12-8-2023

# A conceptual decentralized identity solution for state government

Martin Duclos
*Mississippi State University*, md128@msstate.edu

# A conceptual decentralized identity solution for state government

By

Martin Duclos

Approved by:

Sudip Mittal (Major Professor)
Stephen Torri
George Trawick
T. J. Jankun-Kelly (Graduate Coordinator)
Jason M. Keith (Dean, Bagley College of Engineering)

A Thesis
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Computer Science
in the Department of Computer Science and Engineering

Mississippi State, Mississippi

December 2023

Name: Martin Duclos

Date of Degree: December 8, 2023

Institution: Mississippi State University

Major Field: Computer Science

Major Professor: Sudip Mittal

Title of Study: A conceptual decentralized identity solution for state government

Pages of Study: 34

Candidate for Degree of Master of Science

In recent years, state governments, exemplified by Mississippi, have significantly expanded their online service offerings to reduce costs and improve efficiency. However, this shift has led to challenges in managing digital identities effectively, with multiple fragmented solutions in use. This paper proposes a Self-Sovereign Identity (SSI) framework based on distributed ledger technology. SSI grants individuals control over their digital identities, enhancing privacy and security without relying on a centralized authority.

The contributions of this research include increased efficiency, improved privacy and security, enhanced user satisfaction, and reduced costs in state government digital identity management. The paper provides background on digital identity management in the public sector, discusses existing practices, presents the SSI framework as a solution, and outlines potential future research areas.

Key words: self-sovereign identity, digital identity management, state government, privacy, security, decentralized, verifiable credentials

# DEDICATION

I dedicate this work to my wife, Amy, and my children: Christopher, Audrey, Benjamin, and Addison, in gratitude for their love and support.

# ACKNOWLEDGEMENTS

I'd like to express my sincere thanks to the Department of Computer Science and Engineering at Mississippi State University and NSPARC for giving me the opportunity to complete this thesis.

I want to acknowledge and appreciate the valuable contributions of my committee members, Dr. Torri and Dr. Trawick. They generously dedicated their time and provided me with valuable guidance during the development of this thesis.

I also extend my special thanks to my major professor, Dr. Sudip Mittal, for his continuous support, expert guidance, and patience throughout not only this thesis but also beyond.

# TABLE OF CONTENTS

CHAPTER

## LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

In recent years, there has been a significant shift towards digital transformation in state governments. For instance, the State of Mississippi alone, more than doubled the scope of its online service offering to its residents, both in terms of number of unique services and number of entities providing them [25, 26]. Unsurprisingly, one of the many benefits of delivering services through an online channel is the reduction in cost. A 2015 study conducted by Deloitte revealed that the average cost of transaction is the lowest when using a digital platform [14]. However, this increasing trend in utilizing digital channels to streamline and enhance the delivery of public services has led to a growing need for improved digital identity management suitable for everyday tasks and transactions. As individuals and state government institutions increasingly conduct their interactions online, the advantages of having a reliable, efficient and secure method to authenticate and authorize their interactions becomes essential.

State government institutions are facing significant challenges when it comes to digital identity management. These institutions have the responsibility of overseeing diverse ecosystems that encompass both legacy and modern systems, as well as those obtained commercially off-the-shelf (COTS) or custom-developed to meet their specific needs. In government organizations, decision-making tends to be more autocratic at the department level [37]. This is exacerbated by the notion that traditional government tends to work within the silos of bureaucratic demarcation [39]. However, the implementation of identity management solutions across programs, whether centralized or decentralized, requires coordination among diverse stakeholders. Consequently, it is common to observe the deployment of multiple digital identity management solutions within state government IT environments as opposed to a single one. These solutions vary from basic username and password-based authentication to more sophisticated identity federation solutions. They are employed either individually or in tandem with other approaches to provide users with identity management.

As societal changes drive shifts in government regulations and policies, state systems must cope with new requirements [15]. However, confronted with competing priorities and diminishing resources, state IT personnel often resort to adopting multiple specialized turn-key systems for delivering digital services [40]. As a result, states are left grappling with a fragmented array of systems that are relied upon for mission critical tasks, such as the delivery of online services and digital identity management [1].

As described by Cameron, the internet is inherently lacking a mechanism for verifying and managing the identities of the individuals and organizations connected to it [8]. This poses a significant problem for online transactions where trust is essential. Moreover, this problem is particularly acute in the delivery of online public services, which typically involve the exchange of personally identifiable information (PII). To address the challenges caused by the absence of a trust layer, web application developers typically require users to prove their identity with a username and a password. As users provide their identities to multiple entities, the number of usernames and passwords they must maintain quickly becomes overwhelming. This situation can go from bad to worse if the same password is reused and one set of credentials is compromised. A common cyber-attack method consists of using a username and password combination obtained from a data breach to gain access to other systems utilizing the same username and password [4]. In the aforementioned scenario, the attacker relies on the known fact that many individuals reuse the same credentials across multiple systems, making it effortless for the bad actors to gain access to other systems with the leaked credentials. Online identity management across various entities is a standing issue in the public sector landscape and we propose to solve this problem by leveraging password-less verifiable credentials a part of a larger digital identity management strategy. We expand on our approach in Section 4.

Furthermore, state government institutions may require a proof of identity prior to providing individuals with certain type of services. For example, when an individual requests a service, they may be required to present a document such as a driver's license to verify their identity claim to a government employee. Identity verification can be time-consuming, expensive and necessitate the use of third-party resources. In Section 4 we elaborate on a solution that takes advantage of the portability of verifiable credentials to address this issue efficiently.

As part of their administrative duties, state government administrators will often use the Social Security Number (SSN) as the primary method to identify individuals across multiple programs. However, SSNs are considered Personal Identifiable Information (PII), and a breach or unauthorized release of PII can have severe consequences for all parties involved [4]. As a result, program stakeholders continuously seek ways to improve program evaluations methods while minimizing the risk of PII exposure. In Section 5 we present a method for data matching that doesn't rely on SSNs or other PIIs.

In this paper, we describe a solution for enhancing the online delivery of public services provided by state governments. Our solution is rooted in Self-Sovereign Identity (SSI), a framework built on distributed ledger technology (DLT). SSI is designed for managing digital identities while emphasizing user control and privacy, and avoiding reliance on single point of failure [45, 34, 7]. Within the SSI framework, individuals manage and store their own digital identities. They also retain authority over who can access their personal data and how it's utilized. Privacy of digital identities in SSI is achievable through an approach akin to Public Key Infrastructure (PKI). However, unlike PKI, which relies on a central Certificate Authority (CA) as a trust broker, SSI operates without centralized components. Moreover, as a decentralized identity management framework, SSI ensures high availability, critical for online transactions, by harnessing the power of distributed ledger technologies.

SSI holds the potential to improve the online delivery of public services, offering a more secure, user-centered digital identity management framework that strengthens trust and transparency between users and state government institutions.

By researching the use of SSI, we aim to offer insights into how this modern framework can:

- Increase efficiency
- Enhance privacy and security
- Improve user satisfaction
- Reduce costs

The remainder of this paper is organized as follows: Section 2 provides some background and related work on the topic of digital identity management within the public sector. In Section 3 we describe observed existing practices related to identity management within state government. 4

introduces our conceptual SSI framework as a practical and efficient solution for enhancing digital identity management in state governments. Section 5 outlines potential avenues for future research in the field of digital identity management within the public sector. Finally, Section 6 summarizes the paper's key findings and presents concluding remarks.

# CHAPTER 2

# RELATED WORK AND BACKGROUND

This section summarizes background concepts and some related work in digital identity, distributed ledger technologies, authentication, and trust. We also provide an overview of a generic SSI framework which is at the core of our solution proposed in Section 4.

## 2.1 Digital Identity

A digital identity can take on many forms. In his paper titled “The Laws of Identity”, Cameron et al. define a digital identity as a set of claims made by one digital subject about itself or another digital subject [8]. The authors go on and define a claim as: ”...an assertion of the truth of something, typically one which is disputed or in doubt”, and a digital subject as: “. . . a person or thing represented or existing in the digital realm, which is being described or dealt with”. In comparison, Pfitzmann et al. defined digital identity as a collection of attributes associated with an individual that can be accessed through technical means [33]. Pfitzmann further states that a digital identity is composed of smaller subsets known as partial identities. In other words, a partial identity can be as simple as an email address and name, or it can encompass a range of additional attributes.

Understanding the composition of a digital identity is key for developing secure, reliable, and efficient identity solutions [24]. This is especially true in the context of digital government, where different programs will require the verification of various combinations of claims or partial identities. To avoid the creation of new credentials for each government program or agency, which would contribute to account proliferation, careful planning is essential. We believe that such planning should not only account for future-proofing but also for the cross-portability of credentials from one service verifier to another.

## 2.2 Identity Management

In modern digital systems, the security provided by identity management is a ongoing research and development challenges. State governments have utilized varied identity management systems to manage the authentication and authorization to resources. Many identity management systems are structured as a token based architecture similar to the Public Key Infrastructure (PKI) certificate architecture.

PKI stands as a time-proven solution built on many years of research in cryptography [42]. As a result, PKI is widely considered to be the preferred solution for managing online digital identities. In that role, PKI is used for securing digital identities, ensuring the authenticity of communications, and safeguarding online transactions.

Self-Sovereign Identity (SSI) utilizes an external authority to confirm the veracity of user credentials which is similar to certificate verification procedure in the PKI architecture.

Self-Sovereign Identity (SSI) traces its origins back to the 1991 Pretty Good Privacy (PGP) project [32] (See Section 2.6). The concept of the Web-of-Trust (WoT) also originated from the PGP project [41]. In the context of WoT, a user can choose to trust other entities and as the user continues to add trusted entities to their WoT, other entities can reciprocate if they choose to. The creation of WoT played a significant role in advancing the field of decentralized authentication.

Expanding on WoT, Carl Ellison suggested in a paper that the idea of traditional identity certificate is neither necessary nor sufficient for establishing the identity of a key holder [16]. Ellison proposed a protocol that binds a pair of identities to a pair of public keys, without relying on certificates issued by a Central Authority (CA). This departure from the common trusted entity model, which was novel at the time, remains evident in today's decentralization aspect of the SSI framework.

Leveraging technology standards like WoT and PKI, SSI is being developed to provide a decentralized platform to enable users the ability to utilize their verified credentials across multiple systems. This has the ability to impact organizations such as local, state, and federal governments and their ability to simplify the on-boarding and management of users' access.

## 2.3 Authentication

In digital systems, identity alone isn't sufficient to grant access to restricted information or resources. Authentication is a process that serves as the mechanism through which an entity's claimed identity is validated. In other words, the authentication process acts as the gatekeeper responsible for allowing only users with an authorized identity to gain access to the restricted information or resource. The concept of authentication goes hand-in-hand with the concept of identity. While any entity can claim an identity [6], access to restricted resources can be granted only once the claim is authenticated.

Maintaining security through authenticated access control is of the highest priority, especially in highly secure environments such as government networks.

Traditionally, access control has been maintained through authentication using username and password. Passwords, as a form of credentials, have long been used within digital systems as a means to authenticate an identity. Figure 2.1, illustrates a centralized identity model, commonly used with usernames and passwords. The idea behind a password credential is that it links your identity, such as your profile on a website, to something that presumably only you should know. Passwords, PINs, and answers to security questions refer to a category of authentication factors known as “What you know?”. As previously mentioned is Section 1, the proliferation of credentials in the form of passwords can exacerbate the bad practice of re-using passwords.

Two other types of authentication factors are also widely acknowledged; “Who you are?” and “What you have?”. “Who you are?” pertains to biometric authentication and involves one or more unique biological traits, such as fingerprints, facial recognition, iris scans, or voice prints. Biometric authentication is successful when a digitized biological trait captured from an individual, is compared to a previously provided copy and found to be a match.

The remaining type of authentication factor, ”What you have?”, refers to using physical items or devices as authentication factors. Examples include smart cards, mobile phones, tokens, or other tangible objects that a user possesses. Authentication is successful when the user provides the information that only the physical item or device they possess can provide.

Additionally, utilizing or requiring more than one authentication factor is known as Multi-Factor Authentication (MFA). MFA has become a common practice by which modern systems are secured. However, recent changes in the methods used by threat actors have made MFA more vulnerable

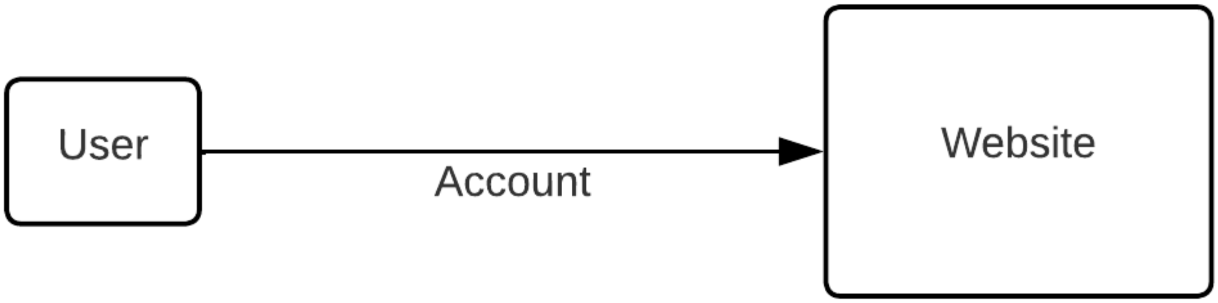

Figure 2.1

**Centralized Identity Model.** A model commonly found all over the internet, the centralized identity model is efficient and simple to implement. Under this model, a single identity provider authenticates users and issues digital credentials, such as usernames and passwords.

than ever. As such, many in the information security world are now suggesting that elevated threat models should not only be secured using MFA but also using a new standard referred to as Fast Online Identity (FIDO) [13]. FIDO provides a means to implement stronger authentication methods within the framework of MFA. It does so by removing the need for passwords and replacing them with cryptographic keys.

The utilization of biometrics and hadrware devices as a substitute for passwords may solve many password related issues. However, in the context of government service delivery, we must consider the effort and resources required to implement such an approach. As such, we believe this burden could prove to be too onerous for both the users and the identity provider, rendering this approach unfeasible.

A more measured approach is the Federated Identity Model, as illustrated in Figure 2.2. Under a federated model, only one set of digital credentials is needed to access multiple systems. As discussed earlier within the context of the Microsoft Passport, the federated model isn't without any shortcomings.

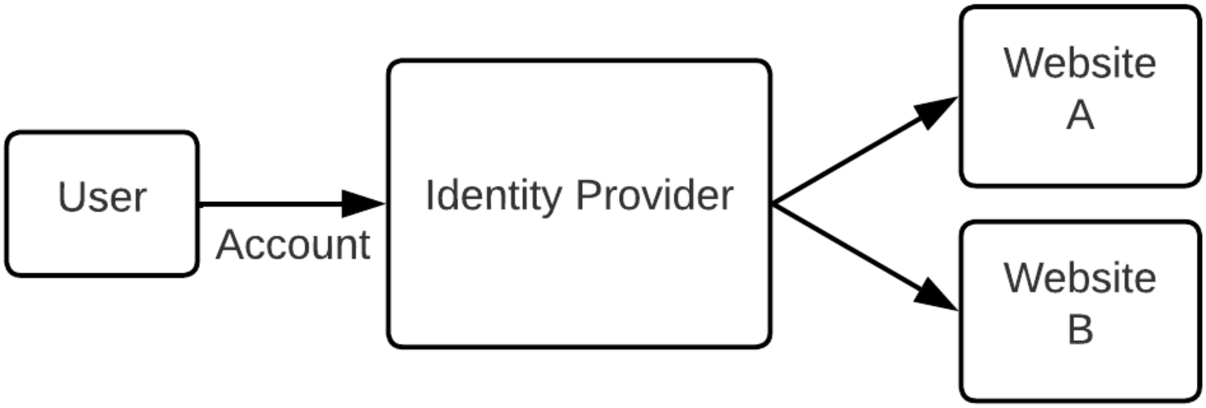

Figure 2.2

**Federated Identity Model.** The federated identity model alleviate the challenges associated with users managing multiple passwords. Users can leverage a single account from an identity provider to engage with multiple websites.

Requiring individuals to prove their identity and establishing trust before accessing secure systems is a fundamental for maintaining privacy and confidentiality as part of a security strategy.

## 2.4 Trust

Trust plays a central role within digital identity management as it forms the fabric upon which secure interactions such as authentication and communication are built [23]. For example, the Web-of-Trust (WoT) project presents a trust model based on reputation [41]. Utilizing nodes within the WoT, trust can be extended to parties that may not have a direct relationship with an entity. Likewise in the case of a federated digital identity model such as Microsoft's Passport, users were required to trust Microsoft as the central authority for authentication [9]. In contrast, within decentralized systems like Bitcoin, users primarily place their trust in the underlying technology rather than a centralized authority. They trust that the technology's cryptographic mechanisms, decentralized architecture, and consensus protocols will ensure the privacy and confidentiality of their transactions.

## 2.5 Decentralized Identity Management

In 2005, the Internet Identity Workshop (IIW) group, established under the Identity Commons umbrella, advanced the concept of a user-centric identity model [2]. IIW also supported the efforts behind OpenID which shares many similarities to modern decentralized identity frameworks such as SSI [17]. While OpenID showed progress, one of its notable benefits, the ability for users to self-register an identity, required a certain level of technical expertise. This left the majority of everyday users reliant on well-known identity providers like Facebook and Google. In other words, the decentralized model at the time, at it's core, still relied on a central entity.

While OpenID showed promise, it still had limitations, including a reliance on centralized identity providers. In contrast, the rapid rise in popularity of Bitcoin in 2009 marked an important shift in how we perceive decentralization. Born out of the idea to create a digital currency and payment system that operates without financial institutions, Bitcoin was created with decentralization at its core. Decentralization in Bitcoin is achieved by leveraging blocks linked together to form a secure, transparent and immutable chain of transactions [28]. The chain is then distributed amongst a network of nodes, ensuring availability.

The benefits provided by Blockchain can also be applied to identity management in the form of a distributed, immutable and transparent ledger. The Distributed Ledger Technology (DLT) can be used to record and verify identity related transactions and credentials. Therefore, it is our view that a decentralized architecture, similar to the one employed by Bitcoin, to be an essential component in offering more secure, transparent and user-centered digital identity management.

While implementing a DLT from the ground up is resource-intensive and impractical for most organizations, the need for decentralized identity management remains. This is where vendor solutions come into play, providing a straight path to taking advantage of decentralization in identity management. In such a scenario, the operation of the decentralized network as well as other components that make up the DLT, are the responsibility of the vendor. We consider this type of arrangement to be better suited to state government who's mission is to serve the public.

## 2.6 Self-Sovereign Identity (SSI)

Building upon the foundation of decentralized identity management discussed previously, we now focus on SSI. As a modern technology, SSI makes it possible for individuals to own, control, and share their personal information without relying on a centralized authority. In absence of a central component the SSI framework relies on three fundamental roles:issuer, holder, and verifier.

These three roles form a trust triangle, the differencing factor of SSI's innovative approach to digital identity management [34]. Together, these essential roles and their relationships offer a practical and efficient avenue for enhancing digital identity management. In the case of our solution, these roles enable individuals to minimize the number of password based credentials. The same roles also make it possible for individuals to prove their identity by keeping to a minimum the information they need to communicate to a verifier. In Section 4, we describe in details the advantages that SSI brings to our solution.

The SSI architecture relies on a set of interconnected technology components that work together to enable secure, transparent, and decentralized digital identity management. Each of these components plays a crucial role in establishing trust, ensuring privacy, and facilitating seamless interactions within the SSI framework. These components serve as the building blocks of a generic SSI architecture, which include Decentralized Identifiers, Verifiable Credentials, Decentralized Public Key Infrastructure, Blockchain and Distributed Ledger Technology, Verifiable Data Registry, Agents, and Digital Wallets.

Once provisioned, these technology components offer a robust platform for the development of a digital identity management system. In the context of our solution, all the components listed above are essential. To gain a deeper understanding of the role played by each component, Reece et al. have presented a comprehensive analysis in their paper on SSI [35], which provides valuable insights into this topic.

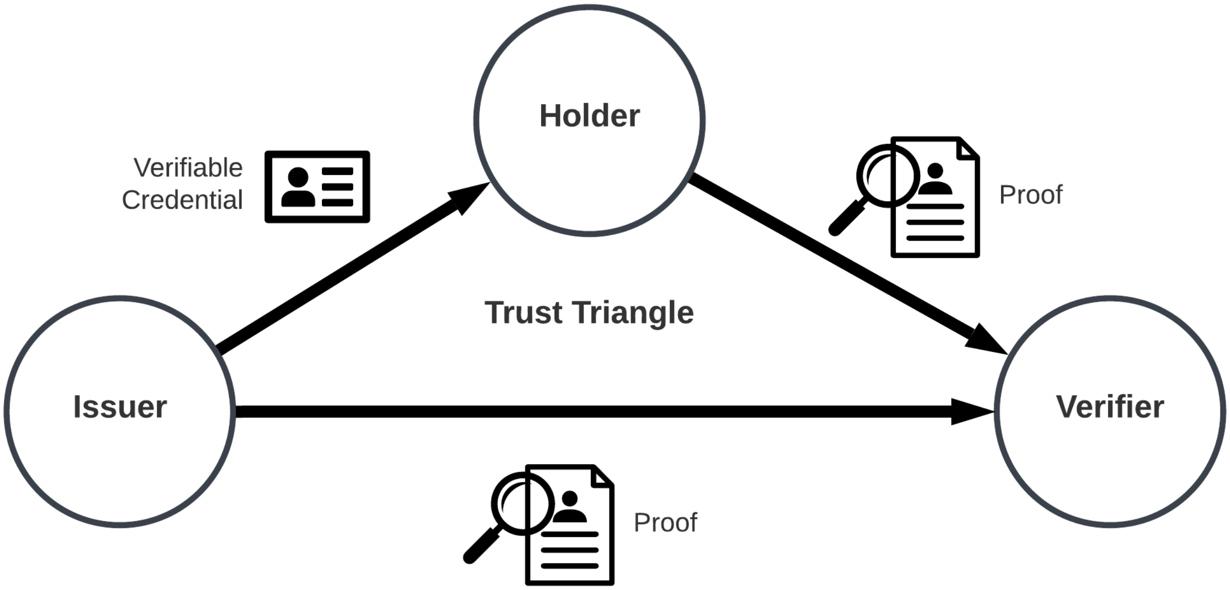

Figure 2.3

**Trust Triangle.** A trust triangle consisting of an issuer, holder, and verifier. Notice the lack of a central authority. Under SSI and many other solutions, the relationships and interactions between the entities are essential for secure and efficient identity management.

# CHAPTER 3

# PUBLIC SECTOR IDENTITY MANAGEMENT STRATEGIES

In this section we provide context on current identity management and verification strategies deployed in the public sector, and their respective limitations.

## 3.1 Systems Design and Architecture

As discussed in Section 1, various requirements are associated with providing online services to the public. State governments typically find that no single solution can meet all of the requirements as they deal with multiple programs and must comply with multiple sets of requirements. As a result, government organizations will often rely on a combination of custom-built and commercial off-the-shelf software systems to address their varied needs [3].

Considering the multitude of software systems in use within state governments, it becomes necessary to narrow our focus in this study to a single system architecture. For this reason we have chosen to concentrate on the monolithic architecture, a prevalent choice within state government circles. Monolithic applications tend to be easy to develop, deploy and maintain, which makes them a good choice for resource limited state agencies IT department [12, 30]. Although, outside the scope of this study, it is worth noting that many agencies still rely on systems designed for mainframe based hardware, while others are developing modern systems based on microservice and cloud native architectures. While modern architectures and design patterns offer numerous advantages in comparison to monolithic systems, they tend to be complicated to develop, maintain and deploy due to their inherent complexity. In summary, monolithic architecture dominates state government systems due to its practicality, especially for resource-limited agencies, despite the advantages offered by more modern architectures.

Monolithic architecture based systems might be the dominant type in state government but they are not without flaws. A monolithic architecture is a software architecture pattern where all components of an application are tightly integrated and packaged together into a single unit deployed on an infrastructure tier. Monolithic architectures have inherent shortcomings in terms of scalability, particularly with horizontal scaling. This constraint limits their ability to handle increasing workloads efficiently. More precisely, monolithic applications are designed as a single unit, making it difficult to scale by adding more application instances or nodes. Consequently, as the application workload increases, scaling vertically becomes the best option. Scaling vertically means adding resources to the existing server infrastructure, which has hard limits and can become expensive. In comparison, decentralized systems are typically composed of smaller, independent components or services that can be scaled independently. We discuss the benefits of decentralized systems with regards to scalability in Section 4.

## 3.2 Identity Management

Managing online identities can be challenging due to the interconnected nature of websites and the necessity for unique credentials for each account. As detailed in Section 2.1 digital identities can be made of one or many partial identities. To ensure the security of a user's partial identity, website developers typically require users to authenticate with a username and a password. As users interact with more websites, the challenges of keeping track of their identities and associated passwords become overwhelming.

Consequently, this proliferation of identities will result in users reusing passwords across different websites and adopting weak passwords. Such bad practices are actually quite prevalent. According to a survey of 3,000 adults conducted by Google in 2019, 65% of the respondents acknowledged the bad practice of reusing passwords in some capacity [20]. Additionally, a study performed by Florencio et al. revealed that users have on average seven distinct passwords [11]. An additional consequence tied to password reuse is that a single compromised account can trigger a domino effect. One single compromised set of credentials and lead to other accounts using the same credentials to also be compromised.

These bad practices are amplified by the situation around state government where certain services and assistance initiatives can be supplemented by those from other programs and agencies. For example, an individual receiving unemployment assistance from an agency may also be eligible for the Supplemental Food and Nutrition Program (SNAP), provided by another agency. Due to the fragmented nature of government systems, as mentioned in Section 1, a user facing this situation will likely be required to assume multiple distinct 'partial identities', also known as accounts.

In the context state government, digital identity management is a complex and multifaceted paradigm involving not only identities and systems but also the human side of navigating through multiple programs and agencies [21]. In Section 4 we suggest a method to alleviate the burden associated with the usage of usernames and passwords and to enhance security of credentials.

### 3.3 Identity Verification

Identity verification is the process of confirming the identity of an individual to ensure they are who they claim to be. It is a crucial component of security and trust in various contexts, including online service delivery.

State agencies commonly perform identity verification to meet reporting and performance requirements. While some have adopted the Federal initiative known as login.gov, many operate independently. Some will purchase access to costly third party database to facilitate the verification process, while others face resource constraints and a lack of inter-agency cooperation. In such cases, individuals bear the burden of providing credentials to each agency, even requiring in-person visits. Additionally, state agencies, like those handling Unemployment Insurance (UI), must strike a balance between assisting those in need and safeguarding against fraud. UI programs have become targets for criminals seeking quick gains, resulting in compromised identities among beneficiaries [31]. This situation puts the agency in a bind where they have to compromise between issuing assistance to those in needs and keeping fraud at bay.

In Section 4, we discuss the advantages provided by SSI to alleviate the burden associated with identity verification, for both the individuals and state agencies.

### 3.4 Privacy and Confidentiality

As part of their administrative duties, state agencies typically conduct program evaluations with the objective of improving efficiency [29]. Such activities will often require state agencies to establish linkages for individuals between multiple data sets. Agencies must frequently perform linkages because the information required to evaluate a specific program might be collected by two or more different systems [44]. Most systems employed by state agencies operate in isolation from other systems and, therefore, lack the concept of data linkages across multiple systems. Isolated systems and the absence of an established common, shareable individual identifier for program participants make program evaluation a daunting task.

As part of the program evaluation task, state agency personnel attempt to link individuals from one program to another using multiple error-prone and time-consuming approaches. Many of these approaches involve a trial-and-error method, where various combinations of data elements, such as name, address, birth date, or other identifying information, are tested to find a common link between the datasets. The trial-and-error approach can be time-consuming and may result in incorrect matches or false positives if the data elements used are incomplete or inaccurate. Agencies often rely on the Social Security Number (SSN) as the primary method to identify individuals across multiple datasets [10]. However, many individuals are becoming reluctant to share their SSN due to privacy and confidentiality concerns. The SSN is considered Personal Identifiable Information (PII), and a data breach or unauthorized release of this information can lead to costly consequences [4].

Our approach, presented in Section 4, discuss in more details how the use of a Decentralized Identifier (DID) can solve many issues plaguing program evaluation.

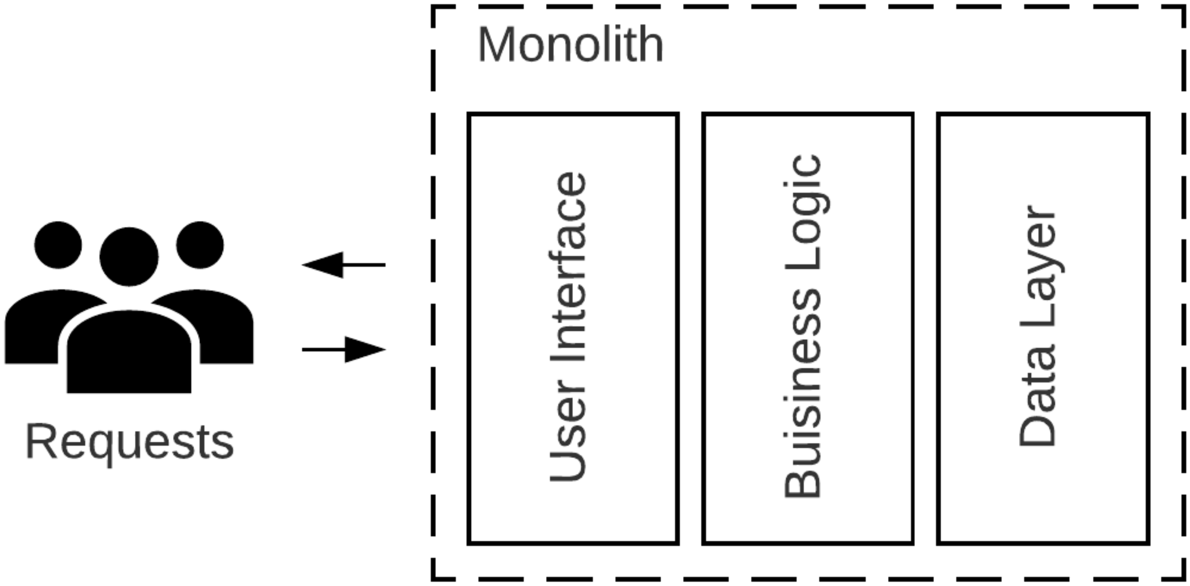

Figure 3.1

**Monolithic Architecture.** In a monolith application, http requests and responses pass between the presentation layer, application layer, and data layer. The same three layers reside on a single tier.

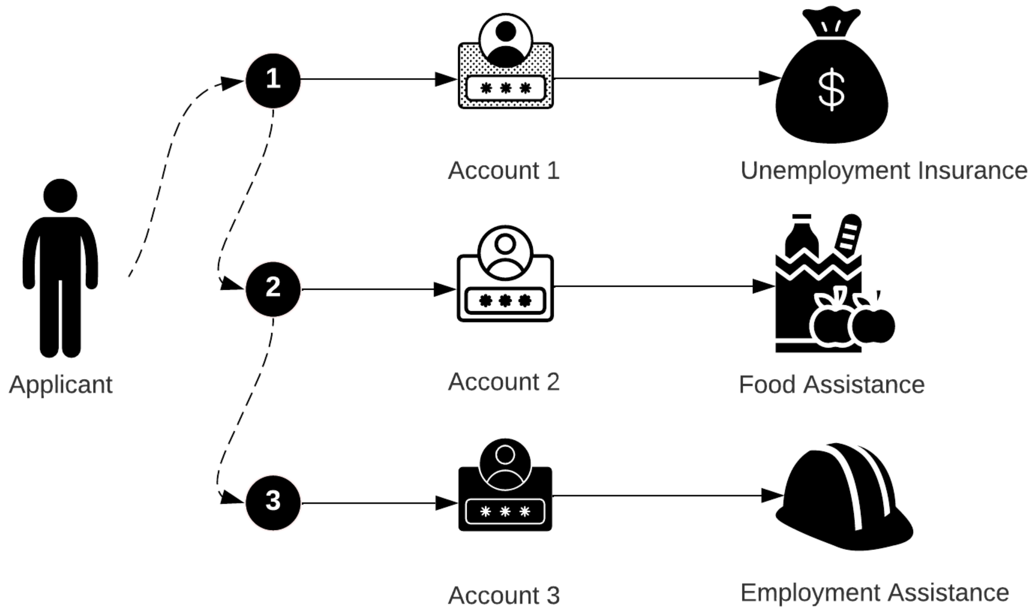

Figure 3.2

**Interactions.** Illustration of the interactions a user must go through in order to receive or apply for services from different programs or agencies. In this example, a user is applying and receiving services provided by three different programs. (1) A user first create an account with the agency responsible for providing unemployment insurance benefits. (2) Next, the user creates another account, this time with the agency responsible for providing food assistance. (3) Finally, the user creates a third account with the program tasked with reemployment assistance. In this example, to apply and receive services from three different programs a user would be required to manage a total of three sets of partial identities, usernames and passwords.

# CHAPTER 4

# ENHANCING PUBLIC SECTOR IDENTITY MANAGEMENT THROUGH SSI

In Section 3, we examined the challenges faced by state governments related to digital identity management. In this section, we delve into potential solutions to address those challenges, through the use of SSI.

## 4.1 Scalability in Decentralized Systems

In Section 3.1 we discussed the limitations of applications based on a monolithic architecture, highlighting that these applications face challenges dealing with increased workload due to their lack of predisposition for horizontal scaling [5].

Horizontally scaling, or scaling out, is also challenging in decentralized systems. However, decentralized systems like SSI have inherent features and design principles that make them well-suited for efficiently handling increased workloads. These features include peer-to-peer interactions, privacy-centric design, and interoperability, among others, which contribute to their suitability for handling scalability challenges.

It's important to recognize that addressing scalability concerns is crucial, especially when the user base consists of the entire population of a state. Recent success stories in the Netherlands and Estonia, where SSI solutions have been deployed at a national level, provide compelling evidence of

SSI's scalability [43]. These national implementations serve as real-world proof that decentralized systems like SSI are well-suited to efficiently handle substantial workloads.

While not all government entities encounter scalability challenges, those adopting SSI can have confidence that their identity management solution will not be the cause of a performance bottleneck.

## 4.2 Enhanced Digital Identity Management

Digital Identity Management is at the core of SSI. In Section 3.2 we identified issues brought forward by the proliferation of accounts and credentials. We can alleviate these issues through the use of passwordless authentication [18].

Passwordless authentication is designed to enhance the security and convenience of user authentication by eliminating the need for usernames and passwords. In a typical password based authentication process, users are required to create and remember usernames and passwords to access their accounts. As described in Section 3.2, such an approach encourages bad security practices on the part of the users receiving online services.

Passwordless authentication can enhance security around online services by eliminating the need for usernames and passwords and therefore reducing account credentials proliferation. We believe this user-centric method provided by an SSI solution can effectively mitigates risks such as phishing attacks and credential stuffing.

SSI Passwordless authentication is possible through the use of Decentralized Identifiers (DID) and a method referred to as DID Auth [36]. In the context of SSI, DIDs are unique identifiers created by users and stored in a decentralized ledger. Figure 4.1 illustrates how DIDs can be used to authenticate users without the need for a central authority [22].

In summary, passwordless authentication is an innovative approach to perform access control, capable of improving the security and convenience of online services.

### 4.3 Improved Identity Verification

Self-Sovereign Identity (SSI) is an emerging user-centric approach to identity management that enables individuals to own and control their personal data. Using SSI, users can establish Verifiable Credentials (VC) that can be shared with service providers in a secure and privacy-preserving manner [38].

VCs are instrumental in addressing the issues related to identity verification described in Section 3.3. When a user needs to receive a service that requires identity verification, the agency performing the verification can issue a VC, which can then be trusted by other agencies. This eliminates the need for another agency to go through a separate identity verification process. This concept is similar to how we leverage a driver's license in the physical world. However, with SSI, once a VC has been established, future transactions can occur entirely in the digital world through built-in trust mechanisms [35]. We anticipate that leveraging VCs would not only save time and effort for the users but also reduce costs and administrative burden for the agencies.

Overall, SSI and the use of VCs, offer a more efficient and secure approach to identity verification, with the potential to improve the user experience and reduce costs for both users and agencies.

## 4.4 Strengthening Privacy and Confidentiality

As stated in Section 3.4, PII is often collected and used by state agencies as an alternative to a common identifier that can be across multiple programs. This requirement implies that states must store this personal information for later use, thereby increasing the chance of disclosure.

Unlike traditional identity management systems that rely on centralized architecture, SSI does not require a central repository of personal information. This helps reduce the risk of data breaches and unauthorized disclosure of sensitive information. More importantly, SSI provides users with a critical piece of information, a Decentralized Identifier (DID). A DID uniquely identifies a user and also provides states with an alternative to using a social security number for program evaluation purposes.

Moreover, the SSI framework incorporates a strong decentralized encryption to protect user data. Decentralized encryption is a technique that distributes encryption keys across multiple devices or nodes in a network, making it more difficult for unauthorized parties to gain access to the data. Additionally, SSI employs privacy-enhancing technologies, such as zero-knowledge proofs and selective disclosure, to further enhance privacy and confidentiality of user information. Zero-knowledge proofs enable users to prove a statement to a verifier without revealing any additional information beyond the statement itself [19]. Selective disclosure allows users to share only necessary information with a verifier while keeping other sensitive information hidden. [27].

SSI enhances privacy and security by giving users more control over their data, fostering trust between users and agencies, thus making it a promising solution for modern identity management in state government.

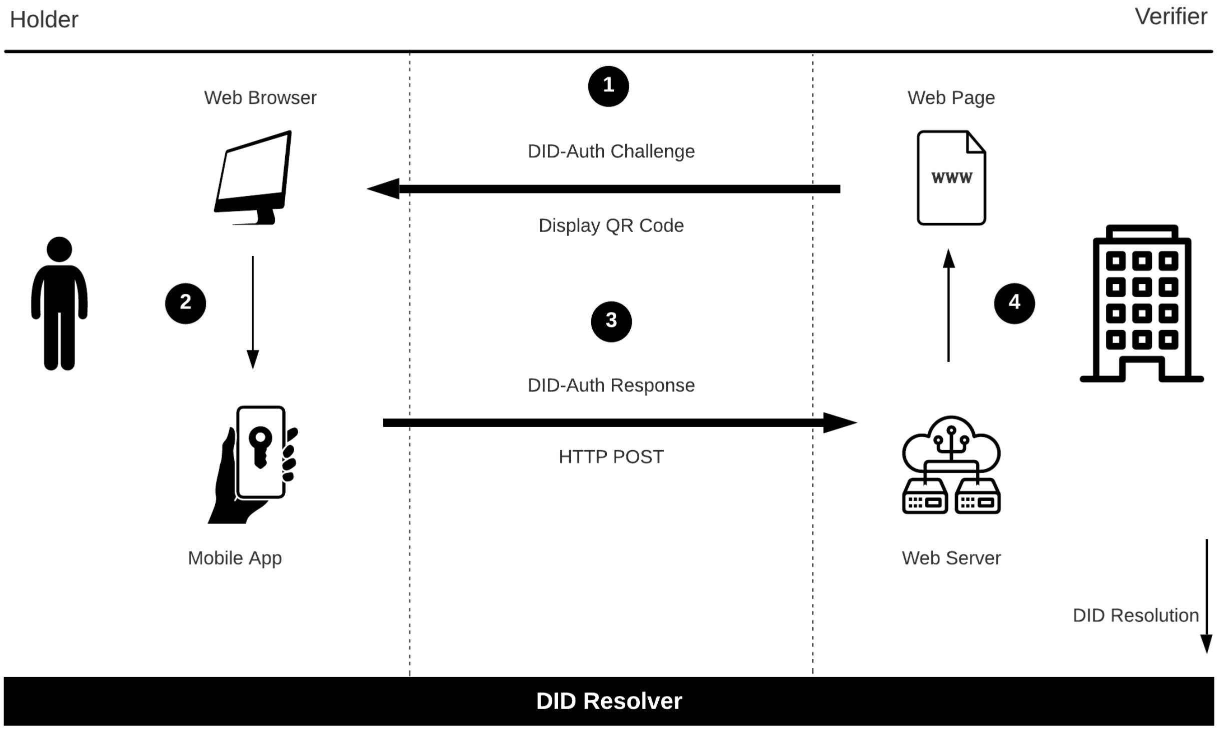

Figure 4.1

**DID Auth.** A form of passwordless authentication, DID Auth enables users to use a verifiable credential to authenticate against online systems. DID Auth provides a more secure, user-centric, and user-friendly alternative to traditional password-based authentication methods. Here's how it works: (1) A verifier, typically an online system, issues a request for authentication. (2) The user processes the request using a digital wallet. (3) The user's digital wallet presents a verifiable credential to the verifier. (4) The verifier validates the legitimacy of the credential against the distributed ledger using a process called DID Resolver."

# CHAPTER 5

# FUTURE RESEARCH

In the realm of SSI within state government organizations, several areas warrant further exploration. One such area of SSI implementation in state government involves the development of tailored schemata designed to meet the unique needs of various government agencies and programs. These tailored schemata could optimize data entry efficiency, security and foster collaboration among agencies.

However, to ensure the safeguard of users' digital identities effectively, it is important to establish a unified threat model. This model would address the specific challenges and vulnerabilities inherent in the intersection of SSI and state government operations. Proactively addressing security risks is essential to ensuring user confidence and adoption.

Furthermore, a novel avenue for future research is the exploration of a hybrid approach to digital identity management. This approach aims to merge traditional identity management systems with SSI, leveraging the benefits of both systems to provide a versatile solution. This hybrid approach could offer scalability and interoperability while maintaining security.

Future research opportunities in the realm of SSI and its adoption within state government organizations hold significant potential. These efforts could improve identity management practices, enhance security measures, and streamline government operations. By addressing these critical areas, valuable insights can be contributed to the evolving field of digital identity in the public sector.

# CHAPTER 6

# CONCLUSIONS

In this paper, we've explored the impact of SSI on identity management within state government organizations. We have presented SSI as a decentralized and scalable solution for digital identity management in state government. We have discussed how passwordless authentication is a core element of SSI, enhancing security and user convenience. We have also presented the role of verifiable credentials and how their usage can reduce costs and administrative burdens for both users and agencies. We have also described how Decentralized Identifiers can not only be used by state agencies for matching records across programs but also to avoid collecting PII. Additionally we have shown how privacy can be enhanced through the use of zero-knowledge proofs and selective disclosure to empower users to control their data.

In conclusion, our research highlights the potential of SSI to transform identity management within state government organizations.

# REFERENCES

[1] G. Affairs, U. S. Senate, and K. Walsh, *Threats and Spending Oversight , Committee on Homeland Security and INFORMATION Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems*, Tech. Rep., U.S. Government Accountability Office, 2021.

[2] C. Allen, "The Path to Self-Sovereign Identity,", 4 2016.

[3] N. Author, "2020 State CIO Survey,", 2020, Accessed: 2023-06-07.

[4] K. Beck, "LinkedIn resetting passwords after 117 million user credentials stolen,", 2016.

[5] G. Blinowski, A. Ojdowska, and A. Przyby lek, "Monolithic vs. microservice architecture: A performance and scalability evaluation," *IEEE Access*, vol. 10, 2022, pp. 20357–20374.

[6] BlueCheck, "What is Identity Authentication?,", 2021.

[7] C. H.-J. Braun, V. Papanchev, and T. Käfer, "SISSI: An Architecture for Semantic Interoperable Self-Sovereign Identity-based Access Control on the Web," *Proceedings of the ACM Web Conference 2023*. 4 2023, pp. 3011–3021, ACM.

[8] K. Cameron, "The Laws of Identity," *Unknown*, 2005.

[9] D. W. Chadwick, "Federated identity management," *International School on Foundations of Security Analysis and Design*, Springer, 2007, pp. 96–120.

[10] J. J. Darrow and S. D. Lichtenstein, "Do You Really Need My Social Security Number - Data Collection Practices in the Digital Age," *North Carolina Journal of Law & Technology*, vol. 10, 2008, p. 1.

[11] F. Dinei, Florêncio, and C. Herley, "A Large-Scale Study of Web Password Habits," *WWW 2007 / Track: Security, Privacy, Reliability, and Ethics Session: Passwords and Phishing*, 2007.

[12] N. Dmitry and S.-S. Manfred., "On micro-services architecture," *International Journal of Open Information Technologies*, vol. 2, no. 9, 2014, pp. 24–27.

[13] J. Easterly, "Next Level MFA: FIDO Authentication,", 2022.

[14] D. A. Economics, "Digital government transformation,", 2015.

[15] W. D. Eggers and M. Turley, "The future of regulation Principles for regulating emerging technologies A report from the Deloitte Center for Government Insights MIKE TURLEY," *Deloitte Insights*, 2018, p. 32.

[16] C. M. Ellison, "Establishing Identity Without Certification Authorities," *Sixth USENIX Security Symposium*. 7 1996, vol. 7, pp. 67–76, USENIX.

[17] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," *IEEE Access*, vol. 7, 2019, pp. 103059–103079.

[18] M. S. Ferdous, A. Ionita, and W. Prinz, "SSI4Web: A Self-sovereign Identity (SSI) Framework for the Web," *International Congress on Blockchain and Applications*. Springer, 2022, pp. 366–379.

[19] U. Fiege, A. Fiat, and A. Shamir, "Zero knowledge proofs of identity," *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, 1987, pp. 210–217.

[20] Google, "Online Security Survey,", Google, Feb. 2019.

[21] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines.(National Institute of Standards and Technology, Gaithersburg, MD)," *NIST Special publicaiton 800-63-3*, vol. 58, no. 2, 2020, pp. 130–137.

[22] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials," *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2020, pp. 71–78.

[23] C. Lynch, "Authenticity and integrity in the digital environment: an exploratory analysis of the central role of trust," *Museums in a digital age*, Routledge, 2013, pp. 314–331.

[24] R. J. McWaters, "A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity An Industry Project of the Financial Services Community — Prepared in collaboration with Deloitte Part of the Future of Financial Services Series •,", 2016.

[25] Mississippi Department of Information Technology Services, *2018 Annual Report*, Tech. Rep., MDITS, 2018.

[26] Mississippi Department of Information Technology Services, *2020 Annual Report*, Tech. Rep. December, MDITS, 2020.

[27] R. Mukta, J. Martens, H.-y. Paik, Q. Lu, and S. S. Kanhere, "Blockchain-based verifiable credential sharing with selective disclosure," *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020, pp. 959–966.

[28] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System,", 2008.

[29] K. E. Newcomer, H. P. Hatry, and J. S. Wholey, *Handbook of Practical Program Evaluation*, chapter PERFORMANCE MEASUREMENT: Monitoring Program Outcomes, Wiley Online Library, 2015, pp. 100–124.

[30] S. Newman, *Monolith to Microservices: Evolutionary Patterns to Transform Your Monolith*, 1 edition, O'Reilly Media, 2019.

[31] U. D. of Labor – Office of Inspector General, *EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY REPORT CARES ACT: INITIAL AREAS OF CONCERN REGARDING IMPLEMENTATION OF UNEMPLOYMENT INSURANCE PROVISIONS*, Tech. Rep., USDOL, 2020.

[32] OpenPGP, "History of OpenPGP,", 2016.

[33] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," *Technical University Dresden*, 2010, pp. 1–98.

[34] A. Preukschat and D. Reed, *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*, Manning, 2021.

[35] M. Reece and S. Mittal, "Self-Sovereign Identity in a World of Authentication: Architecture and Domain Usecases,", 2022.

[36] M. Sabadello, K. Den Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan, and D. Zagidulin, "Introduction to did auth," *Rebooting the Web of Trust VI*, 2018.

[37] M. Schraeder, R. S. Tears, and M. H. Jordan, "Organizational culture in public sector organizations," *Leadership & Organization Development Journal*, vol. 26, 9 2005, pp. 492–502.

[38] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, 2021, pp. 603–613.

[39] P. Shergold, *Learning from Failure: Why large government policy initiatives have gone so badly wrong in the past and how the chances of success in the future can be improved*, Tech. Rep., Australian Public Service Commission, 2015.

[40] N. Staff, "The State of Cloud in State and Local Governments,", June 2021, Accessed: 2023-06-07.

[41] H. Stahl, T. Capilnean, P. Snyder, and T. Yasaka, "Peer to Peer Degrees of Trust a white paper from Rebooting the Web of Trust VII,", 2018.

[42] J. Stapleton, "A Concise History of Public Key Infrastructure,", 2012.

[43] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," *2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 2018, pp. 1336–1342.

[44] U.S. Department of Labor, "Annual WIOA Performance Assessments,", 2023.

[45] Špela Čučko, V. Keršič, and M. Turkanović, "Towards a Catalogue of Self-Sovereign Identity Design Patterns," *Applied Sciences (Switzerland)*, vol. 13, 2023.