10-3-2024

The Neutrality and Dichotomy of Self-Sovereign Identity: An Exploratory Study

Ana Paula de Amorim
TecMinho and ALGORITMI Research Centre, University of Minho, anamorim@tecminho.uminho.pt

Rui Dinis Sousa
Information Systems Department, ALGORITMI Research Centre, University of Minho, rds@dsi.uminho.pt

The Neutrality and Dichotomy of Self-Sovereign Identity: An Exploratory Study

Research-in-Progress

Amorim, Ana Paula, TecMinho and ALGORITMI Research Centre, University of Minho, Portugal, anamorim@tecminho.uminho.pt

Sousa, Rui Dinis, Information Systems Department, ALGORITMI Research Centre, University of Minho, Portugal, rds@dsi.uminho.pt

Abstract

The sudden eradication of the EU vision on Self-Sovereign Identity (SSI) is the focal point of this study. The literature review conducted (findings in a future paper) identifies SSI's ontological confusion, mixing (1) what is Self-Sovereign Identity, with (2) decentralised IAM (Identity and Access Management) systems. This particular paper argues that Self-Sovereign Identity should be viewed as a neutral, technology-agnostic concept. Clarifying the meaning of SSI is crucial given the ongoing crisis of identity theft, an invisible crime that has become the most profitable activity of organised crime. It was necessary to take a step back from the current IS pragmatist approach and work without an empirical net, thus pushing Information Systems research to its "edges". We use "high-level theorising", grounded on engaged scholarship and applied philosophy as a research framework with intuition and metacognition informing our research approach. The findings support the neutrality and dichotomy of Self-Sovereign Identity and introduce an initial quantitative instrument to measure the SSI level of a nation. The subsequent steps of this ongoing research include proposing a unified perspective of SSI and its overall implications, using "provocatype designs" for critical reflections regarding the societal consequences of the EU SSI/AIM solutions/technologies, alongside recommendations for defensive and offensive measures to counteract identity theft and organised crime. Ultimately, Self-Sovereign Identity is framed as a matter of freedom and human rights.

Keywords: Self-Sovereign Identity; IAM-Identity and Access Management; Identity Theft; Organised Crime.

I. Introduction

The sudden eradication of the EU vision on Self-Sovereign Identity (SSI) from key websites on Digital Identity and Digital Blocks prompted the development of this paper.

The literature review conducted (findings in a future paper) identifies SSI's ontological confusion, mixing 1) what is Self-Sovereign Identity, with (2) decentralised IAM (Identity and Access Management) systems. The European Union is launching a new digital IAM (Identity and Access Management), with improved KYC (Know-Your Customer) mechanisms. This new, interoperable IAM system is based on three key pillars: the EUID Digital Wallet, Verifiable Credentials and EBSI (European Blockchain Service Infrastructure), as the European registry of trusted Issuers of verifiable credentials. However, there is no mention anymore o the SSI vision, though a lot of funding (yet to be ascertained) was channelled to the Early Adopters Program of EBSI and the ESSIF (The European Self Sovereign Identity Framework)

This paper argues that Self-Sovereign Identity should be viewed as a neutral, technology-agnostic concept and show that we must continue on this major track, the vision of Self-Sovereign Identity.

The hypothesis this paper explores has to do with the definitions around Self-Sovereign Identity (SSI) and, more to the point, how incomplete or even erroneous most of the current definitions are. It is proposed that Self-Sovereign Identity should be a neutral concept, a vision not linked to any specific technology or identity system (centralised or decentralised), as the research and industry communities predominantly define it. (the literature review demonstrating the ontological confusion around SSI will be presented in a separate paper)The need to clarify the meaning of SSI is crucial, not just because of its "ontological confusion" but mainly due to the "unintended consequences" of any new complex system, especially if we (1) completely miss the point of what SSI is and (2) promise an SSI vision in Europe and not deliver it. “The first and most complete analysis of the concept of unintended consequences was done in 1936 by the American sociologist Robert K. Merton” (Norton 2018). Bowles (2020) takes this “law of unintended consequences” to a whole new level by using speculative and critical design, or as the author calls it, “provocatypes”.

The truth is we are already facing a huge SSI crisis. In fact, we should say we are at war regarding our Self-Sovereign Identity. In this "SSI war" we face two main enemies:

- The "inner enemy" is ignorance: most of us do not know what self-sovereign identity is and that SSI has always been a right of the individual (Qureshi, S. 2022).;
- The "external enemy" is identity theft: an invisible crime that has become the most profitable activity of organised crime, according to the TOC unit of the United Nations (UN-TOC). Furthermore, only 8% of the identities stolen in Europe (2018 and 2019) occurred online (Finanso.se, 2022).

The results will show the dichotomy of Self-Sovereign Identity when faced with Identity Theft and introduce an initial quantitative instrument to measure the SSI level of a nation. This instrument should be regarded as part of the analysis of individual freedoms.

The next steps of this ongoing research include also the proposal of a unified perspective of what SSI is and what it entails for individuals and society. An approach would be to apply Bowel´s “provocatype designs” to provoke critical reflections regarding the societal consequences (Kayanadath 2021) of the emerging digital identity and SSI systems/technologies, particularly its unintended consequences. Finally, defensive and offensive measures should be recommended to counteract identity theft and organised crime. The final goal is to increase SSI levels in Europe and worldwide and the realisation that Self-

Sovereign Identity is a matter of Freedom and Human Rights.

2. Research Framework

2.1 Engaged Scholarship and Applied Philosophy

The EU introduced Self-Sovereign Identity some years ago as a new digital identity paradigm. Being an emerging concept and not agreeing with the current views on SSI as a technology-based concept, there was the need to take a step back from the pragmatist approach to Information Systems (IS) research, as explored by Ågerfalk (2010), which meant working without an empirical net. We follow here the recommendation of Grover & Lyytinen (2015) to push IS inquiry to the "edges" by, among others, "using high-level theorising" Two decisions were made to ground this initial theoretical approach to SSI:

(1) Following the "engaged scholarship" framework, as proposed by Mathiassen (2017), we anchor our research on a relevant real-world problem. At this early stage of understanding SSI, our ongoing research is at the level of "informed basic research," which is one of the four types of engaged scholarship identified in this framework.

(2) Following the path of "applied philosophy" and using our own intuition and metacognition lens as it seems philosophers have done for millennia. The emergence of scientific understanding relies on "skills, imagination, and the capacity for knowledge selectivity" (Poliseli 2020).

3. Research Questions

This exploratory theoretical work began with the following intuitive belief (hypothesis): "Self-Sovereign Identity (SSI) is a neutral concept, independent of which systems or technologies support it." This hypothesis argues that SSI is technology/platform agnostic, though the trust models allowed by web3 can certainly increase the protection of our SSI. However, as this exploratory study will show, technology per se, will never guarantee our Self-Sovereign Identity.

The analysis of SSI neutrality began with the fundamental question: What is sovereignty?

Because of the "ontological crisis" around SSI and the current EU – Digital Strategy's objective of (1) enabling the ownership and control of our personal/private data and (2) increasing our privacy-by-default (as per the GDPR – General Data Protection Regulation) another question materialised around privacy: What is data sovereignty?

To summarise, the understanding of Self-Sovereign Identity and the analysis of its neutrality requires the answer to the following questions:

- RQ1. What is Sovereignty?
- RQ2. What is Data Sovereignty?
- RQ3. Is SSI a neutral concept?

3.1 RQ1: What is Sovereignty?

From a historical perspective, "sovereignty is the right and the power of a person or a nation to govern themselves. Sovereignty is a broad term that influences many modern concepts, such as

identity, individuality, and rationality. These ideas developed together during the nineteenth century and were connected to the Scientific Revolution and the Enlightenment." (Elshaikh n.d.).

"The concept of self-sovereignty helps us understand how people can choose the direction of their own lives by having control over their identities. This is similar to human freedom. As Trotter (2014) described, cited in Qureshi (2022), self-sovereignty is about being fully alive and autonomous

From a "common" lay-lens (dictionaries as sources of knowledge) you arrive at the following definition of sovereignty: "It is an autonomous state, free from external control (Merriam-Webster - online) with the authority to govern itself (Oxford - online).

We cannot dismiss dictionaries as important sources for ontological studies (as in the case of Eckard et al. (2012), for instance).

In fact, this lay definition of sovereignty creates a seamless link between the two definitions presented above and the following technological perspective on data sovereignty from EBSI (European Blockchain Services Infrastructure).

3.2 RQ2: What is Data Sovereignty?

From the lens of EBSI and the Digital Rights Declaration: "*We believe that individuals should have full custody over their own data, controlling which information they show, to whom and for how long. We ensure this by providing a trust model that enables the exchange of Verifiable Credentials in a self-sovereign way*" (EBSI – Digital Rights Declaration).

Using the theoretical foundation of Lauf, et al (2022), Data Sovereignty can be seen as a branch of digital sovereignty of individuals focusing on data self-determination". The authors state that

- "*data sovereignty involves making independent, controlled, and self-determined* ***decisions*** *about what happens to one's own data*."
- "*data sovereignty* ***is the ability to decide*** *in a self-determined way, at any time, and by means of preferences, which entity can use one's own (personal) data for selected purposes*."

3.3 RQ3: Is Self-Sovereign Identity a Neutral Concept?

First, we need to clarify the concept of identity, which is not an easy task. According to Flores (1998), “the precise contours of common-sense understanding of personal identity has stimulated much academic debate, where even the term “personal identity” is ambiguous in a number of ways”. In identity and SSI research, we recommend the work of Menčik (2020) as the best approach to understanding personal identity, by offering a clear distinction between physical, social and psychological identities. Regarding SSI, the focus is mainly on social identity, digital (social) identity. According to Tewari and Mills (2021) digital identity is “a subset of one’s identity, composed only of information that is digitalized”. With this foundational understanding of digital identity related to our social identity (Menčik 2020), and recollecting sovereignty (as autonomy and self-government), then SSI would be a neutral concept (the self-government of our social - digital - identity), and thus technology agnostic. Technology, however, can enable Self-Sovereign Identity.

4. Findings

4.1. SSI Neutrality

The current exploratory analysis of sovereignty and data sovereignty sustains the concept of the neutrality of SSI. SSI is more of a vision, an ideal: "*An idea that individuals must retain control over their personal data and over the representations of their identities (or personas), within a particular identity management system*" (Wang and De Filippi, 2020). These authors also refer to the new privacy-by-default mechanism associated with verifiable credentials (standardised by W3C), namely "*the right to selective disclosure different aspects and components of one's identity*". This work aims to go deeper: "*SSI is both a right and a responsibility of each individual to act/enact/protect one's identity data (data sovereignty)". It is a neutral concept, not dependent on techno-social-legal contexts. Such contexts can either enable or constrain one's SSI".*

4.2 EU is enabling SSI

The EU took three key steps to enable digital data sovereignty and consequently SSI.

The first step was the publication of the European Union's General Data Protection Regulation (GDPR) in 2016 (setting the foundations of data sovereignty). The key principles of data sovereignty set out by GDPR are (1) express explicit and affirmative consent to process private data, (2) the right to data portability (3) the right to be forgotten (in certain cases), and (4) the right to know when personal data has been hacked (and corresponding obligation for companies to notify data breaches) (Albrecht, J. P. , 2023). In summary, GDPR established the foundations of data sovereignty by (1) protecting individuals from "data trolls" and (2) enforcing proactive measures called privacy-by-design and privacy-by default. Citing Ann Cavoukian (Ryerson University), “data trolls” are defined as corporations and web service providers that collect massive volumes of personally identifying and private information, including purchases, locations visited, employment records, tax returns, health records, and social profiles (Toth, K. C., & Anderson-Priddy, A. 2019).

The second step was the launch of EBSI and The Early Adopters Program of SSI Digital Wallets (Digital Data Sovereignty), and the adoption of verifiable credentials (attributes/claims) of the individual (standards developed by W3C).

The Privacy-by-Design / Privacy-by-Default principles of GDPR are highly strengthened by the EU’s adoption of verifiable credentials as this standard allows the individuals to Selective Disclosure (SD) the attributes or claims as they see fit.

The third step was the update of the eIDAS regulation (eIDAS 2.0) and the launch of the EUID Digital Wallet in 2024 (with a focus on Digital Identity towards an improved, interoperable European digital authentication/verification system).

4.3 SSI Dichotomy

SSI is a binary state that changes with identity theft. We either have Self-Sovereignty or not. The same applies to Self-Sovereign Identity. "Dichotomy is a form of logical division. It separates a class into two subclasses: one of which has and the other has not a certain quality or attribute" (Britannica). The same applies to SSI: we either have self-sovereign identity

(ownership and control of our data) or we do not. What is the event that makes us change our state of SSI? Identity Theft.

So, an individual either has SSI or not once his (social) identity is stolen. It is a division into "two mutually exclusive or contradictory groups or entities" (Merriam-Webster). This means when our identity is stolen, we no longer are the sole owners of it. We have no control over what will be done with our stolen data/social identity. Therefore, we no longer have self-sovereignty, identity wise.

Regarding the SSI dichotomy (as a binary state), the analysis is based on Modus Ponens (propositional logic), an inference method used in classical logic. It is a "pattern of deductive reasoning" (Polkowski 2011) and it says that we can infer that Q will be true if both P and P → Q are true (Levenson 2017).

The statements are:

- If being Self-Sovereign means being autonomous (free from outside control or influence) with the ability to self-govern private data/credentials that represent (part of) my "social identity", in other words "being able to own and control private/identity data" (EBSI - Digital Rights Declaration),
- then it stands to reason that,
- If my identity is stolen, I no longer solely own or control my private data (in other words, my social identity); therefore, I no longer have identity self-sovereignty.

Applying the propositional logic of *Modus Ponen* (P→ Q is true and P is true then Q will be true)

- Statement 1 (P → Q): If my identity is stolen, then I no longer have Self-Sovereign Identity.
- Statement 2 (P): My Identity is stolen.
- Conclusion (Q): Therefore, I no longer have Self-Sovereign Identity.

The application of propositional logic (Modus Ponens) to Self-Sovereign Identity, also allowed the design of a first instrument to assess the "level of SSI" per country.

4.4 Assessing the level of SSI per country

Identity theft is rapidly expanding, causing substantial financial loss to millions of people all around the world. This invisible crime is also widespread across European countries, where a growing number of consumers are targeted by sophisticated fraudulent scams each year, both offline and online. Although recent years have witnessed significant progress in identity theft protection technologies and solutions, the survey showed many Western Europeans had significant problems with protecting their sensitive information: 56% of Europeans have experienced at least one type of fraud in the last two years, according to data gathered by Finanso.se (2022). The statistics show that 25% of Europeans exposed to fraud suffered financial damage, causing a total loss of around €24 billion in two years.

This EU survey reported by Finanso.se (2022), also shows that the attack vectors (methods of identity theft) are the following:

- Half of all identity theft attacks in European countries happened by using **e-mail**.
- Another 39% of deceivers used the **phone** and text messages (4%) to attack their victims.
- Online ads and social media platforms follow with 5% and 3%, respectively.

Such attack vectors imply that **EUID and SSI Wallets will be quite ineffective in preventing identity theft** as "online identity theft attacks account for only 8% of Identity theft in European countries" (Finanso.se).

Based on the assumption that SSI is a binary state, we can draw the following conclusions at two different levels of analysis:

- The individual: I either have Self-Sovereignty (my identity has not been stolen) or not (my identity has been stolen).
- The country/nation: if a country has x% of Stolen Identities (SI), then that country has (1-x)% of SSI (Self-Sovereign Identities).

The following table is based on country statistics on Stolen Identities (SI) according to Finanso.se (2022).

Country (2018-2019)	% Stolen Identities (SI)	% of SSI (SSI=1-SI)
United Kingdom	53%	47%
Ireland	50%	50%
Denmark	45%	55%
Netherlands	42%	58%
France	39%	61%
Cyprus, Bulgaria, Hungary, and Estonia	<10%	> 90%

Table 1. Level of SSI per country (2019-2020)

The above is a very basic quantitative instrument to assess how we stand regarding Self-Sovereign Identity every year. Further research is needed, namely to (1) understand the reasons behind such a high level of stolen identities (hopefully, the study from the EU-Migration and Home Affairs (2022) will shed some light), and (2) evaluate a possible correlation between privacy behaviour and stolen identities. As stated before, this research on SSI focuses especially on our social identity, which is the one becoming increasingly digitised, and also the one targeted by data trolls and data thieves.

5. Discussion

5.1 Data Sovereignty and Privacy are key pillars of SSI.

As stated above, GDPR has established the foundations of data sovereignty by protecting individuals from "data trolls" and enforcing proactive measures such as privacy-by-design and privacy-by default. eIDAS 2.0, Verifiable Credentials, Digital Wallets and EBSI are disruptive innovations regarding digital data sovereignty.

These initiatives however will not dent the invisible crime of Identity Theft. Maybe quite the opposite, as we are "offering" a new attack vector (Naik, N., Grace, P., Jenkins, P., Naik, K., & Song, J. (2022.), more valuable than before: "verifiable credentials" and "verifiable identities" stored in digital wallets. EUID and SSI digital wallets will concentrate, "in one place", "verifiable" data regarding one individual. "Verifiable" is the operative word regarding identity theft: it is a trust feature that most private data did not possess previously to these new EU

digital strategy initiatives.

5.2 European KYC² system

However, these solutions are far from enough to protect our SSI. In fact, their main goal and achievement is an improved, interoperable European KYC² system (Know Your Customer/Citizen system) and increased privacy. The above regulations/standards and solutions increase data privacy / sovereignty as per the GDPR (Privacy-by-Default), highlighting two key innovations: Selective Disclosure of Verifiable Credentials and ZNP (Zero Knowledge Proof).

The EU Digital Strategy /Digital Building Blocks have paved the road for a digital Self-Sovereign Identity (GDPR, eIDAS 2.0 and EUID Digital Wallet, EBSI and the Early Adopters Program). But sovereignty needs to be protected. And so does Self-Sovereign Identity.

5.3 The Fragility of Social and Digital Identity

We still have a long road ahead of us due to the gravity and extension of the phenomena of identity theft (mainly when orchestrated by organised crime). The EU and Member States are responsible for protecting their citizens (Ludsin, H., 2013), including one of the most fundamental pillars of freedom: Privacy and Self-Sovereign Identity.

We need to understand how this SSI dichotomy evolves over time and how we can support the victims of identity theft becoming self-sovereignty again. Regaining our SSI is not as simple as revoking the stolen identifiers (for instance) and issuing new others. This could be the worst measure ever.

Time will tell regarding fraud and scam statistics, but "KYC" policies have not managed to stop fraud in the past. So maybe it is time to experiment something different. "*Insanity is doing the same thing, over and over again, and expecting different results*" (unknown author).

6. Conclusion

In conclusion, we need to address "the fragility of social and physical identity" as explored by Menčik (2020). Online identity theft is a real, huge threat (Alilwit 2020) for society and the individual in particular. The only way to mitigate the "tsunami effects" of data breaches and individual identity theft is to understand both phenomena: SSI and Identity Theft and how they relate to one another.

6.1 SSI and the perils of digital identity

Identity Theft targets especially social identity but also physical identity (physical traits) with the compounding danger arising from look-alikes or doppelgängers (Joshi, R. S., et al. 2022)

The "tsunami effects" of a single instance of identity theft/fraud are explored by Gupta, C. M., & Kumar, D. (2020), in "Identity theft: a small step towards big financial crimes" -Journal of Financial Crime. The authors state "Identity theft can lead to multiple crimes which can affect not only individuals but also companies. And when these crimes impact companies, they can actually hamper the economy as a whole".

And we have not yet explored worst-case scenarios when stolen identities are used for espionage or terrorism, which raises the threat level to national defence.

6.2 A vision of SSI for the EU: "The Once and Future King"

We can only hope and demand that the vision of SSI returns soon to the EU, as in the novel The Once and Future King by T. H. White (1958), “exploring human nature regarding power and justice” (wikipedia, 2023). Only this way, will we be able to address the several perils around digital identity and EUID regulation. In doing so, we will achieve another societal revolution, and the EU digital vision of Self-Sovereign Identity becomes an enlightened historical paradigm shift.

O tema central explora a natureza humana em relação ao poder e a justiça, com o jovem Artur se tornando rei e tentando ser um cavaleiro ideal

.

Acknowledgements

We want to thank Kim Jorgensen (postdoc at TecMinho and Algoritmi Centre of University of Minho, Portugal) for the insightful discussions on SSI and for reviewing drafts of this work. This work has been supported by IAPMEI (PRR) under the project Agenda Blockchain.PT (WP7.2 - SSI Digital Wallet).

References

Ågerfalk, P. J. (2010). Getting pragmatic. *European Journal of Information Systems*, *19*(3), 251-256.

Albrecht (2024. General data protection regulation. Most of Member States have updated their legislation, In “Civil Liberties, Justice and Home Affairs - LIBE”, Europarlament. https://www.europarl.europa.eu/legislative-train/theme-area-of- justice-and-fundamental-rights/file-general-data-protection-regulation (accessed at 18.05.2024)

Alilwit, N. (2020, November). Authentication based on blockchain. In *2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC)* (pp. 1-6). IEEE.

Blancke, S., Tanghe, K. B., & Braeckman, J. (2018). "Intuitions in science education and the public understanding of science". *Perspectives on science and culture*, 223-242.

Bowles, C. (2020). Future Ethics: from modern ethical theory to practical advice. *DEUS. https://www.deus.ai/podcast/future-ethics-from-modern-ethical-theory-to-practical-advice* (accessed at 25.07.2024)

Croft, H. T., Falconer, K., & Guy, R. K. (2012). Book *Unsolved problems in geometry: unsolved problems in intuitive mathematics* (Vol. 2). Publisher: Springer Science & Business Media.

Dunne, B. J. (2016). Subjectivity and intuition in the scientific method. In *Intuition: The inside story* (pp. 121-128). Routledge.

EBSI – Digital Rights Declaration. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI+and+the+Digital+Rights+Declaration+-+how+we+design+with+your+rights+in+mind (accessed at 18.05.2024)

Eckard, E., Barque, L., Nasr, A., & Sagot, B. (2012, December). Dictionary-ontology cross-enrichment using TLFi and WOLF to enrich one another. In *CogALex-III-3rd Workshop on Cognitive Aspects of the Lexicon*. Curran Associates, Inc.

Elshaikh, Eman, "Sovereignty", Khan Academy (online). https://www.khanacademy.org/humanities/whp-origins/era-6-the-long-nineteenth-century-1750-ce-to-1914-ce/61-liberal-and-national-revolutions-betaa/a/read-sovereignty-beta (accessed at 18.05.2024)

EU-Migration and Home Affairs (2022). European Commission, Directorate-General for Migration and Home Affairs, (2022). *Study on online identity theft and identity-related crime: final report*, Publications Office of the European Union. https://data.europa.eu/doi/10.2837/197724 (accessed 22.05.2024)

Finanso.se (2022), reporting on the "European Commission Survey on Scams and Fraud Experiences by Consumers" https://finanso.se/one-in-five-europeans-have-experienced-identity-theft-fraud-in-the-last-two-years/ (accessed 22.05.2024)

Flores, F. (1998). Information technology and the institution of identity: reflections since understanding computers and cognition. *Information Technology & People*, *11*(4), 351-372.

Giannopoulou, A. (2023). Digital identity infrastructures: a critical approach of self-sovereign identity. *Digital Society*, *2*(2), 18.

Grover, V., & Lyytinen, K. (2015). New state of play in information systems research. *MIS Quarterly, 39(2), 271-296*

Jia, X., Li, W., & Cao, L. (2019). The role of metacognitive components in creative thinking. *Frontiers in Psychology*, 10, 2404.

Joshi, R. S., Rigau, M., García-Prieto, C. A., de Moura, M. C., Piñeyro, D., Moran, S., ... & Esteller, M. (2022). Look-alike humans identified by facial recognition algorithms show genetic similarities. *Cell Reports*, *40*(8).

Kayanadath, T. (2021). Dark Potentials in Smart Environments (Doctoral dissertation, *Emily Carr University of Art and Design*).

Lauf, F., Scheider, S., Bartsch, J., Herrmann, P., Radic, M., Rebbert, M., ... & Meister, S. (2022). "Linking Data Sovereignty and Data Economy: Arising Areas of Tension". *Wirtschaftsinformatik 2022 Proceedings*. 19. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/19

Ludsin, H., (2013). Returning Sovereignty to the People. *Vanderbilt Journal of Transnational Law, 46, 97*

Mathiassen, L. (2017). Designing engaged scholarship: From real-world problems to research publications. *Engaged Management Review.*

Mencik, D. (2020). "Identity Theft: A Thought Experiment on the Fragility of Identity." *Conatus – Journal of Philosophy* 5, no. 1: 71-83.

Merriam-Webster. https://www.merriam-webster.com/dictionary/dichotomy. (accessed at 18.05.2024)

Michie, S., West, R., & Hastings, J. (2022). Creating ontological definitions for use in science. *Qeios*.

Munoz, C.G. (2019) SSI and eIDAS: a vision on how they are connected - Share your views! | FUTURIUM | European Commission (europa.eu) (accessed at 18.05.2024)

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80-86.

Naik, N., Grace, P., Jenkins, P., Naik, K., & Song, J. (2022). An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity. *Computers & Security*, *120*, 102808.

Norton, Rob (2018). Unintended Consequences. *Chapter of Econlib's Basic Concepts*, *The Library of Economics and Liberty* *https://www.econlib.org/library/Enc/UnintendedConsequences.html* (accessed 25.07.2024)

Poliseli, L. (2020). Emergence of scientific understanding in real-time ecological research practice. *History and Philosophy of the Life Sciences*, *42*(4), 51.

Polkowski, L. (2011). Reasoning Patterns of Deductive Reasoning. In: *Approximate Reasoning by Parts. Intelligent Systems Reference Library*, vol 20. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22279-5_3

Qureshi, S. (2022). Digital transformation at the margins: a battle for the soul of self-sovereignty. *Information Technology for Development Journal (AIS)*, 28(2), 215-229.

RichardWebster, B., Hu, B., Fieldhouse, K., & Hoogs, A. (2022). Doppelganger saliency: towards more ethical person re-identification. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 2847-2857).

Robson, M. J., Cooksey, R., Jabri, M., & Higgs, J. (2011). "The use and disclosure of intuition (s) by leaders in Australian organisations: A grounded theory". Doctoral Thesis. *University of New England*.

Satybaldy, A., Nowostawski, M., & Ellingsen, J. (2020). Self-sovereign identity systems: Evaluation framework. Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14, 447-461.

Schwalm, S., & Alamillo-Domingo, I. (2021). Self-sovereign-identity & eIDAS: a contradiction? Challenges and Chances of eIDAS 2.0. *European Review of Digital Administration & Law - Erdal*. SOMMARIO (erdalreview.eu).

Smith, S. M. (2020). "Universal Identifier Theory". https://raw.githubusercontent.com/SmithSamuelM/Papers/master/whitepapers/IdentifierTheory_web.pdf (accessed 22.05.2024)

Tewari, N., & Mills, A. (2021). Digital Identities-Impact of Information Privacy Awareness on Identity Threats. *In PACIS 2021 Proceedings. (p. 9)*. https://aisel.aisnet.org/pacis2021/9

Toth, K. C., & Anderson-Priddy, A. (2019). Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security & Privacy*, *17*(3), 17-27.

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalised world: Credentials- based identity systems as a driver for economic inclusion. *Frontiers in Blockchain*, 2, 28. *(Special Issue on Identity and Privacy Governance)*, Available at SSRN: https://ssrn.com/abstract=3524367

Wertsch, James V. & Polman, Joseph L. 2001. Chapter "*The Intuitive Mind and Knowledge About History*", Book "Understanding and Teaching the Intuitive Mind", publisher: Routledge.

Wikipedia (2023). The Once and Future King. https:

https://en.wikipedia.org/wiki/The_Once_and_Future_King (accessed 22.07.2024)