D1.3

Specification of System Requirements

Project number:	959072
Project acronym:	mGov4EU
Project title:	Mobile Cross-Border Government Services for Europe
Start date of the project:	1st January, 2021
Duration:	36 months
Programme / Topic:	H2020-SC6-GOVERNANCE-2020, Governance for the future

Deliverable type:	Report
Deliverable reference number:	DT-GOVERNANCE-05-959072 / D1.3 / V1.1
Work package contributing to the deliverable:	WP1
Due date:	June 2021 - M06
Actual submission date:	25th May 2022

Responsible organisation:	ECS
Editor:	Detlef Hühnlein
Dissemination level:	PU
Revision:	V1.1

Abstract:	This deliverable provides an elicitation of major system requirements and a specification of Use Cases.
Keywords:	eID, eIDAS, TOOP, SDG

The project mGov4EU has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 959072.

Editor

Detlef Hühnlein (ECS)

Contributors

Thomas Zefferer (A-SIT)

Steffen Hammer (ECS)

Tobias Wich (ECS)

Rachelle Sellung (FHG)

Andreea Corici (FHG)

Blaž Podgorelec (TUG)

Hans Graux (TLX)

Robert Krimmer (UTARTU)

Carsten Schmidt (UTARTU)

Executive Summary

This deliverable provides an elicitation of major system requirements and a specification of use cases, with a special focus on the three envisioned pilot scenarios (eVoting, Smart Mobility, and Mobile Signature).

For this purpose, the document starts from three strategic goals of the mGov4EU project, which is to (1) pave the way for “mobile first” eGovernment procedures across Europe, which (2) smoothly integrate both the eIDAS [1], as well as the Single Digital Gateway (SDG) [2] regulation in order to (3) enable mobile and user-centric cross-border eGovernment processes.

The present document captures requirements in various categories, such as general system requirements, software requirements, economic and policy requirements, usability requirements, legal requirements and last but not least security and accountability requirements.

For the envisioned pilot scenarios, the document first outlines the planned piloting methodology and then outlines use cases, which serve as input for the forthcoming work packages WP2, WP3 and WP4.

The following table shows the relation between D1.3 and other tasks, work packages and deliverables:

Contributing tasks of this WP	T1.3
Input from other tasks/WPs	T1.1, T1.2
Output to other tasks/WPs	T1.2, T2.1, T2.2, T2.3, T2.4, T2.5, T2.6 (WP3, WP4)
Output to other deliverables	D1.2, D2.1, D2.2, D2.3, D2.4, D2.5, D2.7, (WP3)

Table of Content

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Meaning
AdES	Advanced Electronic Signature
ASR	Abstract System Requirements
CAdES	CMS Advanced Electronic Signature
eID	Electronic identification
EPR	Economic and Policy Requirements
EUDIW	European Digital Identity Wallet
IdP	Identity Provider
JAdES	JSON Advanced Electronic Signature
JPTF	Joint Piloting Task Force
MS	Mobile Signature (Pilot)
PAdES	PDF Advanced Electronic Signature
SDG(R)	Single Digital Gateway (Regulation)
SM	Smart Mobility (Pilot)
SP	Service Provider
UC	Use Case
UR	Usability Requirements
XAdES	XML Advanced Electronic Signature

Chapter 1 Introduction

This deliverable is the result of T1.3 of the mGov4EU project. The aim of this task was to provide a solid foundation for forthcoming work, in particular for:

- WP2, which deals with the design of interfaces, apps and services, and
- WP3, which is responsible for the implementation and system integration of the building blocks and components designed in WP2 and
- the envisioned pilots in WP4.

The outcome of T1.3 is an elicitation of major system requirements (see Chapter 2) and a specification of different use cases, which are expected to be implemented within the three envisioned mGov4EU pilots (eVoting, Smart Mobility and Mobile Signature) defined in WP4.

For this purpose, the document first recalls the three strategic goals of the mGov4EU project (see Section 2.1), which is (1) “mobile first” eGovernment, (2) the alignment of eIDAS [1] with SDG [2] and (3) user-centric cross-border procedures. Against the background of these goals, the document elicits further system requirements (see Sections 2.2, 2.3, 2.4, 2.5 and 2.6), as well as use cases, which are derived from the three mGov4EU pilots and will be planned, conducted, and evaluated through the piloting methodology defined in Section 3.1.

Chapter 2 Major System Requirements

This chapter identifies the major system requirements relevant for the mGov4EU project, which serve as a guideline throughout the duration of the project and are envisioned to be used as a point of reference for the design of building blocks and components (WP2), their implementation (WP3) and the evaluation of the mGov4EU system in WP5.

In addition to general system requirements, further system requirements in different categories are elicited. These include:

- Software Requirements,
- Social, Economic, and Policy Requirements,
- Usability Requirements,
- Legal Requirements, and
- Security and Accountability Requirements.

For each category, there is an established structure and methodological reason that is tailored to the needs of each perspective, which may vary from category to category.

The requirements are specified in textual form using requirement levels according to IETF RFC 2119 [3] as recalled in Table 1:

Requirement Level	**IETF Definition**
MUST / SHALL	This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
MUST NOT / SHALL NOT	This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the Option provides.)

Table 1: Requirement Levels according to IETF RFC 2119 [3]

2.1 General System Requirements

In order to achieve a focused, yet reasonably comprehensive spectrum of high-level requirements for mGov4EU, as a first step, Section 2.1 recalls the three main strategic goals of the mGov4EU project, which are

1) "mobile first" eGovernment (Section 2.1.1),
2) eIDAS [1] as well as SDG [2] alignment (Section 2.1.2) and
3) user-centric cross-border procedures (Section 2.1.3),

and determines requirements relevant for each goal.

2.1.1 Mobile first

A central requirement for the mGov4EU system is that it is usable in a mobile environment in order to enable "mobile first" eGovernment services.

The main requirements set out for the "mobile first" approach applied in mGov4EU are listed in Table 2.

Name	Requirement
R-MF-01	**Optimised for mobile platforms** The UI/UX design of all components and use cases within mGov4EU SHALL be optimised for mobile platforms.
R-MF-02	**Available for Android and iOS** Mobile apps and related libraries SHALL be made available for reasonably current[1] Android and iOS platforms.
R-MF-03	**User-friendly and robust** The mGov4EU solution SHALL be user-friendly, perceivable, operable, understandable and robust. See also Section 2.4 and R-SDGR-03 in Section 2.1.2.
R-MF-04	**Support for EU Digital Identity Wallet** The mGov4EU solution SHALL support the forthcoming EU Digital Identity Wallet and its related operational processes.
R-MF-05	**Support for mobile cross-border processes** The mGov4EU solution SHALL support mobile cross-border processes due to moving to another Member State or having multiple citizenships.

Table 2: Mobile first requirements (MF)

2.1.2 eIDAS and SDG alignment

The eIDAS and SDG alignment can be viewed from two perspectives (SDG and eIDAS), which give rise to different sets of requirements. Therefore we first start with specifying requirements from the SDG perspective and then continue with the eIDAS perspective, which in particular focusses on the

[1] The exact determination of the supported API level will be determined within the development phase considering usage statistics to ensure a reasonable wide coverage.

requirements related to the European Digital Identity Wallet (EUDIW), which has been introduced with the recently published proposal for a revised eIDAS-Regulation [4].

2.1.2.1 SDG perspective

The Single Digital Gateway Regulation (**SDGR**) (EU) 2018/1724 of the European Parliament and of the Council, introducing a single digital gateway aims at "facilitating **online access** to the information, administrative procedures and assistance services that citizens and businesses need to **move within the Union** and to **trade, establish themselves** and **expand their businesses** in another Member State" [2]. The mGov4EU project focuses on online services that citizens need to access from a **mobile device** in a cross-border context due to moving to another Member State or having multiple citizenships (thus having multiple eIDs and residencies).

The key requirements extracted from SDGR in the context of the mGov4EU project are presented in Table 3.

Name	Requirement
R-SDGR-01	**Fully online procedures** The identification of users, the provision of information and final submission SHOULD all be **carried out electronically** and supporting evidence, signature at a distance. Exceptions may occur where special regulations are in place for communication using paper. See [2] (Article 6 "Procedures to be offered fully online").
R-SDGR-02	**Electronic communication and acknowledgement** The procedural steps of requesting the procedure, the output and the completion of the procedure users SHOULD be electronically communicated and acknowledged. See [2] (Article 6 "Procedures to be offered fully online").
R-SDGR-03	**Perceivable, operable, understandable and robust** Online services SHOULD be "perceivable, operable, understandable and robust" in a mobile environment. See [2] (Article 8 "Quality requirements related to web accessibility)
R-SDGR-04	**Clear and transparent information for users** Before the user identifies, it MUST receive clear information, including information regarding the relevant steps of the procedure to be taken by the user, the competent authority details, the accepted means of authentication, identification and signature for the procedure as well as the type and format of evidence to be submitted. See [2] (Article 10 "Quality of information on procedures")
R-SDGR-05	**eID, signatures and seals where supported** The cross-border users MAY identify and authenticate themselves, sign or seal documents electronically, where supported for non-cross-border users. See [2] (Article 13 "Cross-border access to online procedures")
R-SDGR-06	**Provide evidence where supported**

Name	Requirement
	The cross-border users MAY provide evidence of compliance with applicable requirements and to receive the outcome of the procedures in electronic format in all cases where supported for non-cross-border users. See [2] (Article 13 “Cross-border access to online procedures”)
R-SDGR-07	**Explicit request** Processing of requests for evidence MUST only happen at the **explicit request** of the user, which SHOULD be smoothly integrated with the eID procedure. See [2] (Article 14 “Technical system for the cross-border automated exchange of evidence and application of the ‘once-only’ principle”) and R-L-24 in Section 2.5.3.
R-SDGR-08	**Confidentiality** and **integrity** of the evidence MUST be ensured. See [2] (Article 14 “Technical system for the cross-border automated exchange of evidence and application of the ‘once-only’ principle”).
R-SDGR-09	The user MUST be able to **preview the evidence** to be used by the requesting competent authority and to choose whether or not to proceed with the exchange of evidence. The preview of the evidence SHOULD be smoothly integrated with the eID procedure. See [2] (Article 14 “Technical system for the cross-border automated exchange of evidence and application of the ‘once-only’ principle”) and R-L-25 in Section 2.5.3.
R-SDGR-10	A high level of **security for the transmission and processing of evidence** MUST be ensured.
R-SDGR-11	Evidence exchanges MUST be **limited to what is technically necessary** for the exchange of evidence, and then only for the duration necessary for that purpose.

Table 3: Requirements derived from SDGR [2]

The draft version of SDG Implementing Act (SDG-IA) on technical and operational specifications from the 31th March 2021 describes how the SDGR including the Once-Only Principle are to be executed. The draft includes multiple entities, including:

- (a) the procedure portals of evidence requesters (from the Data Consumer side)
- (b) the data services of evidence providers (also known as Data Providers)
- (c) intermediary platforms, where relevant (for example for hiding the complexity of the infrastructure by aggregating data services based on their type or location)
- (d) the national registries and services referred to in Article 8(2), where relevant
- (e) the eIDAS nodes for user authentication and identity matching
- (f) the eDelivery Access Points for assuring interoperability for cross-border services (this refines the requirement **R-SDG-10** from above)
- a set of common services that will be governed by the European Commission

Regarding the common services, they include: (i) the data service directory (DSD) (identifying providers, evidences, and semantic data; and Level of Assurance (LoA) requirements for its accessibility), (ii) the evidence broker (determining equivalence between evidences), (iii) the semantic repository (identifying data models, associated schemata and data formats for each evidence; here formats are specified), (iv) the common user feedback tool and the integration elements and interfaces required to connect the components (a) to (f) from above.

The SDG Implementing Act in preparation, aims at refining the requirements from SDGR, not change them. Thus, in the next table the set of requirements from the implementing act and relevant to

mGov4EU context is presented by stating the equivalent requirement from SDGR or that it brings clarification compared to SDGR.

Name	Requirement
Evidence requester (Data consumer)	
R-SDG-IA-01	**Information for users** The mGov4EU solution MUST inform users of the procedures steps and results. See also R-SDGR-02, R-SDGR-04 and R-SDGR-09.
R-SDG-IA-02	**Directly submitted evidences** The mGov4EU solution MUST allow users to request evidences that could be submitted directly too.
R-SDG-IA-03	**Support of eIDAS eIDs** The mGov4EU solution MUST support eIDAS eIDs. See also R-SDGR-05.
R-SDG-IA-03	**Only one identification process per LoA** Only one identification process MAY be required (federation), unless required LoA changes
R-SDG-IA-4	**Indicate name of provider and evidence type** The explicit request MUST include the name of the provider and the evidence type. See also R-SDGR-07.
R-SDG-IA-5	**Support of logging and accountability** Specific evidence request elements MUST be included for logging and accountability reasons.
R-SDG-IA-6	**Temporary preview of evidence** The portal of the evidence requester MUST provide a preview space, from which data is deleted after the preview See also R-SDGR-09.
Evidence requester (Data consumer)	
R-SDG-IA-7	**Support eDelivery Access Points** The mGov4EU solution MUST support eDelivery Access Points. See also R-SDGR-10.
R-SDG-IA-8	**Handling of evidence (references)** The mGov4EU solution MUST be able to receive and pass on evidence or evidence references.
R-SDG-IA-9	**Unambiguous Identity Matching**

Name	Requirement
	The mGov4EU solution MUST conduct an identity matching process based on eIDAS data. Note, that there is no ambiguity tolerated. See also R-SDGR-10.

Table 4: Requirements from SDG Implementation Act draft from 31 March 2021

2.1.2.2 eIDAS perspective

The recently published proposal for a revised eIDAS-Regulation [4] contains requirements for a European Digital Identity Wallet (EUDIW). As mGov4EU seeks best possible compliance especially with wallet-related aspects of the EC's proposal, EUDIW requirements must also be regarded as relevant system requirements for mGov4EU solutions. In particular, the following EUDIW-related requirements derived from the EC's proposal define relevant system requirements for mGov4EU solutions:

Name	Requirement
R-W-01	**Store identity data, credentials and attributes** The EUDIW SHALL allow the user to store identity data, credentials and attributes linked to her/his identity and to provide them to relying parties on request. See [4], Article 3 (42).
R-W-02	**Support online and offline authentication** The EUDIW SHALL support online and offline[2] authentication. See [4], Article 3 (42), Article 6a (3) (a) and Article 6a (4) (a) (3).
R-W-03	**Creation of qualified electronic signatures and seals** The EUDIW SHALL be capable to create qualified electronic signatures and seals. See [4], Article 3 (42) and Article 6a (3) (a).
R-W-04	**Manage identification data and attestation of attributes** The EUDIW SHALL be capable to request, obtain store, select, combine and share identification data and attestation of attributes. See [4], Article 6a (3) (a).
R-W-05	**Transparency and Traceability** The EUDIW SHALL perform the management of identification data and attestation of attributes in a transparent and traceable manner. See [4], Article 6a (3) (a).
R-W-06	**Common interface to Trust Service Providers (TSPs)** The EUDIW SHALL have a common interface to "qualified and non-qualified trust service providers issuing qualified and non-qualified electronic attestations of attributes or other qualified and non-qualified certificates for the purpose of issuing such attestations and certificates".

[2] This means that it is possible to authenticate in a "local mode" (see [4], Art. 6a (4) (a) (3)) without an internet connection.

Name	Requirement
	See [4], Article 6a (4) (a) (1).
R-W-07	**No information for TSPs about the use of attributes** The EUDIW SHALL ensure that “trust service providers of qualified attestations of attributes cannot receive any information about the use of these attributes”. See [4], Article 6a (4) (b).
R-W-08	**Common interface to Relying Parties** The EUDIW SHALL have a common interface to “relying parties to request and validate person identification data and electronic attestations of attributes”. See [4], Article 6a (4) (a) (2).
R-W-09	**Assurance Level ‘high’** The EUDIW SHALL be “issued under a notified electronic identification scheme of level of assurance ‘high’”. See [4], Article 6a (6).
R-W-10	**Free use** “The use of the European Digital Identity Wallets shall be free of charge to natural persons.” See [4], Article 6a (6).
R-W-11	**Accessible for persons with disabilities** The EUDIW SHALL “be made accessible for persons with disabilities in accordance with the accessibility requirements of Annex I to Directive 2019/882” See [4], Article 6a (10).
R-W-12	**Certification** “The conformity of European Digital Identity Wallets with the requirements laid down in article 6a paragraphs 3, 4 and 5 shall be certified by accredited public or private bodies designated by Member States.” See [4], Article 6c (3).
R-W-13	**Privacy** The EUDIW SHALL respect privacy aspects in the sense that it supports selective disclosure and only provide the minimum attributes necessary (e.g. proof of age instead of date of birth, if requested by relying party accordingly). See [4], Recital (29) and Article 12b (3).
R-W-14	**Supported attributes** The EUDIW SHOULD support arbitrary attributes. The EUDIW SHALL in particular support the minimum list of attributes listed in [4], Annex VI: 1. Address; 2. Age; 3. Gender; 4. Civil status;

Name	Requirement
	5. Family composition; 6. Nationality; 7. Educational qualifications, titles and licenses; 8. Professional qualifications, titles and licenses; 9. Public permits and licenses; 10. Financial and company data. See [4], Annex VI.

Table 5: Wallet Requirements (W)

2.1.3 User-Centric Cross-Border Procedures

The user-centric implementation of cross-border procedures is one of the key elements for the setup of meaningful pilots in the context of the mGov4EU project. Consequently, mGov4EU and the provided solutions have to fulfill the requirement of "Cross-Border by Default", as is it is described in the eGovernment Action Plan 2016-2020 of the EC in a user-centric manner. For this purpose, the following requirement have been defined:

Name	Requirement
R-UCB-01	**Data Provider and Data Consumer in different Member States** At least the Data Provider and one or more Data Consumers MUST reside in different Member States
R-UCB-02	**eID Provider and Data Subject reside in different Member States** At least the eID Provider and one or more Data Subjects MUST reside in different Member States
R-UCB-03	**User-centric cross-border procedures** The cross-border procedure SHALL be implemented in a user-centric manner in which the citizen is actively initiating the request and the result is provided to the citizen for review and further processing. See R-MF-03 and R-MF-04 in Section 2.1.1 as well as R-SDGR-07 and R-SDGR-07 in Section 2.1.2.

Table 6: User-centric cross-border requirements (UCB)

2.2 Software Requirements

This subsection sets out the requirements for software developed within mGov4EU.

In this project the term software refers to software architectures and components.

Name	Requirement
R-SW-01	The developed software SHOULD be modular to ease the maintenance of the software.
R-SW-02	Modules of the software SHOULD have a well-defined interface and as few dependencies as possible.
R-SW-03	An easy-to-setup simulator abstracting one or more components MAY be included in the set of software artifacts in order to ease the implementation of Data

Name	Requirement
	Consumer and Data Provider components, as well as the integration and validation of backend components.
R-SW-04	Server side artefacts SHOULD be easily packable in docker containers.
R-SW-05	The system SHOULD use interfaces and protocols based on open standards as far as possible.
R-SW-06	External components spanning interfaces and protocols used in the system MUST be documented.
R-SW-07	The system MUST NOT expose internal communication endpoints.
R-SW-08	Software components MUST implement all required features so that the component is capable to fulfil its role as defined by the technical architecture.
R-SW-09	Software components MUST feature a logging feature so that technical logs can be produced during operation to record the software's behaviour and to allow for subsequent investigations.
R-SW-10	Software components MUST properly respond (i.e., implement protocols for recovery) to abnormal situations (e.g., failures, errors, etc.).
R-SW-11	Software components MUST be implemented in a way that their performance does not decrease disproportional with a growing number of parallel users.
R-SW-12	Software components MUST be implemented such that they do not raise disproportional hardware requirements to achieve an acceptable performance.
R-SW-13	Software component SHOULD properly process the operations simultaneously performed by multiple users.
R-SW-14	Software interfaces SHOULD be defined in a way to support interoperability and to maximize the re-usability of software components.
R-SW-15	Direct access to databases SHOULD be allowed only for software components that need such (type of) data to perform their core operations successfully.
R-SW-16	Software components SHOULD store and process a minimum amount (i.e., only for service delivery required data) of the end-user data.
R-SW-17	Redundancy in stored data SHOULD be minimized.
R-SW-18	Source code and documentation MUST be available in a form that supports software maintenance.
R-SW-19	Software components SHOULD be easily portable among different host systems.
R-SW-20	Software components SHOULD be properly documented.

Table 7: Software Requirements (SW)

2.3 Economic Requirements

The economic requirements were derived after a process of three preliminary steps. First, various relevant socio-economic theories were identified and explored that could be important regarding the markets of interest of mGov4EU. Second, we considered the market overview that was explored in mGov4EU context in D1.1 and D2.1. Third, these requirements take into consideration a preliminary stakeholder analysis that is a part of D2.1.

The goal of these requirements is to represent the needs of all relevant stakeholders, market interests, and to prevent potential adoption barriers. In addition, the economic requirements also benefit from the learned experience of economic requirement work done in previous projects such as LIGHTest [5], FutureID [6], SkIDentity [7], and SSEDIC [8], [9] .

This theoretical foundation relies on the following identified relevant socio-economic theories that cover the themes of information systems, business administration, and economics. A total of 15 theories ranging from technology acceptance theories to market-centred theories and transaction cost economics have been identified over the course of the past projects. A proper selection and analysis of the appropriate theories allows the identification of the most influential and relevant economic requirements and factors for the stakeholders. The theories used in this case include Porter's Competitive Strategy theory [10], Roger's Diffusion of Innovations theory [11], as well as Williamson's Transaction Cost Economics theory from 1981 [12]. These theories, along with the remaining 13 other theories, encompass a wide range of issues and phenomena that can directly, or indirectly, affect the economics of a product or system. Factors like the asymmetric distribution of information (Agency Theory), a person's behaviour towards innovations (Diffusion of Innovations Theory), and the effect of external environmental factors on the adoption of IT solutions (Technology Organization Environment Framework) are just some of the constituents considered when deriving the following economic requirements for mGov4EU. The following list provides an overview of the relevant theories employed for the determination of the economic requirements:

- Agency Theory [13]
- Agenda-Setting Theory [14]
- Competitive Strategy [10]
- Diffusion of Innovations [11]
- Fit Viability Model [15]
- Fit Viability Model (Adapted to Mobile Commerce Technologies) [16]
- Lemons Market [17]
- Multisided Markets [18]
- Network Effects [19]
- Principal-Agent Theory [13]
- Property Rights Theory [20]
- Stakeholder Theory [21]
- Technology Acceptance Model (TAM) [22]
- Technology Organization Framework [23]
- Transaction Cost Economics [12]
- Unified Theory of Acceptance and Use of Technology (UTAUT) [24]

The development of the following economic requirements aims at anticipating and satisfying the needs and expectations of mGov4EU's stakeholders. This will help mGov4EU in identifying the economic requirements expressed by end-users, identity providers, and service providers in order to provide a system that allows an economically reliable and beneficial use for all its parties involved.

Name	Requirement
R-E-01	**Support of various business models** Different stakeholders and scenarios require different business models. There is no one business model that is suitable for all applications. Therefore, the

Name	Requirement
	mGov4EU building blocks MUST support different business models and applications. (Refer to T2.1, T2.7 regarding Potential MGOV4EU Business Models)
R-E-02	**Support for different compensation sources** An mGov4EU building block requires financial resources for implementation and operation. Therefore, mGov4EU building blocks MUST make it possible to justify/offset the necessary investments. There is no need to burden/relieve all participants financially (possibly free of charge for individual participants). Therefore, mGov4EU MUST support the use of different sources for compensation.
R-E-03	**Support of different models of cost and revenue distribution** An mGov4EU building block requires financial resources for implementation and operation. There could be an imbalance of stakeholders who have costs and others with revenue related to mGov4EU building blocks. Therefore, mGov4EU building blocks MUST make it possible to justify/offset these imbalances. Therefore, mGov4EU MUST support the use of different models of cost and revenue distribution.
R-E-04	**Support for various pricing models and strategies** The willingness to pay of different users: Services vary depending on the application. In order to build a sustainable business model, users and services must be addressed in different ways / levels to address their willingness to pay. Therefore, mGov4EU MUST support price differentiation according to the different willingness to pay for the different services.
R-E-05	**Easy adoption** mGov4EU MUST establish and consider adoption factors of the users and the market. This MUST be done throughout the development process.
R-E-06	**Use of existing validated credentials** End-Users may have numerous validated credentials. Enabling them to use those existing credentials closes barriers to adoption. Hence, mGov4EU MUST support the use of existing credentials.
R-E-07	**Support of a variety of credentials** Given that there are a wide range of different ID credentials provided to End-Users that have various attributes included. The support of a variety of credentials gives users the freedom to choose what credential to use in different circumstances. This would lower barriers for adoption. Therefore, mGov4EU SHOULD support a wide range of credentials.
R-E-08	**Added value for all relevant stakeholders** In order for the relevant stakeholders to use mGov4EU, they MUST be offered added value. Examples of added value could be the following characteristics: added value, increased usability, security or privacy benefits, greater convenience, financial benefits.
R-E-09	**Use case agnostic solution**

Name	Requirement
	A mGov4EU solution MUST be applicable across different relevant use cases. Then it enables the use by a variety of different organizations from different industries and administrations. Only then will adoption become attractive for enough end users and service providers to benefit from network effects. Furthermore, it supports the development of cross-industry cooperation models that can offer a comprehensive range of solutions.
R-E-10	**Support of different deployment models** Different stakeholders and different scenarios require different deployment models. There is no single deployment mode that is suitable for all use cases. Therefore, mGov4EU solution MUST support different deployment models.
R-E-11	**Interoperability** Different scenarios, use cases, and business contexts are characterized by different services and authentication methods. Therefore, a variety of services and authentication methods MUST be supported.
R-E-12	**Mobile-support** The use of mobile devices is essential for both the end user and the professional context. Therefore, mGov4EU MUST support authentication by mobile devices.
R-E-13	**Platform-independence** A wide variety of platforms are used in both the consumer and business environment. In order to maximize the potential user base, mGov4EU SHOULD be designed to be deployed regardless of the platforms used by end user, service providers, etc.
R-E-14	**Support of authentication with notified eIDs** In many eGovernment use cases, users and service providers have an interest in using notified eIDs for the authentication and identification of users. Therefore, mGov4EU Solution MUST support appropriate authentication and identification that enables service providers to obtain the personal information necessary for their use case.
R-E-15	**Easy and affordable implementation for service providers** The financial resources of service providers to implement new software components are a scarce commodity. This means that a mGov4EU solution SHOULD optimize usability and implementation costs for the service providers.
R-E-16	**Low to no costs for end users** Empirical studies show that the willingness of end users to pay for identity management systems is very low or non-existent. Therefore, having little to no charges for end users could be considered as an advantage. Therefore, mGov4EU solution SHOULD have little or no cost to end users.
R-E-17	**Possibility for personalization** Service providers (for the development and provision of personalized products and services), as well as users (comfort function, suitable products) want a possibility

Name	Requirement
	for personalization for numerous use cases. mGov4EUs solution SHOULD provide the possibility for personalization.

Table 8: Economic Requirements (E)

2.4 Usability Requirements

Usability is the extent, to which a product can be used by specific users in a specific context of use, to reach specific goals effectively, efficiently, and satisfyingly. Usability is a key indicator of product quality and in the design process it plays an important role in ensuring that a product is easy and pleasant to use.

The ISO 9241-11 specifies usability core requirements to meet the usability definition. Usability core requirements are effectiveness, efficiency, and the users' satisfaction [25] .

To refine those Core Requirements the ISO 9241-110 defines seven aspects of these general ergonomic principles: suitability for the task, suitability for learning, suitability for individualization, conformity with user expectations, self-descriptiveness, controllability and error tolerance [25].

Based on the usability definition, Nielsen (2012) defines five quality components of usability [26]:

1. Learnability: The ease of performing basic tasks for the first time
2. Efficiency: The speed of performing tasks once a user has experience using the system
3. Memorability: The ability to remember the interface's components
4. Errors: The regularity and severity of, and recovery from, error
5. Satisfaction: The overall pleasantness of the product

The claim of today's product design is not just to have a usable ser Interface, but also that users are having a positive experience with the product. User Experience (UX) as described by Hassenzahl (2008) is a momentary, evaluative feeling (positive or negative) when using technical products and services [27]. A positive UX occurs by satisfying basic human needs. These needs are self-esteem, competence, competition, physicalness, security, stimulation, relatedness and popularity. Designing a good user experience is important as it engages and delights the user and builds trust.

One of the mGov4EU project's goals is to provide a usable and well-designed client interface; therefore, guidelines for Trust and Knowledge based on the common Usability principles and requirements have to be considered. Crucial guidelines, considered in the Usability Requirements are:

1. Usability Requirements for Security Tools [28]
2. Freiburg Usability guidelines [29]
3. Guidelines for Secure Interaction Design [30]
4. Principles and Patterns to Align Usability and Security [31]
5. Idea for Heuristic Evaluation for IT Security Management Tools [32]

The complete list of Usability Requirements can be found in Table 9.

Name	Requirement
R-U-01	**High usability**

Name	Requirement
	Usability and understanding of services and applications MUST be a main benefit to the end-users. Given that end-users may have a wide range of competence with this technology, it is important to make it as simple and usable as possible.
R-U-02	**Established usability guidelines and principles** The User Interface MUST consider established Usability Guidelines and Principles to assure an easy-to-use product and overall Usability.
R-U-03	**Learnability** Learnability is an important Usability Design Principle. In this case even more important because most users have little knowledge of the topic. So first of all, they have to learn how the system works. Learnability MUST be considered in the UI.
R-U-04	**Commonality of language** Ensure that global language requirements are considered, including languages that use special characters. In mGov4EU, tools MUST have a commonality of language.
R-U-05	**User readable terminology** All terminology (Labels, Buttons, Messages etc.) MUST be understandable for users with little technical understanding, users new to the software and the subject. Example: Instead of encrypted email – „Secret message for...“or „email only readable for…“
R-U-06	**Team to answer queries** There SHOULD be a team available to answer questions and queries from end-users as and when they arise.
R-U-07	**User experience** Building on Usability, the mGov4EU Project SHOULD consider User Experience to guarantee good user acceptance. Especially the basic human needs security and competence are important factors in designing a security system. Ideally the System can address those needs to create a good User Experience.
R-U-08	**Adaptive user interface** The User Interface for the mGov4EU project MUST be adaptive, so the content shows well on small screens as well on large ones.
R-U-09	**Easy to grasp metaphors** Often security software uses metaphors which are not easy to understand or are even misunderstood (for example the metaphor for public and private key). Easier to understand and grasp metaphors would help the users to understand the whole concept of the topic on a high Level. There SHOULD be easy to grasp metaphors for users to understand.
R-U-10	**Transparency** There is no need for the user to understand to whole system and every little detail that happens in the background. But the system UI MUST be transparent

Name	Requirement
	enough so the user can understand the overall concept and therefore understand what is happening and what he/she is supposed to do. At any given point the system should be transparent enough whilst not overstraining the user.
R-U-11	**Minimalistic/ simple user interface design** It is found that with security sensible transactions users prefer a simple and minimalistic User Interface, so that they can focus on important stuff and realize what is happening. So, every clutter or non-relevant information MUST be excluded from the UI.
R-U-12	**Empowered users** Users MUST always feel in control of the things are happening in the UI.
R-U-13	**Error handling** In all predictable cases the system MUST hinder the user to make mistakes. But the system should not just block an operation. Instead, it should explain to the user why this operation is not available at the moment. Same with mistakes. If there is an error, or the user makes a mistake the system MUST provide clear and understandable cause, also giving the user clear instruction on how to fix it.
R-U-14	**Cognitive load** Cognitive load MUST be minimized as much as possible. Security is a secondary task for the user. If the user has to remember too much or has to execute too many tasks, the user won't return to the system. There should be as little to remember as possible and as little to execute to achieve the desired goal.
R-U-15	**Accessibility (1) – Alignment to authoritative norms** The tools and solutions created in mGov4EU MUST support accessibility in accordance with current standards and frameworks, such as the Accessibility Directive 2019/882, the Web Content Accessibility Guidelines (WCAG) [33], the Authoring Tool Accessibility Guidelines (ATAG) [34] and the User Agent Accessibility Guidelines (UAAG) [35]. They should be the foundation for accessibility service guidelines and can serve in the development of accessible websites/applications. For example, in explaining how to make web content accessible for people with disabilities and address text, images, forms, sounds and videos, as well as other content of a website or web application.
R-U-16	**Accessibility (2) – Digital Inclusion** mGov4EU solutions MUST be as barrier-free as possible in regards to providing digital accessibility to all eligible user groups and communities. There MUST be support for all applicable types of users in various situations, including those with disabilities or impairments. There must be no exclusion of a specific user group, in order to maximize the user base.
R-U-17	**User Centricity** User Centricity SHOULD place effort in putting the user of the product at the center of product development. The needs and requirements of the user SHOULD be identified, and guide the design and development of any website or application.

Name	Requirement
	The following expectations SHOULD be taken into account[3]: a multi-channel service delivery approach, a single point of contact should be made available to users, and user feedback should be collected and evaluated to improve existing websites or applications.
R-U-18	**User Acceptance** The website/applications SHOULD be designed to meet the requirements of the users. The user decides whether the website/applications meets their requirements or not. An example would be a User Acceptance Testing (UAT)[4] which focused on user testing and not the developer. By testing the accessibility, the product quality can be checked and adjusted if necessary.
R-U-19	**Co-creation** The project SHOULD involve methods and practices of co-creation [36] through out the duration of the project. This implies that the creation of the solutions of mGov4EU should involve the insights and expectations of stakeholders, especially end-users.

Table 9: Usability Requirements (U)

2.5 Legal Requirements

This subsection sets out the legal requirements to be fulfilled in the context of mGov4EU. It is closely related to T5.4 led by partner TLX, which aims at assessing the legal landscape and regulations relevant for mGov4EU. All legal requirements are listed in Table 10 where each of them is dedicated to a specific category.

2.5.1 Privacy and Data Protection Requirements

As the mGov4EU project deals with data from base registries and data around eID, a thorough monitoring of the data protection requirements and privacy requirements is key. The underlying legal framework for these requirements is on the European level based on the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) and probably complemented by some national regulations.

The main aspects that have to be covered are consent and data minimisation of information that are provided by the data subject. For the expected consent the requirements of Art. 6 pp GDPR must be taken into account in a way that consent should be given explicitly for all requested data and that the data subject's consent, if it is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. To respect the principle of data minimisation, the data provided have to be limited to what is necessary in relation to the purposes for which they are processed, adequate and relevant (Art. 5 GDPR). Further data protection and privacy requirements may appear during the more detailed design of the pilot use case and will be described then and / or in the respective deliverable(s).

[3] See https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/glossary/term/user-centricity .

[4] See https://www.userback.io/blog/user-acceptance-testing-explained .

Name	Requirement
R-L-01	**Legal basis (Article 6.1 GDPR)** Any processing of personal data MUST have a legal basis recognised under the GDPR. If personal data is to be processed by a public sector body, the legal basis SHOULD NOT be consent, unless the user has a clear alternative.
R-L-02	**Transparency (Article 13-14 GDPR)** Any processing of personal data MUST be clearly disclosed to the user in accordance with the requirements of the GDPR. This applies both to the storage of personal data on a mobile device, and the processing of personal data in the context of the pilots.
R-L-03	**Data minimisation (Article 5.1 (c) GDPR)** If personal data is shared with a service provider in the context of the pilots, the data sharing MUST be limited to what is strictly necessary for piloting purposes. Personal data storage on the user's device SHOULD be limited to what is reasonably useful for the purposes of mGov4EU.
R-L-04	**Purpose limitation (Article 5.1 (b) GDPR)** If personal data is shared with a service provider in the context of the pilots, the service provider MUST only use the data for piloting purposes. Personal data storage on the user's device MUST NOT be usable by third party applications without the user's consent.
R-L-05	**Accuracy (Article 5.1 (d) GDPR)** Personal data stored on the user's device MUST be correctable, deletable or replaceable by the user.
R-L-06	**Accountability – project contacts (Article 13.1 (a) GDPR)** Users MUST be able to find contact information on the application on their mobile device, leading to a contact person of the mGov4EU project who can provide them with relevant information on data protection aspects of the project.
R-L-07	**Accountability – pilot contacts (Article 13.1 (a) GDPR)** Users MUST be able to find contact information for any pilot services that they use, leading to a contact person of the pilot service provider who can provide them with relevant information on data protection aspects of the pilot.
R-L-08	**Accountability – pilot monitoring (Article 5.2 GDPR)** Whenever mGov4EU is used in a pilot, the outcomes MUST be logged and monitored, at a minimum by the pilot service provider, in order to proactively detect any problems that may occur, and to avoid any adverse effects related to the problems on the user.
R-L-09	**Storage limitation (Article 5.1 (e) GDPR)** Personal data stored on the user's device MUST be automatically deleted at the end of the mGov4EU project, unless the user explicitly chooses otherwise.
R-L-10	**Integrity and authenticity (Article 5.1 (f) GDPR)**

Name	Requirement
	The integrity and authenticity of any personal data sent from the user's device using mGov4EU results MUST be verifiable by the intended recipient.
R-L-11	**Confidentiality - device (Article 5.1 (f) and 24.1 GDPR)** Personal data stored on the user's device MUST be protected with appropriate access controls or effective encryption in order to protect the data against unlawful access if the device is lost.
R-L-12	**Confidentiality - transfer (Article 5.1 (f) and 24.1 GDPR)** Any personal data sent from the user's device using mGov4EU results MUST be protected against unlawful interception through effective encryption.
R-L-13	**DPO involvement (Article 37.1 GDPR)** Any personal data processing in the context of pilots MUST be supervised by a duly qualified data protection officer (DPO) meeting the requirements of the GDPR. The contact information of the DPO MUST be made available to the user of any pilots.
R-L-14	**DPIA (Article 35.1 GDPR)** Any personal data processing in the context of pilots MUST be preceded by a data protection impact assessment (DPIA) created in the context of mGov4EU project. Any piloting constraints (other than those referenced in this deliverable) must be disclosed in the DPIA and adhered to.
R-L-15	**Third country transfers (Article 44 GDPR)** Any personal data sent from the user's device to a third country using mGov4EU results MUST satisfy the transfer requirements from the GDPR. Given the piloting objectives, an explicit consent MAY be used as the legal basis for third country transfers.
R-L-16	**Special categories of data and vulnerable persons (Article 8-9 GDPR)** Personal data processing in the context of pilots MUST NOT relate to minors, or to persons who are legally impaired, nor may it comprise special categories of data (notably data concerning health).
R-L-17	**Confidentiality – Pseudonymity - eVoting (Article 5.1 (b) GDPR)** Personal data processing in the context of the eVoting pilots MUST support the possibility of pseudonymous voting in a manner that prevents the vote recipient from discovering the identity of the user without collusion with a third party.

Table 10: Legal Requirements - Data Protection (L)

2.5.2 eIDAS Requirements

For the mGov4EU project it is foreseen to use eIDAS solutions and to be compliant with the eIDAS requirements. Therefore, the solutions developed and provided by the project have to fulfil the technical, architectural and legal obligations that derive from the requirements of the relying parties (e.g. organisations and citizens). To ensure the interoperability with and for eIDAS and to provide accountability and liability the requirements of the framework for cross-border interoperability must provide:

- confidentiality of the person identification data;
- authenticity/integrity of the person identification data;
- secure identification/authentication of communication end-points.

Based on the usage of eIDAS it can be assumed that the systems in use (e.g. national systems) provide adequate measures to provide confidentiality, authenticity, integrity and communication end-point identification and therefore no further requirements have to be fulfilled.

As it was already described with further details in deliverable D1.1, the eIDAS Regulation is in the revision process and the project has to monitor the process, if any of the possible changes on the legal basis has an impact to the mGov4EU project.

Name	Requirement
R-L-18	**Identity / pseudonymity (Article 5.2 eIDAS Regulation)** The solutions designed by mGov4EU MUST permit the use of pseudonymous credentials, i.e. credentials that do not allow the recipient to discover the identity of the user without collusion with a third party.
R-L-19	**Identity / linkability (Article 7 (d) eIDAS Regulation)** The solutions designed by mGov4EU MUST permit pseudonymous credentials to be linkable to a uniquely identifiable person.
R-L-20	**Identity / notified identities (Article 7 eIDAS Regulation)** The solutions designed by mGov4EU MUST allow the use of electronic identities that can be linked to eIDAS notified identities. It MUST be possible to determine what the eIDAS notified identity is and what its level of assurance is.
R-L-21	**Integrity and authenticity of assertions (Article 35 eIDAS Regulation)** The solutions designed by mGov4EU MUST allow integrity and authenticity of any attribute assertions or other documents exchanged using mGov4EU results to be validated. This functionality MAY be created using electronic seals as defined by the eIDAS Regulation.
R-L-22	**Qualified trust services (Article 20 eIDAS Regulation)** The solutions designed by mGov4EU MUST conceptually be able to support the use of qualified trust services, notably qualified electronic signatures (including for mobile signature piloting) and qualified seals (for signed assertions). Qualified trust services MAY be piloted in practice in mGovEU, but this is not strictly required.
R-L-23	**Signature and LoA requirements (Article 8 and 25 eIDAS Regulation)** Prior to initiating any piloting activities that require electronic signatures or electronic identification, it MUST be determined whether the pilot requires eIDAS compliant identities (and if so, what the applicable level of assurance is), and whether it requires electronic signatures (and if so, whether these should be basic, advanced or qualified signatures as defined in the eIDAS Regulation).

Table 11: Legal Requirements - eIDAS Regulation (L)

2.5.3 SDGR Requirements

The entry into force of the Single Digital Gateway Regulation (SDGR) on the 12th of December 2018 can be seen as a game changing event. It is the first pan-European, horizontal and cross-domain

act of legislation, that provides a basis for the EEA-wide implementation of the 'once-only' principle (OOP). The OOP is one of the key principles the mGov4EU project relies on.

Article 14 SDGR is the basis for the creation of a once-only technical system, which will enable the exchange of evidence across borders for 21 key online procedures, further described in Annex II of the SDGR. Besides that, a specific CEF Digital Preparatory Action for the once-only principle was established to support the Member States and associated countries of the EU in, drafting of the technical specifications of the future OOP technical system, raising awareness and building national capacity, and to develop on the basis of existing CEF (technical) Building Blocks and the outcomes of projects like The Once-Only Principle project (TOOP) the elements of the Single Digital Gateway.

The architecture foreseen is heavily based on reuse of existing CEF Building Blocks, in particular, e-Delivery and eID and includes architectural enhancements proposed in the TOOP project, other EC services/systems and ISA² specifications. Further details and technical specifications, e.g. the need of a preview for the data provided, will be provided by the implementing act that is based on Art. 14 SDGR and is expected by the 12th of June 2021. The mGov4EU project will closely monitor the developments around the setup of the implementing act in 2021 and the announced update for 2022.

Name	Requirement
R-L-24	**Prior request (Article 14.3, 14.4 and 14.7 SDGR)** The user's explicit request MUST be obtained via their mobile device before transferring any evidences from their device to a competent authority when piloting a procedure that falls within the scope of the SDGR. The user MUST be informed that they can abort the process and attempt to complete the procedure without mGov4EU.
R-L-25	**Preview (Article 14.3 and 14.5 SDGR)** The user MUST have the ability to preview and select any evidences via their procedure device before transferring them from their device to a competent authority when piloting a service that falls within the scope of the SDGR. The user MUST be informed of this possibility prior to initiating the transfer.
R-L-26	**Competent authorities – evidence requesters (Article 14.3 SDGR and Article 13 Implementing Act)** The solutions designed by mGov4EU MUST verify whether the recipient of evidences is indeed a competent authority when piloting a procedure that falls within the scope of the SDGR. The user MUST be informed of the identity of the competent authority prior to initiating the transfer.
R-L-27	**Logging (Article 14.3 SDGR and Article 18 Implementing Act)** The solutions designed by mGov4EU MUST enable logging in accordance with the requirements of the SDGR when piloting a procedure that falls within the scope of the SDGR.
R-L-28	**Competent authorities – evidence providers (Article 14.3 SDGR and Article 13 Implementing Act)** The solutions designed by mGov4EU MUST allow evidences made available via the user's mobile device to be linked to competent evidence providers. The evidence providers must be identifiable as competent to the evidence requester.
R-L-29	**Competent authorities – identification (Article 3 Implementing Act)**

Name	Requirement
	Identification processes when piloting a procedure that falls within the scope of the SDGR MUST use electronic identities that can be linked to eIDAS notified identities. It MUST be possible to determine what the eIDAS notified identity is and what its level of assurance is.

Table 12: Legal Requirements - SDG Regulation (L)

2.6 Security and Accountability Requirements

As mGov4EU solutions will potentially process security-sensitive data, security and accountability are key aspects to be considered from the beginning. Accordingly, this section defines relevant requirements related to security and accountability in the following subsections.

2.6.1 Security Requirements

This section defines security requirements to be met by solutions developed by mGov4EU. Security requirements defined in this section remain on a rather generic level. This is necessary, as more detailed security requirements can be defined only once the technical architecture has been defined in WP2 and concrete pilot plans have been made in WP4. The relations between this deliverable and the security requirements defined therein, and other deliverables is illustrated in Figure 1.

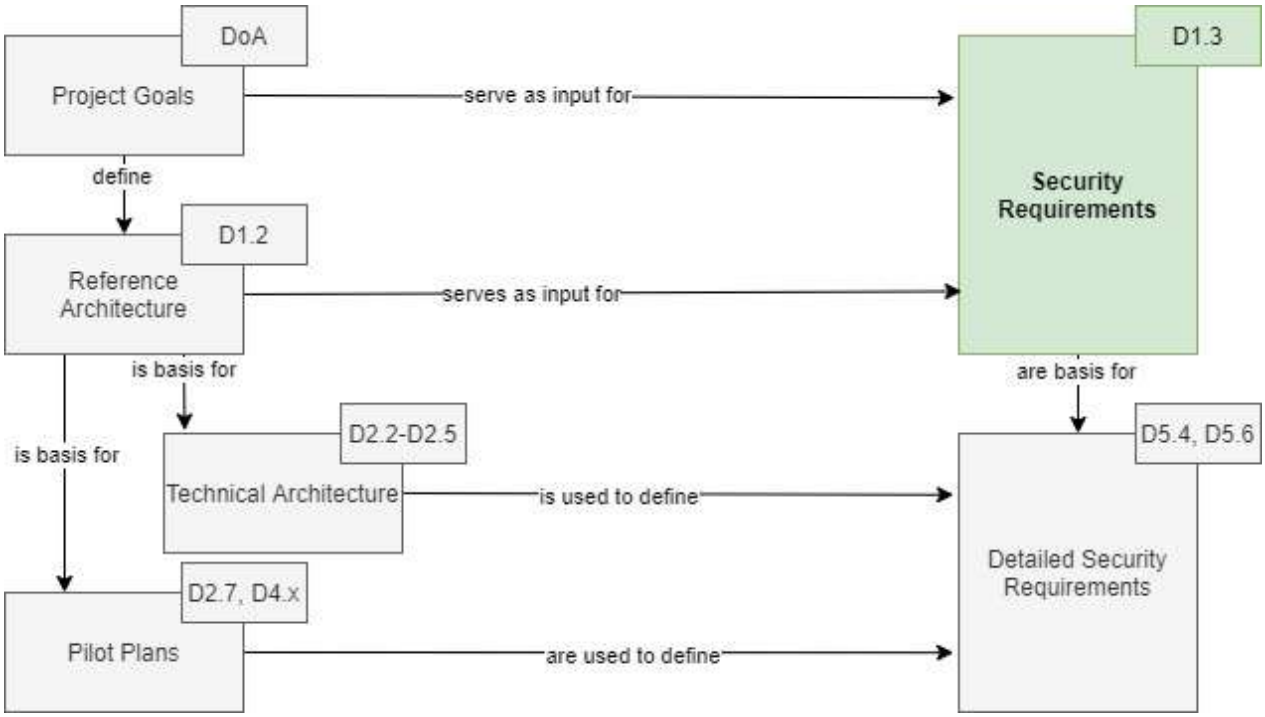

Figure 1: Scope of security requirements defined in this deliverable

As shown in Figure 1, the mGov4EU DoA and the reference architecture defined in D1.2 serve as basis and input for the security requirements defined in this section. The security requirements themselves are the basis for detailed security requirements, which can be specified once the mGov4EU technical architecture elaborated in WP2 and the pilot plans elaborated in WP4 are available. Detailed security requirements will be described in the security evaluation related Deliverables D5.4 and D5.6, respectively.

In the remainder of this section, the security requirements relevant for mGov4EU are defined. Two kinds of requirements are defined. First, abstract security requirements are derived from relevant security targets. Second, additional requirements are defined to specify steps to be taken in order to derive detailed security requirements once required WP2 and WP4 results are available.

2.6.1.1 Abstract Security Requirements for mGov4EU Solutions

Abstract security requirements are derived from relevant security targets. It is common practice to rely on the so-called C-I-A criteria when identifying relevant security targets for IT solutions. The C-I-A criteria cover the security targets confidentiality (C), integrity (I), and availability (A). In some cases, this basic set of security targets is extended by additional aspects such as authenticity, compliance, accountability, or non-repudiation.

The technical solutions to be designed, developed, and operated in mGov4EU are not special in a sense that they show the need to consider special security targets. Given the already rather abstract nature of (extended) C-I-A criteria, it is hence reasonable to use these criteria as a starting point for the identification of relevant security targets. Taking into account already known peculiarities of the envisioned mGov4EU solutions, we use the following extended C-I-A criteria as relevant security targets: confidentiality, integrity, availability, authenticity, non-repudiation.

We assume that the aspect "compliance", which is also commonly used as security target, is covered sufficiently by the legal requirements defined above in this deliverable. The aspect "accountability", which is for sure relevant for mGov4EU, is covered by the requirements defined in Section 2.6.2, and hence not included here.

Based on the above-defined set of relevant security targets, the following abstract security requirements can be derived for mGov4EU solutions:

Name	Requirement
R-AS-01	**Confidentiality of assets** mGov4EU solutions MUST be designed, implemented, and operated such that the **confidentiality** of assets is protected by technical or organizational measures where needed. Unauthorized entities like external attackers MUST NOT have read access to confidential data stored, processed, or transmitted by mGov4EU solutions and its technical components.
R-AS-02	**Integrity of assets** mGov4EU solutions MUST be designed, implemented, and operated such that the **integrity** of assets is protected by technical or organizational measures where needed. Unauthorized entities like external attackers MUST NOT have write access to data stored, processed, or transmitted by mGov4EU solutions and its technical components. Accordingly, either unauthorized entities MUST NOT be able to alter data at all, or such unauthorized modifications must be reliably detectable.
R-AS-03	**Availability of assets** mGov4EU solutions MUST be designed, implemented, and operated such that the **availability** of assets is protected by technical or organizational measures where needed. Malicious entities like external attackers MUST NOT be able to compromise the availability of assets and of technical components that process, store, or transmit these assets.
R-AS-04	**Authenticity of assets** mGov4EU solutions MUST be designed, implemented, and operated such that the **authenticity** of assets is ensured by technical or organizational measures where needed[5]. Recipients of assets MUST be able to reliably verify the origin of the

[5] Note that this abstract security requirement covers both message authentication and entity authentication. When deriving detailed security requirements from this abstract requirement, these two concepts should be further distinguished.

Name	Requirement
	asset, i.e., the identity of the sender. Ensuring the authenticity of an asset implicitly also MUST ensure this asset's integrity. Malicious entities like external attackers MUST NOT be able to verifiably claim origin of an asset originating from another legitimate entity. Furthermore, malicious entities MUST NOT be able to impersonate legitimate entities and send assets on behalf of them.
R-AS-05	**Non-repudiation of assets** mGov4EU solutions MUST be designed, implemented, and operated such that **non-repudiation** of assets is ensured by technical or organizational measures where needed. Entities MUST NOT be able to deny being the origin of an asset. This requirement is closely related to R-ASR-04 on authenticity of assets.

Table 13: Abstract Security Requirements (AS)

2.6.1.2 Requirements for the Derivation of Detailed Security Requirements

Once the concrete mGov4EU technical architectures and pilot plans are available, the abstract security requirements defined above will be used as basis to derive more detailed security requirements. This will be accomplished during the planned security-evaluation activities in WP5. The additional requirements defined below (Table 14) ensure that that the derivation of detailed security requirements will be based on a thorough methodology.

Name	Requirement
R-DDS-01	**Identification of assets** Once the mGov4EU technical architectures and pilot plans are available, relevant **assets** that need to be protected MUST be identified. This includes primary assets (user data, etc.) as well as secondary assets, whose security directly influences the security of primary assets. Dependencies between primary and secondary assets must be modelled accordingly.
R-DDS-02	**Mapping of assets to security targets** For all identified primary assets, the **relevance of the abstract security requirements** MUST be determined. This way, the relevance of the various security targets becomes apparent for all primary assets. The relevance of the security targets and the associated abstract security requirements for secondary assets MUST be derived by employing the defined dependencies between primary and secondary assets.
R-DDS-03	**Identification of threats** Taking into account the relevant security targets, **threats** MUST be identified for all assets. Identified threats MUST be quantified by means of a suitable **risk matrix**, through which risks can be assigned a likelihood and a damage potential.
R-DDS-04	**Derivation of countermeasures** For all threats, appropriate **technical and/or organizational countermeasures** MUST be defined. From the set of necessary countermeasures, detailed security requirements MUST be derived that, then, need to be considered during design, implementation and operation of mGov4EU solutions.

Table 14: Requirements for the Derivation of Detailed Security Requirements (DDS)

2.6.2 Accountability Requirements

In addition to the security requirements defined above, the accountability-related requirements described below also need to be considered.

Name	Requirement
R-ACC-01	**Limitation of impacts on pilot participants** Taking into account the project's piloting activities, piloting partners MUST adopt appropriate technical, legal or organisational measures to ensure that any problems during piloting can be proactively detected and addressed, thus avoiding that errors in project execution can have a real life detrimental impact on pilot participants.
R-ACC-02	**Allocation of and agreement on responsibilities among pilot participants** Prior to initiating any piloting activities, responsibilities SHOULD be explicitly allocated and agreed between pilot participants, thus ensuring that all piloting partners are fully aware of the risks they are expected to mitigate.

Table 15: Accountability Requirements (ACC)

Chapter 3 Overview of mGov4EU Pilot Use Cases

The present chapter outlines the piloting methodology in Section 3.1 and provides an overview of the envisioned pilot use cases in Section 3.2.

3.1 Piloting Methodology

Piloting is one of the key elements of each project. As mGov4EU is a complex project that deals with different piloting areas and further influencing factors have to be taken into account, a methodology is need that provides the necessary flexibility. The mGov4EU project has agreed to use an agile methodology as basis for its piloting approach. Within this section the aspects of the approach will be described. Besides that, the details of different pilot use cases, also referred to as pilots or use cases, are provided in the following sub-sections.

3.1.1 Piloting Approach

The motivation of this decision is based on the complexity of the project and the technical, legal and organisational framework. The agile approach ensures on the one side the necessary flexibility to react to the needs of the pilots and on the other side it provides the rigidity that is required for a project with the intricacy of mGov4EU. The mGov4EU project reuses existing building blocks, developed by previous projects and provided by the EC (Connecting Europe Facility / CEF) and follows the approaches of former large-scale pilots like e-SENS[6] and TOOP[7]. The mGov4EU piloting approach is based on the methodology developed by these projects and customised for the needs of mGov4EU, especially in size and scope.

From a high-level point of view, the different steps of the agile methodology can be described as follows:

- Modelling roles
- Mapping roles to information systems, registries and databases
- Defining Types of Data Objects
- Mapping between information systems (e.g. registries and databases & types of data objects)
- Defining requirements for the Building Blocks to be used
- Managing tasks against the defined goals

To prepare the selection of pilots and the first steps of the piloting lifecycle, a template to be filled by the piloting partners was prepared (see Annex – Use Case template). The template consists of different sections, first there is a high-level description of the use case's scenario overview, its relevance, and goals, continuing in sub-section 1.1. Sub-section 1.2 describes the architecture and the use of building blocks that are to be constructed. Next, there will be a process description, which includes the main actors and roles included in the use case, the flow of events, and other conditions and assumptions needed for the use case in sub-section 1.3. Last, section 1.4 describes the anticipated implementation and impact the use case will have.

Piloting is key for mGov4EU. It is the technical, organisational and legal demonstration of feasibility. Therefore, the project has adopted a holistic approach, taking into account the entire lifetime of a pilot from its very beginning until its final conclusion and beyond. The approach to cover the whole lifecycle is based on the evolution of a pilot over time and identifies the main phases a pilot has to go through in its lifetime in order to reach a successful conclusion and handover.

The different stages of the mGov4EU pilot lifecycle are summarised in Figure 2.

[6] e-SENS Deliverable D5.2 Pilot Lifecycle Management Methodology and Workflow Support Tools

[7] TOOP Wiki: http://wiki.ds.unipi.gr/display/TOOPPILOTS

Figure 2: Stages of Pilot Lifecycle

The pilot starts with the **Recruitment** phase. Pilot intentions of the partners are identified, and proposals are made for specific business processes that bring value to cross-border interactions. Specific services or entire domains may be engaged based on a recruitment that intensifies during this first phase. This is the stage in the pilot lifecycle where the initial identification of prospects seems promising and where the value proposition must be adequately articulated.

The leading use cases that are positively qualified as showing promising value for the mGov4EU project and appear feasible enter into the **Commitment** phase. This phase also contains the detailed design of the usage scenarios to be piloted. Additionally, this is where an agreement is sought, and foreseen to be established, between the project and the pilot proposers, on both sides by competent bodies. Commitment is mutual and if common understanding and agreement is reached the actual piloting can begin.

As part of the **Implementation** phase, activities are undertaken to set up the pilot infrastructure. Besides that the pilot participants will be enabled to use the established infrastructure. Enablement of participants is manifold and includes a technical, business and organizational dimension. The Implementation phase is conducted in multiple agile iterations and includes readiness and conformance testing within each of the piloting partners as well as interoperability testing across the piloting countries.

The **Running** phase is where the infrastructure works for the first time, participants are connected and enabled from a technical, business and organizational point of view and real transactions start to take place. mGov4EU aims to extend into a stage where the pilot reaches sufficient maturity for the infrastructure that it could be used on a daily basis.

Within the final **Evaluation and Handover** phase the piloting partners will evaluate their pilots at national level according to the pilot evaluation methodology that will be defined by the project's Joint Piloting Task Force (JPTF). As part of these activities, they will identify and plan the post-pilot conditions for the sustainability of the respective pilots. The JPTF will coordinate the work of the piloting partners and monitor the pilot execution and the collection of pilot findings. JPTF will analyse and assess business level findings and they will evaluate the pilots at EU level according to the pilot evaluation methodology. The evaluation methodology will be defined by JPFT in collaboration with the related WPs. They will also provide the sustainability plans for all use cases and prepare the handover and adoption. WP 5 will be responsible for the pilot evaluation. JPTF will also coordinate the pilot sustainability assessment, documentation, evaluation and the handover of results to relevant stakeholders.

3.1.2 Joint Piloting Task Force

This section provides an overview of the JPTF. As described before, mGov4EU is a complex project. The responsibilities for the different aspects of the pilots are distributed across the different WPs. To bundle the resources and streamline the activities around the pilots the JPTF was established. This also helps to create synergies and increase the efficiency of the pilot related activities. The JPTF will bear the main responsibility for translating requirements to technology and align it with the needs of the different pilots. Furthermore, it ensures the coherence of the pilots with the sustainability and other requirements.

The JPTF consists of Piloting Task Leaders, Piloting Partners / Member States, the Scientific Leader and the Technical Leader. The JPTF is led by the Scientific Leader of the mGov4EU project. The responsibilities of the Piloting Task Leaders are to compile the pilot design documentation, the motivational scenarios for the pilots and mapping of goals against actors, roles, data objects etc. Furthermore, the JPTF develops the list of requirements for the different pilots based on the input from Piloting Partners / Member States.

The obligations of the Piloting Partners / Member States are to provide a detailed map of data and organizations that are involved within their countries. Besides that, they will define the tasks at a national level. Together, they are reliable for the horizontal task of the agile methodology, provision of formal models, follow-up with pilots for consistency, completeness, and iteration tracking.

3.2 Pilot-related Use Cases

This chapter provides an overview of the three most relevant use cases of mGov4EU, which are related to the pilots.

3.2.1 Online Voting Pilot

The Online Voting Pilot will be conducted in the University of Tartu, where one or more rounds of consultations will be done after integrating the Online Voting system with the mGov4EU framework. The pilot will enable students and/or university staff to authenticate to vote using their electronic national identifiers, as long as they are supported by mGov4EU.

Figure 3 provides an overview of the use cases of the eVoting pilot.

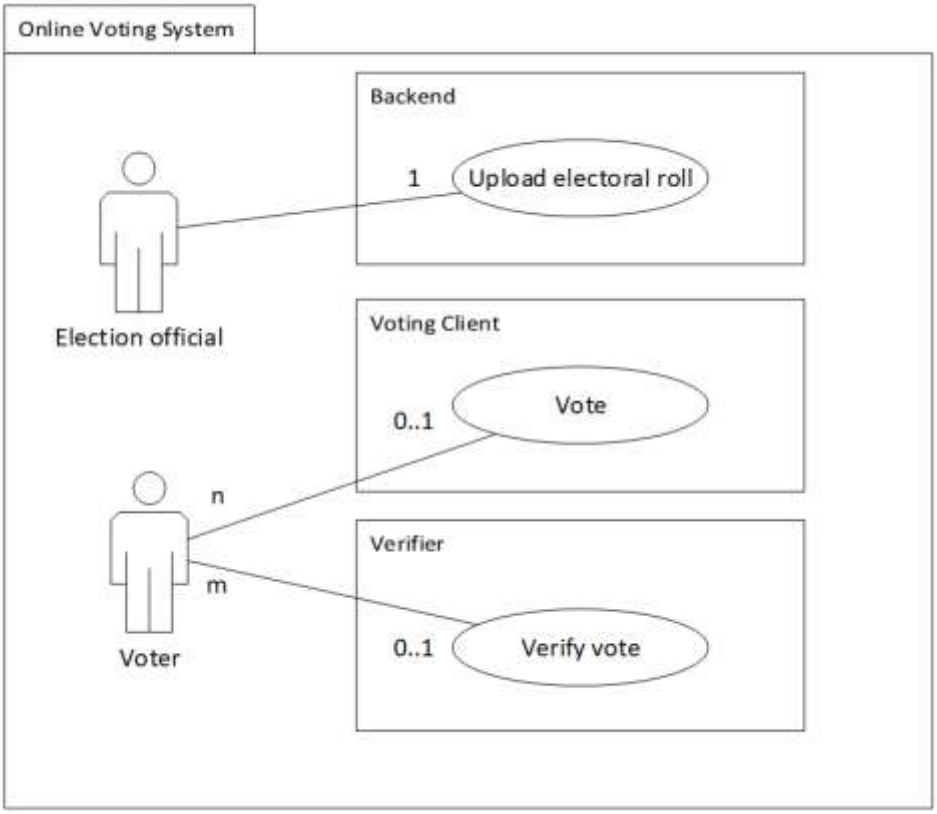

Figure 3: Use Cases for the eVoting pilot

Table 16 provides a short description for each use case of the eVoting pilot.

Name	Use Case
UC-VP-01	**Upload electoral roll** This use case allows an admin user to configure the list of eligible voters that will be allowed to vote on the election, with its eIDAS identification.
UC-VP-02	**Vote** This use case allows a voter user to authenticate to the voting platform through a mGov4EU eIDAS Authentication, and upload his encrypted voting options, signed with the voter's private signing key, if existing, to the election ballot box. Also lets the voter allow the system to collect its anonymous residence data for statistical purpose. This data is collected through the SDGR-related technical sub-system of mGov4EU.
UC-VP-03	**Verify vote** This use case allows a voter to authenticate to the voting platform through a mGov4EU eIDAS Authentication, and check that the voting options that he previously uploaded to the election ballot box are correctly stored.

Table 16: Use Cases within the eVoting pilot (UC-VP)

The following figure (Figure 4) explains the relationship between eVoting, eID and SDG, while Table 17 specifies the requirements related to the eVoting pilot.

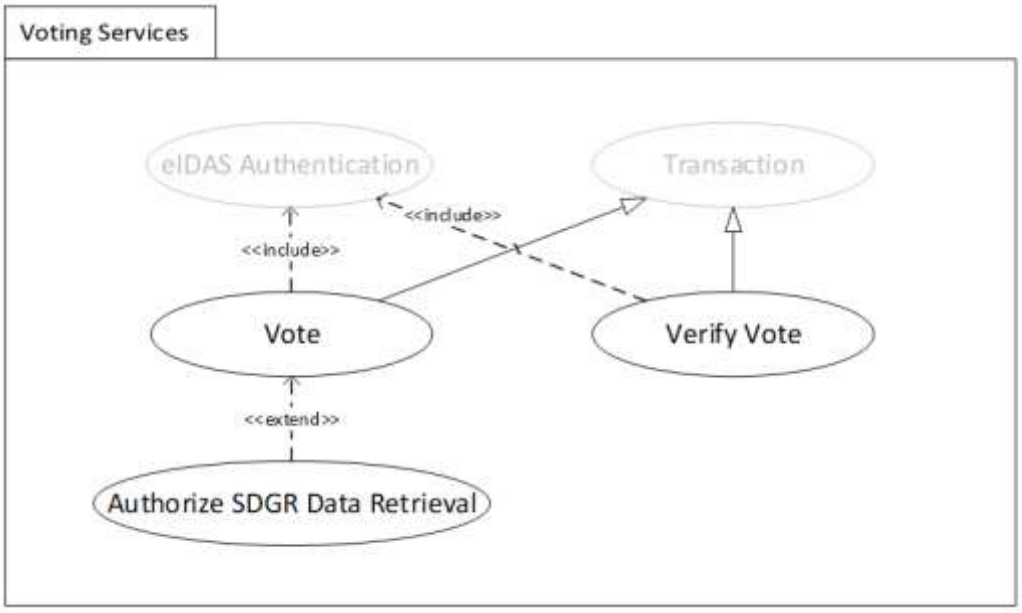

Figure 4: Relationship between eVoting, eID and SDG

Name	Requirement
R-VP-01	**Electoral roll upload** The election official MUST create and upload an electoral roll in the back-office (via backoffice administrator user). This is a list that includes eIDAS compliant identifiers of the voters which are authorized in the election.
R-VP-02	**Voter authentication with eIDAS identifier when voting** The voting client MUST allow the voters to authenticate using their eIDAS compliant electronic identifiers.
R-VP-03	**Vote signature with a dynamically generated key** The voting client MUST sign the vote cast with a key dynamically generated in the voting client and certified with a dynamic CA when the eIDAS identifier does not have the signing capability or it is not implemented.
R-VP-04	**Local vote signing** The voting client SHOULD sign the vote cast from the same device as the one used to generate and cast the vote. However, it MAY use the remote signing capabilities of certain eIDAS identifiers if they do not allow local signing.
R-VP-05	**Closing of session** The voting client MUST close the authenticated session after casting a vote and showing the voting receipt.
R-VP-06	**Voter authentication with eIDAS identifier when verifying vote** The verification solution MUST allow the voters to authenticate using their eIDAS compliant electronic identifiers.
R-VP-07	**Vote signature with the signing key of the identifier, if available** The voting client MAY sign the vote cast using an appropriate private signing key, if available.
R-VP-08	**Collection of residence address for statistics** Before casting a vote, the voter SHALL be requested to give permission to obtain a suitable part (e.g. postal code, NUTS code) of the residence address (SDG) for statistical purposes.

Table 17: Requirements for the eVoting Pilot (VP)

3.2.2 Smart Mobility Pilot

The Smart Mobility Pilot allows young adults to use subsidised taxi rides in rural regions. The main goal of this pilot is to demonstrate that the necessary registration can be realised with foreign eID means in a cross-border setting.

The use cases and system architecture for the Smart Mobility Pilot are depicted in Figure 5 and Table 18 respectively.

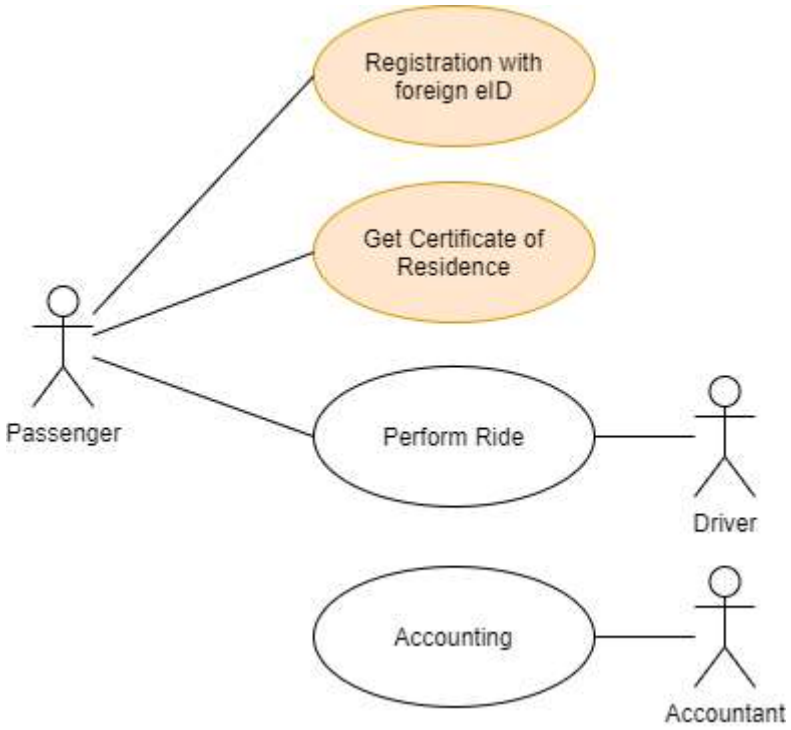

Figure 5: Use Cases for the Smart Mobility Pilot

Name	Use Case
UC-SM-01	**Registration with foreign eID** This use case allows to register for the Smart Mobility system using any supported eID. This use case covers two variants: (1) Registration with a mobile eID and (2) Registration with a conventional eID involving a desktop system and a suitable pairing between a desktop and mobile system.
UC-SM-02	**Get Certificate of Residence** This use case invokes suitable SDGR services in order to obtain a certificate of current residence. The input of this use case will be the minimum data set (Names, date of birth, unique identifier) gathered during the registration phase.

Table 18: Use Cases within the Smart Mobility pilot (UC-SM)

In addition to the two use cases, which are subject to developments within mGov4EU, there are two additional use cases within the Smart Mobility system such as “Perform Ride” and “Accounting”, which are only mentioned here for completeness.

The context of the different use cases and the embedding into the overall system architecture is outlined in Figure 6, while Table 19 specifies requirements related to the Smart Mobility Pilot.

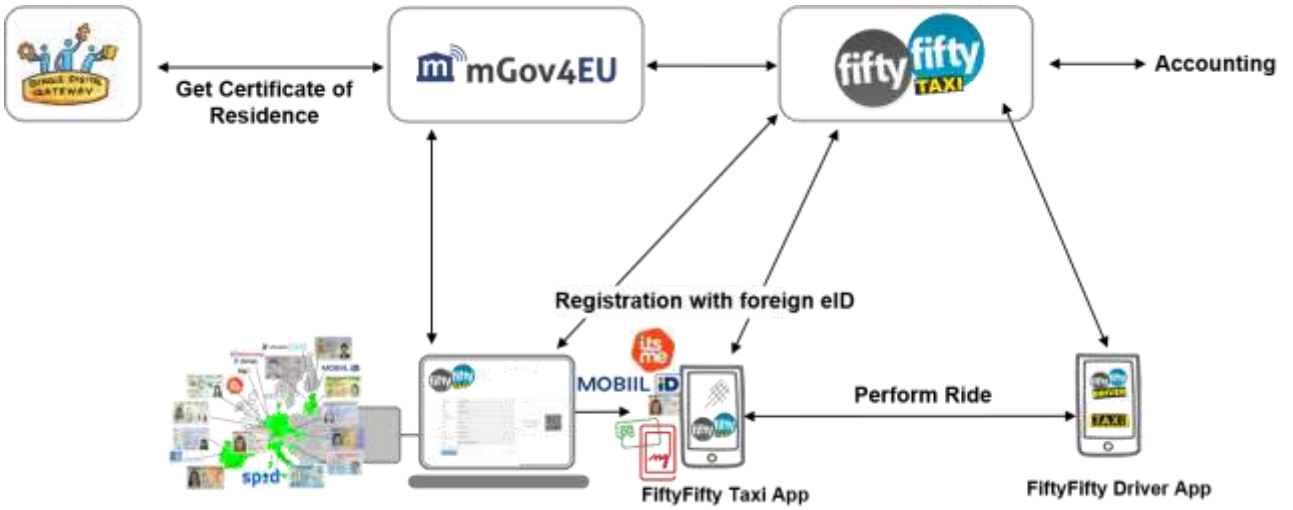

Figure 6: System Architecture for the Smart Mobility Pilot

Name	Requirements
R-SM-01	**Registration with mobile and conventional eID** The "Registration with foreign eID" use case SHALL support the registration with mobile eID and conventional eIDs.
R-SM-02	**Secure and convenient pairing between mobile and desktop system** In order to protect against Man-in-the-Middle attacks, the registration with a conventional eID SHALL provide a suitable pairing mechanism, which is both secure and convenient.
R-SM-03	**Domestic and cross-border Certificate of Residence** The procedure to retrieve a Certificate of Residence using SDGR-related mechanisms SHALL support the domestic retrieval as well as the cross-border retrieval.

Table 19: Requirements for the Smart Mobility pilot (SM)

3.2.3 Mobile Signature Pilot

The use cases for the Mobile Signature Pilot are depicted in Figure 7 and explained in Table 20.

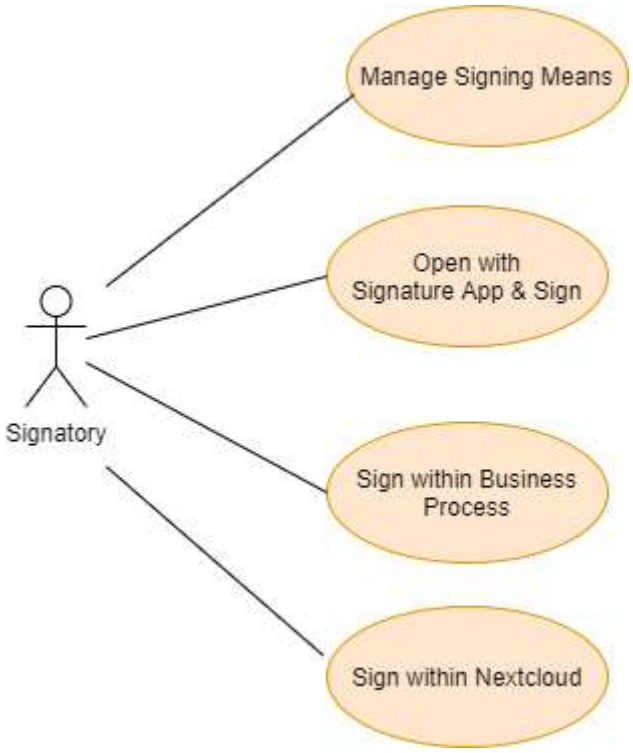

Figure 7: Use Cases for the Mobile Signature Pilot

Name	Use Case
UC-MS-01	**Manage Signing Means** This use case allows to manage the signing means, which will later on be used for signature generation.
UC-MS-02	**Open with Signature App & Sign** This use case allows to open a document which is already available on the smartphone and sign it within the signature app.
UC-MS-03	**Sign within Business Process** This use case allows to create a signature within some business process. For this purpose the document which is to be signed will be provided by some backend service, signed by the signatory and handed back to the business process.
UC-MS-04	**Sign within Nextcloud** This use case allows to create a signature for a document which is available in Nextcloud. This will involve adding a signing option to the Nextcloud context menu for handling files.

Table 20: Use Cases within the Mobile Signature pilot (UC-MS)

The following table specifies requirements related to the Mobile Signature pilot (Table 21).

Name	Requirements
R-MS-01	**Support for different signing means** The system for the Mobile Signing pilot SHALL support different signing means, which SHALL in particular include the supported mobile eID solutions.
R-MS-02	**Support of PAdES signatures** The Mobile Signature pilot SHALL at least support PAdES signatures according to EN 319 142 [37].
R-MS-03	**Support of other AdES signatures** The Mobile Signature pilot MAY support other AdES variants according to EN 319 122 (CAdES) [38], EN 319 122 (XAdES) [39] or TS 119 182 (JAdES) [40] for example.

Table 21: Requirements for the Mobile Signature pilot (MS)

3.3 Other Relevant Use Cases

Other use cases MAY be added during the course of the project.

Chapter 4 Summary and Conclusion

The present document has carved out and specified the main system requirements in various categories as required by the envisioned pilots, and has outlined the main use cases planned to be implemented within the pilots of the mGov4EU project.

The requirements analysis captured requirements in various categories, such as general system requirements, software requirements, economic and policy requirements, usability and accessibility requirements, legal requirements and last but not least security and accountability requirements.

The use cases and requirements for the pilots covered the eVoting pilot, the Smart Mobility pilot and the Mobile Signature pilot.

A preliminary version of this document provided input for the specification of the reference architecture in D1.2 and this document together with the reference architecture provides the starting point for the design phase in WP2, which in turn will form the basis for the implementation phase in WP3. The implemented components will be used within the pilots in WP4 and the requirements specified here will form the basis for the evaluation in WP5.

Chapter 5 Bibliography

[1] European Commission, Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[2] European Commission, Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending. 2018. [Online]. Available: http://data.europa.eu/eli/reg/2018/1724/oj

[3] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, IETF RFC 2119. 1997.

[4] European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity', SEC(2021) 228 final.

[5] 'LIGHTest', LIGHTest Project. https://www.lightest.eu/ (accessed Feb. 23, 2021).

[6] FutureID Project, 'Survey and Analysis of Existing eID and Credential Systems, Deliverable D32.1'. 2013. [Online]. Available: http://www.futureid.eu/data/deliverables/year1/Public/FutureID_D32.1_WP32_v1.0_Survey%20of%20existing%20eID%20and%20credential%20systems.pdf

[7] SkIDentity, 'Skidentity-Project Website', Skidentity-Project Website, 2014. http://www.skidentity.de/

[8] SSEDIC-Consortium, 'SSEDIC (Scoping the Single European Digital Identity Community) Project', 2013. http://www.eid-ssedic.eu/

[9] M. Kubach, H. Leitold, H. Roßnagel, C. H. Schunck, and M. Talamo, 'SSEDIC.2020 on Mobile eID', in Open Identity Summit 2015, Berlin, Germany, 2015, pp. 29–41.

[10] M. E. Porter, Competitive strategy. New York; London; Toronto: Free Press, 1998.

[11] Everett. M. Rogers, Diffusion of Innovations, 5th ed. New York: Free Press, 2003.

[12] O. E. Williamson, 'The Economics of Organization: The Transaction Cost Approach', American Journal of Sociology, vol. 87, no. 3, pp. 548–577, Nov. 1981.

[13] J.-J. Laffont and D. Martimort, The Theory of Incentives: The Principal-Agent Model. Princeton University Press, 2001.

[14] M. E. McCombs and D. Shaw, 'The Agenda-Setting Function of Mass Media', POQ, no. 36, pp. 176–187, 1972.

[15] A. K. Tjan, 'Finally a way to put your internet portfolio in order', Harvard Business Review, vol. 79(2), pp. 76–85, 2001.

[16] T.-P. Liang, C.-W. Huang, Y.-H. Yeh, and B. Lin, Adoption of mobile technology in business: a fit-viability model. 2007. [Online]. Available: http://www.ecrc.nsysu.edu.tw/liang/paper/1/Adoption%20of%20Mobile%20Commerce%20(IMDS%202007).pdf

[17] G. A. Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism', The Quarterly Journal of Economics, no. 84, p. 488, 1970.

[18] D. S. Evans, 'Some Empirical Aspects of Multi-sided Platform Industries', Review of Network Economics, vol. 2, no. 3, pp. 191–209, 2003.

[19] M. L. Katz and C. Shapiro, 'Systems Competition and Network Effects', Journal of Economic Perspectives, vol. 8, no. 2, pp. 93–115, 1994.

[20] H. Demsetz, 'Toward a Theory of Property Rights', American Economic Review, no. 57, pp. 347–359, 1968.

[21] R. E. Freeman, Strategic management : a stakeholder approach. Boston: Pitman, 1984.

[22] F. Davis, 'A technology acceptance model for empirically testing new end-user information systems - theory and results', PhD Thesis, Massachusetts Institute of Technology (MIT), Massachusetts, 1985.

[23] L. G. Tornatzky and M. Fleischer, The Processes of Technological Innovation. Lexington, Massachusetts: Lexington Books, 1990.

[24] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, 'User Acceptance of Information Technology: Toward a Unified View', Management Information Systems Quarterly (MISQ), vol. 27, no. 3, pp. 425–478, Sep. 2003.

[25] Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts, ISO 9241-11. 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en

[26] J. Nielsen, 'Usability 101: Introduction to Usability', 2012. [Online]. Available: https://www.nngroup.com/articles/usability-101-introduction-to-usability/

[27] M. Hassenzahl, 'User Experience (UX): Towards an Experiential Perspective on Product Quality', 2008.

[28] A. Whitten and J. D. Tygar, 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0', 1999.

[29] S. Wolgemuth, U. Jendricke, D. Gerd tom Markotten, F. Dorner, and G. Müller, 'Sicherheit und Benutzbarkeit durch Identitätsmanagement', Institut für Informatik und Gesellschaft, Abt. Telematik Albert-Ludwigs-Universität Freiburg, 2003.

[30] K.-P. Yee, 'Aligning security and usability', IEEE Security & Privacy, vol. 2, no. 5, pp. 48–55, 2004.

[31] S. Garfinkel, 'Design principles and patterns for computer systems that are simultaneously secure and usable', Dissertation, Massachusetts Institute of Technology (MIT), 2005. [Online]. Available: http://dspace.mit.edu/bitstream/handle/1721.1/33204/67550192.pdf?sequence=1&origin=publication_detail

[32] P. Jaferian, K. Hawkey, A. Sotirakopoulos, and K. Beznosov, 'Heuristics for Evaluating IT Security Management Tools', in Human-Computer Interaction, vol. 4, 2011, pp. 1633–1638.

[33] W3C, 'Web Content Accessibility Guidelines (WCAG)'. [Online]. Available: https://www.w3.org/WAI/standards-guidelines/wcag/

[34] W3C, 'Authoring Tool Accessibility Guidelines (ATAG)'. [Online]. Available: https://www.w3.org/WAI/standards-guidelines/atag/

[35] W3C, 'User Agent Accessibility Guidelines (UAAG) Overview'. [Online]. Available: https://www.w3.org/WAI/standards-guidelines/uaag/

[36] K. O. Venkat Ramaswamy, The co-creation paradigm.

[37] European Telecommunications Standards Institute (ETSI), Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures; Part 1: Building Blocks and PAdES Baseline Signatures, ETSI EN 319 142-1, Version 1.1.1. 2016.

[38] European Telecommunications Standards Institute (ETSI), Electronic Signatures and Infrastructures (ESI); CAdES Digital Signatures; Part 1: Building Blocks and CAdES Baseline Signatures, ETSI EN 319 122-1, Version 1.1.1. 2016.

[39] European Telecommunications Standards Institute (ETSI), Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures; Part 1: Building Blocks and XAdES Baseline Signatures, ETSI EN 319 132-1, Version 1.1.1. 2016.

[40] European Telecommunications Standards Institute (ETSI), Electronic Signatures and Infrastructures (ESI); JAdES digital signatures built on JSON Web Signatures; Part 1: Building blocks and JAdES baseline signatures, Draft ETSI TS 119 182-1. 2020.

Annex – Use Case template

Following the use case template that mGov4EU partners filled in as described in Section 3.1.

1. Description

This is a description of the XYZ use case. First there will be a high-level description of the use case's scenario overview, its relevance, and goals in sub section 1.1. Continuing, sub-section 1.2 describes the architecture and the use of building blocks that are to be constructed in WP3. Next, there will be a process description, which includes the main actors and roles included in the use case, the flow of events, and other conditions and assumptions needed for the use case in sub section 1.3. Last, section 1.4 describes the anticipated implementation and impact the use case will have.

1.1. Use Case - Scenario Overview, Relevance and Goals

1.1.1. Introduction

Name of Use Case/Scenario

Domain context of the use case, prior activities etc.

(not extended - this section should be no more than 5-6 lines)

1.1.2. Problem summary

Describe the nature of the problem, businesses/administrations involved and the current volume of service usage.

1.1.3. Goals of the Use Case/Scenario – Value, Quality and Domain importance

Explain here the functional, technical and business goals, how quality will be ensured and why the UC is a priority for the business domain

1.1.3.1. Functional goals

Describe what functions will be implemented and what results be achieved by performing all the steps of the scenario, such as "company registered", "mandate added", etc. To what extent the problem gets solved (to whom, to what extent, for national and foreign beneficiaries

1.1.3.2. Business case and organizational goals

Provide some evidence (basic figures if existing) on the benefit to the administrations and the End Users (Economic Operators), Continuation of previous efforts, reuse of prior infrastructure, etc. showing added value

1.1.3.3. Quality goals and performance indicators

Describe – if known – the quality goals or "soft"/non-functional goals that should be considered when performing the use case scenario and indicators used for measuring the attainment of the corresponding quality goals, whenever possible. How much time, money or other resources saved per transaction/interaction will take place for different parties?

1.1.4. Relevance to Mobile-First , eIDAS, and SDG/OOP

How the pilot fulfils these requirements

1.1.4.1. Mobile-First

1.1.4.2. eIDAS

1.1.4.3. SDG/OOP

Which service from with the Annex 2 of the SDGR does this pilot address?

1.1.5. Cross Border Relevance

This section would describe how the cross border dimension is addressed. Include possible partners that could be relevant here

1.1.6. Policy and Legal context

What is the relevant legal national and European framework, requirements, and constraints?

Are there any legal barriers that need to be addressed (e.g. mandatory authorizations, notification requirements etc.)?

What policy objectives are fulfilled or supported?

1.2. Architecture and use of Building Blocks

This section elaborates on how the pilot uses and combines eIDAS and SDG elements to achieve its goals. It also elaborates on which building blocks in WP3 will be most relevant.

1.2.1. Overview diagram of architecture and topology

Describe the underlying and expected architecture to be used

One diagram to show the high-level topology and architecture

1.2.2. Use of technologies and Building Blocks

Name the technologies and building blocks to be used; please highlight if you want to re-use BBs from former LSPs and/or CEF

(if relevant)

1.2.2.1. Use of Mobile Technologies

1.2.2.2. Use of eIDAS layer

1.2.2.3. Use of SDG/OOP layer

1.2.3. Interactions between Technical Components

Describe the interaction between technical components, e.g. mobile app, data register, eIDAS nodes, etc.

1.2.4. Use of established infrastructure at EU and MS level

From EU and national initiatives, CEF Core Service Platforms and Generic Services, etc.

(if relevant)

1.3. Process Description

1.3.1. Main Actors and Roles involved in the Use Case Scenario

Describe the requirements and role of administrations and of economic operators.

Describe the requirements and roles of data consumers and data providers

Roles of users involved in the scenario, such as Civil Servant, Business Representative, etc.)

1.3.2. Steps of the Use Case/Scenario and Flow of events

Main process flow in steps, showing interaction between the actors and the flow of information

Actions to be performed by players of the corresponding Roles in the course of the scenario, in a rough chronological order, without yet going into details about conditions, loops, and branching

1.3.3. Data objects involved

Registries or other data sources and their corresponding data objects to be read and/or updated within the use case/scenario.

Provide a clear description of the data and its source/ origin, expected uses, duration of storage and means/term of deletion where applicable.

1.3.4. Pre-conditions, Post-conditions, Assumptions etc.

Describe (if existent and known)

1.4. Implementation and Impact

This section explores how the use case's implementation will impact on users and stakeholders. It highlights the consortium potential, in terms of which partners will have which role in the pilots use case. Lastly, it reflects on how advanced key stakeholders involved in the implementation of the pilots are.

1.4.1. Expected impact on users and stakeholders

Description of expected positive and negative impacts on user and stakeholders, included in terms of data protection and ethics.

1.4.2. mGov4EU Consortium potential

Name the countries/beneficiaries wishing to pilot this use case (in terms of local partners supporting the pilot and/or country of residence of pilot users where relevant)

Name the end users (e.g. administrations, economic operator) that act as data consumers

Name the end users (e.g. administrations, economic operator) that act as data providers

1.4.3. Readiness of participants

How mature and close to implementation are the prospective data consumers and data providers