ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ
ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΜΕΤΑΠΤΥΧΙΑΚΟ
ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΑ &
ΕΠΙΚΟΙΝΩΝΙΑΚΑ
ΣΥΣΤΗΜΑΤΑ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΤΗΡΙΟ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ
ΣΥΣΤΗΜΑΤΩΝ

ΚΕΝΤΡΟ ΕΡΕΥΝΑΣ ΓΙΑ
ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ
ΔΙΑΚΥΒΕΡΝΗΣΗ

Single sign on / wallet as a service systems: application scenarios in local administration

[Μαρία-Ζωή Κονίδη]
[3252021007, icsdm521007@icsd.aegean.gr]

Επιβλέπων: Καθηγητής, Ιωάννης Χαραλαμπίδης

Φεβρουάριος 2023
www.aegean.icsd.gr/is-lab

Η Διπλωματική Εργασία παρουσιάστηκε ενώπιον
του Διδακτικού Προσωπικού του Πανεπιστημίου Αιγαίου
Σε Μερική Εκπλήρωση των απαιτήσεων για την απόκτηση του μεταπτυχιακού
διπλώματος ειδίκευσης «Πληροφοριακά & Επικοινωνιακά Συστήματα»

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ
ΕΠΙΚΥΡΩΝΕΙ ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΗΣ
ΜΑΡΙΑΣ-ΖΩΗΣ ΚΟΝΙΔΗ

ΙΩΑΝΝΗΣ ΧΑΡΑΛΑΜΠΙΔΗΣ, Επιβλέπων

Καθηγητής

Τμήμα Μηχανικών Πληροφοριακών
και Επικοινωνιακών Συστημάτων

ΑΛΕΞΙΟΣ ΚΑΠΟΡΗΣ, Μέλος

Επίκουρος Καθηγητής

Τμήμα Μηχανικών Πληροφοριακών
και Επικοινωνιακών Συστημάτων

ΧΡΗΣΤΟΣ ΓΚΟΥΜΟΠΟΥΛΟΣ, Μέλος

Αναπληρωτής Καθηγητής

Τμήμα Μηχανικών Πληροφοριακών
και Επικοινωνιακών Συστημάτων

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε για το μεταπτυχιακό πρόγραμμα σπουδών «Πληροφοριακά και Επικοινωνιακά Συστήματα» του Πανεπιστημίου Αιγαίου 2021-2023. Στόχος της εργασίας, είναι η ανάλυση σχετικών τεχνολογιών Single sign on και wallet as a service systems και η προδιαγραφή εφαρμογών τους σε έναν ελληνικό Δήμο.

Για την υλοποίηση της διπλωματικής μου εργασίας, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κο Ιωάννη Χαραλαμπίδη, την Uni Systems Greece, εταιρεία στην οποία εργάζομαι, καθώς και όλη την κοινοπραξία του ευρωπαϊκού ερευνητικού έργου H2020 GLASS (Grant Agreement No: 959879).

Περίληψη

Η παρούσα διπλωματική εργασία εκπονήθηκε για το μεταπτυχιακό πρόγραμμα σπουδών «Πληροφοριακά και Επικοινωνιακά Συστήματα» του Πανεπιστημίου Αιγαίου 2021-2023.

Στόχος της εργασίας, είναι η ανάλυση σχετικών τεχνολογιών Single sign on και Wallet as a Service systems και η προδιαγραφή εφαρμογών τους σε έναν ελληνικό Δήμο.

Αρχικά, θα αναλυθεί το τρέχον τεχνολογικό επίπεδο σε συστήματα Single sign on και Wallet as a Service και θα περιγραφούν οι εφαρμογές των συστημάτων αυτών στη βιομηχανία και την κοινωνία.

Στη συνέχεια, θα παρουσιαστεί το ευρωπαϊκό ερευνητικό έργο GLASS (Grant Agreement No: 959879), οι νέες του υποδομές και προτάσεις, καθώς και τα σενάρια εφαρμογής του στην Τοπική Αυτοδιοίκηση. Πιο συγκεκριμένα θα αναλυθούν οι στόχοι, τα προσδοκώμενα αποτελέσματα, οι παροχές σε έναν ελληνικό Δήμο και στους πολίτες, ο τρόπος λειτουργίας, καθώς και οι απαιτούμενες υποδομές και προϋποθέσεις.

Τέλος θα εντοπιστούν οι προτάσεις και θα αναλυθούν οι ευκαιρίες που θα προκύψουν και θα παρουσιαστούν τα συμπεράσματα της έρευνας.

Λέξεις - Κλειδιά: Single sign on, πορτοφόλι ως υπηρεσία, δημόσιος τομέας, τεχνολογική καινοτομία, πολιτικά συστήματα και θεσμοί, διακυβέρνηση, καινοτομία του δημόσιου τομέα, ηλεκτρονική διακυβέρνηση, ψηφιακός μετασχηματισμός, ψηφιακές δημόσιες υπηρεσίες, διαλειτουργικότητα

Abstract

This thesis was prepared for the postgraduate program "Information and Communication Systems" of the University of the Aegean 2021-2023.

The aim of the thesis is the analysis of relevant technologies Single sign on and Wallet as a Service systems and the specification of their applications in the local administration.

Initially, the current technological level of Single sign on and Wallet as a Service systems will be analysed and the applications of these systems in industry and society will be described.

Then, the European research project GLASS (Grant Agreement No: 959879) will be presented, its new infrastructures and proposals, as well as the scenarios of its implementation in the Local Government. More specifically, the objectives, the expected results, the benefits to a municipality and to the citizens, the mode of operation, as well as the required infrastructure and conditions will be analysed.

Finally, the proposals and opportunities will be identified, and the conclusions of the research will be presented.

Keywords: Single sign on, wallet as a service, public sector information, Technological innovation, Political systems and institutions, governance, public sector innovation, eGovernance, Digital Transformation, Digital public services, Interoperability

Table of Contents

Table of Tables

Table of Figures

1. Introduction

1.1 Context of the thesis

The rapid growth of Internet technologies, mobile communications, cloud infrastructures and distributed applications have brought an unprecedented impact to all spheres of the society and a great potential towards the establishment of novel eGovernance models (Wimmer, 2020). These models should deploy core values such as improved public services and administrative efficiency, open government capabilities, improved ethical behaviour and professionalism, improved trust and confidence in governmental transactions (Jean Damascene Twizeyimana, 2019). Towards the modernization of their services and the reduction of the associated bureaucracy, public administrations need to transform their back-offices, upgrade their existing internal processes and services, and provide privacy-preserving and secure solutions. It is necessary to leverage key digital enablers, such as open services and technical building blocks (eID, eSignature, eProcurement, eDelivery and eInvoice), shared and reusable solutions based on agreed standards and specifications (Single Digital Gateway), as well as common interoperability practices (e.g., European Interoperability Framework). This leads to the upgrade of services that enable cross-border data sharing among public administrations, businesses and citizens.

Governance models, in general, do not adopt a citizen-centric paradigm (Ghareeb, Darwish, & & Hefney, 2019); they do not take into account citizens' needs and expectations of new services, often excluding them from operational and decision-making processes. Moreover, documentation exchanges, processes and contact points do not function as a whole; they are rather dispersed and not sufficiently inter-connected among countries and organisations. Transparency and accountability are additional aspects of major importance towards building a good and fair governance model (Bertot, Jaeger, & & Grimes, 2010). Admittedly, governments that employ models to make information sharing and decision-making processes transparent improve the principle of accountability and augment the participation of citizens and other stakeholders in related actions (Teresa M. Harrison, 2014). The corresponding digital transformation of public services can reduce administrative burdens, enhance productivity of governments, minimising at the same time all the extra cost of traditional means to increase capacity, and ultimately improve the overall quality of interactions with and within public administrations (Androutsopoulou, Karacapilidis, Loukis, & Charalabidis, 2019)

It is finally noted that an interesting approach towards defining an eGovernance model has been presented in (Finger, 2003). In this approach, authors conceptualise eGovernance across three dimensions, namely eGovernance as customer satisfaction, eGovernance as processes and interactions, and eGovernance as tools; the proposed model accordingly distinguishes between three different policy-levels, three different types of actors involved, three different policy functions, and three different degrees of making use of the (new) ICTs.

1.2 Scope of the Thesis

This thesis has been produced in the context of the analysis of Single sign on and Wallet as a Service systems relevant technologies and the specification of their applications in the local administration.

Initially, the current technological level of Single sign on and Wallet as a Service systems will be analysed and the applications of these systems in industry and society will be described.

Then, the European research project GLASS (Grant Agreement No: 959879) will be presented, its new infrastructures and proposals, as well as the scenarios of its implementation in the Local Government. More specifically, the objectives, the expected results, the benefits to a municipality and to the citizens, the mode of operation, as well as the required infrastructure and conditions will be analysed.
Finally, the proposals and opportunities will be identified, and the conclusions of the research will be presented.

1.3 Structure

The thesis is divided into the following sections:

- Section 1 introduces the research and the methodology used.
- Section 2 analyses the current technological level of Single sign on / wallet as a service system.
- Section 3 describes the single sign on / wallet as a service systems' applications in industry and society.
- Section 4 presents the H2020 GLASS project, along with its infrastructure and proposed solutions.
- Section 5 outlines the GLASS demonstrators and, more specifically, the application scenarios of the project in the local administration.
- Section 6 describes the establishment and applications of GLASS solutions in a Greek Municipality and the issues that may arise.
- Section 7 provides suggestions, barriers and opportunities regarding the adoption of such solutions.
- Section 7 concludes the document.

2. Analysis of the current technological level in Single sign on / Wallet as a service systems

2.1 Single sign-on (SSO) systems

Single sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials. More, specifically, it is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network (Guilin Wang, 2013).
SSO works based upon a trust relationship set up between an application, known as the service provider, and an identity provider. This trust relationship is often based upon a certificate that is exchanged between the identity provider and the service provider. This certificate can be used to sign identity information that is being sent from the identity provider to the service provider so that the service provider knows it is coming from a trusted source. In SSO, this identity data takes the form of tokens which contain identifying bits of information about the user like a user's email address or a username.

The login flow usually looks like this:

1. A user browses to the application or website they want access to, aka, the Service Provider.
2. The Service Provider sends a token that contains some information about the user, like their email address, to the SSO system, aka, the Identity Provider, as part of a request to authenticate the user.
3. The Identity Provider first checks to see whether the user has already been authenticated, in which case it will grant the user access to the Service Provider application and skip to step 5.
4. If the user hasn't logged in, they will be prompted to do so by providing the credentials required by the Identity Provider. This could simply be a username and password, or it might include some other form of authentication like a One-Time Password (OTP).
5. Once the Identity Provider validates the credentials provided, it will send a token back to the Service Provider confirming a successful authentication.
6. This token is passed through the user's browser to the Service Provider.
7. The token that is received by the Service Provider is validated according to the trust relationship that was set up between the Service Provider and the Identity Provider during the initial configuration.
8. The user is granted access to the Service Provider.

When the user tries to access a different website, the new website would have to have a similar trust relationship configured with the SSO solution and the authentication flow would follow the same steps.

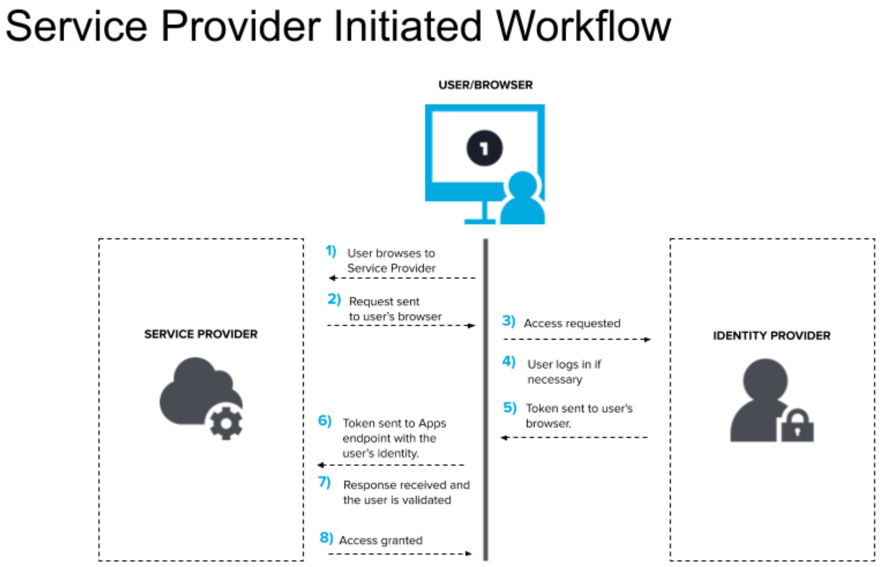

Service Provider Initiated Workflow
USER/BROWSER
1
SERVICE PROVIDER
1) User browses to Service Provider
2) Request sent to user's browser
3) Access requested
4) User logs in if necessary
5) Token sent to user's browser.
6) Token sent to Apps endpoint with the user's identity.
7) Response received and the user is validated
8) Access granted
IDENTITY PROVIDER

Figure 1: Service Provider Initiated Flow (source: https://www.onelogin.com/learn/how-single-sign-on-works)

2.1.1 Security of SSO

There are many reasons why SSO can improve security. A single sign-on solution can simplify username and password management for both users and administrators. Users no longer have to keep track of different sets of credentials and can simply remember a single more complex password. SSO often enables users to just get access to their applications much faster.

SSO can also cut down on the amount of time the help desk has to spend on assisting users with lost passwords. Administrators can centrally control requirements like password complexity and multi-factor authentication (MFA). Administrators can also more quickly relinquish login privileges across the board when a user leaves the organization.

Single Sign-On does have some drawbacks. For example, you might have applications that you want to have locked down a bit more. For this reason, it would be important to choose an SSO solution that gives you the ability to, say, require an additional authentication factor before a user logs into a particular application or that prevents users from accessing certain applications unless they are connected to a secure network.

2.1.2 Types of SSO configurations

Some SSO services use protocols, such as Kerberos or Security Assertion Markup Language (SAML):

- In a Kerberos-based setup, once user credentials are provided, a ticket-granting ticket (TGT) is issued. The TGT fetches service tickets for other applications the user wants to access, without asking the user to re-enter credentials.
- SAML is an Extensible Markup Language standard that facilitates the exchange of user authentication and authorization data across secure domains. SAML-based SSO services involve communications among the user, an identity provider that maintains a user directory and a service provider.

- Smart card-based SSO asks an end user to use a card holding the sign-in credentials for the first login. Once the card is used, the user does not have to re-enter usernames or passwords. SSO smart cards store either certificates or passwords.

2.1.3 SSO security risks

Although single sign-on is a convenience to users, it presents risks to enterprise security. An attacker who gains control over a user's SSO credentials is granted access to every application the user has rights to, increasing the amount of potential damage.

In order to avoid malicious access, SSO should be coupled with identity governance. Organizations can also use two-factor authentication (2FA) or multifactor authentication with SSO to improve security.

Social SSO

Google, LinkedIn, Apple, Twitter and Facebook offer popular SSO services that enable end users to log in to third-party applications with their social media authentication credentials. Although social single sign-on is a convenience to users, it can present security risks because it creates a single point of failure that can be exploited by attackers.

Many security professionals recommend end users refrain from using social SSO services because, once attackers gain control of a user's SSO credentials, they can access all other applications that use the same credentials.

Enterprise SSO

Enterprise single sign-on (eSSO) software and services are password managers with client and server components that log a user on to target applications by replaying user credentials. These credentials are almost always a username and password. Target applications do not need to be modified to work with the eSSO system.

SSO advantages:

In addition to being much simpler and more convenient for users, SSO is widely considered to be more secure. This may seem counterintuitive: how can signing in once with one password, instead of multiple times with multiple passwords, be more secure? Proponents of SSO cite the following reasons:

- Stronger passwords: Since users only have to use one password, SSO makes it easier for them to create, remember, and use stronger passwords. In practice, this is typically the case: most users do use stronger passwords with SSO.
  What makes a password "strong"? A strong password is not easily guessed and is random enough that a brute force attack is not likely to succeed.
- No repeated passwords: When users have to remember passwords for several different apps and services, a condition known as "password fatigue" is likely to set in: users will re-use passwords across services. Using the same password across several services is a huge security risk because it means that all services are only as secure as the service with the weakest password protection: if that service's password database is compromised, attackers can use the password to hack all of the user's other services as well. SSO eliminates this scenario by reducing all logins down to one login.

- Better password policy enforcement: With one place for password entry, SSO provides a way for IT teams to easily enforce password security rules. For example, some companies require users to reset their passwords periodically. With SSO, password resets are easier to implement instead of constant password resets across a number of different apps and services, users only have one password to reset. (While the value of regular password resets has been called into question, some IT teams still consider them an important part of their security strategy.)
- Multi-factor authentication: Multi-factor authentication refers to the use of more than one identity factor to authenticate a user. For example, in addition to entering a username and password, a user might have to connect a USB device or enter a code that appears on their smartphone. Possession of this physical object is a second "factor" that establishes the user is who they say they are. Multi-factor authentication is much more secure than relying on a password alone. SSO makes it possible to activate multi-factor authentication at a single point instead of having to activate it for three, four, or several dozen apps, which may not be feasible.
- Single point for enforcing password re-entry: Administrators can enforce re-entering credentials after a certain amount of time to make sure that the same user is still active on the signed-in device. With SSO, they have a central place from which to do this for all internal apps, instead of having to enforce it across multiple different apps, which some apps may not support.
- Internal credential management instead of external storage: Usually, user passwords are stored remotely in an unmanaged fashion by applications and services that may or may not follow best security practices. With SSO, however, they are stored internally in an environment that an IT team has more control over.
- Less time wasted on password recovery: In addition to the above security benefits, SSO also cuts down on wasted time for internal teams. IT has to spend less time on helping users recover or reset their passwords for dozens of apps, and users spend less time signing into various apps to perform their jobs. This has the potential to increase business productivity.

SSO disadvantages:

- It does not address certain levels of security each application sign-on may need.
- If availability is lost, users are locked out of all systems connected to SSO.
- If unauthorized users gain access, they could access more than one application.

SSO vendors

Multiple vendors offer SSO products, services and features.
SSO vendors include the following:

- Rippling enables users to sign into cloud applications from multiple devices.
- Avatier Identity Anywhere is SSO for Docker container-based platforms.
- OneLogin by One Identity is a cloud-based identity and access management platform that supports SSO.
- Okta is a tool with SSO functionality. Okta also supports 2FA and is primarily used by enterprises.

2.2 Wallet as a Service

Wallet as a Service (WaaS) is a highly secure and scalable crypto wallet infrastructure, offering flexible options for digital assets management for businesses and institutions of all sizes. It's a digital wallet solution covering all the essential stress points of the modern digital wallet - the perfect balance between ease of use and security, successful and quick integration with multiple blockchains, key recovery system, and low-cost fees.

2.2.1 Self-Sovereign Identity (SSI) Digital Wallet

Digital identity is a core element of any digital platform for its successful operation. However, it has been one of the most difficult areas for cyber experts to master and provide a complete solution, which is capable of proving the identity of any entity in cyberspace, similar to that of the physical world. Over the years, several Identity Management (IDM) models have been proposed and employed. However, until recently no model was able to resolve the issue of sovereignty of an identity and storage control of its associated personal and confidential data (Jenkins, 2020). This issue of sovereignty has affected several other related issues with respect to identity such as security, privacy and safeguarding (Windley, 2017). With the introduction of blockchain, a new identity management model called SSI was introduced which aims to solve all the above issues and offers a user full sovereignty of their identity and storage-control of their associated personal and confidential data. Alongside ownership of an identity, it maintains all private information in a Digital Wallet owned and controlled by the user. The Digital Wallet is analogous to a physical wallet saving all digital credentials as physical entities, however, these credentials in the Digital Wallet are digitally signed verifiable credentials and much faster to issue and verify than their physical counterpart (Reed, 2016).

SSI is an emerging model referred to as IDM 3.0, therefore it requires careful evaluation of its various aspects for it to become an operative IDM. Previously, several specifications for evaluating its predecessor federated IDM 2.0 model were proposed (Jenkins, 2017), (Jenkins, 2016).

2.2.2 Identity Management Models

Centralised Identity Management Model (IDM 1.0)

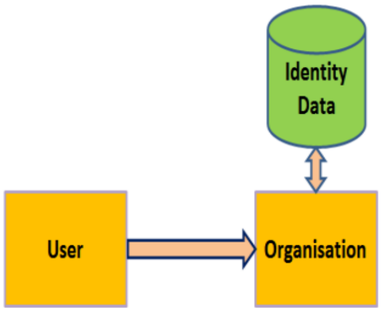


Figure 2: Centralised Identity Management Model (IDM 1.0)

The centralised IDM model is the oldest IDM model, in which an organization issues credentials to their users permitting them to use their services. The trust relationship between organisation and user is based on a shared secret, in most cases, this is typically a login password associated with a username (Ruff, 2018). The user's identity related personal and confidential data is always stored and controlled by the organisation. Additionally, the user repeats this process and requires separate credentials for each organisation or system, they wish to obtain service from.

Federated Identity Management Model (IDM 2.0)

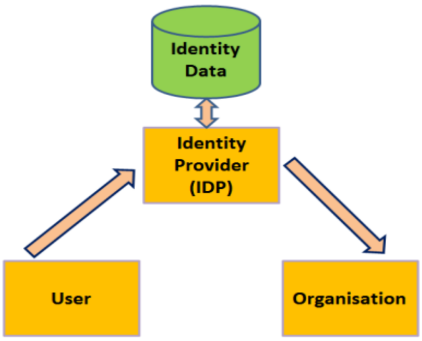


Figure 3: Federated Identity Management Model (IDM 2.0)

This federated IDM model solves two major issues: 1) it removes the organisational burden of managing identity and credentials securely by introducing a third-party called the IDentity Provider (IDP), which is an additional task alongside the main business operations and 2) it removes the burden from users to manage several identity related credentials for several systems by offering a Single-Sign On (SSO) facility (Jenkins, 2016), (N. Naik, 2017). However, this IDM model has one similar issue in that the abundance of identity related personal and confidential data of a user is held by the IDP and therefore the user has no control over this information.

Self-Sovereign Identity Management Model (IDM 3.0)

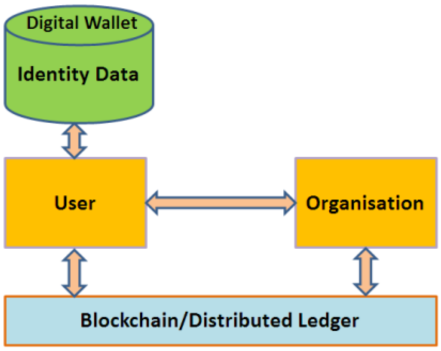


Figure 4: Self-Sovereign Identity Management Model (IDM 3.0)

This self-sovereign IDM model is an improvement on the federated IDM model, where it removes the third-party IDP and offers a direct connectivity between a user and organisation. Furthermore, it resolves the main issue of ownership of identity related personal and confidential data of a user by offering its full control through the use of a Digital Wallet. The Digital Wallet saves all the identity related personal and confidential data which is owned and controlled by the user on the device controlled by the user. SSI assumes three key roles i.e., Issuer, Holder and Verifier, in its ecosystem as shown in Fig. 5. An issuer creates and issues credentials to a holder. A holder receives credentials from an issuer, holds it and when required, it shares these credentials with a verifier. A verifier receives and verifies credentials presented by a holder.

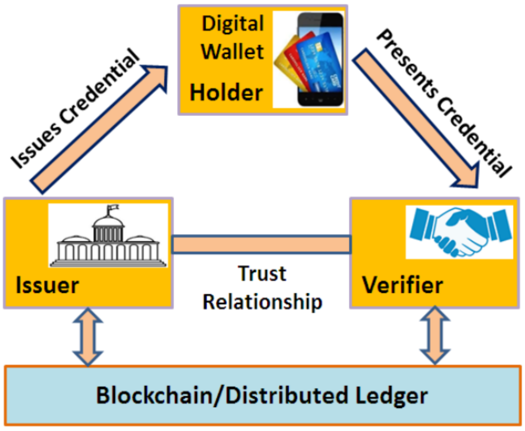


Figure 5: Self-Sovereign Identity Ecosystem

This SSI implementation is based on the Verifiable Credential (VC) (W3C, 2019) and Decentralized IDentifier (DID) (W3C, 2019) standards which are proposed for creating a cryptographically verifiable digital identity that is fully governed by its owner (Sovrin.org., 2018). A VC is used to represent similar information on the Web to that of a physical credential in the real world. The DID is a permanent, universally unique identifier and cannot be taken away from its owner who owns the associated private key, which is completely different from other ephemeral identifiers such as a mobile number, IP address and domain name (Sovrin.org., 2018).

2.3 eIDAS Regulatory Framework

Electronic identification, authentication and trust services (eIDAS)[1] is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. The eIDAS Regulation will help business, citizens and public authorities carry out secure and seamless electronic interactions.
It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification and repeals 1999/93/EC from 13 December 1999.
It entered into force on 17 September 2014 and applies from 1 July 2016. All organizations delivering public digital services in an EU member state must recognize electronic identification from all EU member states from September 29, 2018.

The eIDAS regulation:

- ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services available online in other EU countries;
- creates a European internal market for trust services by ensuring that they will work across borders and have the same legal status as their traditional paper based equivalents.

Only by providing certainty on the legal validity of these services will businesses and citizens use digital interactions naturally.

More specifically, eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services. Both the signatory and the recipient can have more convenience and security. Instead of relying on traditional methods, such as mail or facsimile, or appearing in person to submit paper-based documents, they may now perform transactions across borders, like "1-Click" technology.

eIDAS has also created standards for which electronic signatures, qualified digital certificates, electronic seals, timestamps, and other proof for authentication mechanisms enable electronic transactions, with the same legal standing as transactions that are performed on paper.

[1] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

3. Single sign on / wallet as a service systems' applications in industry and society

E-governance is a process that aims to enhance a government's ability to simplify all the processes that may involve government, citizens, businesses, and so on. The rapid evolution of digital technologies has often created the necessity for the establishment of an e-Governance model. There is often a need for an inclusive e-governance model with integrated multi-actor governance services and where a single market approach can be adopted. e-Governance often aims to minimise bureaucratic processes, while at the same time including a digital-by-default approach to public services. This aims at administrative efficiency and the reduction of bureaucratic processes. It can also improve government capabilities, and enhances trust and security, which brings confidence in governmental transactions. However, solid implementations of a distributed data sharing model within an e-governance architecture are far from a reality; hence, citizens of European countries often go through the tedious process of having their confidential information verified.

Our current age is often known as the digital era, where data is a significant resource that scales up constantly. Data contains sensitive information that could relate to the confidential information of users, businesses, stakeholders, and so on. In a simple data-sharing model, often one entity owns a document and gives access rights to other entities, which could be achieved through role-based access control (RBAC) (Maile, 2022) or attribute-based access control (ABAC) (Keith, 2020), (Keith, 2021). Data security is a method that aims to protect confidential information from unauthorised access (Danny, 2019). Data handled by public authorities must be protected when it is associated with individuals' sensitive details. However, a lack of cyber situational awareness and abuse of sensitive data can cause great concern for citizen privacy. Moreover, a third party, such as a public authority and/or agency, often governs the way confidential data is maintained, and due to manual business flows and sluggish interaction methods, a business often fails to build trust and confidence with its partners (Piotr, 2019), (Neil, 2020). Hence, existing data-sharing approaches often tend to be a serious threat to citizen privacy.

Achieving the full potential of data sharing, can rely on the deploying of technologies to securely and efficiently collect and transmit the relevant data, thus making them accessible to authorised users (Sookhak, Jabbarpour, Safa, & Yu, 2021). This data could be related by an electronic health record (EHR) in an e-Health domain, or via a citizen's confidential identity information. One of the main issues in many existing data-sharing scenarios is that it puts the user's privacy and information security at risk of a data breach. Many organisations have thus adopted centralised systems for data management and sharing, but this can result in various attacks due to a single point-of-failure (SPoF) approach (Dandan, et al., 2017). Although some decentralised distributed methods indicate promising outcomes, the majority of these methods are either research prototypes or based on weak implementations, resulting in significant challenges.

In order to protect sensitive or confidential information, various data protection principles are often in place to require the participating parties to adhere to specific regulations, such as General Data Protection Regulation (GDPR) (Matt, 2020). Overall, GDPR is endorsed by the European Union (EU) and is a privacy and security law that enforces certain policies to organisations when acquiring user’s data (Danny, 2019). One of the key principles of GDPR is that data cannot be processed if there is no consent from the subject. Regardless of various principles to protect data, a data breach may still occur due to neglecting potential risks or adopting weak methods of securing the data (Luke, 2020). According to a 2021 data breach report by IBM, the average global cost of a data breach per organisation was USD 4.24 million (IBM, 2021). The report also suggests that the data breach cost in the United Kingdom rose from USD 3.90 million in 2020 to USD 4.67 million in 2021. Generally, centralised approaches to data sharing are one of the main factors that can cause serious threats to citizen privacy.

In a distributed environment, a collection of computing devices can be connected to share confidential and sensitive data and reduce communication overheads. To overcome this, blockchain can be used as a decentralised, distributed, immutable ledger technology in a trustworthy way (Sayeed & Marco-Gisbert, 2019). Along with this, sectors such as healthcare, voting, asset management, and insurance have shown great improvements in terms of efficiency and security (Stamatellis, Papadopoulos, Pitropakis, Katsikas, & Buchanan, 2020). Blockchain has also solved other real-world problems, such as in cross-border payments, identity theft, and so on. It can thus also help in protecting confidential data within centralised government systems and within public sectors (Gwyneth, 2021).

A public blockchain is an open network allowing any party to be part of the ecosystem, whereas a permissioned blockchain authorises only the permitted entities to be part of the network. A permissioned blockchain comprises of an access-control method where an administrator grants permissions only to the authorised entities to join a secure channel.

An e-Governance solution primarily focuses on providing a transparent, efficient and coherent service to the citizens (Avijit, 2020), (Krimmer, Dedovic, Schmidt, & Corici, 2021). It can connect various entities, such as citizens, government agencies, and trusted institutions into a single domain. The main aim is to enhance the quality of government services so that it improves citizen access to governmental processes through digital methods. An e-Governance solution often improves government capabilities, behaviour and professionalism, and such as in the trust and confidence in governmental transactions.

Sharma et al. (Sharma, Kumar Kar, & Gupta, 2021) define that these types of approaches to improved e-governance are crucial for improving the bureaucratic relationship between the government, citizens, and policymakers and enforce accountability in governance processes by improving public access to information and transparency. Krimmer et al. (Krimmer, Dedovic, Schmidt, & Corici, 2021) define that a key factor of achieving a digital single market requires a strong focus on cross-border integration with the development of e-governance approaches.

4. The GLASS project, its new infrastructure and proposals

Due to the rapid growth of Information and Communication Technology (ICT) and its increasing pervasiveness across all parts of society, the role of the government is changing. The Internet, mobile communications, cloud infrastructures, distributed technologies and digitization have brought a uniquely positive impact to all spheres of the society and even more potentialities into the establishment of the eGovernment model. eGovernment is commonly defined as governments' use of ICTs combined with organizational change to improve the structures and operations of governments (Field, Muller, Lau, Gadriot-Renard, & Vergez, 2003) (Jean Damascene Twizeyimana, 2019). The core values eGovernment is expected to yield are: (i) improved public services and administrative efficiency; (ii) Open Government capabilities; (iii) improved ethical behaviour and professionalism; (iv) improved trust and confidence in government; and (v) improved value and well-being. The vision for future eGovernment research actions in the EU is to extend the borders of ICT, increase the interoperability and efficiency of public sector organisations and offer user-centric and secure services (Codagnone, 2020).

Towards the modernization of their services, public administrations need to transform their back-offices, upgrade their existing internal processes and services, and provide privacy-preserving and secure solutions for a new governance model. It is necessary to build upon key digital enablers, such as open services and technical building blocks (eID, eSignature, eDelivery and eInvoice), shared and reusable solutions based on agreed standards and specifications (Single Digital Gateway (Commission, 2019)), as well as common interoperability practices (European Interoperability Framework - (Commission, 2016), (Commission, 2017)). This leads to the upgrade of services that enable cross-border data sharing among EU public administrations, businesses and citizens. A vital part of delivering digital eGovernment services is related to the security principles that demand the adequate identification of citizens and businesses that interact with these entities, including providers, public administrations, local authorities and other institutions, while also assuring data protection and privacy. Further access control depends on authentication and authorization mechanisms, whose effectiveness and appropriateness vary according to the techniques used, as well as the quality and robustness of the attributes and identifiers incorporated.

Transparency and accountability are further aspects of utmost importance to the concept of the good and fair governance model. Digital technologies in public administrations are also related to increased transparency and fairness in at least three aspects. First, it relates to the transparency in decisions made by public servants, largely related to opening of data to the public (Bertot, Jaeger, & & Grimes, 2010). Second, it refers to reduced human involvement and human biases (disintermediation). Third, the increased transparency should also result from the more effective policy implementation and service provision, especially in the areas of taxation and payments. Governments that employ models to make information sharing and decision-making processes transparent improve the principle of accountability and augment the participation of citizens and other stakeholders in related actions (Teresa M. Harrison, 2014).

The need for a new eGovernance paradigm through the establishment of multi-actor governance services is a key element towards a European Single Market. Digital

Transformation of public services can remove existing digital and physical barriers, reduce administrative burdens, enhance productivity of governments, minimizing at the same time all the extra cost of traditional means to increase capacity, and eventually improve the overall quality of interactions with (and within) public administrations. The EU Single Market model cannot function effectively without cross-border digital public services. Such services facilitate access to markets, increase confidence and stimulate competition across the Single Market. Administrations should help businesses operate online across borders within the Single Market, simplify access to information under EU business and company laws, and enable businesses to easily operate and expand in any Member State through end-to-end public services.

The process by which governments have moved towards digitalization is not necessarily aligned with the technology breakthrough of the academic and industry advances (Barcevičius, et al., 2019). Governance models in the EU, in general, do not adopt a common citizen-centric paradigm (Ghareeb, Darwish, & & Hefney, 2019); documentation exchanges, processes, and contact points do not function as a whole, but are rather dispersed and not sufficiently inter-connected among the Member States and between approved organizations outside the EU (Vieira, 2018). Additionally, many of already adopted eGovernment practices do not take into account citizen’s needs and expectations of new services, neither at least their preferences for the status quo of traditional government services, excluding them from operational and decision-making processes and challenging their trust. For all the above reasons, there is a huge potential for a more open, transparent, trustworthy, cross-border, inclusive, citizen-centric and effective eGovernance model, should the latest technological achievements be combined, extended and adopted by the eGovernment sector.

4.1 The GLASS Vision and Technological Solution

GLASS is a Horizon 2020 project funded by the European Union (Grant Agreement: 959879) to create a new paradigm for the sharing and transfer of personal information, with the citizen in control. It will provide a distributed framework for sharing common services of public administrations across the EU for citizens, businesses and governments. GLASS started on January 1st, 2021, and will complete its funded phase on December 31st, 2023. It brings together 12 partners from 7 countries. More specifically, large enterprises and dynamic SMEs, academic partners and research organisations as well as local and public authorities.

GLASS will significantly enhance the administrative processes for governments, the quality of their services and the overall efficiency of the public sector. To achieve this, we propose a novel eGovernance paradigm that creates new digital governance pathways through the application of emerging technologies and breakthrough cross-sector services. For this GLASS will deploy mobile distributed applications (dApps) to deliver, among others, efficient, reliable and secure data sharing and transparent auditing mechanisms and communication channels throughout its value chain, while preserving data ownership and privacy. The project will examine the effectiveness and efficiency of cutting-edge technologies (e.g. distributed ledger technologies, deep learning and security), enabling document sharing, identity authentication, information exchange, transaction monitoring and validation, and will extend the existing interaction relationships between the stakeholders (G2C, G2B, G2G) with a service that connects businesses to citizens (B2C). The project will exploit public ledgers to facilitate the auditability not only from the regulatory perspective, but also from the civilian, in a continuous manner. GLASS will contribute to an integrated government strategy that unlocks further economic and social benefits for the society, is compliant with eIDAS[2] or FIDO[3] and further investigate the possibility of approved organizations outside the EU to participate in a European-wide eGovernance model. GLASS renders the interactions of citizens and businesses with public administrations crossborder, faster, efficient, more convenient, transparent and more cost-effective, as well as interoperable with the current systems in use.

GLASS vision is to introduce a citizen-centric, eGovernance model for public administration services, which automates the processes and safeguards the integrity of interactions among citizens, businesses and public authorities. Driven by the eGovernment Action Plan 2016-2020 and by taking advantage of emerging ICT technologies, such as Peer-to-Peer (P2P) networks, distributed ledgers and deep learning, GLASS will develop and deliver a public, distributed infrastructure, based on the InterPlanetary File System (IPFS[4]) and a distributed ledger. The project will design, implement and thoroughly assess a single sign-on Wallet as a Service (WaaS) platform that interconnects distinct distributed applications (dApps) responsible for ID authentication, document sharing, information exchange and transactions validation, in compliance with the Single Digital Gateway (SDG) guidelines, enabling a single point of access to information, without a single point of failure in the services. The proposed underlying mechanisms make our solution interoperable with existing and newly developed centralized applications and systems. By these means, all interactions among citizens, businesses and public authorities become transparent under a trustworthy and secure environment, while clear guidelines are set for citizens' data ownership. Our goal is to make public administrations and public institutions open, efficient and inclusive, providing borderless, digital, personalised and citizen-driven public services for the EU population.

GLASS offers citizens and businesses efficient and secure mobile public services and co-creation mechanisms setting the foundations for a new eGovernment paradigm that enables governments to be extrovert, while preserving trust among EU public and private entities.

In accordance with related EU policy priorities, we propose a set of actions that advance the mobile services delivered to citizens and contribute to the digital by default principle for government and local authorities. GLASS enables beneficiaries to participate and operate in a by design efficient, cost-effective, secure and cross-border distributed network for data exchange and service delivery. To further increase its impact, the project will investigate the possibility of modeling the compliance of the proposed solution with currently used mechanisms by approved organizations beyond the EU. Overall, GLASS aspires to be the backbone of a new generation, citizencentric, cross-border eGovernance model, where public authorities, enterprises and businesses can be supervised and audited by the community and regulatory authorities towards the further democratization and openness of the public services.

[2] https://digital-strategy.ec.europa.eu/en/policies/discover-eidas
[3] https://fidoalliance.org/
[4] https://ipfs.tech/

GLASS will enable organisations to join a secure and trustable distributed network to demonstrate the capacity of a modernised eGovernance model. Figure 6 illustrates the breakthrough solution of the GLASS approach compared to the current paradigm. In this regard, GLASS acts as the paradigm for various cross-sector and cross-border governance operations applications. The proposed distributed Governance framework will utilize the IPFS-P2P public distributed network, which will play the role of the file storage system in a distributed manner, with respect to the pillars that an eGovernance model aims to support. IPFS is a content-addressable storage, P2P, hypermedia communication protocol which is designed to create a permanent, decentralized method of data storage and sharing. Complementary to the P2P network, a distributed ledger will track and continuously supervise all the transactions occurring between users, keeping an immutable transaction record with traceability functionalities, while ensuring trust. GLASS will operate these services through distributed applications (dApps), which are software applications deployed on the distributed ledger that communicate with each other to complete a specific task and run on multiple systems simultaneously. The dApps will enable the document exchange and data sharing over the network and will act as the main interface gateways, so that operational stakeholders (citizens, businesses, public administrations) can use the services of the network through their mobile devices. Smart contracts will define their functionality and will be designed to operate over the distributed ledger. The single sign-on Wallet will provide a single documentation management tool for different applications running on the same ledger, without a single point of failure. All the documents exchanged within the network will be encrypted and stored in the IPFS, while the transaction records will be generated on the ledger. GLASS will also develop the AI Data Schema Transformer to enable interoperability between heterogeneous and non-standardized data schemas, allowing any public entity, regardless of its interoperability readiness, to join the network and transform its services.

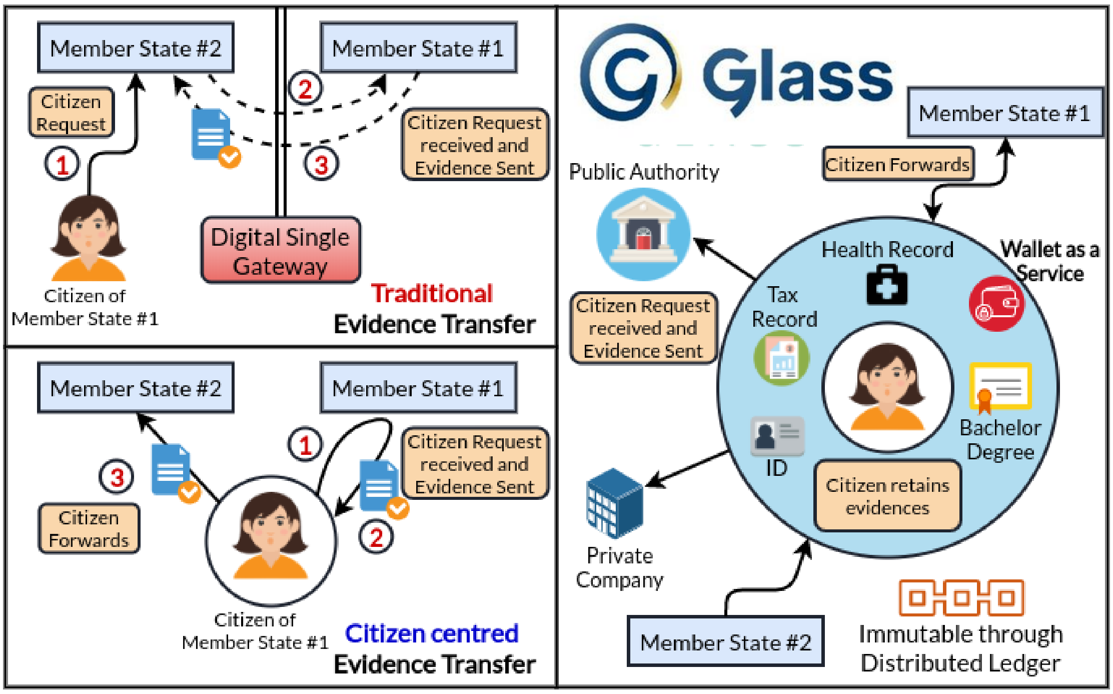


Figure 6: GLASS approach as opposed to current practices

4.2 The GLASS Concept and the GLASS eGovernance Model

The main driving force of the project will be the GLASS eGovernance Model that will be defined in the early stages of the project to become the core reference model for the implementation of the technical and development activities. This model will be used to define the main entities that will participate in the GLASS network, their roles, responsibilities, activities and benefits, always keeping in mind important aspects such as the legal framework, institutional/regulatory policies, constraints and innovation potentialities that impact eGovernance strategies.

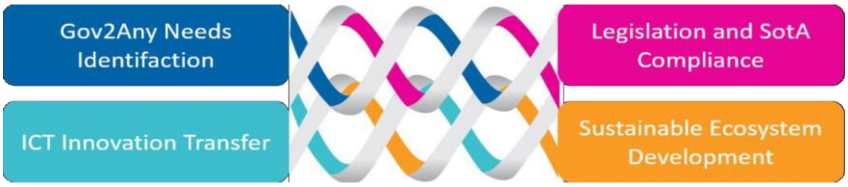

Gov2Any Needs Identifaction
Legislation and SotA Compliance
ICT Innovation Transfer
Sustainable Ecosystem Development

Figure 7: Main activities formulating the GLASS concept

GLASS aims to renovate the way the public sector operates, by introducing novel ICTs which are proven to be beneficial for various industrial domains and can truly redesign the way the public sector is delivering its services, with a strong focus on trust, security, reproducibility and value generation for all stakeholders. As such, the overall GLASS concept (as shown in Figure 7) is based on the exploration of the following major sub-activities which are closely related and can be witnessed as a quadruple helix: (i) Identification of needs and stakeholders of all the Gov-2-Any services; (ii) Legal Framework and eGovernance Strategic Actions Compliance; (iii) Innovation Transfer by the application of novel ICTs in the domain; and (iv) Tangible Impact Generation in a Sustainable eGovernance Ecosystem Development.

The last two dimensions (Innovation transfer and Ecosystem Development) will drive the GLASS concept forward, as they are key factors for the continuous improvement and take-up of the project's results and also the ones that can make a difference, in contrast to previous approaches, where very solid research results remained unutilised due to the lack of ways to properly showcase their added value, as well as creating and engaging the right target group for their dissemination and adoption.

Starting from this point, the consortium believes that the successful recipe for carrying out such a work is grounded on the unanimous acceptance of the outputs by the broad community of stakeholders, which is better achieved by incorporating the community's views achievements and opinions in the final results, not only as references and citations but through close collaboration and consultation from the very starting point that actually results in the cogeneration and co-creation of the final outputs by all parties.

Based on the above, it is obvious that the GLASS concept is strongly based on the idea of introducing a novel eGovernance model based on the utilisation of cutting-edge technologies for the collaboration and service delivery amongst diverse actors, that could heavily impact the public sector's efficiency and effectiveness, and that could be pushed further though a sound business case that will be developed to deliver value to all engaged stakeholders and that will lead to sustainability. The GLASS eGovernance model will be based on the recent advancements of the domain, following a thorough state of the art analysis that will be conducted early at the beginning of the project. It will be constructed in a collaborative manner, by engaging various stakeholders of the domain, through the utilization of structured questionnaires and of face-2-face interviews, conducted by the consortium partners. The goal is to build a holistic, yet extendable model that is able to fulfil the needs of diverse stakeholders and that is in the position to be extended as needed to accommodate the requirements of other actors willing to join GLASS at a later stage. The consortium will work by constructing a set of supportive components, which altogether will be used to define and revise the proposed model to support an open ecosystem that can evolve and therefore can have varying needs and needs to comply with different regulations and norms. Thus, the project will introduce the GLASS Framework, which will incorporate and implement the aforementioned steps and means in order to deliver the GLASS eGovernance model.

In more detail, the GLASS Framework includes the following high-level conceptual components:

- A methodology for identifying emerging trends in the eGovernance domain that is relevant to the technological background envisioned in GLASS.
- A Legislation Analysis and Compliance method, which is responsible for mapping the legal requirements and the EC directives regarding data sharing, and eServices to the core innovations of GLASS.
- A Requirement Analysis method for analysing the needs and the requirements from the public sector, as well from the other collaborating actors such as citizens, businesses, NGOs, etc.
- An Adoption methodology that is providing the guidelines to interested stakeholders on how to become part of the GLASS ecosystem and integrate the model to their current operational processes.
- A Business Case and Sustainability plan that is used to accelerate adoption, highlight the benefits for participating organisations and define the value sharing principles for the overall ecosystem.
- The GLASS eGovernance model, which acts as the core output of the overall framework. It will be used to help the different organizations set their roles and responsibilities, standards, tasks, organizational structure, goals, mechanisms of control, when it comes to adopting the GLASS solution. It will also include an evaluation mechanism to optimize its internal processes and improve its efficiency with the help of the technological components of the system As such, the eGovernance model will be used not only to incorporate the GLASS technical solution into the boundaries of the organization but to streamline various processes that can witness a direct improvement with the appliance of GLASS. Furthermore, it will renovate existing standards and procedures, towards making the organization more cost-efficient, robust and interoperable with its environment, transforming it into a key player in the GLASS ecosystem, based always on the services it can offer. The GLASS eGovernance model is expected to be of dynamic nature, as there will be the need to constantly consider and eventually integrate new types of stakeholders, services and standards, therefore a feedback loop to the requirements analysis is designed, to re-trigger these operations that will result in upgraded versions of the model and its ingredients.

The aforementioned components will be implemented at the beginning of the project, deriving to the formulation of the GLASS eGovernance Model, that will be the main driver of the development activities of the different WPs that deal with the technical implementation of the proposed solution.

The GLASS solution builds on an adaptive eGovernance model that envisages to turn public administrations and public institutions open, efficient and inclusive, providing borderless, digital, personalised and citizen-driven public services. In turn, the GLASS eGovernance model is designed along four (4) core principles that enable a variety of innovative interactions among citizens, businesses and public authorities through an open, transparent, and secure approach. These core principles are:

- digital by default;
- once-only principle;
- transparent by design;
- interoperable by design.

Figure 8 illustrates these principles along with their enablers, as discussed in the rest of this section.

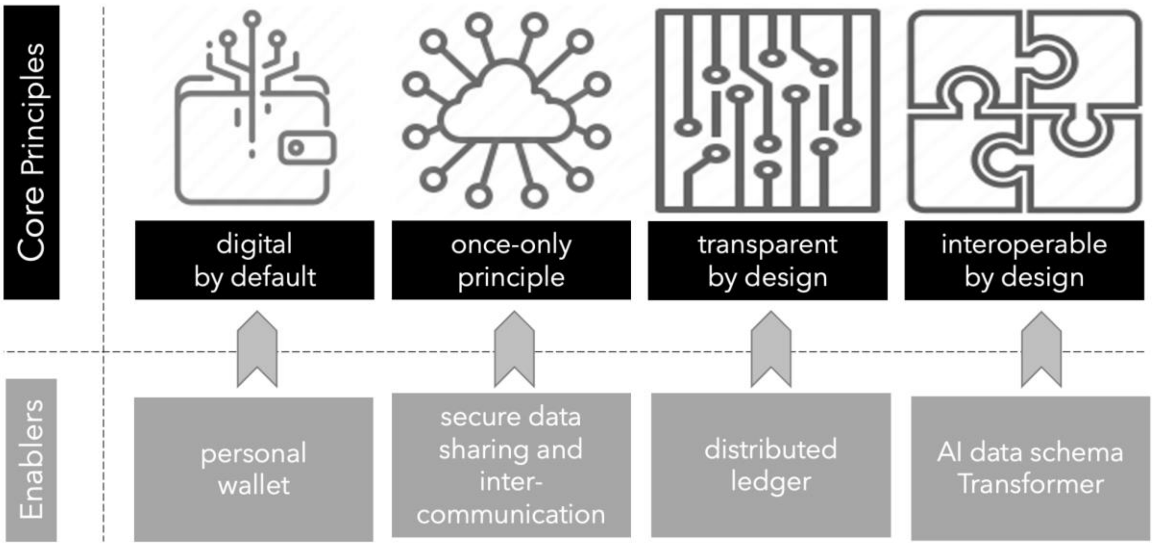


Figure 8: The core principles of the GLASS eGovernance model

4.2.1 Digital by Default

The digital by default principle focuses on turning the provision of services provided by government, authorities and private sector, including the interagency cooperation as well as the interactions with physical and legal entities, to be performed digitally, rather than physically and in person.

Towards digital transformation, digital by default principle represents the "being digital" concept that refers to service delivery offered by a government to its constituents through digital means, providing (i) Personalization, (ii) Enhanced User Experience and (iii) a Single Identity, meaning a point of interaction with public institutions and authorities.

The GLASS eGovernance model sets the pathway towards designing public services as distributed applications are deployed on high performance and secure environments and are openly accessible by the citizens and the business community.

A distributed application provides users with a personal wallet to perform a plethora of digital services, safeguarding the integrity of individuals' data shared between the operational stakeholders, while also managing sensitive information of users in a privacy-preserving approach. This application serves as the Single Identity and Point of Entrance in the Digital Service Marketplace.

4.2.2 Once-only principle

It is common for citizens and companies to provide the same information multiple times when interacting with public administrations. The once-only principle concept ensures that citizens and companies only have to provide certain information to a public authority and/or administrations only once. Therefore, public administrations will focus on reusing, or sharing, data and documents already supplied, in a transparent and secure way.

The GLASS eGovernance model offers secure data sharing and intercommunication functionalities, through which a user-centric identity management ensures that documentation and users' data including sensitive information is stored in a distributed file network that is easily accessible through a personal wallet. The once-only principle serves as a core component of the governance model, setting the baseline for the minimization of bureaucratic processes. It leads to:

- reduced citizens queuing;
- less administrative burden;
- increased efficiency;
- enhanced personal information protection, and
- less cumbersome communication across borders

4.2.3 Transparent by design

Transparency in the public sector refers to the ability of citizens to oversee the government. Transparency by design is a key characteristic of a modern, digital oriented governance model by ensuring transparency of the interactions among citizens and businesses with public authorities enabling democratisation and openness of the public administration services.

Transparency includes the visibility within the administrative environment that aims to allow public authorities, citizens and businesses to examine, interact and further understand administrative rules, data, and services.

In GLASS, every interaction among citizens, public authorities and businesses is safely recorded, following privacy standards and GDPR regulation, in a distributed ledger ensuring that information is distributed within the network. The network offers immutability, traceability and validity to the transactions, while the standardised format for each type of documentation does not allow users to issue the same documentation more than one time.

4.2.4 Interoperable by design

Interoperability in governments aims to establish a methodology in which different types of information to be exchanged among different systems, including the definitions of their semantics, are not determined a priori. Interoperability of systems by design focuses on the reusability of information and services that already exist and may be available from various sources, facilitating the cooperation among public administrations, citizens and companies.

Cutting edge technologies such as the **AI data schema Transformer** encompasses the EU well-established interoperability standards to produce an automated public Neural Network that serves a 'question & answering' middleware, enabling intercommunication among different types of systems, bridging interoperability gaps and providing EU organisations with a concrete step towards the adoption of EU-wide interoperability standards.

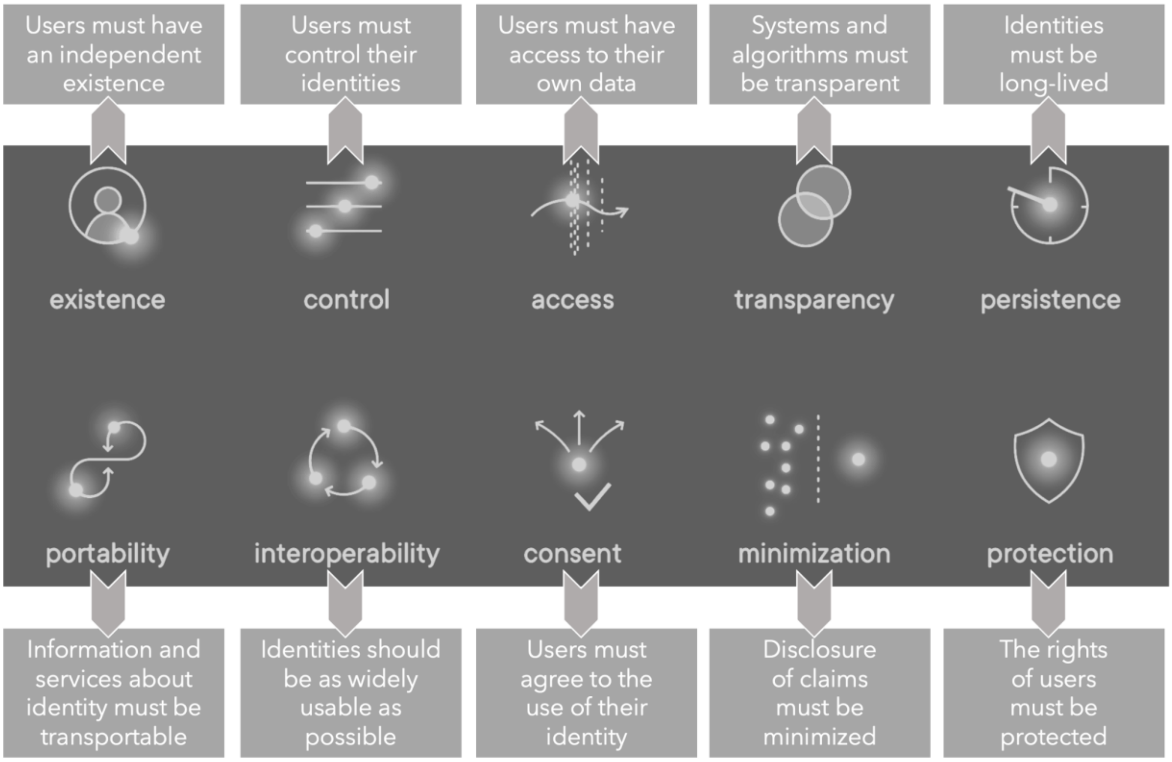

Users must have an independent existence
Users must control their identities
Users must have access to their own data
Systems and algorithms must be transparent
Identities must be long-lived
existence
control
access
transparency
persistence
portability
interoperability
consent
minimization
protection
Information and services about identity must be transportable
Identities should be as widely usable as possible
Users must agree to the use of their identity
Disclosure of claims must be minimized
The rights of users must be protected

Figure 9: The 10 principles of self-sovereign identity (based on a figure appearing at https://jolocom.io/blog/a-universal-identity-layer-we-can-only-build-together/)

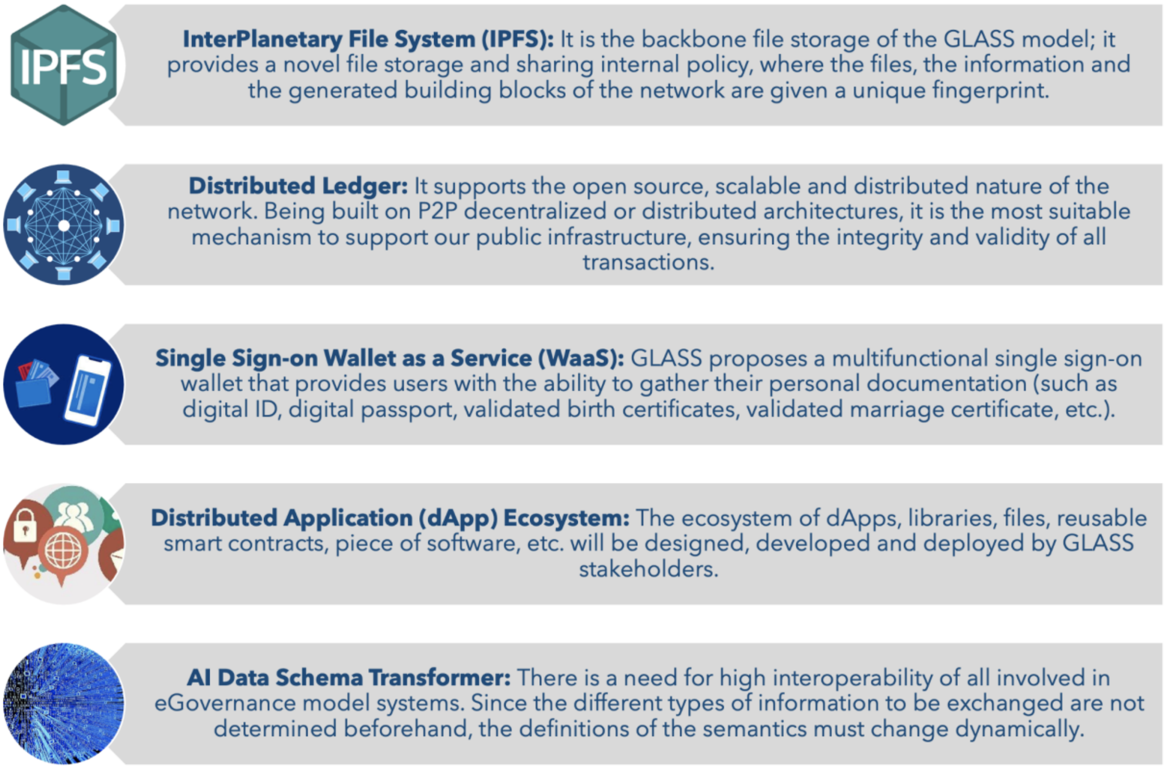
4.2.5 Self-sovereign identity

In addition to the four core principles presented above, GLASS contributes to a wider adoption of decentralised identifiers for eGovernment services by adhering to the Self Sovereign Identity (SSI) paradigm (Figure 9), where users are able to manage their own identity in the absence of a centralised coordinating authority (Mir, Kar, & Gupta, 2021). SSI is a term defining a novel way of thinking about identity; it has been defined as a model of digital identity where individuals and entities alike are in full control over: (i) central aspects of their digital identity, including their underlying encryption keys; (ii) creation, registration, and use of their decentralised identifiers; (iii) control over how their credentials and related personal data are shared and used (Jolocom, 2019). SSI aims to reduce the administrative costs, automate and fasten the transactions among its users, while delivering new ways for users to manage their privacy and waive the need for multiple logins.

Through the adoption of the SSI paradigm for **identity management**, GLASS offers a secure cross-border network for public service delivery, where users control their own identity. It provides direct access to citizens and businesses to public services through the GLASS ecosystem of distributed applications that support document sharing, identity authentication, information exchange, transaction monitoring and validation. Users can access the services of the GLASS network after proving the ownership of specific attributes demanded for each transaction. This is achieved through digital identifiers stored in the decentralised file system and managed through the wallet, so that users can decide what information is used, how it is processed and with whom it is shared.

4.3 Technical Solution Overview & Conceptual Architecture

The GLASS eGovernance model creates new digital governance pathways through the integration of emerging technologies and breakthrough cross-sector services. It deploys decentralised applications to deliver efficient, reliable and secure data sharing, auditing mechanisms and communication channels for the eGovernment sector. Figure 10 provides a brief introduction of the key technologies integrated in the GLASS eGovernance model.



InterPlanetary File System (IPFS): It is the backbone file storage of the GLASS model; it provides a novel file storage and sharing internal policy, where the files, the information and the generated building blocks of the network are given a unique fingerprint.

Distributed Ledger: It supports the open source, scalable and distributed nature of the network. Being built on P2P decentralized or distributed architectures, it is the most suitable mechanism to support our public infrastructure, ensuring the integrity and validity of all transactions.

Single Sign-on Wallet as a Service (WaaS): GLASS proposes a multifunctional single sign-on wallet that provides users with the ability to gather their personal documentation (such as digital ID, digital passport, validated birth certificates, validated marriage certificate, etc.).

Distributed Application (dApp) Ecosystem: The ecosystem of dApps, libraries, files, reusable smart contracts, piece of software, etc. will be designed, developed and deployed by GLASS stakeholders.

AI Data Schema Transformer: There is a need for high interoperability of all involved in eGovernance model systems. Since the different types of information to be exchanged are not determined beforehand, the definitions of the semantics must change dynamically.

Figure 10: Key technologies in GLASS

As illustrated in Figure 11, the individual modules of the proposed solution are designed to be built on top of the IPFS and a distributed ledger. This extended combination of distributed technologies and infrastructures constitutes the backbone of the GLASS solution, which is capable of efficiently addressing the complexity of the processes, providing at the same time the security, trustworthiness, immutability and auditability required by contemporary public services.

By combining functionalities enabled by Distributed Ledger Technologies (DLTs) and IPFS, the GLASS solution allows users to control their data without compromising security or limiting third parties to provide personalised services. IPFS has specific features that remedy the performance issues of dApps, improving their performance through an ad hoc engagement of existing computational and storage resources. These features include: (i) content indexing, (ii) hash lookup, (iii) distributed naming system, (iv) persistence and clustering of data that reduce latency, (v) decentralised archiving, and (vi) compliance with privacy regulations.

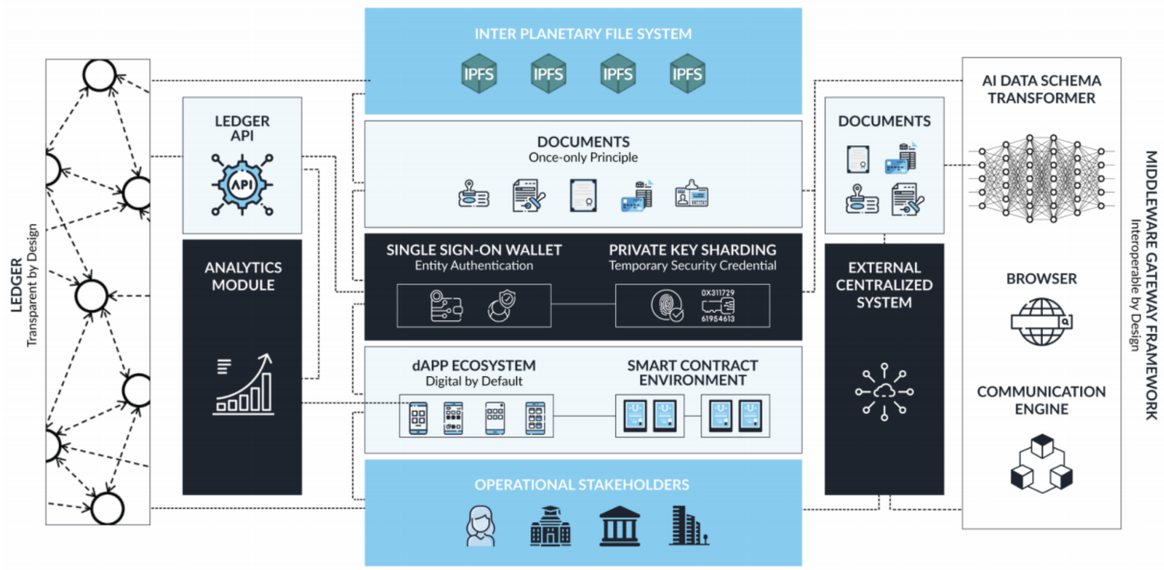


Figure 11: The architecture of the GLASS solution

The public ledger stores the users' digital identities, access consent logs, and selected authentication transactions. It co-supports the public sharing resource infrastructure, providing the IPFS with advanced operational and technological capabilities, starting from security and privacy, up to immutability of transactions. It is located at the heart of the network to monitor and continuously record every approved interaction among the users' nodes. One of the major challenges is how to overcome the public nature of the ledger to ensure the security, privacy and anonymity of information. Towards this direction, GLASS proposes a combination of private and public keys to exchange information among end-users and services. In this way, a service does not observe raw data; instead, it runs its computations directly on the network and obtains the final results only after the consent of the user. GLASS uses DLTs since, from the data safety, authenticity and non-repudiation point of view, they provide an easily accessible and immutable history of all contract-related data, adequate for building applications with trust, accountability, and transparency.

The dApps are used to deliver dedicated services to users. They comprise smart contracts and are hosted in the nodes of the distributed network. The overall performance and storage capacity are increased through the participation of new nodes joining the network. GLASS renders legal and regulatory decisions simple, since law and regulations are programmed by smart contracts in the network and are enforced automatically, while the ledger acts as legal evidence for storing such data.

A single sign-on Wallet is responsible for managing multiple services provided by various dApps, such as document sharing and information exchange, enabling a single sign-on user-centric document repository. This tool allows stakeholders to manage and share their personal and sensitive documents among different application environments in a single management kit, which can function in a fully distributed way, without a single point of failure. Hence, providing resilience and a continuum of service.

In addition, a middleware layer includes:

- a Secure Gateway Channel on-the-fly to assure a secure intercommunication among systems, databases, apps, etc.

- an AI Data Schema Transformer, which is based on well-defined libraries and AI models and encompasses the EU interoperability standards to effectively identify and transform data schemas, models and structures, and enable machine-to-machine communication among different types of systems across the EU. Synthetic data collections that map and simulate real data types (i.e., citizens ID, passport, birth certificate, criminal record, etc.) for different EU countries provide the backbone of this module's perception
- a Transactions-based Analytics Module that runs as a back-end service on the network, gathering transaction histories and providing insights to users through an appropriate interface
- a Browser Service Module that acts as a search engine and facilitator of the network and other modules (i.e., the dApp ecosystem), providing users with diverse functionalities (locate files, documentation, services, entities, etc.) through user-friendly interfaces.

This extended digital service availability enables any physical and/or legal entity (such as public administration, business and citizens) to integrate their own external centralised system in the network, enabling interoperability between users, cross-border and cross-sector organisations.

To effectively satisfy the desired interoperability by design principle, GLASS deploys a machine learning based environment that automatically recognizes data structures in existing centralised systems. Specifically, GLASS applies the notion of smart data structures by employing deep learning techniques to recognize and transform data schemas, data structures and data types. GLASS applies data fusion techniques to meaningfully integrate heterogeneous information from multiple data sources that would otherwise remain uncorrelated and unexploited. To build a highly tuned system tailored to the specific needs of eGovernment services, GLASS identifies the data distributions and examines possible optimizations in the index structures to identify data patterns.

Such a holistic framework creates a novel eGovernance mechanism for communication, data sharing and information retrieval among centralised systems and decentralised/distributed applications. Stakeholders are able to use the single sign-on Wallet and the individual modules running on the network, while also having unrestricted access to the dApp ecosystem. This ecosystem hosts different dApps for each distinct service supported by the network, which are custom designed and deployed to meet the needs of the end users. The functionalities and the interdependencies of the dApps are formulated and defined with the use of dedicated smart contracts and user interfaces, hosted under the ecosystem. The dApp ecosystem includes libraries of commonly deployed smart contracts, enabling their reuse and activating users/developers to build and deploy their own applications. Finally, the distributed file storage architecture gives the opportunity to stakeholders to host their own custom applications in the network, thus contributing to its expansion and scalability.

4.4 GLASS Technical Description

Public Distributed Infrastructure: The baseline where GLASS components are built is the Peer to Peer (P2P) network architecture. A number of participants (nodes) that join in an open network, have equal functionalities, equally share the computational workload of the services without a central management authority among them. GLASS aims to combine the functionalities of an unstructured P2P network (IPFS) and a distributed ledger into a single framework.

InterPlanetary File System (IPFS): IPFS includes a public governance model and a distributed public file storage network under the same umbrella. By establishing IPFS as the backbone file storage of the GLASS model, we provide a novel file storage and sharing internal policy, where the files, the information and the generated building blocks of the network are given a unique fingerprint, called the cryptographic hash. IPFS gives the opportunity to users to search files and documents by its content, instead of the traditional approach where the documents are searched by the location of the server. A major advantage of this distributed approach is that it enables functionalities such as downloading files directly from network's nodes which are not centrally managed by one organization. When a node looks up for files to either view or download, the request to the network is to search for the nodes that are storing the content behind that file's hash. Each network node (citizen, business, public administration) stores only content that it is of interest, along with some indexing information that helps to outline what is stored and in which node, as Figure 12 demonstrates. The data within the network (which also uses the IPFS protocol) has a content identifier (CID), acting as the hash. The hash is unique to the content that it came from. CID acts as the label that locates files within the IPFS.

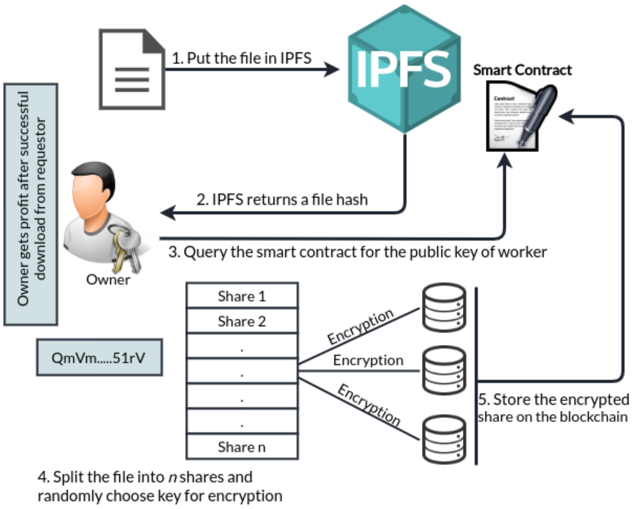

1. Put the file in IPFS
IPFS
Smart Contract
2. IPFS returns a file hash
3. Query the smart contract for the public key of worker
Owner gets profit after successful download from requestor
Owner
QmVm.....51rV
Share 1
Share 2
Share n
Encryption
Encryption
Encryption
5. Store the encrypted share on the blockchain
4. Split the file into n shares and randomly choose key for encryption

Figure 12: IPFS file storage process

More specifically, it forms a certain type of address based on the content of the file, neither the location nor the size. CIDs are the original content's hash. Consequently, (i) any differences in content within a file should produce a different CID and (ii) if a file with exactly the same content is added to two different IPFS nodes using the same settings, they should produce exactly the same CID. Hashes identify content and IPLD[5] translates the data between data structures, provided by different distributed systems. Regarding data structures, IPFS turns files into Direct Acyclic Graphs (DAGs[6]), similarly to other distributed systems. More specifically, IPFS uses Merkle-DAG, which is the state of art practice for representation of directories and files. To construct a Merkle-DAG representation, IPFS splits the content into blocks. By splitting the content into blocks, we are able to collect the file in parts from different sources, in a similar way as the BitTorrent[7].

Distributed Ledger: The distributed ledger will support the open source, scalable and distributed nature of the network, providing complementary functionalities and benefits

[5] https://ipld.io/
[6] DAG is a finite directed graph that consists of vertices and edges with no directed cycles
[7] https://www.bittorrent.com/

to the IPFS. Ledgers can only be built on P2P decentralized or distributed architectures, thus making it the most suitable mechanism to support our public infrastructure, by ensuring the integrity and validity of all the transactions. The back-end module of the validation ledger technology will use an energy-efficient consensus protocol. It will be customly designed to match the authenticated data sharing needs of the project (deployed on GLASS' P2P network) under the same nodes which host the IPFS protocols, presenting a hybrid distributed/decentralized public infrastructure. The consensus protocol will define the sequence on which the nodes will validate the transactions, thus the time/speed that the network reaches consensus. The development of the back-end validation ledger will be built based on open-source platforms and methodologies (e.g., Hyperledger Fabric, Ethereum, Hedera Hash graph), providing and delivering high degrees of confidentiality, resilience, flexibility, and scalability. In the case of Hyperledger Fabric we can ensure the existence of an immutable ledger, where the data is tampered-proof, trust-worthy, easily audited, configurable and publicly available, preserving in this way the privacy of the user. The ledger will only hold hashes and proofs of transactions, while the original data, information and/or documents will be stored distributedly in the network. The consensus mechanism for the documentation exchange will be structured on a proof of authentication protocol.

The ledger will include a Membership Service Provider (MSP) component that will offer user-node authentication and validation before joining the network, cryptographic mechanisms and protocols for issuing and validating certificates. The ledger will also offer the capacity for creation of channels and private data collections, allowing groups of participants to create separate ledgers for transactions (sharding). By combining such distributed mechanisms and systems within the same network we leverage the advantages of the Distributed Ledger Technology (DLT), (e.g., immutability), enabling and maintaining at the same time the role of the log file of all internal events/transactions, the storage, functionality and operation capacity provided by the distributed file storage system.

All the requests from/to a node, either citizen or business will be stored in the ledger in the form of a hashed-log event, timestamped transaction. All the documents, circling around the network will be double encrypted and stored in the distributed IPFS storage infrastructure. This data will be reflected to the validation ledger by a series of hashing and encryption methodologies such as pointer encryption and cryptographic hash functions for messaging authentication.

The GLASS ledger initially will provide stratified access only to consortium partners, maintaining the control of the ledger. As the implementation progresses, other involved parties, authenticated by the GLASS consortium, will be allowed to join the network, share computational resources and services, espouse the IPFS protocols to download and upload data to the public infrastructure, and eventually read and write to/from the ledger. This approach will prevent malicious users from joining the network.

Single Sign-on Wallet as a Service (WaaS): GLASS proposes a multifunctional single sign-on wallet that will provide users with the ability to gather their personal documentation eg. digital ID, digital passport, validated birth certificates, validated marriage certificate, etc. In general terms, the single sign-on wallet as a platform will manage users' transactions from interactions with multiple services delivered through dedicated dApps which are hosted under GLASS' ecosystem, designed by public authorities and private organizations designed to meet the specific needs of citizens. The wallet offers citizens permission to decide what information to share, with whom and when.

GLASS' WaaS transforms the day-to-day internal protocols of public bodies as well as their daily interaction patterns with large numbers of citizens who request their public services, enabling a two-way digital interaction path, without central authorities, making citizens owners of their personal data. The wallet's distributed services will be controlled by an integrated web-based interface, designed according to Web Accessibility Directive standards, to enable the participation of all relevant communities including elderly people, people with disabilities and migrants. Its background services will directly communicate with the backbone infrastructure mechanisms and IPFS protocols, i.e., hash tables, file tables, content identifier and transaction record.

As the definition suggests, the single sign-on module becomes a critical part of a complex and distributed environment, where multiple services from various providers are hosted. The single sign-on extended capacity that will provide access to multiple dApps, running in parallel, will be given through a distributed single sign-on API. The single sign-on API provides simple username and password management, improved identity protection, increased speed where it is most needed, security risks reduction, providing in this way the maximum user-centric experience. Also includes functionalities such as, password grant (sign-in directly on the web), authorization code grant (user authorizes third-party), implicit grant (third-party web app sign-in), web services API that can effectively authenticate requests, seamless user authorization experience on client-side technology (Web, Mobile or IoT). The functionalities of the wallet will be enhanced by the Unified Digital Identity Device (UDID), which is a hardware device that uses a random variance to generate a sequence of reconstruction of private keys and bit-padding.

The request or push of information from/to a public administration requires firstly the identification of the user and as a second step his/her authorization. GLASS introduces a private key generator mechanism that leverages sharding methodologies to split private keys into pieces and distribute them within the network. Sharding refers to a method of splitting and storing a single logical dataset in multiple databases. Each subkey is held on a separate node to spread the workload and increase security. Specific data related to key identification can remain present in all subshards, while some can appear only in a single shard. Each shard acts as a single source for this subset of data. In GLASS, sharding will be applied, rendering each shard useless unless enough are assembled to reconstruct the original key. In this way, we ensure that private keys remain completely secure and secret during the cross-chain mapping process. No authentication data will be stored in the wallet, local or mobile devices (e.g., computers, mobile phones, hard drives, etc.), to protect users and avoid possible loss of personal information either from malicious bypassing or human errors (loss of mobile phone). User's initial authentication and subscription in the WaaS platform will be performed either by physical presence in authorized public administrations or by digital means, through a dedicated dApp, where users can provide and verify their personal information to successfully join the network and obtain their credentials. Every time a dApp requests to share personal documentation or data, towards the completion of the transaction, users should follow the three-step authentication protocol to verify his/her identity and provide her consent through a push notification in a predefined device, increasing the efficiency of digital transactions while eliminating possible frauds. Therefore, we achieve to design a service that can be used for delivering services of public administrations and businesses, minimizing the data generated as well as the internal processes of the organization, maximizing at the same time the capacity of the network.

Distributed Application (dApp) Ecosystem: The ecosystem of dApps, libraries, files, reusable smart contracts, piece of software, etc. will be designed, developed and deployed by the GLASS stakeholders. DApps are basically pieces of software that run on a distributed protocol. Because of the distributed architecture of the network, dApps share the burden of the computational load for their services with multiple nodes, thus providing a continuum of service without a central point of failure. Compared to centralised applications, dApps are more reliable, in terms of scalability and security. A dApp stores data in a decentralised database and uses decentralised computing resources to work. In that way, if a node that is running a particular application goes down, another node can resume the task, providing a continuum of service. GLASS' ecosystem challenges research questions towards the establishment of a public environment where business and public administrations work closely to develop dApps to deliver services and organize their internal protocols and bureaucratic procedures.

Smart Contracts: Smart contracts will be utilised to support and define the functionality of each dApp. A series of "101" lessons, basic JavaScript dApps, interfaces designed in React, libraries, best practises, coding workshops and already running smart contracts, among others; will support the functionality of the dApp ecosystem, ease the process and adaptation of the users, providing the technological skills needed for custom dApp development.

Middleware Enhanced Service Suite: To supplement the individual technological components, a middleware set of services is designed to enhance the performance of the overall GLASS framework, providing the extra features which lead to the operational functionalities that the GLASS eGovernance model will deliver. The Middleware Enhanced Service Suite consists of the following modules: (i) Communication engine on the fly, (ii) AI data schema Transformer, (iii) Browser Service Module and (iv) Transaction Analytics module.

Communication Getaway Channel on the fly: This channel is responsible for establishing secure communication channels, on the fly (ad hoc), between different structure-based systems, e.g., public authority centralised system - decentralised transaction ledger. This functionality enables the gradual adaptation of the distributed governance methodology, while providing documentation handling services, such as uploading, downloading and sharing of documents requests from the users to the IPFS.

AI Data Schema Transformer: There is a need for high interoperability of all involved in the eGovernance model systems, in order to create a multidimensional, hybrid architecture that can be adaptive to the specific needs of public administrations. Since the different types of information to be exchanged are not determined a-priori, the definitions of the semantics have to change dynamically. The main barrier for interoperability is related to the dimensions of heterogeneity, which include: (i) data, (ii) middleware, (iii) software and (iv) non-functional heterogeneity. Our approach aims to address this challenge through the use of Machine Learning techniques on data structures. The AI Data Schema Transformer will act as a middleware component that will identify the representation of data from existing centralized systems and will create an adaptive learning index that will allow the interoperability of the current systems with the proposed distributed network. We will take into account new aspects of the sharing of the data and the processes, such as the understanding of the data and the processes, the access security, and owner rights, to create an adaptable standard model capable of integrating the requirements of the models of the different components.

4.5 Actors and Roles

4.5.1 Citizens

GLASS as an eGovernance paradigm aims to become more responsive to the needs of the citizens, ease the interaction of citizens with governments and increase the participation of citizens in public policies. GLASS is designed to maintain a common methodology, providing a similar user experience whether dealing with the Public Sector, Private Sector or other citizens.

In GLASS, the citizen is placed at the centre of its own data, attributes and evidence (Figure 13). No matter who the citizen liaises with, the citizen can choose what information is released to its counterparty.

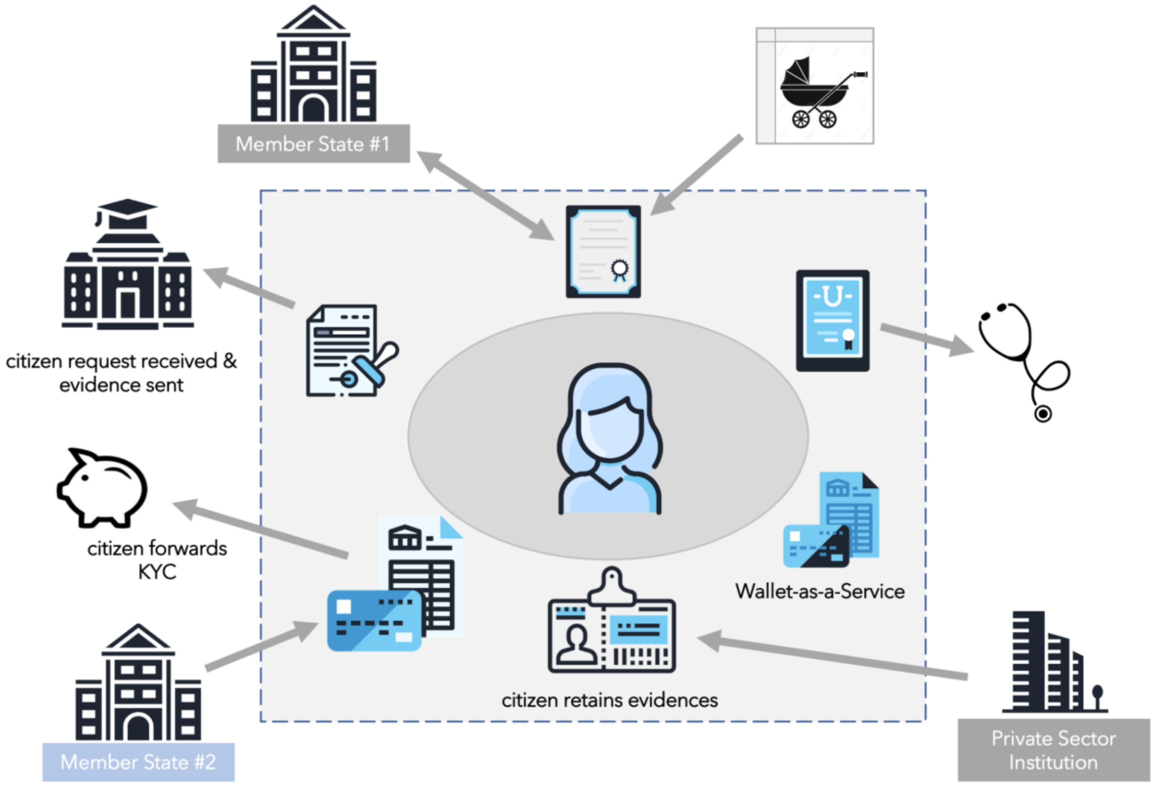

Member State #1
citizen request received & evidence sent
citizen forwards KYC
Wallet-as-a-Service
citizen retains evidences
Member State #2
Private Sector Institution

Figure 13: The Citizen at the centre of its data

GLASS supports the inclusive by design policy of the EU and addresses the different needs of EU citizens of special groups, such as elderly, people with disabilities or people with limited digital knowledge.

GLASS will provide services to people who have limited online presence, increasing the overall number of participants in the network, thus improving the user experience for everyone and delivering more services, more often. The overall solution takes into consideration the main obstacles that prevent citizens from digital services, which are the ability to actually go online, the ability to use the Internet, as well as the lack of motivation and trust to use digital services; and offers these services through easy-to-use, user-friendly mobile apps.

4.5.2 Government

GLASS introduces a citizen-centric eGovernance model for public administration services, which automates the processes and safeguards the integrity of interactions among citizens, businesses and public authorities.

In addition, GLASS introduces a new paradigm for evidence and record transfer. The project designs, implements and thoroughly assesses a single sign-on Wallet as a Service (WaaS) platform that interconnects distinct distributed applications (dApps) responsible for ID authentication, document sharing, information exchange and transactions validation, in compliance with the Single Digital Gateway (SDG) guidelines, enabling a single point of access to information, without a single point of failure in the services.

GLASS considers the eGovernment Action Plan 2016-2020. The proposed underlying mechanisms makes GLASS interoperable with existing and newly developed centralised applications and systems. By these means, all interactions among citizens, businesses and public authorities become transparent under a trustworthy and secure environment, while clear guidelines are set for citizens’ data ownership.

The goal of GLASS is to make public administrations and public institutions open, efficient and inclusive, providing borderless, digital, personalised and citizen-driven public services for the EU population.

4.5.3 Business

The 24.5 million SMEs in Europe, representing 99% of European businesses and providing €1.4 billion in value added services, form a very large and mostly homogenous attack surface that cyber-criminals find irresistible. Over 22 million of these (classified as ‘Micro’ SMEs or MEs) are the backbone of Europe's economy. In the past five years, they have created around 85% of new jobs and provided two-thirds of the total private sector employment in the EU. The European Commission considers SMEs and entrepreneurship as key to ensuring economic growth, innovation, job creation, and social integration in the EU.

These private sector organisations interact with the citizens or the public sector. They participate in the ecosystem by sharing information and documents with the requesting parties (public sector, citizens) or by requesting/verifying evidence from them. As in the case of citizens, a company in GLASS is placed at the centre of its own data, attributes and evidence (Figure 14). No matter who the company liaises with, it can choose what information is released to its counterparties.

GLASS can improve efficiency in managing company documentation especially when operating in an international market. It can also save time when entering formal public procurements and will offer businesses certification and notarisation efficiencies when companies can hold their own notarised evidence.

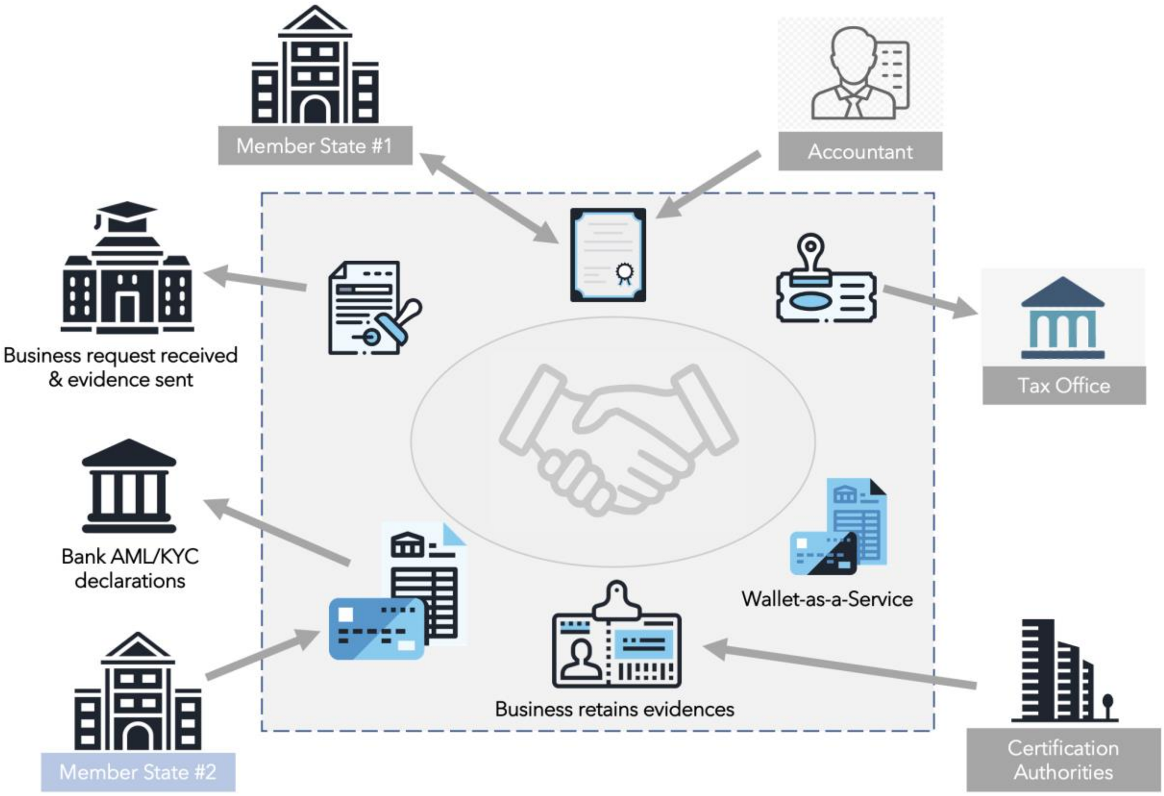

Member State #1
Accountant
Business request received & evidence sent
Tax Office
Bank AML/KYC declarations
Wallet-as-a-Service
Business retains evidences
Member State #2
Certification Authorities

Figure 14: The Company at the centre of its data

5. GLASS demonstrators (application scenarios in local administration)

The pilot scenarios considered to enable use case creation were three (3) real case scenarios concerning paperless cross-border bureaucratic processes. The first one covers the case where an individual wishes to move to a foreign EU country for working or educational purposes. The second scenario covers the case of the short-term, cross-border moving (e.g., short-term work, education, traveling) of marginalized people such as elderly, disabled people etc., demanding special treatment and special services to facilitate their moving. The third scenario demonstrates the GLASS solution for validation of the education achievements by an employee seeking to hire young individuals.

For every case, a persona is introduced, and the actors that play a part in is shown. For every persona, along with their profile, their motivation for using the GLASS solution and frustrations with the traditional methods are given. Their current situation is also written. In the case of scenario #2, persona's health conditions are noted alongside other information.

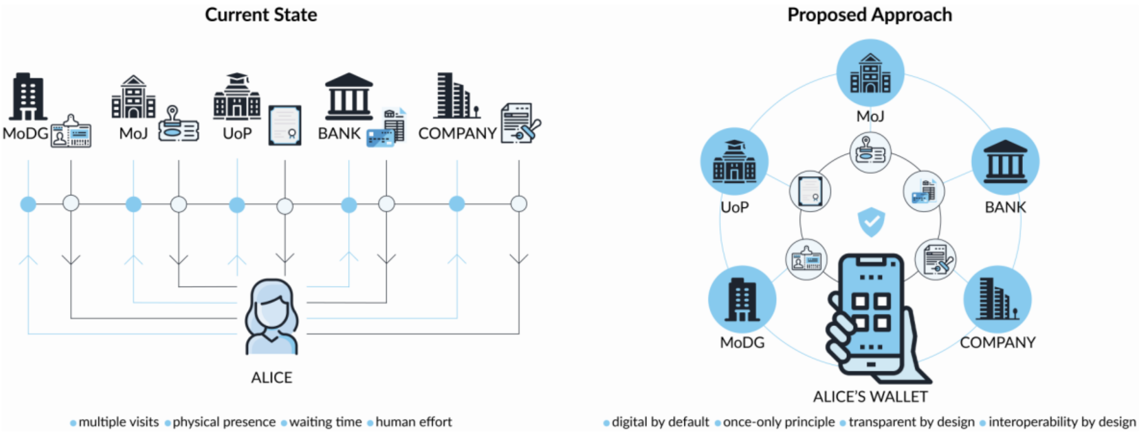


Figure 15: Current state vs. The proposed approach

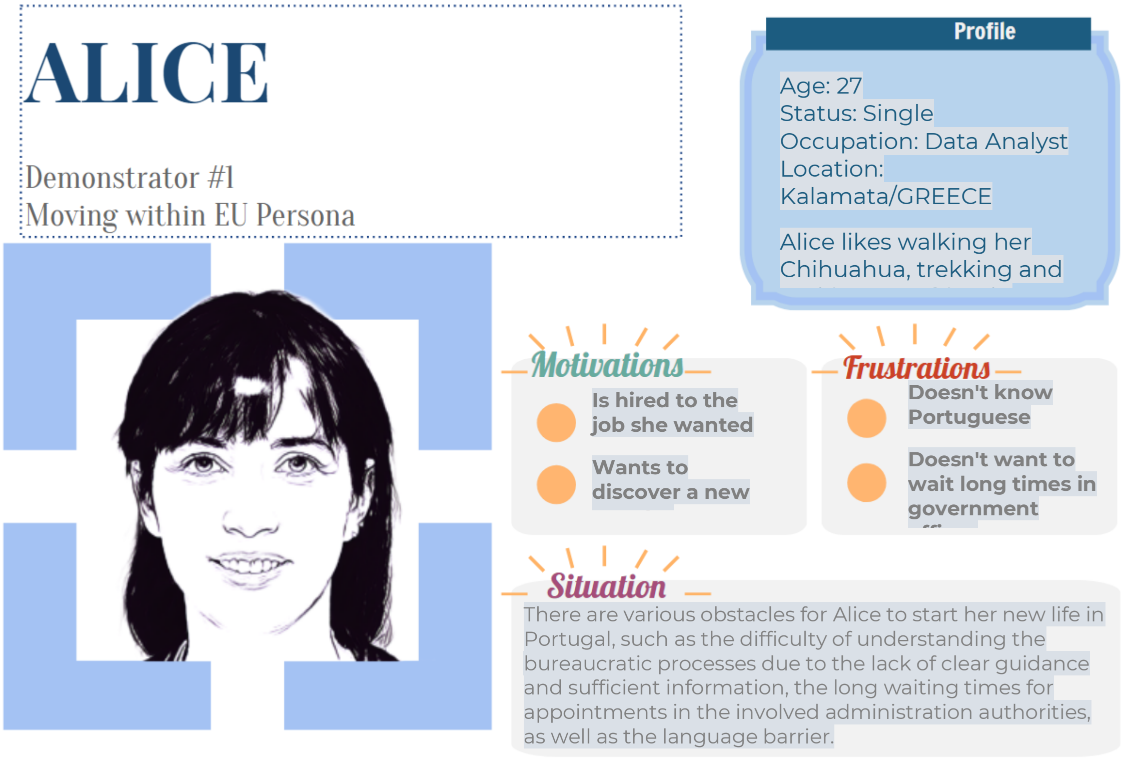
5.1 Demonstrator #1: Alice goes to Portugal #1: Alice

Motivation: There are several advantages from moving abroad for a certain period for study or work purposes, such as better career prospects through professional and educational advancement, development of a global network of contacts, cultivation of cultural awareness and a global mindset, learning of a new language or making new relationships, to name a few. The EU offers significant opportunities to anyone wishing to move abroad and promotes fair employment conditions for all, as part of the European Pillar of Social Rights, since working mobility enables employment and labour force to adapt to the ever-increasing challenges in economy, migration and society within all Member States. Every citizen of the EU has the right to work and live in any Member State without being discriminated on grounds of nationality; this is declared as a fundamental freedom guaranteed by the Treaty on European Union (art. 3, 39, 40) and Community law. However, moving abroad can be a highly demanding and cumbersome process in terms of bureaucratic processes and associated paperwork. There are various obstacles for someone willing to move to a foreign country to work legally and obtain all the relevant documentation, such as the difficulty of understanding the bureaucratic processes due to the lack of clear guidance and sufficient information, the long waiting times for appointments in the involved administration authorities, as well as the language barrier. The goal of this demonstrator is to create an innovative user-centric system that simplifies the bureaucratic processes for citizens, businesses and public administrations, validates the effectiveness and efficiency of the GLASS technology, and provides easier moving pathways towards the EU Digital Single Market. It is worth mentioning that all the documents to be stored and the distributed procedures to issue such documents will support the policies of the European eGovernment Action Plan 2016-2020 and all the associated priorities, including the Digital by Default, Openness & Transparency and Once-only priorities.

Problem Setting: Starting from Greece, Alice finds a vacant job position in Portugal. She applies for the job and thankfully she gets hired. Unfortunately, in Portugal, she has to deal with a series of bureaucratic processes in order to issue the obligatory ID card and social security number, open a bank account etc.; for each of these processes, she needs to provide a proof of ID as well as a pile of documentation (from Greece) stamped and authenticated by both Portugal and Greek Authorities. To obtain a Portuguese Residence title, rent an apartment and open a bank account, she needs to present at least a validated ID documentation, birth certificate, a nationality certification validated by a Greek Authority and proof that she works in Portugal. Obtaining these documents manually is certainly a time-consuming effort. For instance, consider the case where the Portuguese authority demands Alice’s birth certificate to issue a social security number. Adopting the GLASS solution, in case the document will be issued for the first time, Alice will request from the Greek Authority the validated data. The ministry will issue the document with the validated data, and Alice will give the permission to forward it to the Portuguese Authority. On the other hand, if this type of documentation has been previously issued, the Portuguese authority can obtain it directly from Alice through her Wallet which stores all the necessary information. After this transaction is completed, Alice can access and securely share her Portuguese social security number through her Wallet. Now, the employer can directly get the validated social security number from the Portuguese Authority, after her approval, to register her credentials to their internal payroll system that demands a social security number from all employees. All data in the previous transactions are encrypted and decrypted using state of the art encryption mechanisms in alignment with the European guidelines for privacy protection. Using a dApp of the GLASS ecosystem, Alice can use her validated digital identity through the Wallet to request remotely the required documentation from the respective Greek Authority, the Portuguese Authority and her employer. The Greek Authority will digitally issue and validate the documentation and instantly push encrypted data into the distributed network, while the transaction among the users will be recorded. All the transactions, including requests, notifications, and permissions are monitored and stored protecting Alice’s privacy. Through the personalized Wallet, each individual can provide any authority with access to the relevant documents, which are

stored in the secure and privacy preserving IPFS infrastructure of GLASS always with the approval of the user.

Added Value: Several actions need to be carried out when moving to a foreign country for a new job, such as obtaining a valid visa and a permit, and exchanging the relevant documents with employers. Most likely, there are things that one cannot do until registering, including opening a permanent bank account and signing a contract to rent an apartment. In many EU countries, a Social Security Number (SSN) is required before signing a rental contract such actions are usually hard to get accomplished, not in terms of legislation, but because of the several visits people have to make to the relevant public authorities, such as the police station or the municipality office. Using the wallet proposed in GLASS, individuals will be able to easily share all the required documents and information needed to obtain a SSN with the relevant authority through a mobile app, increasing in this way the efficiency of the government services, tackling the language barrier and reducing the number of the physical visits and associated long waiting times. After successfully getting a job, the HR representative of the organization will need to obtain the identified documents to proceed with the hiring process. With GLASS, employees will have the ability to provide and/or revise their required document through a mobile app, minimizing the chance of forged documentation, enhancing the transparency and security of information exchange in accordance with the relevant legislation and decreasing the overall waiting time. Opening a bank account or renting an apartment can be highly demanding in terms of legal paperwork since in many cases there is a request to deliver the economic or criminal profile of the individual, a process that requires cross-border exchange of information. Through the use of the GLASS service, the bank or the owner of the apartment can request the specific paperwork directly from the user’s wallet and the user can provide the link to the uploaded document stored in the IPFS network directly and securely. Every transaction is stored in a public blockchain to enhance the security of information and eliminate any forgery attempts.



ALICE

Demonstrator #1
Moving within EU Persona

Profile

Age: 27
Status: Single
Occupation: Data Analyst
Location:
Kalamata/GREECE

Alice likes walking her Chihuahua, trekking and

Motivations

- Is hired to the job she wanted
- Wants to discover a new

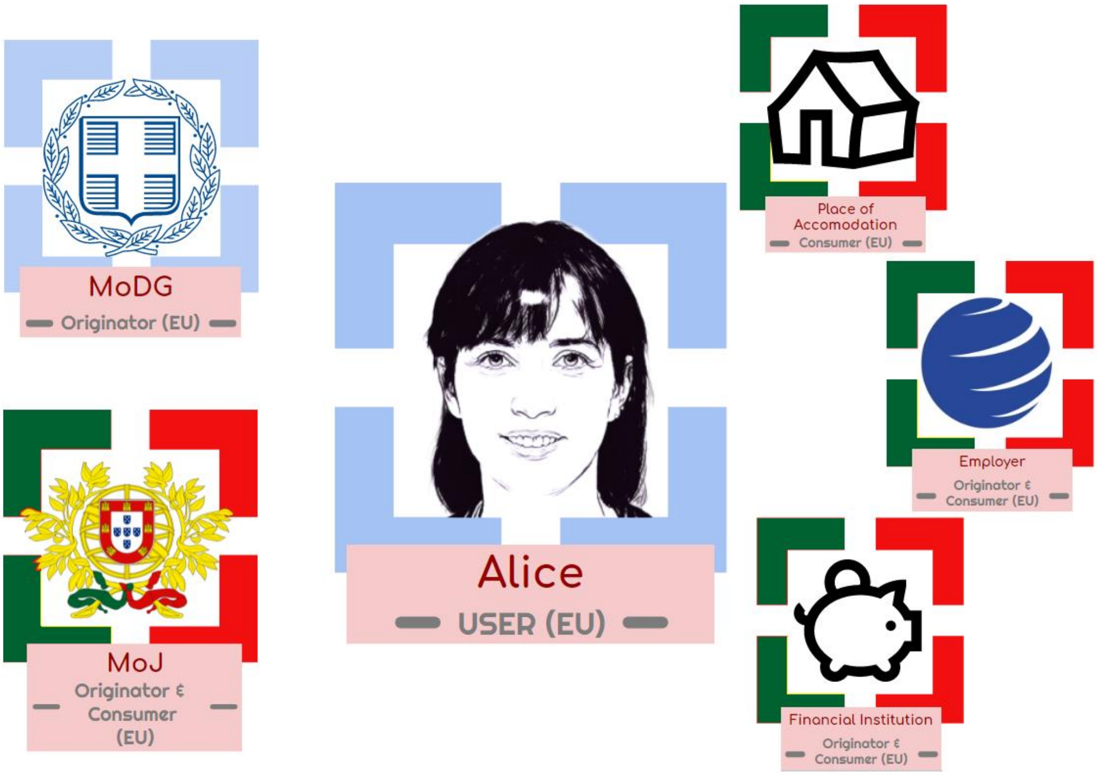
Frustrations

- Doesn't know Portuguese
- Doesn't want to wait long times in government

Situation

There are various obstacles for Alice to start her new life in Portugal, such as the difficulty of understanding the bureaucratic processes due to the lack of clear guidance and sufficient information, the long waiting times for appointments in the involved administration authorities, as well as the language barrier.

Actors:



Alice downloads the Wallet app

- Alice needs to obtain a Portuguese Residence title, rent an apartment and open a bank account in Portugal.
- Her new workplace recommends using GLASS wallet for gathering the required documents and applying.
- Thus, she registers her account using her identification documents.

Alice gathers information about required documents

- Alice gets an initial list from the employer and finds out she can easily apply to these documents through GLASS.

Evidence List:

- a proof of validated ID documentation
- birth certificate
- a nationality certification validated by a Greek Authority
- proof that she works in Portugal

Alice applies for documents in Greece

- Alice logins to her wallet, and she logins to the Greek Authority's API using her Greek Tax Credentials.
- She requests her ID, passport, birth certificate, nationality certificate from the Greek Authority.
- For the Employment Proof, Alice decides to upload her offer letter from the employer to her wallet.

Alice receives her documents

- Alice receives a notification that her documents are ready.
- Alice opens her wallet and saves the documents to her wallet.
- While she is browsing through the Greek Authority site, she decides to request her criminal records, school records and medical history, just in case.

Alice applies for Social Security Number in Portugal

- Now that Alice has gathered the initial documents, Alice is ready to apply for social security number she needs in Portugal.
- She opens her wallet, and creates a smart contract, attaches her ID, birth certificate and employer's offer letter and issues this to the Portuguese Authority. After this she connects to the Portuguese Authority's API and uploads her nationality certificate to complete her application.

Alice receives second batch of evidences

- Alice then gets another notification that her other documents are ready.
- She saves her evidences in her wallet.
- She also receives the notification that her social security number is ready and she can forward this to her employer to register her credentials to the payroll system.

Alice finds a rental house and opens bank account

- Alice finds a cozy apartment with ocean views while searching.
- To rent this apartment, she needs a few documents, as well as a bank account in Portugal.
- She goes to the bank and is again asked for her ID and Social Security Number. As she already has those in her wallet, she opens her account easily.

Alice rents the apartment

- The owner of the apartment wants to know her economic situation as well as her criminal status.
- Thankfully Alice already has the documents ready in her wallet, she creates a contract and attaches the documents, she grants this contract as one time only, and issues this to the owner's company.

Happy End!

- Alice receives the approval message from the rental and has everything ready for her next life in Portugal!

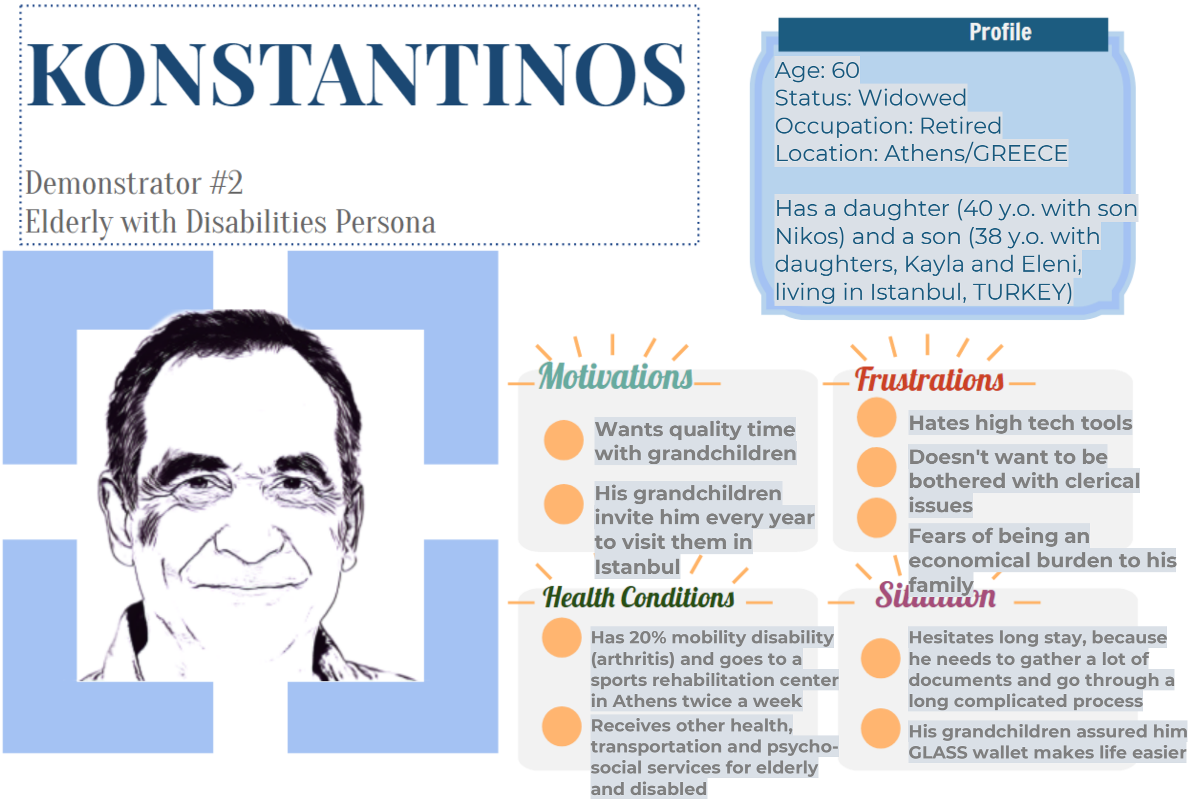
5.2 Demonstrator #2: Konstantinos visiting Istanbul for 6 months

Motivation: Elderly people may move abroad temporarily or permanently for various reasons, such as to receive some kind of treatment, get care from their family, or just travel around for pleasure. Their right to lead a life of independence and participate in social and cultural life is recognized by the European Union in the Charter of Fundamental Rights (article 25 - the rights of the elderly). However, when elderliness is accompanied by disability, moving abroad becomes quite difficult. Elderly people need and usually receive privileged treatment tailored to their special conditions from local authorities in their home country, like discounted and private transportation, health services, sport rehabilitation and psycho-social services. However, when they move to another country, they usually cannot benefit from these kinds of services as they are not officially recognized by the local authorities. If they want to apply to these authorities to receive services provided to elderly citizens with disabilities, bureaucratic processes and associated paperwork are demanding and tiring, mainly due to the lack of clear guidance and sufficient information, the long waiting times for appointments in the involved administration authorities, as well as the language barrier. Moreover,

the application process usually requires several physical visits, which makes the whole process even more problematic.
This demonstrator will showcase the potential of the GLASS solution for transactions taking place between a country of the EU (Greece) and a country outside the EU (Turkey), which can be administratively challenging, especially for people with special needs, such as the elderly and disabled. Our goal is to simplify the bureaucratic processes for (senior) citizens with disabilities when it comes to travelling for a short or medium period of time and evaluate our solution in such a demanding scenario. It is worth mentioning that all the documents to be stored and the distributed procedures to issue such documents will support the policies of the European e-government Action Plan 2016-2020 and all the associated priorities, including the Digital by Default, Openness & Transparency and Once-only priorities.

Problem Setting: Starting from Athens, Konstantinos is invited to visit his grandchildren in Istanbul for 6 months. The grandchildren would like to take care of Konstantinos since he is 60-years old, disabled man and has not been out of Athens for many years. Happily, Konstantinos accepts the invitation and decides to live in Istanbul for 6 months to spend time with his grandchildren and also visit and enjoy the city. However, in order to facilitate his wellbeing, he needs some services for health, transportation, sports rehabilitation and psycho-social services (services that he had access to while in Athens). Unfortunately, in order to access these services offered by the Directorate of People with Disabilities at Istanbul Metropolitan Municipality, he has to deal with a series of bureaucratic processes; he has to provide a proof of validated ID documentation, a validated disability report taken from a hospital (stamped and approved in Greece), health insurance valid in Turkey, and a residence paper which shows his residence address in Turkey (stamped and approved by Turkish authorities). Obtaining these documents and delivering them physically to the Directorate of People with Disabilities in Istanbul is a really difficult and time-consuming process for a disabled person. Thanks to the GLASS solution, Konstantinos will gather the required documents and request from the Greek Authorities the validated data. If this type of documentation has been previously issued, the Directorate of People with Disabilities in Istanbul can access the documents directly from the Wallet of Konstantinos. After this transaction is completed, through his Wallet, Konstantinos can access the approval document that shows which kind of services for disabled he can access and any other related requirements during his stay in Istanbul. He does not need to go to the Directorate or call them to learn the status of his application. Moreover, all related transactions will be recorded in GLASS. Thus, the history of Konstantinos (what kind of services he accessed before in his country and also the other countries, how long and how often he benefited from these services, etc.) will also be accessible and traceable by the Directorate of People with Disabilities in Istanbul through the GLASS solution, in case they are requested from Konstantinos (and approved by him). This will thoroughly facilitate the approval of the services to be offered to Konstantinos.

Added Value: Several actions need to be carried out when applying for the privileges provided for elderly people with disabilities, such as obtaining validated ID documentation, disability report, health insurance, residence paper and exchanging the relevant documents with municipalities. Using the wallet proposed in GLASS, individuals will be able to easily share the required documents and information needed to obtain access to services for disabled with the relevant authority through a mobile app, increasing in this way the efficiency of the government services, tackling the language and culture barrier, differences and misalignment in the requested information, and reducing (or even eliminating) the number of physical visits and associated long waiting times. After successfully registering to the program offered for elderly citizens with disabilities, other third-party service providers like transportation companies or health institutes will need to see the documents validating that the person is qualified to receive special treatment. With GLASS, these service providers will have the ability to access the required validation through a mobile app and see the coverage and the limits of the program. On the other hand, the program beneficiary will be able to track the coverage and the limits of the services through the Wallet solution developed in GLASS. As far as the municipality is concerned, GLASS will decrease their workload to process, validate and approve the applications by reducing paperwork, minimizing the chance of forged documentation, enhancing the transparency and security of information exchange in accordance with the relevant legislation, and decreasing the overall transaction processing time.



KONSTANTINOS

Demonstrator #2
Elderly with Disabilities Persona

Profile

Age: 60
Status: Widowed
Occupation: Retired
Location: Athens/GREECE

Has a daughter (40 y.o. with son Nikos) and a son (38 y.o. with daughters, Kayla and Eleni, living in Istanbul, TURKEY)

Motivations

- Wants quality time with grandchildren
- His grandchildren invite him every year to visit them in Istanbul

Frustrations

- Hates high tech tools
- Doesn't want to be bothered with clerical issues
- Fears of being an economical burden to his family

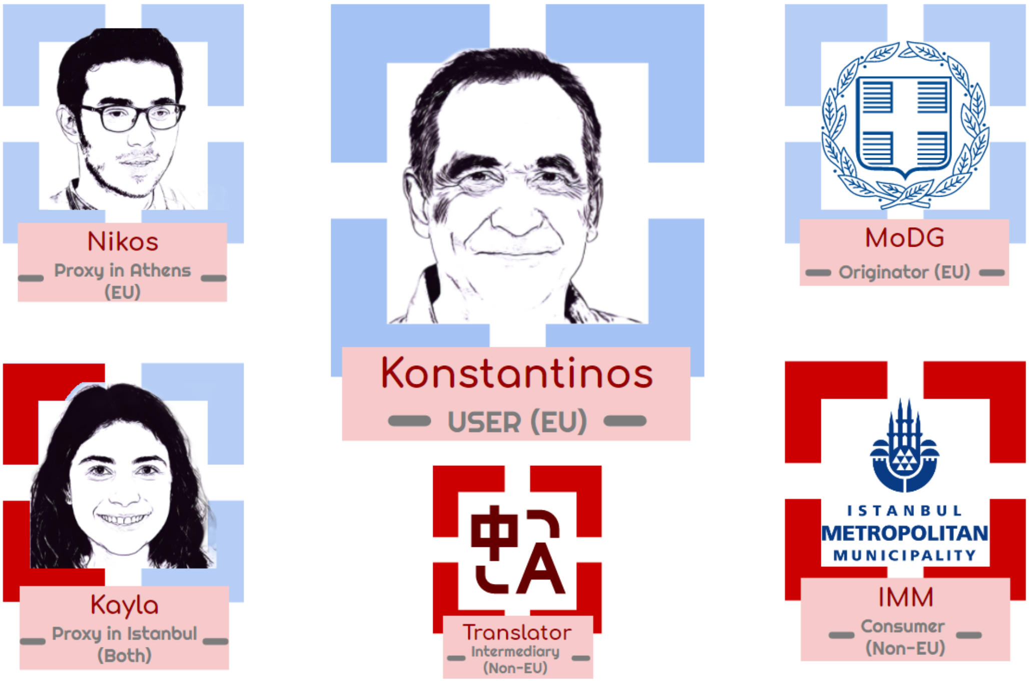
Health Conditions

- Has 20% mobility disability (arthritis) and goes to a sports rehabilitation center in Athens twice a week
- Receives other health, transportation and psycho-social services for elderly and disabled

Situation

- Hesitates long stay, because he needs to gather a lot of documents and go through a long complicated process
- His grandchildren assured him GLASS wallet makes life easier

Actors :



Konstantinos downloads the Wallet app with the encouragement from his grandchildren

- He registers his account using his identification documents.
- He assigns his grandson Nikos (who lives in Athens) as his Proxy. For this he creates a smart contract within the Wallet and grants Proxy rights to his grandson in order to start his application process. He sets this grant for a month. He issues this contract to Nikos.
- Nikos confirms this request after logging into his own wallet and viewing his inbox. The contract is added to his wallet.

Nikos receives the list on behalf of Konstantinos

- Nikos gets the required list of evidences published for Konstantinos. They both view the List of Evidence as this was received in their inboxes. They decide to require the help of Konstantinos' granddaughter Kayla for the evidences need to be procured in Turkey.

Evidence List to be delivered to Directorate of People with Disabilities in Istanbul:

- a proof of validated ID documentation
- a validated disability report taken from a hospital (stamped and approved in Greece)
- health insurance valid in Turkey
- a residence paper which shows his residence address in Turkey (stamped and approved by Turkish authorities)

Konstantinos adds his granddaughter as Proxy

- Konstantinos again creates a smart contract within the Wallet and grants Proxy rights to his granddaughter to gather the evidences on his behalf. He again sets this grant for a month. He attaches this list in his contract. He issues this contract to Kayla.
- Kayla receives Konstantinos' contract in her inbox. Kayla opens the contract and confirms this request. This contract is added to Kayla's Wallet.

Konstantinos has his disability report ready.

- Nikos opens his Wallet, connects to the Greek Authority's API. Sends his proxy contract and uploads and attaches Konstantinos' report for approval.

Nikos also requests Konstantinos' citizen ID and passport.

- Nikos opens his Wallet, connects to Greek Authority's API. Sends his proxy contract and *requests* his grandfather's current identity documents.
- Nikos also requests his grandfather's medical history from the Greek Authority, as he might need it someday in Istanbul

Kayla applies for documents in Istanbul

- Kayla applies for insurance and Residence Paper, wishing the insurance company was integrated to Wallet.
- Kayla applies for Residence Papers via Turkish e-government system.

Konstantinos understands how easy to use GLASS Wallet is.

- A few days after Nikos' application, Konstantinos receives the approved report and his identification documents on the way to his physio-therapy session.
- He saves the documents to his wallet; he also starts getting excited about his visit to Istanbul.
- He buys a guidebook on the way home.

Kayla uses an authorized translator

- Kayla creates a contract, attaching her Proxy contract, Konstantinos' disability report to request translation of this document to Turkish.
- The translator accepts the contract and attach the requested document to the contract after translation and sends it back to Kayla.
- Kayla and Konstantinos save this document to the wallet.

All the documents are gathered

- In Istanbul, Kayla uploads the insurance and residence papers using her Proxy status to Konstantinos' wallet.
- With this Konstantinos is ready to apply to the Directorate of People with Disabilities in Istanbul.

Konstantinos revokes proxy

- Konstantinos revokes the proxy contract of Nikos as they assembled the documents.
- Kayla forwards all the required evidences to Istanbul Authority, including her Proxy contract to the evidences.
- Granddaughters start getting Konstantinos' room ready.

Happy End!

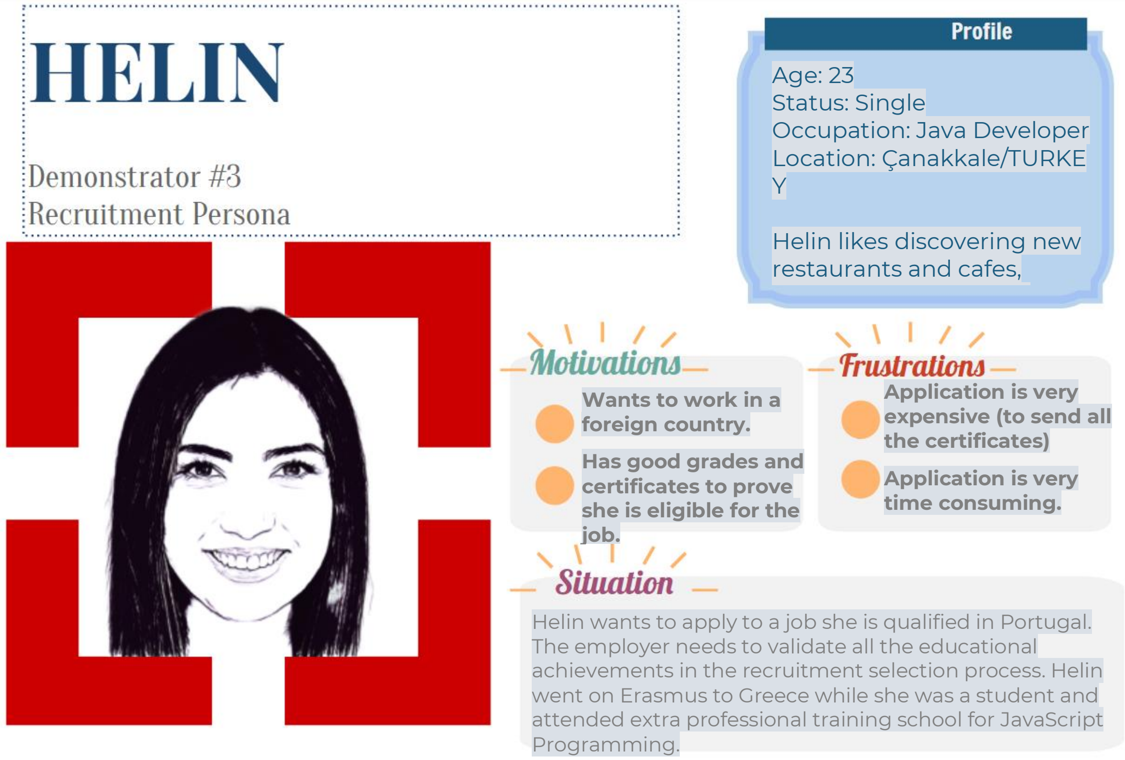
- She puts Konstantinos' Greek ID in the evidence list but they want his passport. Thus, the application was rejected.
- Kayla adds the passport and sends the contract again.
- Konstantinos' request is approved.
- Konstantinos comes to Istanbul, knowing that his needs will be met. His sports therapy sessions already booked.

5.3 Demonstrator #3: Helin is hired as a Java developer

Motivation: This demonstrator follows the principles of the general case study towards paperless bureaucratic processes. We will design and deploy a solution that will allow any citizen to carry with him/her on his/her digital wallets the required evidence of educational achievements, provided by formal education institutions (e.g., Universities, Technical Schools, Secondary schools, etc) accredited by their respective countries (typical managed by the corresponding Ministries of Education). These certificates can also be Professional Training certifications (provided by accredited training schools) in any type of area (e.g., cybersecurity, hotel management or JavaScript programming). In addition to carrying the evidence of educational achievements in a format that can be verifiable in real-time by anyone to whom the job candidate grants access, letters of recommendation can also be accessed and properly verified without having to contact the issuer of such recommendations. The current process is time consuming, prone to fraud, and expensive (when it is required to send all educational certifications).

Problem Setting: The wallet will be the secure entry point to the citizen´s educational history, which will include all relevant transactions and will not be limited to the final results of the scholar achievement. In this case, it is possible to store all personal achievements such as enrolling in a class, completing a class, completing a degree, report a score, etc. Intercommunication with external databases for storage (for example, the actual recommendation letter issued by a specific person) will be supported, as well the mechanisms to limit the access to specific information for a limited time period. All transactions will be stored in the validation ledger and will be demonstrated with the usage of the Unified Digital Identity Device (UDID) as well as regular mobile devices.

Added Value: As described in the in the case of Alice, the process to move to a foreign country for a new job is complex, often riddled with inconsistencies, such as requiring a local bank account before being able to rent an apartment, while at the same time requiring a local address before being able to open a bank account. Accordingly, it is very hard for employers to assess the real knowledge of a new employee, who uses only the (claimed) academic achievements as a good indicator. However, the process of validating the employee's claims is almost always based on trust between the parties due to the inherent complexity of validation. When required a formal validation, it is necessary for the employee (often at high financial cost and with a significant time delay) to obtain authenticated copies of the major certifications (typically University degrees). In this demonstrator, Helin from Turkey gets a job in Portugal as a Java developer. The goal is to enable the validation of all educational achievements (Java courses, Hackathons, Summer Schools, Online certifications, etc.) in the recruitment selection process of Helin in a trusted way, while at the same time guaranteeing compliance with GDPR, since all information shared will be only accessible with the explicit consent from Helin and cannot be shared between the controller of the data (Portuguese employer) and any other third parties. Thus, enabling trust among cross-border and unknown parties and bridging the current gaps in the hiring process.



HELIN

Demonstrator #3
Recruitment Persona

Profile

Age: 23
Status: Single
Occupation: Java Developer
Location: Çanakkale/TURKEY

Helin likes discovering new restaurants and cafes,

Motivations

- Wants to work in a foreign country.
- Has good grades and certificates to prove she is eligible for the job.

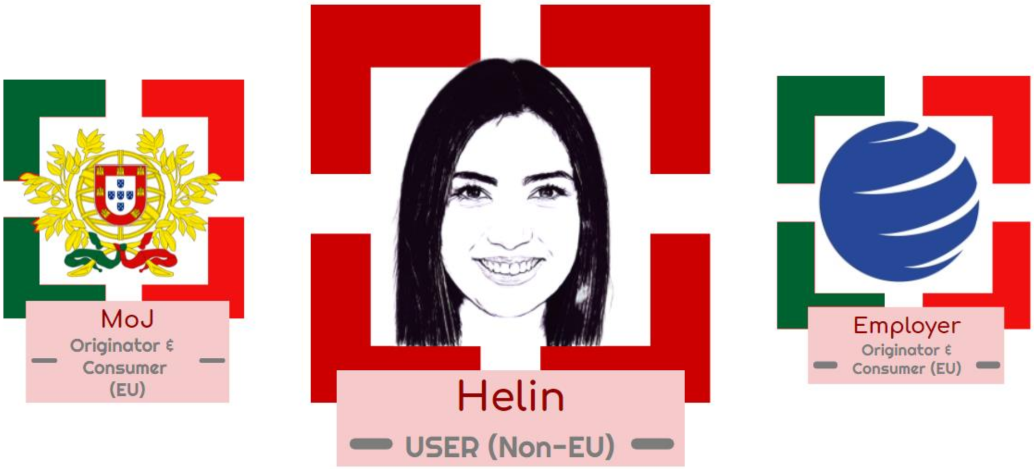
Frustrations

- Application is very expensive (to send all the certificates)
- Application is very time consuming.

Situation

Helin wants to apply to a job she is qualified in Portugal. The employer needs to validate all the educational achievements in the recruitment selection process. Helin went on Erasmus to Greece while she was a student and attended extra professional training school for JavaScript Programming.

Actors:



Helin is excited as she finds the perfect job

- Helin was browsing recruitment ads when she saw the call for a Java Developer.
- As Helin is a Computer Programming graduate who likes coding in JavaScript, she gets very excited and decides to apply.
- She understands that she needs to include all of her related educational achievements written in her CV.

Helin downloads the GLASS Wallet

- Instead of applying the traditional way, Helin decides to use GLASS Wallet for her application.
- She creates and validates her personal account.
- She uploads her university diploma into Wallet.

Helin remembers her certificates from Erasmus

- A few years ago, Helin went to Greece for Erasmus and attended some additional programming classes and received certificates of participation.
- Helin uploads these documents to Wallet

Helin is ready to apply

- Helin opens her Wallet and creates a new smart contract for her application.
- She selects the employer’s human resources group, sets validity period for a month with unlimited access frequency and authorized 3rd party access rights.
- Human resources group include delegated professionals to evaluate her skills.
- She attaches the validated documents, her diploma and CV to the contract.

Helin gets the job after a thorough examination

- After attending several rounds of interviews and the initial examination of her documents, the employer decides to hire Helin.
- Helin receives her offer mail and starts her application for work permit.
- She is very happy with how easy GLASS made her application process and decides to continue using GLASS whenever she can!

6. GLASS framework in a Greek Municipality

The GLASS project has the potential to transform the way municipalities manage their e-government and citizen services. It aims to create a distributed file exchange network that allows for secure and transparent sharing of documents and data across borders. This technology can be particularly useful for municipalities, as they often deal with sensitive and confidential information that needs to be shared with other government agencies or departments, as well as with citizens and businesses. In this section, I elaborate on the establishment of the GLASS framework in a Greek municipality as well as its potential applications and the benefits that it can provide to both citizens and local government.

6.1 Establishment of the GLASS framework

Implementing the GLASS framework in a municipality requires a coordinated effort between several different stakeholders, including government officials, IT professionals, and citizens. This procedure would involve several steps. Here is a general overview of the process:

Planning: The first step would be to develop a plan for implementing GLASS in the municipality. This plan should include a timeline for implementation, as well as specific milestones and deliverables. It should also outline the roles and responsibilities of each stakeholder involved in the implementation process. This would involve identifying the specific applications of GLASS that would be most beneficial to the municipality, as well as the resources required to implement the system.

Needs' assessment: In this step, an assessment of the specific needs of the municipality in terms of document management and information sharing will take place. This would involve identifying the types of documents and data that need to be shared, the users who need access to the system, and the specific security and privacy requirements that must be met.

Analysis of the existing infrastructure: Once the plan is in place and the needs assessment is complete, the next step would be to conduct a comprehensive analysis of the existing e-government infrastructure. This analysis should identify the specific areas where GLASS can be applied, as well as any technical or logistical challenges that may need to be addressed before implementation. In addition, the municipality would need to identify the appropriate technology to meet those needs.

Installation and configuration of the system: Once the technology has been identified, the system would need to be installed and configured. This would involve setting up the necessary servers, databases, and software, and configuring the system to meet the municipality's specific requirements.
The GLASS system relies on the exchange of data between different parties, so it would be essential to establish data management protocols to ensure that data is exchanged securely and efficiently. This would involve establishing procedures for data sharing, as well as ensuring that data is protected from unauthorized access or manipulation. In this step, the establishment of the technical infrastructure required to support GLASS will take place. This would involve deploying the necessary hardware and software, as well as configuring the system to meet the specific needs of the municipality.

One of the key components of implementing the GLASS framework is the development of a decentralized file exchange network. This network should be designed to enable secure and efficient exchange of documents between different government agencies, as well as between the government and citizens. The network should be based on open standards and should be interoperable with existing e-government systems, ensuring compliance with relevant legal and regulatory frameworks.

Development of policies and procedures: To ensure the secure and effective use of the GLASS system, the municipality would need to develop policies and procedures for its use. This would involve developing guidelines for user access, document sharing, data security, and other important aspects of the system's use.

Training: To ensure that GLASS is used effectively, it would be necessary to provide training to relevant stakeholders, such as government employees, contractors, and citizens. This training would include instruction on how to use the system, as well as best practices for data management and security. Once the system is up and running, users would need to be trained on how to use it effectively and securely.

Pilot Testing: Once the system is installed, configured, and tested, and before implementing GLASS on a large scale, it would be advisable to conduct a pilot test to ensure that the system works as intended and to identify any issues that need to be addressed. This pilot test could involve a small number of users from specific departments or a limited set of applications and would provide an opportunity to refine the system before it is deployed more widely.

Deployment: Once the GLASS system has been tested and refined, it can be deployed across the municipality. This would involve making the system available to all relevant stakeholders and ensuring that all necessary procedures and protocols are in place to support its use.

Maintenance and upgrades: It would be necessary to establish a maintenance and upgrade plan to ensure that the GLASS system continues to function effectively over time. This would involve regular monitoring and maintenance of the system, as well as periodic upgrades to address changing needs or technological developments.

Monitor and evaluate: Finally, the municipality would need to monitor and evaluate the use of the GLASS framework to ensure that it is meeting its objectives and to identify areas for improvement. This could involve conducting user surveys, analysing system usage data, and making changes to the system or its policies and procedures as needed.

Overall, the establishment of the GLASS system in a Greek municipality would be a complex and multifaceted process. It also requires engagement with citizens and other stakeholders to ensure that their needs and concerns are addressed. The exact process for installing and implementing the GLASS solutions in a Greek municipality would depend on the specific requirements and needs of the municipality in question. However, the potential benefits of GLASS in terms of increased security, transparency, and efficiency in municipal government make it a valuable investment for any municipality looking to improve its e-government and citizen services.

6.2 Applications of GLASS solutions in a Greek Municipality

The GLASS project and its technology could have several potential applications in a municipality, particularly in the areas of e-government and citizen services. Listed below are some examples.

6.2.1 E-procurement

One of the main areas where GLASS could be applied in a Greek municipality is e-procurement. Procurement is a critical function of local government, as it involves the purchase of goods and services necessary for the provision of public services. GLASS's decentralized document access control and validation features could be used to provide a secure and efficient way to exchange and validate procurement documents. This could help to reduce the risk of fraud and increase transparency in the procurement process, ultimately leading to better outcomes for both citizens and local government.

6.2.2 E-identification

Another area where GLASS could be applied is e-identification and e-authentication. GLASS's attribute-based credentials (ABCs) could be used to provide secure and privacy-preserving access to a variety of e-government services in the municipality, such as tax and license applications. This could help to eliminate the need for physical presence or manual document verification, making it easier for citizens to access these services. Additionally, GLASS's ABCs could be used to enable secure and privacy-preserving data sharing between different government agencies, reducing duplication of effort and improving the overall efficiency of the government.

6.2.3 E-residency

GLASS could also be used to enable e-residency in a Greek municipality. E-residency is a digital identity solution that allows non-resident citizens to participate in municipal elections and other civic processes. GLASS's decentralized identity management and e-voting features could be used to enable e-residency in the municipality, providing a more inclusive and transparent democratic process. This could help to increase citizen engagement and satisfaction, as well as improve the overall legitimacy of the government.

6.2.4 Centralized document management system

One way in which the GLASS project can be applied in a municipality is through the creation of a centralized document management system that allows for secure and efficient sharing of documents between different departments and agencies within the municipality. For example, a city planning department may need to share zoning documents with the local building department or with developers, while the public works department may need to share engineering plans with the transportation department. By using the GLASS system, all of these documents can be securely shared in a transparent and efficient manner, with each user having access to only the information that they need.

6.2.5 Communication of citizens with the municipality

Another way in which the GLASS project can be applied in a municipality is through the creation of a citizen-facing portal that allows for secure and transparent communication between citizens and government agencies. For example, a citizen may need to apply for a permit or license or may need to submit a complaint or request for service. By using the GLASS system, citizens can securely submit their requests and receive updates on their status, while government agencies can efficiently manage and process these requests.

6.2.6 Information sharing between different municipalities

In addition, the GLASS project can also be applied in a municipality to facilitate cross-border collaboration and information sharing between different municipalities or government agencies. For example, neighbouring municipalities may need to share information on transportation or environmental issues that affect both communities. By using the GLASS system, these municipalities can securely share information and coordinate their efforts to address common issues.

6.2.7 Other municipal applications

Finally, GLASS's smart contract capabilities could be used in a variety of municipal applications, such as managing public land leases or issuing building permits. Smart contracts are self-executing contracts that are stored on a blockchain, enabling secure and efficient contract management and execution. GLASS's smart contract capabilities could help to reduce the risk of fraud and increase transparency in these processes, ultimately leading to better outcomes for both citizens and local government.

In addition to the specific applications outlined above, GLASS has the potential to provide several benefits to both citizens and local government. For citizens, GLASS can help to improve access to e-government services, reduce the burden of physical document verification, and increase the transparency and accountability of the government. For local government, GLASS can help to improve the efficiency and effectiveness of government processes, reduce the risk of fraud, and increase the overall trust and legitimacy of the government.

In conclusion, the GLASS project has the potential to transform the way municipalities manage their e-government and citizen services and can provide several benefits to both citizens and local government, ultimately leading to better outcomes for everyone involved. Also, the GLASS project has the potential to revolutionize the way that municipalities manage and share sensitive information. By providing a secure, transparent, and efficient system for sharing documents and data, the GLASS system can help to improve collaboration between government agencies and departments, increase transparency and accountability, and provide better services to citizens and businesses. As such, the GLASS project is a critical step towards a more secure, transparent, and efficient municipal government.

6.3 Existing systems similar to GLASS

There are various e-government systems in Greece and other countries that aim to improve the efficiency and effectiveness of government processes and services. However, there are not many systems that are directly comparable to GLASS, which is a decentralized file exchange network with a focus on attribute-based credentials and smart contracts.

In Greece, there are several e-government systems that have been implemented over the past few years, such as the "Single Digital Gateway"[8] and the "Unified Digital Registry of Citizens"[9]. The Single Digital Gateway is an online portal that provides access to a variety of public services, including the ability to exchange documents securely with government agencies, while the Unified Digital Registry of Citizens is a centralized database that stores citizen data and enables access to various government services. While these systems have improved the efficiency of government processes and services, they are centralized in nature and do not offer the same level of security and privacy as GLASS.

In other countries, there are also various e-government systems that have been implemented. For example, Estonia's e-government system[10] is often cited as a model for other countries. Estonia's system includes a variety of e-services, such as e-voting, e-taxation, and e-health, and is based on a decentralized architecture that utilizes blockchain technology. While Estonia's system is decentralized like GLASS, it does not utilize attribute-based credentials or smart contracts in the same way. Also, in France, the "FranceConnect" platform[11] allows citizens to use their existing social media or email accounts to access a range of public services, including tax and healthcare services. Similarly, the Netherlands has the DigiD system[12], which provides citizens with a single set of credentials to access a wide range of government services.

On the other side, there are systems often developed by government agencies or technology companies to facilitate secure document exchange and information sharing between different organizations.

In addition to the Single Digital Gateway mentioned before, that includes the ability to exchange documents securely with government agencies, there are also similar systems in use or under development in other countries. For example, the European Union has developed the eDelivery solution[13], which is a secure messaging service that allows different organizations to exchange documents and data securely. Also, in Germany, the "De-Mail" system[14] provides a secure way for citizens and businesses to communicate with government agencies and other organizations online.

Other examples of similar systems include the US Department of Defense Information System for Security (DISS)[15], which is used to manage classified information, and the Australian Government's Trusted Digital Identity Framework[16], which is used to verify the identities of individuals accessing government services online.

[8] https://digitalstrategy.gov.gr/digital_services_portal
[9] https://notify.gov.gr/
[10] https://e-estonia.com/
[11] https://joinup.ec.europa.eu/collection/eidentity-and-esignature/document/france-connect-id-federation-system-simplify-administrative-processes
[12] https://www.digid.nl/en/
[13] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery
[14] https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Digitale-Verwaltung/De-Mail/de-mail_node.html
[15] https://www.dcsa.mil/is/diss/
[16] https://www.digitalidentity.gov.au/tdif

While each of these systems may have different features and capabilities, they all share a common goal of improving document management and information sharing through secure and transparent mechanisms. The development and implementation of these systems is often driven by the need to improve government efficiency, reduce costs, and enhance security and privacy for users.

Overall, while there are various e-government systems in Greece and other countries, there are not many systems that are directly comparable to GLASS. GLASS's decentralized architecture, attribute-based credentials, and smart contract capabilities are unique features that could potentially provide significant benefits to municipalities and governments.

6.4 integration of SSO infrastructures from EU countries

National SSO (Single Sign-On) infrastructures are used in several EU countries to provide a secure and convenient way for citizens to access various government services online. These infrastructures are typically built on top of existing eID (electronic ID) systems that have been deployed at the national level.

As mentioned in Section 2.3, the European Commission has launched several initiatives aimed at promoting the development of a trusted digital identity ecosystem across the EU, including the eIDAS regulation, which aims to ensure cross-border recognition and interoperability of national eID schemes.

Also, as mentioned in Section 6.3, several EU countries have already developed their own national SSO infrastructures, or they are in the process of developing their own national SSO infrastructures, while others are exploring the possibility of adopting a common SSO solution.

In general, the adoption of national SSO infrastructures is part of a broader requirement towards digital transformation in the public sector, which seeks to enhance the efficiency, accessibility, and security of online public services, while also helping to streamline administrative processes and reduce bureaucracy.

With the existence of national SSO infrastructures, a question arises, whether a new solution, like GLASS, is necessary for the operation of a country's public services and if it provides added value.

If a national SSO infrastructure exists and is functioning well, there may not be a need for a separate more holistic SSO platform. While a national SSO infrastructure can be effective in providing access to government services, a separate, more holistic SSO framework, like GLASS, may be necessary in several scenarios. Thus, the need for a separate platform depends on the specific use case and user needs. More specifically:

- **Cross-border access:** If users need to access online services in different countries that use different national SSO infrastructures, a separate more holistic SSO platform may be needed to provide a seamless login experience.
- **Integration of different types of services:** National SSO infrastructures are typically designed to provide access to government or public services. Still, if users need to access other types of services such as private sector services or social media, a separate SSO platform may be necessary to integrate these services.

- **Improved user experience:** A solution like GLASS, could probably provide a better user experience and easy to use functionalities.
- **Broader adoption:** A separate, more holistic SSO platform may be necessary to encourage broader adoption of SSO technology, particularly among private sector organizations that may not be inclined to adopt a government provided SSO solution.

With the parallel integration of national SSO infrastructures from several EU countries and another separate holistic SSO platform, several issues can arise. More specifically:

- **Technical interoperability issues:** National SSO infrastructures may use different technical specifications and standards, making it challenging to integrate them into a single holistic SSO platform. This could lead to technical interoperability issues that result in login failures or other issues for users.
- **Complexity for users:** If there are multiple national infrastructures and a separate platform, users may need to remember different login credentials for each system. This could increase the complexity and friction of the login process, potentially leading to frustration and reduced adoption.
- **Data privacy and security concerns:** Integrating multiple SSO systems could increase the risk of data breaches and cyber-attacks, especially if these systems are not designed with strong security measures in place. Sensitive user information, such as login credentials and personal data, may be at risk if not adequately protected.
- **Legal and regulatory compliance:** The integration of multiple SSO systems may raise legal and regulatory compliance concerns, particularly regarding data protection and privacy. Different national regulations and legal frameworks may make it challenging to develop a standardized approach to SSO integration.
- **Maintenance and support:** Integrating multiple SSO systems may require additional maintenance and support, which could be costly and time-consuming. This could also lead to delays in updating and upgrading systems, potentially leaving users vulnerable to security threats.

To mitigate these issues and solve the problem of the parallel integration, the use of a framework like GLASS is suggested. Primarily, a separate holistic SSO platform could improve cross-border transactions. More specifically:

- **Seamless cross-border authentication:** A solution like GLASS could provide a standardized approach to cross-border authentication, making it easier for users to access services across different countries. This could reduce friction and delays in cross-border transactions, making it more efficient for users.
- **Compliance with cross-border regulations:** A separate, more holistic SSO platform could ensure compliance with relevant cross-border regulations, such as the General Data Protection Regulation (GDPR) in the EU. This could help prevent cross-border legal issues and make it easier for service providers to comply with cross-border regulations.
- **Increased trust in cross-border transactions:** GLASS framework could help increase trust in cross-border transactions by providing a secure and reliable authentication method. This could help reduce fraud and improve the overall security of cross-border transactions.
- **Improved interoperability:** A holistic platform could provide a common interface for cross-border transactions, making it easier for service providers to integrate with other countries' SSO systems. This could reduce technical

interoperability issues and make it easier for users to access services across different countries.

- **Increased cross-border adoption:** By providing a standardized and efficient approach to cross-border transactions, GLASS platform could help increase adoption of cross-border services. This could provide new opportunities for service providers and improve the overall efficiency of cross-border transactions.

In addition to the above benefits, more explanations about the suggested adoption of GLASS framework, are presented below that are linked with the issues mentioned. More specifically:

- **Technical interoperability:** A solution like GLASS could help address technical interoperability issues by providing a common interface for accessing services across different national SSO infrastructures. The platform could use a common set of technical standards and protocols, allowing it to seamlessly integrate with existing national SSO systems. It is important to ensure that the holistic SSO platform is compatible with the existing national SSO infrastructure.
- **Simplify user experience:** A separate holistic SSO platform could simplify the login process and reduce the need for multiple login credentials for different services. The platform could provide a single sign-on solution for accessing a range of services, making it easier and more convenient for users. It is essential to ensure that the user interface of the holistic SSO platform is easy to use and user-friendly.
- **Data privacy and security:** GLASS platform could provide additional security measures to protect user data and reduce the risk of data breaches. The platform could use advanced encryption and authentication protocols, as well as robust security testing and certification processes. It is crucial to ensure that the holistic.
- **Legal and regulatory compliance:** Frameworks like GLASS could help address legal and regulatory compliance issues by providing a standardized approach to SSO integration. The platform could comply with relevant data protection and privacy regulations, making it easier for service providers to ensure compliance when integrating with the platform.
- **Maintenance and support:** A more holistic SSO platform could provide centralized maintenance and support, reducing the need for service providers to maintain their own SSO infrastructure. The platform could provide regular updates and upgrades, as well as technical support for users and service providers. It is essential to ensure that this platform is designed for scalability and can handle increasing demand as adoption grows.

In summary, a separate holistic SSO platform could help address the issues that arise with the parallel integration of national SSO infrastructures from several EU countries. The platform could simplify the login process, provide additional security measures, ensure legal and regulatory compliance, and provide centralized maintenance and support. However, it is crucial to ensure that the platform is compatible with existing national SSO infrastructure, user-friendly, secure, compliant, and scalable. Moreover, it is essential to establish clear standards and guidelines for the integration of all systems and ensure that these systems comply with relevant data protection regulations and undergo rigorous security testing before deployment.

7. Suggestions, barriers, opportunities

7.1 GLASS's innovation potential

GLASS's innovation potential appears in bridging centralised, decentralised and distributed systems that leads to a unique development environment for designing, coding, compiling and deploying distributed applications. The dApps running on the network function under the same ledger that provides interconnection functionalities and enhanced capabilities among them and with the Interplanetary File Storage System (IPFS), acting like a warehouse keeper. GLASS' distributed applications will be:

- Open Source: The application governed by the network and all changes must be decided by the consensus, or a majority, of its users.
- Decentralized: All records of the application's operation will be stored on the public distributed validation ledger to avoid pitfalls of centralisation.
- Privacy Preserving: Private data collections can be created, which allow a defined subset of organizations on a channel the ability to endorse, commit, or query private data without having to create a separate channel.
- Proof of value-based: The community will agree on a cryptographic algorithm to show proof of value. For example, Bitcoin uses Proof of Work (PoW) and Ethereum is using Proof of Stake (PoS).

GLASS envisages to design and deploy a novel eGovernance model and supporting mechanisms to provide citizens, businesses and public authorities the ability to safely and efficiently request, share, exchange official documents such as ID, birth certificates, etc. and fulfil professional obligations and duties as well as personal desires.

The novelty and added value of the proposed GLASS solution will be demonstrated through three (3) real case scenarios concerning Paperless Cross-Border Bureaucratic Processes. The first one covers the case where an individual wishes to move to a foreign EU country for working or educational purposes. The second scenario covers the case of the short-term, cross-border moving (e.g., short-term work, education, traveling) of marginalized people such as elderly, disabled people etc., demanding special treatment and special services to facilitate their moving. The third scenario demonstrates the GLASS solution for validation of the education achievements by an employee seeking to hire young individuals. The demonstrators will examine and validate the interoperability of the proposed digital wallets, along with the interconnection with the dApps, in a cross-border and cross-sector environment.

The benefits and associated impact of the GLASS eGovernance model for the three main types of actors being considered in the context of the project are summarised below:

7.1.1 GLASS for citizens

- The GLASS eGovernance model is more responsive to the needs of the citizens, eases the interaction of citizens with governments and increases the participation of citizens in public policies.
- GLASS is designed to maintain a common methodology, providing a similar user experience whether dealing with the Public Sector, Private Sector or other citizens.
- The citizen is placed at the centre of their own data, attributes and evidence.

- No matter who the citizen liaises with, the citizen can choose what information is released to its counterparty.

7.1.2 GLASS for governments

- The goal of GLASS is to make public administrations and public institutions open, efficient and inclusive, providing borderless, digital, personalised and citizen-driven public services for the EU population.
- GLASS introduces a citizen-centric eGovernance model for public administration services, which automates the processes and safeguards the integrity of interactions.
- GLASS uses a new paradigm for evidence and record transfer: a single sign-on Wallet as a Service (WaaS) platform will interconnect applications for ID authentication, document sharing, information exchange and transactions validation, in compliance with the SDG guidelines.

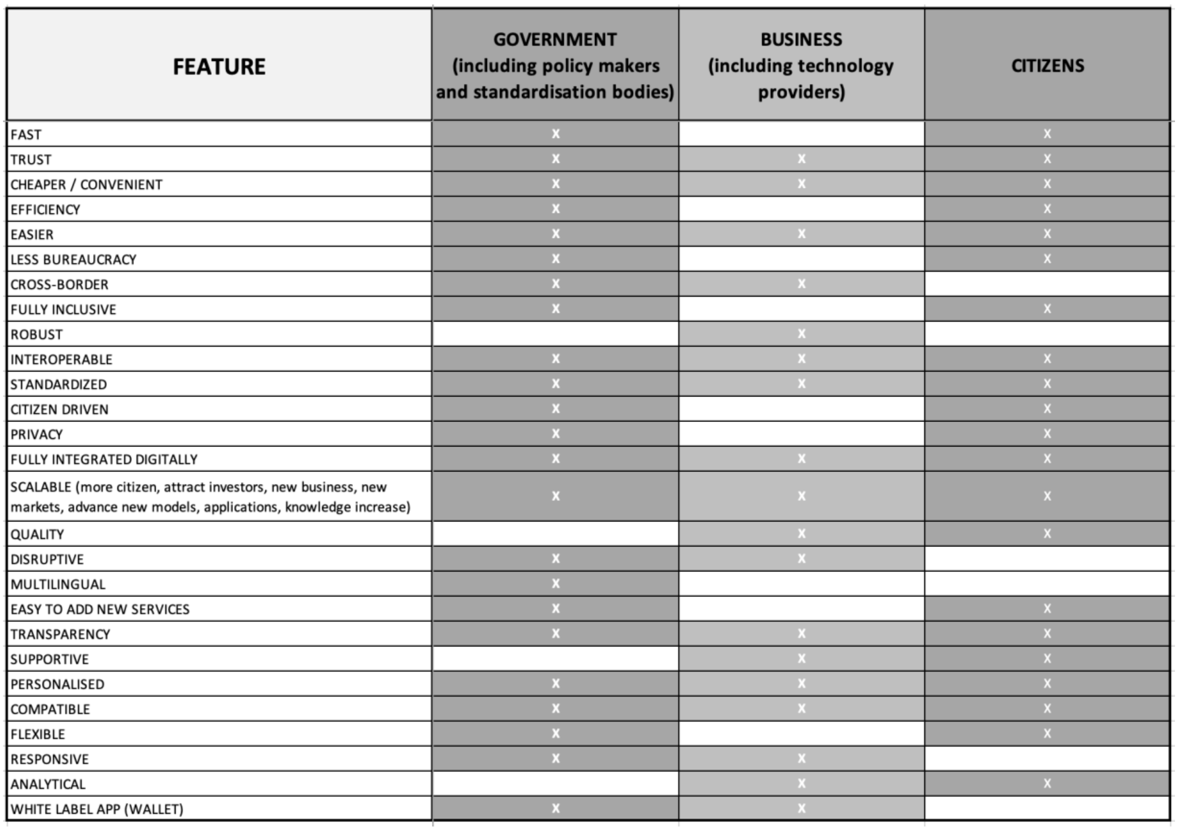
7.1.3 GLASS for business

- The European Commission considers the 24 million SMEs as the entrepreneurship key to ensuring economic growth, innovation, job creation, and social integration in the EU.
- GLASS can improve efficiency in managing company documentation especially when operating in an international market.
- GLASS can also save time when entering formal public procurements and will offer businesses certification and notarisation efficiencies when companies can hold their own notarised evidence.

7.1.4 GLASS features and impact for the benefit of actors

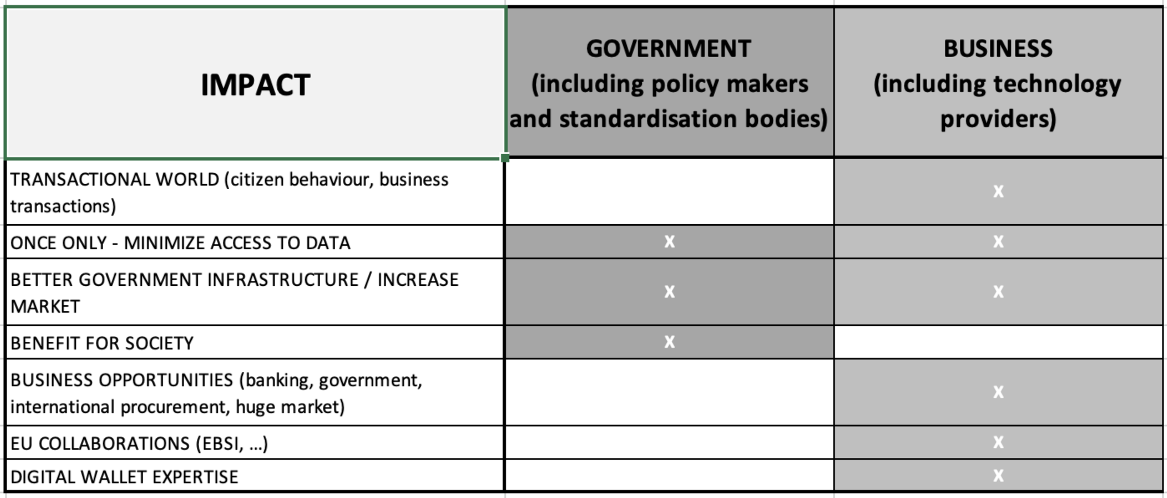
The main features of the overall GLASS solution that are of benefit to each of the stakeholders are listed in Table 1. The impact of the overall GLASS solution for Government and Business is shown in Table 2.

Table 1: GLASS features that are of benefit to the GLASS actors



FEATURE	GOVERNMENT (including policy makers and standardisation bodies)	BUSINESS (including technology providers)	CITIZENS
FAST	x		x
TRUST	x	x	x
CHEAPER / CONVENIENT	x	x	x
EFFICIENCY	x		x
EASIER	x	x	x
LESS BUREAUCRACY	x		x
CROSS-BORDER	x	x	
FULLY INCLUSIVE	x		x
ROBUST		x	
INTEROPERABLE	x	x	x
STANDARDIZED	x	x	x
CITIZEN DRIVEN	x		x
PRIVACY	x		x
FULLY INTEGRATED DIGITALLY	x	x	x
SCALABLE (more citizen, attract investors, new business, new markets, advance new models, applications, knowledge increase)	x	x	x
QUALITY		x	x
DISRUPTIVE	x	x	
MULTILINGUAL	x		
EASY TO ADD NEW SERVICES	x		x
TRANSPARENCY	x	x	x
SUPPORTIVE		x	x
PERSONALISED	x	x	x
COMPATIBLE	x	x	x
FLEXIBLE	x		x
RESPONSIVE	x	x	
ANALYTICAL		x	x
WHITE LABEL APP (WALLET)	x	x	

Table 2: Impact of GLASS for Government and Business



IMPACT	GOVERNMENT (including policy makers and standardisation bodies)	BUSINESS (including technology providers)
TRANSACTIONAL WORLD (citizen behaviour, business transactions)		x
ONCE ONLY - MINIMIZE ACCESS TO DATA	x	x
BETTER GOVERNMENT INFRASTRUCTURE / INCREASE MARKET	x	x
BENEFIT FOR SOCIETY	x	
BUSINESS OPPORTUNITIES (banking, government, international procurement, huge market)		x
EU COLLABORATIONS (EBSI, …)		x
DIGITAL WALLET EXPERTISE		x

As shown in Table 1, the features of GLASS that will be of benefit to all three actor categories are ten. Namely, the GLASS model should provide *trust*, be *cheaper and convenient, easy to use, interoperable, standardised, fully integrated digitally, scalable, transparent, personalised and compatible.*

Besides its benefits, the GLASS model will have an impact on a *transactional world, better government infrastructure, increasing market, benefit for society, creating more business opportunities, EU collaborations, and digital wallet expertise.*

7.2 Legal and Ethical Issues

7.2.1 General legal and ethics considerations

GLASS EU legal framework, the innovations of the GLASS project tie in with a number of current day legal and ethical evolutions. Partly, these are driven by the consideration that some of the GLASS use cases focus on e-government scenarios. Much as in the private sector, public authorities are also confronted with the need to address multiple challenges concurrently, including the shift to mobile services, the increased expectations of seamless and user-friendly digital services, the role of artificial intelligence in enabling faster and higher quality services, and the desire for strategic autonomy and data sovereignty in the face of continuous consolidation of major service providers.

While these trends pose challenges for all stakeholders, the public sector, in particular, is held to a higher standard, in terms of legitimacy, privacy and confidentiality. Citizens generally cannot ‘opt out’ of public services or seek competing services in the market. For that reason alone, public authorities have to apply stringent legal and ethical safeguards to protect their citizens against abuses and incidents. Undoubtedly, the three principal European legal and ethical drivers towards more citizen-centric e-governance are:

- The **General Data Protection Regulation (GDPR)**, as the central legal framework for protecting citizen’s personal data. Its provisions cover (among other points) the right to transparency, the right to access, correct and delete data, and the right to control data flows to non-EEA countries to a certain extent.
- The **Single Digital Gateway Regulation (SDGR)**, as the central legal framework for cross border once-only information exchanges between public authorities in the Member States. Beyond stating the principle that once-only exchanges are possible at citizens’ request, Article 14 also contains specific safeguards to protect citizens against abuses and incidents.
- The **Electronic Identification and Authentication Services Regulation (eIDAS)**, as the central legal framework for both electronic identification in cross border public sector services, and for trust services (such as electronic signatures and time stamps) that constitute critical building blocks for any online transaction.

Other relevant frameworks include the European legislation in relation to critical infrastructure (the so-called NIS Directive), the information security legislation captured in the Cybersecurity Act, and the critical infrastructures protection framework of the Critical Infrastructures Directive. Moreover, various new legislative initiatives are underway that can strongly affect the future of GLASS. Data is increasingly recognised as a critical asset that requires decentralised control, which represents a shift in policy focus compared to the Digital Single Market Strategy. This has resulted in multiple recent new legislative proposals, including the proposal for a Data Governance Act; the proposal for an AI Regulation; and the proposal for a revision of the eIDAS Regulation. All these frameworks contain legal requirements and ethical safeguards, which must be reflected in the GLASS governance model. These requirements are briefly presented below.

7.2.2 Summary of general governance requirements from a legal and ethical perspective

Data protection and privacy

From a data protection perspective, the reliance on DLT and on distributed file storage via the IPFS requires a strong emphasis on data minimisation. Unencrypted personal data should never be stored on the IPFS, but moreover care should be taken that, by default, personal data stored in the IPFS should expire. When DLT is used to manage personal data, the DLT should not be used to store substantive personal data, but rather pointers to personal data stored externally from the DLT implementation, which is the only way to substantially comply with the legal requirement that personal data must be deleted when it is no longer useful.

Additionally, the GLASS project aims to support proxies to facilitate access and exchange of personal data. This is useful but requires some degree of supervision on the definition and scoping of the proxies, appropriate logging to determine actual use of the proxies, and transparency towards relying parties on the intervention of a proxy.

Finally, GLASS relies on smart contracts as an innovative approach to implementing data protection by design. This is beneficial, but transparency is required to ensure that users understand the effects of the contract in a clear way.

e-Government and once-only

With respect to e-government services, the European legal and policy landscape is currently dominated by the recent SDG, which foresees a very specific concept and architecture for exchanges of information between public administrations. GLASS is not an implementation of this concept and architecture, since GLASS has a much stronger focus on user control, data sovereignty, distributed technology, and trust frameworks that are based on technical solutions rather than legal mandates. GLASS sees the user as the holder of their own data and puts the user in greater control than under the SDG. Moreover, GLASS has no limitation to public sector use cases, and permits functionalities such as extended access and usage rights management.

As a result, GLASS does not perfectly comply with the vision of the SDG Regulation, but this is also not necessary. It is more important that GLASS integrates the functional, ethical and legal controls that the SDGR foresees, such as initiating data sharing only at the prior request of the user, and only initiating a data transfer after a preview by the user.

Identity and authentication

With respect to identification and authentication, GLASS can substantially build on the mechanisms of the eIDAS Regulation. Use of European regulated identities is not legally required, and neither is the use of regulated qualified signatures or seals; but these are supported and recognised by the GLASS infrastructure since this facilitates cross border recognition within the EU.

A common challenge is that signatures and seals applied to documents will serve to determine integrity and authenticity; but not to determine the legal value or authority of a document. On that point, GLASS will implement a lightweight solution that can act as a proof of concept. A second challenge is the role of the GLASS Admin service, which will be in charge of onboarding users. This implies that identity checks must be done. GLASS will use the identity assurance criteria established under the eIDAS Regulation for this purpose. The assessment would not have specific legal authority since it is done purely within and by GLASS consortium members; nonetheless, this approach would be suitable for piloting purposes.

The European legal framework is currently undergoing substantial revisions to provide better support for ledgers, attribute attestations and eWallets. GLASS will continue to monitor these, so that it can contribute to advancing the legal and ethical state of the art in Europe.

Responsibilities and liabilities

With respect to the responsibilities and liabilities of various stakeholders, these vary depending on the roles within the GLASS consortium. Briefly summarised, the liabilities and responsibilities in relation to IPFS usage are largely covered and exempted under the intermediary liability regime of the eCommerce Directive; this is arguably the least problematic aspect of GLASS.

The accuracy and correctness of the documents stored in the Wallet or on the IPFS is mainly resolved by the use of electronic seals and signatures, where the sole responsibility and liability of the GLASS consortium is to ensure that these are not corrupted in any way, so that responsibility and liability for the contents remain entirely and exclusively with the evidence issuers. In that respect, the GLASS consortium need not assume any particular responsibilities.

Where the responsibility and liability of GLASS does need to be managed are the components where GLASS is supposed to undertake a fundamental verification role. Mainly this relates to the design and functioning of the eWallet; the role of the GLASS Admin, both in onboarding users and in registering proxies; the legal validity and competences in relation to specific evidence (i.e., when is a document that looks like a diploma or birth certificate an actually legally valid diploma/birth certificate?); and managing the permissible use cases.

Security requirements

With respect to information security, the existing EU level legal framework is not particularly prescriptive, other than the generic requirement to implement appropriate security measures.

Such measures will include securing access to the eWallet through specific authentication of the user; encryption of all evidence and other information in the eWallet, on the ledger and in the IPFS; and systematic logging of transactions, including creation and execution of smart contracts. Additionally, some recommendations are taken from the Cybersecurity Act and relate to monitoring and mitigation of any known dependencies and vulnerabilities, integrating appropriate updating and phase-out functionalities, and implementing appropriate incident response policies.

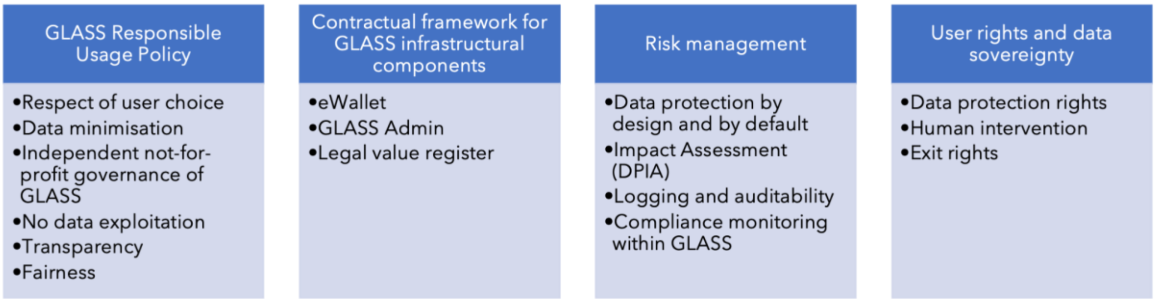
Cross border challenges and non-European piloting

The ambition of GLASS is not to create a purely EU level solution, but to build a framework that can be used and applied globally, while respecting European fundamental rights and standards. This is complicated, given that most of the known legal framework is specific to the EU.

Within the GLASS project, this challenge is mitigated to some extent by incorporating demonstrators that involve non-EU Member States as partners, which will allow testing of the validity of the general principles and requirements in this report, and identification of any national level requirements that differ fundamentally from European approaches. However, European fundamental rights and values remain a core requirement throughout the GLASS project.

7.2.3 Building GLASS Governance from a legal and ethical perspective

Given the aforementioned requirements, it is important to have in place a strategy for operationalising them as a part of the GLASS governance model. The general approach is depicted in Figure 16. As shown, four pillars will support the operationalisation of GLASS legal requirements:



GLASS Responsible Usage Policy
- Respect of user choice
- Data minimisation
- Independent not-for-profit governance of GLASS
- No data exploitation
- Transparency
- Fairness

Contractual framework for GLASS infrastructural components
- eWallet
- GLASS Admin
- Legal value register

Risk management
- Data protection by design and by default
- Impact Assessment (DPIA)
- Logging and auditability
- Compliance monitoring within GLASS

User rights and data sovereignty
- Data protection rights
- Human intervention
- Exit rights

Figure 16: GLASS legal governance components

- A **GLASS Responsible Usage Policy** will provide behavioural requirements for any aspects of GLASS that cannot be automated and enforced by technological means only. This is intended to be a statement of the principles along which all participants in the GLASS ecosystem (including the issuers, verifiers, GLASS Admin and GLASS consortium members) are required to conduct themselves.
- A clear **contractual framework**, in the form of standardised terms and conditions, will be drafted and maintained for any services provided by the GLASS consortium, including the eWallet, the GLASS Admin onboarding, and the basic register describing the legal competences and legal value of piloted documents.
- A **risk management** approach will be applied, including notably the completion of a data protection impact assessment (DPIA) satisfying the requirements of the GDPR in relation to the demonstrators. This will ensure that the principles of data protection by design and by default are adhered to, that transactions are logged in an auditable manner, and that compliance with legal requirements is monitored in GLASS.
- Finally, **a statement of user rights and data sovereignty principles** should be provided, describing fundamentally what the rights of GLASS users are, and how they can exercise them.

8. Conclusions

GLASS introduces a transparent, cross-border and citizen-centric eGovernance model for public administration services, which automates the processes and safeguards the integrity of interactions among citizens, businesses and public authorities.

From a technical point of view, this solution is based on a single sign-on Wallet mechanism that interconnects distinct decentralised applications (dApps) responsible for ID authentication, information sharing and transactions validation, enabling a single point of access to information. By taking advantage of emerging ICT technologies, such as Peer-to-Peer (P2P) networks, Distributed Ledger Technologies (DLTs) and smart data structures, GLASS deploys a public distributed infrastructure, based on the InterPlanetary File System (IPFS). The proposed solution is fully in line with the Government 3.0 paradigm, in that it meaningfully integrates a diverse set of disruptive and established ICTs.

From a social point of view, the GLASS eGovernance model aims to make public administrations and public institutions open, efficient and inclusive, providing borderless, digital, personalised and citizen-driven public services. The proposed solution offers citizens and businesses efficient and secure mobile public services and co-creation mechanisms, enabling governments to be extroverted and to preserve trust among public and private entities. The services delivered to citizens contribute to the digital by default principle for government and local authorities. In addition, the GLASS eGovernance model enables beneficiaries to participate and operate in a by design efficient, cost-effective, secure and cross-border distributed network for data exchange and service delivery.

The most important values of GLASS are the citizen-centricity where the citizen fully controls its own data, being fully transferable and compatible with EU standards and from citizens' points of view to be an easy to use and secure e-Wallet where Vulnerable Groups' needs become a key element on the implementation. Taking into account the benefit of stakeholders and citizens, it is necessary to share the pilot operations' results with the customer segments by mobilizing more pilots in relevant activities and events so that stakeholders will be able to visualize how to offer their expertise or an offering to end users so that citizens should be aware.

GLASS introduces a digital, transparent and inclusive by design eGovernance model, which is fully aligned to the European e-Government Action Plan 2016-2020 requirements towards meeting the Digital by Default, Openness and Transparency, and Once-only priorities. This model aims to establish a paperless cross-border protocol that minimises bureaucracy while enabling innovative user-centric services for citizens, businesses and public administrations.

Overall, Single Sign on Wallet as a Service systems and especially GLASS eGovernance model, contribute significantly to the digital transformation of eGovernment transactions. More specifically:

- it deploys a novel digital channel of communication and collaboration between citizens, businesses and governments.
- it addresses fundamental weaknesses of the existing eGovernment transactions in terms of bureaucracy, complexity, and unnecessary data entry.

- it leverages existing resources and infrastructures.
- it can be applied in several real-life scenarios, such as in the identification control in airports, where passengers need to be checked before departing and after reaching their destination, and in the management of the currently elaborated COVID-19 vaccination certificates.
- it enables an immutable and transparent solution, according to which entries can be publicly audited while anonymity is protected.

If a national SSO infrastructure already exists and is functioning well, there is a question about the need for a separate more holistic SSO platform, like GLASS. The need for a separate platform depends on the specific use case and user needs.

In general, a separate holistic SSO platform could help address the issues that arise with the parallel integration of national SSO infrastructures from several EU countries and the cross-border transactions. The platform could simplify the login process, provide additional security measures, ensure legal and regulatory compliance, and provide centralized maintenance and support. However, it is crucial to ensure that the platform is compatible with existing national SSO infrastructure, user-friendly, secure, compliant, and scalable. Moreover, it is essential to establish clear standards and guidelines for the integration of all systems and ensure that these systems comply with relevant data protection regulations and undergo rigorous security testing before deployment.

9. References

Androutsopoulou, A., Karacapilidis, N., Loukis, E., & Charalabidis, Y. (2019). Transforming the communication between citizens and government through ai-guided chatbots. *Government Information Quarterly 36(2)*, 358-367.

Avijit, B. (2020). *What Is E-Governance or Electronic Governance?* Retrieved from https://schoolofpoliticalscience.com/what-is-e-governance/

Barcevičius, E., C. G., Codagnone, C., Gineikytė, V., Klimavičiūtė, L., Liva, G., . . . Vanini, I. (2019). Exploring Digital Government transformation in the EU - Analysis of the state of the art and review of literature. *Publications Office of the European Union*.

Bertot, J. C., Jaeger, P. T., & & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government information quarterly*, 264-271.

Codagnone, C. a. (2020). Roadmapping eGovernment research. *Visions and Measures towards Innovative Governments*.

Commission, E. (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

Commission, E. (2017). Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

Commission, E. (2019). Retrieved from https://ec.europa.eu/growth/single-market/single-digital-gateway_en

Dandan, H., Yajuan, Z., Junfeng, L., Chen, L., Mo, X., & Zhihai, S. (2017). Research on Centralized Data-Sharing Model Based on Master Data Management. *MATEC Web Conference.*

Danny, P. (2019). *What Is GDPR? Everything You Need to Know about the New General Data Protection Regulations*. Retrieved from https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Field, T., Muller, E., Lau, E., Gadriot-Renard, H., & Vergez, C. (2003). The E-Government Imperative. *OECD Journal on Budgeting*, 61-96.

Finger, M. P. (2003). From e-Government to e-Governance? Towards a model of e-Governance. *3rd European Conference on E-Government*, (pp. 119-130).

Ghareeb, A. M., Darwish, N. R., & & Hefney, H. A. (2019). E-government adoption: literature review and a proposed citizencentric model. *Electronic Government, an International Journal*, 392-416.

Guilin Wang, J. Y. (2013). Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.*

Gwyneth, I. (2021). *What Problems Does Blockchain Solve?* Retrieved from https://101blockchains.com/problems-blockchain-solve/

IBM. (2021). *IBM Security. Cost of a Data Breach Report 2021*. Retrieved from https://www.ibm.com/security/data-breach

Jean Damascene Twizeyimana, A. A. (2019). The public value of E-Government – A literature review, Government Information Quarterly. 167-178.

Jenkins, N. N. (2016). A secure mobile cloud identity: Criteria for effective identity and access management standards: Criteria for effective identity and access management standards. *4th IEEE International Conference on Mobile Cloud Computing, Services and Engineering.* IEEE.

Jenkins, N. N. (2016). An analysis of open standard identity protocols in cloud computing security paradigm. *14th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2016).* IEEE.

Jenkins, N. N. (2017). Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID Connect. *11th International Conference on Research Challenges in Information Science (RCIS)* (pp. 163-174). IEEE.

Jenkins, N. N. (2020). Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. *8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud).* IEEE.

Jolocom. (2019). *A Decentralized, Open Source Solution for Digital Identity and Access Management.* Retrieved from https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf

Keith, C. (2020). *What Is Attribute-Based Access Control (ABAC)?* Retrieved from https://www.okta.com/uk/blog/2020/09/attribute-based-access-control-abac/

Keith, C. (2021). *The Definitive Guide to Attribute-Based Access Control (ABAC).* Retrieved from https://www.nextlabs.com/products/technology/abac/

Krimmer, R., Dedovic, S., Schmidt, C., & Corici. (2021). *Developing Cross-Border E-Governance: Exploring Interoperability and Cross-Border Integration.* Springer.

Krimmer, R., Dedovic, S., Schmidt, C., & Corici, A. (2021). Developing cross-border e-Governance: Exploring interoperability and cross-border integration. In Proceedings of the International Conference on Electronic Participation. Granada, Spain.

Luke, I. (2020). *The 6 Most Common Ways Data Breaches Occur*. Retrieved from https://www.itgovernance.eu/blog/en/the-6-most-common-ways-data-breaches-occur

Maile, M. (2022). *Understanding Role-Based Access Control (RBAC).* Retrieved from https://www.strongdm.com/rbac

Matt, B. (2020). *What Is GDPR? The Summary Guide to GDPR Compliance in the UK*. Retrieved from https://https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Mir, U., Kar, A., & Gupta, M. (2021). AI-enabled digital identity – inputs for stakeholders and policymakers. *Journal of Science and Technology Policy Management*.

N. Naik, P. J. (2017). Choice of suitable identity and access management standards for mobile computing and communication. *24th International Conference on Telecommunications (ICT)* (pp. 1-6). IEEE.

Neil, F. (2020). *GDPR: Third-Party Data Processors' Responsibilities*. Retrieved from https://www.itgovernance.eu/blog/en/gdpr-third-party-data-processors-responsibilities

Piotr, F. (2019). *What You Must Know about 'Third Parties' under GDPR and CCPA*. Retrieved from https://iapp.org/news/a/what-you-must-know-about-third-parties-under-the-gdpr-ccpa/

Reed, T. a. (2016). The inevitable rise of self-sovereign identity," . *The Sovrin Foundation*.

Ruff, T. (2018). *The three models of digital identity relationships*. Retrieved from https://medium.com/evernym/ the-three-models-of-digital-identity-relationships-ca0727cb5186

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Application Science*.

Sharma, S., Kumar Kar, A., & Gupta, M. (2021). Unpacking Digital Accountability: Ensuring efficient and answerable e-governance service delivery. *14th International Conference on Theory and Practice of Electronic Governance*, (pp. 260-269). Athens, Greece.

Sookhak, M., Jabbarpour, M., Safa, N., & Yu, F. (2021). Blockchain and smart contract for access control in healthcare: A survey issues and challenges and open issues. *Network Computer Applications*.

Sovrin.org. (2018). *A protocol and token for self-sovereign identity and decentralized trust*. Retrieved from https://sovrin.org/ wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors* .

Teresa M. Harrison, D. S. (2014). Transparency, participation, and accountability practices in open government: A comparative study. *Government Information Quarterly*, 513-525.

Vieira, R. (2018). The cyberpolitical space of the European Union: an overview of e-Government, e-Democracy and interoperability in the European space and its citizenship. *UNIO – EU Law Journal*, 117-127.

W3C. (2019). *A primer for Decentralized Identifiers*. Retrieved from https://w3c-ccg.github.io/did-primer/

W3C. (2019). *Verifiable Credentials Data Model 1.0*. Retrieved from https://www.w3.org/TR/vc-data-model/

Wimmer, M. V. (2020). Transforming government by leveraging disruptive technologies: Identification of research and training needs. *JeDEM - eJournal of eDemocracy and Open Government*, 87-113.

Windley, P. (2017). *Fixing the five problems of internet identity*. Retrieved from https://www.windley.com/archives/2017/10/fixing%20the%20five%20problems%20of%20internet%20identity.shtml