

Safety and Security Interactions in eIDAS-compliant Trust Services

ARTUR ENGELS, University of Twente, The Netherlands

ABSTRACT

eIDAS regulation proposed by the EU was created to unify the European Digital Single Market with a single reliable and secure framework for digital identification. Nevertheless, attacks like phishing for credentials bypass the framework entirely and target the users themselves. Moreover, extra protection against attacks on the system or the user (security) may interfere with the intended operation as a reliable identification or trust service or pose a threat to user's well-being (safety). Additionally, most of research on eIDAS implementations investigates single specific use cases, potentially missing the threats resulting from prolonged, repetitive or simultaneous interactions. This research is to analyse the safety (protection against failures of the system and harm to the user) and security (defence against attacks) concerns in the context of electronic identification in the case of a Dutch digital citizen and investigate the interplay of security and safety in the eIDAS-compliant trust services with a focus on holistic interactions. We start with a literature review, then present the digital landscape and role of eIDAS in it using Account Access Graphs and then analyse the interactions and model the safety and security of the system with the attack-fault trees combination.

Keywords

eIDAS, safety, security, interactions, account access graphs, attack fault tree

1. INTRODUCTION

The development of the European digital landscape, with the transactions moving to the digital realm and yet increasing proportion of online communication, make a reliable security infrastructure for it more of a necessity. To provide a secure and reliable communication not only within the member states, but also across them, the European Union (EU) passed the eIDAS regulation, which stands for "electronic identification and trust services" It was envisioned to standardise the electronic identification across the EU allowing for authentication and seamless digital transactions between the parties across all member states [7]. By the eIDAS regulation, a revised version of 03.06.2021, also known as eIDAS 2.0, is meant in this report [6]. Moreover, eIDAS is to incorporate the state-of-the-art security into the working of the eID and services.

It has been shown, however, that security and safety are often interconnected and may only be analysed jointly [3]. For example, if a person's medical information can be accessed solely by that person themselves, it is secure, yet not safe, as the medical workers may not be able to access relevant information to assist the person in case of an emergency. The eIDAS framework and the services implementing it are concerned with personal and other sensitive information, including contracts and certificates, therefore the question of safety and security is of pivotal significance.

The definitions for the safety and security are as introduced in [17], safety being defence against the unintended failures of the system and threats to the welfare of the user, while security is defence against malicious attacks on a system or a person intending detriment to the subject.

This research is to investigate the interaction of the safety and security in the eIDAS framework and its existing and developing implementations, with a focus on compounding effects of the multi-role relations between the users. The research includes a literature review and a comparative case study of a Dutch digital citizen.

2. METHODOLOGY

The research has three main stages: review of the existing literature and related works, case definition and case analysis. This section presents the research questions and explains the research process, the concepts used and the study design decisions.

2.1. Problem Statement

The eIDAS regulation largely passed unnoticed by the public with poor understanding of the services bringing the ideas into power even if regularly used [12]. As a result, even though the regulation is not exactly novel, not much research exists on some specific aspects of the European initiative. Such, the mainstream research does not distinguish between safety and security of the system or focuses solely on security. Moreover, at the moment of writing there are no large case studies with multiple simultaneous and historic interactions between the parties, potentially missing the effect of accumulation of user information. The identification of the outlined gaps resulted in the formulation of the following research question:

RQ: What safety and security interactions are present in the implementations of the eIDAS framework as a result of multi-relational interactions between entities?

Following that, a set of sub-question was formulated to acquire all prerequisite knowledge to answer the research question:

SQ1: How to define safety of the electronic identity and trust services?

SQ2: How to define security of the electronic identity and trust services?

SQ3: What are the interactions between the safety and security in the field of electronic identification and trust services?

SQ4: How to model interactions between safety and security?

SQ5: What are the safety concerns currently faced by the eIDAS framework?

SQ6: What are the security concerns currently faced by the eIDAS framework?

2.2. Study Design

The research started with a literature review to establish all the relevant definitions and prepare the knowledge base for identifying gaps, as well as formulating and answering the research question and sub-questions outlined in the problem statement section. After that, we formulate the case study of the Dutch digital citizen and model the digital landscape of the user with an account access graph (AAG). Modelling the accounts and corresponding information ecosystem of the current state of affairs allows for comparison to the changes introduced by the eIDAS services. However, since the account access graph is mainly concerned with the

security of the system [8], safety had to be modelled alternatively, such as with a fault tree. To identify the safety and security concerns, we used the overlap between AAG and attack trees described in [8] to assist with identification of attack routes. The AAG, in other words, was used as an extension of the case description to aid the identification of feared events and their relationships to then be modelled with an Attack-Fault Tree (AFT). The final part of the research includes that analysis of the feared events and their interactions, modelling the interactions with an AFT and drawing conclusions about the safety and security of the eIDAS framework in similarly to the approach proposed by [17] (see Figure 1). However, we deviated slightly from the approach by modelling detailed AFT that includes failures of meeting the safety/security requirements and properties as specific bottom-level feared events. As a result we represent the requirements and the properties acquired in steps 3 and 4 visually in the AFT. Moreover, the interactions of those properties could be modelled just as well.

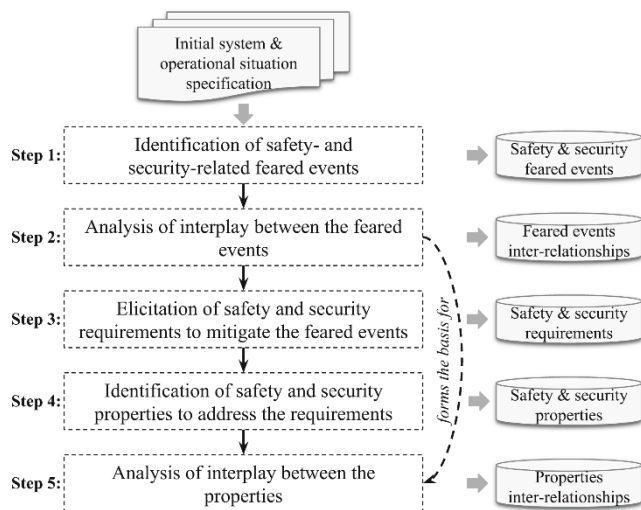


Figure 1: approach to analysing the origins of safety and security interactions (from [17])

2.3. Literature review

We conducted a literature review to prepare the knowledge base for the following analysis. As data sources we used primarily Google Scholar and OCLC WorldCat. The first query included terms “eIDAS”, “security” and “safety” and a year range of 2021-2024 due to interest in the revised version of eIDAS introduced in 2021 that introduced new requirements and specified some aspects of the regulation, making research in the later years more relevant for this study. The first search resulted in 1030 papers. Inclusion of the keyword “interaction” lowered the number of papers to 743, yet did not yield a significant increase in the number of relevant articles. A search for papers on “eIDAS” and “attack-tree” from 2021 resulted in 13 papers, while “eIDAS” and “fault-tree” provided only one paper on risk management that was also found with the previous query, which was later excluded due to the language criteria.

To familiarise with the modelling of safety and security interactions, we conducted the second round of review. The query “safety & security & security|safety-interaction” resulted in 2050 papers. Addition of the keyword “model” reduced that number to 1920. Sorting by relevance, the two pages contained all necessary information to provide an overview of techniques for analysis and

modelling of safety and security interactions. We then conducted a comparison of the contents of those works and their references for inconsistencies. The following section presents some of the works found during the literature review that this research builds upon.

2.4. Related Works

The work of Budde et al. [2021] and works of Nicoletti et al. [2023] and Quamara et al. [2023] define safety, security and their interactions, as well as present the state-of-the-art methods and models for joint safety-security analysis. These studies aim at developing a rigorous foundation for such analysis and identification of interactions between safety and security. The article of Quamara et al. [2023] specifically provides a strong methodological foundation for this research. The model proposed in the article may be used to analyse the origins of the safety and security interactions in the field of electronic identification and, specifically, the eIDAS framework.

In his master’s thesis, Konstantinidis [2021] explores the state and the direction of development of Identity and Access Management (IAM) in the European Union. They review what IAM includes, the approaches to IAM and the regulatory background, including the eIDAS regulation. Their study introduces the concepts relevant to this study, that is digital identity, eIDAS, identity and access management, etc. The study provides a good general overview of the concepts allowing for a more thorough understanding of the topics. Unlike in our work, the focus is on IAM in general, yet there is overlap in certain use cases.

The work of de Castro Ribeiro [2023] outlines the eIDAS framework in detail, one of the goals of the paper being thorough explanation of the eIDAS regulation and technologies adjacent to it allowing for an in-depth analysis of the process and how it may be further improved upon. They also provide a detailed explanation of an implementation of the wallet outlined by the revised eIDAS regulation: WalletID. Unlike in our work, security of the system is mentioned in [5] but is not the main object of the research.

Besides the literature found on the databases, we took part in the European Identity and Cloud Conference where Sharif and Sciarretta [2024] presented their findings on the security landscape of eIDAS. Their work served a pivotal role in assessment of the threats related to the implementations of eIDAS. Nevertheless, the focus of their work is on differences in security compared to traditional identity management systems while our research distinguishes between safety and security threats and aims to find the interactions between the two.

2.5. Account Access Graphs

Account Access Graph models the account ecosystem of the user with vertices representing the accounts or credentials and the directed edges – provision of access [9]. [1] presents the definition of the AAG model used in this work:

Let \mathcal{V} be a countably infinite set of vertices (representing, e.g., accounts, devices, credentials), \mathcal{L} be a countably infinite set of labels (for access methods) and \mathcal{A} be a set of participants.

An account access graph with state is a triple $G = (V, E, A)$ where $V \subset \mathcal{V}$ is a finite set of vertices, $E : (V \times V) \rightarrow 2^{\mathcal{L}}$ is a map labelling pairs of vertices with finite sets of access methods, pairs of vertices labelled with a non-empty set of access methods are edges, and $A : V \rightarrow 2^{\mathcal{A}}$ is a map labelling vertices with a finite set of participants.

A participant can access a node if they have access to all parents of the node with the same label on the connecting edges. The node states specify participants' access to nodes at a particular point in time. We also adopt assignment of the nodes to one of three types as described in [4]: account, authentication and access.

In this paper we introduced three following changes to the model visualisation due to the scale of the model:

- Use of coloured edges: we can assign a colour to a subset of the edges with the shared starting node for easier disambiguation of the edges in bigger models or with a lot of intersections. Unlike coloured edges in [9], the colour in this work does not carry information about the access method;
- Merging the edges that share a starting node to save space. The labels, if any are present (see next bullet point), should then be placed after the separation point of the edges;
- Omitting the edge labels if they are unique, that is, if the access to a node is provided by a set containing one node, visualise the edge between the two nodes without a label, enhancing readability of the model. This is not a necessary step as the labels may provide some information on the manner of access. When converting to the formal definitions from the visualisation, assign (arbitrary) unique labels to the unlabelled edges.

The changes introduced to the model affect only the visualisation to aid comprehensibility and do not affect the underlying definitions described in [1] and [9].

2.6. Attack and Fault Trees








Fault and attack trees are the formalisms commonly used for documentation of safety and security risks respectively with potential for joint safety and security analysis by using attack tree fault tree combinations [3]. The acyclic directed graph structure (despite the name) with logic gates represents the propagation of the faults/attacks modelled with nodes through the system via directed edges from the lower to the higher levels [13]. The trees usually contain a top-level event, typically corresponding to the total system failure or the end goal of an attack, which is reached from other nodes via Boolean gates. The activation of a node signifies its failure, therefore for an AND gate to activate, all incoming nodes (children) must fail and for an OR gate to activate, any of the children must be active. The main difference between the fault and attack trees is their underlying meaning resulting in diverging additions to model the characteristic features of faults or attacks (such as probabilistic nature of failures and their compounding effect) and modelling the dynamic scenario's. Nevertheless, a wide variety of fault and attack tree combinations exist better or worse fitted for specific analyses [13]. The methodology for modelling and analysing safety-security interactions we adopted is one proposed in [17] (see Figure 1). We selected the Attack-Fault Tree ontology due to its sufficient capabilities of event and interaction representation, similarity of the underlying dynamic fault trees to the AAG capabilities and scalability. Still, we encountered some limitations, such as inherent acyclicity preventing bi-directional causality (e.g. in case two passwords are the same, it is possible to acquire password 1 from password 2 and vice versa), lack of disambiguation between safety- and security-related events after a combination of both and lack of the NOT gate limiting the accuracy and clarity of the representation of the antagonistic events. The nodes representing the feared events are colour-coded, the blue ones corresponding to the safety-related events, orange – security-related and grey – safety- or security-related or

both. We found four types of interactions between safety and security in the literature. Those are, following the definitions of [13] and [17]:

- Conditional dependency – if B is conditionally dependent on A, occurrence of A implies occurrence of B,
- Mutual reinforcement – A reinforces B if presence of B in a set of events activating another event implies presence of A. Reinforcement is mutual when A and B reinforce one another,
- Antagonism – two events are antagonistic if occurrence of both leads to a contradiction, and
- Independence – no interaction.

This paper will take a closer look at the scenarios when any interaction is present: the first three types of interaction.

3. CASE DESCRIPTION

We decided to limit the scope of the research to the Netherlands and as the subject of analysis is concerned with private data of a natural person, the selected case is one of a Dutch digital citizen. As the aim of the study is to analyse the outcome of the complex interactions between the entities (natural/juridical persons, the government and its branches) including multiple relations between any two entities with diverse roles, the types of entities had to be defined to be added to the set of participants. We took interactions with an educational institution recognised by the government as a starting point with the relevant other entities added to the scope. The educational institution can formally interact with a person either as an entity that can provide and verify the level of education or as an employer. We distinguish two participants corresponding to those roles:  for the role of educational institution and  for the employer role. The other icons with the corresponding roles are  for the government and its services,  for the bank,  – the healthcare providers,  – the health insurance and, finally,  being the user. In this study we do not distinguish between government branches and put them all under the government participant as the interaction with all of them is quite similar from the information flow point of view [2]. We included the bank to cover the financial part of the user's environment, health insurance is required to study and work in the Netherlands and we included the healthcare providers as a party close to the government and the insurance, as well as using the same data.

The graph (Figure 2) shows all the user information the user themselves has access to with some authentication nodes representing information that is not used as an authentication method in this scope, yet is sensitive by itself and/or can be used to identify a person or as an external authentication method. It can be noted that there are pieces of information that are widely known, such as name, date of birth, address, e-mail address and phone number. Those by themselves are usually not recognised as particularly sensitive pieces of information, which may lead to oversharing and loss of anonymity on the internet [15]. Those nodes also serve as an indicator to where the user information is stored and how it can be accessed. For example, besides having access to a corresponding access node, there are four main ways to obtain most of those: government platform, work account, educational institution account and the payment system, which constitute four semi-isolated branches representing different aspects of the user's life. Those are

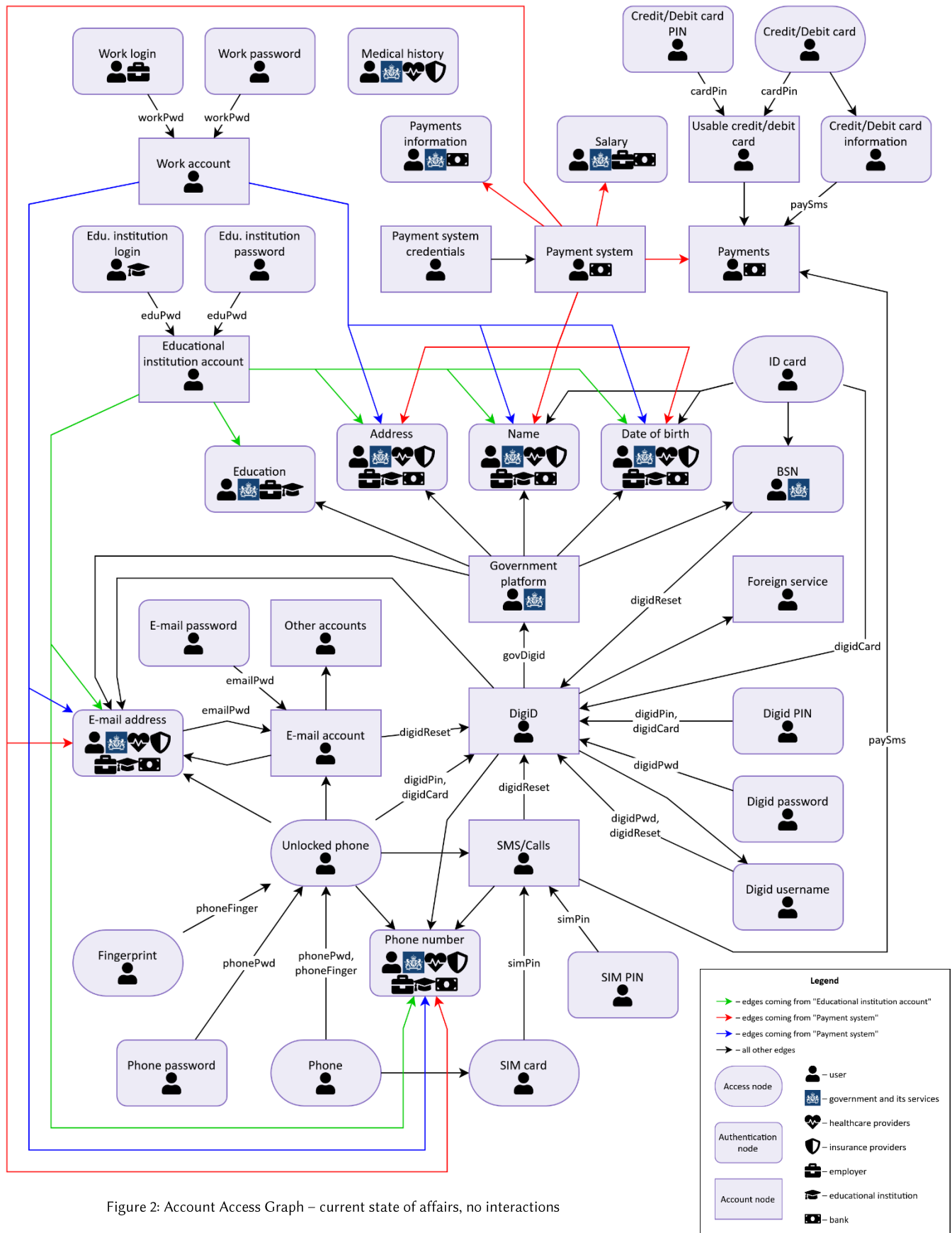


Figure 2: Account Access Graph – current state of affairs, no interactions

the end accounts of the highest importance as control over those allows almost unrestricted access to all user information and actions. The other nodes as important as these four are the e-mail account, SMS/calls and DigiID. We exclude social media and similar accounts from the scope due to informality and inconsistency of those accounts and, therefore, not being affected by the eIDAS regulation to the same extent. Unauthorised access to the seven aforementioned accounts may lead to impersonation and acts on behalf of the user. The eIDAS regulation has the biggest effect on the Dutch platform for electronic identification, DigiID, granting it support to serve as identification abroad, thus the inclusion of the *Foreign service* node. Another node to be noted is the *Medical history*. Even with the access to it by the health providers and, by extension, the government and the insurance, it is impossible to access it without extra services as of now, with the access by the user usually implemented via the general practitioner in person [10].

The model presented has some underlying assumptions, such as:

- The user is logged into their e-mail account on the phone, which is quite often the case due to convenience [14];
- The bank has direct access to the payment system and can freely manipulate the transactions (access to payments). This assumption is justified by the banks' control over their customers' assets. Even if the banks tend to avoid interference with the user's financial activity, the possibility of such interference is present from the side of the financial institutions;
- The government services and platforms are all merged into the *Government platform* as they constitute parts of a greater system and have the same way to access them.

As was mentioned, eIDAS framework builds up on the existing eID infrastructure of the European member states, therefore it will expand the usability of the DigiID rather than replace it. The introduction of the European wallet proposed by the revised eIDAS regulation is to provide an alternative and a more secure way to share pieces of information, which can be reasonably expected to be any information currently accessible through DigiID as both would deal with information provided by the government and its affiliates. Yet, the wallet may provide more freedom in how that information is shared, potentially allowing for creation of derivatives of the existing information [6]. The EUDI Wallet, therefore can be seen as an account to assign new direct access rights to authentication nodes, or dynamic access control system.

4. ANALYSIS

With a general understanding of the information and account landscape in the Netherlands, we can define the safety and security in the scope of electronic identification and trust services. Recall, that safety is concerned with intentional operation of the system and welfare of the user, while security is protection against malicious attacks (Section 1). The purposes of eID and trust services are mainly to verify a person's identity, actions, presence or agreement.

4.1. Safety of electronic identification

We then define the safety of the system, seen as to maintain the intended operation of the system and well-being of the user, as the system allowing the execution of and assisting with the tasks of verifying the actions, presence or agreement of a person. The general safety concerns that may follow from this definition, with the corresponding examples, include:

- loss of access – loss of credentials, device, lack of internet;
- inability to provide access – medical information cannot be accessed in case of emergency;
- inability to verify – a signature cannot be verified as the user's;
- loss of integrity – inaccurate information due to lack of verification of changes done by the user, irreversibility of actions;
- inconvenience/loss of quality – lack of trust towards the system, attachment to the network;
- misuse of the system by the user – no or weak password.

We have included misuse of the system by the user in the list of safety concerns due to two main reasons: first, the misuse being possible may be seen as a failure of the system to address the importance of the user's actions leading to potential harm to the user, and second, due to lack of malice in the desire of the user to harm oneself. Though, the misuses of the system may be intentional and deterministic, making them more similar in nature to security threats.

Those concerns and their examples are the starting list of the feared events related to the safety of the system. In addition, [18] provides a list of vulnerabilities or faults on which the attackers may rely in execution of their attacks. Assuming lack of malicious intent in the introduction of the faults into the system (additionally addressed in Section 5), we use those to complete the list of the safety-related feared events *Table 1*.

Table 1: Safety- and security-related feared events.

Safety	Security
Injection possible	Data storage attack
Registration on a non-compliant entity	Attacker finds expired/revoked credential
Insecure cryptography	Attacker uses expired/revoked credential
Unencrypted data storage	Attacker tries to revoke credential
Unsafe data storage	Malicious app created
Illegitimate credential/data storage	Device theft
Faulty user consent mechanism	Attacker acquires device password
Inadequate anonymisation	Attacker recovers the key
One system for multiple user roles	Attacker generates the key
Data minimisation violation	Attacker acquires the key
Faulty credential refresh/update mechanism	Trusted list access
Faulty credential status check mechanism	Issuer/verifier infiltration
Invalid credential accepted	Issuer/verifier operator deception
Non-repudiation	Attacker uses stolen credentials
Insecure credential revocation mechanism	Attacker's goal is unavailability
User uses expired/revoked credential	DDoS attack
No internet connection	Safety and Security
No clear way to verify the validity of the app	Data breach
User mistakes malicious app for a legitimate one	Credential leakage
Device loss	Illegitimate credential revocation
No or weak device password	Valid credential rejected
Weak key recovery mechanism	Trusted list compromise
Faulty key generation mechanism	Issuer/verifier abuse
Attacker's network used	Attacker's app used
Malicious app is given excessive rights	Attacker injects custom attributes
Insecure communication	Attacker in possession of user's device
Logs contain sensitive information	Attacker controls user's device
Local storage contains sensitive information	Compromised device access
Insecure backup	Configuration modification
Cached sensitive input	Attacker has the key
Unsafe local data storage	Attacker intercepts communication
Unencrypted credentials stored locally	Messages intercepted
Insecure communication	Metadata/credential tampering
Lack of operator training	Attacker mistaken as the user
Lack of resources	Repudiation
Availability	Credential stolen
Health emergency	Unavailability
Medical information unknown	Theft of sensitive information
	Entity impersonation
	Health damage

4.2. Security of electronic identification

The security of the system is defined as protection against the malicious attacks that aim to harm the system or the user. In information systems the three main parameters of a secure system are confidentiality, integrity and availability. The attacks on an information system then can be described as an action intending to tamper confidentiality, integrity or availability. Those can be specified upon with the threats concerning one or more of them, such as those outlined by [16] and [18]: spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege, linking, identifying, non-repudiation, detecting, data disclosure, unawareness unintervenability and non-compliance. These threats are potential goals of an attacker that can be achieved via attack on the information system described in the AAG (Figure 2). We interpreted the threat categories defined by [18] as safety- or security-related feared events in accordance with the definitions. The final list of the feared events can be found in Table 1. This list includes both the general feared events and the events corresponding to the failures to meet the requirements to mitigate other feared events.

4.3. Safety and security interactions

As the next step we organised the safety and security concerns into an Attack-Fault Tree (Figure 3) showing the dependencies and potential routes of attack/failure propagation. We inferred the dependencies from the textual descriptions of possible routes of attacks and vulnerabilities assisting with attacks, as well as from assessing the origins and outcomes of the failures. Notably, some events that may be the goal of the attacker in some scenarios appear to be intermediate in the others. For example, spoofing, (e.g. credential theft) may be a goal of its own for one attacker, while another may use the stolen credentials for impersonation or to make the service unavailable. Therefore, besides the top-level events *reduced trust* and *health damage*, we identified five other ones as high importance: *Credential stolen*, *Repudiation*, *Theft of sensitive information*, *Entity impersonation* and *Unavailability*. Those are potential goals of the attacker, which, consequently, typically have many incoming connections corresponding to a variety of ways in which they may be achieved.

The interactions this research is concerned with are conditional dependence, (mutual) reinforcement and antagonism. The identified interactions are presented here in the same order.

4.3.1. Conditional dependence

Conditional dependence occurs when an event satisfies the condition for another to occur resulting in a definite propagation of failures/attacks. We can observe conditional dependence on the diagram when a child and a parent node are connected directly or through an OR gate. With higher separation we achieve conditional dependence between A and B can whenever a node B can be reached via an AND gate, to which all the inputs are themselves conditionally dependent on A, yet such relations do not exist in the modelled scenario. We have analysed the connections between the feared events in the model against the definition to identify all instances of conditional dependence between the feared events.

As the definitions of the interactions are not limited by being interactions only between safety and security [18], we decided to identify safety-safety and security-security interactions first. Beyond simple cause-outcome relationship (*faulty credential update mechanism* \rightarrow *failure to invalidate the credential*), combination of conditional dependencies can represent such things as:

- generalisations of vulnerabilities, like in the case of *injection possible*, *registration on a non-compliant entity*, *insecure cryptography* and *unencrypted data storage* all considered *unsafe data storage*,
- various ways the same failure/attack result can be achieved: invalid credential can be accepted due to failure to invalidate the credential or a faulty status check mechanism; *issuer/verifier abuse* may be accomplished by infiltrating an issuer/verifier organisation or modifying the trusted list to be recognised as an issuer/verifier, or
- a sequence of possible actions of the attacker: *trusted list access* \rightarrow *trusted list compromise* \rightarrow *issuer/verifier abuse*.

That makes conditional dependencies crucial in planning preventing measures against attacks/failures.

We can observe similar relationships in safety-security interactions, such, the attacker controlling the device is a case of *compromised device access*. Many conditional dependencies outline various approaches to the same goal, such as the ways in which credentials can be stolen. The full list of conditional dependencies is presented in the Table 2 below.

Table 2: Conditional dependencies

Dependent	Type	Condition	Type
Unsafe data storage	Safety	Injection possible	Safety
		Registration on non-compliant entity	Safety
		Insecure cryptography	Safety
		Unencrypted data storage	Safety
Data minimisation violation	Safety	Illegitimate credential/data storage	Safety
		Faulty user consent mechanism	Safety
		Inadequate anonymisation	Safety
		One system for multiple user roles	Safety
Attacker uses expired/revoked credential	Security	Attacker finds expired/revoked credential	Security
Failure to invalidate the credential	Safety	Faulty credential refresh/update mechanism	Safety
Invalid credential accepted	Safety	Failure to invalidate the credential	Safety
		Faulty credential status check mechanism	Safety
Valid credential rejected	Both	Faulty credential status check mechanism	Safety
		Illegitimate credential revocation	Both
User mistakes the malicious app for a legitimate one	Safety	No clear way to verify the validity of the app	Safety
Attacker in possession of user's device	Both	Device theft	Security
		Device loss	Safety
Attacker has the key	Both	Attacker acquires the key	Security
Trusted list compromise	Both	Trusted list access	Security
		Attacker's network used	Safety
Attacker intercepts communication	Both	Attacker's app used	Both
		Attacker's network used	Safety
Compromised device access	Both	Attacker controls user's device	Both
Unsafe local data storage	Safety	Logs contain sensitive information	Safety
		Local storage contains sensitive info	Safety
		Insecure backup	Safety
Issuer/verifier abuse	Both	Issuer/verifier infiltration	Security
		Trusted list compromise	Both
		Cached sensitive input	Safety
Credential stolen	Both	Credential leakage	Both
		Issuer/verifier abuse	Both
		Attacker injects custom attributes	Both
		Messages intercepted	Both
Repudiation	Both	Issuer/verifier abuse	Both
		Metadata/credential tampering	Both
Unavailability	Both	No internet connection	Safety
		Valid credential rejected	Both
		Lack of resources	Safety
Reduced trust	Both	Theft of sensitive information	Both
		Entity impersonation	Both
		Repudiation	Both
		Non-repudiation	Safety
		Unavailability	Both

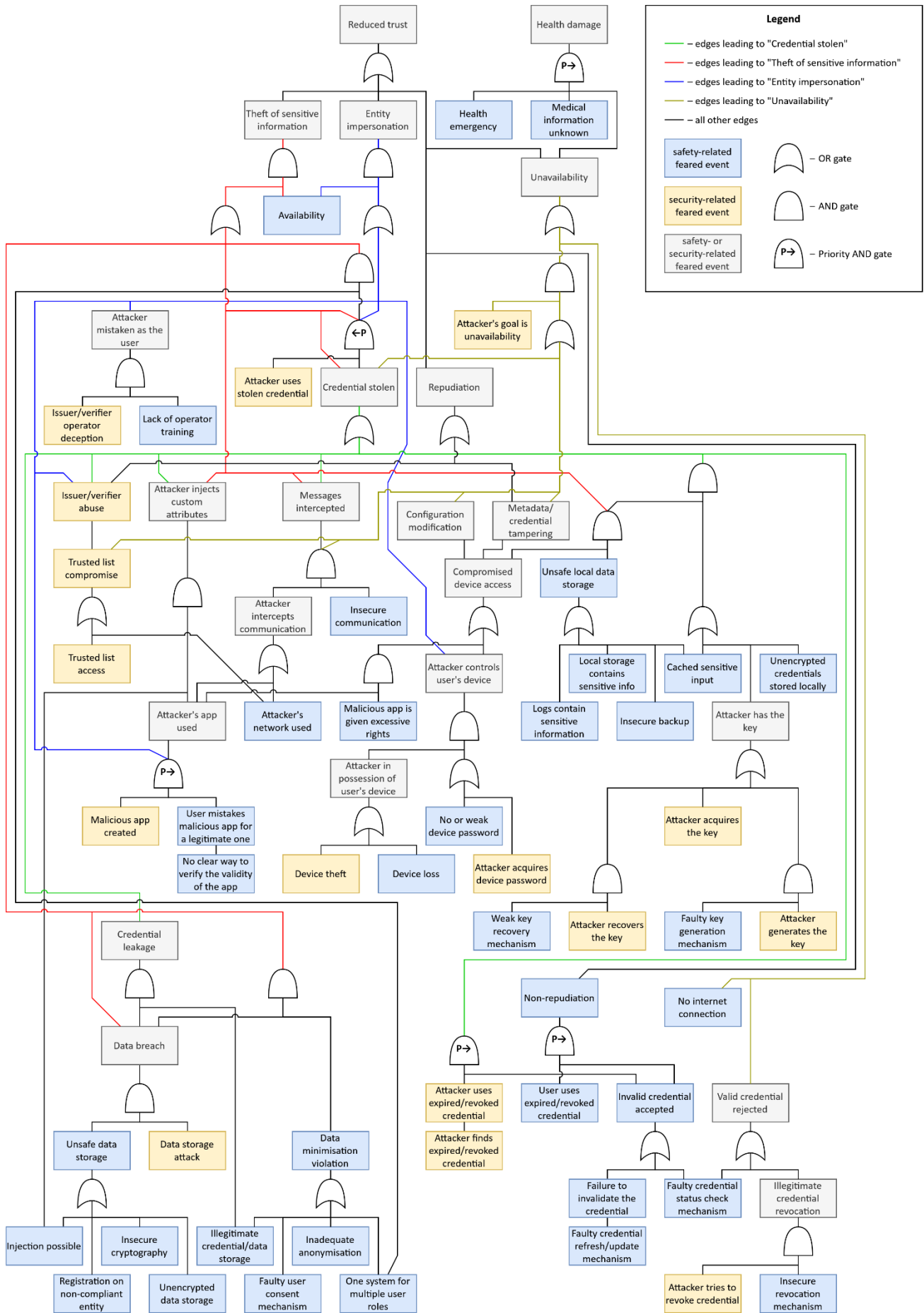


Figure 3: Attack-Fault Tree

4.3.2. Mutual reinforcement

Reinforcement between events happen whenever protective measures against one contribute to protection against another, allowing for optimisation. As mentioned in [13], mutual reinforcement usually occurs due to the events connected exclusively to the same AND-gates. We also identified the cases of unidirectional reinforcement, which often occur when the nodes are still connected to the same AND-gate, but the reinforcing node has other outgoing connections. In case OR-gate precedes an AND-gate, the reinforcement may propagate to the nodes connected to the OR gate, given they stay exclusively connected to the AND-gate (*attacker in possession of user's device* reinforcing *no or weak device password*). Moreover, one can describe reinforcement as transitive in a way that if A reinforces B and B reinforces C, A reinforces C.

We found the cases of reinforcement by going through the feared events (iterate with k), finding the smallest possible sets of events that would imply the k occurs and checking for implication between the preceding events in those sets according to the definition. (if A is in the set, B must be in the set) Table 3 and Table 4 below present all cases of reinforcement found in the study. Quite often the cases of reinforcement reflect the utilisation of system vulnerabilities or failures by the attacker to achieve their goals.

Table 3: Unilateral reinforcement.

Reinforcing	Type	Reinforced	Type
Data breach	Both	Data minimisation violation	Safety
Invalid credential accepted	Safety	Attacker uses expired/revoked credential User uses expired/revoked credential	Security Safety
Attacker in possession of user's device	Both	No or weak device password Attacker acquires device password	Safety Security
Attacker's app used	Both	Malicious app is given excessive rights	Safety
Compromised device access	Both	Unsafe local data storage	Safety
Unsafe local data storage	Safety	Attacker has the key Unencrypted credentials stored locally	Both Safety
Credential stolen	Both	Attacker uses stolen credential	Security
Attacker's goal is unavailability	Security	Configuration modification	Both
Availability	Safety	Attacker mistaken as the user Credential stolen	Both Both
Unavailability	Both	Health emergency Medical information unknown	Safety Safety

Table 4: Mutual reinforcement.

Node 1	Type	Node 2	Type
Unsafe data storage	Safety	Data storage attack	Security
Attacker tries to revoke credential	Security	Insecure revocation mechanism	Safety
Malicious app created	Security	User mistakes malicious app for a legitimate one	Safety
Weak key recovery system	Safety	Attacker recovers the key	Security
Faulty key generation mechanism	Safety	Attacker generates the key	Security
Attacker intercepts communication	Both	Insecure communication	Safety
Issuer/verifier operator deception	Security	Lack of operator training	Safety
Lack of resources	Safety	DDoS attack	Security
Health emergency	Safety	Medical information unknown	Safety

4.3.3. Antagonism

Antagonism denotes contradicting safety and security requirements. In those cases, reinforcement of one part of the system requires sacrifice of the protection of another. Due to the choice of the model the antagonistic events had to be found and added manually. The main and the most obvious example of the antagonism in the modelled environment is the Availability – Unavailability conflict. Availability allows the intended operation of the system, while letting potential attackers abuse it in pursuit of their goals of

Theft of sensitive information and Entity impersonation. Nevertheless, it is not uncommon for information systems to halt operation in events of suspicious activity until the problem is resolved [18]. Other examples may include use of a more secure communication or prohibition of external app use, leading to higher computational requirements of the system, increasing the chance of lack of resources.

5. DISCUSSION AND FUTURE WORK

Given the definition of security is based on the presence of a malicious intent behind the actions, its use in real scenarios is limited by the extent to which malicious actions can be identified and detected. The issue is only more prominent in the cases concerning national and international security, such as with the eIDAS. A software bug, for example may be introduced into the system by mistake or as an act of sabotage. Given the general nature of the analysis and lack of information contradicting the categorisation made assumes the lack of malicious intent behind the safety-related feared event. Nevertheless, in case conflicting information is found, the model may be adjusted accordingly.

Another problem of modelling actions of real people is unpredictability of the decisions. While AFT allows modelling decisions being made with nodes depicting will of a person, they usually do not add much value in terms of analysis of safety or security concerns. We therefore decided to omit intermediate decisions in cases when antagonism does not occur. Such a model assumes the intention of the attacker to cause as much damage as possible.

Unlike account access graphs, attack trees are acyclic in nature, not allowing for the dependencies like acquisition of password 1 from password 2 or password 2 from password 1 in case the passwords are the same.

Flexibility of the wallet system allowing for choosing what information is stored and what information is provided to an entity complicates the assessment of the risks and potential damage in case of failure/attack. The general events like *Theft of sensitive information*, therefore cannot fully reflect what information is acquired. The visualisation provided attempts to consider various data sources and extra information by use of multiple approaches and use of split and an additional AND gate for introduction of catalysts as can be seen on *Figure 4*.

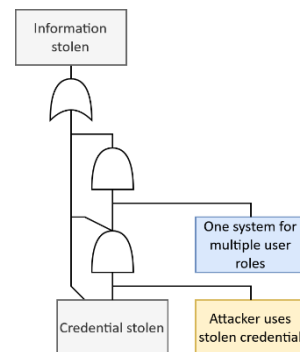


Figure 4: Compounding effects of attacks/faults.

Future work may include expansion of the methodology and, more specifically, modelling capabilities of AFT's to mitigate the limitations identified in this case by, for example, allowing cyclic dependencies and incorporating the algorithm for calculating the convergence of probabilities and cost in case of the cycle with a maximum function or a weighted sum of the values of the incoming nodes.

As per safety and security interactions, further work shall revise the findings of this research when more information on the final implementation of the EUDI wallet is available and new use cases are incorporated. The underlying assumption of the system operating in the Netherlands in a similar fashion to the DigiD service may be challenged with a passage of time.

This work also attempted to analyse all interactions between the feared events, regardless of their type, which, to the best knowledge of the author, has not been done previously. We found no significant limitations of this approach so far, but further work may be needed on the validity of such approach to provide a more rigorous foundation for the analysis of safety and security threats in conjunction. Moreover, the model may benefit from additional types of events with narrower definitions to more accurately represent the scenario. Such, from the limitations found in this work, distinguishment of the user error as a separate category of feared events has a potential to define the safety and security more precisely with less ambiguity.

6. FINDINGS AND CONCLUSION

The goal of this paper was to identify safety and security concerns in the field of electronic identification and trust services, as well as the interactions between the two. An additional requirement was to consider the implications of the holistic relationships between the entities. In this paper we have:

- identified the digital landscape of a Dutch citizen and modelled it with an Account Access Graph (Figure 2),
- defined safety and security in the scope of eIDAS,
- identified the safety and security threats in eIDAS-compliant trust services (Table 1),
- modelled the safety-security interactions with an Attack-Fault Tree (Figure 3) allowing for further analysis,
- identified 43 cases of conditional dependence (Table 2), 15 cases of unidirectional reinforcement (Table 3), 9 cases of mutual reinforcement (Table 4) and 3 cases of antagonism (Section 4.3.3).

The most notable findings we have identified are:

- availability – unavailability antagonism on a high level, being a constant trade-off between safety and security regardless of the attack route,
- lack of other cases of antagonism: only three cases of antagonism may indicate a possibility for creating a system, which is both safe and secure, yet that may have increased complexity of the system creating more potential points of failure,
- most of the reinforcing nodes are safety-related or both safety- and security-related, further allowing to maintain control over the safety and security of the system by enhancing the quality of the implementation of the regulation.

The specifics of the dynamic access control system, however, introduced a level of complexity, which could not be addressed in full. The discussion section of this study outlines the limitations and proposes adjustments to the methodology that would potentially enhance the modelling capabilities and aid the analysis of the feared events.

ACKNOWLEDGMENTS

I would like to thank my supervisor, Dr Christina Kolb for the help she provided during the process of writing this paper, such as presenting invaluable feedback and guiding me in the process of writing an academic paper.

REFERENCES

- [1] Luca Arnaboldi, David Aspinall, Christina Kolb, and Saša Radomirović. 2024. Tactics for Account Access Graphs. In *Lecture Notes in Computer Science*. Springer Nature Switzerland, 452–470. https://doi.org/10.1007/978-3-031-51479-1_23
- [2] Nitesh Bharosa, Silvia Lips, and Dirk Draheim. 2020. Making e-Government Work: Learning from the Netherlands and Estonia. In *Lecture Notes in Computer Science*. Springer International Publishing, 41–53. https://doi.org/10.1007/978-3-030-58141-1_4
- [3] Carlos E. Budde, Christina Kolb, and Mariëlle Stoelinga. 2021. Attack Trees vs. Fault Trees: Two Sides of the Same Coin from Different Currencies. In *Lecture Notes in Computer Science*. Springer International Publishing, 457–467. https://doi.org/10.1007/978-3-030-85172-9_24
- [4] Andre Büttner and Nils Gruschka. 2024. Evaluating the Influence of Multi-Factor Authentication and Recovery Settings on the Security and Accessibility of User Accounts. In *Proceedings of the 10th International Conference on Information Systems Security and Privacy*, SCITEPRESS - Science. <https://doi.org/10.5220/0012319000003648>
- [5] João Manuel Alexandrino de Castro Ribeiro. 2023. SSI Technology in the context of eIDAS 2.0. Universidade do Porto. Retrieved from <https://hdl.handle.net/10216/156528>
- [6] COM/2021/281 final. 2021. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281>
- [7] Muhammad Abdullah Hamid, Ifrah Dar, Isha Fatima, and Nouman Cheema. 2023. Digital Identity and Legal Rights: the EU’s eIDAS Regulation as a Model for Global Digital Trust. In *Democracy, Rule of Law, and Protection of Human Rights in the European Union*, Malkhaz Nakashidze (ed.). Batumi Shota Rustaveli State University, 88–107. Retrieved from <http://jeanmonnetchair.edu.ge/wp-content/uploads/2023/12/Jean-Monnet-Edited-Book.pdf>
- [8] Sven Hammann. 2021. Secure, Private, and Personal: Advancing Digital Identity. Doctoral Thesis. ETH Zurich, Zurich. <https://doi.org/10.3929/ethz-b-000494496>
- [9] Sven Hammann, Saša Radomirović, Ralf Sasse, and David Basin. 2019. User Account Access Graphs88. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS ’19)*, ACM. <https://doi.org/10.1145/3319535.3354193>
- [10] Bas Hoogenbosch, Jeroen Postma, Janneke M de Man-van Ginkel, Nicole AM Tiemessen, Johannes JM van Delden, and Harmieke van Os-Medendorp. 2018. Use and the Users of a Patient Portal: Cross-Sectional Study. *Journal of Medical Internet Research* 20, 9 (September 2018), e262. <https://doi.org/10.2196/jmir.9418>
- [11] Giannis Konstantinidis. 2021. Identity and Access Management for e-Government Services in the European Union – State of the Art Review. University of the Aegean. Retrieved from <https://hellenicus.lib.aegean.gr/handle/11610/23968>

- [12] Michael Kubach, Christian H. Schunck, Rachelle Sellung, and Heiko Roßnagel. 2020. Self-sovereign and Decentralized identity as the future of identity management? (2020). https://doi.org/10.18420/OIS2020_03
- [13] Stefano M. Nicoletti, Marijn Peppelman, Christina Kolb, and Mariëlle Stoeltinga. 2023. Model-based joint analysis of safety and security: Survey and identification of gaps. *Computer Science Review* 50, (November 2023), 100597. <https://doi.org/10.1016/j.cosrev.2023.100597>
- [14] Ketan Pandya. 2022. User Preferences for Email Tasks on Different Platforms. (2022). <https://doi.org/10.17615/2DDF-H784>
- [15] Minjung Park and Sangmi Chai. 2018. The Value of Personal Information: An Exploratory Study for Types of Personal Information and Its Value. *Asia Pacific Journal of Information Systems* 28, 3, 154–166. <https://doi.org/10.14329/apjis.2018.28.3.154>
- [16] Daniela Pöhn, Michael Grabatin, and Wolfgang Hommel. 2023. Modeling the Threats to Self-Sovereign Identities. (2023). https://doi.org/10.18420/OID2023_07
- [17] Megha Quamara, Christina Kolb, and Brahim Hamid. 2023. Analyzing Origins of Safety and Security Interactions Using Feared Events Trees and Multi-level Model. In *Lecture Notes in Computer Science*. Springer Nature Switzerland, 176–187. https://doi.org/10.1007/978-3-031-40953-0_15
- [18] Amir Sharif and Giada Sciarretta. 2024. The eIDAS2.0 Era: Exploring the Security Landscape of Digital Identity Wallets. In *European Digital Identity and Cloud (EIC) Conference*, Berlin, Germany. Retrieved from https://www.kuppingercole.com/get/1550_-1610_dr._amir_sharif_dr._giada_sciarretta.pdf

A USE OF AI

During the preparation of this work the author used no artificial intelligence tools.