ISSN 2281-5147

SELF-SOVEREIGN IDENTITY: THE REVOLUTION IN DIGITAL IDENTITY

Cristian Lepore*

Abstract

Digital identity is important for businesses and governments to grow. When apps or websites ask us to create a new digital identity or log in using a big platform, we do not know what happens to our data. That is why experts and governments are working on creating a safe and trustworthy digital identity. This identity would let anyone file taxes, rent a car, or prove their financial income easily and privately. This new digital identity is called Self-Sovereign Identity (SSI). In our work, we propose an SSI-based model to evaluate different identity options and we then prove our model value on the European identity framework.

Table of Contents

SELF-SOVEREIGN IDENTITY: THE REVOLUTION IN DIGITAL IDENTITY 59

Abstract 59

Keywords 60

1. Introduction 60

2. What is digital identity 61

*Cristian is a cybersecurity fellow and ESR at the University Paul Sabatier. He is the primary maintainer of the SecTeal compiler and the original architect of the AuthclicK application. In 2020, Cristian focused his activity on formal models and digital identity. In 2021, he assessed the self-sovereign identity European framework (eIDAS) to figure out possible challenges and solutions. Previously, Cristian worked in the industry as a cryptographic engineer and infrastructure analyst. In the LeADS project, he will gain the critical thinking to lead the next wave of innovation and push his research forward

.This work is supported by the European Union's funded project Legality Attentive Data Scientists (LeADS) under Grant Agreement no. 956562.

ISSN 2281-5147

3. Self-Sovereign Identity 64
4. The European study case..... 65
4.1 Limitations..... 68
5. Building the future of identity 69
6. Conclusion 72

Keywords

Digital identity - Self-sovereign identity – Security – eIDAS - European ID

1. Introduction

Digital identity is crucial for businesses and governments because it helps build trust with customers and citizens (Camp, 2004). In our connected world, we often need to create new online accounts or log into different websites and apps. This raises important questions about how our personal information is managed and kept safe (Ansaroudi et al., 2023). It's completely normal to be concerned about the risk of our data being misused or stolen.

To tackle these issues, experts in the industry and governments are teaming up to develop secure and trustworthy digital identities for people. This new approach, known as Self-Sovereign Identity (SSI), represents a major step forward in how we think about identity (Satybaldy et al., 2020). With this approach, individuals can better protect their personal information and have more control over how their data is managed.

With Self-Sovereign Identity, people can easily and privately show things like tax statements, rent cars, or prove their income without giving away extra personal information (et al Alvaro Martin, 2019). For instance, when applying for a rental car, a person can present their driver's license and insurance information without needing to disclose their home address or date of birth. Similarly, when applying for a loan, they can share their verified income statement directly from their financial institution

ISSN 2281-5147

without exposing unnecessary personal details, like their full social security number or banking history. This approach empowers individuals to control their data and share only what is necessary, enhancing both privacy and security.

Currently, there are no clear rules to guide experts in creating and distinguishing Self-Sovereign Identity solutions, making it challenging to assess the impact of new technologies. For example, does a mobile wallet truly empower individuals to control their identities? What specific mechanisms allow users to have control over their personal data and identity? What factors determine whether an SSI system is truly secure?

To answer these questions, we began with a simple explanation of Self-Sovereign Identity, supported by practical examples (Section 3), and outlined the European Union's efforts in developing a secure identity system for citizens (Section 4). This was supplemented with easily understandable examples, along with a proposed approach to evaluate Self-Sovereign Identity (Section 5). Additionally, we created an image that illustrates our approach and described its components using everyday objects. In the future, clear rules would be highly beneficial for evaluating solutions proposed by private companies and governments.

2. What is digital identity

The Internet is like a massive web connecting computers and smartphones around the globe, enabling people to communicate, share information, and explore contents. From catching up on the latest news and watching entertaining videos to connecting with friends on social media, the Internet has transformed the way we live and interact. Nowadays, it is hard to imagine a day without searching for answers to questions or shopping online from the comfort of our homes.

In its early days, the Internet was a playground for a small community of academics and researchers who trusted one another (Johnson Jeyakumar et al., 2022). Because of this, security was not a major concern; they believed that everyone online had good intentions. However, as the Internet grew and became a central part of everyday life, its landscape changed dramatically. Today, nearly everyone owns a smartphone and relies on the Internet for everything from work and communication to entertainment.

ISSN 2281-5147

Unfortunately, this increase in Internet use has also led to serious security issues. Problems like online fraud, identity theft, and hacking of social media accounts are now common threats that can affect anyone, from individuals to large businesses ('A Brief History of the Internet', 2023). These issues can lead to stolen personal information, financial loss, and a feeling of vulnerability in the online world. In summary, while the Internet offers incredible opportunities for connection and information, it also poses risks that we must navigate carefully. To address these challenges, the concept of digital identity has emerged as a potential solution.

Digital identity is a term that refers to how you present yourself in the online world (Davie et al., 2019). It encompasses everything from basic personal information – like your name, date of birth, and email address – to the way you behave and interact with others on the internet. Think of it as your online persona, which follows you around whenever you visit websites or use apps on your phone (*Digital Identity in the ICT Ecosystem*, 2023).

To better frame the concept, let's describe the (online) identity in a way that's easy to understand, using the example of setting up an Instagram account, a platform where people connect by sharing images, videos, and stories from their lives. Imagine you decide to join Instagram to share your experiences with friends and family. The first step is to create an account, which is like establishing your identity in the digital world (Commission, 2023). You start by filling out some personal information, which helps define who you are online. This includes picking a unique username, entering your full name, and providing your email address. Next, you create a secure password to protect your account. Now your profile is beginning to take shape. This profile serves as your digital identity on Instagram. You can upload a profile picture that represents you – maybe a fun snapshot from a recent trip or a casual selfie. Additionally, you can write a short bio that shares a bit about yourself, like "Adventure seeker and photography enthusiast." This bio helps others understand your interests immediately. Once your profile is set up, it becomes your digital business card, showcasing who you are and what you love. You start posting content – photos of your travels, snapshots of your daily life, or even videos of special moments. Each piece of content you share, along with captions and hashtags, contributes to building your online identity. For example, if you post a picture from a recent mountain hiking trip, your friends can react to it by liking or commenting on the photo. This

ISSN 2281-5147

interaction not only enhances your online identity but also fosters a sense of community, connecting you with others who share similar interests. Your Instagram profile is more than just a collection of photos; it represents your personality, passions, and experiences in the digital landscape. Over time, as you engage with others and share more content, your digital identity evolves, reflecting the unique story of who you are and how you connect with the world.

In addition to regular posts, you also use Instagram Stories, which allow you to share more casual and fleeting moments. Stories disappear after 24 hours and offer a glimpse into different aspects of your life, like having coffee with friends or enjoying a breathtaking view. These daily interactions enrich your digital identity, making you more accessible and relatable. As you start following other users, you build a social network. Each time you interact with their content – whether through comments or direct messages – you contribute to a mutually connected environment. If you follow many travel accounts, Instagram will suggest similar profiles and show you relevant content, personalizing your experience on the platform.

In summary, your experience on Instagram extends beyond sharing photos; it reflects your identity, passions, and relationships. Every post, comment, and interaction help shape the overall image of who you are in the digital world, creating bonds and connections that go beyond the screen.

As of today, in many situations, people's identities are managed by the government or other authorized organizations. This means that governments have the power to control how a person's identity is used in society. This situation can feel like a form of "hostage-taking," because individuals are dependent on the rules set by these authorities to access services, travel, or participate in certain activities. For example, governments decide who gets a passport, who is allowed to vote, and who can access healthcare, all based on verified identity information. In this way, people's identities become a tool that the government uses to control access to rights and opportunities.

Many people today have little control over how their personal information is handled online. Decisions about what happens with their data are often made by companies or organizations without clearly explaining it to the public. This lack of transparency has led to the development of a new approach to managing personal identity information, designed to give individuals more power over their own data. This concept allows people to take charge of their identity information, deciding what to

ISSN 2281-5147

share, with whom, and under what conditions. By doing so, they gain more control and privacy in the digital world. One of the most advanced models in this area is called Self-Sovereign Identity (SSI) (Laatikainen et al., 2021). SSI is built on the idea that individuals, not intermediaries, should own and manage their personal data. It empowers users to securely store their identity information and share it only, when necessary, without needing a central authority to approve or manage their actions (Soltani et al., 2021).

3. Self-Sovereign Identity

Self-Sovereign Identity (SSI) is a new way of thinking about how people manage and control their personal information in the digital world. Traditionally, our personal data – like our name, address, or online profiles – is stored and controlled by large organizations like social media companies, banks, or government institutions (Ehrlich et al., 2021). We trust these intermediaries to keep our data safe, but they often have access to more information than necessary and could be vulnerable to breaches or misuse. SSI turns this model upside down. With SSI, you own your digital identity, just like you own your passport or ID card in the real world. You get to decide who sees your information, what details you want to share, and for how long (Ruff, 2018).

Let's take the example of Giulia, a European citizen who needs to apply for a tourist visa for an international trip. Traditionally, Giulia would have to collect and send several physical or digital documents – like her passport, bank statements, and proof of residence – via email or mail to the embassy. This process can be time-consuming, potentially risky, and involves sharing more personal information than necessary.

In an SSI system, things work differently and much more smoothly. Giulia has a unique digital identity, which is stored in a digital wallet (an application) on her phone or computer. In this digital wallet, Giulia holds verified credentials such as her passport information, proof of her financial stability from her bank, and government certifications that prove her nationality.

When Giulia applies for a visa, instead of sending all her documents, she simply shares the relevant details directly from her wallet. For example, she can allow the embassy to verify her nationality and passport details, as well as her financial status, without showing unnecessary information like her home address or full banking history. Giulia

ISSN 2281-5147

decides exactly what information to share and for how long the embassy can access it. Once the visa process is complete, she can easily revoke access to her data, ensuring that her personal information is not unnecessarily exposed for longer than needed.

The security of this system is much higher because the information Giulia shares has already been verified by trusted authorities like her government or bank, significantly reducing the chances of fraud or document forgery. Also, since everything is handled through her digital wallet, the need to send documents back and forth or navigate cumbersome bureaucratic procedures is eliminated. The process is quicker, more private, and more secure.

But SSI is not limited to visa applications. Giulia could use the same wallet to prove her identity when opening a new bank account, sign a job contract, or demonstrate her qualifications when applying for a new position. The system allows her to control her data, share only what's necessary, and ensure her privacy is respected throughout different interactions – all through a single, easy-to-use digital platform.

In Europe, there are several initiatives aimed at improving digital identity systems, with governments, universities, and businesses working together to make it happen (Sharif et al., 2022). These programs are designed to give citizens more security and control over their personal information, while also making digital services more transparent and reliable for everyone.

4. The European study case

In the 2010s, the European Union (EU) took a leading role in exploring how a regional online identity system could benefit its citizens. This led to the creation of eIDAS (Electronic Identification, Authentication and Trust Services), a groundbreaking initiative aimed at providing all Europeans with a secure digital identity (Susanna, 2022). The idea behind eIDAS is to give people a reliable way to prove their identity online, much like using a passport or ID card in the physical world. However, the journey to achieving this has been far from simple.

The eIDAS system officially came into effect in 2016 (Commission, 2016). Initially, each EU country had a lot of control over how they managed their citizens' digital

ISSN 2281-5147

identities. While this seemed like a flexible approach, it resulted in uneven progress across the region. By the late 2010s, fewer than half of Europeans had access to a usable electronic identity, which limited the effectiveness of the system (Sharif et al., 2022).

It was in 2020 that the EU recognized the need for a more unified approach. This realization led to a major shift: instead of each country working independently, the EU began pushing for a single, standardized digital identity system across all member states. This system would be based on Self-Sovereign Identity (SSI).

A revision of the original regulation, in February 2022, led to the introduction of the Architecture Reference Framework (ARF) (Commission, 2023), a blueprint for how this unified digital identity should work. The first draft of this framework came out in February 2023, and discussions continue as it evolves.

As of today, several technical and legal documents guide the development of this European digital identity system. The key component is a "digital wallet" that will serve as a personal online ID for European citizens. It is expected to be fully operational by the end of 2026.

When finished, the system will offer a major convenience to citizens across Europe. For example, a person could use their digital identity to access services or request official documents (like civil registration records) online, even while living or traveling abroad, without having to physically return to their home country. This marks a big step toward seamless digital integration within the EU, making life simpler for millions of people across the region.

Let's explore how the European digital identity system, introduced by eIDAS, works and how it can benefit people in everyday situations. Marco, an Italian citizen, is eager to continue his studies and has found an interesting course at a university in Spain. To enroll, he uses the European digital identity system provided by eIDAS, which simplifies the entire process.

Instead of filling out lengthy forms and dealing with paperwork, Marco logs onto the Spanish university's website. He notices an option to use his European digital identity for the enrollment process. This system allows people across the EU to securely verify

ISSN 2281-5147

their identity and share necessary personal data. Using his smartphone, Marco opens his digital wallet – an app that holds his ID and important documents. He selects his identity and begins the authentication process, which uses biometric recognition (like his fingerprint) to confirm it is really him.

Once verified, Marco is presented with a list of personal information the university needs for enrollment, such as his name, date of birth, and details of his high school diploma. With just a few taps, he selects the relevant information and gives his consent to share it with the university. The system automatically fills out the enrollment form for him, saving Marco from manually entering his details, making the process faster and more efficient.

Additionally, Marco needs to submit supporting documents, such as proof of residency and recommendation letters. Conveniently, these documents are already stored in his digital wallet. Instead of scanning and uploading them separately, Marco can easily attach the required files from his digital wallet directly to the application.

After submitting everything, Marco receives instant confirmation both via email and on his digital wallet app. The system also lets him track his application status in real time, keeping him informed of any updates. If the university needs further details, they can request the information through the platform. Marco can respond quickly, knowing that his personal data remains safe and secure, thanks to the privacy protections built into the eIDAS system.

Once his enrollment is accepted, Marco is notified and can finalize his registration online. Again, using his digital identity, he signs any required documents, without the need for printing or mailing anything. This entire process – from authentication to document submission and signature – is secure, convenient, and timesaving, allowing Marco to focus on preparing for his studies in Spain.

Thanks to eIDAS, the entire enrollment process is smooth and efficient. Marco has not only simplified the university enrollment procedure but also gained greater control over his personal data.

ISSN 2281-5147

4.1 Limitations

While the eIDAS system offers many advantages for Marco, there are several issues that need to be addressed.

One of the problems is the slow pace at which some countries have adopted the eIDAS system. Some countries have fallen behind, and this discrepancy can cause confusion in the use of cross-border digital identities (*Study to Support the Impact Assessment for the Revision of the eIDAS Regulation | Shaping Europe's Digital Future*, 2021). For example, Marco wants to use his Italian digital ID card to open a bank account in Spain, but he finds that the Spanish bank has not yet integrated the system for European recognition. In fact, many banks in Spain do not accept digital identities from other countries. As a result, Marco is forced to use paper documents and go through a lengthy and complicated registration process.

In other cases, both countries may support the European digital identity system, but there are issues with the certification of identity providers. For example, Maria, a German citizen, has just learned about the Lissi digital identity service (*Interact with European Digital Identity Wallets According to eIDAS 2.*). She decides to register to take advantage of the possibility to access other online services, not only in Germany but also in other European countries. After a few months, Maria applies for a scholarship in France. She wants to use her German identity card, but the French online service cannot accept Maria's document. This is because Lissi does not meet the security requirements required by France. Maria is confused, as she thought her new digital identity would allow her to use French services as well. Now, not only does Maria need paper documents, but she also has to travel to France in person to sign the documents.

To solve these issues, a single certification recognized at the European level is necessary. This would allow a digital identity service to be accepted in another part of Europe, thereby increasing citizens' trust. However, from this point of view, eIDAS leaves countries too much room for maneuver, slowing down the harmonization process.

Finally, the adoption of the system by the public and companies is still limited. Many citizens and businesses still harbor doubts and uncertainties about digital identities, mainly due to a lack of understanding and concerns about privacy. Imagine Maria

ISSN 2281-5147

wants to use an online service that requires authentication through a digital identity. When registering, she is offered the option of using eIDAS but is skeptical, fearing that her information could be compromised. Similarly, Sophie, the owner of a local business, wants to digitize her system but is reluctant to use eIDAS for the same reasons. Without proper training and information on the benefits of eIDAS, both Maria and Sophie decide not to use it, continuing to prefer traditional methods. This lack of trust hinders the adoption of eIDAS, limiting opportunities for citizens and businesses to access more modern and efficient services.

In conclusion, while the eIDAS system presents significant advantages for users like Marco and Maria, its effectiveness is hindered by notable shortcomings, particularly the lack of harmonization among EU member states.

5. Building the future of identity

Implementing eIDAS and self-sovereign identity requires significant effort, both technically and legally, to ensure that all the different online accounts we use, such as social media and banking services, can work together seamlessly. Additionally, each European country will need to recognize identities from other countries. For example, a French account must be recognized in Germany and vice versa. Each country will propose its own wallet based on different technical implementations. At this point, we still do not know how many wallets will coexist, potentially more than 27. This means that various implementations of national identity will also coexist.

Suppose you want to link your Instagram profile to a European identity, making it easier and safer to access various online services with a single identity recognized everywhere. You might choose to use a French digital wallet. This wallet could not only contain your official documents, such as your ID card or driver's license, but also your social media accounts and other services. This wallet must be recognized by other countries, and we still do not know the best existing identity solution.

In this context, our goal is to create a common set of rules to assess which of the many existing solutions is truly self-sovereign. This common set of rules can also be used to facilitate the integration of existing accounts with new online accounts.

ISSN 2281-5147

- *What we do*

To explain our work, we use a simple analogy by referring to a concept familiar to us. Imagine a messy desk full of pens, papers, and other objects. If you receive a phone call and need to jot down notes quickly, finding a pen amidst the chaos becomes complicated. Now, picture the advantages of an organized desk. You can instantly find what you need. Imagine that everything is sorted and stored in labeled boxes. That streamlines your work. To make the labels easily distinguishable, you might choose to use simple geometric symbols. For example, a triangle could indicate the box for pens, a square could represent printer cartridges, and so on.

This way of cataloging items becomes critically important in the digital world, where technologies evolve rapidly.

- *Our approach*

The various online accounts we use, such as banks, corporate email, etc., metaphorically represent the objects on our desk. First, we organize these accounts and the related technologies into a model called Trust Over IP. This model, developed a few years ago by a non-profit organization, aims to guide experts in designing new technologies.

Imagine being an influencer who wants to create an account on Instagram. Now, imagine you can link a digital version of your passport or ID card to your Instagram account. This would allow anyone to verify that the account truly belongs to you. Once your account is linked to this digital identity, your name becomes proof of the account's verification. The information is securely stored and cannot be altered or forged. In short, mapping an Instagram account within the Trust Over IP framework means linking the account's digital identity to a verified structure.

With our work so far, what we have is a very precise description of an account. We could describe an Instagram account using labels. For example, the first step would be called "Creating a Digital Identity," to which we would assign a specific label. The collection of all labels would describe our online account.

ISSN 2281-5147

At this point, we want to provide a universal description of our accounts. That is, we want to be able to describe every existing account in a simple and clear way for everyone. For instance, we'd like all websites to easily indicate the procedure for creating an account, or for deleting it, etc. To do this, we have described the objects using a common language for everyone. A sort of universal language. This language is called ontology and can be used to describe Self-Sovereign Identity (SSI). Therefore, our ontology becomes a universal description of our digital accounts. The ontology becomes a kind of guideline for creating, deleting, and modifying our online accounts, regardless whether it is a bank account or an Instagram account.

Finally, the ontology can be associated with a definition of SSI. At this regard, we elaborated a new definition of SSI from past works. The result is a list of properties that focus on individual's privacy and protection of information. Figure 1 shows an overview of our research. The elements are represented with rectangles and squares in the figure. The right side represents the different users' digital accounts. Trust Over IP is represented in the center as a rectangular box. Our descriptive language is on the left. The arrows indicate the processes of associating elements between the rectangles.

- *The outcome*

The output of our approach is to be able to evaluate any digital identity system. Citizen in Europe will be aware of what nation will propose the best identity based on control of information.

ISSN 2281-5147

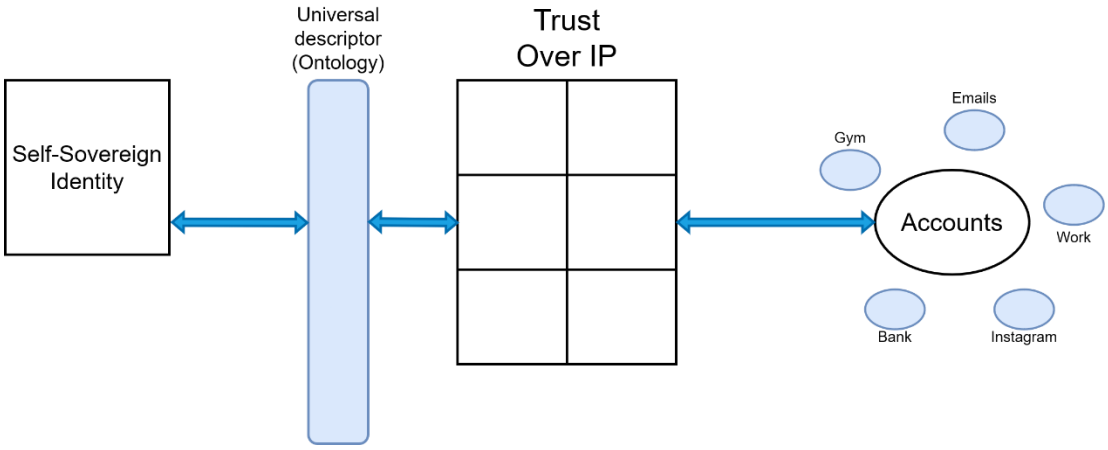

Figure 1. A schematic overview of the research work.

6. Conclusion

In conclusion, the adoption of a self-sovereign digital identity system, such as Self-Sovereign Identity (SSI), represents a crucial step towards a future where individuals will have full control over their personal data. The example of the European Union with the eIDAS system demonstrates that the integration of such technologies can simplify processes like authentication, access to public services, and the management of personal information, ensuring greater security and privacy. However, challenges remain, including the lack of standards and uniformity across various existing online accounts. This applies to both private accounts and solutions proposed at the European level by different countries. This slows down the adoption of new technologies by countries.

To build a more secure and connected future, it is essential to continue working on harmonizing regulations and educating citizens about the benefits of digital identities. Our approach is aimed at evaluating existing identity systems. It supports the collective effort of governments, businesses, and users to create a truly autonomous and universal digital system capable of ensuring privacy and data security in all online interactions.

ISSN 2281-5147

References

A Brief History of the Internet. (2023, September 29). *Internet Society*. https://www.internetsociety.org/internet/history-internet/brief-history-internet/

Ansaroudi, Z. E., Carbone, R., Sciarretta, G., & Ranise, S. (2023). *Control is Nothing Without Trust a First Look into Digital Identity Wallet Trends*. 113–132.

Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N., & Jararweh, Y. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications. *Information Processing & Management*, *59*(6), 103061.

Camp, J. (2004). Digital identity. *IEEE Technology and Society Magazine*, *23*(3), 34–41.

Commission, E. (n.d.). *DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Regulation Proposal 2021/0136 (COD)*.

Commission, E. (2023). *ARF - architecture reference framework. January 2023*.

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The trust over ip stack. *IEEE Communications Standards Magazine*, *3*(4), 46–51.

Digital identity in the ICT ecosystem: An overview. (2023, October 23). ITU. https://www.itu.int:443/en/publications/ITU-D/Pages/publications.aspx

Ehrlich, T., Richter, D., Meisel, M., & Anke, J. (2021). Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Praxis Der Wirtschaftsinformatik*, *58*(2), 247–270. https://doi.org/10.1365/s40702-021-00711-5

et al Alvaro Martin, A. I. S. (2019). Digital Identity: The current state of affairs. *BBVA Research*, 1–46.

Interact with European Digital Identity Wallets according to eIDAS 2. (n.d.). Retrieved 16 October 2024, from https://www.lissi.id/

Johnson Jeyakumar, I. H., Chadwick, D. W., & Kubach, M. (2022). A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN. *Open Identity Summit 2022*.

ISSN 2281-5147

Laatikainen, G., Kolehmainen, T., & Abrahamsson, P. (2021). *Self-sovereign identity ecosystems: Benefits and challenges*. Scandinavian Conference on Information Systems.

Ruff, T. (2018). *7 Myths of Self-Sovereign Identity*. https://medium.com/@timothy.ruff/67aea7416b1

Satybaldy, A., Ferdous, M. S., & Nowostawski, M. (2024). A Taxonomy of Challenges for Self-Sovereign Identity Systems. *IEEE Access*.

Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. (2022). The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences*, *12*(24), 12679.

Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, *2021*, 1–26.

Study to support the impact assessment for the revision of the eIDAS regulation | Shaping Europe's digital future. (2021, June 9). https://digital-strategy.ec.europa.eu/en/library/study-support-impact-assessment-revision-eidas-regulation

Susanna, T. (2022). *Revision of the eIDAS Regulation: Findings on its implementation and application*.

Young, K. (2010, May 27). *The Identity Spectrum*. Identity Woman. https://identitywoman.net/the-identity-spectrum/

ISSN 2281-5147