Research Article

Max Sauer*, Christoph Becker, Lukas Kneis, Andreas Oberweis, Simon Pfeifer, Akim Stark and Jan Sürmeli

A case study of the MEUSec method to enhance user experience and information security of digital identity wallets

https://doi.org/10.1515/icom-2024-0057
Received October 29, 2024; accepted March 7, 2025;
published online March 31, 2025

Abstract: Digital identity wallets enable the storage and management of digital identities and verifiable credentials in one place on end users' devices. This includes discount vouchers or customer cards, and security-critical data such as ID cards or driving licences. However, digital identity wallets face significant challenges due to weaknesses in user experience and information security. Users often find it difficult to understand the concept of digital identity wallets, resulting in personal information being inadvertently shared with untrusted parties. Additionally, user experience and information security can influence each other, so that both aspects must be evaluated and improved together. To this end, the Method for Enhancing User Experience and Information Security (MEUSec) can be used. This article reports on an experimental application of the MEUSec method to the wallet "Hidy" with two research goals: First, to evaluate the MEUSec method and the quality of its results against a set of criteria, and second, to collect suggestions for improving the user experience and information security of the Hidy wallet. In total, 41 weaknesses and 7 strengths of user experience and information security, 32 heuristics and 26 improvement suggestions for the Hidy wallet could be identified.

Keywords: digital identity wallets; user experience; information security; usable security; evaluation

1 Digital identity wallets for all European citizens

As digitalisation progresses, the range of digital services is growing. People want to use digital services to save themselves the physical journey, e.g., to government agencies. In order to ensure trustworthy interactions with digital services, it is necessary to verify the identity and individual attributes of entities (e.g., persons, organizations, animals or devices).[1]

In the digital space, a digital identity is the set of attributes that identify an entity.[2] Digital identities can use digital credentials to prove their identity. A digital credential is a certificate of identity, qualification, or authorization. It is issued by third parties (issuers) and can be presented to third parties called verifiers.[1] A digital credential that is verifiable and cryptographically secured is called a verifiable credential (VC).[3] Holders can store their VC in so-called digital identity wallets (short: wallets).

A wallet is a software application that allows holders of VC to store, manage, and present their VC in one place on their (mostly mobile) devices. This allows holders to decide for themselves which VC stored in the wallet they want to present to verifiers. A wallet has six basic functions: (1) It provides a *VC overview* containing all stored VC. (2) There is a *detailed view* showing VC details. (3) Stored VC can be *deleted*. (4) The wallet has an area for *help or frequently asked questions*. (5) The wallet has a *backup function*

***Corresponding author: Max Sauer**, FZI Research Center for Information Technology, 76131 Karlsruhe, Germany,
E-mail: sauer@fzi.de. https://orcid.org/0000-0002-6734-3767
Christoph Becker, **Lukas Kneis**, **Andreas Oberweis**, **Simon Pfeifer**, **Akim Stark** and **Jan Sürmeli**, FZI Research Center for Information Technology, 76131 Karlsruhe, Germany,
E-mail: christoph.becker@fzi.de (C. Becker), kneis@fzi.de (L. Kneis), oberweis@fzi.de (A. Oberweis), pfeifer@fzi.de (S. Pfeifer), stark@fzi.de (A. Stark), suermeli@fzi.de (J. Sürmeli).
https://orcid.org/0000-0001-8843-2649 (C. Becker),
https://orcid.org/0009-0009-4778-4969 (L. Kneis),
https://orcid.org/0000-0002-5304-8433 (A. Oberweis),
https://orcid.org/0009-0001-4815-6149 (S. Pfeifer),
https://orcid.org/0009-0005-4718-1202 (A. Stark),
https://orcid.org/0000-0001-6617-3674 (J. Sürmeli)

[1] In other terminologies, verifiers are known as relying parties.

allowing users to create a backup of all their identity-related data, including VC, contacts/connections and a history. (6) The wallet has a function to *restore the backup data*.[4]

The topic of wallets is becoming increasingly relevant due to the entry into force of the revised regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) regulation in May 2024: Every European Member State must provide its citizens with a digital identity wallet by November 2026.[5]

In order to achieve a high level of acceptance of wallets by the citizens, wallets should offer a sufficient user experience and information security. *User Experience* (UX) is defined as the “user’s perceptions and responses that result from the use and/or anticipated use of a system, product or service”.[6] UX has seven different attributes: utility, desirability, findability, accessibility, credibility, value and usability.[7,8] *Information security* (InfoSec) is defined as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability”.[9]

However, research shows that current wallets have several UX and InfoSec weaknesses.[10–14] Even tech-savvy wallet users have difficulties setting up the wallet and managing their VC, as wallets are too complex and not intuitive.[10] In order to improve UX and InfoSec, it is not enough to consider both aspects separately, as both aspects can influence each other.[15,16] For example, complex InfoSec mechanisms can lead to a poor UX, while the UX can contribute to relevant InfoSec information being overlooked. Therefore, UX and InfoSec of wallets must be jointly evaluated and improved so that the roll out of wallets to EU citizens can be a success. To evaluate and improve UX and InfoSec of wallets, the MEUSec method by Sauer et al.[17] can be used. However, a detailed evaluation of the MEUSec method is still pending.

This article provides two key contributions extending the previous work in Ref. 17: (A) The MEUSec method was evaluated by applying it to the Hidy wallet[2] using various evaluation criteria. (B) By applying the MEUSec method, the UX and InfoSec of the Hidy wallet were evaluated and improvement suggestions were collected. A total of 41 weaknesses and 7 strengths of UX and InfoSec, 32 derived heuristics (including 5 from literature) and 26 improvement suggestions were identified. Heuristics provide quality guidelines, regarding criteria such as UX or InfoSec, which can be fulfilled to certain degrees by different systems.[18] Such heuristics can be used in requirements engineering to specify or evaluate the satisfaction of requirements for systems under development, or to evaluate and compare existing systems. Well-known UX heuristics are the heuristics from Nielsen[19] and InfoSec heuristics from Realpe et al.[20]

This article is structured as follows: Section 2 describes the problem definition and related work. Afterwards, the MEUSec method for evaluating and improving UX and InfoSec of wallets is described in Section 3. Furthermore, Section 4 describes the goals and approach of this research contribution. In Section 5, the application of the MEUSec method to the Hidy wallet is described. First, the application of each method step is explained (Sections 5.1–5.8). Afterwards, in Section 5.9, the identified UX and InfoSec strengths and weaknesses of the Hidy wallet are discussed and placed in the context of the results from the literature. The evaluation of the MEUSec method is explained in Section 6. In the beginning, Section 6.1 describes the evaluation results of the MEUSec method based on the evaluation criteria from Section 4. Section 6.2 discusses the evaluation results of the MEUSec method and relates them to existing evaluation procedures from the literature. Section 6.3 contains suggestions for improving the MEUSec method. Afterwards, the limitations of the method evaluation are described in Section 7. Section 8 concludes the paper and gives an outlook on future work.

2 UX and InfoSec weaknesses of digital identity wallets

Existing wallets have several UX and InfoSec weaknesses, which is particularly problematic as all EU member states must provide their citizens with such a wallet by 2026:[5]

Test subjects of Korir et al.[11] expressed concerns about the InfoSec of their personal information, fearing it could be stolen or mistakenly shared with wrong online services. Additionally, the use of QR codes caused interruptions that reduced efficiency. It should also be considered that wallet interactions on mobile devices often occur not just with applications on a laptop, but also with other mobile applications. QR codes become unnecessary when the interaction occurs solely on a smartphone, as credentials are already stored within the wallet, allowing users to share their credentials with a button click, without the need for scanning a QR code.

Khayretdinova et al.[10] identified learnability issues of the wallet functions. For instance, test subjects were able

[2] https://www.hidy.eu (accessed on 08/23/2024).

to obtain their first VC with help but failed when attempting to get a second VC using the same method. Moreover, even technically skilled test subjects in the study of Khayretdinova et al.[10] faced challenges in setting up the wallet and managing their VC, as the wallet was complex and not intuitive. This can lead to user frustration or InfoSec issues, such as the accidental sharing of VC. Additionally, participants were unclear about where their VC and data were stored. Some tried to delete data from the server, even though the data was stored locally on their smartphones.

The evaluation by Satybaldy[13] found that some wallets lack secure authentication methods to protect the sensitive data. In one of the wallets examined, biometric authentication did not function properly. Additionally, users had difficulty locating the recovery code and understanding its purpose and functionality.

Sellung and Kubach[14] found that none of the considered wallets allows users to transfer their account and its VC to another wallet, whether to the same wallet on a different smartphone or to wallets from other providers. This results in a lock-in effect, making it difficult for users to switch to a different wallet.

Test subjects of Sartor et al.[12] found the terminology used in the wallet too technical, with terms like “Credentials” and “DID” being confusing. They also requested more assistance, particularly a tutorial during the wallet setup to explain basic functions. Additionally, there was a demand for backup and recovery features, as well as search and sorting functions for VC.

In the wallet evaluation by Sauer et al.[21] test subjects expressed that they want more help hints in the wallet. They perceived some design elements, such as pop-ups, as annoying and commented that shown text was too much to read at once. Test subjects suggested that intuitive icons and symbols should get a stronger emphasis, reducing the need for text. Moreover, test subjects felt the need for more success and failure messages, e.g., when sharing or storing VC in the wallet.

Due to the described weaknesses, UX and InfoSec of wallets should be improved. It is important that UX and InfoSec are evaluated and improved together, as they can influence each other. This influence can either be negative, positive or neutral:

(a) *Negative influence:* Whitten and Tygar[16] evaluated an encryption application and found several UX weaknesses that led to InfoSec weaknesses. The majority of the test subjects were unable to sign and encrypt a message. 3 of the 12 test subjects even revealed their private key. In addition, Reese et al.[22] evaluated the UX of 5 two-factor authentication methods with different levels of InfoSec. They found that 8 of 12 test subjects had difficulty entering a sent 6-digit code before it expired, resulting in a decrease in UX.

In the wallet evaluation by Sauer et al.[21] only 5 of 24 test subjects perceived a warning about an unverified issuer, which could lead to the unwanted issuance of a VC by an untrustworthy party. Additionally, the Thinking aloud results showed that some basic wallet functions were not understood by the test subjects in the user study, which could potentially lead to unintentional actions impacting InfoSec.

(b) *Positive influence:* Hinds and Ekwueme[23] developed an authentication procedure with graphical passwords. This enabled them to improve UX and InfoSec. After 30 days, most users could still remember their password with 86 % accuracy.

(c) *No (significant) influence:* Zhang et al.[24] evaluated how the conventional Android unlock pattern (3 × 3 layout) can be improved. They were able to improve InfoSec of the unlock pattern without significantly affecting UX. According to wallets, Sauer et al.[21] evaluated the UX of different authentication methods. They found that the UX does not change significantly from a 4-digit pin to a 6-digit pin – whereas the InfoSec is increased.

In summary, this means that UX and InfoSec should not be evaluated and improved separately, but should be considered together.

3 MEUSec – a method for enhancing user experience and information security

Sauer et al.[17] developed a method for evaluating and improving UX and InfoSec of wallets: *Method for Enhancing UX and InfoSec* (in short: MEUSec).

Four roles must be filled for the application of the MEUSec method: One *method user* (MU), one *InfoSec expert* (ISE), one *UX expert* (UXE) and *wallet users* (WU).

The MEUSec method consists of 8 steps (each consisting of individual activities), which are briefly described below:

- *Step 1 – Definition of evaluation object:* First, the MU defines the wallet functions to be evaluated using a proposed list of functions (1.1). The ISE and MU then identify security relevant components and potential attackers (1.2) and finally define the InfoSec evaluation scope (1.3).
- *Step 2 – Preparation of user-based evaluation:* The ISE, MU and UXE define requirements of the WU selection (2.1) and test cases (2.2) for the later Thinking aloud.[25]

The MU then acquires the WU (2.3) and sets up the test cases on the test devices (2.4).

- *Step 3 – Execution of user-based evaluation:* The MU starts the lab recordings (3.1) and each WU performs Thinking aloud (3.2) on the test devices. Finally, the MU archives the lab recordings (3.3).
- *Step 4 – Evaluation of user-based evaluation results:* The MU, UXE and ISE look together at the Thinking aloud recordings of the WU and collect strengths and weaknesses of UX and InfoSec with the help of a predefined template (4.1). In addition, they derive UX and InfoSec heuristics using a predefined template (4.2). Finally, the MU creates a collection of the formulated heuristics (4.3).
- *Step 5 – Preparation of expert-based evaluation:* The MU, UXE and ISE look at an external collection of heuristics proposed by the MEUSec method and select suitable heuristics to add to their own collection (5.1). This collection consists of a list of publications about heuristics, e.g., 19, 20, 26. Afterwards, they decide whether all defined wallet functions are covered by heuristics. If not, UXE and ISE conduct a literature search (5.2) and add the missing heuristics to their own collection (5.3). If yes, these activities (5.2 and 5.3) can be skipped and the ISE can continue with the next activity, namely that ISE updates the InfoSec relevant components and potential attackers if necessary (5.4). Furthermore, the MU and ISE update the InfoSec evaluation scope and heuristics if necessary (5.5). Finally, the MU, UXE and ISE assign weights to the heuristics according to their relevance (5.6).
- *Step 6 – Execution of expert-based evaluation:* The UXE and ISE test the defined wallet functions (6.1) and rate a fulfillment score for each heuristic (6.2). The MU creates an interaction matrix[27] of the defined heuristics (6.3) and the MU, UXE and ISE fill the interaction matrix through discussions (6.4). Each pair of heuristics is assigned one interaction property: (a) ‘conflicting’, which means that the respective heuristics influence each other negatively, (b) ‘complementary’, which means that heuristics influence each other positively or (c) neutral, which means that heuristics do not (significantly) influence each other. Finally, the MU adds the interaction properties to the heuristic collection (6.5).
- *Step 7 – Evaluation and validation of expert-based evaluation results:* The MU aggregates the scores of the heuristics for all UX and InfoSec attributes (7.1), e.g., one score each for the UX attributes desirability, accessibility and usability and one score each for the InfoSec attributes confidentiality, integrity and availability. Afterwards, the MU aggregates a score for UX and InfoSec based on the individual attribute scores (7.2). Furthermore, the MU, UXE and ISE conduct a feedback discussion on whether problems have arisen in the assessment of the heuristic fulfilment levels (7.3). If yes, the corresponding heuristics must be updated (7.4) and the evaluation be repeated from step 6. If no, the MU adds the own heuristic collection to the external heuristic collection (7.5).
- *Step 8 – Enhancement of UX and InfoSec:* The MU, UXE and ISE try to find solutions for conflicting heuristics through discussion (8.1). If no solution is found for a conflicting pair of heuristics, either the UX or InfoSec is prioritized by the MU in discussion with the UXE and ISE (8.2). For this purpose, the corresponding heuristics from either prioritized UX or InfoSec are used to improve the wallet. The MU, UXE and ISE then collect improvement suggestions for the complementary and neutral heuristics (8.3). Complementary and neutral heuristics have no negative influence, so that the heuristics themselves usually already specify the improvement suggestions.

Figure 1 visualizes the described generalized 8 steps of the MEUSec method. A more detailed process model of the 8 steps with their individual activities is online available.[3]

4 Goals and approach

The motivation for the work leading to this paper was twofold. From a practical point of view, the goal was to apply the MEUSec method to evaluate a specific wallet, namely the Hidy wallet.[4] Additionally, a scientific evaluation of the MEUSec method, with regards to its feasibility and the results’ quality, was essential to its further development. Those goals led to a nested evaluation approach, consisting of a *wallet evaluation* and a *method evaluation.*

In the wallet evaluation, the MEUSec method described in Section 3 was applied to the Hidy wallet developed by the University of Applied Sciences Mittweida.[5] The goal was to evaluate and improve UX and InfoSec of the Hidy wallet. As the Hidy wallet was studied in the SDIKA project,[6] it was possible to interview the developers and access the source

[3] https://doi.org/10.5281/zenodo.10529247 (accessed on 10/24/2024).

[4] https://www.hidy.eu (accessed on 08/23/2024).

[5] https://www.hs-mittweida.de/en (accessed on 08/23/2024).

[6] https://www.sdika.de (accessed on 01/27/2025).

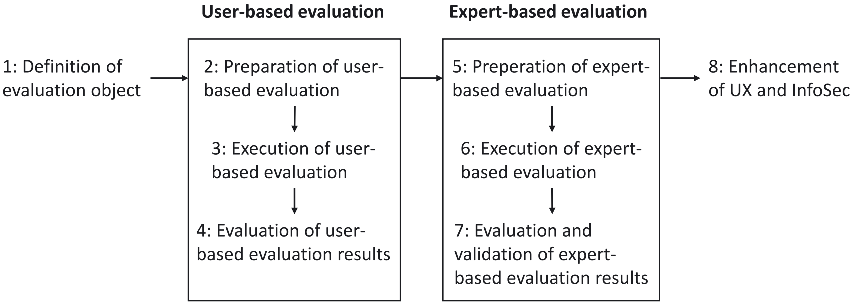
User-based evaluation
Expert-based evaluation
1: Definition of evaluation object
2: Preparation of user-based evaluation
3: Execution of user-based evaluation
4: Evaluation of user-based evaluation results
5: Preperation of expert-based evaluation
6: Execution of expert-based evaluation
7: Evaluation and validation of expert-based evaluation results
8: Enhancement of UX and InfoSec

Figure 1: Summary of the 8 MEUSec method steps by Sauer et al.[17]

code. Thus, the evaluation was not only feasible, but also provided the opportunity to feed evaluation results into further iterations.

The roles of the MEUSec method were filled as follows: The MU was a research scientist who had no experience with UX, InfoSec and wallets. This selection of the MU was made specifically for the later evaluation in order to evaluate whether the MU can also be a person who has no experience with UX, InfoSec and wallets when using the MEUSec method. The ISE was a research scientist who conducts research in the field of InfoSec. The UXE was a research scientist who conducts research in the field of UX. The WU were acquired later in the application of the MEUSec method and are therefore described in the corresponding Section 5.2. The evaluation object – the Hidy wallet – is also described in the corresponding Section 5.1.

The method evaluation utilized the wallet evaluation. To this end, the ISE, UXE and MU took notes after each of the 8 MEUSec method steps for each evaluation criterion. In addition, an external person was involved taking notes on each evaluation criterion independently of the roles without intervening, e.g., measuring times per step. After the application of the MEUSec method, there was a joint discussion round to collect further evaluation results. The following evaluation criteria of[28,29] were used, which are basically divided into the quality of the method results and the feasibility of the method:

(E1) **Quality of the method results**

(E1.1) Completeness: Has each defined wallet function been evaluated with regard to UX and InfoSec, i.e., is there at least one UX heuristic and at least one InfoSec heuristic per defined wallet function, of which the degree of fulfillment has been evaluated? Are all implications to the other heuristics evaluated for each heuristic? Has at least one improvement suggestion been identified for each heuristic with a fulfillment level below 100 %, considering the implications to the other heuristics?

(E1.2) Consistency: Is a standardised evaluation scheme used to evaluate the degree of fulfillment of all heuristics? Is a standardised evaluation scheme used to evaluate the interaction properties of the heuristics (complementary, conflicting or neutral)? Are there no contradictory improvement suggestions?

(E1.3) Correctness: Do the proposed improvements really bring improvements? Experts should score the heuristics again, assuming that the improvement suggestions have been implemented, and check whether the score has improved.

(E1.4) Traceability: Are the scores and implications to the used heuristics traceable? Is the prioritisation of UX or InfoSec of conflicting heuristics and their justification traceable? Are the identified improvement suggestions traceable?

(E1.5) Clarity: Are the heuristics clearly formulated? Have the fulfillment levels of the heuristics been clearly defined? Are the implications of the heuristics clearly formulated? Are improvement suggestions clearly formulated?

(E1.6) Relevance: Do the UX and InfoSec scores serve as a comparison for the following application of the MEUSec method? Do the identified implications serve for the formulation of improvement suggestions? Are the improvement suggestions pertinent/relevant, i.e., are the improvement suggestions expected to improve the identified UX and InfoSec weaknesses (considering the implications)?

(E2) **Method feasibility**

(E2.1) Effectiveness: Can the MEUSec method be used to evaluate UX and InfoSec, considering the implications of UX and InfoSec? Can the

MEUSec method be used to find improvement suggestions for UX and InfoSec, considering the implications of UX and InfoSec?

(E2.2) Efficiency: Can the MEUSec method be used to evaluate and improve UX and InfoSec (considering the implications of UX and InfoSec) with a minimum use of resources, i.e., time and costs?

(E2.3) Acceptance: Is the MEUSec method accepted by UXE, ISE and MU?

5 Wallet evaluation

The application of the MEUSec method to the Hidy wallet is described below by explaining the results of the 8 method steps and their activities (Sections 5.1–5.8). The detailed artifacts are available online.[7] Finally, Section 5.9 concludes with the discussion of the wallet evaluation results.

5.1 Step 1: definition of evaluation object

Input of Step 1: The Hidy wallet[8] by the University of Applied Sciences Mittweida[9] was used as evaluation object.

(1.1) Define wallet functions to be evaluated: Initially, the MU defined the wallet functions to be evaluated by selecting them from a suggested list of Krauß et al.[30] The following wallet functions have been defined for evaluation by the MU:

(a) Storing VC, in particular presentation and verification of the trustworthiness of the VC issuer.
(b) Management of VC, in particular quick access to stored VC, deletion of VC and the display of VC.
(c) Transfer of stored VC, in particular presentation and verification of the trustworthiness of the verifier, presentation and verification of the purpose of use of VC to be shared.

In addition to the wallet functions selected from the list of Krauß et al.[30] the following wallet functions were defined by the MU:

(d) Payment function, in particular requesting and making payments and
(e) General operating functions, such as returning to previous screens.

(1.2) Identify security relevant components and potential attackers and (1.3) define scope of InfoSec evaluation: The ISE identified the security relevant components and potential attackers by viewing the wallet documentation. He also discussed these with the MU to define the scope of the InfoSec evaluation: (a) Malicious issuer who can create and sign VC, compromising integrity and confidentiality. (b) Issuer provides unwanted information in the VC (e.g., hidden health information) so that the issuer and verifier can co-operate, which compromises confidentiality and (c) Malicious verifier that uses VC for itself, which compromises confidentiality and integrity.

Output of Step 1: Defined evaluation object.

5.2 Step 2: preparation of user-based evaluation

Input of Step 2: Defined evaluation object from Step 1 (see Section 5.1).

(2.1) Determine requirements of the WU selection: The MU, UXE and ISE specified that 10 WU should be involved in Thinking aloud, differing in terms of gender, age, private operating system (e.g., iOS), previous experience with wallets and cryptocurrencies, IT affinity, German language skills and physical limitations (e.g., visual impairment). Nielsen and Landauer[31] recommend 5 WU for a user test. Due to the many different properties of the WU selection, it was decided to carry out the test with 10 WU.

(2.2) Define test cases for wallet functions: The MU, UXE and ISE planned the WU tasks for Thinking aloud. They created a paper guide with tasks for the WU to perform when conducting Thinking aloud:

(1) Open the Hidy wallet on the home screen.
(2) Request a payment of 5,000 Satoshi[10] to their Hidy wallet.
(3) Wait for the payment to arrive. At this point you would transfer Satoshis from an external application. In this case, the Hidy wallet is already topped up with Satoshis.
(4) You can now close and reopen the Hidy wallet.
(5) Add “Demo shop” to your wallet features.
(6) Buy any ticket in the demo shop.
(7) Display the ticket in the Hidy wallet.
(8) You realise that you have bought the wrong ticket.
(9) Delete the ticket from the Hidy wallet.

(2.3) Acquire WU: The WU were invited by the MU according to the defined characteristics (see Table 1) to a Thinking

[7] https://doi.org/10.5281/zenodo.13844611 (accessed on 10/24/2024).

[8] https://www.hidy.eu (accessed on 08/23/2024).

[9] https://www.hs-mittweida.de/en (accessed on 08/23/2024).

[10] A Satoshi is equivalent to one hundred millionth of a Bitcoin.

Table 1: Demographic data of WU.

ID	Gender	Age	German skills	Job	IT affinity	Private operating system	Previous experience	Physical limitations
1	Male	26–40	Native	Researcher	Medium	iOS	Wallets	–
2	Male	26–40	Native	Manager	High	iOS	Wallets	–
3	Male	26–40	Native	–	High	iOS	Wallets	–
4	Male	16–25	Native	Researcher	High	Android	–	–
5	Female	26–40	Native	Event manager	Medium	iOS	Wallets	Glasses
6	Male	16–25	Fluent	Student	Medium	Android	–	–
7	Female	16–25	Medium	Student	Medium	Android/iOS	Wallets	–
8	Female	41–60	Native	CEO assistance	Low	Android	–	Glasses
9	Male	41–60	Native	IT admin	High	Android	Cryptocurrencies	Glasses
10	Female	61–80	Native	Educator	Low	Android	Wallets	Glasses

aloud slot of about 30 min. To collect the demographic data, the WU were given a questionnaire to complete. They also had to sign a declaration of consent for data processing. Table 1 shows the demographic data of the 10 WU.

(2.4) Set up test cases on end devices: The Hidy wallet was set up on an IPhone 14 Pro Max. In addition, the defined WU tasks were printed out so that the WU could use them for Thinking aloud. The devices for recording the smartphone screen and the WU (image and sound recording) were also set up.

Output of Step 2: Prepared user-based evaluation.

5.3 Step 3: execution of user-based evaluation

Input of Step 3: User-based evaluation prepared in Step 2 (see Section 5.2).

(3.1) Start lab recordings, conduct Thinking aloud (3.2) and (3.3) stop lab recordings and archive files: The MU first gave each WU (see Table 1) instructions (such as the paper guide from Section 5.2) and started the video and sound recordings. Then each WU performed the Thinking aloud[25] with the paper guide under the supervision of the MU and UXE. Then, the MU stopped and archived the video and audio recordings. The WU received 20€for participating in the evaluation.

Output of Step 3: Thinking aloud recordings of each WU.

5.4 Step 4: evaluation of user-based evaluation results

Input of Step 4: Lab recordings archived in Step 3 (see Section 5.3).

(4.1) Collect strengths and weaknesses of UX and InfoSec: The MU, UXE and ISE reviewed the recordings made in the previous step. While doing so, they identified strengths and weaknesses by looking for actions that the WU either performed with ease or struggled to perform. Both strengths and weaknesses were recorded in a template proposed by the method, as seen in Table 2. The template contains a unique ID, a name with description of the issue and whether it is a strength or weakness regarding either InfoSec or UX. The previously in Section 5.1 defined wallet functions were assigned, as well as attributes regarding UX and InfoSec as defined by Morville[7] and DIN EN ISO/IEC 24760-1.[1] The selection of suitable attributes is decided by a discussion between MU, UXE and ISE. Since during the review of the first three recordings only weaknesses were identified, because they were more obvious, the MU, UXE and ISE shifted their focus towards identifying strengths as well as weaknesses. Some UX and InfoSec weaknesses occured with multiple WU. Since the number of WU was chosen higher than the recommended 5 WU, this was to be expected. A weakness identified during evaluation was, that the VC are not displayed with names and can therefore only be identified by the associated image. Since this image needs to be loaded,

Table 2: Example of a weakness entry.

ID	01
Name	VC have no names
Description	VC do not have a name/description and can only be distinguished by the stored images. These are dependent on the internet connection, without this the VC cannot be distinguished/managed. No name is visible on the offer screen either.
Weakness/strength	Weakness
UX/InfoSec	UX
Attributes	Usability, usefulness, findability, desirability, value
Wallet functions	Quick access to saved VC (NF-5). Delete, save and display of VC.

network connectivity is required to distinguish the VC. Since this is both a UX and an InfoSec weakness, two separate entries were made. From an InfoSec point of view this affects the attributes "Confidentiality" and "Authenticity" since the WU might accidentally present the wrong VC to a verifier. It concerns the wallet functions "Transmission of saved VC", "Saving VC" and "Display of VC". The UX entry for the missing names can be seen in Table 2 while the entry for the InfoSec weakness can be accessed online (see footnote 7) with all other identified strengths ($n = 7$) and weaknesses ($n = 41$).

(4.2) Derive heuristics for UX and InfoSec: The MU, UXE and ISE derived heuristics based on the previously established strengths and weaknesses. A single strength or weakness might have multiple heuristics derived from it. A total of 27 heuristics were derived, which can be accessed online (see footnote 7). For example, both the heuristic "All VC should have unique names" (seen in Table 3) and "Images of VC should be displayed" are derived from the weakness "VC have no names".

(4.3) Create collection and add derived heuristics: The MU used the previously defined heuristics to create a collection, which is available online (see footnote 7). The collection contains a consistent representation of all heuristics.

Output of Step 4: Heuristics for UX and InfoSec determined.

5.5 Step 5: preparation of expert-based evaluation

Input of Step 5: Heuristics for UX and InfoSec determined in Step 4 (see Section 5.4).

(5.1) Select heuristics from external collection and add them to own collection: The MU, ISE and UXE jointly went through the list of possible heuristics by Sauer et al.[26] and added heuristics that were considered useful to extend their own collection. Therefore, the list of heuristics (see footnote 7) has been expanded from 27 to 32 heuristics. The added heuristics are:

(a) The app should offer a search function for VC,
(b) the app should be interoperable with other systems,
(c) it should be possible to create profiles and assign VC to them,
(d) data should be encrypted and transmission secure, and
(e) the app is intended to notify the user of available updates.

(5.2) Literature research of heuristics, strengths and weaknesses of UX and InfoSec and (5.3) Derive heuristics for UX and InfoSec and add them to own collection: The MU, ISE and UXE decided not to conduct a literature search because the extended list of heuristics from Activity 5.1 covers the required functions. This decision is also included in the method and is therefore part of the process. This decision also eliminates Activity 5.3, which is intended to adapt the heuristics found during the literature search and add them to the collection.

(5.4) Update security relevant components and potential attackers and (5.5) update scope of InfoSec evaluation and heuristics: A new attacker has been identified who is gaining access to the storage of the device. If backups are unencrypted, they could be read directly by the attacker. Otherwise, standard attack vectors, such as weak passwords for the encryption of the backups, could be exploited. A second new attacker has been identified who is using known InfoSec vulnerabilities of the general operating functions.

(5.6) Assign weights to heuristics: The MU, ISE and UXE went through the heuristics together and assigned weights to them. The weights chosen were between 1 and 5, with 1 being barely important and 5 being essential. The defined weights can be seen in the list of heuristics (see footnote 7).

Output of Step 5: Heuristics of UX and InfoSec determined and weighted. The list of heuristics created is available online (see footnote 7).

Table 3: Example of a heuristic entry.

ID	01
Name	All VC should have unique names
Description	VC should have unique names and descriptions and these names should be used consistently across all screens.
UX/InfoSec	UX
Attributes	Usability, usefulness, findability, desirability, value
Wallet functions	Management of VC.Quick access to saved VC (NF-5).Delete, save and display of VC. Transfer of saved VC (NF-12).Check and display the trustworthiness of the counterparty (NF-17 and NF-18).Check and display the intended use of the data to be shared (NF-19 and NF-20).

5.6 Step 6: execution of expert-based evaluation

Input of Step 6: Heuristics of UX and InfoSec determined and weighted in Step 5 (see Section 5.5).

(6.1) Test defined wallet functions and (6.2) Rate fulfillment score for each heuristic: The ISE and UXE tested the defined wallet functions and rated each heuristic in the collection by its rate of fulfillment on a scale from "1: Not fulfilled" to "5: completely fulfilled". Both the score and a reasoning for the score were added to the list of heuristics (see footnote 7).

(6.3) Create interaction matrix of defined heuristics: The MU created an interaction matrix to evaluate the interactions of different heuristics with each other. Since each heuristic interacts with every other heuristic and these interactions are not symmetrical (as in: heuristic A can affect heuristic B, but heuristic B might not affect heuristic A making their interactions asymmetrical) the number of fields in the matrix grows fast with an increasing number of heuristics. Since filling out the interactions for all 32 heuristics was deemed unfeasible in a reasonable amount of time, only heuristics with the weight of 5 were included in the interaction matrix. This reduced the number of heuristics from 32 to 12 and the number of fields in the matrix from 992 to 132. The resulting interaction matrix is available online (see footnote 7).

(6.4) Fill interaction matrix through discussion: The MU, ISE and UXE discussed the interactions of the selected heuristics. There are three possible interaction properties: "complementary", "neutral" and "conflicting". If the interaction between heuristic A and heuristic B is complementary, it means that fulfillment of heuristic A also helps fulfilling heuristic B. In a neutral interaction the two heuristics don't affect each other and in case of a conflicting interaction, fulfillment of heuristic A will hinder the fulfillment of heuristic B. No conflicting heuristics were found in the discussion, which is why the interaction matrix only contains neutral and complementary entries. Table 4 shows some heuristics with their interacting properties. Each row represents the effect a heuristic has on other heuristics, while a column in the interaction matrix represents how a heuristic is affected by others. For example, heuristic 02 is complementary to heuristic 11, because unique names for VC improve the comprehensibility of InfoSec instructions. Conversely, heuristic 11 is neutral to heuristic 02, because comprehensible InfoSec instructions do not affect unique names for VC. The entire interaction matrix is available online (see footnote 7).

(6.5) Integrate heuristic interactions in own collection: The MU added the interactions to the list of heuristics (see footnote 7). Since most interactions were deemed to be "neutral", only interactions that are "complementary" are explicitly noted in the list of heuristics.

Output of Step 6: (a) Interaction matrix of defined heuristics created and (b) heuristics scored.

5.7 Step 7: evaluation and validation of expert-based evaluation results

Input of Step 7: Heuristics scored in Step 6 (see Section 5.6).

(7.1) Aggregate scores for each attribute: First, for each heuristic, its weight and degree of fulfillment were multiplied to determine the score for that heuristic. These scores were then totaled for the attributes assigned to the heuristics. Thus, an absolute score was calculated for each attribute which can be seen in the first row in Table 5 for UX attributes and Table 6 for InfoSec attributes. The average score for the attributes was determined by dividing the absolute score by the number of referenced heuristics. These scores fill the second row of the Tables 5 and 6. With the maximum score per attribute, which results from the product of weight with maximum fulfillment score, the average maximum score can be calculated by dividing it by the number of heuristics, as shown in third and fourth row of the tables. Finally, the ratio of the average score to the average maximum score was calculated. This ratio was used to assess the degree of fulfillment for the respective attributes.

(7.2) Aggregate scores for UX and InfoSec: The scores from Activity 7.1 were used to determine the average score, average maximum score and the ratio of these scores at UX and InfoSec level. To do this, the mean value was determined using the mean values of the attributes that belong to UX or InfoSec. The results are shown in Tables 5 and 6.

Table 4: Example of heuristics in the interaction matrix.

	02: unique names for VC	**11: comprehensible InfoSecinstructions**	**29: interoperability**
02: Unique names for VC	X	Complementary	Neutral
11: Comprehensible InfoSecInstructions	Neutral	X	Complementary
29: Interoperability	Neutral	Neutral	X

Table 5: Example of calculated UX scores.

Scores	UX						
	Usefulness	Desirability	Findability	Usability	Accessibility	Credibility	Value
Absolute	72	40	116	212	49	19	78
Average	9	6.67	10.55	10.6	9.8	6.33	9.75
Max	150	100	200	375	90	55	155
Avg. max	18.75	16.67	18.18	18.75	18	18.33	19.38
Ratio	0.48	0.4	0.58	0.57	0.54	0.35	0.5
Average	8.96						
Avg. max	18.29						
Ratio	0.49						

Table 6: Example of calculated InfoSec scores.

Scores	InfoSec				
	Confidentiality	Integrity	Availability	Authenticity	Reliability
Absolute	62	5	33	60	12
Average	12.4	5	8.25	15	12
Max	115	25	90	100	20
Avg. max	23	25	22.5	25	20
Ratio	0.54	0.2	0.37	0.6	0.6
Average	10.53				
Avg. max	23.10				
Ratio	0.46				

The scores can be used in a further application of the MEUSec method to check whether the improvement suggestions from Step 8 have really led to an improvement.

(7.3) Feedback discussion and (7.4) Adjust heuristics: The feedback discussion was brief, as there were no problems with the heuristics and they did not need to be adjusted. As a result, Activity 7.4 was not required.

(7.5) Add own collection of heuristics to external collection of heuristics: This activity is part of the application when the software tool is fully developed and can be used to share the list of heuristics with other users. In this case, this activity can be seen as publishing the list of heuristics to Zenodo (see footnote 7) and making it available to interested parties.

Output of Step 7: Scores of UX and InfoSec aggregated.

5.8 Step 8: enhancement of UX and InfoSec

Input of Step 8: The interaction matrix defined in Step 6 (see Section 5.6) was used to collect improvement suggestions, as a different approach must be selected for each interaction property of the individual heuristics.

For conflicting heuristics, it must first be checked whether conflict solutions can be found. If not, either InfoSec or UX must be prioritised by using either the UX heuristic as a improvement suggestion or the InfoSec heuristic. The neutral and complementary heuristics serve directly as suggestions for improvement, as they do not influence each other negatively.

(8.1 and 8.2) Find solutions for conflicting heuristics and prioritize UX or InfoSec: As no conflicting heuristics have been identified in the interaction matrix, this activities could be skipped.

(8.3) Suggest improvements for the wallet based on complementary and neutral heuristics: Improvement suggestions could directly be derived for neutral and complementary heuristics, because they do not negatively affect each other. Therefore, the MU, ISE and UXE discussed the neutral and complementary heuristics to define improvement suggestions. A total of 26 improvement suggestions were collected and formulated in standardized form: ID, description and affected heuristics. Table 7 shows some improvement suggestions as examples. All improvement suggestions are available online (see footnote 7).

Output of Step 8: List of improvement suggestions.

Table 7: Example of improvement suggestions.

ID	Description	Affected heuristics
1	VC should have meaningful names and descriptions and these names should be used consistently across all screens.	01, 02
3	Function names should be consistent and understandable.	05
9	InfoSec hints should catch the user's eye and be easy to understand. A more detailed description with risks should be available. This also includes symbols used and explicit approval of InfoSec relevant actions. 'Anonymous issuer' warning must be emphasized. Symbol in the warning notice must be replaced, 'X' is confused with close.	11
14	Users should be made aware of the need for backups to prevent the loss of VC. The system should provide a backup function and a restore function.	17
20	Sensitive functions and data should only be accessible after successful authentication. Re-authentication after reopening the app. Protect transactions with additional authentication.	24
22	The app should offer different languages for users to choose from, also a 'Plain language' option.	26
23	The wallet should have a search, sort and filter function.	28
25	It should be possible to create, edit, group and delete different profiles. It should be possible to assign VC to different profiles. It should be possible to create self-issued VC in the profiles.	30
26	Security updates should be installed automatically. If no update has been carried out, the app should notify the user of the updates.	32

5.9 Discussion of the wallet evaluation results

By conducting the evaluation, certain insights have been gained that further enhance the study of the implications between UX and InfoSec, especially usable security. These strengths, weaknesses, as well as improvement suggestions have been presented to the Hidy developers after conducting the evaluation. The resulting documents are available to the developers and can be used for further development. As of writing, the wallet is a prototype that is still a work in progress.

The strengths and weaknesses of the Hidy wallet identified using the MEUSec method are now discussed and compared with those from the literature.

As Sartor et al.[12] show, the terminology used in their evaluated wallet is too technical and was not understood by test subjects. This weakness is linked to the design guideline "Use of understandable terms" by Sellung and Kubach[14] and was also identified by applying the MEUSec method to the Hidy wallet, e.g., as seen with terms like "credential" (see Section 5.4). This lack of understanding can lead to further problems, as users may struggle to perform basic tasks or misinterpret important features of the wallet. Furthermore, the technical terminology creates a barrier for less experienced users, reducing accessibility and potentially deterring adoption. It also raises security concerns, as users who do not fully understand key instructions are more likely to make mistakes. Ultimately, this undermines trust in the wallet and limits its target audience to highly technical users.

Sartor et al.[12] also found that the initial tutorial of their evaluated wallet was not helpful enough for users. In addition, Khayretdinova et al.[10] identified that test subjects faced challenges in setting up their evaluated wallet and managing their VC due to the wallet's complexity and lack of intuitive design. By applying the MEUSec method to the Hidy wallet, it was discovered that an introductory tutorial should be implemented in the Hidy wallet, related to the design guideline "User Onbording" by Sellung and Kubach.[14] The basic concept, functionalities and important tasks for users should be explained with the help of this tutorial at the first start of a wallet. In the past, basic functionality of wallets was not understood at all, like in the evaluation by Sauer et al.[21] and by Korir.[11]

In the evaluation of Sauer et al.[21] test subjects wanted more help hints in their evaluated wallet. This was also found in the evaluation of the Hidy wallet as there were no help hints and some elements like an "App Link" had no explanation at all, leaving test subjects wondering what its function was. This problem is tackled by the design guideline "Help and feedback" by Sellung and Kubach.[14] The guideline suggests using a clickable "i" or "?" that provides the user with additional information.

Sauer et al.[21] expressed that information can be hidden in a credential which is not shown to the user. This can happen in the Hidy wallet because the detail view does not show all stored information in the credential.

Like test subjects in the study of Satybaldy,[13] test subjects in the Hidy wallet evaluation experienced error messages that were not helpful. For example, an error message states "Creation failed" without telling the test subjects that the problem lies in the missing internet connection. Another error message stating "Sending failed" appeared after a successful purchase in the demo shop. The guideline "Error handling" by Sellung and Kubach[14] states that error messages should be explained to the user and give clear instructions on how to fix them.

More weaknesses found in the Hidy wallet are not represented in literature but conflict with other design guidelines from Sellung and Kubach.[14] The inconsistent naming of buttons and the use of different currencies in the demo shop and in the Hidy wallet conflict with the guideline "Use of consistent terms". Overlapping success messages and screens that are hard to distinguish because they are too similar violate the guideline "Simplicity of use". The guideline "Placement of information" requires that elements should be clearly recognized by the correct placement of text. This is not fulfilled, as added applications and credentials are only displayed using images and not their names. There are missing "back" buttons and keyboard fields that cannot be closed go against the "Operability" guideline, as these are not conform with user expectation. The "Home" screen does not meet users expectations and the demo shop interaction did not feel normal, as there was no receipt sent by e-mail and the resulting credential is not refundable and the deletion is irrevocable. This contradicts the guideline "Familiarity and Relatability" as this differs from experiences with other online shops and apps. In addition the detail view of a ticket credential did not offer additional meaningful information to the user.

While the Hidy wallet requires authentication every time the app is opened and the account balance is not directly revealed, the purchase history can be viewed directly, which should also be hidden by default. The guideline "Properly securing the wallet and functions" states that all sensitive data must be protected. The "Home" screen is perceived as clear, which is connected to the guideline "Minimalistic and simple design", but there are loading screens, which are not recognizable as such, because the loading bar at the top of the screen is barely visible. This confuses the user and interrupts the users focus on the important functions.

In addition to the strengths and weaknesses of wallets found in the literature and in addition to the related design guidelines from Sellung and Kubach,[14] the following strengths and weaknesses of wallets were identified by applying the MEUSec method.

A weakness of the Hidy wallet is that it fails to clearly communicate to users that the app offers additional features beyond the basic wallet functionality. Despite these additional features, the app is still primarily a wallet, but this distinction is not reflected in its name. As a result, users often search for their purchased tickets in the demo shop rather than the wallet, and they mistakenly try to download the demo shop from the application store, assuming that it is an external app.

Another weakness is that the wallet currently only offers the German language. Therefore, some test subjects had problems using the Hidy wallet because they could not understand German well enough.

A strength of the Hidy wallet is that test subjects found the wallet application on the home screen simply because of its name.

6 Method evaluation

In Section 6.1, the evaluation results regarding the MEUSec method based on the evaluation criteria from Section 4 are described. Afterwards, the methods evaluation results are discussed in Section 6.2. Moreover, suggestions for improving the MEUSec method – which resulted from the evaluation of the method – are explained in Section 6.3.

6.1 Method evaluation results

The method evaluation results are described below on the basis of the defined evaluation criteria (see Section 4).

6.1.1 Quality of the method results (E1)

Firstly, the evaluation results of (E1) the quality of the method results are described:

(E1.1) Completeness
For each defined wallet function, at least one UX and InfoSec heuristic could be created and the degree of fulfillment evaluated. Due to the high number of the created heuristics and the limited resources, the interaction matrix was not created for all heuristics, but only for those with the highest priority. All interaction properties could be evaluated for these heuristics. It is assumed that this would also have been possible for the remaining heuristics. At least one improvement suggestion could be found for each heuristic with a fulfillment degree below 100 % considering the effects on the other heuristics. The set of considered wallet functions had to be adapted during the evaluation, as some heuristics also affected functions that had not previously been considered.

(E1.2) Consistency
The MEUSec method provides a standardized way to evaluate the fulfillment of the heuristics and their interaction properties. During the evaluation, no contradictory improvements emerged. One problem the MU, ISE and UXE encountered during the evaluation was that the process lacks a baseline which can be consulted in order to justify a scoring in Step 7. When reading the ratings a second time, the estimation often changed, because other heuristics had to be put into relation. Some discovered weaknesses concerned all users, but others were only relevant for certain groups. The MEUSec method should somehow be able to incorporate this information.

(E1.3) Correctness
As the proposed heuristics express best practices gained from expert knowledge, the MU, ISE and UXE assume that they lead to a more secure and usable piece of software. They rate the method artifacts (e.g., defined heuristics, scores, interaction properties and final improvement suggestions) as correct. Additional statements regarding correctness cannot be made, because the method has only been applied once to the Hidy wallet. In a further application of the method, the UX and InfoSec scores would have to be used to check whether the improvement suggestions have actually led to an improvement.

(E1.4) Traceability
The scoring and estimation of the implications, the prioritisation of the heuristics and identified improvement suggestions are all traceable, as they result directly from the thought process of the ISE and UXE experts and get recorded by the MU. If there were any uncertainties, the different roles could discuss each decision among them.

(E1.5) Clarity
The heuristics, their respective fulfillment levels and their implications were clearly formulated, as the people that have created them are the same that need to understand and use them. This could be different if heuristics are taken from a catalogue that has been created by other people for different software systems. During this application of the MEUSec method, the fulfillment of the heuristics were clearly defined, as it was easy to see whether they were implemented or not. In Step 1, the ISE had difficulties defining security relevant components and an appropriate attacker model without in-depth knowledge about the system under evaluation. In Step 6, the MU was unaware of the interaction matrix being asymmetrical, during the initial creation of the interaction matrix. This was later fixed to incorporate both interactions per heuristic pair. Additionally, the meaning of the scores calculated in Step 7 was unclear to the MU. Since there is no baseline or defined goal for these scores, it was unclear how to rate the calculated values. Through discussion with the ISE and UXE it became clear that these scores can be used to measure relative performance after improvements have been made to the system under test.

(E1.6) Relevance
The UX and InfoSec scores could be used for comparison in the application of the MEUSec method, as they had been specifically gathered for this use case. The identified implications also sufficed for the formulation of improvement suggestions. The improvement suggestions were relevant and are expected to improve the identified UX and InfoSec weaknesses, as they directly follow from the heuristics, their scoring and their prioritization. The ISE and UXE assume that the scores could also be used in further iterations of the MEUSec method, to test if the suggestions lead to improvements, but a more thorough evaluation is needed to verify this claim.

6.1.2 Method feasibility (E2)

Now, the evaluation results of (E2) the method feasibility are described:

(E2.1) Effectiveness
In order to achieve effectiveness, UXE, ISE and MU discussed the degree of target achievement, i.e., the relationship between the actual MEUSec method results and the targets. The targets were to evaluate the UX and InfoSec, in particular their implications, of the Hidy wallet and to collect improvement suggestions based on this. A total of 41 weaknesses and 7 strengths of UX and InfoSec, 32 heuristics and 26 improvement suggestions were found. User-based and expert-based results were obtained, with which heuristics could be created. This made it possible to determine the fulfillment scores. Using the interaction matrix, corresponding improvement suggestions could be found for each UX and InfoSec weakness or heuristic, depending on the interaction properties. This means that the targets were achieved and therefore the UXE, ISE and MU rated the MEUSec method as effective.

(E2.2) Efficiency
To evaluate efficiency, the times required by UXE, ISE and MU for each step were measured: In total, UXE needs 1,365 min (22.75 h), ISE needs 1,265 min (21.08 h) and MU needs 1,206 min (20.1 h). The sum of the individual times of UXE, ISE and MU is therefore **3,836 min (63.93 h)**. The

Table 8: Required times in minutes.

Role	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8	Total
ISE	55	42	–	555	158	395	5	55	1,265
UXE	–	42	155	555	158	395	5	55	1,365
MU	75	122	170	555	158	25	46	55	1,206
Max(Step[x])	75	122	170	555	158	395	46	55	1,576
Total	130	206	325	1,665	474	815	56	165	3,836

total execution time of the MEUSec method (since roles are involved in steps in parallel) is **1,576 min (26.27 h)**. Moreover, the WU' times (included in Step 3) totalled 150 min (2.5 h).

In this measurement, only the time needed to execute the different steps in the MEUSec method is measured. Additional time and cost for training employees in using the MEUSec method, as well as actually implementing the resulting improvement suggestions is not included in these measurements.

The detailed times in minutes can be viewed in Table 8. The table row "Max(Step[x])" refers to the actual time for each step, as roles perform steps simultaneously. The table row "Total" means the times of the rolls added together, without taking parallel steps into account.

In addition, the costs were extrapolated, taking into account that the MU does not incur any costs. The following costs have been calculated: (a) UX designer or researcher: 83€/h,[11] (b) ISE: 101€/h[12] and (c) WU: 20€/user test.[13]

After multiplying the costs by the times, the total costs are 1,888.25€ for UXE, 2,129.08€ for ISE and 200€ for WU, which equates to a total cost of **4,217.33€**.

Furthermore, a general consensus was that the method could further benefit from extended templates that automate parts of the steps, e.g., a template that automatically calculates scores for UX and InfoSec (and their attributes) of all heuristics.

This would especially benefit the execution of Step 7, where the creation of the template by the MU took up a large portion of the time necessary to perform the step.

After considering the times, costs and benefits, the UXE, ISE and MU subjectively rated the MEUSec method as efficient. With the MEUSec method, evaluation results can be obtained from actual WU and experts, improvement suggestions, scores for comparing the results of further MEUSec method applications and several artefacts (heuristics, strengths, weaknesses) can be used in further MEUSec method applications that do not need to be repeated.

However, it was not entirely clear to the ISE how the definition of potential attackers and security relevant components in Step 1 should be carried out, which the MEUSec method still leaves open. This also applies to the MU when defining the WU and their properties in Step 2. In addition, the paper guide of Thinking aloud was created before the test cases are set up in Step 2. The paper guide had to be changed after the test cases were created.

(E2.3) Acceptance

UXE, ISE and MU expressed a high level of acceptance of the MEUSec method, especially because the MEUSec method has proven to be effective and efficient for them. Individual weaknesses have already been outlined in the evaluation results of the previous evaluation criteria. Furthermore, they added that some steps could be facilitated by a software tool: Creation of the interaction matrix with the heuristics, the aggregation of heuristic scores, definition of strengths, weaknesses, heuristics and MU properties using templates, visual representation of interaction properties of heuristics (e.g., conflicting heuristics) for finding improvement suggestions.

6.2 Discussion of the method evaluation results

Before developing the MEUSec method, Sauer et al.[32] conducted a systematic literature review to identify and compare existing procedures for evaluating the implications of UX and InfoSec. Some identified evaluation procedures (GOMS,[33] SecureUse score,[34] eye tracking[35] and questionnaires such as SUS,[36] UEQ,[37] UEQS[38] and AttrakDiff[39]) are pure UX evaluation procedures (without InfoSec scope) that can be applied to different software variants that differ in one security relevant parameter,[40–42] e.g., the authentication procedure. In this way, evaluation results about the implications of UX and InfoSec can be obtained. For example, a pure UX evaluation procedure is applied to a wallet with a 4-digit PIN and then to the (almost) same wallet with a 6-digit PIN. This makes it possible to evaluate the extent to which the UX changes when InfoSec is

[11] Average value of https://www.freelancermap.de (accessed on 08/23/2024).

[12] Average value of https://www.freelancermap.de (accessed on 08/23/2024).

[13] Costs are based on previous user tests.

increased. However, this makes evaluating the implications of UX and InfoSec time-consuming, as only one security relevant parameter of the software system under evaluation can be changed per iteration. During the application of the MEUSec method, the implications of UX and InfoSec can be evaluated by creating the interaction matrix in one step, when assigning the interaction properties rather than evaluating only one security relevant parameter of the whole system.

With a heuristic evaluation,[43] UX and InfoSec heuristics can be used to evaluate UX and InfoSec, but the implications between the heuristics and thus between UX and InfoSec are not evaluated. This is another advantage of the interaction matrix of the MEUSec method, as the implications between heuristics are evaluated.

Deriving heuristics and then formulating improvement suggestions based on the heuristics is more time and cost intensive than formulating improvement suggestions directly. However, this approach is more useful and effective as the heuristics can be used to determine a score for UX and InfoSec (and their attributes such as usability and integrity). The heuristics and the scores can then be reused in another application of the MEUSec method to check whether the improvement suggestions have really led to improvements (by comparing the new scores with the old scores).

Furthermore, the MEUSec method includes both an expert-based and user-based approach and not just one of the two, as the opinions of experts and users can differ.[44] Of course, time and costs can be saved by using solely a user-based evaluation or only an expert-based evaluation. However, the combination of both approaches increases the quality of the results. A user-based evaluation alone is not sufficient for the InfoSec evaluation, as the users only evaluate the user interface and not any in-depth security components. Only one of the evaluation methods identified by Sauer et al.[32] includes both experts and end users. However, this in turn requires the evaluation of different software variants that differ in a security parameter. The remaining methods identified by Sauer et al.[32] are either expert- or end-user-based and should therefore not be used alone, but in combination, as the opinions of experts and users can differ.[44] One evaluation procedure identified by Sauer et al.[32] that comes very close to a user- and expert-based approach is the heuristic walkthrough.[45] Heuristic walkthrough[45] first includes cognitive walkthrough[46] and then heuristic evaluation.[43] In cognitive walkthrough,[46] evaluators put themselves in the role of end users and test the software system using predefined tasks. This is followed by a free-form evaluation using a heuristic evaluation. The MEUSec method is based on the heuristic walkthrough, but the cognitive walkthrough has been replaced by Thinking aloud.[25] This has the advantage that actual end users are involved and not just evaluators who put themselves in the role of end users, as the opinions of experts and users can differ.[44]

The Thinking aloud method[25] – as a user-based approach in the MEUSec method – is in itself a pure UX evaluation procedure (without InfoSec scope). However, a previous evaluation[21] has shown that the Thinking aloud method can also be used to evaluate UX aspects that have an impact on InfoSec. For example, users have expressed that they want to have a confirmation popup in the wallet when security-critical actions are performed, such as storing VC from unverified issuers in the wallet. This makes Thinking aloud suitable for the user-based evaluation of the MEUSec method.

Nevertheless, when using the MEUSec method, there is a risk of abstracting problems that could affect specific contexts and user groups. For example, heuristics could be used that are too abstract so that specific problems are not found or specific user properties are not addressed, e.g., when a heuristic related to accessibility does not consider individuals with specific accessibility difficulties.

In the MEUSec method, own heuristics are first formulated on the basis of the user-based evaluation and then heuristics from other heuristics are added to the own heuristics if necessary. This is more time-consuming than using heuristics from other heuristics directly. However, this minimizes the risk that user-based evaluation results are not sufficiently considered. This order was therefore deliberately chosen when applying the MEUSec method.

6.3 Suggestions for improving the MEUSec method

Based on the evaluation results of the MEUSec method (Section 6.1) and the discussion (Section 6.2), some improvement suggestions became apparent. These are summarized below.

Improvement suggestion (1) emerged in Step 1, while security relevant components and potential attackers should be identified by the ISE. While there are widely-known and accepted ways to define attacker capabilities in cryptography like Dolev and Yao,[47] practical InfoSec is more fuzzy in this regard. The method could profit from a pre-selection of standardized attacker models with their respective capabilities, that can either be directly used by the ISE or adapted.

Improvement suggestion (2) came up when the MU was uncertain about what properties a WU constitutes. A template for these properties could help the MU to better understand these properties.

Improvement suggestion (3) concerns the paper guide of Thinking aloud: In its current form, the paper guide is static once the test cases have been set up. During our evaluation, it became clear that the paper guide must be adaptable, so it can be changed once again after the test cases have already been set up.

Improvement suggestion (4) came up during the creation of the heuristics. After the heuristics had been created, several of them were identified to share commonalities, so they could be easily summarized. This can be done in an additional reviewing step after the initial creation.

Improvement suggestion (5) is directly related to improvement suggestion 4, as the total number of heuristics greatly affects the time that is needed to create and fill out the interaction matrix. Besides summarizing, restrictions on the heuristics for the matrix could be made, for example by only taking heuristics with a poor degree of fulfillment into account.

Improvement suggestion (6) concerns the scoring in Step 7. After the initial scoring, the roles felt the need to once again talk about the scores, as heuristics that had been rated later on had an affect on heuristics rated earlier. This means that the scoring can not be seen as absolute, but rather as relative between the considered heuristics.

Improvement suggestion (7) is related to all steps of the method. Early on, the roles noticed that the process could greatly benefit from a template for documenting the method, so no information gets forgotten or is otherwise lost. This improvement could even be taken further, by having a software tool supporting the process.

Improvement suggestion (8) concerns the traceability of the decision making: While all roles could follow and agree on scores and the prioritisation, for archiving purposes or re-usage having a rationale on the taken decisions could help.

Improvement suggestion (9) is to move the feedback discussion (activity 7.3) and the adjustment of the heuristics (activity 7.4) so that they are performed after the activity of determining the fulfillment degree for each heuristic (activity 6.2). This means that any problems that occur with the heuristics can be rectified immediately. In addition, the feedback discussion and the adjustment of the heuristics should be combined, because during the feedback discussion only questions about the heuristics had to be clarified and the feedback discussion therefore did not require its own activity.

Improvement suggestion (10) is to combine the activities “test wallet functions” and “score heuristics” into one activity, i.e., to score the heuristics while testing the wallet functions. When evaluating the degree of fulfillment of the heuristics, UXE and ISE found that they had to test the wallet again and again because they could not remember exactly what happened when using the wallet in the previous activity.

Improvement suggestion (11) is to adjust the fulfillment score of the heuristics from 1–5 to 0–4. When calculating the scores in step 7, it became apparent that the calculated average score ratios were between 0.2 and 1, which does not match the scale normally expected of such scores.

Improvement suggestion (12) is to give the artifacts a changelog and allowing them to be adapted consistently with the other artifacts. Because during the implementation of the method, the already created artifacts had to be adjusted. This was not originally planned and should therefore be included.

7 Limitations

While the method evaluation contributed to the understanding of the MEUSec method and its feasibility, its setup carried some limitations to be discussed here.

First of all, it has to be mentioned that the experiments were carried out for the domain of Digital Identity Wallets. While we strongly believe that the approach can be transferred to other domains, further experiments on software systems from other application areas are needed to support this claim.

Second, the experiments were carried out by people that are proficient in their respective areas (UX and InfoSec), but neither of the people involved did know the implementation details of the wallet. For a thorough analysis, someone with deeper knowledge of the implementation details is needed, that knows about certain pitfalls and has invested more thought about the inner workings of the system. This especially holds true for the InfoSec part: InfoSec is a vast field and embraces organisational and high level concepts as well as technical deep dives. The quality of the InfoSec observation is therefore directly related to the information and time that is given to the ISE expert. It is impossible to make relevant statements about the security of parts of the system or the whole system, when documentation as well as source code are missing.

Third, the effectiveness of the improvement suggestions can only be evaluated in detail by applying the MEUSec method to the Hidy wallet a second time. The scores could then be used to check whether the improvement suggestions have actually led to improvements.

Fourth, there were no conflicts between heuristics found in this evaluation. As a result, the corresponding activities were not carried out and were therefore not evaluated. The lack of conflicts could be due to the individual creation of the heuristics and then selection of additional ones, or simply because conflicts are rare. In any case, this part requires further evaluation.

Fifth, no literature search was conducted, as the heuristics already covered the required functions. Therefore, this activity was not evaluated and should be part of future evaluations, particularly with regard to information on the targeted creation of search queries and limiting the scope.

The last limiting point regards the time needed for conducting all experiments. During conduction, the involved people decided to focus only on the relevant heuristics with a high priority, in order to complete the assessment. For a comprehensive observation of all heuristics, the needed time plays a crucial factor, as the task binds experts that could be needed otherwise.

8 Conclusion and future work

Existing wallets have significant UX and InfoSec weaknesses. In order to increase UX and InfoSec to an adequate level, both aspects must be taken into account, as they can influence each other.

This article contains two key contributions: On the one hand, the MEUSec method was applied to the Hidy wallet to evaluate the UX and InfoSec and to identify improvement suggestions. On the other hand, the MEUSec method was evaluated through the application and on the basis of various evaluation criteria, i.e., essentially the feasibility of the method and the quality of the method results.

By applying the MEUSec method to the Hidy wallet, a total of 41 weaknesses and 7 strengths of UX and InfoSec were identified and 32 UX and InfoSec heuristics were derived. Based on this, 26 improvement suggestions for the Hidy wallet were collected.

With regard to the evaluation of the MEUSec method itself, it was rated positively with regard to the defined evaluation criteria of feasibility and quality of results. Another evaluation conducted by different experts could further strengthen this rating, as different people tend to rate the relevance of heuristics differently. Nevertheless, a few improvement suggestions were identified based on the evaluation results.

In the future, the collected improvement suggestions for the MEUSec method will be incorporated into the MEUSec method. A software tool will then be developed to support the execution of the MEUSec method. This should improve the feasibility of the MEUSec method and the quality of the method results, especially with regard to efficiency. For example, the software tool offers a structured external collection of heuristics to choose from and can automatically create an interaction matrix of the defined heuristics so that it no longer has to be done manually. In addition, the scores of UX and InfoSec can be calculated automatically by aggregating the corresponding scores of the heuristics using the software tool. The software tool and the MEUSec method will be applied again to a wallet in order to re-evaluate them, in particular to compare the new evaluation results with the evaluation results obtained so far. This will make it possible to evaluate what works better with the software tool and what does not. In addition, the MEUSec method will be applied to a software system other than wallets in order to evaluate its adaptability. At this stage, it is conceivable that this could work without major adjustments.

Acknowledgments: We would also like to thank University of Applied Sciences Mittweida for providing us with the Hidy Wallet and its documentation.
Research ethics: Not applicable.
Informed consent: Informed consent was obtained from all individuals included in this study, or their legal guardians or wards.
Author contributions: All authors have accepted responsibility for the entire content of this manuscript and approved its submission.
Use of Large Language Models, AI and Machine Learning Tools: None declared.
Conflict of interest: The authors state no conflict of interest.
Research funding: The content of this paper is a result of the project Showcase Secure Digital Identities Karlsruhe (SDIKA, grant 01MN21004B). This Project is supported by the Federal Ministry for Economic Affairs and Climate Action (BMWK) on the basis of a decision by the German Bundestag.
Data availability: The raw data can be obtained on request from the corresponding author.

References

1. ISO, D. E. DIN EN ISO 24760-1:2022-03. IT Security and Privacy — A Framework for Identity Management — Part 1: Terminology and Concepts. **2022**.
2. Grassi, P. A.; Garcia, M. E.; Fenton, J. L. Digital Identity Guidelines: Revision 3. Tech. Rep. NIST SP 800-63-3; National Institute of Standards and Technology: Gaithersburg, MD, 2017.
3. Preukschat, A.; Reed, D. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*; Manning: Shelter Island, 2021.
4. Podgorelec, B.; Alber, L.; Zefferer, T. What is a (Digital) Identity Wallet? A Systematic Literature Review. In *Proceedings of the 46th Annual Computers, Software, and Applications Conference (COMPSAC '22)*; IEEE: Los Alamitos, CA, USA, 2022; pp. 809—818.

5. Parliament, E. Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. *Regulation* **2024**.
6. ISO, D. E. DIN EN ISO 9241-210:2020-03. Ergonomics of Human-System Interaction — Part 210: Human-Centred Design for Interactive Systems (ISO_9241-210:2020). **2020**.
7. Morville, P. Experience Design Unplugged. In *Proceedings of the 32nd Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH '05)*; ACM Press: Los Angeles, California, 2005; p. 10.
8. Morville, P.; Sullenger, P. Ambient Findability: Libraries, Serials, and the Internet of Things. *Ser. Libr.* **2010**, *58* (1–4), 33–38.
9. Nieles, M.; Dempsey, K.; Pillitteri, V. Y. NIST Special Publication 800-12: An Introduction to Information Security. **2017**.
10. Khayretdinova, A.; Kubach, M.; Sellung, R.; Rossnagel, H. Conducting a Usability Evaluation of Decentralized Identity Management Solutions. In *Selbstbestimmung, Privatheit und Datenschutz*; Friedewald, M., Kreutzer, M., Hansen, M., Eds.; Springer Fachmedien Wiesbaden: Wiesbaden, 2022; pp. 389–406.
11. Korir, M.; Parkin, S.; Dunphy, P. An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control. In *Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022; pp. 195–211.
12. Sartor, S.; Sedlmeir, J.; Rieger, A.; Roth, T. Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets. In *Proceedings of the 30th European Conference on Information Systems (ECIS 2022)*, 2022.
13. Satybaldy, A. Usability Evaluation of SSI Digital Wallets. In *Privacy and Identity Management*; Bieker, F., Meyer, J., Pape, S., Schiering, I., Weich, A., Eds.; Springer Nature Switzerland: Cham, Vol. *671*, 2023; pp. 101–117.
14. Sellung, R.; Kubach, M. Research on User Experience for Digital Identity Wallets: State-of-the-Art and Recommendations. In *Open Identity Summit 2023*, 2023.
15. Distler, V.; Lenzini, G.; Lallemand, C.; Koenig, V. The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. In *New Security Paradigms Workshop (NSPW '20)*; ACM: Online USA, 2020; pp. 45–58.
16. Whitten, A.; Tygar, J. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium*: Washington, D.C., 1999.
17. Sauer, M.; Becker, C.; Oberweis, A.; Pfeifer, S.; Sürmeli, J. MEUSec — Method for Enhancing User Experience and Information Security. In *Advances in Mobile Computing and Multimedia Intelligence*; Delir Haghighi, P., Fedushko, S., Kotsis, G., Khalil, I., Eds.; Springer Nature Switzerland: Cham, Vol. *15341*, 2025; pp. 39–53.
18. Yáñez Gómez, R.; Cascado Caballero, D.; Sevillano, J.-L. Heuristic Evaluation on Mobile Interfaces: A New Checklist. *Sci. World J.* **2014**, *2014*, 1–19.
19. Nielsen, J. Enhancing the Explanatory Power of Usability Heuristics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '94)*; ACM Press: Boston, Massachusetts, United States, 1994; pp. 152–158.
20. Realpe, P. C.; Collazos, C. A.; Hurtado, J.; Granollers, A. A Set of Heuristics for Usable Security and User Authentication. In *Proceedings of the 17th International Conference on Human Computer Interaction*; ACM: Salamanca Spain, 2016; pp. 1–8.
21. Sauer, M.; Becker, C.; Oberweis, A.; Pfeifer, S.; Stark, A.; Sürmeli, J. User Experience and Information Security Implications of Digital Identity Wallets. In *Proceedings of the 14th International Conference on Information Communication and Management (ICICM '24)*, 2025.
22. Reese, K.; Trevor, S.; Dutson, J.; Armknecht, J.; Cameron, J.; Seamons, K. A Usability Study of Five Two-Factor Authentication Methods. In *Proceedings of the 15th Symposium on Usable Privacy and Security*, 2019.
23. Hinds, C.; Ekwueme, C. Increasing Security and Usability of Computer Systems with Graphical Passwords. In *Proceedings of the 45th Annual Southeast Regional Conference (ACMSE '07)*; ACM: Winston-Salem, North Carolina, 2007; pp. 529–530.
24. Zhang, L.; Guo, Y.; Guo, X.; Shao, X. Does the Layout of the Android Unlock Pattern Affect the Security and Usability of the Password? *J. Inf. Secur. Appl.* **2021**, *62*, 103011. .
25. Nielsen, J. *Usability Engineering*; Academic Press: Boston, 1993.
26. Sauer, M.; Becker, C.; Oberweis, A.; Schork, S.; Sürmeli, J. User Experience and Information Security Heuristics for Digital Identity Wallets. In *Proceedings of the 8th International Conference on Computer-Human Interaction Research and Applications (CHIRA '24)*, 2025.
27. Nechansky, H. The Interaction Matrix: from Individual Goal-Setting to the Four Modes of Coexistence. *J. Kybernetes* **2016**, *45*, 87–106.
28. Al-subaie, H. S.; Maibaum, T. S. Evaluating the Effectiveness of a Goal-Oriented Requirements Engineering Method. In *Proceedings of the 4th International Workshop on Comparative Evaluation in Requirements Engineering (CERE '06)*; IEEE: Minneapolis, MN, 2006; pp. 8–19.
29. Kromrey, H. Evaluation — ein vielschichtiges Konzept. Begriff und Methodik von Evaluierung und Evaluationsforschung. Empfehlungen für die Praxis. *Soz. Ber.* **2001**, *24*, 105–131.
30. Krauss, A.-M.; Sellung, R. A.; Kostic, S. Ist das die Wallet der Zukunft? Ein Blick durch die Nutzendenbrille beim Einsatz von digitalen Identitäten. *HMD Prax. Wirtsch.* **2023**, *60* (2), 344–365.
31. Nielsen, J.; Landauer, T. K. A Mathematical Model of the Finding of Usability Problems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '93)*; ACM Press: Amsterdam, The Netherlands, 1993; pp. 206–213.
32. Sauer, M.; Alpers, S.; Becker, C. Comparison of Methods for Analyzing the Correlation of User Experience and Information Security. In *Proceedings of the 5th International Conference on Software Engineering and Development (ICSED '23)*; ACM: Singapore, 2024; pp. 8–16.
33. John, B.; Kieras, D. The GOMS Family of User Interface Analysis Techniques: Comparison and Contrast. *J. ACM Trans. Comput. Hum. Interact.* **1996**, *3*, 320–351.
34. Dutta, S.; Madnick, S.; Joyce, G. SecureUse: Balancing Security and Usability within System Design. In *Proceedings of the 18th international Conference on Human-Computer Interaction*; Stephanidis, C., Ed. Communications in Computer and Information Science; Springer International Publishing: Cham, 2016; pp. 471–475.

35. Bojko, A. Eye Tracking in User Experience Testing: How to Make the Most of it. In *Proceedings of the 14th Annual Conference of the Usability Professionals' Association (UPA)*, 2005.
36. Brooke, J. SUS: A Quick and Dirty Usability Scale. In *Usability Evaluation in Industry*Jordan, P. W., Thomas, B., Weerdmeester, B. A., McClelland, A. L., Hrsg.; 1996; CRC Press: UK, S. 189–194.
37. Laugwitz, B.; Held, T.; Schrepp, M. Construction and Evaluation of a User Experience Questionnaire. In *HCI and Usability for Education and Work*; Springer Berlin Heidelberg, Vol. *5298*, 2008; pp. 63–76. Series Title: Lecture Notes in Computer Science.
38. Schrepp, M.; Hinderks, A.; Thomaschewski, J. Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S). *Int. J. Interact. Multimed. Artif. Intell.* **2017**, *4*, 103.
39. Hassenzahl, M.; Burmester, M.; Koller, F. AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität. In *Mensch & Computer 2003*; Vieweg+Teubner Verlag: Wiesbaden, Vol. *57*, 2003; pp. 187–196. Series Title: Berichte des German Chapter of the ACM.
40. Darwish, A.; Bataineh, E. Eye Tracking Analysis of Browser Security Indicators. In *Proceedings of the International Conference on Computer Systems and Industrial Informatics 2012*; IEEE: Sharjah, United Arab Emirates, 2012; pp. 1–6.
41. Kwon, T.; Shin, S.; Na, S. Covert Attentional Shoulder Surfing: Human Adversaries are More Powerful than Expected. *IEEE Trans. Syst. Man Cybern. Syst.* **2014**, *44* (6), 716–727.
42. Marky, K.; Zollinger, M.-L.; Roenne, P.; Ryan, P. Y. A.; Grube, T.; Kunze, K. Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes. *ACM Trans. Comput.-Hum. Interact.* **2021**, *28* (5), 1–36.
43. Nielsen, J.; Molich, R. Heuristic Evaluation of User Interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '90)*; ACM Press: Seattle, Washington, United States, 1990; pp. 249–256.
44. Jaspers, M. W. A Comparison of Usability Methods for Testing Interactive Health Technologies: Methodological Aspects and Empirical Evidence. *Int. J. Med. Inform.* **2009**, *78*, 340–353.
45. Sears, A. Heuristic Walkthroughs: Finding the Problems Without the Noise. *Int. J. Hum.-Comput. Interact.* **1997**, *9* (3), 213–234.
46. Wharton, C.; Rieman, J.; Lewis, C.; Polson, P. The Cognitive Walkthrough Method: A Practitioner's Guide. In *Usability Inspection Methods*; John Wiley & Sons, Inc.: USA, 1994; pp. 105–140.
47. Dolev, D.; Yao, A. C. On the Security of Public Key Protocols. *J. IEEE Trans. Inf. Theory* **1983**, *29*, 198–208.