entity and can now begin the contractual relationship.

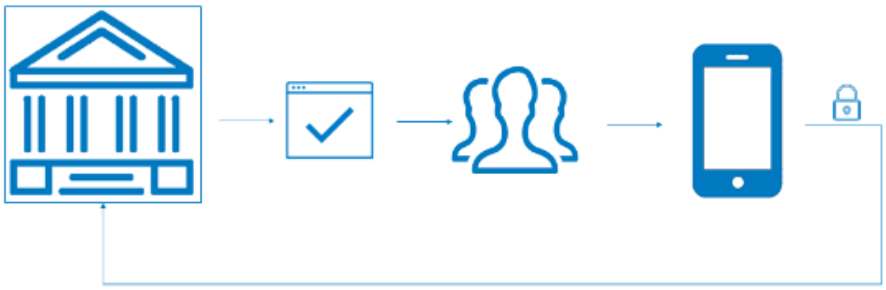

*Figure 3 - Financial entity and customer final interaction*

The main communication flows are explained in the following diagram. The user will identify himself or herself towards the credit file platform during the process to allow the platform to retrieve his or her financial data but, after the financial file has been obtained, this information is anonymized ensuring the users anonymity towards the bank. The use of the OLYMPUS proxy allows the credit file platform to be unaffected by the project, however if the system is to go into production, the OLYMPUS functionality would be implemented and integrated by the credit file platform.

The anonymized data prevents the financial entity from having access to the user's personal information before performing an actual contractual relationship. This promotes the user's privacy and at the same time reduces the banks need to process sensitive information and accommodates GDPR compliance.

Simultaneously, the bank will be bound to the offer made to the anonymous user, ensuring that the bank cannot unfairly discriminate between potential customers.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

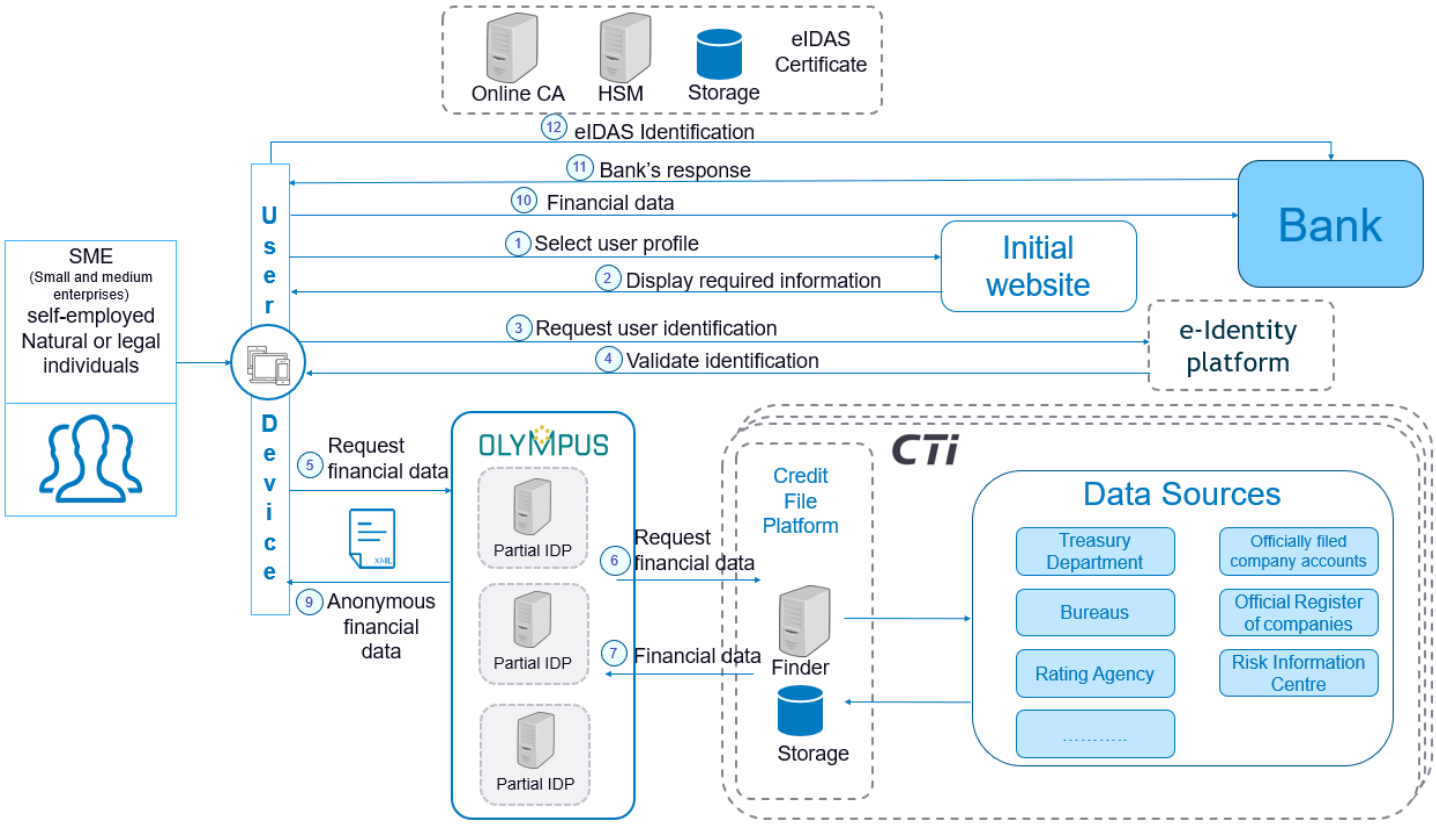


*Figure 4 - Complete process*

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

## 3.8. SEQUENCE DIAGRAM

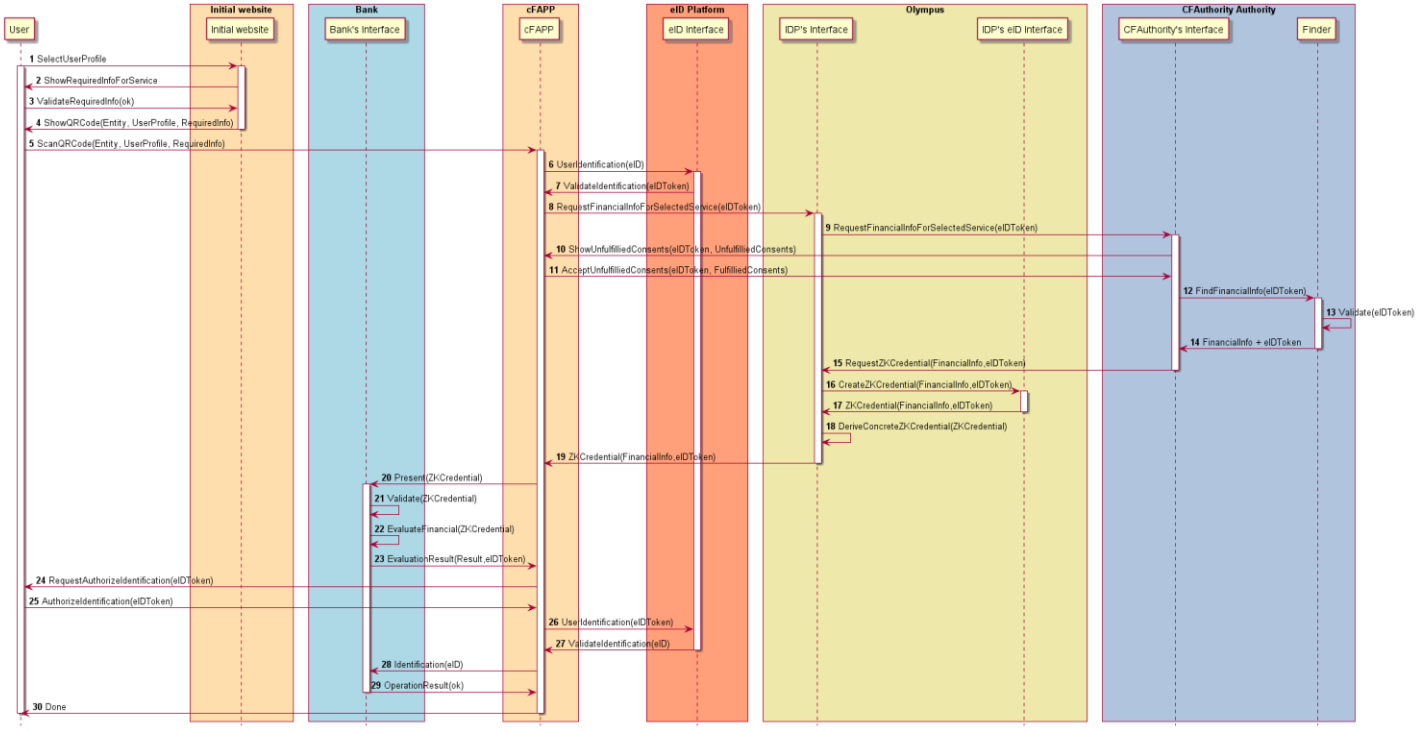


*Figure 5 - Credit file diagram*

## 3.9. EXCEPTIONS

In case a cryptographic verification fails (signature, digest, untrusted root anchor, etc) the execution flow is stopped, and both the user and verifier are presented an error message.

## 3.10. SPECIAL REQUIREMENTS

While the credit file platform may be oblivious to the OLYMPUS technology due to the proxy, the bank must trust the token/proof produced by the OLYMPUS IdP.

## 3.11. ASSUMPTIONS

The user is assumed to be registered with the credit file platform.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

## 3.12. NOTES AND ISSUES

The use case requires the OLYMPUS virtual IdP to be distributed. This will increase the security by splitting the signing key material on to multiple servers that must be compromised for an attack to succeed. This distribution process can be performed among different authorities or legal entities as it is reflected in Figure 4 with the dotted line around each partial IdP, meaning that each IdP that forms the virtual IdP can be deployed by a different legal entity. This distribution among different entities does not affect the functionality itself, but it does have legal and practical implications to privacy, security and the relationships among the involved parties.
We have highlighted within D3.2 the potential impact that a truly distributed vIdP might have on privacy. This impact was also variable depending on OLYMPUS final design (i.e. in case modifications are to be introduced in order to force the collaboration of the IdPs to access or manage the data, therefore increasing privacy beside security).

Nevertheless, the Credit File use case presents a design where this aspect cannot properly be realized as there exists a prior aggregation of the data in the credit file platform database. This, however, does not exclude the improvements introduced by OLYMPUS with regard to current solutions and might also involve other legal consequences.

More specifically, we are taking as point of departure the distribution of the vIdP among different legal entities. Hence, their relationships must be properly regulated pursuing data protection regulations. Although we are still missing some details (proper of a real deployment), in order to determine the role of the parties involved in the data processing, account taken of the use case description we consider that the most likely possibility is that the different legal entities would be considered as joint controllers.

In such scenario, pursuing article 26 of the GDPR the parties involved in the data processing must subscribe an agreement whereby they would distribute responsibilities. More specifically, these responsibilities refer for example to determining the legal entity in charge of providing the information about the processing, carrying a DPIA or before whom users can claim the exercise of their rights. Nonetheless, the content set out by the article 26 is the minimum content and we would highly recommend extending it in case of real drafting.

It should be noted that we have concluded this scenario to be the most likely by applying the reflections pointed out in D3.2. Although the legal entity governing the credit file platform has undoubtedly a central role, the partial IdPs are setting up a common architecture, hence the different legal entities would opt to participate enabling the data processing through thereof.

Nevertheless, we shouldn't exclude the other possibilities with regard to the role developed by the parties involved in the processing. It is also possible that the parties are qualified as sole controllers (e.g. this might happen in case that the legal entities integrating the vIdP make use of the architecture

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

for their own and different purposes). In this scenario, the GDPR does not envisage the necessity of subscribing an agreement, but we would also recommend this practice.

Final possibility would be that the legal entity ruling the credit file platform were qualified as data controller, while the other legal entities integrating the vIdP might be qualified as data processors. In this case, the article 28 of the GDPR contains a set of conditions when selecting the legal entity that might act as data processor (i.e. it must fulfill a minimum of security guarantees), as well as it determines that the relationship between the controller and the processor shall be regulated by an agreement or unilateral act containing the provisions established by this article (i.e. the data processor will strictly process the data following the instructions given by the controller or that it will guarantee the confidentiality of the data).

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

# 4. UC2 - MOBILE DRIVER LICENSE

The mDL is designed to mainly serve the purpose of secure face-to-face identification *using an official identity document*. This can be used for various purposes, such as age verification in a shop or nationality verification when crossing a border.

## 4.1. DESCRIPTION

In short, the objective of this use case is to demonstrate minimal and selective disclosure of personal information based on international standards like ICAO 9303 (e-Passport), and ISO 18013 (Driver's License) taking into consideration in particular the ISO 18013 part 5 [6] under development for the mobile Driver's License.

Within this project, we want to demonstrate the use case of a citizen willing to buy a restricted good or service (for example, a bottle of wine), using the mobile Driver License (mDL) - an electronic version of an ID document in the citizen's smartphone.

Similar to the work done in ReliAble euRopean Identity EcoSystem (ARIES) [7][8][9], this use case instead of disclosing the full dataset of the mDL, the user provides the appropriate information about age, making proof that he or she is older or younger than a certain age.

Based on ISO 18013-5 we focus on the interface between:

1. The mDL holder (e.g. driver or citizen) and the mDL verifier (e.g. merchant or officer) and
2. The mDL verifier and the Issuing Authority (IA) that can be considered to hold the primary registry of mDL holder's information.

At the moment the approach is designed to support attended cases. That is, verification should be made by an individual verifier and not an unattended system.

Please notice, the interconnection between mDL holder and the IA is not, and will not be, governed by this standard. This interconnection includes the enrolment mDL process such as vetting, establishing trust and provide access to the mDL holder and his/her mobile phone.

Depending on the IA's decision, an mDL may be available offline only or alternatively may also be online. Offline means that both the mDL holder and the mDL verifier are not connected to the IA through any network.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

In ISO 18013-5 online assumes connectivity between the mDL Verifier and the IA of the holder's mDL. All IAs worldwide that are following the standard should be available for access by any mDL Verifier without any pre-registration. In the Online case the mDL holder might also be connected to his/her IA (not any IA worldwide).

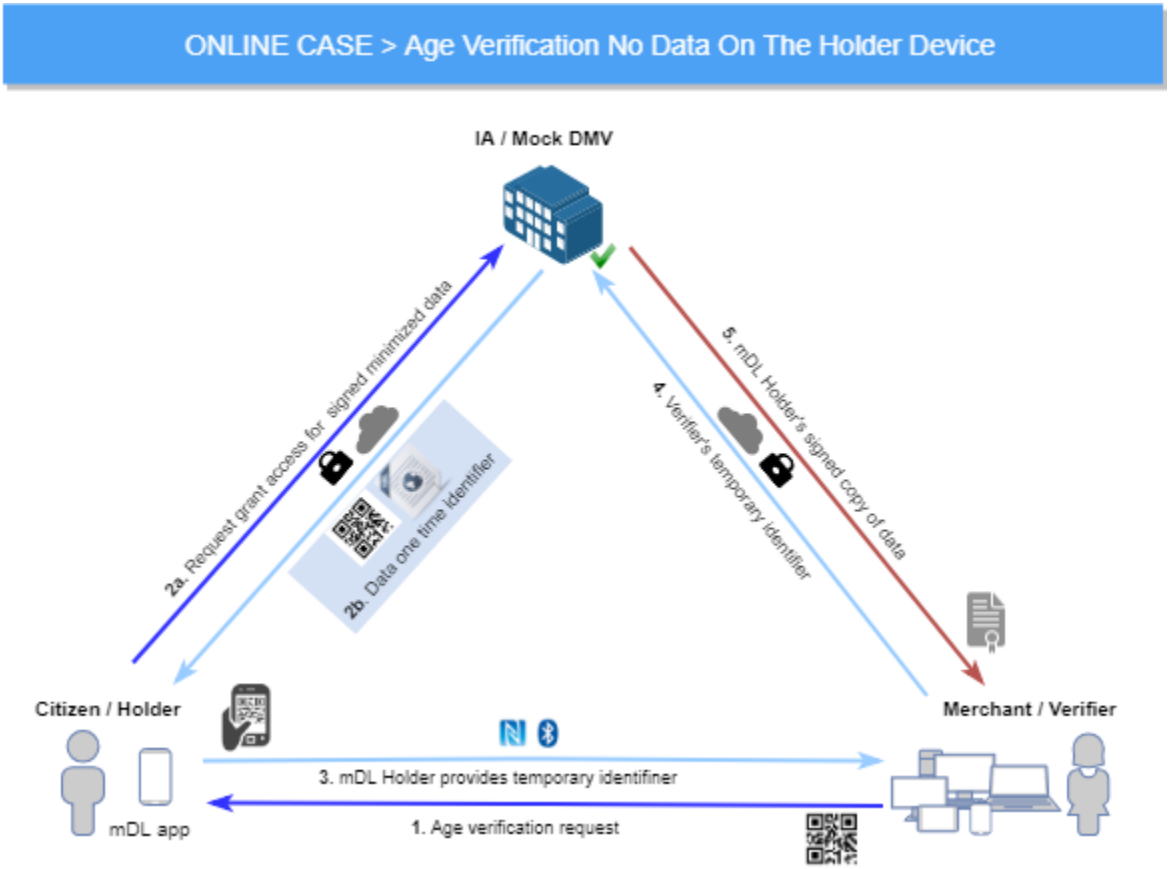


*Figure 6 - Online Case 3-corner Flow according to ISO18013-5*

## 4.2. ACTORS

The target audience would be individuals needing to perform age verification to relying parties such as merchants or officers, SMEs to access and/or receive age-controlled services and products that require the individual to be above a certain age.

The following entities participate in this use case:

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

- Issuing Authority (IA) - Governmental or State agency responsible for issuing the Driver's License. In some cases, it is also called Department of Motor Vehicle (DMV). In the demonstrator of this use case, we provide a "Mock DMV" in the form a database with sample user data. The Issuing Authority is another system interacting with the Mock DMV and is formed by the components formatting and signing mDL data and credentials.

- User - an individual that has an electronic Driver's License (mDL) in a mobile device. The user will run the mDL app.

- Verifier - an individual or entity that needs to validate the identity and attributes of an mDL holder. Examples of verifiers are merchants and law enforcement agents. The verifier will run the mDL verifier.

## 4.3. REQUIREMENTS

| ID | Type | Description | Rationale | Fit Criterion | Originator | Priority | Conflicts | History |
|---|---|---|---|---|---|---|---|---|
| **mDL.RQ.1** | nF | The mDL holder should take advantage of an Internet connection | To refresh/update mDL data | Last refresh date | SCY | L | | |
| **mDL.RQ.2** | nF | The mDL verifier device shall have screen capable to show a portrait image according to ICAO specs, support BLE, QR capable Optical Reader/Camera and NFC.<br>The mDL verifier shall use Android OS devices such as Pixel 2 or Pixel 3 or equivalent | To support any possible mDL holder | Hardware specs | SCY | M | | |
| **mDL.RQ.3** | nF | The mDL holder shall have screen capable to show a QR and either BLE and/or NFC. Camera is also recommended.<br>The mDL holder shall use Android OS devices such as Pixel 2 or Pixel 3 or equivalent | To enable data exchange | Hardware specs | SCY | M | | |
| **mDL.RQ.4** | F | To initiate age verification the verifier requests verbally or using minimal | The user shall enable app to get ready for | mDL app is readable | SCY | L | | |

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | data from the mDL holder | age verification | | | | | |
| **mDL.RQ.5** | F | The mDL holder utilizes access-control to enable mDL usage (e.g. PIN) | App protection | mDL app is readable | SCY | L | | |
| **mDL.RQ.6** | F | The mDL verifier may be pre-registered to the IA or not | Verifier registration is optional | mDL verifier is ready to check upon initialization | SCY | L | | |
| **mDL.RQ.7** | F | The mDL verifier can see the picture of the mDL holder to identify person under age verification | Identification of mDL holder | Portrait picture is presented on verifier | SCY | L | | |
| **mDL.RQ.8** | nF | The mDL data shall be protected | mDL data integrity and authenticity | Validation of signatures or hashes | SCY | M | | |
| **mDL.RQ.9** | F | The mDL holder data shall be safeguarded for privacy while being verified | Anonymized Proof of Age | Age verification success | SCY | H | | |
| **mDL.RQ.10** | F | Appropriate library/API to perform anonymization initialization (credentials issuing client API) | Initialize credential receipt process | Received anonymized credentials are properly prepared | SCY | M | | |
| **mDL.RQ.11** | F | The mDL app on Android OS shall be able to use appropriate library/API to perform anonymization initialization | Anonymization client-side | Age verification success | SCY | H | | |
| **mDL.RQ.12** | F | The mDL verifier on Android OS shall be able to perform anonymization verification | Anonymization verification | Age verification success | SCY | H | | |
| **mDL.RQ.13** | nF | Keys used by the IA to sign data and issue credentials shall be protected against misuse | mDL data integrity | Protections of keys backed by an HSM | MUL | H | | |
| **mDL.RQ.14** | F | Certificate profiles compliant with ISO 18013-5 draft | Integrity and interoperability | Age verification success | MUL | H | | |

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **mDL.RQ.15** | | Prevent the mDL holder to be recognized after successive age checks by verifiers (same or different) | Unlinkability | Successive age checks cannot link to the mDL holder | ALX | H | | |

## 4.4. PRECONDITIONS

The user must be previously enrolled/registered in the mobile Driver's License platform.

He must also have downloaded and installed the mDL app in his mobile device.

## 4.5. PRIORITY

mDL.RQ 9, 10, 11, 12, 13, 14 and 15 are High priority.

## 4.6. FREQUENCY OF USE

An end user could use this use case when needing to perform age verification in front of relying parties, which may be up to several times per week (estimated 1-5 per week).

In the case of a verifier that has to perform age verification to its customers that may increase the frequency of use up to multiple times per day depending on the number of customers.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

## 4.7. NORMAL COURSE OF EVENTS

The mDL holder has in his mobile device a data structure with the Driver's License information authenticated by the Issuing Authority. For the offline case the data is stored locally in the device after being downloaded from the IA.


*Figure 7 - Merchant verifier and mDL Holder*

The verification process is as follows:

1. The user wants to buy a restricted selling good (e.g. wine).
2. The merchants asks for ID for minimum age verification.
3. The user starts the mDL app and pairs with the merchant's mDL verifier (via NFC tap or QR-code scan), establishing a Bluetooth or NFC or WiFi connection.
4. The mDL verifier sends a request for age proof to the mDL app through NFC or QR.
5. The user consents to sending the requested data about age proof which are transferred by the mDL app to the mDL verifier through Bluetooth or NFC or WiFi.
6. The mDL verifier checks the authenticity and integrity of the data.
7. The mDL verifier notifies the merchant about the result of the validation.
8. The session between the verifier and the user is terminated.

**Offline Case**

In OLYMPUS, we proposed a solution for the offline case, which require the user to do storage of security critical material on its device.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

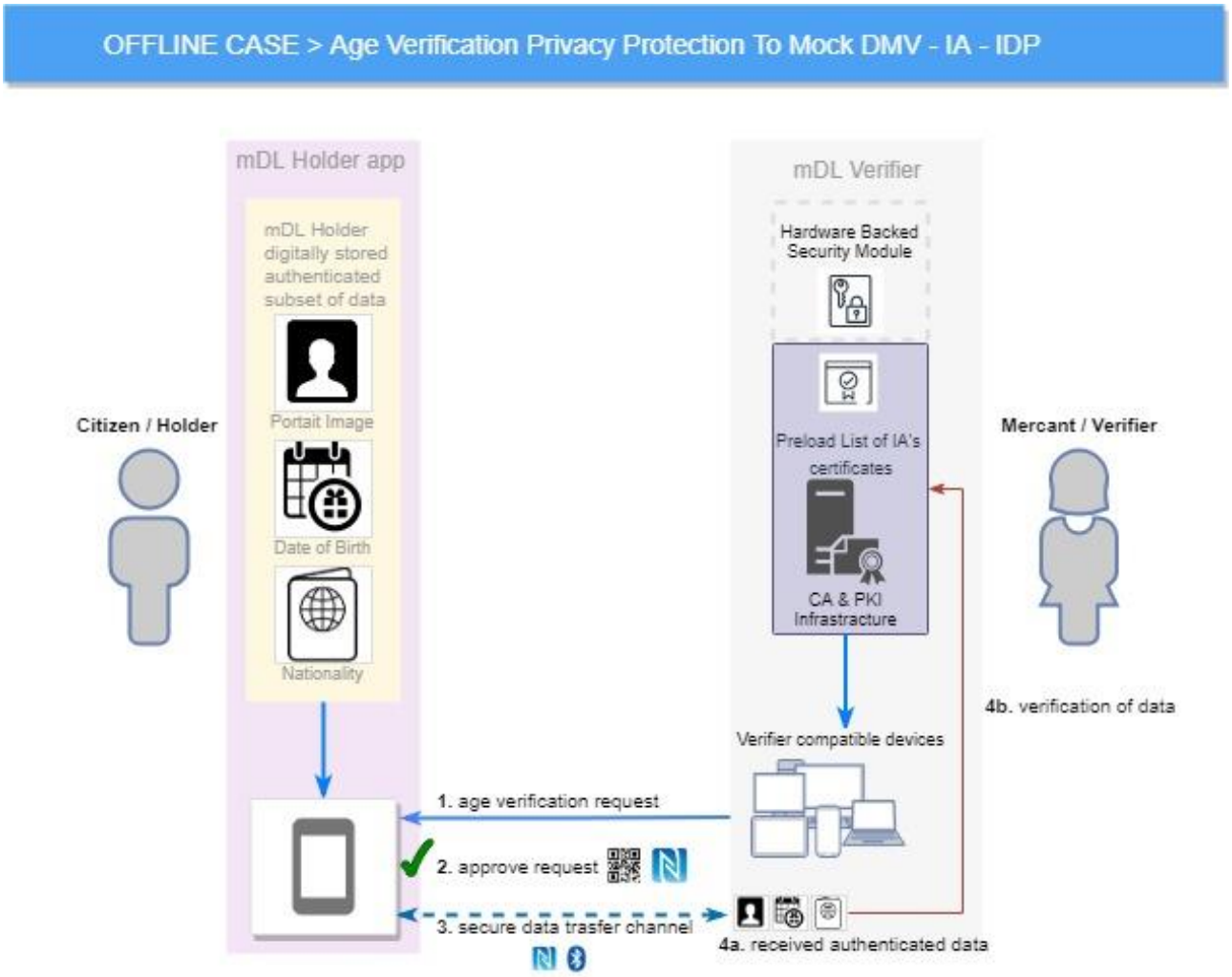


*Figure 8 - Offline Case Basic Flow*

The mDL holder has stored authenticated data by the IA that asserts integrity and authenticity to values of the following ISO 18013 fields, such as:

- Date of birth.

Additionally, the verifier may receive

- Portrait image as a means of visual identification.
- Nationality.
- Date of expiration of the mDL.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

- Date of next update of the mDL.

The date of next update is there to facilitate more secure storage of the mDL.

The business flow of the case is described as follows (see Figure 10):

1. Initialization of the age verification request may be performed using one of the following engagement channels:
    a. Out-of-bound (e.g. verbal, or a sign).
    b. Presentation of a QR code by the verifier's app an explicit request for age verification.
    c. Over-the-air short-range communication channel from the verifier app (optional when and if this is supported by user and verifier devices).
2. The mDL holder app receives the request for age verification.
3. Given consent, the mDL holder app uses a communication channel between itself and the mDL verifier app to transfer data in a short-range manner (to ensure verifiable presence of the user).
4. Once a secure channel is available the mDL holder app provides the mDL verifier a proof that it holds the requested information, authenticated by an IA.
5. The mDL verifier checks the received data and performs verification based on / trusting the IA's public certificate. It is assumed that the mDL verifier has a pre-loaded list of IAs' certificates received through a trusted channel. Optionally the verifier can go online, if available, to verify the certificate chain online against CRLs.

*Key anonymity, privacy and unlinkability aims:*

- In terms of privacy, the aim is to ensure minimal data disclosure. Therefore, only information about the mDL holder's age threshold is leaked to the mDL verifier.
- For unlinkability, the aim is to prevent the mDL holder from being recognized between successive checks by the same, or different mDL verifiers for age verification purposes.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

**Online Case**

We proposed an approach for the online case to avoid long-term storage of security critical material, based on ISO 18013-5 (2.2019):

a. The mDL verifier requests age verification from the mDL holder, by asking for:
    1. Date of birth.
    2. Nationality.
    3. Additionally, the verifier may receive:
        a) Date of expiration of the mDL.
        b) Date of next update of the mDL.
        c) Portrait image as a mean of visual identification.
    4. Initialization of the age verification request maybe performed using one of the following engagement channel alternatives:
        a) Out-of-bound (e.g. verbal, or a sign).
        b) Presentation of a QR code by the verifier's device.
        c) Over-the-air short-range communication (optional when and if this is supported by user and verifier devices).

b. The mDL holder gives consent to reveal the requested information.

c. The mDL holder then authenticates itself towards the IA/IDP and receives a time-constrained and authenticated token certifying the requested information.

d. The mDL holder processes and passes on this token to the mDL verifier.

e. The mDL verifier checks the token and accepts it, based on its trust in the IA.

Please note that the proposed approach does not require the Verifier to be connected/online (see Figure 12).

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

*Key anonymity, privacy and unlinkability aim:*

- In terms of privacy, the aim is to ensure minimal data disclosure. Therefore, only information about the mDL holder's age threshold is leaked to the mDL verifier.
- In terms of unlinkability the aim is to ensure that the token is constructed by the IA/IDP does not link a particular mDL holder to a particular mDL verifier. Furthermore, different tokens from one mDL holder to the same, or different, mDL verifiers should not be linkable.

At the moment the ISO 18013-5 draft provides the option for the mDL verifier to be registered against the Issuing Authority. In this case, the mDL holder can be linked by the IA to the verifier. Furthermore, the standardis following a track towards requiring that the mDL verifier contacts the IA for each verification request which will break unlinkability.

In order to provide unlinkability when a registered Verifier is online, an anonymized identifier is proposed to be used in order to access PII in IA back end systems.

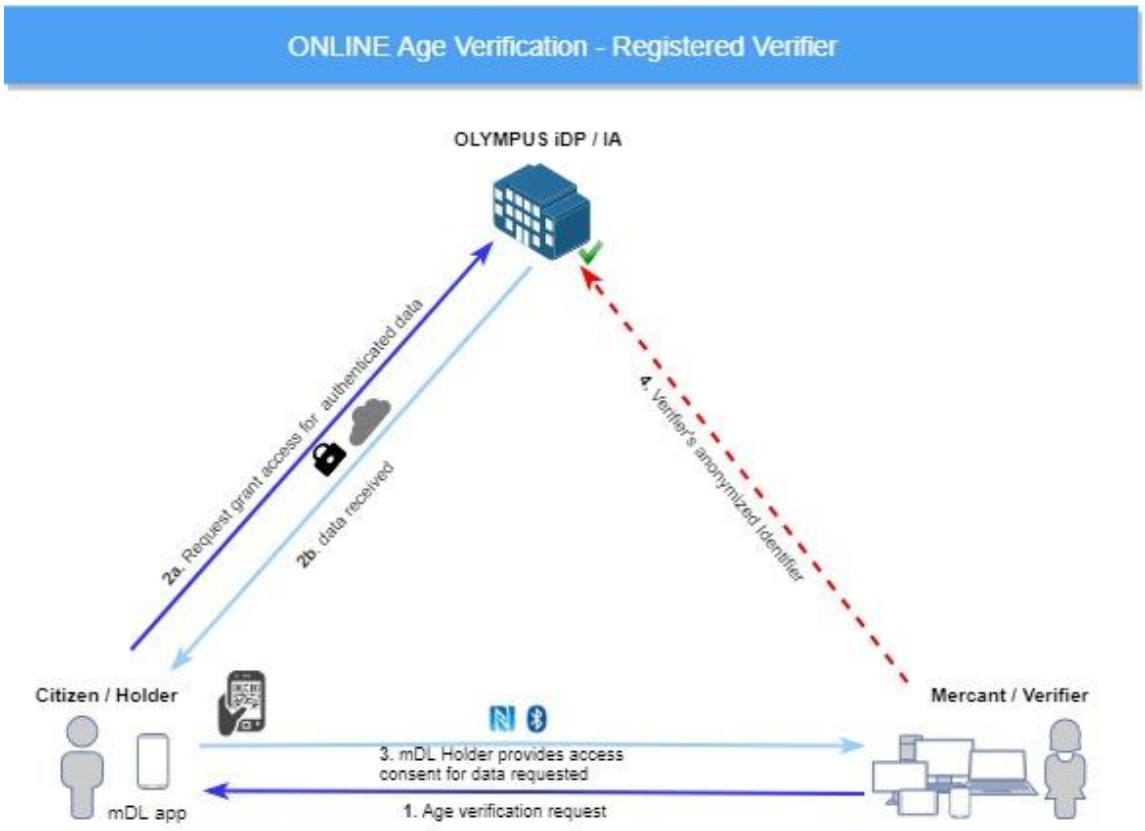


***Figure 9 - Online Case with Registered Verifier possible Flow***

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

### Enrolment

Enrolment is IA's decision and it is not governed by specific minimum requirements. However, an eID enrolment requirement needs to be taken into consideration if high level of assurance needs to be reached.

In this demonstrator, from a user's perspective, we will develop an enrolment flow as follows:

1. The user downloads the mDL app to his/her mobile device.
2. The mDL app is ready for enrolment once opened.
3. The mDL app may request typing in personal information beyond the DL, such as SSN or an IA enrolment code previously provided to the user out-of-band.
4. Once verified, the mDL app contacts the IA and learns authenticated data reflecting the DL.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

## 4.8. SEQUENCE DIAGRAM

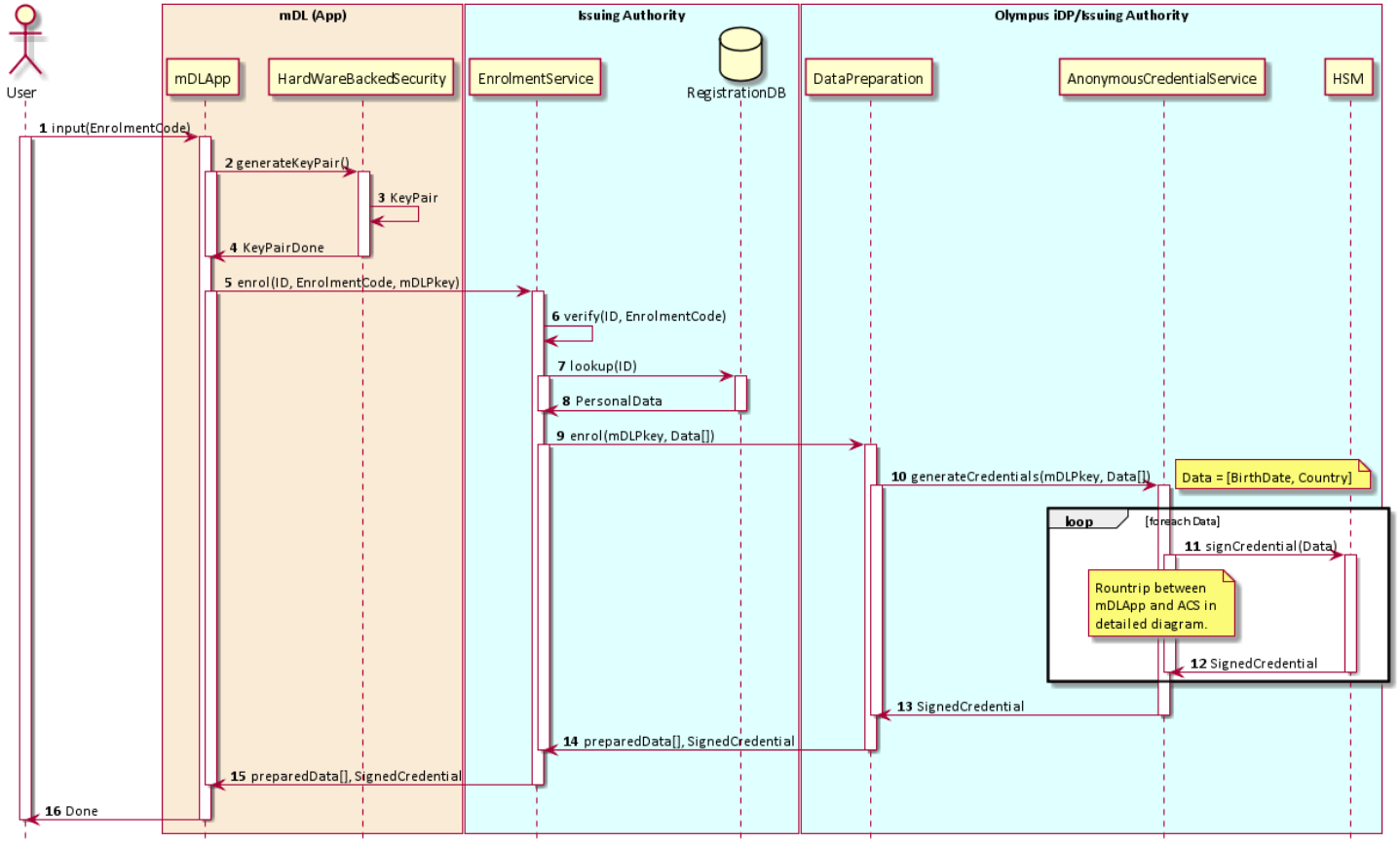


*Figure 10 - mDL Enrolment*

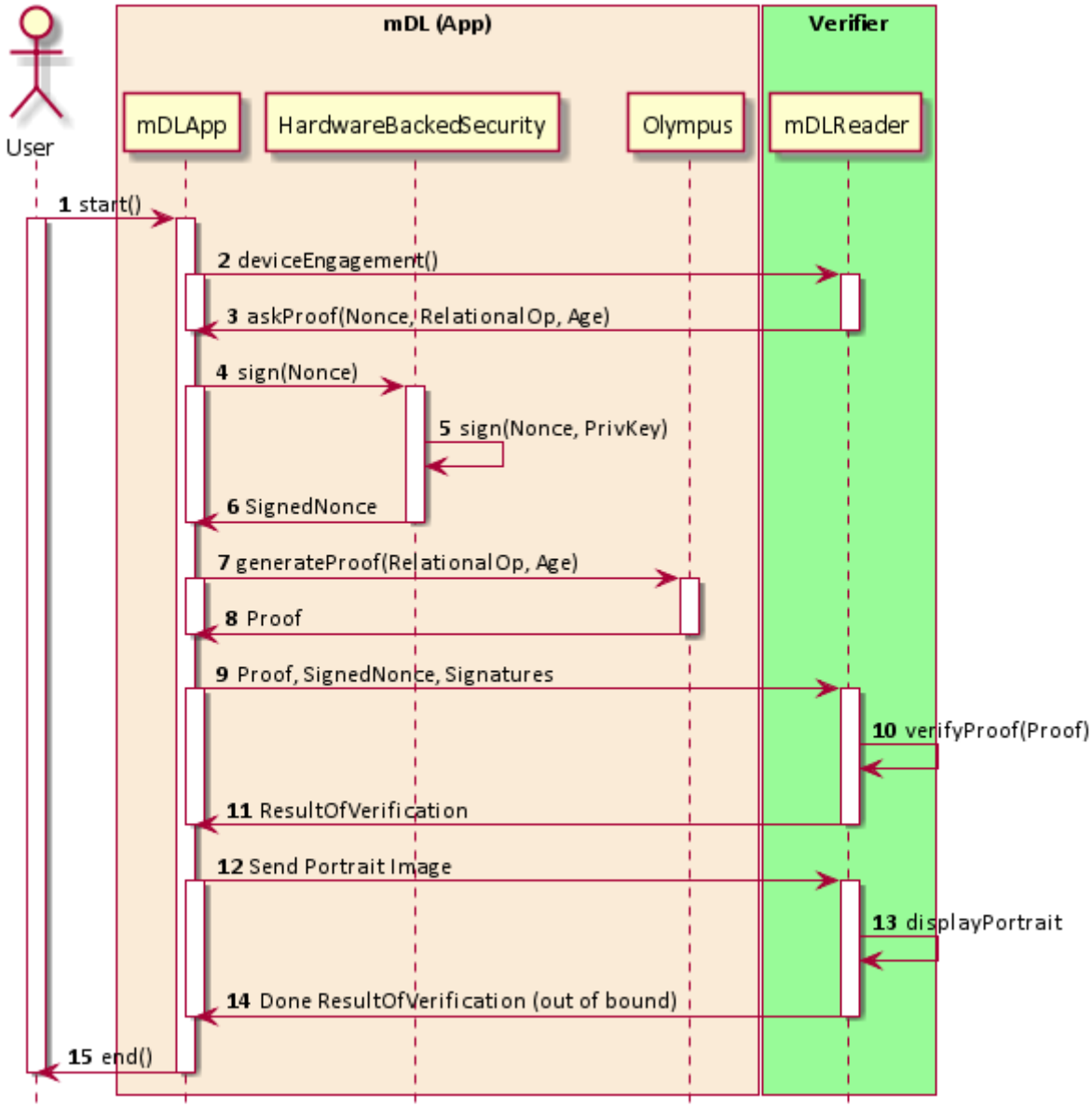


*Figure 11 - mDL verification age Offline*

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

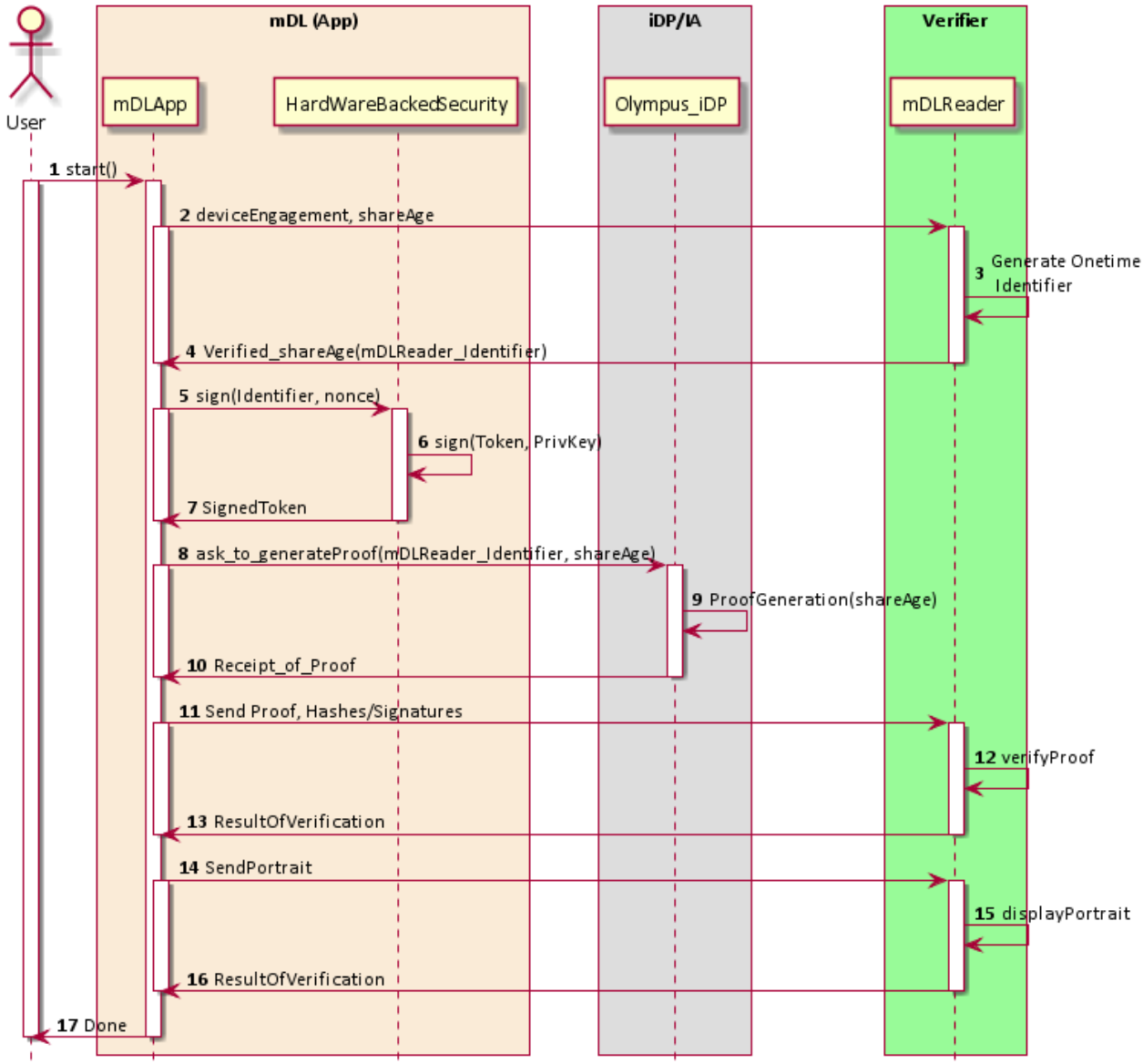


*Figure 12 - mDL verification using alternative online approach with connection and no mDL PII data info*

## 4.9. EXCEPTIONS

In case a cryptographic verification fails (signature, digest, untrusted root anchor, etc) the execution flow is stopped, and both the User and Verifier are presented an error message.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

## 4.10. SPECIAL REQUIREMENTS

1. The verifier's device must include a camera capable to read QR codes, NFC with API stack (full access for HCE host card emulation and emulation of NDEF tags) and BLE full API. It must also include a modern and adequate analysis-supporting screen (to display an ICAO portrait image when necessary).
2. The user's device must include a modern and adequate analysis-supporting screen to display a QR code as well as it must include BLE full API and/or NFC with API stack (full access for HCE host card emulation and reading NDEF tags). Camera is also recommended.
3. To achieve higher security the user's device may include hardware backed security module at the least, and preferably a TEE and/or mobile HSM equivalent.
4. A CA & PKI Infrastructure needs to be in place in order to provide IA signing certificate authority.
5. The verifier's device shall support connection to Olympus / mock DMV-IA at given times.
6. The user's device shall support connection to Olympus / mock DMV-IA at given times.

## 4.11. ASSUMPTIONS

Age verification is performed in person i.e. in attended cases from a relying party person.

## 4.12. NOTES AND ISSUES

In devices where there is hardware back security available, it is possible to store securely the amount of mDL data and to prevent unauthorized reading.

On rest of devices, risk assessment can be performed to allow storing the data in a software based secure wallet.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

# 5. CONCLUSIONS

This document has described a set of Use Cases and their corresponding functional requirements where real world problems are resolved with the technology building blocks of the OLYMPUS project. Most of the problems under research are related with data privacy and minimal disclosure of information.

In particular, two cases have been presented: Credit File and Mobile Driver License.

The first, raises the need to provide privacy and non-traceability to users when choosing banking services in which, nowadays, it is necessary to reveal a large amount of sensitive information that can be used for other purposes by banks and IdPs. The Olympus project faces this problem by providing minimum disclosure principles and the oblivious authentication in the IdP.

Second, the Mobile Driver License case raises the challenge of authenticating a user based on an official document (driver's license). Currently, this process reveals too much information and Olympus, faces this situation by applying cryptographic procedures (Zero knowledge proofs) in order to reveal only the desired data when, for example, the user is acquiring a restricted good (i.e, a bottle of wine) in a store.

Finally, throughout the project, demonstrators will be developed integrating the results of WP4 and WP5. This document establishes the requirements for such demonstrators and provides a baseline for comparing the results of the project with the initial plan.

# 6. REFERENCES

[1] 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) *Official Journal of the European Union*, Vol. L119 (4 May 2016), pp. 1-88

[2] J. Camenisch and E. Van Herreweghen, “Design and implementation of the idemix anonymous credential system,” in Proceedings of the 9th ACM Conference on Computer and Communications Security, ser. CCS ’02. New York, NY, USA: ACM, 2002, pp. 21-30.

[3] J. Camenisch and A. Lysyanskaya, “An efficient system for non-transferable anonymous credentials with optional anonymity revocation,” in Advances in Cryptology—EUROCRYPT 2001. Springer, 2001, pp. 93-118.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 786725

[4] J. Camenisch, Y. Gilad, A. Lehmann, Z. Nagy, G. Neven, “Unlinkable Threshold Password-Authenticated Single Sign-On using Privacy-ABCs”, September 2013

[5] J. Camenisch, Y. Gilad, A. Lehmann, Z. Nagy, G. Neven, “Threshold Password-Authenticated Single Sign-On using Threshold Signatures”, September 2013

[6] Draft N1644 ISO/IEC CD 18013-5:2018(E), Information technology -- Personal identification -- ISO-compliant driving license -- Part 5: Mobile Driving License application (mDL)

[7] J. B. Bernabé, J. L. H. Ramos, and A. F. Gómez-Skarmeta, “Holistic privacy-preserving identity management system for the internet of things,” Mobile Information Systems, vol. 2017, pp. 6384186:1-6384186:20, 2017. [Online]. Available: https://doi.org/10.1155/2017/6384186

[8] J. L. C. Sanchez, J. B. Bernabe, and A. F. Skarmeta, “Integration of anonymous credential systems in iot constrained environments,” IEEE Access, vol. 6, pp. 4767-4778, 2018.

[9] Jorge Bernal Bernabe, Antonio Skarmeta, Nicolás Notario, Julien Bringer and Martin David, Towards a Privacy-preserving Reliable European Identity Ecosystem. AFP2017 - ENISA Annual Privacy Forum 2017, June 2017, Vienna.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 786725

# ANNEXES

## ANNEX 1: EXPLANATION OF USE CASE ELEMENTS

### Description

- The description will introduce the use case in order to understand the scenario and help to identify the possible actors.

### Actors

- An actor is a person or other entity external to the software system being specified who interacts with the system and performs use cases to accomplish tasks.
- Different actors often correspond to different user classes, or roles, identified from the customer community that will use the product.

### Requirements

| ID | Type | Description | Rationale | Fit Criterion | Originator | Priority | Conflicts | History |
|---|---|---|---|---|---|---|---|---|
| **Unique identificator** | Functional, specific non-functional or Constraint | A 1 sentence desc. | Why is important | Measurement that makes the requirement testable. | The person who raised this requirement | Your rating scale eg:H,M,L or MOSCOW or scale 1-10 | Other requirements that cannot be met if this one is | Your review checkpoints |

### Preconditions

- The set of conditions that must be met so that a use case can be initiated.

### Postconditions

- Reflects the state in which the system remains once the use case has been executed.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725

**Priority**

- Indicate the relative priority of implementing the functionality required to allow this use case to be executed. The priority scheme used must be the same as that used in the software requirements specification.

**Frequency of use**

- Describes how often it is expected to happen the use case.

**Normal course of events**

- Describes the normal interaction in the use case.

**Sequence diagram**

- It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

**Exceptions**

- Describe any anticipated error conditions that could occur during execution of the use case and define how the system is to respond to those conditions. Also, describe how the system is to respond if the use case execution fails for some unanticipated reason. Number each exception using the Use Case ID as a prefix, followed by “EX” to indicate “Exception”. Example: X.Y.EX.1.

**Includes**

- List any other use cases that are included (“called”) by this use case. Common functionality that appears in multiple use cases can be split out into a separate use case that is included by the ones that need that common functionality.

**Special requirements**

- Identify any additional requirements, such as non-functional requirements, for the use case that may need to be addressed during design or implementation. These may include performance requirements or other quality attributes.

**Assumptions**

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 786725

- List any assumptions that were made in the analysis that led to accepting this use case into the product description and writing the use case description.

**Notes and issues**

- List any additional comments about this use case or any remaining open issues or TBDs (To Be Determined) that must be resolved. Identify who will resolve each issue, the due date and what the resolution ultimately is.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725