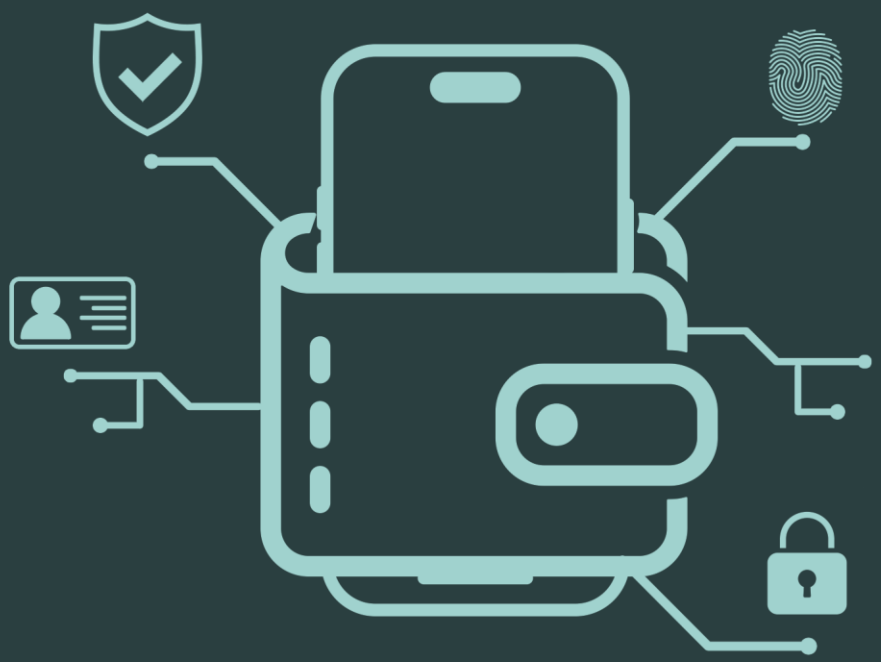
User Experience und Informationssicherheit beim Einsatz von Digital Identity Wallets



Max Sauer

User Experience und Informations-sicherheit beim Einsatz von Digital Identity Wallets

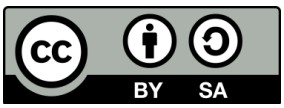
von Max Sauer

Dissertation, genehmigt von der KIT-Fakultät für Wirtschaftswissenschaften des Karlsruher Instituts für Technologie (KIT)

Tag der mündlichen Prüfung: 11. Dezember 2025
Hauptreferent: Prof. Dr. Andreas Oberweis
Korreferentin: Prof. Dr. Simone Braun

Impressum

Autor: Max Sauer
Covergrafik: Acelya Soylu – https://buchcoverdesign.online
Stand: 26.01.2026



DOI: 10.5445/IR/1000189330

User Experience und Informationssicherheit beim Einsatz von Digital Identity Wallets

Zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften
(Dr.-Ing.)

von der KIT-Fakultät für Wirtschaftswissenschaften
des Karlsruher Instituts für Technologie (KIT)

genehmigte

DISSERTATION

von

Max Sauer, M.Sc.

Tag der mündlichen Prüfung: 11. Dezember 2025
Hauptreferent: Prof. Dr. Andreas Oberweis
Korreferentin: Prof. Dr. Simone Braun

Karlsruhe

Genderhinweis

Aus Gründen der besseren Lesbarkeit wird in dieser Arbeit das generische Maskulinum verwendet und auf eine geschlechtsneutrale Formulierung verzichtet. Nachfolgende männliche Schreibweisen beziehen sich immer auf alle Geschlechter.

Danksagung

Diese Arbeit entstand während meiner Zeit als wissenschaftlicher Mitarbeiter am FZI Forschungszentrum Informatik (FZI) im Forschungsbereich Software Engineering.

Die Vollendung dieser Dissertation markiert einen wichtigen Meilenstein in meinem Leben. Auf diesem Weg durch die Welt der Forschung und des Wissens wurde ich von zahlreichen Menschen begleitet, die meine Reise auf vielfältige Weise bereichert haben.

In erster Linie möchte ich meinen Dank und meine aufrichtige Wertschätzung meinem Doktorvater Prof. Dr. Andreas Oberweis aussprechen. Ihre fachliche Expertise und Ihr Engagement haben meine (akademische) Entwicklung maßgeblich beeinflusst.

Ich bedanke mich außerdem bei Prof. Dr. Simone Braun für die Erstellung des Zweitgutachtens. Durch die damalige Betreuung meiner Masterarbeit an der Hochschule Offenburg hast du mir nicht nur geholfen, meine wissenschaftlichen Fähigkeiten weiterzuentwickeln, sondern mich auch auf das FZI aufmerksam gemacht. Diese Gelegenheit hat meine akademische Laufbahn entscheidend geprägt, wofür ich dir sehr dankbar bin.

Danken möchte ich auch Prof. Dr. Melanie Volkamer für die Teilnahme an der Prüfung und Prof. Dr. Stefan Nickel für die Übernahme des Prüfungsvorsitzes.

Ein besonderer Dank gilt Prof. Dr. Jan Sürmeli. Deine engagierte Betreuung und deine Impulse haben maßgeblich zum Erfolg meiner Arbeit beigetragen. Zudem hat mich dein inspirierender und empathischer Umgang mit Menschen schon immer sehr beeindruckt. Ebenso spreche ich meinen Dank an Prof. Dr. Sascha Alpers aus. Du hast mir während meiner Anfangszeit am FZI einen tieferen Einblick in die Wissenschaft vermittelt und mich in den ersten Schritten meines Promotionsvorhabens begleitet.

Mein Dank gilt zudem meinen Kollegen des FZI und der Forschungsgruppe Betriebliche Informationssysteme am Institut für Angewandte Informatik und Formale Beschreibungsverfahren des Karlsruher Instituts für Technologie (KIT). Die gute Zusammenarbeit und die produktiven Diskussionen haben meine Forschung bereichert. Vor allem möchte ich meine Kollegen Christoph Becker, Marius Take, Lukas Kneis, Thomas Mayer, Akim Stark, Judith Junker und Alexander Dregger betonen.

Außerdem bedanke ich mich bei allen studentischen Abschlussarbeitern und Hilfskräften, die mich bei einigen Aufgaben während meines Promotionsvorhabens unterstützt haben. Hierbei hervorheben möchte ich Simon Pfeifer und Sabine Schork.

Ferner bedanke ich mich bei den Mitgliedern der sogenannten Nutzerakzeptanz-Arbeitsgruppe, die verschiedene Experten der Nutzerakzeptanz aus den Forschungsprojekten SDIKA, ID-Union, ID-Ideal und ONCE vereint. Die zahlreichen Diskussionen haben das Thema stark vorangetrieben. Hierbei besonders betonen möchte ich Anna-Magdalena Krauß von der Hochschule für Technik und Wirtschaft Dresden, Sandra Kostic vom Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC) und Rachelle Sellung vom Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO).

Vor allem möchte ich aber auch meiner Familie und meiner Frau von Herzen danken. Euer Glaube an meine Fähigkeiten hat mir in schwierigen Momenten Rückhalt gegeben.

Die Erstellung dieser Arbeit war ein aufregendes Abenteuer, das ohne die genannten Personen nicht möglich gewesen wäre. Vielen Dank an alle, die an meinem Weg teilgenommen haben. Die Zukunft hält zweifellos weitere Herausforderungen, Entdeckungen sowie Abenteuer bereit und ich bin zuversichtlich, dass sie noch viele aufregende Möglichkeiten bieten wird.

Karlsruhe, im Januar 2026 Max Sauer

Kurzfassung

Digital Identity Wallets (kurz Wallets) sind das digitale Pendant zu physischen Brieftaschen. Sie ermöglichen es, sämtliche digitale Nachweise in einer einzigen digitalen Applikation zu speichern, zu verwalten und daraus selbstbestimmt zu teilen. Beispielsweise können Benutzer ihren digitalen Studierendennachweis in der Wallet speichern und mit Online-Shops teilen, um von vergünstigten Angeboten zu profitieren.

Untersuchungen zeigen, dass Wallets mehrere Schwächen der User Experience (kurz UX) und Informationssicherheit besitzen. Beispielsweise wird die grundlegende Funktionsweise von Wallets nicht verstanden, was dazu führen kann, dass sensible Daten ungewollt geteilt werden. Die Schwächen von Wallets sind besonders problematisch, da jeder Mitgliedsstaat der Europäischen Union bis Ende 2026 seinen Bürgern eine solche Wallet zur Verfügung stellen muss. Eine gleichzeitige Verbesserung von UX und Informationssicherheit ist herausfordernd, da sich beide Aspekte gegenseitig negativ oder positiv beeinflussen können. Beispielsweise können komplexe Sicherheitsmechanismen zu einer Verschlechterung der UX führen. Deshalb sollten UX und Informationssicherheit von Wallets gemeinsam evaluiert und auf ein ausreichendes Niveau verbessert werden.

Die vorliegende Arbeit beschäftigt sich mit der Entwicklung von Methoden und Werkzeugen zur Evaluation und Verbesserung der UX und der Informationssicherheit von Wallets. Zunächst wurden bestehende Verfahren zur Evaluation des Zusammenhangs zwischen UX und Informationssicherheit recherchiert und miteinander verglichen. Danach wurden einige dieser Evaluationsverfahren auf einen Wallet-Prototyp angewendet, um Erkenntnisse über die Evaluationsverfahren und die Wallet zu gewinnen. Darauf aufbauend wurden Qualitätsrichtlinien der UX und Informationssicherheit (sogenannte Heuristiken) für Wallets erarbeitet und ein eigenes Evaluationsverfahren entwickelt – die MEUSec-Methode. Mit der MEUSec-Methode lassen sich UX und Informationssicherheit von Wallets evaluieren und Verbesserungsvorschläge finden, insbesondere unter Berücksichtigung der Implikationen von UX und Informationssicherheit.

Die MEUSec-Methode wurde exemplarisch auf die Hidy-Wallet angewendet, um einerseits die Hidy-Wallet und andererseits die Methode zu evaluieren. Auf Basis der Evaluationsergebnisse wurde die Methode verbessert und es wurde ein Software-Tool zur Unterstützung der Anwendung der Methode entwickelt. Danach wurde die Methode mithilfe des Software-Tools auf die Lissi-Wallet angewendet. So konnten die Lissi-Wallet, die Methode und das Software-Tool evaluiert werden. Abschließend wurden die Methode und das Software-Tool erneut auf Basis der Evaluationsergebnisse verbessert.

Inhaltsverzeichnis

Kurzfassung ..... **v**

Abbildungsverzeichnis ..... **xi**

Tabellenverzeichnis ..... **xiii**

Definitionsverzeichnis ..... **xv**

Abkürzungsverzeichnis ..... **xvii**

1 Einleitung **1**
1.1 Motivation und Problemstellung 1
1.2 Zielsetzung und Beiträge der Arbeit 4
1.3 Aufbau der Arbeit 6

2 Grundlagen: Digital Identity Wallets **11**
2.1 Digitale Identität 11
2.2 Verifizierbarer digitaler Nachweis 15
2.3 Rollen und Anforderungen 19
2.4 Funktionalität von Wallets 20
2.5 Technologien und Standards 23

3 Grundlagen: User Experience **27**
3.1 Definition 27
3.2 Usability 30
3.3 Human-Centered Design 32
3.4 Dark Patterns 36

4 Grundlagen: Informationssicherheit **39**
4.1 Definition und Schutzziele 39
4.2 Schwachstelle, Bedrohung, Angriff und Risiko 41
4.3 Security Engineering 42
4.3.1 Strukturanalyse 43
4.3.2 Schutzbedarfsermittlung 44
4.3.3 Bedrohungsanalyse 45
4.3.4 Risikoanalyse 45

5 Evaluation von User Experience und Informationssicherheit **47**
5.1 Zusammenhang zwischen User Experience und Informationssicherheit 47
5.2 Diskussion von Evaluationsverfahren 50
5.2.1 SecureUse Score 53

5.2.2 Heuristische Evaluation und Heuristiken 54
5.2.3 Security Usability Symmetry 57
5.2.4 Cognitive Walkthrough 58
5.2.5 Heuristic Walkthrough 59
5.2.6 Verfahren nach Gonzalez u. a. 60
5.2.7 Verfahren nach Alarifi u. a. 60
5.2.8 Thinking aloud 61
5.2.9 GOMS 62
5.2.10 Diary Study 64
5.2.11 Fokusgruppen 64
5.2.12 Eye Tracking 65
5.2.13 Fragebögen 66
5.2.14 Gegenüberstellung und Diskussion 67
5.3 Durchführung einer Evaluation der User Experience und Informationssicherheit von Wallets 70
5.3.1 Ausgangslage und verwandte Arbeiten 70
5.3.2 Durchführung der Evaluation 72
5.4 Ableitung von User Experience- und Informationssicherheit-Heuristiken für Wallets 83

6 MEUSec-Methode 93
6.1 Beschreibung der Methode 93
6.1.1 Allgemeines 94
6.1.2 Vorgehensmodell 95
6.2 Entwicklung und Entwurfsentscheidungen der Methode 107
6.3 Beschränkungen und Voraussetzungen der Methode 111
6.4 Einordnung der Methode 112

7 Evaluation der ersten Version der MEUSec-Methode 115
7.1 Vorgehensweise 116
7.2 Evaluationsergebnisse der Hidy-Wallet 119
7.3 Einordnung der Stärken und Schwächen der Hidy-Wallet 132
7.4 Evaluationsergebnisse der MEUSec-Methode 135
7.5 Limitationen 141

8 Software-Tool 143
8.1 Vorgehensweise der Entwicklung 144
8.2 Anforderungserhebung 146
8.3 Entwurf 149
8.4 Funktionsbeschreibung 155

9 Evaluation der zweiten Version der MEUSec-Methode und der ersten Version des Software-Tools 161
9.1 Vorgehensweise 162
9.2 Evaluationsergebnisse der Lissi-Wallet 165
9.3 Einordnung der Stärken und Schwächen der Lissi-Wallet 182
9.4 Evaluationsergebnisse der MEUSec-Methode 184
9.5 Evaluationsergebnisse des Software-Tools 188
9.6 Limitationen 195
9.7 Vergleich und Diskussion der Evaluationsergebnisse 196

10 Fazit und Ausblick 199
10.1 Fazit 199
10.2 Ausblick 201

Literaturverzeichnis 205

Abbildungsverzeichnis

Abbildung 1: Aufbau der Arbeit 9
Abbildung 2: Aussteller, Inhaber und Prüfer von VC 17
Abbildung 3: Ausstellung, Speicherung und Präsentation von VC 18
Abbildung 4: Ausstellung, Speicherung, Präsentation und Widerruf von VC 18
Abbildung 5: DID, VC und VDR 25
Abbildung 6: UX-Attribute 29
Abbildung 7: UX- und Usability-Attribute 32
Abbildung 8: Human-Centered Design 35
Abbildung 9: Beispiele von Dark Patterns 38
Abbildung 10: Schwachstelle, Bedrohung, Risiko und Angriff 42
Abbildung 11: Beispiel eines Netztopologieplans 43
Abbildung 12: Beispiel eines Bedrohungsbaums mit Risiken 46
Abbildung 13: Ergebnisse der systematischen Literaturrecherche 52
Abbildung 14: Beispiel für ein Tornado-Chart 54
Abbildung 15: Ablauf einer exemplarischen Nutzung des Software-Prototyps 73
Abbildung 16: SUS-Wert je Prototyp-Variante 75
Abbildung 17: SUS-Gesamtwert des Prototyps je Altersgruppe 75
Abbildung 18: UEQ-S-Wert je Prototyp-Variante 76
Abbildung 19: UEQ-S-Gesamtwert des Prototyps je Altersgruppe 76
Abbildung 20: Login-Zeiten 77
Abbildung 21: Stadtmobil-Konto – Ergebnisse des Eye Tracking 78
Abbildung 22: VC-Speicherung – Ergebnisse des Eye Tracking 79
Abbildung 23: Entwicklungsschritte der MEUSec-Methode 93
Abbildung 24: 8 Schritte der MEUSec-Methode 96
Abbildung 25: Schritt 1 der MEUSec-Methode 98
Abbildung 26: Schritt 2 bis 4 der MEUSec-Methode 101
Abbildung 27: Schritt 5 bis 7 der MEUSec-Methode 105
Abbildung 28: Schritt 8 der MEUSec-Methode 106
Abbildung 29: Vorgehensweise der Entwicklung des Software-Tools 146

Abbildung 30: Architekturmodell des Software-Tools 151
Abbildung 31: Entity-Relationship-Modell des Software-Tools 154
Abbildung 32: Software-Tool – Schieberegler-Funktion 158
Abbildung 33: Entwicklungsprozess von MEUSec-Methode und Software-Tool 161

Tabellenverzeichnis

Tabelle 1: Modelle zur Verwaltung digitaler Identitäten 15
Tabelle 2: Vergleich von Wallet-Arten 23
Tabelle 3: Schutzbedarfskategorien 44
Tabelle 4: Evaluationsverfahren kategorisiert nach Art der Evaluierenden 67
Tabelle 5: Evaluationsverfahren kategorisiert nach Usability/UX 69
Tabelle 6: Korrelationsphase – Beispiel der UX-Heuristiken 86
Tabelle 7: Korrelationsphase – Beispiel der Informationssicherheit-Heuristiken 86
Tabelle 8: Evaluation der Verständlichkeit der initialen Heuristiken 88
Tabelle 9: Beispiel einer entwickelten UX-Heuristik 89
Tabelle 10: Beispiel einer entwickelten Informationssicherheit-Heuristik 90
Tabelle 11: Ergebnisse der heuristischen Evaluation der Versuchsgruppe 91
Tabelle 12: Ergebnisse der heuristischen Evaluation der Kontrollgruppe 92
Tabelle 13: Beispiel einer Interaktionsmatrix 103
Tabelle 14: Begründungen der MEUSec-Methode 110
Tabelle 15: Hidy-Wallet – Demografische Daten der Probanden 121
Tabelle 16: Hidy-Wallet – Beispiel einer Informationssicherheit-Schwäche 123
Tabelle 17: Hidy-Wallet – Beispiel einer UX-Schwäche 124
Tabelle 18: Hidy-Wallet – Beispiel einer UX-Heuristik 125
Tabelle 19: Hidy-Wallet – Beispiel einer Informationssicherheit-Heuristik 125
Tabelle 20: Hidy-Wallet – Ausschnitt der Interaktionsmatrix 128
Tabelle 21: Hidy-Wallet – Scores der UX-Attribute 129
Tabelle 22: Hidy-Wallet – Scores der Informationssicherheit-Attribute 130
Tabelle 23: Hidy-Wallet – Ausschnitt der Verbesserungsvorschläge 132
Tabelle 24: Hidy-Wallet – Ausführungszeiten der MEUSec-Methode 139
Tabelle 25: Lissi-Wallet – Bedrohungsszenarien 168
Tabelle 26: Lissi-Wallet – Testfälle der Wallet 170
Tabelle 27: Lissi-Wallet – Demografische Daten der Probanden 171
Tabelle 28: Lissi-Wallet – Beispiel einer Informationssicherheit-Schwäche 173
Tabelle 29: Lissi-Wallet – Beispiel einer UX-Schwäche 173
Tabelle 30: Lissi-Wallet – Beispiel einer Informationssicherheit-Heuristik 174

Tabelle 31: Lissi-Wallet – Beispiel einer UX-Heuristik 175
Tabelle 32: Lissi-Wallet – Ausschnitt der Interaktionsmatrix 178
Tabelle 33: Lissi-Wallet – Scores der UX-Attribute.....179
Tabelle 34: Lissi-Wallet – Scores der Informationssicherheit-Attribute.....179
Tabelle 35: Lissi-Wallet – Ausschnitt der Verbesserungsvorschläge 181
Tabelle 36: Lissi-Wallet – Ausführungszeiten der MEUSec-Methode.....186

Definitionsverzeichnis

Definition 2-1: Digitale Identität 12
Definition 2-2: VC 16
Definition 2-3: Wallet 21
Definition 3-1: UX 29
Definition 3-2: Usability 32
Definition 3-3: Dark Patterns 37
Definition 4-1: Informationssicherheit 40
Definition 5-1: Heuristik der UX oder Informationssicherheit 55

Abkürzungsverzeichnis

DID	Decentralized Identifier
eID	Elektronische Identität
ER-Modell	Entity-Relationship-Modell
HCD	Human-Centered Design
HCI	Human-Computer Interaction
JSON-LD	JSON for Linked Data
KI	Künstliche Intelligenz
VC	Verifiable Credential
VDR	Verifiable Data Registry
VP	Verifiable Presentation

1 Einleitung

Im ersten Kapitel werden zunächst die Motivation und Problemstellung in Abschnitt 1.1 verdeutlicht. Danach werden die Zielsetzung und die Beiträge der Arbeit in Abschnitt 1.2 erläutert. Anschließend wird der Aufbau der Arbeit in Abschnitt 1.3 beschrieben.

1.1 Motivation und Problemstellung

Die fortschreitende Digitalisierung wirkt sich auf nahezu alle Lebensbereiche aus und verändert die Art und Weise, wie Menschen miteinander interagieren, ihren Alltag gestalten und unterschiedliche Dienstleistungen nutzen. Von Online-Überweisungen, über Beantragungen amtlicher Dokumente, bis hin zum Online-Dating – all dies kann schnell und bequem über ein mobiles Endgerät erfolgen. Allerdings erfordert die Digitalisierung sichere und benutzerfreundliche Lösungen, um sich digital eindeutig und verlässlich identifizieren zu können.

In der physischen Welt erfolgt die Identifizierung durch physische Nachweise, wie Personalausweise, Führerscheine oder Bankkarten, die häufig in einer physischen Brieftasche aufbewahrt werden. Im digitalen Raum ist eine vergleichsbare Lösung notwendig, die es Benutzern ermöglicht, digitale Nachweise sicher und benutzerfreundlich zu verwalten. Eine *Digital Identity Wallet* (Anke und Richter, 2023; Podgorelec u. a., 2022) – nachfolgend *Wallet* genannt – stellt das digitale Pendant zur physischen Brieftasche dar. Anstatt eine Vielzahl an Nachweisen in einer physischen Brieftasche aufbewahren zu müssen, lassen sich digitale Nachweise an einer Stelle in einer Applikation auf dem Smartphone – der Wallet – verwalten. Beispielsweise können Benutzer den digitalen Nachweis ihres Personalausweises und ihres Wohngeldbescheids in der Wallet speichern und nachfolgend mit der zuständigen Behörde teilen, um einen digitalen Nachweis ihres Sozialpasses[1] zu erhalten. Dieser kann anschließend wiederum in der Wallet gespeichert und mit verschiedenen Prüfern geteilt werden, um Rabatte (zum Beispiel vergünstigter Zoo-Besuch) zu erhalten.

Wallets ermöglichen ihren Benutzern, selbstbestimmt zu entscheiden, wann und mit wem sie digitale Nachweise teilen möchten. So behalten die Benutzer die Kontrolle über ihre

[1] Durch einen Sozialpass erhalten Menschen mit geringem finanziellem Einkommen Ermäßigungen auf Angebote im gesellschaftlichen, kulturellen und sportlichen Bereich. Ein Beispiel für einen Sozialpass ist der Karlsruher Pass: https://karlsruher-pass.de.

persönlichen Daten. Dies ist nicht nur im E-Government relevant (beispielsweise bei der Beantragung des digitalen Sozialpasses), sondern auch im E-Commerce. Benutzer können persönliche Daten in der Wallet speichern und selbstbestimmt mit verschiedenen Online-Shops teilen. Dadurch erhalten Benutzer maßgeschneiderte, datenschutzkonforme Produktempfehlungen, ohne dass ungewollt Daten durch Online-Shops abgegriffen werden (Braun u. a., 2024).

Auch in anderen Domänen sind Wallets von Bedeutung, wie in der Mobilität und im Finanzwesen. Beispielsweise kann ein Wallet-Benutzer die digitalen Nachweise seines Führerscheins, seiner vorhandenen Haftpflichtversicherung und seiner Bonitätsauskunft in der Wallet speichern. Bei der Buchung eines Car-Sharing-Angebots können diese digitalen Nachweise dann mit dem Car-Sharing-Anbieter geteilt werden. So kann der Wallet-Benutzer gegenüber dem Car-Sharing-Anbieter nachweisen, dass der Wallet-Benutzer über eine gültige Fahrerlaubnis verfügt, dass potenzielle Schäden durch die Haftpflichtversicherung abgedeckt sind und die finanzielle Zuverlässigkeit gewährleistet ist (Anke und Richter, 2023).

Nationale und internationale Initiativen treiben die Entwicklung und Forschung von Wallets voran. Am 20. Mai 2024 trat die überarbeitete Fassung der Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS 2.0) in Kraft. Diese Verordnung bildet den regulatorischen Rahmen für die Bereitstellung sicherer und interoperabler digitaler Identitätslösungen innerhalb der Europäischen Union. Jeder Mitgliedsstaat der Europäischen Union ist durch eIDAS 2.0 verpflichtet, seinen Bürgern eine europaweit verwendbare Wallet bis zum 21. November 2026 zur Verfügung zu stellen. Mit dieser Wallet sollen sich Bürger europaweit identifizieren und ihre digitalen Nachweise interoperabel verwalten können (Europäische Union, 2024).

Auf nationaler Ebene förderte die Bundesregierung beispielsweise das Schaufensterprogramm „Sichere digitale Identitäten“[2], um die wissenschaftliche Untersuchung und die praktische Anwendung von Wallets in Deutschland weiter voranzutreiben. Das Schaufensterprogramm umfasste 4 Forschungsprojekte, die Projektpartner aus verschiedenen Regionen Deutschlands vereinen, um unterschiedliche Aspekte von Wallets in verschiedenen Anwendungsfällen zu untersuchen. Teilergebnisse dieser Dissertation entstanden im Forschungsprojekt „Schaufenster Sichere Digitale Identitäten Karlsruhe (SDIKA)“[3] – eines der 4 Forschungsprojekte. SDIKA fokussierte sich auf die Erprobung von Anwendungsfällen in den Regionen Karlsruhe und Rhein-Neckar. Anwendungsfälle waren beispielsweise das Buchen eines Car-Sharing-Angebots mittels einer Wallet im Bereich der Mobilität und die Beantragung einer Meldebescheinigung mittels einer Wallet im

[2] https://digitale-identitaeten.de/schaufensterprojekte
[3] https://sdika.de

Bereich des E-Governments. Zusätzlich wurden verschiedene Querschnittsthemen betrachtet, wie beispielsweise Benutzererfahrung (User Experience, kurz UX) und Informationssicherheit, rechtliche Aspekte und digitale Souveränität.

Gartner Inc. (2024) prognostiziert, dass bis 2026 weltweit mindestens 500 Millionen Menschen regelmäßig Wallets nutzen werden. Umso wichtiger ist es, dass Wallets leicht zu bedienen und sicher sind, das heißt, dass Wallets ein angemessenes Level an UX und Informationssicherheit besitzen. Forschungsergebnisse zeigen jedoch, dass bestehende Wallets unterschiedliche Schwächen der UX und Informationssicherheit aufweisen.

Beispielsweise zeigen die Forschungsergebnisse von Sartor u. a. (2022), dass Benutzer der Wallet die Terminologie als zu technisch empfinden (etwa wenn Begriffe wie „Agents“ verwendet werden) und Schwierigkeiten haben, in der Wallet verwendete ähnlich klingende Begriffe zu unterscheiden (wie die Begriffe „Connections“ und „Contacts“). Die grundlegende Funktionalität von Wallets wird von Benutzern oftmals nicht verstanden (Khayretdinova u. a., 2022). Es fehlt an Hilfsoptionen und an einem einführenden Tutorial, damit (insbesondere technikunerfahrene) Benutzer die wesentliche Funktionsweise von Wallets verstehen (Sellung und Kubach, 2023). Zudem ist Benutzern häufig unklar, dass die Daten in der Wallet nur auf den eigenen Geräten der Benutzer gespeichert werden. Außerdem werden fehlende Such- und Sortier-Funktionen sowie mangelnde Informationen über die Verwendbarkeit von digitalen Nachweisen kritisiert (Sartor u. a., 2022). Des Weiteren haben manche Benutzer Schwierigkeiten, Sicherungen und Wiederherstellungen von Backups in der Wallet auszuführen (Satybaldy, 2023).

Die Schwächen der UX und der Informationssicherheit von Wallets können dazu führen, dass Benutzer die Wallet nicht regelmäßig nutzen oder sie sogar vollständig von ihren Endgeräten entfernen. Durch Fehlbedienungen oder unzureichende Sicherheitsmaßnahmen können sensible Daten unbeabsichtigt offengelegt werden. Dies würde nicht nur das Vertrauen in die Technologie verringern, sondern auch die geplante breite Nutzung und langfristige Akzeptanz gefährden, was besonders problematisch ist, da die Europäische Union (2024) bis Ende 2026 eine flächendeckende Einführung von Wallets anstrebt.

Zusätzlich zu den genannten Schwächen der UX und Informationssicherheit von Wallets können sich UX und Informationssicherheit aber auch gegenseitig beeinflussen. Beispielsweise kann sich die Informationssicherheit negativ auf die UX auswirken, wenn Benutzer komplexe oder aufwändige Sicherheitsmechanismen verwenden. Dies kann dazu führen, dass Sicherheitsmechanismen übersprungen oder nicht richtig von Benutzern verwendet werden (Whitten und Tygar, 1999). Des Weiteren kann sich die UX negativ auf die Informationssicherheit auswirken. In einer Studie konnte gezeigt werden, dass 18 von 24 Wallet-Benutzern einen Hinweis zum Exportieren eines digitalen Nachweises nicht gelesen haben, was die Informationssicherheit gefährdet. Zudem haben 19

von 24 Wallet-Benutzern den Sicherheitshinweis über die fehlende Vertrauenswürdigkeit des Ausstellers eines digitalen Nachweises beim Speichern in der Wallet übersehen (Sauer u. a., 2025b).

Zusammenfassend sollen UX und Informationssicherheit von Wallets auf ein akzeptables Level verbessert werden, sodass eine breite Akzeptanz von Wallets in der Gesellschaft erreicht werden kann. Daher sollen in der vorliegenden Arbeit UX und Informationssicherheit nicht separat evaluiert und verbessert werden, sondern gemeinsam.

1.2 Zielsetzung und Beiträge der Arbeit

Diese Arbeit befasst sich mit der Evaluation und der Verbesserung der UX und Informationssicherheit von Wallets, um eine breite Akzeptanz und Benutzung von Wallets in der Gesellschaft zu ermöglichen, insbesondere im Hinblick auf die anstehende Einführung einer europaweiten Wallet. Zukünftig sollen Benutzer ihre Wallet sicher und komfortabel verwenden können. Hierzu sollen UX und Informationssicherheit von Wallets nicht unabhängig voneinander evaluiert und verbessert werden, denn UX und Informationssicherheit können sich gegenseitig negativ oder positiv beeinflussen. Beispielsweise können sich komplexe Sicherheitsmechanismen negativ auf die UX auswirken, indem sie die Benutzung erschweren oder Benutzer dazu verleiten, sicherheitskritische Funktionen zu umgehen, was wiederum zu einer Abnahme der Informationssicherheit führen kann (Whitten und Tygar, 1999).

Ziel der Arbeit ist es, den Zusammenhang zwischen UX und Informationssicherheit von Wallets bewertbar zu machen und Verbesserungsvorschläge der UX und Informationssicherheit von Wallets zu finden. Dazu soll eine Methode entwickelt und ein Software-Tool für die Anwendung der Methode bereitgestellt werden.

Im Rahmen der Zielerreichung soll untersucht werden, inwiefern sich existierende Verfahren für die Evaluation des Zusammenhangs zwischen UX und Informationssicherheit eignen, ob sich existierende Verfahren für Wallets adaptieren lassen und wie die Durchführung adaptierter Verfahren durch Software-Tools unterstützt werden kann.

Im Folgenden wird die Herangehensweise zur Zielerreichung beschrieben. Zusätzlich werden die jeweiligen originellen Beiträge der Arbeit erläutert.

Zunächst sollen bestehende Verfahren identifiziert werden, mit denen sich der Zusammenhang zwischen UX und Informationssicherheit bewerten lassen. Es sollen lediglich diejenigen Aspekte der Qualitätsattribute UX und Informationssicherheit evaluiert werden, die sich auf die Aspekte des jeweiligen anderen Qualitätsattributs auswirken. Die

identifizierten Verfahren sollen bewertet und vergleichend einander gegenübergestellt werden.

Beitrag 1: Es wurde eine systematische Literaturrecherche durchgeführt, um vorhandene Verfahren zur Evaluation des Zusammenhangs zwischen UX und Informationssicherheit zu recherchieren. Die identifizierten Evaluationsverfahren wurden anhand verschiedener Kriterien bewertet und einander gegenübergestellt sowie jeweils diskutiert, inwiefern sich mit ihnen der Zusammenhang zwischen UX und Informationssicherheit evaluieren lässt.

Anschließend sollen identifizierte Verfahren adaptiert werden, um ein eigenes Verfahren zu entwickeln, das sich auf Wallets anwenden lässt. Hierzu sollen Qualitätsrichtlinien der UX und Informationssicherheit (sogenannte Heuristiken) für Wallets entwickelt werden. Die Heuristiken sollen im entwickelten Verfahren verwendet werden können.

Beitrag 2: Es wurden identifizierte Evaluationsverfahren aus Beitrag 1 auf eine Wallet angewendet, um einerseits Erkenntnisse über die Evaluationsverfahren zu gewinnen und andererseits konkrete Evaluationsergebnisse hinsichtlich UX und Informationssicherheit der Wallet zu erhalten.

Beitrag 3: Auf Basis der Evaluationsergebnisse der Wallet aus Beitrag 2 wurden Heuristiken der UX und Informationssicherheit für Wallets entwickelt und evaluiert.

Beitrag 4: Einige der identifizierten Evaluationsverfahren aus Beitrag 1 wurden mithilfe der Erkenntnisse über die Verfahren aus Beitrag 2 adaptiert und es wurde damit eine neue Methode namens MEUSec entwickelt. Mit der MEUSec-Methode lässt sich der Zusammenhang zwischen UX und Informationssicherheit von Wallets evaluieren und es lassen sich Verbesserungsvorschläge für Wallets finden. Die MEUSec-Methode wurde iterativ entwickelt, unter anderem durch Diskussionen mit verschiedenen Experten der UX, Informationssicherheit und Wallets aus Wissenschaft und Wirtschaft.

Anschließend soll die MEUSec-Methode ein erstes Mal evaluiert werden, indem diese auf eine Wallet angewendet wird. Die MEUSec-Methode soll anschließend mithilfe der Evaluationsergebnisse verbessert werden.

Beitrag 5: Die MEUSec-Methode aus Beitrag 4 wurde das erste Mal evaluiert, indem die MEUSec-Methode auf die Hidy-Wallet[4] angewendet und verschiedene Evaluationskriterien verwendet wurden. Dadurch wurden einerseits die UX und Informationssicherheit der Hidy-Wallet evaluiert und andererseits wurde die MEUSec-Methode evaluiert. Die MEUSec-Methode wurde auf Basis der Evaluationsergebnisse verbessert.

[4] https://hidy.eu

Anschließend soll ein Software-Tool entwickelt werden, mit dem sich die MEUSec-Methode anwenden lässt. Schritte der MEUSec-Methode sollen dadurch effizienter und automatisiert durchgeführt werden können.

Beitrag 6: Zur Unterstützung der Anwendung der MEUSec-Methode wurde ein Software-Tool entwickelt. Zunächst wurde eine Anforderungserhebung durchgeführt. Danach folgte der Entwurf des Architekturmodells, des User Interface und des Datenmodells. Anschließend wurde das Software-Tool programmiert.

Danach soll die MEUSec-Methode mithilfe des Software-Tools auf eine weitere Wallet angewendet werden, um die MEUSec-Methode und das Software-Tool zu evaluieren. Hierzu sollen dieselben Evaluationskriterien der ersten Evaluation verwendet werden, um die Evaluationsergebnisse abschließend miteinander vergleichen zu können.

Beitrag 7: Die verbesserte MEUSec-Methode aus Beitrag 5 wurde evaluiert, indem diese auf die Lissi-Wallet[5] angewendet wurde. Zusätzlich wurde das Software-Tool aus Beitrag 6 zur Unterstützung eingesetzt. Es wurden dieselben Evaluationskriterien der ersten Evaluation aus Beitrag 5 verwendet. So konnten die Ergebnisse der ersten Evaluation mit denen der zweiten Evaluation verglichen werden. Danach wurden die MEUSec-Methode und das Software-Tool mittels der Evaluationsergebnisse verbessert.

1.3 Aufbau der Arbeit

Die vorliegende Arbeit beinhaltet im Folgenden zunächst 3 Grundlagenkapitel, die zum weiteren Verständnis der Arbeit dienen.

Die Grundlagen zu Digital Identity Wallets werden in *Kapitel 2* beleuchtet. Zuerst werden die Begriffe Entität und (digitale) Identität in Abschnitt 2.1 erläutert. Außerdem werden 3 Modelle zur Verwaltung von digitalen Identitäten beschrieben und anhand verschiedener Kriterien verglichen. Anschließend wird in Abschnitt 2.2 auf (verifizierbare) digitale Nachweise eingegangen. Zudem werden die beim Austausch von verifizierbaren digitalen Nachweisen beteiligten Rollen und deren Funktionen thematisiert. Die Ausstellung, Speicherung, Präsentation und der Widerruf von verifizierbaren digitalen Nachweisen durch die beschriebenen Rollen werden anhand eines beispielhaften Prozesses erläutert. Nachdem die verschiedenen Rollen eingeführt sind, werden deren Anforderungen in Abschnitt 2.3 verdeutlicht. Darauffolgend wird in Abschnitt 2.4 auf die Funktionalität von Digital Identity Wallets eingegangen. Zudem werden Digital Identity Wallets zu anderen Arten von Wallets (wie beispielsweise Google- und Apple-Wallet) abge-

[5] https://lissi.id

grenzt. Abschließend werden in Abschnitt 2.5 relevante Technologien und Standards digitaler Identitäten beschrieben sowie deren Zusammenhang zu den erwähnten Rollen hergestellt.

Die Grundlagen zur UX werden in *Kapitel 3* beschrieben. Zuerst wird der Begriff UX in Abschnitt 3.1 eingeführt und verschiedene Attribute der UX werden erläutert. Anschließend wird der Begriff Usability eingeführt und verschiedene Attribute der Usability werden erläutert. Um eine möglichst gute UX zu erreichen, kann das Human-Centered Design als einen Ansatz zur Entwicklung interaktiver Systeme angewendet werden. Das Human-Centered Design wird in Abschnitt 3.3 thematisiert, indem zunächst 6 Grundsätze und anschließend 4 Aktivitäten des Human-Centered Design beschrieben werden. Zuletzt wird in Abschnitt 3.4 der Begriff Dark Pattern erläutert und es werden 5 Arten von Dark Pattern beschrieben.

Die Grundlagen zur Informationssicherheit werden in *Kapitel 4* thematisiert. Zuerst wird in Abschnitt 4.1 der Begriff Informationssicherheit erläutert und dessen Schutzziele vorgestellt. Anschließend werden in Abschnitt 4.2 die Begriffe Schwachstelle, Bedrohung, Angriff und Risiko voneinander abgegrenzt. Nachfolgend wird in Abschnitt 4.3 auf das Security Engineering eingegangen, indem zunächst die Strukturanalyse und die Schutzbedarfsermittlung beleuchtet werden. Anschließend werden die Bedrohungsanalyse und die Risikoanalyse beschrieben.

Nachdem die Grundlagen erläutert sind, wird in *Kapitel 5* auf die Evaluation von UX und Informationssicherheit eingegangen. Zuerst wird in Abschnitt 5.1 der Zusammenhang zwischen UX und Informationssicherheit erläutert. Hierbei werden verschiedene Arten der Beeinflussung von UX und Informationssicherheit beschrieben und mit Beispielen verdeutlicht. Mittels einer systematischen Literaturrecherche wurden verschiedene Evaluationsverfahren identifiziert, mit denen sich der Zusammenhang zwischen UX und Informationssicherheit (teilweise) evaluieren lässt. Diese Evaluationsverfahren werden in Abschnitt 5.2 diskutiert. Zusätzlich werden die Evaluationsverfahren anhand verschiedener Kriterien bewertet und einander gegenübergestellt. Die Anwendung einiger dieser Evaluationsverfahren auf eine Wallet wird in Abschnitt 5.3 beschrieben. Dadurch konnten einerseits weitere Erkenntnisse über die Evaluationsverfahren gewonnen werden und andererseits Evaluationsergebnisse der UX sowie der Informationssicherheit der Wallet erhoben werden. Auf Basis der Evaluationsergebnisse und weiterer Rechercheergebnisse wurden Qualitätsrichtlinien, sogenannte Heuristiken, der UX und Informationssicherheit von Wallets abgeleitet und evaluiert. Die Entwicklung und die Evaluation dieser Heuristiken werden in Abschnitt 5.4 dargelegt.

In *Kapitel 6* wird die im Rahmen der Arbeit finale Version der MEUSec-Methode (dritte Version) erläutert, mit der sich UX und Informationssicherheit von Wallets evaluieren

und Verbesserungsvorschläge finden lassen. In Abschnitt 6.1 erfolgt die Beschreibung der MEUSec-Methode. Die Entwicklung und die Begründungen von Entwurfsentscheidungen der MEUSec-Methode werden in Abschnitt 6.2 thematisiert. Danach werden die Beschränkungen und Voraussetzungen der MEUSec-Methode in Abschnitt 6.3 erläutert. In Abschnitt 6.4 wird die MEUSec-Methode mit anderen Ansätzen aus der Literatur verglichen.

In *Kapitel 7* wird die Evaluation der ersten Version der MEUSec-Methode beschrieben. Die erste Version der MEUSec-Methode wurde auf die Hidy-Wallet angewendet und anhand verschiedener Evaluationskriterien bewertet. Dadurch enstanden grundsätzlich 2 Beiträge: die Evaluation der Hidy-Wallet und die Evaluation der MEUSec-Methode. Die Vorgehensweise der Evaluation wird in Abschnitt 7.1 beschrieben. Die Evaluationsergebnisse der Hidy-Wallet werden in Abschnitt 7.2 erläutert und in Abschnitt 7.3 eingeordnet. In Abschnitt 7.4 werden die Evaluationsergebnisse der MEUSec-Methode beschrieben. Die Limitationen der Evaluation werden in Abschnitt 7.5 verdeutlicht. Nach der Evaluation wurden die gewonnenen Erkenntnisse in die MEUSec-Methode eingearbeitet, sodass eine zweite Version der MEUSec-Methode entstand.

Zur Unterstützung der Anwendung der MEUSec-Methode wurde ein Software-Tool entwickelt. Die im Rahmen der Arbeit finale Version des Software-Tools (zweite Version) wird in *Kapitel 8* beschrieben. Zuerst wird das Vorgehensmodell der Entwicklung in Abschnitt 8.1 erläutert. Anschließend werden die Anforderungen an das Software-Tool in Abschnitt 8.2 beschrieben. Im Rahmen des Entwurfs des Software-Tools wurde ein Datenmodell und ein Architekturmodell erstellt. Zusätzlich wurden Wireframes des User Interface entwickelt. Wireframes vermitteln die grundlegende Struktur, Hierarchie und Funktionalität eines User Interface (Almani und Alrwais, 2024). Der Entwurf wird in Abschnitt 8.3 beschrieben. Anschließend erfolgt die Funktionsbeschreibung des Software-Tools in Abschnitt 8.4.

In *Kapitel 9* wird die Evaluation der zweiten Version der MEUSec-Methode und der ersten Version des Software-Tools beschrieben. Die zweite Version der MEUSec-Methode wurde auf die Lissi-Wallet angewendet und zusätzlich die erste Version des Software-Tools zur Hilfe eingesetzt. Dadurch entstanden grundsätzlich 3 Beiträge: die Evaluation der Lissi-Wallet, die Evaluation der MEUSec-Methode und die Evaluation des Software-Tools. In Abschnitt 9.1 wird die Vorgehensweise der Evaluation beschrieben. Die Evaluationsergebnisse der Lissi-Wallet werden in Abschnitt 9.2 erläutert und in Abschnitt 9.3 eingeordnet. Die Evaluationsergebnisse der MEUSec-Methode werden in Abschnitt 9.4 ausgeführt. In Abschnitt 9.5 werden die Evaluationsergebnisse des Software-Tools dargestellt. Die Limitationen der Evaluation werden in Abschnitt 9.6 aufgezeigt. Die Evaluationsergebnisse werden anschließend mit denen der ersten Evaluation (aus Kapitel 7) in Abschnitt 9.7 verglichen. Nach der Evaluation wurden die gewonnenen

Erkenntnisse in die MEUSec-Methode und in das Software-Tool eingearbeitet, sodass die im Rahmen der Arbeit finale dritte Version der MEUSec-Methode und die finale zweite Version des Software-Tools entstanden.

Kapitel 10 zieht abschließend ein Fazit und gibt einen Ausblick auf offen gebliebene Forschungsfragen.

Die verwandten Arbeiten werden jeweils in den entsprechenden Abschnitten erläutert.

Abbildung 1 gibt einen Überblick über den Aufbau der Arbeit.

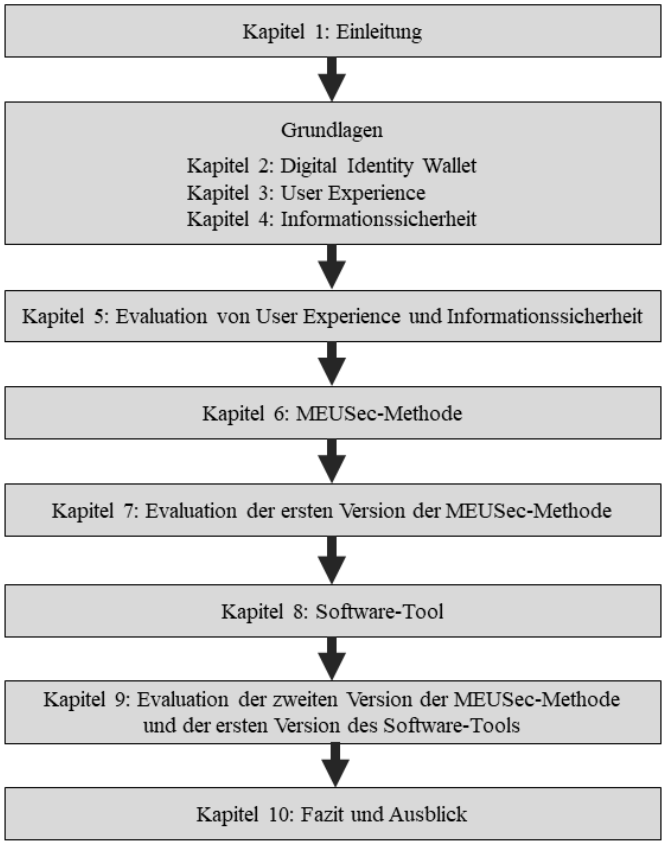


Abbildung 1: Aufbau der Arbeit

2 Grundlagen: Digital Identity Wallets

Dieses Kapitel beschreibt die Grundlagen von Digital Identity Wallets. Zunächst wird der Begriff der digitalen Identität in Abschnitt 2.1 erläutert. Anschließend wird der Aufbau von verifizierbaren digitalen Nachweisen und ihre Nutzung in Abschnitt 2.2 beschrieben. Die beim Austausch von verifizierbaren digitalen Nachweisen involvierten Rollen und deren Anforderungen werden in Abschnitt 2.3 thematisiert. Danach wird die Funktionalität von Digital Identity Wallets in Abschnitt 2.4 beschrieben. Besonders hervorzuheben ist dabei die herausgearbeitete Abgrenzung zu anderen Wallet-Arten, die in der Literatur bislang fehlt. Die Begriffe der unterschiedlichen Wallet-Arten werden häufig unscharf verwendet. Abschnitt 2.5 schließt mit relevanten Technologien und Standards.

2.1 Digitale Identität

Mit der fortschreitenden Digitalisierung erweitert sich das Angebot an digitalen Diensten. Um vertrauenswürdige Interaktionen mit diesen Diensten zu gewährleisten, ist eine Prüfung der Identität und einzelner Attribute notwendig. In der physischen Welt dienen körperliche Merkmale (beispielsweise Fingerabdruck oder Iris) und verschiedene Dokumente (beispielsweise Personalausweis oder Bibliotheksausweis) in verschiedenen Anwendungsfällen zur Identifizierung. Im digitalen Raum sind äquivalente Mechanismen notwendig, um Entitäten eindeutig zu identifizieren und unterschiedliche Entitäten voneinander unterscheiden zu können.

Zur Definition des Begriffs der digitalen Identität werden im Folgenden zunächst die Begriffe „Entität“ und „Identität“ eingeführt. Anschließend wird der Begriff „Digitale Identität“ erläutert und die für diese Arbeit geltende Definition vorgestellt.

Eine Entität ist ein „Gegenstand, der […] erkennbar eine eigene Existenz hat“ (DIN EN ISO/IEC 24760-1:2022, 2022). In (DIN EN ISO/IEC 24760-1:2022, 2022) wird der Begriff „Existenz“ nicht definiert. Der Begriff lässt sich jedoch so interpretieren, dass eine Entität abgrenzbar und unterscheidbar ist. Beispiele für eine Entität sind eine „Person, eine Organisation, ein Gerät, eine Gruppe solcher Begriffe, ein menschlicher Teilnehmer an einem Telekommunikationsdienst, eine SIM-Karte, ein Reisepass, eine Netzwerkkarte, eine Softwareanwendung, ein Dienst oder eine Website“ (DIN EN ISO/IEC 24760-1:2022, 2022). Neben den in (DIN EN ISO/IEC 24760-1:2022, 2022) genannten

Beispielen können auch Tiere und Fahrzeuge als Entitäten bezeichnet werden. Ausschlaggebend ist, dass Entitäten abgrenzbar und unterscheidbar sind.

Einer Entität kann eine Menge von Attributen (Eigenschaften) zugeordnet werden, zum Beispiel kann ein Mensch blaue Augen haben. Eine Identität besteht aus einer Teilmenge dieser Attribute, die eine bestimmte Entität eindeutig beschreibt. Eine Entität kann durch mehr als eine Identität eindeutig bestimmt werden. Identifikatoren sind eine besondere Art von Attributen. Ein Identifikator hat die Eigenschaft, dass dieser alleine als Identität dient. In der Praxis wird hierfür entweder eine eindeutige Zeichenkette, wie beispielsweise eine DID (siehe Abschnitt 2.5), oder eine Zusammensetzung von vorhandenen Attributen, wie beispielsweise Name, Vorname und Adresse, verwendet (DIN EN ISO/IEC 24760-1:2022, 2022).

Nach Grassi u. a. (2017) wird eine Entität im digitalen Raum durch eine oder mehrere digitale Identität(en) eindeutig beschrieben. Eine Entität kann beispielsweise durch eine digitale Identität für die E-Mail-Kommunikation und eine andere für das Online-Banking eindeutig beschrieben werden. Eine digitale Identität muss keine Attribute der Entität im realen Leben preisgeben, wie beispielsweise das Alter.

Die Definition von Grassi u. a. (2017) beschreibt lediglich die Zielsetzung einer digitalen Identität, nicht jedoch deren konkreten Aufbau. Für die vorliegende Arbeit wird die nachfolgende Definition 2-1 einer digitalen Identität zugrunde gelegt. Diese ergibt sich aus der Zusammenführung der zuvor dargestellten Definitionen von Entität, Identität und digitaler Identität.

Definition 2-1: Digitale Identität

Eine digitale Identität ist eine Menge an Attributen, die eine Entität im digitalen Raum identifiziert und in einem Datensatz zusammengefasst ist.

Nach Ehrlich u. a. (2021) existieren 3 Modelle für die Verwaltung von digitalen Identitäten, die sich besonders durch Informationssicherheit, User Experience, Verbreitung, Datenqualität, Datenschutz, Standardisierung, Integrationsaufwand und primäre Nutzung differenzieren:

1. Isolierte Identitätslösung

Eine isolierte Identitätslösung ist eine digitale Identität, die nur für einen spezifischen Dienst einsetzbar ist, wie beispielsweise für das Benutzerkonto eines Online-Shops. Jeder Dienst verwaltet seine isolierte Identitätslösung eigenständig (beispielsweise in einer eigenen Datenbank) und führt die Authentifizierung selbst durch. Somit ist der Dienst

zugleich Herausgeber und Akzeptanzstelle der isolierten Identitätslösung. Dies hat den Vorteil, dass keine Abhängigkeiten zwischen konkurrierenden Organisationen und Dritten bestehen. Außerdem wird die Privatsphäre der isolierten Identitätslösung erhöht, da das Nutzungsverhalten bei anderen Diensten schwieriger verfolgt werden kann. Gleichzeitig können die identitätsbezogenen Daten innerhalb des Dienstes nach den Anforderungen der isolierten Identitätslösung justiert und verarbeitet werden. Ein Nachteil ist, dass mit der steigenden Anzahl isolierter Identitätslösungen auch der Aufwand für die sichere und effiziente Verwaltung identitätsbezogener Daten wächst (Ehrlich u. a., 2021).

2. Föderierte Identitätslösung

Eine föderierte Identitätslösung ist eine digitale Identität, die mithilfe einer zentralen Instanz, dem sogenannten Identity Provider, bei unterschiedlichen Diensten verwendet werden kann, ohne für jeden Dienst ein neues Benutzerkonto anlegen zu müssen. Der Identity Provider ist zugleich Herausgeber und Akzeptanzstelle der föderierten Identitätslösung, da er die identitätsbezogenen Daten verwaltet. Dies senkt den Verwaltungsaufwand der identitätsbezogenen Daten. Allerdings können identitätsbezogene Daten durch den Identity Provider falsch verarbeitet werden, wodurch beispielsweise soziale oder wirtschaftliche Nachteile für Inhaber der identitätsbezogenen Daten entstehen können. Zusätzlich ist eine föderierte Identität abhängig von der Verfügbarkeit und Vertraulichkeit des Identity Providers (Ehrlich u. a., 2021).

Eine staatliche Identitätslösung, wie der elektronische Personalausweis mit elektronischer Identität (eID), ist ein Sonderfall der föderierten Identitätslösung. Eine staatliche Identitätslösung besitzt ein hoheitliches Authentifizierungsmittel mit zusätzlicher digitaler Repräsentation. Das bedeutet, dass die identitätsbezogenen Daten nicht zentral verwaltet werden, sondern eine dedizierte Infrastruktur (der sogenannte eID-Server) die identitätsbezogenen Daten an den Online-Dienst weiterleitet. Beim elektronischen Personalausweis sind die identitätsbezogenen Daten in einem kontaktlos lesbaren Chip im physischen Personalausweis gespeichert (Ehrlich u. a., 2021). Mithilfe der AusweisApp2 können die gespeicherten identitätsbezogenen Daten von einem berechtigten Online-Dienst ausgelesen werden. Dazu benötigen Benutzer den elektronischen Personalausweis mit eID, einen 6-stelligen persönlichen Pin, die AusweisApp2 und ein Smartphone oder Kartenlesegerät. Wenn ein Online-Dienst eine Anfrage zum Nachweis der Identität stellt, können Benutzer ihren elektronischen Personalausweis mit der eID an das Smartphone oder an das Kartenlesegerät halten und den 6-stelligen Pin eingeben. Anschließend wird zunächst geprüft, ob der Online-Dienst die staatliche Berechtigung zur Abfrage der identitätsbezogenen Daten besitzt. Denn Online-Dienste müssen zur Nutzung der eID erforderliche Standards erfüllen und eine Freigabe zum Auslesen von identitätsbezogenen Daten einholen. Nach positiver Prüfung werden die identitätsbezogenen Daten durch den Online-Dienst ausgelesen. Benutzer können sich damit also gegenüber Online-Diensten ausweisen, ohne sich

jeweils neu registrieren zu müssen (Bundesministerium des Innern und für Heimat, 2023). Aus der erforderlichen Freigabe des Auslesens von identitätsbezogenen Daten durch die eID resultiert ein hohes Niveau der Informationssicherheit. Allerdings wird die eID aufgrund dieser regulatorischen Anforderungen nur von wenigen Online-Diensten verwendet. Zudem resultiert daraus eine geringe Verbreitung in der Europäischen Union (Ehrlich u. a., 2021).

3. Selbstbestimmte Identitätslösung

Eine selbstbestimmte Identitätslösung ist eine digitale Identität (Self-Sovereign Identity, SSI), die nicht von einem zentralen Identity Provider verwaltet wird. Die Kontrolle über die Speicherung, Verwaltung und Weitergabe der identitätsbezogenen Daten liegt bei den Benutzern selbst. Die identitätsbezogenen Daten werden in Form von kryptografisch gesicherten digitalen Nachweisen (siehe Abschnitt 2.2) ausgestellt, die in einer digitalen Brieftasche (Wallet) durch die Benutzer selbstständig dezentral verwaltet werden können. Benutzer können dadurch selbst entscheiden, welche identitätsbezogenen Daten sie mit welchen Online-Diensten teilen wollen. Aufgrund der kryptografisch gesicherten digitalen Nachweise ist die Überprüfung der geteilten Daten ohne Kontakt zum Herausgeber möglich. Eine selbstbestimmte Identitätslösung schützt somit die Privatsphäre und ist standardisiert. Zudem fördert sie die User Experience und Informationssicherheit, indem sie es den Benutzern ermöglicht, Daten selbstbestimmt und kryptografisch gesichert zu teilen. Selbstbestimmte Identitätslösungen sind derzeit allerdings noch wenig verbreitet, gewinnen jedoch zunehmend an Bedeutung (Ehrlich u. a., 2021).

Diese Arbeit fokussiert sich auf selbstbestimmte Identitätslösungen und Wallets (siehe Abschnitt 2.4) als zentrale Softwarekomponenten von SSI, da diese eine besonders hohe gesellschaftliche Relevanz aufweisen. Jeder EU-Mitgliedstaat muss seinen Bürgern bis 2026 eine Wallet zur Verfügung stellen und Wallets anderer EU-Mitgliedsstaaten akzeptieren (Europäische Union, 2024). Allerdings wurde in diesem Bereich bislang wenig Forschung betrieben und bisherige Untersuchungen zeigen, dass Wallets verschiedene Schwächen der User Experience und Informationssicherheit besitzen (siehe Abschnitt 5.3.1). Eine Reduktion oder sogar Beseitigung dieser Schwächen könnte die Akzeptanz von Wallets in der Bevölkerung und der Wirtschaft deutlich fördern.

Tabelle 1 bewertet und vergleicht die genannten Modelle zur Verwaltung digitaler Identitäten nach ihren wesentlichen Unterscheidungsmerkmalen. Dabei wird die eID des Personalausweises als Sonderfall föderierter Identitätslösungen separat bewertet.

	Isoliert	**Föderiert**	**eID des Personalausweises**	**Selbstbestimmt**
Informationssicherheit	Unklar	Hoch	Sehr hoch	Sehr hoch

Verbreitung	Hoch	Hoch	Gering	Sehr gering
User Experience	Mittel	Hoch	Gering	(Potenziell) Hoch
Datenqualität	Unklar	Unklar	Hoch	Hoch
Datenschutz	Unklar	Unklar	Hoch	Hoch
Standardisierung	Nein	Ja	Ja	Ja
Integrationsaufwand	Mittel	Gering	Sehr hoch	Implementierungsabhängig
Primäre Nutzung	Onlinedienste	Onlinedienste, Unternehmensanwendungen	Öffentliche Verwaltung, zur Identifizierung einer Person	Beliebiger Einsatz

Tabelle 1: Modelle zur Verwaltung digitaler Identitäten, (Ehrlich u. a., 2021). Begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Damit beispielsweise Personen nicht im Namen von anderen Personen in Online-Shops einkaufen oder minderjährige Personen nicht an Glückspielen teilnehmen, ist es wichtig, dass nur berechtigte Personen eine digitale Identität im digitalen Raum einsetzen dürfen. Um dies zu gewährleisten, können verifizierbare digitale Nachweise eingesetzt werden (Anke und Richter, 2023). Auf diese wird in Abschnitt 2.2 detailliert eingegangen.

2.2 Verifizierbarer digitaler Nachweis

Durch die steigende Digitalisierung wächst die Anzahl an digitalen Diensten. Menschen wollen digitale Dienste nutzen, um sich beispielsweise den physischen Weg zur Behörde zu sparen. Mithilfe der unterschiedlichen Grundmodelle digitaler Identitäten (siehe Abschnitt 2.1) werden immer mehr digitale Identitäten erschaffen. Eine digitale Identität muss sich im digitalen Raum für digitale Dienste ausweisen (Skierka, 2022).

Personen können sich ausweisen, „[…] indem eine allseitig als glaubwürdig anerkannte Autorität in einem Dokument bestätigt, dass einer bestimmten natürlichen Person Merkmale wie Name, Vorname oder Adresse zugeschrieben werden“ (Hornung, 2005).

Nach Pohlmann (2022) ist ein digitaler Nachweis „eine [digitale] Bescheinigung der Identität, Qualifikation, Befähigung oder Befugnis, die einer Einzelperson von einem Dritten (Aussteller), zum Beispiel Einwohnermeldeamt, Straßenverkehrsamt, Hochschule usw. ausgestellt wurde“.

Anke & Richter (2023) beschränken sich nicht nur auf die Bescheinigung der Identität, Qualifikation, Befähigung oder Befugnis von Einzelpersonen (wie es Pohlmann (2022) tut), sondern beziehen sich auch auf Organisationen und Objekte.

Ein digitaler Nachweis, der überprüfbar und kryptografisch gesichert ist, nennt sich verifizierbarer Nachweis (Verifiable Credential, VC). Ein VC besteht aus mindestens einem Claim (dt. Behauptung) über eine Entität, wie beispielsweise Alter oder Wohnort. Zudem beinhaltet ein VC auch Metainformationen, wie beispielsweise Aussteller, Typ oder Ablaufdatum. Des Weiteren inkludiert ein VC einen sogenannten Proof (dt. Prüfung). Dieser belegt, dass ein VC und dessen Behauptung(en) von einem bestimmten Aussteller für einen bestimmten Inhaber erstellt wurden (Pohlmann, 2022).

In der vorliegenden Arbeit wird die folgende Definition 2-2 eines VC zugrunde gelegt.

Definition 2-2: VC

Ein VC ist ein Datensatz zur Bescheinigung der Identität, Qualifikation, Befähigung oder Befugnis von Entitäten im digitalen Raum. Ein VC beinhaltet:

- Claim(s), das heißt, mindestens eine Behauptung über mindestens eine Entität,
- Proof(s), das heißt, kryptografische Informationen, die eine Überprüfung ermöglichen und
- Metainformationen zu Aufbau und Bedeutung.

Nach Pohlmann (2022) sind beim Austausch von VC im Kontext von SSI (siehe Abschnitt 2.1) 3 Entitäten involviert:

(1) Aussteller (Issuer) sind Organisationen oder Unternehmen, die VC ausstellen, wie beispielsweise Hochschulen, die Studierendenausweise ausstellen.

(2) Prüfer (Verifier) sind Akzeptanzstellen oder Anwendungen, die VC fordern, um damit Inhalte oder Aussagen über bestimmte Attribute in einem Prozess oder einer Anwendung zu nutzen und weiter zu verarbeiten. Die Verifizierung der digitalen Signatur kann dabei automatisiert erfolgen, zum Beispiel durch kryptografische Challenge-Response-Verfahren. Hierbei kann dem Inhaber eines VC eine Herausforderung (Challenge) gestellt werden, die dann kryptografisch verarbeitet werden muss, um eine verschlüsselte Antwort (Response) zurückgeben zu können. Anschließend wird geprüft, ob die kryptografische Verarbeitung richtig durchgeführt wurde (Pohlmann, 2022). Beispielsweise kann eine Challenge eine Zeichenfolge sein, die mit einem geheimen Schlüssel konkateniert wird und dann als Response unter Verwendung einer Hash-Funktion zurückgegeben wird. Eine Hochschule kann ihren Studierenden einen digitalen Studierendenausweis ausstellen. Dieser kann daraufhin innerhalb der Hochschule bei Klausuren oder außerhalb der Hochschule für einen vergünstigten Eintritt bei einem Kino geprüft werden. Bei diesem Beispiel wird deutlich, dass VC von der ausstellenden aber auch von einer anderen Institution geprüft werden können. Aussteller und Prüfer sind dabei Rollen.

(3) Inhaber (Holder) können VC von Ausstellern anfordern, speichern und selbstbestimmt entscheiden, welche VC sie mit Prüfern teilen möchten. Ein Inhaber kann bei-

spielsweise seinen Studierendenausweis von der Hochschule (Aussteller) anfordern und danach wieder mit der Hochschule (Prüfer) teilen, um rabattiert in der Mensa zu essen.

Abbildung 2 visualisiert die beschriebenen Akteure mit deren Zusammenhängen.

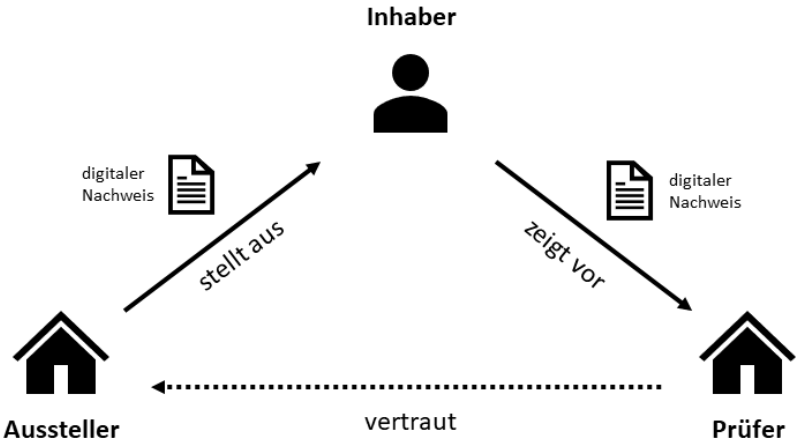


Abbildung 2: Aussteller, Inhaber und Prüfer von VC. (Pohlmann, 2022). Vereinfachte Darstellung.

Beispielhaft möchte Person A (Inhaber) ein VC ihres Sozialpasses[6] erhalten, um damit vergünstigten Kinoeintritt zu erlangen. Um das VC ihres Sozialpasses zu erhalten, benötigt sie beispielsweise das VC ihres Personalausweises und das VC ihres Wohngeldbescheids. Das VC ihres Personalausweises lässt sie sich vom Bundesministerium des Innern und Heimat (Aussteller) mithilfe ihrer AusweisApp2 ausstellen. Das VC ihres Wohngeldbescheids bekommt sie beispielsweise von der Wohngeldbehörde ausgestellt. Nun besitzt Person A das VC ihres Personalausweises und ihres Wohngeldbescheids. Diese VC präsentiert sie nun bei der Kommune (zunächst Prüfer), in der sie wohnt und welche die VC prüft, um anschließend von dieser Kommune (nun Aussteller) das VC ihres Sozialpasses zu erhalten. Person A präsentiert nun das VC des Sozialpasses beim Ticketkauf im Kino (Prüfer) und erhält dadurch vergünstigten Eintritt.

Abbildung 3 visualisiert das beschriebene Beispiel. In der Abbildung stehen „Personalausweis“, „Wohngeldbescheid“ und „Sozialpass“ für die jeweiligen VC als Pendant zu den heute existierenden physischen Nachweisen.

[6] Durch einen Sozialpass erhalten Menschen mit geringem finanziellem Einkommen, Ermäßigungen auf Angebote im gesellschaftlichen, kulturellen und sportlichen Bereich. Ein Beispiel für einen Sozialpass ist der Karlsruher Pass: https://karlsruher-pass.de.

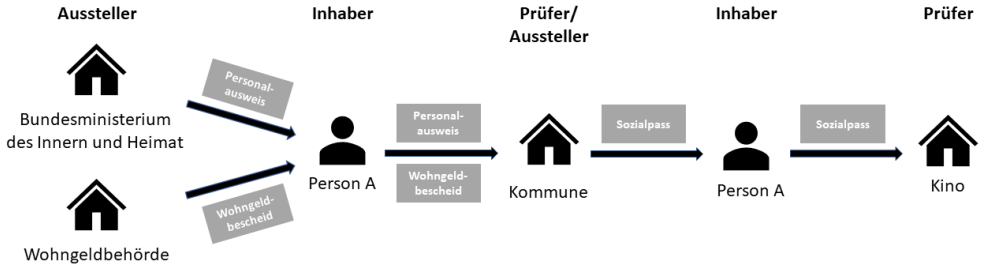


Abbildung 3: Ausstellung, Speicherung und Präsentation von VC

Zudem können VC ihre Gültigkeit verlieren, indem diese zeitliche Limitationen besitzen oder durch den Aussteller oder Inhaber widerrufen werden (Chadwick u. a., 2019).

Beispielhaft wurde der in Abbildung 3 aufgezeigte Prozess um den Widerruf des VC des Sozialpasses von Person A erweitert. Die Kommune hat die Information erhalten, dass Person A kein Wohngeld mehr bezieht und hat daraufhin das VC des Sozialpasses von Person A entzogen. Als Person A erneut Wohngeld bezog, ließ sie sich das VC des Sozialpasses erneut ausstellen und präsentierte dieses ihrem örtlichen Schwimmbad, um Rabatt beim Eintritt zu erhalten.

Abbildung 4 zeigt den beschriebenen Prozess modelliert als ein UML-Sequenzdiagramm.

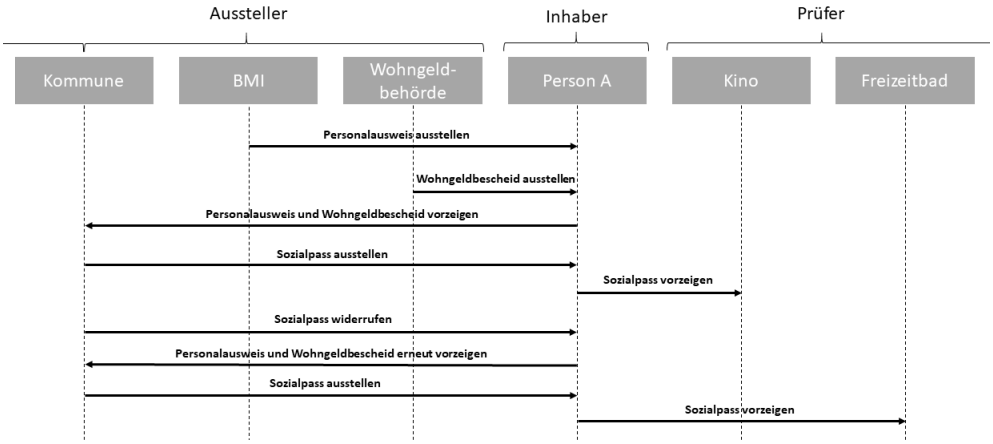


Abbildung 4: Ausstellung, Speicherung, Präsentation und Widerruf von VC. „BMI“ steht dabei für „Bundesministerium des Innern und für Heimat“.

Wenn Inhaber ihre VC an Prüfer präsentieren, werden die benötigten VC nicht selbst übermittelt. Stellvertretend wird aus den benötigten VC eine sogenannte Verifiable Presentation (VP) erstellt und durch den Inhaber mit einem Proof versehen. Durch diesen zusätzlichen Proof kann verifiziert werden, dass die VP tatsächlich von einem bestimm-

ten Inhaber hervorgeht und für diese Transaktion erstellt wurde. Wenn stattdessen lediglich das VC geteilt werden würde, könnte der Prüfer die VC für eigene Zwecke missbrauchen (Pohlmann, 2022).

2.3 Rollen und Anforderungen

In Abschnitt 2.2 wurden bereits Rollen erwähnt, die beim Austausch von VC involviert sind. Nun werden die Rollen weiter beschrieben und beispielhaft einige Anforderungen hervorgehoben, die in unterschiedlichen digitalen Ökosystemen, also dem Zusammenspiel unterschiedlicher Akteure, gelten.

Aussteller müssen die Berechtigung des Inhabers überprüfen, bevor die VC ausgestellt werden. Hierzu können verschiedene Identifikationsverfahren eingesetzt werden, wie beispielsweise das Video-Ident-Verfahren[7], Post-Ident-Verfahren[8] oder die Verwendung der eID. Je nach Anwendungsfall können auch andere VC für die Identifikation eingesetzt werden (Pohlmann, 2022).

Inhaber von VC müssen in der Lage sein, ihre an sie ausgestellten VC in einer Wallet (siehe Abschnitt 2.4) zu speichern und vor dem Zugriff Dritter zu schützen. Nach Speicherung von VC können Inhaber selbstbestimmt entscheiden, ob sie VC oder bestimmte Attribute von VC an Prüfer präsentieren möchten. Hierbei sollten nur die Daten geteilt werden, die tatsächlich für den Prüfer notwendig sind. Weitere Anforderungen sind eine möglichst hohe User Experience (siehe Kapitel 3) und Informationssicherheit (siehe Kapitel 4). Außerdem sollen Inhaber von VC ihre Identitätsdaten plattform- und dienstübergreifend nutzen können, sodass keine Lock-in Effekte entstehen (Ehrlich u. a., 2021).

Prüfer erhalten die VP von Inhaber der VC und müssen die VP auf Gültigkeit, Authentizität, Integrität und Herkunft prüfen. Für Prüfer ist es wichtig, dass möglichst viele Inhaber von VC ihren Dienst einfach nutzen können. Hierfür ist insbesondere ein einfacher Zugang ohne zusätzliche Registrierung notwendig. Des Weiteren müssen Prüfer ohne hohen Aufwand Inhaber von VC eindeutig für rechtsichere Transkationen identifizieren können (Ehrlich u. a., 2021).

Zudem besteht eine EU-Verordnung über elektronische Identifizierung, Authentifizierung und Vertrauensdienste – kurz: eIDAS (Europäische Union, 2024). Diese beinhaltet

[7] Die Identifizierung erfolgt online per Video-Chat durch Präsentation des Personalausweises oder des Reisepasses an einen Mitarbeiter eines zertifizierten Identifizierungsdienstes.

[8] Die Identifizierung erfolgt in einer Filiale der Deutschen Post, indem der Personalausweis oder der Reisepass einem Mitarbeiter vorgezeigt wird.

verbindliche Regelungen und somit Anforderungen für elektronische Transaktionen im europäischen Binnenmarkt. Beispielsweise werden darin 3 verschiedene Vertrauensniveaus für elektronische Identifizierungsmittel definiert: Niedrig, substanziell und hoch. Diese Vertrauensniveaus bestimmen, wie sicher und vertrauenswürdig ein elektronisches Identifizierungsmittel ist und welche Anforderungen an die Identifizierung gestellt werden. Zum Beispiel dürfen nur gewisse behördliche Online-Dienste mittels der eID durchgeführt werden, sodass das Vertrauensniveau „hoch“ eingehalten wird.

2.4 Funktionalität von Wallets

In der physischen Welt werden Nachweise üblicherweise in einer Geldbörse aufbewahrt, um diese vor Diebstahl zu schützen und eine hohe Verfügbarkeit zu gewährleisten (Preukschat und Reed, 2021).

In der digitalen Welt werden VC in Digital Identity Wallet (kurz: Wallets, von engl. Wallet für Brieftasche) gespeichert, verwaltet und mit Prüfern (siehe Abschnitt 2.2) geteilt (Ehrlich u. a., 2021).

Zusätzlich zu den VC können kryptografische Daten in der Wallet gespeichert werden. Diese kryptografischen Daten umfassen private und öffentliche Schlüssel sowie digitale Signaturen. Sie werden verwendet, um die Identität zu verifizieren und VC sicher zu speichern sowie zu übertragen. Sie gewährleisten somit die Informationssicherheit der identitätsbezogenen Daten (Podgorelec u. a., 2022).

Wallets wurden bisher in Deutschland beispielsweise im Rahmen des vom Bundesministerium für Wirtschaft und Klimaschutz geförderten Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten“ (Bundesministerium für Wirtschaft und Klimaschutz, 2020) untersucht. Auf europäischer Ebene werden aktuell Wallets in 4 Großprojekten erprobt, damit EU-Bürger einen sicheren und benutzerfreundlichen Zugang beispielsweise zu digitalen öffentlichen Diensten, Bankkonten, Bildungszertifizierungen und Unterzeichnungen von Verträgen erhalten (Europäische Kommission, 2023). Die bisher gewonnenen Ergebnisse bilden einen Ausgangspunkt für weiterführende Untersuchungen und Anwendungen.

In der vorliegenden Arbeit wird die folgende Definition 2-3 nach Podgorelec u. a. (2022) einer Wallet zugrunde gelegt.

Definition 2-3: Wallet

Eine Wallet ist ein Software-System, in dem Benutzer ihre identitätsbezogenen Daten selbstbestimmt speichern und verwalten können. Die gespeicherten identitätsbezogenen Daten können durch Benutzer in der Wallet selbstbestimmt selektiert und mit Prüfern geteilt werden. Die Wallet ermöglicht außerdem die sichere Speicherung der zu den identitätsbezogenen Daten zugehörigen kryptografischen Daten.

Krauß u. a. (2023b) betrachteten 6 verschiedene Wallets und identifizierten 12 Kernfunktionen (AF1-AF12), die sie 4 Kategorien zuordneten:

Kategorie: Allgemein (nach Krauß u. a. (2023b))

(AF1) Übersicht von gespeicherten VC: In der Wallet werden die von den Benutzern gespeicherten VC aufgelistet.

(AF2) Detailansicht von gespeicherten VC: Benutzer können Details zu jedem gespeicherten VC in der Wallet einsehen.

(AF3) Zurücksetzen der Wallet: Gespeicherte VC können mit einer Benutzerinteraktion in der Wallet gelöscht werden.

(AF4) Hilfe & häufig gestellte Fragen: Die Wallet besitzt einen Hilfe-Bereich und/oder einen Bereich, in dem häufig gestellte Fragen beantwortet werden.

(AF5) Backup: Die Wallet besitzt eine Funktion, mit der Benutzer ein Backup ihrer identitätsbezogenen Daten erstellen können, wie beispielsweise von VC oder Kontakten/Verbindungen zu Ausstellern und Prüfern.

(AF6) Wiederherstellung: Die Wallet besitzt eine Funktion, um Backup-Daten wiederherzustellen.

Kategorie: Komfort (nach Krauß u. a. (2023b))

(AF7) Suche: Die Wallet besitzt eine Suchfunktion, mit der nach gespeicherten VC und Verbindungen zu Ausstellern sowie Prüfern gesucht werden kann.

(AF8) Favoriten: Benutzer können in der Wallet gespeicherte VC als Favoriten kennzeichnen, um schnelleren Zugriff zu erhalten.

(AF9) Automatische Vorauswahl: Benutzer erhalten bei einer eingehenden Datenanfrage in der Wallet eine Vorauswahl an geeigneten Daten aus gespeicherten VC.

Kategorie: Sicherheit (nach Krauß u. a. (2023b))

(AF10) Schutz der Wallet: Die Wallet enthält einen gesicherten Zugangsmechanismus zum Entsperren. Dabei stehen den Benutzern mehrere Möglichkeiten (beispielsweise PIN, Kennwort, Biometrie, etc.) zur Verfügung, aus denen sie auswählen können.

Kategorie: Transparenz (nach Krauß u. a. (2023b))

(AF11) Historie: In der Wallet werden alle Interaktionen mit Ausstellern und Prüfern aufgelistet und chronologisch geordnet.

(AF12) Übersicht je Aussteller und Prüfer: Die Wallet beinhaltet eine Auflistung aller Interaktionen je Aussteller und Prüfer. Diese Auflistung ist somit eine gefilterte Ansicht der Historie (AF11).

Zusätzlich zu der in dieser Arbeit fokussierten Wallet-Art (Digital Identity Wallets) existieren noch weitere Wallet-Arten, die im Folgenden abgegrenzt werden:

In **Cryptocurrency Wallets** (dt. Kryptowährung-Wallets) lassen sich Kryptowährungen verwalten und Transkationen durchführen (Senden und Empfangen von Kryptowährungen). Hierzu kommuniziert die Cryptocurrency Wallet mit einer Blockchain, indem sie öffentliche und private Schlüssel speichert, die für das Senden und Empfangen von Kryptowährungen erforderlich sind (Suratkar u. a., 2020). Im Gegensatz zu Digital Identity Wallets lassen sich in Cryptocurrency Wallets keine VC speichern. Beispiele für Cryptocurrency Wallets sind die Trust Wallet[9], Coinbase Wallet[10] und die MetaMask Wallet[11].

Mit der **Apple Wallet**[12] und **Google Wallet**[13] lassen sich mobile Zahlungen durchführen. Zusätzlich können darin Kreditkarten, Kundenkarten, Eintrittskarten, Bordkarten, Geschenkkarten und E-Autoschlüssel gespeichert werden (Apple Inc., 2024; Google LLC, 2024). Des Weiteren erlaubt die Apple Wallet lediglich das Speichern bestimmter Nachweise, wie beispielsweise Mitarbeiterausweise. Ferner lassen sich in limitierten Regionen der Führerschein und Personalausweis in der Apple Wallet speichern (Apple Inc., 2024). Im Vergleich zu Digital Identity Wallets fokussieren sich die Apple Wallet und Google Wallet auf das digitale Bezahlen. Zusätzlich lassen sich in der Apple Wallet und Google Wallet nur limitierte, bestimmte Nachweise speichern.

[9] https://trustwallet.com
[10] https://coinbase.com
[11] https://metamask.io
[12] https://apple.com/wallet
[13] https://wallet.google/intl/de_de

Mit **Banking Wallets** lassen sich Finanzen verwalten und Zahlungen tätigen. Der Begriff „Banking Wallet“ wurde selbst definiert, da in der Literatur kein gängiger Begriff gefunden werden konnte. Beispiele für Banking Wallets sind die OpenBank Wallet[14] und die Paypal Wallet[15]. Im Gegensatz zu Digital Identity Wallets lassen sich darin keine VC speichern, sondern Finanzen verwalten und Zahlungen tätigen.

Tabelle 2 fasst die beschriebenen Merkmale der Wallet-Arten zusammen.

	Verwendungszweck	**Gespeicherte Daten**	**Beispiele**
Digital Identity Wallet	Verwaltung von VC	Jegliche VC, wie Personalausweis, Reisepass, Führerschein, Shopping-Präferenzen oder Kundenkarten	Hidy Wallet[16], Lissi Wallet[17]
Cryptocurrency Wallet	Verwaltung von Kryptowährungen	Private Schlüssel, Kryptowährungsadressen, Transaktionen	Trust Wallet[9], Coinbase Wallet[10], MetaMask Wallet[11]
Apple Wallet und Google Wallet	Kontaktloses Bezahlen, Verwaltung von Zahlungsmethoden und bestimmten VC	Kredit/-Debitkarten, Kundenkarten, Eintrittskarten, Bordkarten, Geschenkkarten und E-Autoschlüssel	Apple Wallet[12], Google Wallet[13]
Banking Wallet	Finanzverwaltung und Zahlungen tätigen	Finanzdaten von verschiedenen Bankkonten	Openbank Wallet[14], Paypal[15]

Tabelle 2: Vergleich von Wallet-Arten

2.5 Technologien und Standards

Im Kontext digitaler Identitäten (siehe Abschnitt 2.1), VC (siehe Abschnitt 2.2), deren Rollen und Anforderungen (siehe Abschnitt 2.3) und Wallets (siehe Abschnitt 2.4) werden verschiedene Technologien und Standards eingesetzt:

[14] https://openbank.de/app-wallet-mobiles-bezahlen
[15] https://paypal.com/de/digital-wallet
[16] https://hidy.eu
[17] https://lissi.id

Ein Decentralized Identifier (DID) ist eine eindeutige Adresse für Entitäten und dient zur Authentifizierung sowie dem Austausch von VC. Die Erstellung und Verwaltung eines DID erfolgt dezentral und ist von keiner zentralen Autorität abhängig. Entitäten können mehrere DIDs erzeugen und eigenständig verwalten. Ein DID identifiziert eine spezifische Ressource, das sogenannte DID-Dokument. Das DID-Dokument ist ein JSON-Objekt, das öffentliche Schlüssel, Eigenschaften und Metainformationen des Inhabers enthält. Der sogenannte DID-Resolver löst ein DID auf und gibt das zugehörige DID-Dokument zurück. Ein DID besteht aus 3 Komponenten: Schema, DID-Methode und methodenspezifischer Identifikator. Die erste Komponente legt das Schema „did“ fest. Die zweite Komponente gibt die DID-Methode an, die verwendet wird, um den DID zu erstellen, aufzulösen, zu aktualisieren und zu widerrufen. Die dritte Komponente ist ein eindeutiger Identifier der DID-Methode (Sporny u. a., 2022). Ein Beispiel einer DID lautet: „did:example:abcdefg1234567“.

Jeder Inhaber eines DID erstellt ein asymmetrisches Schlüsselpaar (privater und öffentlicher Schlüssel). Der private Schlüssel wird sicher beim Inhaber gespeichert, beispielsweise in einer Wallet (siehe Abschnitt 2.4). Der öffentliche Schlüssel wird im DID-Dokument gespeichert. Dadurch kann der Inhaber nun kryptografisch, durch die Nutzung des asymmetrischen Schlüsselpaares (beispielsweise mittels einem Challenge-Response-Verfahren), den Besitz des DID nachweisen (Pohlmann, 2022). So ist es möglich, den Inhaber und den Aussteller eines VC zu verifizieren, da ein DID im VC gespeichert werden kann.

Ehrlich u. a. (2021) definieren eine Verifiable Data Registry (VDR) eines SSI-Ökosystems. Ein SSI-Ökosystem besteht aus verschiedenen Akteuren, wie Aussteller, Inhaber und Prüfer von VC (siehe Abschnitt 2.2) sowie Technologien und Standards (siehe Abschnitt 2.5) für selbstbestimmte Identitäten (siehe Abschnitt 2.1). „Eine Verifiable Data Registry (VDR) ist ein dezentrales Datenregister, das im SSI-Ökosystem als eine Vertrauensschicht fungiert, um unter anderem einen vertrauenswürdigen Austausch von öffentlichen Schlüsseln der Aussteller zu gewährleisten“ (Pohlmann, 2022). In einer VDR können DIDs, Informationen über Verifizierungsmechanismen zur Überprüfung von VC, Schemata von VC und Gültigkeitsdefinitionen gespeichert werden. Da eine VDR eine hohe Verfügbarkeit und Skalierbarkeit aufweisen sowie resistent gegen Manipulationen sein muss, können Blockchains als VDR verwendet werden (Ehrlich u. a., 2021).

Abbildung 5 visualisiert den Zusammenhang der erläuterten Technologien und Standards und erweitert Abbildung 2 der SSI-Rollen. Hierbei meint die Integrität eines VC, dass die übertragenen Daten nicht verändert wurden.

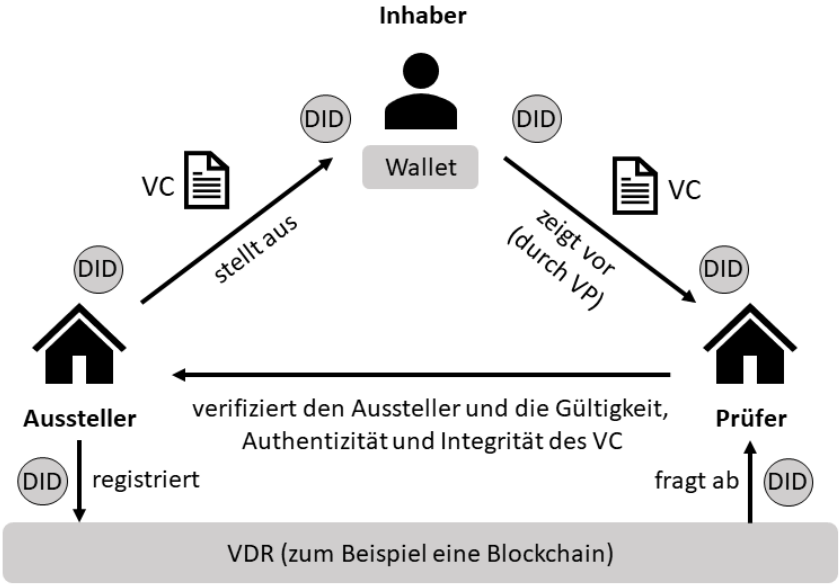


Abbildung 5: DID, VC und VDR. (Pohlmann, 2022). Begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

3 Grundlagen: User Experience

Dieses Kapitel beschreibt die Grundlagen der User Experience. Zunächst wird der Begriff User Experience in Abschnitt 3.1 definiert. Danach erfolgt eine Beschreibung des Begriffs Usability in Abschnitt 3.2. Der darauffolgende Abschnitt 3.3 beschreibt den Prozess des Human-Centered Designs, mit dem eine möglichst gute User Experience gestaltet werden kann. Der letzte Abschnitt 3.4 erläutert Dark Patterns, durch die Benutzer zu ungewollten Handlungen verleitet werden können.

3.1 Definition

User Experience (UX) beschreibt die „Wahrnehmungen und Reaktionen einer Person, die aus der tatsächlichen und/oder der erwarteten Benutzung eines Systems, eines Produkts oder einer Dienstleistung resultieren“ (DIN EN ISO 9241-210:2020-03, 2020). Als Wahrnehmungen und Reaktionen werden „Emotionen, Vorstellungen, Vorlieben, Wahrnehmungen, Wohlbefinden oder Unbehagen, Verhaltensweisen und Leistungen“ (DIN EN ISO 9241-210:2020-03, 2020) verstanden. UX „ist eine Folge des Markenbilds, der Darstellung, Funktionalität, Systemleistung, des interaktiven Verhaltens und der Unterstützungsmöglichkeiten eines Systems, eines Produkts oder einer Dienstleistung. Sie ergibt sich auch aus dem psychischen und physischen Zustand des Benutzers aufgrund seiner Erfahrungen, Einstellungen, Fähigkeiten, Möglichkeiten und seiner Persönlichkeit sowie des Nutzungskontextes“ (DIN EN ISO 9241-11:2018, 2018). Zu Benutzern eines Systems, eines Produkts oder einer Dienstleistung zählen Personen, die dieses betreiben, Personen, die dessen Ergebnisse nutzen, und Personen, die den Betrieb unterstützen (einschließlich durch Wartung und Schulung) (DIN EN ISO 9241-210:2020-03, 2020).

UX ist ein momentanes, wertendes Gefühl (positiv oder negativ) während der Interaktion mit einem Produkt oder einer Dienstleistung. Menschen nehmen interaktive Produkte in 2 unterschiedlichen Dimensionen wahr: die pragmatische und die hedonische Qualität. Die erste Dimension ist die pragmatische Qualität, die sich auf die wahrgenommene Fähigkeit des Produkts zum Erreichen von sogenannten „Tun-Zielen“ bezieht. Diese „Tun-Ziele“ sind Ziele von Benutzern, damit sie Aufgaben erfolgreich ausführen können, wie beispielsweise einen Anruf tätigen. Die zweite Dimension ist die hedonische Qualität, welche die durch Benutzer wahrgenommene Fähigkeit eines Produkts beschreibt, sogenannte „Sein-Ziele“ zu erfüllen. „Sein-Ziele“ beschreiben den mentalen Zustand sowie emotionale und persönliche Ziele, die Benutzer vor, während oder nach der Nutzung erreichen (Hassenzahl, 2008). Ein Beispiel für ein „Sein-Ziel“ ist, wenn sich ein Benutzer

gesund fühlt, da er die maximale Anzahl an Kalorien pro Tag nicht überschreitet und die Fitness-Applikation ihn darüber informiert.

Nach Morville (2005) hat UX 7 Attribute:

Utility (dt. Nützlichkeit) beschreibt das Ausmaß der Eignung, des Nutzens und der Zweckdienlichkeit eines Systems (Nielsen, 1993). Beispielsweise ist ein Navigationssystem nützlich, wenn für gewünschte Zielorte passende Routen gefunden werden.

Desirability (dt. Begehrlichkeit) beschreibt, inwiefern Benutzer ein System, Produkt oder eine Dienstleistung positiv und attraktiv wahrnehmen (Rosenbaum u. a., 2008). Beispielsweise erhöhte sich die Begehrlichkeit einer neuen Videoschnittsoftware, als die Videoproduzenten die leistungsstarken Bearbeitungsfunktionen und die regelmäßigen Updates zur Verbesserung der Stabilität und Performance entdeckten.

Findability (dt. Auffindbarkeit) beschreibt das Ausmaß, in dem Benutzer gesuchte Elemente auffinden können (Rosenbaum u. a., 2008). Beispielsweise wurde eine Suche in die Webseite einer Universität integriert, damit Studierende direkt nach den jeweiligen Prüfungsordnungen suchen können. Daraus folgt eine höhere Auffindbarkeit.

Usability (dt. Benutzerfreundlichkeit) beschreibt das „Ausmaß, in dem ein System, ein Produkt oder eine Dienstleistung durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“ (DIN EN ISO 9241-11:2018, 2018). Beispielsweise wurde eine Bildungssoftware durch eine klare Navigation, gut lesbaren Text und verständliche Schaltflächen verbessert. Daraus folgt eine höhere Usability.

Accessibility (dt. Barrierefreiheit) beschreibt den „Umfang, in dem Produkte, Systeme, Dienstleistungen, Umgebungen und Einrichtungen durch Menschen aus einer Bevölkerungsgruppe mit den weitesten Benutzererfordernissen, Merkmalen und Fähigkeiten genutzt werden können, um identifizierte Ziele in identifizierten Nutzungskontexten zu erreichen. Ziel des Entwurfs im Hinblick auf die Barrierefreiheit ist die Erweiterung der Zielgruppe, sodass die Produkte, Systeme, Dienstleistungen, Umgebungen und Einrichtungen einem größeren Personenkreis in unterschiedlicheren Nutzungskontexten zur Verfügung stehen“ (DIN EN ISO 9241-11:2018-11, 2018). In Abgrenzung zu Benutzeranforderungen beschreiben Benutzererfordernisse die Bedürfnisse und Ziele der Benutzer, unabhängig von einer spezifischen Lösung, während Benutzeranforderungen spezifische Funktionen und Eigenschaften festlegen, die ein System, Produkt oder eine Dienstleistung besitzen muss, um die Benutzererfordernisse zu erfüllen. „Weiteste Benutzererfordernisse“ meinen in diesem Kontext, dass nicht nur die Benutzererfordernisse einer bestimmten Gruppe von Menschen erfüllt werden, sondern auch die Vielfalt an Benutzererfordernisse aller Menschen berücksichtigt werden, beispielsweise auch von

Menschen mit körperlichen Beeinträchtigungen. Beispielsweise besitzen die Betriebssysteme Windows und MacOS Sprachausgaben, damit sie auch von Menschen mit Blindheit verwendet werden können.

Credibility (dt. Glaubwürdigkeit) beschreibt das Ausmaß, inwiefern Benutzer ein System, ein Produkt oder eine Dienstleistung vertrauenswürdig finden (Rosenbaum u. a., 2008). Beispielsweise besitzt eine Webseite verifizierte Kundenbewertungen, sodass die Glaubwürdigkeit erhöht wird.

Value (dt. Wert) beschreibt den Mehrwert, der durch die Nutzung eines Systems, eines Produkts oder einer Dienstleistung resultiert (Rosenbaum u. a., 2008). Beispielsweise wurde die Gesichtserkennung als Authentisierungsmethode in ein Software-System implementiert. Dies erhöht den Wert, da sich Benutzer schneller authentisieren können. Es wird ein Mehrwert gegenüber anderen Software-Systemen geschaffen.

Abbildung 6 visualisiert die beschriebenen Attribute der UX.

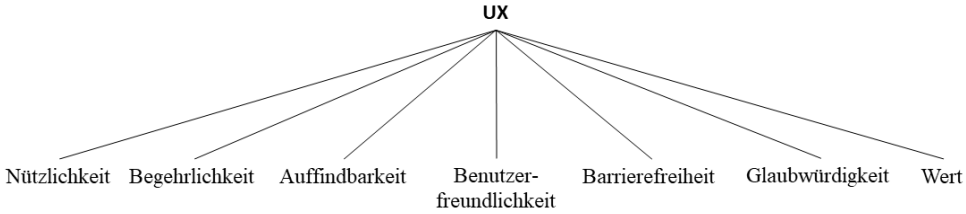


Abbildung 6: UX-Attribute. Zusammengefasst nach Morville (2005).

In der vorliegenden Arbeit wird die folgende Definition 3-1 der UX zugrunde gelegt.

Definition 3-1: UX

UX ist ein momentanes, wertendes Gefühl (positiv oder negativ). UX beschreibt Wahrnehmungen und Reaktionen der Benutzer von Systemen, Produkten oder Dienstleistungen vor, während und nach der Nutzung. UX ist eine Folge des Markenbilds, der Darstellung, Funktionalität, Systemleistung, des interaktiven Verhaltens und der Unterstützungsmöglichkeiten eines Systems, eines Produkts oder einer Dienstleistung. UX ergibt sich auch aus dem psychischen und physischen Zustand des Benutzers aufgrund seiner Erfahrungen, Einstellungen, Fähigkeiten, Möglichkeiten und seiner Persönlichkeit sowie des Nutzungskontextes. Attribute der UX sind Nützlichkeit, Begehrlichkeit, Auffindbarkeit, Usability, Barrierefreiheit, Glaubwürdigkeit und Wert.

Da die Usability teilweise mit der UX verwechselt wird und einige Evaluationsverfahren lediglich die Usability betrachten, ohne gesamthaft die UX zu bewerten (vgl. Brooke, 1996; Wharton u. a., 1994), wird die Usability im folgenden Abschnitt 3.2 weiter erläutert und von der UX abgegrenzt.

3.2 Usability

Die Usability ist das „Ausmaß, in dem ein System, ein Produkt oder eine Dienstleistung durch bestimmte Benutzer in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen“ (DIN EN ISO 9241-11:2018, 2018). Dabei wird explizit von „bestimmten“ Benutzern, einem „bestimmten“ Nutzungskontext und „bestimmten“ Zielen gesprochen, da diese explizit zur Betrachtung der Usability eines Systems, Produkts oder Dienstleistung festgelegt werden müssen. Die Usability variiert zwischen unterschiedlichen Benutzern, da sie von den Eigenschaften, Fähigkeiten und anderen individuellen Unterschieden der Benutzer und von der jeweiligen Aufgabe, die sie ausführen, abhängen (DIN EN ISO 9241-11:2018, 2018). Beispielsweise hat eine Entwicklungsumgebung für Softwareentwickler einen hohen Grad an Usability, für Pflegepersonal dagegen einen niedrigen Grad an Usability.

Nach der DIN EN ISO 9241-11:2018 (2018) hat die Usability 3 Attribute:

Effectivity (dt. Effektivität) ist „das Ausmaß der Übereinstimmung von tatsächlichen und angestrebten Ergebnissen“ (DIN EN ISO 9241-11:2018, 2018). Sie besteht aus der Vollständigkeit und Genauigkeit, mit denen Benutzer bestimmte Ziele erreichen. Die Vollständigkeit ist „das Ausmaß, in dem die Benutzer des Systems, des Produkts oder der Dienstleistung in der Lage sind, alle angestrebten Ergebnisse zu erreichen“ (DIN EN ISO 9241-11:2018, 2018). Beispielsweise prüft eine Person X vor dem Zoo-Besuch, ob der Zoo geöffnet ist, und findet die gesuchte Öffnungszeit auf der Webseite des Zoos. Die Genauigkeit ist „der Grad der Übereinstimmung eines tatsächlichen mit einem angestrebten Ergebnis“ (DIN EN ISO 9241-11:2018, 2018). Beispielsweise möchte eine Person Y einen Film aufnehmen, was ihr mithilfe der Aufnahmefunktion des Smart-TVs gelingt.

Efficiency (dt. Effizienz) meint „die im Verhältnis zu den erreichten Ergebnissen eingesetzten Ressourcen“ (DIN EN ISO 9241-11:2018, 2018). Ressourcen sind beispielsweise „Zeit, menschlicher Aufwand, Geld und Materialien“ (DIN EN ISO 9241-11:2018, 2018), die üblicherweise im Nutzungskontext verbraucht werden. Beispielsweise löscht eine Person X jede Tabellenspalte einzeln, ohne zu wissen, dass die Tabelle gesamthaft löschbar ist. Die Art und Weise der Nutzung durch Person X ist effektiv, allerdings ist das Löschen der einzelnen Tabellenspalten ineffizienter als die gesamte Tabelle auf einmal zu löschen.

Satisfaction (dt. Zufriedenstellung) „ist das Ausmaß, in dem die physischen, kognitiven und emotionalen Reaktionen des Benutzers, die aus der Benutzung eines Systems, eines Produkts oder einer Dienstleistung resultieren, in Übereinstimmung mit den Benutzererfordernissen und Benutzererwartungen“ (DIN EN ISO 9241-11:2018, 2018). Physische Reaktionen beschreiben „Gefühle des Wohlbefindens oder Unbehagens“ (DIN EN ISO

9241-11:2018, 2018). Beispielsweise kann eine Abnahme der Sehkraft durch eine erhöhte Bildschirmzeit folgen. Kognitive Reaktionen beschreiben „Einstellungen, Vorlieben und Wahrnehmungen […]. Sie ergeben sich aus der Erfahrung aufgrund der Nutzung des Betrachtungsgegenstands und können auch durch die Erfahrungen mit ähnlichen Systemen und durch die Meinungen anderer Personen beeinflusst werden“ (DIN EN ISO 9241-11:2018, 2018). Beispielsweise schwärmt eine Person X von ihrem neuen Smartphone. Eine Person Y wird durch Person X beeinflusst und kauft sich das gleiche Smartphone. Emotionale Reaktionen beschreiben die Gesamtheit des Gefühl- und Gemütslebens, die sich aus Stimmung, Emotion und Motivation zusammensetzt. Beispielsweise kann ein Computerspiel Aufregung und Neugierde bei einer Person X hervorrufen.

Nach Nielsen (1993) beinhaltet die Usability zusätzlich zu den bereits genannten Attributen noch die Attribute Lernfähigkeit, Einprägsamkeit und Fehler:

Learnability (dt. Lernfähigkeit) beschreibt die Fähigkeit, neues Wissen, Fähigkeiten oder Verhaltensweisen zu erwerben, sodass Benutzer schnell mit einem System arbeiten können (Nielsen, 1993). Beispielsweise beinhaltet ein Software-System interaktive Tutorials, die es Benutzern erleichtern, Funktionen des Software-Systems zu erlernen.

Memorability (dt. Einprägsamkeit) beschreibt das Ausmaß, inwiefern sich Benutzer an die Interaktion mit einem System, Produkt oder einer Dienstleistung erinnern und diese bei zukünftiger Interaktion ohne Schwierigkeiten wiederverwenden können (Nielsen, 1993). Beispielsweise kann sich eine Person X nach einem Jahr der letzten Benutzung problemlos einloggen, da der Button „Anmelden mit Dienst Y“ sofort erkennbar ist.

Errors (dt. Fehleranfälligkeit) beschreibt die Fehler des Benutzers, die bei der Interaktion mit einem System, Produkt oder Dienstleistung zur Nicht-Erreichung von gewünschten Zielen führen. Fälschlicherweise durchgeführte Aktionen, die durch Benutzer schnell korrigiert werden können und dennoch zur Zielerreichung führen, werden als geringfügige Fehler beschrieben und nicht in die Bewertung eingeschlossen, da diese bereits von der Effizienz inkludiert werden (Nielsen, 1993). Beispielsweise nutzt eine Person X eine Online-Bestellplattform und möchte ihre Lieferadresse aktualisieren. Nach dem Speichern wird jedoch versehentlich die Rechnungsadresse geändert, da beide Eingabefelder ähnlich benannt und ohne klare visuelle Trennung dargestellt sind. Der Fehler bleibt zunächst unbemerkt und führt später zur Zustellung der Rechnung an die falsche Adresse.

Abbildung 7 visualisiert die beschriebenen Usability-Attribute und erweitert die UX-Attribute aus Abbildung 6. Die Effektivität umfasst die Fehleranfälligkeit, sodass auf eine separate Aufführung der Fehleranfälligkeit in Abbildung 7 verzichtet wurde.

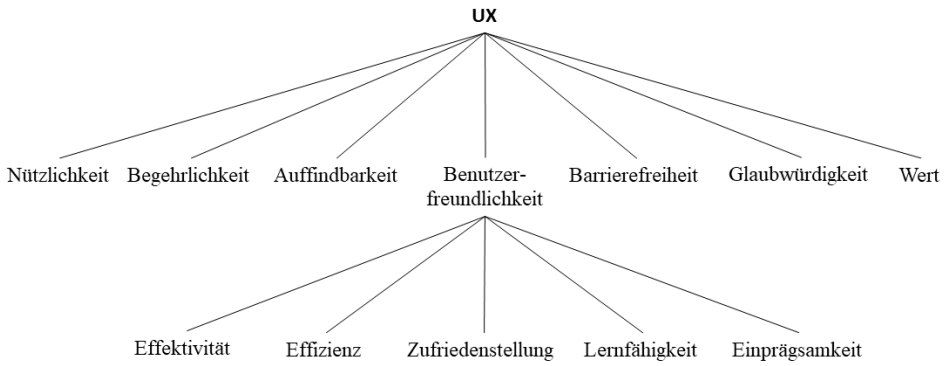


Abbildung 7: UX- und Usability-Attribute. Zusammengefasst nach DIN EN ISO 9241-11 (2018), Morville (2005) und Nielsen (1993).

In der vorliegenden Arbeit wird die folgende Definition 3-2 der Usability zugrunde gelegt.

Definition 3-2: Usability

Usability ist das Ausmaß, in dem Benutzer ihre Ziele in einem System, Produkt oder Dienstleistung effektiv, effizient, zufriedenstellend, leicht erlernbar und einprägsam erreichen können. Die Usability kann bei unterschiedlichen Nutzungskontexten und Benutzern variieren. Attribute der Usability sind Effektivität, Effizienz, Zufriedenstellung, Lernfähigkeit und Einprägsamkeit.

Um eine möglichst gute UX (und damit eine möglichst gute Usability) zu erreichen, lässt sich das Human-Centered Design nach DIN EN ISO 9241-210:2020-03 (2020) verwenden. Dieses wird in Abschnitt 3.3 erläutert.

3.3 Human-Centered Design

Entwurfsentscheidungen haben einen wesentlichen Einfluss auf die UX. Das Human-Centered Design (HCD, dt. Menschenzentrierte Gestaltung) zielt darauf ab, eine möglichst gute UX zu erreichen, indem Produkte, Systeme und Dienstleistungen unter stetiger Berücksichtigung der menschlichen Bedürfnisse entworfen werden (DIN EN ISO 9241-210:2020-03, 2020): „Menschzentrierte Gestaltung ist ein Ansatz zur Entwicklung interaktiver Systeme, der darauf abzielt, Systeme gebrauchstauglich und zweckdienlich zu machen, indem er sich auf die Benutzer, deren Erfordernisse und Anforderungen konzentriert und menschliche Faktoren/Ergonomie sowie Kenntnisse und Techniken zur Gebrauchstauglichkeit anwendet“ (DIN EN ISO 9241-210:2020-03, 2020).

Nach der DIN EN ISO 9241-210:2020-03 (2020) bestehen 6 Grundsätze des HCD:

Der Systementwurf basiert auf einem umfassenden Verständnis der Benutzer, Aufgaben und Arbeitsumgebungen: Der Systementwurf erfolgt kontextabhängig, da Benutzer spezifische Aufgaben in spezifischen Arbeitsumgebungen verfolgen (DIN EN ISO 9241-210:2020-03, 2020). Beispielsweise kann das Videokonferenz-Tool, mit dem ein Benutzer von Zuhause mit Freunden kommuniziert, eine möglichst gute UX aufweisen. Dahingegen kann sich die UX des Videokonferenz-Tools für einen Geschäftsführer im Arbeitsalltag als miserabel herausstellen.

Die Benutzer werden in den Systementwurf und in die Entwicklung miteinbezogen: Benutzer sollten in den Systementwurf und die Entwicklung eingebunden sein, indem sie beispielsweise in der Evaluation des Systementwurfs involviert sind. Die Benutzer sollten ein breites Spektrum an Fähigkeiten, Eigenschaften und Erfahrungen repräsentieren, die die Vielfalt der Benutzer im realen Betrieb widerspiegeln. Die Art und Häufigkeit dieser Einbindung können je nach Art des Projekts während des Entwicklungsprozesses variieren (DIN EN ISO 9241-210:2020-03, 2020).

Die Verfeinerung und Anpassung des Systementwurfs erfolgen fortlaufend mittels benutzerzentrierter Evaluation: Benutzerfeedback ist entscheidend für einen benutzerzentrierten Systementwurf, damit der Systementwurf die Benutzeranforderungen erfüllt. Der Systementwurf sollte fortlaufend durch Benutzerfeedback angepasst werden, das heißt, vom ersten bis zum finalen Systementwurf (DIN EN ISO 9241-210:2020-03, 2020).

Der Prozess der HCD verläuft iterativ: Der Prozess der HCD verläuft üblicherweise iterativ, da die Benutzeranforderungen zu Beginn der Entwicklung schwer zu erheben sind. Während des Entwicklungsprozesses können einige Anforderungen und Erwartungen von Benutzern und anderen Beteiligten erst im Laufe der Zeit deutlich werden (DIN EN ISO 9241-210:2020-03, 2020).

Die gesamte UX wird berücksichtigt, nicht nur die Usability: Im Prozess der HCD sollte nicht nur die Usability berücksichtigt werden, sondern weitergefasst die UX. Das heißt, es sollten beispielsweise auch Erfahrungen des Benutzers mit vorherigen oder anderen Systemen und Fragestellungen (wie Markenkennzeichnung und Werbung) beim Systementwurf bedacht werden (DIN EN ISO 9241-210:2020-03, 2020). Um eine möglichst gute UX zu erreichen, ist „die Berücksichtigung organisatorischer Auswirkungen, Benutzerdokumentation, Online-Hilfe, unterstützende Betreuung und Instandhaltung (einschließlich Beratung und Kundenkontaktstellen), Schulung, langfristiger Gebrauch, und Produktverpackung (einschließlich der Eindrücke bei der ersten Inbetriebnahme)“ (DIN EN ISO 9241-210:2020-03, 2020) essentiell.

Fachübergreifende Kompetenzen und Gesichtspunkte fließen in den Systementwurf ein: Die Teamzusammensetzung der Personen, die sich mit dem Systementwurf beschäf-

tigen, sollte multidisziplinär sein, damit beispielsweise Kompromissentscheidungen mit umfassender Expertise diskutiert werden können. Ein zusätzlicher Vorteil eines multidisziplinären Teams ist, dass die Teammitglieder ein besseres Verständnis für die Einschränkungen und Realitäten der anderen Fachbereiche entwickeln (DIN EN ISO 9241-210:2020-03, 2020). Beispielsweise können Marketingexperten den Entwicklern dabei helfen, die Benutzerbedürfnisse und Marktpräferenzen besser zu verstehen. Gleichzeitig können Entwickler den Marketingexperten technische Einschränkungen und Machbarkeit von Marketingstrategien aufzeigen.

Der Prozess des HCD beinhaltet 4 miteinander verbundene Aktivitäten (DIN EN ISO 9241-210:2020-03, 2020):

Verständnis und Beschreibung des Nutzungskontexts: Der Nutzungskontext wird durch „Benutzermerkmale, Aufgaben und die organisatorische, technische und physische Umgebung“ (DIN EN ISO 9241-210:2020-03, 2020) bestimmt. Um den Nutzungskontext für das zukünftige System zu bestimmen, ist es ratsam, Informationen über den aktuellen Nutzungskontext zu sammeln und zu analysieren. Dies kann durch die Untersuchung bestehender oder ähnlicher Systeme, Produkte oder Dienstleistungen erfolgen. Fragen und Probleme können dadurch im Nutzungskontext identifiziert werden. Außerdem können Leistungs- und Zufriedenheitsniveaus festgelegt werden. Diese Informationen sind entscheidend, um sicherzustellen, dass Bedürfnisse, Probleme und Einschränkungen des Nutzungskontexts erfüllt werden. Die Beschreibung des Nutzungskontexts muss dabei die Ziele und Einschränkungen von Benutzern oder Benutzergruppen sowie von weiteren Stakeholdern enthalten. Außerdem müssen die Merkmale der Benutzer oder Benutzergruppen in der Beschreibung dokumentiert sein, wie beispielsweise Gewohnheiten, Vorlieben und Fertigkeiten. Des Weiteren soll die Beschreibung die Ziele der Benutzer oder Benutzergruppen und die Gesamtziele des Systems, des Produkts oder der Dienstleistung enthalten. Lösungen für Ziele, die im Konflikt stehen, sollten dokumentiert werden. Außerdem müssen die Merkmale der Aufgaben der Benutzer oder Benutzergruppen vorliegen, wie beispielsweise die Art, in der Benutzer typischerweise Aufgaben ausführen, die Häufigkeit, die Zeitdauer, die Abhängigkeiten oder parallel auszuführende Aufgaben. Ferner sollte die Umgebung des Systems beschrieben werden, das heißt, die technische Umgebung (zum Beispiel Hardware oder Software), die physikalische Umgebung (zum Beispiel thermische Bedingungen, Beleuchtung oder Raumgestaltung) sowie die soziale und kulturelle Umgebung (zum Beispiel Arbeitsweise, Organisationsstruktur oder Einstellungen) (DIN EN ISO 9241-210:2020-03, 2020).

Spezifikation der Nutzungsanforderungen: Nutzungsanforderungen von Benutzern und weiteren Stakeholdern müssen auf Basis des Nutzungskontexts identifiziert werden. Diese sollten die Ziele der Benutzer und Einschränkungen durch den Nutzungskontext enthalten. Konflikte zwischen Nutzungsanforderungen (zum Beispiel zwischen Ge-

schwindigkeit und Genauigkeit) sollten gelöst und dokumentiert werden. Zudem sollten die Nutzungsanforderungen so definiert werden, dass eine nachfolgende Prüfung möglich ist. Außerdem sollten die Nutzungsanforderungen durch relevante Benutzer und Stakeholder verifiziert sein, während der Projektdauer aktualisiert werden und in sich widerspruchsfrei sein (DIN EN ISO 9241-210:2020-03, 2020).

Erarbeitung des Systementwurfs: Die Erarbeitung eines Systementwurfs beinhaltet 4 wesentliche Teilaktivitäten. Zunächst sollten Benutzeraufgaben, die Mensch-Maschine-Interaktion (Human-Computer-Interaction, HCI) und die Benutzungsschnittstelle zur Erfüllung der Nutzungsanforderungen entworfen und modelliert werden. Anschließend sollte der Systementwurf konkretisiert werden, etwa durch Prototypen, Modelle oder Simulationen. Danach sollte der Systementwurf auf Basis der gewonnenen Erkenntnisse angepasst werden. Abschließend wird der Systementwurf an diejenigen übermittelt, die für die Umsetzung verantwortlich sind (DIN EN ISO 9241-210:2020-03, 2020). Beim Systementwurf sollen die Grundsätze nach DIN EN ISO 9241-110:2020-10 (2020) berücksichtigt werden: „Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Konformität mit Benutzererwartungen, Lernförderlichkeit, Steuerbarkeit, Fehlertoleranz und Individualisierbarkeit“ (DIN EN ISO 9241-210:2020-03, 2020).

Evaluation des Systementwurfs: Der Systementwurf sollte bereits früh in der Entwicklung evaluiert werden, damit ein besseres Verständnis der Benutzeranforderungen gewonnen werden kann. Außerdem können durch die Evaluation neue Informationen über die Stärken und Schwächen des Systementwurfs sowie die Erfüllung von Benutzeranforderungen erhoben werden. Ferner können Vergleiche zwischen Systementwürfe durchgeführt werden (DIN EN ISO 9241-210:2020-03, 2020).

Abbildung 8 visualisiert die beschriebenen Aktivitäten.

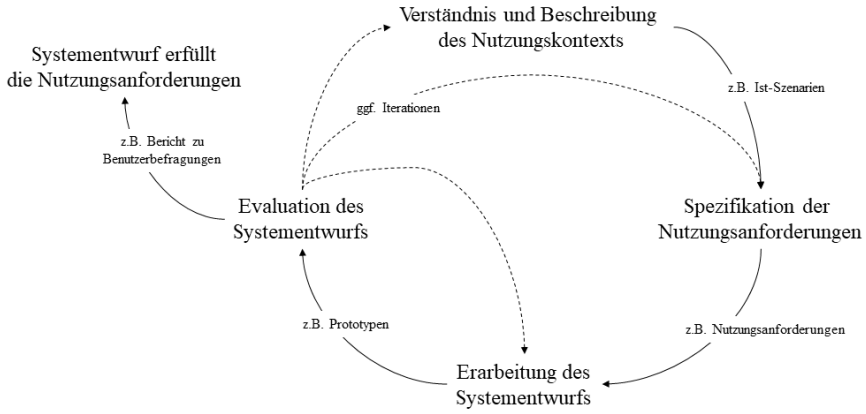


Abbildung 8: Human-Centered Design. (DIN EN ISO 9241-210, 2020). Begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Durch den Entwurf von Systemen mittels HCD kann sich die Gesamtqualität der Systeme erhöhen, die Wirtschaftlichkeit von Organisationen verbessern, die Produktivität der Benutzer erhöhen und es können Wettbewerbsvorteile entstehen (DIN EN ISO 9241-210:2020-03, 2020).

3.4 Dark Patterns

„Dark Patterns sind Entwurfsentscheidungen eines User Interface, die einen Online-Dienst begünstigen, indem sie Benutzer zu unbeabsichtigten und potenziell schädlichen Entscheidungen zwingen, lenken oder täuschen“ [aus dem Englischen übersetzt nach Mathur u. a. (2019)].

Gray u. a. (2018) unterscheiden zwischen 5 Arten von Dark Patterns:

Nagging (dt. Gezeter) meint eine subtile Ablenkung von der erwarteten Funktionalität, die sich über mindestens eine Interaktion von Benutzern hinweg erstrecken kann. Nagging äußert sich häufig als wiederholte Störung während der Interaktion(en) von Benutzern, wobei die gewünschte Aufgabe der Benutzer durch andere, nicht direkt damit verbundene Aufgaben unterbrochen wird. Nagging kann verschiedene Formen annehmen, wie beispielsweise Pop-Ups, welche das User Interface überlagern, Audio-Benachrichtigungen, die den Benutzer ablenken, oder andere Aktionen, die den Fokus des Benutzers stören oder umlenken.

Obstruction (dt. Hinderung) beschreibt die Hinderung einer Aufgabe, indem Interaktionen für Benutzer komplexer erscheinen, als sie tatsächlich sind. Ziel ist es, von einer bestimmten Handlung abzulenken. Beispielsweise erstellt ein Benutzer ein Konto und möchte es wieder schließen. Das Design suggeriert, dass hierzu ein Support-Mitarbeiter angerufen werden muss, der nur zu speziellen Zeiten arbeitet. Es wird also bewusst von der Konto-Schließung abgelenkt, mit dem Ziel, dass das Konto bestehen bleibt.

Sneaking (dt. Einschleichen) meint die Verschleierung von relevanten Informationen für Benutzer. Sneaking kann verschiedene Formen annehmen: Eine Aktion scheint ein bestimmtes Ergebnis zu erzielen, führt stattdessen aber zu einem unerwünschten Ergebnis. Außerdem können sich hinter Aktionen versteckte Kosten verbergen oder unerwünschte Produkte in den Warenkorb gelegt werden. Ferner können Abonnements automatisch verlängert werden, ohne dass Benutzer eine Information darüber erhalten.

Interface interference (dt. Schnittstellenstörung) beschreibt die Manipulation des User Interface, sodass bestimmte Funktionen oder Informationen gegenüber anderen prägnanter dargestellt werden. Dies soll Benutzer verwirren oder die Entdeckbarkeit wichtiger Aktionen einschränken. Interface interference kann verschiedene Formen annehmen:

(Kritische) Informationen können versteckt platziert werden, damit diese nur mit zusätzlichem Suchaufwand gefunden werden. Benutzerentscheidungen können durch Vorselektion manipuliert werden. Außerdem kann das User Interface so manipuliert werden, dass Missverständnisse der Hierarchie und der Art des Inhalts auftreten oder dass Handlungsdruck bei den Benutzern aufgebaut wird.

Forced action (dt. erzwungene Aktion) meint das erzwungene Ausführen von bestimmten Aufgaben, um danach auf eine bestimmte Funktionalität zugreifen oder diese weiterausführen zu können. Eine Forced action kann als eine Funktion getarnt sein, um einen Prozess vermeintlich abzuschließen. Forced action kann verschiedene Formen annehmen: Social Pyramid (dt. Sozialpyramide) beschreibt, dass Benutzer andere Benutzer einladen müssen, um einen Dienst (weiter) nutzen zu können. Ansonsten können Benutzer dazu verleitet werden, mehr Informationen als nötig preiszugeben, die dann meistens an Dritte weitergegeben werden. Ferner können Benutzer dazu verleitet werden, dass bestimmte Aktionen wiederholt und unerwünscht ausgeführt werden müssen. Dies wird meistens in Online-Games verwendet, in denen Benutzern schwierige Level angeboten werden, die nach mehrmaligem Versuch nur mit zu kaufenden Vorteilen bezwungen werden können.

In der vorliegenden Arbeit wird die folgende Definition 3-3 eines Dark Pattern zugrunde gelegt.

Definition 3-3: Dark Patterns

Dark Patterns sind Entwurfsentscheidungen eines User Interface, die einen Online-Dienst begünstigen, indem sie Benutzer zu unbeabsichtigten und potenziell schädlichen Entscheidungen zwingen, lenken oder täuschen. Ausprägungen von Dark Patterns sind: Nagging, Obstruction, Sneaking, Interface interference und Forced action.

Abbildung 9 zeigt zur Veranschaulichung verschiedene Dark Patterns. Im linken Smartphone-Screen verleitet das Design dazu, dass die Benutzer auf den prägnanten Button drücken, damit die Widerrufung der Einwilligung abgebrochen wird. Die Einwilligung kann nur durch Klick auf den kleineren Text unter dem prägnanten Button widerrufen werden. Im mittleren Smartphone-Screen verleiten die Farben der Buttons dazu, dass die Benutzer auf den grünen Button drücken und somit ihre Daten teilen. Im rechten Smartphone-Screen verleitet das Design aufgrund der grünen Farbe und des prägnanten Buttons dazu, dass das Jahres-Abonnement abgeschlossen wird.

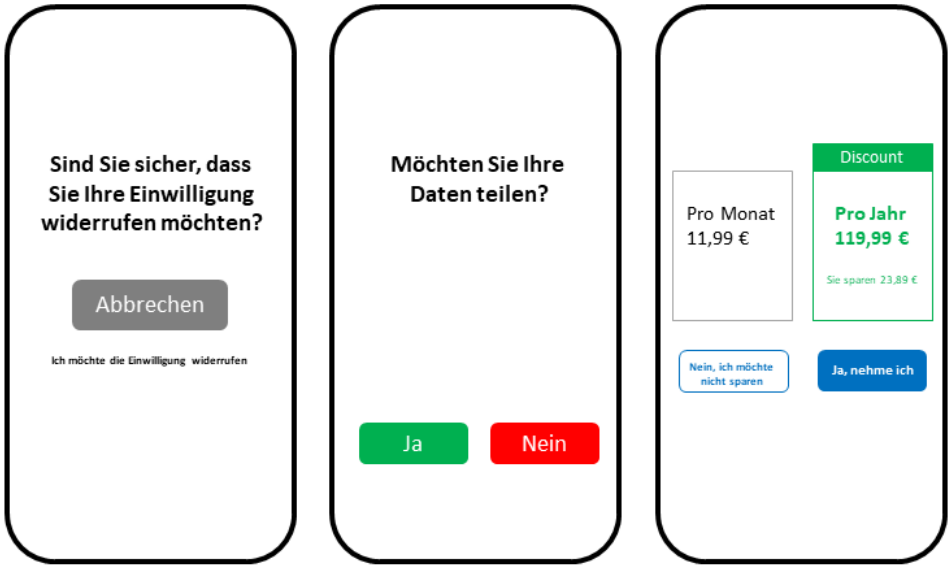


Abbildung 9: Beispiele von Dark Patterns

4 Grundlagen: Informationssicherheit

In Kapitel 4 werden die Grundlagen der Informationssicherheit vermittelt, soweit sie für die vorliegende Arbeit erforderlich sind. Zunächst wird in Abschnitt 4.1 eine Definition des Begriffs „Informationssicherheit“ gegeben und die Schutzziele der Informationssicherheit werden beschrieben. Danach werden die Begriffe „Schwachstelle“, „Bedrohung“, „Angriff“ und „Risiko“ in Abschnitt 4.2 erläutert. Abschließend wird auf das Security Engineering in Abschnitt 4.3 eingegangen, indem die Begriffe „Strukturanalyse“, „Schutzbedarfsermittlung“, „Bedrohungsanalyse“ und „Risikoanalyse“ beschrieben werden.

4.1 Definition und Schutzziele

Nach Eckert (2012) ist die Informationssicherheit von IT-Systemen „[…] die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen“.[18]

Die 3 primären Schutzziele der Informationssicherheit sind Vertraulichkeit (engl. Confidentiality), Integrität (engl. Integrity) und Verfügbarkeit (engl. Availability). Die Informationssicherheit gewährleistet den Schutz von Informationen, indem sie die genannten Schutzziele sicherstellt (DIN EN ISO/IEC 27000, 2020; Nieles u. a., 2017).

Die Norm DIN EN ISO/IEC 27000 (2020) definiert **Vertraulichkeit** als „Eigenschaft, dass Information unbefugten Personen, Entitäten oder Prozessen […] nicht verfügbar gemacht oder offengelegt wird“.

Der Begriff **Integrität** meint den „Schutz vor unzulässiger Veränderung oder Vernichtung von Informationen […]“ [aus dem Englischen übersetzt nach Nieles u. a. (2017)]. Unterschieden werden die Datenintegrität und die Systemintegrität: Datenintegrität meint die „Eigenschaft, dass Daten nicht auf unbefugte Weise verändert worden sind“ [aus dem

[18] Unter Funktionssicherheit (engl. Safety) versteht sich „[…] die Eigenschaft eines Systems, dass die realisierte Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt. Ein funktionssicheres System nimmt keine funktional unzulässigen Zustände an“ (Eckert, 2012).

Englischen übersetzt nach Nieles u. a. (2017)]. Systemintegrität meint die „Eigenschaft, die ein System hat, wenn es seine beabsichtigte Funktion unbeeinträchtigt ausführt, frei von unbefugten Manipulationen des Systems, ob absichtlich oder versehentlich“ [aus dem Englischen übersetzt nach Nieles u. a. (2017)].

Das Schutzziel **Verfügbarkeit** meint die „Gewährleistung eines rechtzeitigen und zuverlässigen Zugriffs auf Informationen sowie deren Nutzung“ [aus dem Englischen übersetzt nach Nieles u. a. (2017)].

Ferner bestehen erweiterte Schutzziele, die sich den 3 primären Schutzzielen unterordnen lassen: Authentizität (engl. authenticity), Nichtabstreitbarkeit (engl. non-repudiation) und Zuverlässigkeit (engl. reliability) (DIN EN ISO/IEC 27000, 2020).

Authentizität lässt sich dem primären Schutzziel Integrität unterordnen (Nieles u. a., 2017) und meint die „Eigenschaft, dass eine Entität das ist, was sie angibt zu sein“ (DIN EN ISO/IEC 27000, 2020).

Nichtabstreitbarkeit lässt sich dem primären Schutzziel Integrität unterordnen (Nieles u. a., 2017) und meint die „Fähigkeit, das Eintreten eines behaupteten Ereignisses oder einer behaupteten Handlung samt ihren ursächlichen Entitäten nachzuweisen“ (DIN EN ISO/IEC 27000, 2020).

Zuverlässigkeit lässt sich dem primären Schutzziel Verfügbarkeit unterordnen (Pohl, 2004) und meint die Eigenschaft eines Systems, „zu gewährleisten, dass die spezifizierte Funktion zuverlässig […] erbracht wird“ (Eckert, 2012).

In der vorliegenden Arbeit wird die Definition 4-1 der Informationssicherheit zugrunde gelegt. Diese beinhaltet die Definition nach Eckert (2012), jedoch ohne Einschränkung auf funktionssichere Systeme. Die in dieser Arbeit gewonnenen Erkenntnisse sollen auch auf nicht-funktionssichere Systeme anwendbar sein. Außerdem wurden die 3 primären Schutzziele nach DIN EN ISO/IEC 27000 (2020) bzw. nach Nieles u. a. (2017) ergänzt.

Definition 4-1: Informationssicherheit

Informationssicherheit ist die Eigenschaft eines Systems, eine unautorisierte Informationsveränderung oder -gewinnung zu verhindern. Die eingesetzten Maßnahmen müssen die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit erfüllen.

In der vorliegenden Arbeit wird auf eine umfassende Evaluation der Informationssicherheit verzichtet, da eine solche Evaluation andere methodische Ansätze fordert und den

Umfang dieser Arbeit übersteigen würde. Beispielsweise erfolgt keine Evaluation des Quellcodes. Stattdessen konzentriert sich die Arbeit auf die Evaluation jener Aspekte der UX und Informationssicherheit, die sich gegenseitig beeinflussen können (siehe Abschnitt 5.1).

4.2 Schwachstelle, Bedrohung, Angriff und Risiko

Schwachstellen in IT-Systemen können von Angreifern ausgenutzt werden, wodurch die Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigt werden (Eckert, 2012). Eine Schwachstelle beschreibt „eine Schwäche eines Systems oder einen Punkt, an dem das System verwundbar werden kann. Eine Verwundbarkeit […] ist eine Schwachstelle, über die die Sicherheitsdienste des Systems umgangen, getäuscht oder unautorisiert modifiziert werden können“ (Eckert, 2012).

Um mögliche Schwachstellen zu identifizieren, lassen sich vom Bundesamt für Sicherheit in der Informationstechnik (2020) klassifizierte Gefährdungsfaktoren verwenden, wie beispielsweise Naturkatastrophen, Diebstahl oder fehlerhafte Nutzung.

Ein System kann durch **Bedrohungen** gefährdet werden, die darauf abzielen, Schwachstellen oder Verwundbarkeiten auszunutzen und dadurch die Informationssicherheit des Systems zu beeinträchtigen. Bedrohungen resultieren aus passiven und aktiven Angriffen auf das System (Eckert, 2012).

Passive Angriffe meinen die unautorisierte Informationsgewinnung und betreffen den Verlust der Vertraulichkeit, wie beispielsweise das Ausspähen von Passwörtern, sogenannte Sniffer-Angriffe (Eckert, 2012).

Aktive Angriffe meinen die unautorisierte Modifikation von Daten und betreffen die Integrität und Verfügbarkeit. Die aktiven Angriffe teilen sich in 2 Klassen auf: Maskierungsangriffe (auch bekannt als Spoofing-Angriffe) und Denial-of-Service-Angriffe. Maskierungsangriffe verfolgen das Ziel, eine falsche Identität vorzugeben, um beispielsweise sensible Informationen zu erhalten oder um Server-Anfragen mit modifizierten Daten zu beantworten. Denial-of-Service-Angriffe verfolgen das Ziel, die Verfügbarkeit von Systemkomponenten oder -diensten zu mindern, indem beispielsweise Rechnernetze mit einer hohen Anzahl an Nachrichten konfrontiert werden, sodass eine Überlastung der Rechnernetze folgt (Eckert, 2012).

Des Weiteren sind Bedrohungen unterschiedliche Gewichte zuzuschreiben, die je nach Funktionalität und Einsatzumgebung eines Systems variieren (Eckert, 2012). Beispielsweise stellt ein Angriff auf eine Krankenhaus-Datenbank eine erhebliche Bedrohung für das Krankenhaus dar, da sensible Daten eingesehen und verändert werden können, sodass

ein höherer Schutzbedarf notwendig ist. Im Gegensatz dazu stellt ein unautorisierter, lesender Zugriff auf Informationen einer öffentlichen Datenbank keine schwerwiegende Bedrohung dar, sodass ein geringerer Schutzbedarf vorliegt.

Um die Gefährdungssituation zu bewerten, ist es erforderlich, die Risiken von potenziellen Bedrohungen zu untersuchen. Hierfür müssen die zu schützenden Güter (engl. Assets) und ihre Risiken bewertet werden (Eckert, 2012).

Das **Risiko** einer Bedrohung setzt sich aus der Eintrittswahrscheinlichkeit und dem Schadensausmaß zusammen. Es hängt von den Angreifermodellen ab, in denen potenzielle Angreifer mit ihren Fähigkeiten und Zielen definiert werden (beispielsweise klassifiziert nach Kenntnissen oder Ressourcen). Mithilfe von Bedrohungsanalysen und Risikoanalysen (siehe Abschnitt 4.3) lassen sich die Bedrohungen und deren Risiken bewerten (Eckert, 2012).

Abbildung 10 visualisiert die beschriebenen Begriffe mit deren Zusammenhängen.

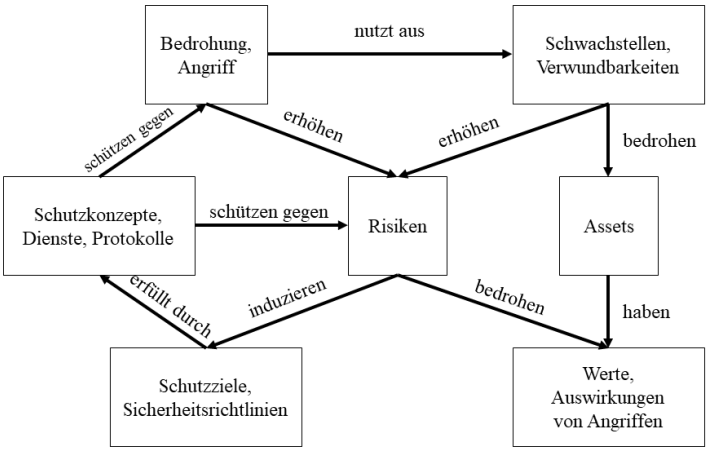


Abbildung 10: Schwachstelle, Bedrohung, Risiko und Angriff. (Eckert, 2012). Begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

4.3 Security Engineering

Abschnitt 4.3 widmet sich dem Security Engineering. „Beim Security Engineering geht es darum, Systeme so zu entwickeln, dass sie auch bei Böswilligkeit, Fehlern oder Missgeschicken verlässlich bleiben. Diese Disziplin konzentriert sich auf die Werkzeuge, Prozesse und Methoden, die für den Entwurf, die Implementierung und die Prüfung gesamter Systeme sowie für die Anpassung bestehender Systeme an die Entwicklung ihrer Umgebung erforderlich sind“ [aus dem Englischen übersetzt nach Anderson

(2010)]. Zunächst werden die Strukturanalyse in Abschnitt 4.3.1 und die Schutzbedarfsermittlung in 4.3.2 beschrieben. Danach folgen die Bedrohungsanalyse in Abschnitt 4.3.3 und die Risikoanalyse in Abschnitt 4.3.4.

4.3.1 Strukturanalyse

Um Bedrohungen und Risiken eines Systems zu bewerten, sollte zunächst eine Strukturanalyse durchgeführt werden, um die funktionalen Eigenschaften, die Einsatzumgebung und den Verwendungszweck des Systems zu verstehen. Die Festlegung von Anforderungen erfolgt in Form eines Pflichtenhefts, welches die funktionalen Anforderungen sowie die Anforderungen an Leistung, Zuverlässigkeit und Sicherheit des zu entwickelnden Systems umfasst. Die geplanten bzw. vorhandenen Systemkomponenten und -dienste sollten mit ihren Funktionen beschrieben werden, beispielsweise mithilfe einer grafischen Darstellung, dem Netztopologieplan (Eckert, 2012).

Abbildung 11 zeigt beispielhaft einen vereinfachten Netztopologieplan eines Forschungsinstituts. Einige Komponenten des Netztopologieplans sind durch einen Switch miteinander vernetzt. Ein „Switch leitet ein Datenpaket gezielt an einen Rechner weiter“ (Eckert, 2012). Der Datenverkehr zum Internet erfolgt hingegen über eine Firewall.

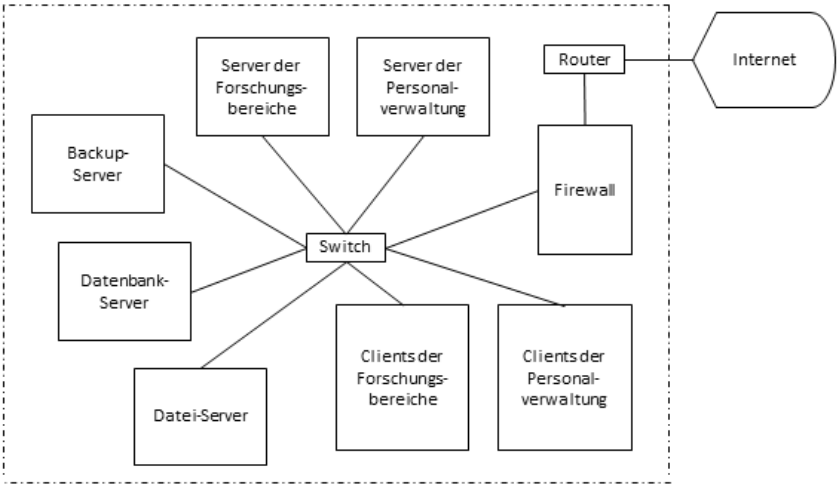


Abbildung 11: Beispiel eines Netztopologieplans. Unter Verwendung der Notation von Eckert (2012).

Zusätzlich zu einem grafischen Netztopologieplan sollten die Eigenschaften der Komponenten und Verbindungen dokumentiert werden (zum Beispiel tabellarisch). Mögliche Eigenschaften sind beispielsweise Betriebssysteme oder zugehörige Anwendungen (Eckert, 2012).

4.3.2 Schutzbedarfsermittlung

Nach der Strukturanalyse wird der Schutzbedarf des Systems bewertet. Da der Schutzbedarf schwer quantifizierbar ist, erfolgt die Bewertung meist qualitativ anhand von Schutzbedarfskategorien (Eckert, 2012).

Das Bundesamt für Sicherheit in der Informationstechnik (2017) empfiehlt 3 Schutzbedarfskategorien, die in Tabelle 3 dargestellt sind.

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 3: Schutzbedarfskategorien. (Bundesamt für Sicherheit in der Informationstechnik, 2017).

Zur Ermittlung des Schutzbedarfs anhand der Schutzbedarfskategorien werden verschiedene Schadensszenarien mit in die Bewertung einbezogen, wie beispielsweise die 6 Schadensszenarien vom Bundesamt für Sicherheit in der Informationstechnik (2017):

(a) Verstöße gegen Gesetze, Vorschriften und Verträge,

(b) Beeinträchtigung des informationellen Selbstbestimmungsrechts,

(c) Beeinträchtigung der persönlichen Unversehrtheit,

(d) Beeinträchtigung der Aufgabenerfüllung,

(e) negative Auswirkungen auf das Ansehen und

(f) finanzielle Auswirkungen.

Ein Schadensfall kann auf mehrere Schadensszenarien zutreffen. Beispielsweise kann ein Ausfall einer Anwendung sowohl die Aufgabenerfüllung verhindern als auch finanzielle Einbußen verursachen (Bundesamt für Sicherheit in der Informationstechnik, 2017).

Um die Schutzbedarfskategorien „niedrig bis mittel“, „hoch“ und „sehr hoch“ voneinander abzugrenzen, definiert das Bundesamt für Sicherheit in der Informationstechnik (2017) konkrete Schwellenwerte für die jeweiligen Schadensszenarien. Diese Schwellenwerte legen fest, ab welchem Punkt ein Schadensszenario als „niedrig bis mittel“, „hoch“ oder „sehr hoch“ eingestuft wird. Die Zuordnung eines Schadensszenarios zu einer dieser Kategorien erfolgt basierend auf den möglichen Auswirkungen dieses Szenarios, wie sie in den Schadensszenarien des Bundesamt für Sicherheit in der Informations-

technik (2017) beschrieben sind. Dazu gehören etwa rechtliche Konsequenzen, finanzielle Verluste und Beeinträchtigungen der Aufgabenerfüllung.

4.3.3 Bedrohungsanalyse

Sobald der Schutzbedarf festgelegt ist, sollte der Ist-Zustand des Systems bestimmt werden, um Defizite im Vergleich zum Soll-Zustand – dem ermittelten Schutzbedarf – zu identifizieren. Hierfür wird zunächst eine Bedrohungsanalyse ausgeführt, um die bestehenden Bedrohungen systematisch zu ermitteln. Grundsätzlich existieren 2 Vorgehensweisen: die Erstellung einer Bedrohungsmatrix und die Erstellung eines Bedrohungsbaums (Eckert, 2012).

Die Spalten der Bedrohungsmatrix beinhalten die potenziellen Auslöser der Bedrohungen, wie beispielsweise Systemadministratoren oder mobiler Code. Die Zeilen der Bedrohungsmatrix beinhalten die Gefährdungsbereiche, wie beispielsweise Bedrohungen durch externe Angriffe oder Missbrauch erteilter Berechtigungen. In der Matrix werden die potenziellen Angriffszenarien festgehalten (Eckert, 2012).

In einem Bedrohungsbaum ist auf oberster Ebene ein potenzielles Angriffsziel und damit eine potenzielle Bedrohung definiert. In den unteren Ebenen folgen Zwischenziele, die jeweils mit UND- bzw. Oder-Bedingungen verknüpft sind. Daraus ergeben sich unterschiedliche Angriffspfade, die unterschiedliche Angriffsschritte zum Erreichen des Angriffsziels auf oberster Ebene beinhalten (Eckert, 2012).

4.3.4 Risikoanalyse

Nachdem die Bedrohungen durch eine Bedrohungsanalyse (siehe Abschnitt 4.3.4) erfasst wurden, sollte eine Risikoanalyse durchgeführt werden, um die Risiken der Bedrohungen zu bewerten. Hierzu werden die Wahrscheinlichkeiten für das Eintreten verschiedener Bedrohungen und die potenziellen Schäden berücksichtigt. So lässt sich ein quantitativer Wert für ein Risiko durch Multiplikation der Eintrittswahrscheinlichkeit mit der Schadenshöhe bestimmen. Die Schadenshöhe ergibt sich aus den primären und sekundären Schäden. Primäre Schäden entstehen beispielsweise durch Produktionsstillstände, Kosten für Ersatzbeschaffung, Personal oder Reparaturen. Beispiele für sekundäre Schäden sind Schäden durch einen Imageverlust oder durch einen Vertrauensverlust bei Kunden. Die Eintrittswahrscheinlichkeit eines Schadens hängt von 2 zentralen Aspekten ab: dem Aufwand, den ein Angreifer investieren muss, um erfolgreich zu sein, und dem potenziellen Gewinn, den er daraus ziehen könnte. Zur Bewertung des Aufwands werden oft Penetrationstests durchgeführt, bei denen Angriffsverhalten simuliert wird, um zu identi-

fizieren, welche Schwachstellen eines Systems ausgenutzt und welche Schäden verursacht werden können (Eckert, 2012).

Die einzelnen Risiken lassen sich in einem Bedrohungsbaum (siehe Abschnitt 4.3.3) den einzelnen Zwischenzielen zuordnen, um somit ein Risiko für das Angriffsziel auf oberster Ebene festzulegen (Eckert, 2012). Beispielhaft zeigt Abbildung 12 einen Ausschnitt eines Bedrohungsbaums, der als Angriffsziel auf oberster Ebene das Ausspähen eines Wallet-Passworts beinhaltet. Zudem werden die Zwischenziele „Ausspähen der Passwort-Eingabe“, „unverschlüsselte Übertragung“ und „Zugriff auf gespeicherte Passwörter“ auf den unteren Ebenen aufgeführt. Den Zwischenzielen wurden verschiedene Risiken zugeordnet, sodass auf ein Risiko für das Angriffsziel „Ausspähen des Wallet-Passworts“ geschlossen werden kann, indem das höchste Risiko der Zwischenziele angesetzt wird. Um dieses Risiko zu reduzieren, sollten Passwörter nur verschlüsselt übertragen werden.

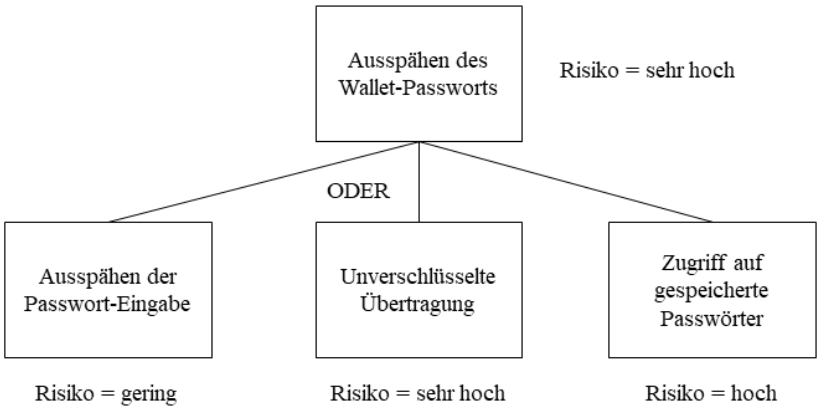


Abbildung 12: Beispiel eines Bedrohungsbaums mit Risiken. Unter Verwendung der Notation von Eckert (2012).

5 Evaluation von User Experience und Informationssicherheit

Kapitel 5 adressiert das Spannungsfeld der UX und Informationssicherheit beim Einsatz von Software-Systemen. Einleitend wird in Abschnitt 5.1 der Zusammenhang zwischen UX und Informationssicherheit erläutert. Hierbei werden die unterschiedlichen Beeinflussungsarten zwischen UX und Informationssicherheit systematisch aufgezeigt und anhand praktischer Beispiele verdeutlicht. Abschnitt 5.2 umfasst die Ergebnisse einer erstmaligen, systematischen Literaturrecherche über Verfahren zur Evaluation des Zusammenhangs von UX und Informationssicherheit. Für jedes identifizierte Verfahren wird diskutiert, inwiefern sich damit der Zusammenhang von UX und Informationssicherheit evaluieren lässt. Am Ende des Abschnitts werden die recherchierten Verfahren miteinander verglichen. Danach wird in Abschnitt 5.3 auf die UX und Informationssicherheit von Wallets eingegangen. Konkret werden ausgewählte Evaluationsverfahren aus Abschnitt 5.2 auf eine Wallet angewendet, um bisher unentdeckte Implikationen von UX und Informationssicherheit der Wallet zu identifizieren. Abschließend werden in Abschnitt 5.4 erstmals für Wallets entwickelte Qualitätsrichtlinien, sogenannte Heuristiken, der UX und Informationssicherheit vorgestellt, die auf den Ergebnissen aus Abschnitt 5.3 basieren. Insgesamt werden in Kapitel 5 somit neuartige, wissenschaftlich relevante Beiträge vorgestellt, die das Themenfeld der UX und Informationssicherheit theoretisch, methodisch und praxisorientiert erweitern.

5.1 Zusammenhang zwischen User Experience und Informationssicherheit

UX und Informationssicherheit sind wichtige Qualitätsattribute von Software-Systemen. Benutzer wollen ihre sensiblen Daten schützen, allerdings gleichzeitig auch eine intuitive und einfache Bedienung erleben. Um die Akzeptanz von Software-Systemen zu fördern, sollten UX und Informationssicherheit auf ein möglichst gutes Niveau verbessert werden. Hierzu ist es wichtig, dass beide Qualitätsattribute nicht separat voneinander betrachtet werden, da sie sich gegenseitig beeinflussen können. Die vorliegende Arbeit fokussiert sich auf diesen Zusammenhang zwischen UX und Informationssicherheit. Es werden diejenigen Aspekte von UX und Informationssicherheit betrachtet, die sich gegenseitig beeinflussen können, ohne eine tiefgreifende Evaluation der Informationssicherheit (wie beispielsweise durch Analyse des Quellcodes oder durch Penetrationtests) durchzuführen. Im Folgenden werden zunächst Beispiele für die verschiedenen Beeinflussungsarten von

UX und Informationssicherheit beschrieben. Anschließend werden die Beeinflussarten zusammengefasst.

Whitten & Tygar (1999) evaluieren die Verschlüsselungsanwendung PGP 5.0 und finden mehrere Schwächen der UX, die zu Schwächen der Informationssicherheit führen. Die Mehrheit der Probanden ist nicht in der Lage, eine Nachricht zu signieren und zu verschlüsseln. 3 der 12 Probanden geben sogar ihren privaten Schlüssel preis. Whitten & Tygar (1999) kommen zum Schluss, dass PGP 5.0 aufgrund mangelnder UX keine wirksame Informationssicherheit gewährleistet.

18 Jahre später stellen sich Zimmermann u. a. (2017) die Frage, ob die identifizierten Schwächen von Whitten & Tygar (1999) mittlerweile behoben wurden. Durch die Evaluation der Verschlüsselungsanwendungen Enigmail und gpg4o finden Zimmermann u. a. (2017) heraus, dass bereits einzelne von Whitten & Tygar (1999) identifizierte UX-Schwächen behoben wurden, allerdings weiterhin mehrere UX-Schwächen vorliegen, welche die Informationssicherheit beeinflussen. Beispielsweise sollte das Schlüsselmanagement vereinfacht und Hilfestellungen angeboten werden (wie etwa ein einführendes Tutorial), um Benutzungsfehler zu reduzieren.

Auch Adams & Sasse (1999) argumentieren, dass viele Sicherheitsmängel durch mangelnde UX verursacht werden. Sicherheitsmaßnahmen sollten nicht nur effektiv sein, sondern auch intuitiv und einfach nutzbar.

Sasse u. a. (2001) appellieren, dass Sicherheitsdesigner Ursachen für unerwünschtes Nutzerverhalten ermitteln und diese angehen, um wirksame Sicherheitssysteme zu entwerfen. Sicherheitsmechanismen sollten nahtlos in das Nutzungsverhalten integriert werden und möglichst keine Störungen verursachen. Denn Sicherheitsmaßnahmen werden von Benutzern oft als Hindernisse wahrgenommen, was zu Nichteinhaltung oder Umgehung führen kann.

Furnell u. a. (2006) zeigen, dass sich einige essentielle Sicherheitsfunktionen von Internet Explorer, Outlook Express und Microsoft Word als signifikante Herausforderungen für einen großen Teil der Probanden aufgrund von UX-Schwächen darstellen. Die Ergebnisse verdeutlichen die Notwendigkeit von benutzbaren Sicherheitsfunktionen, um eine höhere Informationssicherheit zu schaffen.

West u. a. (2008) argumentieren, dass Benutzer als schwächstes Glied in der Informationssicherheit gelten. Aufgrund einer unzureichenden UX können Benutzer Warnungen übersehen und falsche Sicherheitseinstellungen treffen. Daher müssen potenzielle Fehlbedienungen von Benutzern bei der Entwicklung von Software-Systemen berücksichtigt werden, um Fehler zu reduzieren.

Kulyk u. a. (2017) untersuchen, auf wieviel UX Probanden verzichten würden, um mehr Informationssicherheit bei Online-Wahlen zu erhalten. Die Ergebnisse zeigen, dass die Probanden etwa auf 26 Punkte (Skala 0 bis 100 Punkte) der UX verzichten würden, wenn sie ein System mit höherer Informationssicherheit benutzen könnten.

Weitere verwandte Publikationen adressieren die UX und Informationssicherheit verschiedener Authentifizierungsmethoden.

Johnston u. a. (2003) appellieren, dass beim Entwurf von Sicherheitsmechanismen ein angemessenes Verhältnis zwischen Informationssicherheit und UX gefunden werden sollte. Andernfalls könnten Benutzer beispielsweise dazu neigen, Passwörter auf Notizzetteln zu notieren, was zur Abnahme der Informationssicherheit führt.

Auch Ma & Feng (2011) evaluieren die UX verschiedener Passwörter, wie beispielsweise textbasierte und grafische Passwörter. Es zeigt sich, dass die untersuchten grafischen Passwörter mehr Zeit und Aufwand für die Authentifizierung erfordern als die untersuchten textbasierten Passwörter.

Reese u. a. (2019) evaluieren die UX von 5 Zwei-Faktor-Authentifizierungsmethoden mit unterschiedlichen Informationssicherheit-Niveaus. Sie finden heraus, dass 8 von 12 Probanden Schwierigkeiten bei der Eingabe eines zugesendeten 6-stelligen Codes haben, bevor dieser abläuft, sodass die UX abnimmt.

Bosnjak & Brumen (2019) evaluieren die UX verschiedener Passwörter, wie beispielsweise textbasierte und grafische Passwörter, bei denen bestimmte Felder auf einem Schachbrett ausgewählt werden sollen. Sie finden heraus, dass trotz der Vorteile von grafischen Passwörtern die grafischen Passwörter am schwächsten abschneiden und die Probanden die größten Schwierigkeiten haben, sich nach dem zweiwöchigen Zeitraum an diese zu erinnern.

Zhang u. a. (2021) evaluieren, wie sich das herkömmliche Android-Entsperrungsmuster (3x3-Layout) verbessern lässt. Sie verbessern die Informationssicherheit des Entsperrungsmusters, ohne die UX nennenswert zu beeinflussen.

Zusammenfassend können sich UX und Informationssicherheit auf 9 unterschiedliche Arten gegenseitig beeinflussen:

(1) *Positive Beeinflussung*; (1.1) aus der Verbesserung der UX folgt eine Verbesserung der Informationssicherheit oder (1.2) aus der Verbesserung der Informationssicherheit folgt eine Verbesserung der UX. Beispielsweise kann eine Erhöhung der Kontraste des User Interface zur Verbesserung der UX führen, da Texte besser gelesen werden können, insbesondere durch Sehbeeinträchtigte. Dadurch können Sicher-

heitshinweise besser wahrgenommen werden, sodass sich die Informationssicherheit verbessern könnte. Des Weiteren können Benutzer durch einen leicht erkennbaren Sicherheitshinweis davon abgehalten werden, ihre Daten an nicht vertrauenswürdige Stellen zu teilen.

(2) *Negative Beeinflussung*: (2.1) aus der Verbesserung der UX folgt eine Verschlechterung der Informationssicherheit oder (2.2) aus der Verbesserung der Informationssicherheit folgt eine Verschlechterung der UX. Beispielsweise kann sich die Informationssicherheit durch Verwendung einer Zwei-Faktor- anstatt einer Ein-Faktor-Authentifizierungsmethode verbessern und dadurch die UX verschlechtern, da die Authentifizierung von Benutzern als umständlicher empfunden werden könnte.

(3) *Keine (nennenswerte) Beeinflussung*: (3.1) aus der Verbesserung der UX folgt keine (nennenswerte) Beeinflussung der Informationssicherheit, (3.2) aus der Verschlechterung der UX folgt keine (nennenswerte) Beeinflussung der Informationssicherheit, (3.3) aus der Verbesserung der Informationssicherheit folgt keine (nennenswerte) Beeinflussung der UX, (3.4) aus der Verschlechterung der Informationssicherheit folgt keine (nennenswerte) Beeinflussung der UX oder (3.5) UX und Informationssicherheit beeinflussen sich nicht. Beispielsweise integriert ein Onlineshop eine Filteroption von Produkten, sodass sich die UX verbessern könnte und die Informationssicherheit nicht beeinflusst wird. Ferner könnte beispielsweise die Verwendung eines 6-stelligen Pins anstatt einem 4-stelligen Pin die Informationssicherheit verbessern und die UX nicht (nennenswert) verschlechtern.

Da sich UX und Informationssicherheit gegenseitig beeinflussen können, sollten die beiden Aspekte nicht isoliert voneinander evaluiert werden. Daher wurde zunächst nach Verfahren recherchiert, mit denen sich der Zusammenhang zwischen UX und Informationssicherheit evaluieren lässt. Die identifizierten Evaluationsverfahren werden im folgenden Abschnitt 5.2 diskutiert.

5.2 Diskussion von Evaluationsverfahren

Zunächst wurde eine systematische Literaturrecherche von Sauer u. a. (2024a) durchgeführt, um bereits bestehende Verfahren zur Evaluation des Zusammenhangs zwischen UX und Informationssicherheit zu recherchieren:

Zuerst wurden die Datenbanken Scopus, IEEE Xplore, ScienceDirect, Google Scholar, DBLP und ACM Digital Library mit folgenden Suchtermen durchsucht:

Suchterm 1: (“analysis methods“ OR “evaluation methods“) AND “correlation“ AND “security“ AND (“uux“ OR “usability“ OR “user experience“)

Suchterm 2: (“analysis methods“ OR “evaluation methods“) AND “security“ AND (“uux“ OR “usability“ OR “user experience“)

Suchterm 3: (“analysis methods“ OR “evaluation methods“) AND “usable security“

Da die Datenbanksuche eine hohe Anzahl an Suchergebnissen ergab (beispielsweise Suchterm 2 mit 17600 Suchergebnissen in Google Scholar), wurden maximal die ersten 300 Suchergebnisse pro Suchterm und Datenbank berücksichtigt. Diese Stichprobe wurde zunächst als ausreichend angesehen, da die relevanten Konferenzen, Workshops, Zeitschriften und Publikationen von Forschungsgruppen später noch durchsucht und eine Vorwärts-/Rückwärtssuche durchgeführt werden sollte. Aus der Datenbanksuche resultierten initial 2941 Publikationen, die anschließend anhand 3 Filterkriterien gefiltert wurden. Zuerst wurden diejenigen Publikationen exkludiert, deren Titel und Zusammenfassungen sich nicht auf UX und Informationssicherheit bezogen (Filterkriterium 1). So blieben 122 Publikationen übrig, deren Dubletten daraufhin gefiltert wurden (Filterkriterium 2). Die 86 verbliebenen Publikationen wurden daraufhin vollständig gelesen und gefiltert, wenn kein Verfahren zur Evaluation des Zusammenhangs zwischen UX und Informationssicherheit erwähnt wurde (Filterkriterium 3). Aus den 2941 Publikationen aus den Datenbanken verblieben schlussendlich 25 Publikationen.

Die durch die Datenbanksuche identifizierten Publikationen wurden nach Watson & Webster (2020) in einem Graphen angeordnet, in dem die Publikationen durch Kanten mit den Knoten „Datenbanken“, „Konferenzen“, „Workshops“, „Zeitschriften“, „Forschungsgruppen“, „Rückwärtssuche“ und „Vorwärtssuche“ verbunden sind. Durch eine hohe Anzahl an Kanten wurden die relevanten Konferenzen/Workshops, Zeitschriften sowie Forschungsgruppen visuell ersichtlich. Der gesamte Graph ist online verfügbar[19].

Als relevant klassifizierte Konferenzen/Workshops: Symposium on Usable Privacy and Security (SOUPS), Human Factors in Computing Systems (CHI), New Security Paradigms Workshop (NSPW), Availability, Reliability and Security (ARES), Human Computer Interaction (AIPO) und Human-Computer Interaction (IFIP).

Als relevant klassifizierte Zeitschriften: Human-Computer Interaction, Interacting with Computers, IEEE Security & Privacy, Computers & Security und Array.

Als relevant klassifizierte Forschungsgruppen: SECUSO (Karlsruher Institut für Technologie) und GRIHO (University of Lleida).

[19] https://sdika.de/files/2023-miroboard-slr-results.pdf

Diese wurden vollständig nach relevanten Publikationen mit den definierten Filterkriterien 1-3 durchsucht. Nach Filterung mithilfe von Filterkriterium 1 blieben aus den initialen 23668 Publikationen noch 238 Publikationen übrig, nach Filterkriterium 2 verblieben 218 Publikationen und nach Filterkriterium 3 verblieben 85 Publikationen.

Anschließend wurde eine Rückwärtssuche aller nach Filterkriterium 3 verbliebenen 110 (25+85) Publikationen durchgeführt. Nach Filterkriterium 1 verblieben 71 Publikationen, nach Filterkriterium 2 verblieben 58 Publikationen und nach Filterkriterium 3 verblieben 29 Publikationen.

Abschließend wurde eine Vorwärtssuche aller nach Filterkriterium 3 verbliebenen 139 (25+85+29) Publikationen mithilfe von Google Scholar durchgeführt. Nach Filterung der initial recherchierten 12085 Publikationen mithilfe von Filterkriterium 1 verblieben 218 Publikationen, nach Filterkriterium 2 verblieben 145 Publikationen und nach Filterkriterium 3 verblieben 79 Publikationen.

Zusammenfassend wurden durch die Recherche in den Datenbanken, Konferenzen/Workshops, Zeitschriften, Forschungsgruppen und Vorwärts-/Rückwärtssuche insgesamt nach Filterung 189 Publikationen identifiziert. Als finaler Schritt wurden die in den Publikationen erwähnten Evaluationsverfahren gesammelt und Dubletten beseitigt. Dadurch konnten 22 Evaluationsverfahren (einschließlich 10 Fragebögen) identifiziert werden.

Abbildung 13 visualisiert die beschriebenen Ergebnisse der systematischen Literaturrecherche. Dabei steht „T“ für die Anzahl der Publikationen vor Filterung. „F1-F3“ stehen für die Anzahl der Publikationen nach Filterung mittels der Filterkriterien 1-3. „EV“ steht für die Anzahl der extrahierten Evaluationsverfahren.

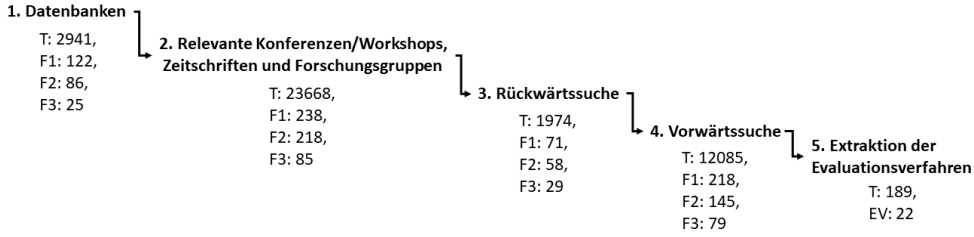


Abbildung 13: Ergebnisse der systematischen Literaturrecherche. Zusammengefasst nach Sauer u. a. (2024a).

Die identifizierten Evaluationsverfahren werden im Folgenden vorgestellt und es wird jeweils diskutiert, inwiefern sich damit der Zusammenhang zwischen UX und Informationssicherheit evaluieren lässt. Abschließend werden die recherchierten Evaluationsverfahren in Abschnitt 5.2.14 einander gegenübergestellt.

5.2.1 SecureUse Score

Beschreibung des Verfahrens. Dutta u. a. (2016) entwickelten eine Metrik zur Bewertung der Usability und eine Metrik zur Bewertung der Informationssicherheit. Die Metrik der Usability beinhaltet 3 weitere Metriken der Effektivität, Effizienz und Zufriedenheit. Die Effektivität wird durch einen UX-Experten mithilfe der zugehörigen Metrik bewertet und beschreibt, wie effektiv sich verschiedene Software-Funktionen durch Benutzer ausführen lassen. Der Wert 0 bedeutet, dass eine Software-Funktion nicht erfolgreich ausgeführt werden konnte. Die Werte von 1-4 beschreiben, dass eine Software-Funktion teilweise erfolgreich ausgeführt werden konnte. Der Wert 5 beschreibt, dass eine Software-Funktion vollständig erfolgreich ausgeführt werden konnte. Die Effizienz wird durch einen UX-Experten mithilfe der zugehörigen Metrik bewertet und beschreibt, wie effizient (benötigte Zeit) sich verschiedene Software-Funktionen durch Benutzer ausführen lassen. Der Wert 0 bedeutet, dass eine Software-Funktion nicht erfolgreich ausgeführt werden konnte. Die Werte reichen von 1 (ineffiziente Ausführung) bis 5 effiziente Ausführung). Die Zufriedenheit wird von mindestens einem Benutzer des Software-Systems mithilfe der zugehörigen Metrik bewertet. Bei mehreren Benutzern wird der Durchschnittswert der Zufriedenheit verwendet. Die 3 Werte der Effektivität, Effizienz und Zufriedenheit werden summiert und ergeben einen Gesamtwert der Usability. Die Metrik der Informationssicherheit kann die Werte 0 (niedriges Niveau der Informationssicherheit) bis 15 (hohes Niveau der Informationssicherheit) annehmen. Die Informationssicherheit wird durch einen Experten der Informationssicherheit mithilfe der zugehörigen Metrik bewertet. Die ermittelten Werte der Usability und der Informationssicherheit können zum Vergleich in einem Tornado Chart (Abrams, 2010) visualisiert werden.

Abbildung 14 zeigt beispielhaft ein solches Tornado-Chart. Dieses zeigt die Werte der Informationssicherheit und Usability von 7 unterschiedlichen bewerteten Varianten eines Software-Systems. Varianten sind verschiedene Ausprägungen eines Software-Systems. In dieser Arbeit werden Varianten betrachtet, die sich genau in einem Parameter voneinander unterscheiden. Parameter können beispielsweise unterschiedliche Sicherheitsmechanismen sein, wie verschiedene Authentifizierungsverfahren oder Verschlüsselungsalgorithmen.

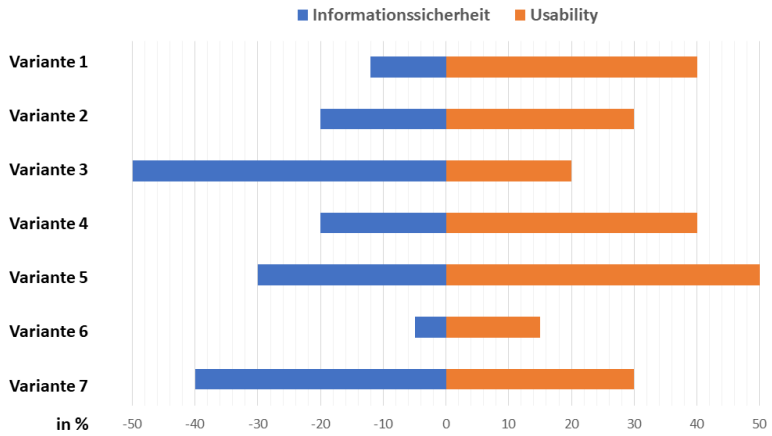


Abbildung 14: Beispiel für ein Tornado-Chart

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Durch die erwähnten Metriken lassen sich zwar Werte für die Usability und Informationssicherheit bestimmen, allerdings lässt sich die Beeinflussung beider Eigenschaften nicht durch eine einmalige Anwendung der Metriken bewerten. Falls verschiedene Varianten eines Software-Systems vorliegen, die sich lediglich in einem Parameter unterscheiden (zum Beispiel verschiedene Authentifizierungsverfahren), kann die Beeinflussung beider Eigenschaften bestimmt werden. Beispiel: Variante X verwendet rote Sicherheitshinweise und Variante Y schwarze Sicherheitshinweise. Die Metriken werden nun für beide Varianten verwendet, um jeweils die Usability und Informationssicherheit zu bewerten. Nun wird deutlich, dass Variante X eine höhere Informationssicherheit aufweist und sich gleichzeitig die Usability nicht nennenswert verändert. Das heißt, die rote Schriftfarbe der Sicherheitshinweise trägt dazu bei, dass Sicherheitshinweise öfters und bewusster wahrgenommen werden. Gleichzeitig resultiert aus der roten Schriftfarbe kein nennenswerter Störfaktor, also keine schlechtere Usability. Ferner lassen sich mithilfe der Metriken nur die Usability und keine weiteren UX-Attribute (siehe Abbildung 7) bewerten.

5.2.2 Heuristische Evaluation und Heuristiken

Beschreibung des Verfahrens. Nielsen und Molich (1990) entwickelten das Verfahren „Heuristische Evaluation“, mit dem sich die Usability eines Software-Systems bewerten lässt. Dabei wird das Software-System auf verschiedene Usability-Probleme mithilfe von Heuristiken untersucht.

Bader u. a. (2017) beschreiben eine Heuristik im Kontext von Evaluationen als Regel, mit der bestimmte, erwünschte Eigenschaften eines Untersuchungsgegenstandes untersucht

und verbessert werden können, sodass eine positiv wahrgenommene Usability erreicht wird.

Nielsen (1994) beschreibt eine Heuristik als breitgefasstes Usability-Prinzip, mit dem ein Software-System untersucht wird, um Usability-Probleme zu finden.

Yáñez Gómez u. a. (2014) definieren eine Heuristik als Richtlinie, deren Erfüllung geprüft wird, wenn die UX eines realen Systems oder Prototyps evaluiert und verbessert wird.

Ferner wurden nicht nur Heuristiken der Usability entwickelt, sondern auch Heuristiken anderer UX-Attribute und Heuristiken der Informationssicherheit: Quiñones u. a. (2020) entwickelten Heuristiken weiterer UX-Attribute (zum Beispiel Auffindbarkeit und Nützlichkeit) für Soziale Netzwerke. Beispielsweise sollten Soziale Netzwerke den Benutzern nur Informationen basierend auf deren Präferenzen anzeigen und Informationen ausblenden, welche die Benutzer explizit nicht sehen möchten.

Realpe u. a. (2016) entwickelten Heuristiken der Informationssicherheit, wie etwa eine Heuristik, dass kritische Bereiche eines Software-Systems niemals für Benutzer, sondern nur für Administratoren, zugänglich sein sollen und dass Zeichen eines Passworts bei Eingabe nicht standardmäßig einsehbar sind.

Mithilfe einer Sammlung von Heuristiken kann die UX oder die Informationssicherheit von Systemen unterschiedlicher Reifegrade (zum Beispiel reales System oder Prototyp) bewertet werden, indem der Erfüllungsgrad jeder Heuristik bewertet wird.

In der vorliegenden Arbeit wird die folgende Definition 5-1 einer Heuristik der UX oder Informationssicherheit zugrunde gelegt.

Definition 5-1: Heuristik der UX oder Informationssicherheit

Eine Heuristik der UX oder Informationssicherheit ist eine Richtlinie für die UX oder die Informationssicherheit von Systemen. Ein System kann eine Heuristik zu einem gewissen Grad erfüllen (nicht erfüllt bis vollständig erfüllt).

Im Folgenden wird der Begriff Heuristik als Sammelbegriff für eine Heuristik der UX oder Informationssicherheit verwendet.

Molich & Nielsen (1990) entwickelten initial 9 Heuristiken der Usability (ein Attribut der UX, siehe Abschnitt 3.2):

(H1) Simple and Natural Dialogue: Dialoge sollten keine irrelevanten oder selten benötigten Informationen enthalten. Jede überflüssige Information konkurriert mit der Sichtbarkeit von relevanten Informationen. Alle Informationen sollten in einer natürlichen und logischen Reihenfolge erscheinen.

(H2) Speak the User's Language: Informationen sollten den Benutzern mit vertrauten Begriffen übermittelt werden, ohne dabei technische Begriffe zu verwenden.

(H3) Minimize the User's Memory Load: Das Kurzzeitgedächtnis der Benutzer ist begrenzt. Das System sollte Benutzer dabei unterstützen, sich möglichst wenige Informationen merken zu müssen. Die Anweisungen für die Benutzung des Systems sollten sichtbar und leicht auffindbar sein.

(H4) Be Consistent: Für Benutzer sollte klar erkennbar sein, ob unterschiedliche Begriffe, Situationen oder Handlungen dieselbe Bedeutung haben.

(H5) Provide Feedback: Das System sollte Benutzer stets über den aktuellen Systemzustand informieren, indem es rechtzeitiges und verständliches Feedback liefert.

(H6) Provide Clearly Marked Exits: Ein System sollte Benutzer niemals in Situationen festhalten, aus denen kein klar erkennbarer Ausweg besteht. Wenn versehentlich eine System-Funktion verwendet wird, sollte es stets eine klar erkennbare Möglichkeit geben, die Situtation schnell und unkompliziert zu verlassen.

(H7) Provide Shortcuts: Merkmale, die ein System leicht erlernbar machen (zum Beispiel ausführliche Dialoge) sind für erfahrene Benutzer oft umständlich. Abkürzungen (Shortcuts) sollten in das System eingebaut werden, sodass das System sowohl für unerfahrene als auch für erfahrene Benutzer geeignet ist.

(H8) Provide Good Error Messages: Gute Fehlermeldungen sollten defensiv, präzise und konstruktiv formuliert sein. Defensive Fehlermeldungen machen deutlich, dass das Problem auf einen Systemfehler zurückzuführen ist, und vermeiden es, die Benutzer zu kritisieren. Präzise Fehlermeldungen geben den Benutzern präzise Informationen über die Ursache des Fehlers. Konstruktive Fehlermeldungen geben hilfreiche Hinweise darauf, welche Schritte die Benutzer als Nächstes unternehmen können.

(H9) Error Prevention: Das System sollte durch ein durchdachtes Design zur Fehlervermeidung beitragen, anstatt auf reaktive Fehlermeldungen angewiesen zu sein.

Später fügte Nielsen (1994) den 9 zuvor entwickelten Heuristiken eine weitere hinzu:

(H10) Help and Documentation: Auch wenn das System ohne Dokumentation verwendet werden können sollte, sollte eine Dokumentation zur Hilfe bereitgestellt werden. Die Dokumentation sollte leicht auffindbar sein, sich auf die Aufgaben der Benutzer konzentrieren, konkrete Schritte zur Hilfe auflisten und nicht zu umfangreich sein.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Fanelle u. a. (2020) evaluierten die Usability von verschiedenen CAPTCHA-Varianten mithilfe einer Teilmenge der Heuristiken von Molich & Nielsen (1990). Die CAPTCHA-Varianten besaßen unterschiedliche Niveaus der Informationssicherheit, die separat voneinander mithilfe der Heuristiken evaluiert wurden. Durch die Evaluation konnte gezeigt werden, welche CAPTCHA-Varianten (k)ein adäquates Niveau der Usability und Informationssicherheit besitzen. Da mittlerweile auch Heuristiken der Informationssicherheit entwickelten wurden, wie beispielsweise von Realpe u. a. (2016), kann die Heuristische Evaluation auch verwendet werden, um die UX und die Informationssicherheit zu bewerten. Allerdings lässt sich die gegenseitige Beeinflussung nicht unmittelbar mit einer Heuristischen Evaluation bewerten. Dazu müsste evaluiert werden, inwiefern sich einzelne Heuristiken der UX und Informationssicherheit gegenseitig beeinflussen.

5.2.3 Security Usability Symmetry

Beschreibung des Verfahrens. Die von Braz u. a. (2007) entwickelte „Security Usability Symmetry“ ist eine Variante der Heuristischen Evaluation (siehe Abschnitt 5.2.2). Damit lassen sich die Usability und Informationssicherheit von interaktiven Systemen bewerten, indem Usability- und Sicherheitsexperten verschiedene Usability- und Sicherheitsprobleme mithilfe von Heuristiken sammeln. Braz u. a. (2007) entwickelten Heuristiken der Usability und Informationssicherheit speziell für Multifunction Teller Machines, eine Variante von Bankautomaten. Hierzu verwendeten sie das von Seffah u. a. (2006) entwickelte hierarchische Modell namens „Quality in Use Integrated Measurement“ (QUIM), mit dem die Usability in Faktoren, dann in Kriterien und schließlich in spezifische Metriken subsummiert werden kann. Die identifizierten Probleme der Usability werden nach der Häufigkeit des Auftretens, den Folgen und der Dauerhaftigkeit des Problems bewertet. Die identifizierten Probleme der Informationssicherheit werden nach Vertraulichkeit, Authentifizierungsmöglichkeit, Integrität, Nichtabstreitbarkeit, Zugriffskontrolle und Verfügbarkeit bewertet.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Braz u. a. (2007) verwendeten die Security Usability Symmetry, um die Usability und die Informationssicherheit von Multifunction Teller Machines, eine Variante von Bankautomaten, zu bewerten. Dazu verwendeten sie die mit QUIM entwickelten Heuristiken der Usability und Informationssicherheit. Mit ihrem Verfahren lässt sich allerdings nicht unmittelbar

die Beeinflussung von Usability und Informationssicherheit bewerten. Da die Security Usability Symmetry eine Variante der Heuristischen Evaluation (siehe Abschnitt 5.2.2) ist, müsste zudem die Beeinflussung der einzelnen Heuristiken evaluiert werden.

5.2.4 Cognitive Walkthrough

Beschreibung des Verfahrens. Wharton u. a. (1994) entwickelten ein Verfahren namens „Cognitive Walkthrough“, mit dem sich die UX, insbesondere die Lernfähigkeit, bewerten lässt. Dabei führen die Evaluierenden verschiedene Aufgaben in einem Software-System aus, um UX-Schwachstellen zu identifizieren, die für zukünftige Benutzer Herausforderungen darstellen könnten. Hierzu werden zunächst der Evaluationsgegenstand und die zukünftigen Benutzer mit ihren Merkmalen (zum Beispiel IT-Affinität oder Alter) definiert. Anschließend werden die Aufgaben, welche die Evaluierenden im Software-System durchlaufen sollen, festgelegt. Bevor die Evaluierenden die Aufgaben ausführen, sollten sie sich mit den anfangs definierten Merkmalen der zukünftigen Benutzer vertraut machen. Unterschiedliche Benutzer sind unterschiedlichen Hürden bei der Benutzung eines Software-Systems ausgesetzt, wie beispielsweise Benutzer mit einer Rot-Grün-Sehschwäche. Außerdem sollten sich die Evaluierenden mit den bevorstehenden Aufgaben, die sie im Software-Systems ausführen werden, vertraut machen. Die Aufgaben sollten so konkret und realistisch wie möglich sein. Anschließend führen die Evaluierenden die definierten Aufgaben im Software-System aus und sammeln Usability-Probleme. Hierzu können die Evaluierenden 4 beispielhafte Fragen verwenden: „Wird der Benutzer versuchen, den richtigen Effekt zu erzielen? Wird der Benutzer erkennen, dass die korrekte Aktion zur Verfügung steht? Wird der Benutzer eine Verbindung zwischen der korrekten Aktion und dem gewünschten Effekt erkennen? Wenn die richtige Aktion durchgeführt wurde, erkennt der Benutzer, dass Fortschritte in Richtung des angestrebten Ergebnisses gemacht werden?“ [aus dem Englischen übersetzt nach Wharton u. a. (1994)].

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Herzog & Shahmehri (2007) evaluierten die UX und deren Auswirkungen auf die Informationssicherheit von 13 verschiedenen Firewalls mithilfe von Cognitive Walkthrough. In der Regel läuft eine Firewall im Hintergrund, ohne dass eine Interaktion durch Benutzer erforderlich ist. Falls aber ein sicherheitskritisches Ereignis eintritt, bekommen die Benutzer einen Warnhinweis und eine sofortige Entscheidung über das weitere Vorgehen ist notwendig. Wenn die Benutzer den Warnhinweis nicht verstehen, können fehlerhafte Konfigurationen durchgeführt und schlussendlich das Niveau der Informationssicherheit gemindert werden. Durch die Evaluation wurden einerseits verschiedene Entwurfsalternativen mit unterschiedlichen Informationssicherheit-Niveaus auf ihre UX-Probleme untersucht und die Ergebnisse miteinander verglichen. Andererseits wurden auch UX-

Probleme je Entwurfsalternative gesammelt und die potenziellen Auswirkungen je UX-Problem auf die Informationssicherheit diskutiert. Durch Cognitive Walkthrough kann also der Zusammenhang zwischen UX und Informationssicherheit durch Experten diskutiert und bewertet werden. Da Cognitive Walkthrough ein expertenbasiertes Evaluationsverfahren ist, fehlt aber die Sicht der tatsächlichen Endanwender.

5.2.5 Heuristic Walkthrough

Beschreibung des Verfahrens. Heuristic Walkthrough (Sears, 1997) vereint die Verfahren Heuristische Evaluation (siehe Abschnitt 5.2.2) und Cognitive Walkthrough (siehe Abschnitt 5.2.4). Bei einer heuristischen Evaluation gibt es keine vordefinierten Aufgaben, welche die Evaluierenden durchführen (Freiform-Evaluation). Zudem beschränkt sich das Verfahren darauf, das Software-System anhand von Heuristiken zu bewerten, ohne weitere Aspekte in die Bewertung einzubeziehen. Bei einem Cognitive Walkthrough hingegen werden vordefinierte Aufgaben mit Zuhilfenahme von 4 Leitfragen ausgeführt. Einerseits können dadurch weitere relevante Aspekte vergessen werden, da die Evaluierenden nur die vordefinierten Aufgaben ausführen. Andererseits wird die spontane, explorative Benutzung unterbunden, die typischerweise auftritt, wenn Benutzer ein Software-System eigenständig erkunden und lernen, damit umzugehen. Heuristic Walkthrough versucht diese Nachteile zu korrigieren, indem 2 Durchläufe zur Bewertung durchgeführt werden. Im ersten Durchlauf wird die Evaluation mithilfe von zuvor priorisierten Aufgaben durchgeführt. Die Priorität bezieht sich oft auf die Wichtigkeit der Aufgabe oder darauf, wie oft potenzielle Benutzer Aufgaben ausführen würden. Den Evaluierenden steht es frei, jede Aufgabe in beliebiger Reihenfolge und so lange wie nötig zu untersuchen. Sie können wieder die 4 Leitfragen für die Evaluation verwenden. Der erste Durchlauf soll somit sicherstellen, dass die Erfahrungen der Evaluierenden mit dem Software-System aufgabenorientiert sind – vergleichbar mit zukünftigen Benutzern, die lernen, das System zu benutzen. Im zweiten Durchlauf soll eine Freiform-Evaluation mithilfe von zuvor definierten Heuristiken durchgeführt werden. Die Evaluierenden können sich zusätzlich an den im ersten Durchgang gewonnenen Erkenntnissen, den zuvor definierten Aufgaben und den 4 Leitfragen orientieren.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Abu-Salma u. a. (2017) verwendeten Heuristic Walkthrough, um die UX und deren Implikationen der Informationssicherheit des Instant-Messaging-Diensts Telegram zu bewerten. Beispielsweise stellten sie fest, dass Telegram einen Standard-Chat und einen separat gesicherten Chat anbietet. Standardmäßig werden Telegram-Benutzer beim Klicken auf einen Kontakt zu einem nicht extra gesicherten Chat weitergeleitet. Telegram-Benutzer erhalten beim Klicken auf einen Kontakt keine unmittelbare Auswahl zum Öffnen des separat gesicherten Chats. Wie bereits erwähnt, vereint Heuristic Walkthrough den Cognitive

Walkthrough (siehe Abschnitt 5.2.4) und die Heuristische Evaluation (siehe Abschnitt 5.2.2.). Das heißt, beim Cognitive Walkthrough lassen sich zwar UX-Probleme und deren Implikationen zur Informationssicherheit finden, allerdings fehlt die Sicht der Endanwender, da lediglich Experten involviert sind. Bei einer heuristischen Evaluation kann zwar die UX und Informationssicherheit durch Heuristiken bewertet werden, allerdings wird die Bewertung der Zusammenhänge zwischen den Heuristiken nicht berücksichtigt.

5.2.6 Verfahren nach Gonzalez u. a.

Beschreibung des Verfahrens. Gonzalez u. a. (2009) entwickelten zunächst verschiedene Metriken, mit denen sich die UX und Informationssicherheit von E-Commerce-Webseiten bewerten lassen. Um die UX und Informationssicherheit von E-Commerce-Webseiten zu bewerten, wird jeder Metrik ein Score von 0 (negativ) bis 10 (positiv) zugordnet. Zusätzlich wird jeder Metrik eine Priorität von 0 (irrelevant) bis 10 (relevant) zugeordnet. Die Scores werden jeweils pro Metrik mit den Prioritäten multipliziert und aufsummiert, sodass jeweils ein Gesamtscore für die UX und für die Informationssicherheit resultiert.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Gonzalez u. a. (2009) verwendeten das entwickelte Verfahren mit deren Heuristiken, um die UX und Informationssicherheit von 30 verschiedenen E-Commerce-Webseiten zu bewerten. Durch das Verfahren lässt sich zwar jeweils ein Score für die UX und Informationssicherheit von E-Commerce-Webseiten berechnen, der gegenseitige Zusammenhang lässt sich damit aber nicht unmittelbar bewerten. Hierzu müsste die E-Commerce-Webseite verschiedene Varianten besitzen, die sich jeweils in einem Parameter der UX oder Informationssicherheit unterscheiden. Beispielsweise könnte eine erste Variante der E-Commerce-Plattform ein Passwort mit einer Mindestlänge von 6 Zeichen zulassen, während eine alternative Variante eine Mindestlänge von 10 Zeichen fordert. Nun kann das Verfahren von Gonzalez u. a. (2009) auf beide Varianten angewendet werden, um den Zusammenhang zwischen UX und Informationssicherheit beider Varianten zu bewerten. Ferner wurden die entwickelten Metriken speziell für E-Commerce-Webseiten entwickelt. Es müsste daher geprüft werden, inwiefern sich die entwickelten Heuristiken auf andere Software-Systeme, wie zum Beispiel Wallets, anwenden lassen.

5.2.7 Verfahren nach Alarifi u. a.

Beschreibung des Verfahrens. Alarifi u. a. (2017) entwickelten zunächst Metriken zur Bewertung der Usability und Informationssicherheit von E-Banking-Systemen. Daraufhin entwickelten sie ein Verfahren, mit dem sich der Zusammenhang zwischen UX und

Informationssicherheit von E-Banking-Systemen bewerten lässt: Anfangs wurden die Hardware- und Software-Assets einer Bank identifiziert und die Ziele hinsichtlich Usability und Informationssicherheit festgelegt. Seitens der Informationssicherheit wurden die Bedrohungen des E-Banking-Systems modelliert. Seitens der Usability wurde subjektives Feedback von Kunden und IT-Managern eingeholt. Außerdem wurden Daten von Benutzern gesammelt und ausgewertet. Anschließend wurden Konflikte der Usability und Informationssicherheit identifiziert und geprüft, ob sich Lösungen für die Konflikte finden lassen. Wenn sich für alle Konflikte Lösungen finden lassen, können die von Alarifi u. a. (2017) entwickelten Metriken verwendet werden, um die UX und Informationssicherheit zu bewerten. Falls keine Lösungen für Konflikte gefunden werden, werden zunächst die Auswirkungen eines Usability-Problems mit den Auswirkungen des assoziierten Informationssicherheit-Problems verglichen. Danach wird entschieden, ob die Usability oder Informationssicherheit bevorzugt werden soll. Anschließend werden die Risiken der Entscheidung bewertet, eine Strategie zur Abschwächung der Risiken festgelegt und eine Kosten-Nutzen-Analyse durchgeführt. Nachfolgend wird die Bewertung der Usability und Informationssicherheit mithilfe der entwickelten Metriken durchgeführt. Am Ende werden Empfehlungen zur Verbesserung vorgeschlagen.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Das von Alarifi u. a. (2017) entwickelte Verfahren lässt sich einsetzen, um den Zusammenhang zwischen Usability und Informationssicherheit von E-Banking-Systemen zu bewerten. Konkret werden Konflikte zwischen Usability und Informationssicherheit sowie Verbesserungsvorschläge gesammelt. Aspekte der Usability und Informationssicherheit, die sich positiv beeinflussen, werden nicht für die Formulierung der Verbesserungsvorschläge berücksichtigt. Außerdem bewertet das entwickelte Verfahren lediglich die Usability als ein Attribut der UX. Denkbar wäre allerdings, dass auch Metriken für weitere UX-Attribute entwickelt werden, damit sich auch andere UX-Attribute mit dem Verfahren bewerten lassen. Ferner wurde das Verfahren und die Metriken speziell für E-Banking-Systeme entwickelt. Es müsste daher geprüft werden, inwiefern sich die entwickelten Metriken auf andere Software-Systeme, wie zum Beispiel Wallets, anwenden lassen.

5.2.8 Thinking aloud

Beschreibung des Verfahrens. Thinking aloud (Nielsen, 1993) – dt. lautes Denken – ist ein benutzerbasiertes Evaluationsverfahren. Verschiedene Benutzer verwenden ein System und verbalisieren dabei ihre Gedanken. Dadurch kann der Moderator nachvollziehen, mit welchen Inhalten sich Benutzer beschäftigen, ob Fragen aufkommen und welche Emotionen sie verspüren. Eine Variante von Thinking aloud nennt sich Retrospective Testing (dt. retrospektive Prüfung). Hierbei wird das Nutzungsverhalten der Benutzer aufgenommen und nach der Verwendung durch die Benutzer anhand der

Aufnahme verbal kommentiert. Dies hat den Vorteil, dass der Moderator das aufgenommene Video beliebig stoppen und Benutzer ausführlicher befragen kann, ohne während der eigentlichen Bedienung eingreifen zu müssen. Zudem können die Kommentare der Benutzer ausführlicher sein, da sie nicht gleichzeitig versuchen, durch das System zu navigieren. Fernen kann das Retrospective Testing durch abschließendes verbales Kommentieren der Aufnahme einfach mit anderen Evaluationsverfahren kombiniert werden.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Marky u. a. (2020b) verwendeten Thinking aloud, um die UX und deren Implikationen zur Informationssicherheit eines E-Voting-Systems zu bewerten. Unter den Probanden befanden sich Experten für Informationssicherheit, die Implikationen der UX und Informationssicherheit sammelten. Anschließend wurden die Ergebnisse des Thinking aloud detaillierter mit den Probanden diskutiert und somit nochmals Implikationen der UX und Informationssicherheit gesammelt. Zusammenfassend lässt sich der Zusammenhang zwischen UX und Informationssicherheit durch Thinking aloud bewerten, indem einerseits Experten für Informationssicherheit die durch die Probanden identifzierten UX-Probleme betrachten (Retrospective Testing) und auf dieser Grundlage Implikationen zur Informationssicherheit dokumentieren. Andererseits können die Probanden Experten für Informationssicherheit sein und die Implikationen zur Informationssicherheit verbal während dem Thinking aloud äußern. Nach Nielsen (1993) kann Thinking aloud zu einem falschen Eindruck der tatsächlichen Ursachen der UX-Probleme führen, wenn Benutzer eigene Hypothesen der Ursachen aufstellen. So könnte ein Benutzer behaupten, dass ein Button zum Upload einer Datei deaktiviert gewesen sei. Tatsächlich war der Button aktiv, wurde jedoch kurzzeitig durch ein Lade-Icon überlagert. Die selbst gegebene Erklärung verdeckt die eigentliche Ursache.

5.2.9 GOMS

Beschreibung des Verfahrens. Nach John & Kieras (1994) ist Goals, Operators, Methods and Selection rules (GOMS) ein Verfahren, um die Usability eines Software-Systems zu evaluieren und Vorhersagen über Benutzerinteraktionen zu treffen. Goals meint Ziele, die Nutzer mit dem System erreichen wollen, zum Beispiel eine E-Mail versenden. Operators meint Operationen, also Aktionen der Benutzer, um ein Ziel zu erreichen, zum Beispiel den Browser öffnen, das E-Mail-Postfach öffnen und den Button zum Verfassen einer E-Mail drücken. Methods meint Methoden, die alle Operationen beinhalten, zum Beispiel eine E-Mail über den Browser versenden. Selection rules meinen Selektionsregeln, die zum Einsatz kommen, wenn mehrere Methoden existieren, um ein Ziel zu erreichen. Wenn beispielsweise eine E-Mail versendet werden soll, erfolgt dies über eine Smartphone-Anwendung anstatt über den Browser.

Es existieren mehrere GOMS-Varianten:

Das Keystroke-Level-Model (KLM) ermöglicht Vorhersagen über die Ausführungszeit, indem eine Zeit für jede Operation definiert wird und die einzelnen Zeiten aufsummiert werden. Das KLM wird in Form einer Sequenz erstellt und enthält für jede Operation eine Beschreibung, Dauer und Kategorie.

Bei Card, Moran und Newell (CMN)-GOMS wird eine Zielhierarchie erstellt, indem Methoden in einer Pseudocode-Notation dargestellt werden. Zusätzlich werden hierbei Selektionsregeln verwendet, falls mehrere Methoden existieren.

Natural GOMS-Language (NGOMSL) verwendet eine natürlichsprachige Pseudocode-Notation. Jedes Ziel wird auf die erforderlichen Operationen heruntergebrochen. Für jede Operation wird eine Ausführungszeit definiert, sodass die Gesamtausführungszeit vorhergesagt werden kann. Außerdem lässt sich mithilfe von NGOMS die Gesamtlernzeit vorhersagen, indem die Lernzeit für jede Operation definiert wird.

Cognitive-Perceptual-Motor (CPM)-GOMS basiert im Gegensatz zu den anderen GOMS-Varianten nicht auf einem sequenziellen Interaktionsprozess, sondern orientiert sich an einem realitätsnäheren Multitasking-Verhalten. So können Augenbewegungen und Mausklickbewegungen parallel berücksichtigt werden. Die einzelnen Operationen und ihre Abhängigkeiten werden in einem Ablaufdiagramm dargestellt. Die Gesamtausführungszeit lässt sich durch jene Folge von Operationen bestimmen, die in Summe die längste Ausführungszeit benötigt.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Kwon u. a. (2014) verwendeten CPM-GOMS, um Ausführungszeiten einzelner Benutzeraufgaben eines Authentifizierungsverfahren zu modellieren und dadurch die Gesamtausführungszeit zu bewerten. Ferner können UX-Experten die einzelnen Operationen zur Erreichung von Benutzerzielen betrachten, um UX-Probleme zu sammeln. Das heißt, unterschiedliche Software-Varianten mit unterschiedlichen Informationssicherheit-Niveaus können jeweils mit GOMS bewertet werden, um den Zusammenhang zwischen UX und Informationssicherheit zu bewerten. Denkbar wäre auch, dass Experten für Informationssicherheit die einzelnen Operationen hinsichtlich ihrer Informationssicherheit analysieren. Die gesammelten Probleme der UX sowie der Informationssicherheit und deren gegenseitige Beeinflussung können daraufhin durch Experten der UX und Informationssicherheit diskutiert werden. GOMS ist ein expertenbasiertes Evaluationverfahren und berücksichtigt damit nicht die tatsächlichen Bedürfnisse von Endnutzern.

5.2.10 Diary Study

Beschreibung des Verfahrens. Nach Cirucci & Pruchniewska (2021) wird eine Diary Study (dt. Tagebuchstudie) angewendet, indem verschiedene Benutzer einen Untersuchungsgegenstand bedienen und ihre Eindrücke in einem Tagebuch protokollieren. Der Untersuchungszeitraum reicht dabei von wenigen Tagen, über Monate bis hin zu Jahren. Eine Diary Study ist darauf ausgelegt, langfristige Verhaltensweisen von Benutzern zu verstehen, wie beispielsweise Benutzungszeiten oder -zwecke. Einerseits kann eine Diary Study offengehalten werden, das heißt, Benutzer dokumentieren ihre Erfahrungen mit dem Untersuchungsgegenstand ohne Vorgaben. Andererseits können den Benutzern vordefinierte Fragen gegeben werden, die sie zu bestimmten Zeiten am Tag oder nach Beendigung bestimmter Aufgaben beantworten sollen. Benutzer können beispielsweise gefragt werden, welche Software-Funktionen sie verwendet haben, wann und wie lange sie diese benutzt haben und was schlecht/gut bei der Benutzung lief.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Mare u. a. (2016) führten eine Diary Study durch, bei der 26 Teilnehmer ihre Eindrücke bei der täglichen Verwendung von unterschiedlichen Authentifizierungsverfahren (Passwörter, Fingerabdruck, etc.) dokumentierten. So konnten sie Erkenntnisse der UX (zum Beispiel Fehlerraten und Schwierigkeiten während der Benutzung) von verschiedenen Authentifizierungsverfahren mit unterschiedlichen Informationssicherheit-Niveaus gewinnen. Das heißt, mithilfe einer Diary Study können qualitative Erkenntnisse von Endnutzern über den Zusammenhang zwischen UX und Informationssicherheit gewonnen werden. Da eine Diary Study ein benutzerbasiertes Evaluationsverfahren ist, fehlen allerdings die Erkenntnisse von Experten für UX und Informationssicherheit. Außerdem ist eine Diary Study für die Gewinnung von Evaluationsergebnissen über einen längeren Zeitraum hinweg ausgelegt und nicht um kurzfristig Evaluationsergebnisse zu erhalten. Dies kann insbesondere dann problematisch sein, wenn zeitnahe Rückmeldungen für eine iterative Entwicklung benötigt werden.

5.2.11 Fokusgruppen

Beschreibung des Verfahrens. Mithilfe von Fokusgruppen (Krueger und Casey, 2015) können Bedürfnisse und Gefühle von Benutzern eines Software-Systems bewertet werden. Dazu diskutieren die Benutzer in unterschiedlichen Gruppen verschiedene Stärken und Schwächen der UX, wie beispielsweise Hürden, die während der Benutzung aufgetreten sind. Ein Moderator leitet die Diskussion und stellt offene Fragen. Die Fragen zu Beginn sind allgemeiner gehalten, damit die Benutzer zum Nachdenken und Diskutieren angeregt werden. Im weiteren Verlauf werden die Fragen spezifischer und gezielter. Einerseits sollte der Moderator dabei sicherstellen, dass die Diskussion aufrecht erhalten

bleibt, insbesondere dass alle Benutzer zur Diskussion beitragen und nicht eine Meinung dominiert. Andererseits darf er nicht zu stark eingreifen, damit Ideen und Kommentare nicht verhindert werden. Die Ergebnisse der unterschiedlichen Gruppen werden abschließend dokumentiert und miteinander verglichen.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Marky u. a. (2020a) entwickelten ein 2-Faktor-Authentifizierungsverfahren, das sie mithilfe von Fokusgruppen evaluierten. In den Fokusgruppen waren sowohl Experten der UX als auch der Informationssicherheit involviert. Das heißt, mithilfe von Fokusgruppen kann der Zusammenhang zwischen UX und Informationssicherheit diskutiert werden, wenn sowohl Experten der UX als auch der Informationssicherheit in den einzelnen Fokusgruppen involviert sind. Da die Meinungen von Experten von tatsächlichen Bedürfnissen der Endnutzer abweichen können (Jaspers, 2009), sollten auch Endnutzer miteinbezogen werden. Das heißt, es sollten Fokusgruppen mit Endnutzern als auch mit Experten der UX und Informationssicherheit durchgeführt werden.

5.2.12 Eye Tracking

Beschreibung des Verfahrens. Mithilfe von Eye Tracking (Bojko, 2005) können Blickrichtungen und -bewegungen von Benutzern gemessen bzw. berechnet werden. Ein hohes Benutzerinteresse und eine hohe Informationsdichte von bestimmten User Interface-Elementen zeigen sich in einer erhöhten Anzahl an Augenfixierungen. Eine hohe Fixationsdauer kann darauf hindeuten, dass zu viele, mehrdeutige oder unklare Informationen des User Interface zu sehen sind, was die Informationsverarbeitung der Benutzer verlängert. Die Reihenfolge der betrachteten User Interface-Elemente, die Anzahl der Augenfixierungen und die Zeit bis zur ersten Augenfixierung sind Kennzahlen für die Effektivität eines Software-Systems. Eine hohe Wichtigkeit eines User Interface-Elements spiegelt sich in einer hohen Besuchshäufigkeit, einem hohen Prozentsatz von Benutzern, die das User Interface-Elemente mit den Augen fixieren, und darin wider, dass das User Interface-Element als eines der ersten User Interface-Elemente fixiert wird. Das Gerät zur Messung der Augenbewegungen wird als Eye Tracker bezeichnet. Es existieren verschiedene Eye Tracker, die sich in der Art, mit der sie die Position der Augen verfolgen, und in ihrer physischen Form unterscheiden. Manche Eye Tracker sind besonders für Benutzertests an einem Bildschirm geeignet, während andere darauf ausgelegt sind, das Blickverhalten in natürlichen Umgebungen zu erfassen.

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Darwish & Bataineh (2012) verwendeten Eye Tracking, um die Augenfixierungen von Probanden bei der Bedienung einer Phishing-Webseite zu evaluieren. Beispielsweise wurden relevante Sicherheitshinweise aufgrund des Designs übersehen. Außerdem wurde ersichtlich,

dass die Einführung von Farben im Hintergrund der Domain die durchschnittliche Zeit bis zur Augenfixierung der Domain verbessert bzw. reduziert hat. Mit Eye Tracking lässt sich also herausfinden, inwiefern sich bestimmte User Interface-Elemente auf die Informationssicherheit auswirken, beispielsweise ob sicherheitsrelevante Informationen von Benutzern betrachtet werden. Außerdem kann bewertet werden, inwiefern sich Informationssicherheitsmechanismen auf die UX auswirken, indem beispielsweise die Zeit zur Beendigung einer Benutzeraufgabe (Effizienz) für verschiedene Software-Varianten mit unterschiedlichen Informationssicherheitsmechanismen gemessen wird. Dazu müssen allerdings verschiedene Software-Varianten mit unterschiedlichen Informationssicherheit-Niveaus vorliegen, die sich lediglich durch einen veränderten Parameter der Informationssicherheit unterscheiden, zum Beispiel durch ein anderes Authentifizierungsverfahren. Eye Tracking ist ein benutzerbasierts Evaluationsverfahren. Die Meinungen von Experten der UX und Informationssicherheit werden dabei nicht berücksichtigt.

5.2.13 Fragebögen

Beschreibung des Verfahrens. Sauer u. a. (2024a) identifizierten 10 Fragebögen, die eingesetzt wurden, um den Zusammenhang zwischen UX und Informationssicherheit zu bewerten:

Usefulness, Satisfaction and Ese of use (USE) (Lund, 2001), UX Needs Scale (Lallemand und Koenig, 2017), Attrakdiff 2 (Hassenzahl u. a., 2003), After-Scenario Questionnaire (ASQ) (Lewis, 1991), Kurzversion von User Experience Questionnaire (UEQS) (Schrepp u. a., 2017), Subjective Mental Effort Question (SMEQ) (Sauro und Dumas, 2009), User Experience Questionnaire (UEQ) (Laugwitz u. a., 2008), System Usability Scale (SUS) (Brooke, 1996), Questionnaire for User Interface Satisfaction (QUIS) (Chin u. a., 1988) und Lewis' Post-Study System Usability Questionnaire (PSSUQ) (Lewis, 1995).

Diskussion des Zusammenhangs zwischen UX und Informationssicherheit. Fragebögen können eingesetzt werden, um die UX von verschiedenen Software-Varianten mit unterschiedlichen Informationssicherheit-Niveaus zu bewerten. Beispielsweise verwendeten Marky u. a. (2021) die Fragebögen SUS und UEQ zur Bewertung der UX von verschiedenen Wahlsystemen, die sich durch unterschiedliche Niveaus der Informationssicherheit unterschieden. Die Informationssicherheit kann allerdings durch die identifizierten Fragebögen nicht bewertet werden. Das heißt, die unterschiedlichen Informationssicherheit-Niveaus der Software-Varianten müssen separat (mithilfe von anderen Evaluationsverfahren) bewertet werden.

5.2.14 Gegenüberstellung und Diskussion

Nun werden die identifizierten Verfahren aus den vorherigen Abschnitten 5.2.1 bis 5.2.13 zunächst anhand von 3 Kriterien bewertet und einander gegenübergestellt. Anschließend werden die Erkenntnisse zusammengefasst und diskutiert.

Ein geeignetes Verfahren zur Bewertung des Zusammenhangs zwischen UX und Informationssicherheit sollte sowohl Usability- als auch andere UX-Attribute in die Bewertung miteinbeziehen. Zusätzlich sollte es Experten- sowie Endnutzer involvieren, da die Meinungen stark voneinander abweichen können (Jaspers, 2009) und Endnutzer keinen Einblick auf sicherheitsrelevante Komponenten eines Software-Systems haben. Zudem ist es wichtig, dass das Verfahren bereits in der Entwurfsphase eines Software-Systems eingesetzt werden kann, damit frühzeitig Verbesserungsvorschläge berücksichtigt werden können.

(EK1) Art der Evaluierenden: Hiermit soll bewertet werden, ob das jeweilige Verfahren Experten der UX/Informationssicherheit und/oder Endnutzer miteinbezieht.

Nur eines der identifizierten Verfahren ist experten- und endnutzerbasiert, nämlich SecureUse Score. 7 Verfahren sind ausschließlich expertenbasiert: Heuristische Evaluation, Security Usability Symmetry, Cognitive Walkthrough, Heuristic Walkthrough, Verfahren nach Gonzalez u. a. und Alarifi u. a. sowie GOMS. 5 Verfahren sind ausschließlich endnutzerbasiert: Thinking aloud, Diary Study, Fokusgruppen, Eye Tracking und Fragebögen (Sauer u. a., 2024a).

Die folgende Tabelle 4 zeigt die identifizierten Verfahren und die Art der Evaluierenden.

	Endnutzer	Experten
SecureUse Score	X	X
Heuristische Evaluation		X
Security Usability Symmetry		X
Cognitive Walkthrough		X
Heuristic Walkthrough		X
Verfahren nach Gonzalez u. a.		X
Verfahren nach Alarifi u. a.		X
Thinking aloud	X	
GOMS		X
Diary Study	X	
Fokusgruppen	X	
Eye Tracking	X	
Fragebögen	X	

Tabelle 4: Evaluationsverfahren kategorisiert nach Art der Evaluierenden. (Sauer u. a., 2024a). Übersetzt aus dem Englischen.

(EK2) Integrationszeitpunkt: Mithilfe des Integrationszeitpunkts wird bewertet, ob das jeweilige Verfahren bereits in der Entwurfsphase eines Software-Systems angewendet werden kann, beispielsweise bei Mockups.

Nach Sauer u. a. (2024a) lassen sich alle recherchierten Verfahren bereits in der Entwurfsphase eines Software-Systems anwenden, um relevante Erkenntnisse bereits früh im Entwicklungsprozess zu erheben.

(EK3) Usability/UX: Einige der Verfahren betrachten in der Bewertung des Zusammenhangs zwischen UX und Informationssicherheit ausschließlich Usability als ein Attribut der UX. Ferner wurden auch Verfahren identifiziert, die sich breiter auf die Bewertung der UX konzentrieren, das heißt, ohne speziellen Fokus auf einzelne UX-Attribute. Daher wird mit EK3 bewertet, ob sich mit dem jeweiligen Verfahren Usability und/oder andere UX-Attribute bzw. allgemeiner UX bewerten lassen.

Nach Sauer u. a. (2024a) lassen sich mit 10 der identifizierten Verfahren ausschließlich Usability bewerten: SecureUse Score, Heuristische Evaluation, Security Usability Symmetry, Cognitive Walkthrough, Heuristic Walkthrough, Verfahren nach Gonzalez u. a. und Alarifi u. a., Thinking aloud, GOMS und Fokusgruppen. Mit 2 Verfahren lassen sich ausschließlich UX ohne Fokus auf die Usability bewerten: Diary Study und Eye Tracking. Unter den Fragebögen kann ausschließlich Usability mit 6 Fragebögen bewertet werden: USE, ASQ, SMEQ, SUS, QUIS und PSSUQ. Die UX ohne Fokus auf die Usability lässt sich durch 4 Fragebögen bewerten: UX Needs Scale, Attrakdiff 2, UEQ-S und UEQ. Da mittlerweile auch diverse Heuristiken anderer UX-Attribute als Usability entwickelt wurden, lassen sich mit der Heuristischen Evaluation und dem Heuristic Walkthrough auch andere UX-Attribute (als Usability) bewerten. Durch eine Fokusgruppe können nicht nur Usability-Schwächen diskutiert werden, sondern auch Schwächen anderer UX-Attribute, wie beispielsweise Barrierefreiheit.

Die folgende Tabelle 5 zeigt die identifizierten Verfahren und die diskutierten Aspekte hinsichtlich der Bewertung von Usability und UX. Da sich in diesem Kriterium auch Fragebögen unterscheiden, wurden diese einzeln aufgeführt und kategorisiert.

	Usability	UX
SecureUse Score	X	
Heuristische Evaluation	X	X
Security Usability Symmetry	X	
Cognitive Walkthrough	X	
Heuristic Walkthrough	X	X
Verfahren nach Gonzalez u. a.	X	
Verfahren nach Alarifi u. a.	X	
Thinking aloud	X	X

GOMS	X	
Diary Study	X	X
Fokusgruppen	X	X
Eye Tracking		X
USE	X	
UX Needs Scale		X
Attrakdiff 2		X
ASQ	X	
UEQ-S		X
SMEQ	X	
UEQ		X
SUS	X	
QUIS	X	
PSSUQ	X	

Tabelle 5: Evaluationsverfahren kategorisiert nach Usability/UX. (Sauer u. a., 2024a). Übersetzt aus dem Englischen.

Zusammenfassend lässt sich sagen, dass SecureUse Score das einzige identifizierte Verfahren ist, das sowohl Experten als auch Endnutzer inkludiert. Allerdings lassen sich damit nur die Informationssicherheit und Usability bewerten, aber keine weiteren UX-Attribute. Die restlichen Verfahren sind entweder experten- oder endnutzerbasiert und sollten daher nicht alleine angewendet, sondern kombiniert werden. Da mittlerweile nicht nur Heuristiken der Usability, sondern auch Heuristiken weiterer UX-Attribute entwickelt wurden, lassen sich durch die Heuristische Evaluation und Heuristic Walkthrough auch weitere UX-Attribute (als Usability) bewerten. Die Bewertung der Beeinflussung von einzelnen Heuristiken ist allerdings in den Verfahren nicht vorgesehen und muss zusätzlich durchgeführt werden. Auch mit Thinking aloud, Diary Study und Fokusgruppen lassen sich nicht nur Usability, sondern auch weitere UX-Attribute bewerten. So können UX-Schwächen durch Endnutzer gesammelt und Implikationen zur Informationssicherheit diskutiert werden. Darüber hinaus müssen bei SecureUse Score, GOMS, Eye Tracking und den identifizierten Fragebögen unterschiedliche Software-Varianten, die sich in einem Parameter unterscheiden, vorliegen, um Aussagen über die Beeinflussung von UX und Informationssicherheit treffen zu können. Die Bewertung muss für jede Software-Variante neu durchgeführt und verglichen werden. Die Verfahren nach Gonzalez u. a. und nach Alarifi u. a. sowie Security Usability Symmetry wurden lediglich für spezifische Software-Systeme entwickelt.

Nach Gegenüberstellung und Bewertung der recherchierten Evaluationsverfahren anhand der 3 Kriterien EK1 bis EK3 lässt sich Folgendes feststellen:

Keines der recherchierten Verfahren lässt sich verwenden, um den Zusammenhang zwischen UX, insbesondere mit Berücksichtigung weiterer UX-Attribute als Usability,

und Informationssicherheit sowohl experten- als auch endnutzerbasiert zu evaluieren. Daher soll im Rahmen dieser Arbeit eine Methode entwickelt werden, die einerseits den Zusammenhang zwischen UX und Informationssicherheit evaluieren kann, andererseits aber auch Verbesserungsvorschläge gibt. Dazu lassen sich gegebenenfalls identifizierte Verfahren adaptieren. Denkbar wäre beispielsweise eine Adaption von Heuristic Walkthrough (bestehend aus Cognitive Walkthrough und Heuristische Evaluation) und Thinking aloud. Durch Heuristic Walkthrough lassen sich auch weitere UX-Attribute als Usability evaluieren. Cognitive Walkthrough könnte durch Thinking aloud ersetzt werden, damit tatsächliche Endnutzer in der Evaluation involviert sind und nicht nur Experten, die sich in Endnutzer hineinversetzen. Ferner sind die Verfahren Heuristic Walkthrough und Thinking aloud beide bereits in der Entwurfsphase von Software einsetzbar. Die gegenseitige Beeinflussung von UX und Informationssicherheit könnte daraufhin zwischen den einzelnen Heuristiken bewertet werden. Die Heuristiken, mit den Erkenntnissen der Beeinflussung untereinander, könnten daraufhin als Verbesserungsvorschläge von UX und Informationssicherheit dienen.

5.3 Durchführung einer Evaluation der User Experience und Informationssicherheit von Wallets

Nach der Recherche von Verfahren zur Evaluation des Zusammenhangs von UX und Informationssicherheit wurden einige der Verfahren auf einen Wallet-Prototyp angewendet. Dadurch wurden Erkenntnisse einerseits über den Wallet-Prototyp und andererseits über die Evaluationserverfahren gewonnen. Abschnitt 5.3.1 erläutert zunächst bereits bekannte Schwächen der UX und Informationssicherheit von Wallets. Abschnitt 5.3.2 beschreibt die Durchführung der Evaluation.

5.3.1 Ausgangslage und verwandte Arbeiten

Wallets besitzen unterschiedliche Schwächen der UX und Informationssicherheit:

Selbst technisch versierte Probanden von Khayretdinova u. a. (2022) hatten Probleme beim Einrichten der Wallet und beim Verwalten von Verifiable Credential (VC, siehe Definition 2-2), da die Wallet für die Probanden schwer zu bedienen und nicht intuitiv war. Dies kann zu Frustration von Wallet-Benutzern oder zu Sicherheitsproblemen führen, wie beispielsweise ungewolltes Teilen von VC. Ferner war einigen Probanden nicht klar, wo ihre VC bzw. Daten gespeichert werden. Teilweise wurde versucht, Daten

vom Server zu löschen, obwohl die Daten nur lokal auf dem Smartphone gespeichert wurden.

Khayretdinova u. a. (2022) identifizierten Schwächen hinsichtlich der Erlernbarkeit von Wallet-Funktionen. Beispielsweise haben Probanden das erste VC mit einer Hilfestellung erhalten und erfolglos versucht, ein zweites VC auf gleiche Art und Weise zu erlangen.

Probanden von Sartor u. a. (2022) empfanden die in der Wallet verwendete Terminologie zu technisch formuliert, da beispielsweise „Credentials“ und „DID“ verwendet wurde. Außerdem forderten Probanden mehr Hilfestellungen, insbesondere ein Tutorial beim Einrichten der Wallet, das die Grundfunktionen erklärt. Ferner kam der Wunsch nach einer Backup- und Recovery- sowie Such- und Sortier-Funktion von VC auf.

Sellung & Kubach (2023) identifizierten keine Wallet, mit der sich der Account und die zugehörigen VC in eine andere Wallet übertragen lassen (weder in die gleiche Wallet auf anderen Smartphones, noch in Wallets anderer Anbieter). Daraus entsteht ein Lock-In-Effekt, da der Wechsel zu einer anderen Wallet umständlich ist.

Die Evaluation von Satybaldy (2023) ergab, dass einige Wallets keine sicheren Authentifizierungsverfahren besitzen, um die sensiblen Daten in der Wallet zu schützen. Bei einer der untersuchten Wallets funktionierte die biometrische Authentifizierung nicht korrekt. Zudem hatten Wallet-Benutzer Probleme, den Wiederherstellungscode zu finden und die Funktionsweise sowie den Nutzen davon zu verstehen.

Probanden von Korir u. a. (2022) äußerten Sicherheitsbedenken hinsichtlich unautorisierter Datenzugriffe und der möglichen Weitergabe ihrer Daten ohne ausdrückliche Zustimmung. Ferner waren QR-Codes die Ursache für einige Unterbrechungen der Benutzung, was die Effizienz minderte. Zudem sollte stärker berücksichtigt werden, dass Wallets auf Mobilgeräten nicht nur mit Anwendungen auf Laptops interagieren, sondern auch mit anderen Anwendungen auf demselben Mobilgerät.

Aufgrund der beschriebenen Schwächen der UX und Informationssicherheit von existierenden Wallets müssen UX und Informationssicherheit von Wallets auf ein adäquates Niveau verbessert werden. Insbesondere im Hinblick auf die EU-weite Einführung von Wallets bis Ende 2026 ist dies von Bedeutung. Dafür ist es wichtig, dass die UX und Informationssicherheit von Wallets nicht nur separat evaluiert und verbessert werden, sondern auch der Zusammenhang zwischen UX und Informationssicherheit betrachtet wird, da sich UX und Informationssicherheit beeinflussen können (siehe Abschnitt 5.1). Deshalb wurde eine eigene Evaluation durchgeführt, die identifizierte Verfahren aus Abschnitt 5.2 inkludiert und die im Folgenden weiter beschrieben wird.

5.3.2 Durchführung der Evaluation

Sauer u. a. (2025b) evaluierten zunächst die UX eines Software-Prototyps, der die Interaktion einer Wallet mit einer Mobilitätsplattform demonstriert. Anschließend leiteten Sauer u. a. (2025b) die Implikationen zwischen UX und Informationssicherheit ab.

Methode:

Der Software-Prototyp beinhaltete grundsätzlich 2 Teile: (1) Die Aktivierung des Car-Sharing Providers „stadtmobil“[20] in der Mobilitätsplattform „regiomove“[21] mittels eines Videoidentifikationsverfahrens des Führerscheins und (2) der Export des Führerschein-VC aus regiomove in eine Wallet. In Teil 1 sollte zunächst auf einem Smartphone die regiomove-App geöffnet und zu den Account-Einstellungen über einen Button in der Menüleiste navigiert werden. In den Account-Einstellungen sollte zum Untermenü „Konto bearbeiten“ navigiert und darin zum stadtmobil-Menü gewechselt werden. Nun erschienen verschiedene Möglichkeiten zur Freischaltung von stadtmobil und es sollte auf den Button „Weiter“ gedrückt werden. Daraufhin sollten fiktive Personalausweis- und Führerscheindaten eingegeben werden. Anschließend wurde ein fiktives Videoidentifikationsverfahren durchgeführt. Danach wurde stadtmobil erfolgreich freigeschaltet und es sollte zum stadtmobil-Menü navigiert werden. Über einen Button „Führerschein exportieren“ konnte nun das Führerschein-VC in die Wallet exportiert werden. Bei Klick des Buttons erschien zunächst ein Menü, auf dem die Wallet ausgewählt werden sollte. Anschließend öffnete sich die entsprechende Wallet und eine Authentifizierung wurde durchgeführt. Hier unterteilte sich der Prototyp in 4 Varianten, die jeweils ein anderes Authentifizierungsverfahren besaßen: 4-stelliger Pin, 6-stelliger Pin, Passwort „Sdik4%23“ und Fingerscan. Danach erschien ein Dialog, der die Daten des VC und einen Bestätigungsbutton zur Speicherung des VC in der Wallet beinhaltete. Sobald dieser Bestätigungsbutton gedrückt wurde, erschien ein zusätzlicher Dialog, um die Speicherung des VC in der Wallet zu bestätigen.

Abbildung 15 visualisiert den beschriebenen Prozess. Zusätzlich sind die entsprechenden Screens und eine detailliertere Beschreibung unter (Sauer u. a., 2024c) einsehbar.

[20] Stadtmobil ist ein deutscher Car-Sharing-Anbieter, der die gemeinschaftliche Nutzung von Kraftfahrzeugen organisiert und seinen registrierten Kunden Fahrzeuge zeitlich befristet gegen eine Vergütung zur Verfügung stellt. https://stadtmobil.de.

[21] Regiomove ist eine regionale Mobilitätsplattform des Karlsruher Verkehrsverbunds (KVV). Sie integriert Angebote des Bus- und Schienenverkehrs mit Car- und Bikesharing-Diensten und stellt deren Planung, Buchung und Abrechnung über eine zentrale digitale Anwendung bereit. https://kvv.de/mobilitaet/regiomove.

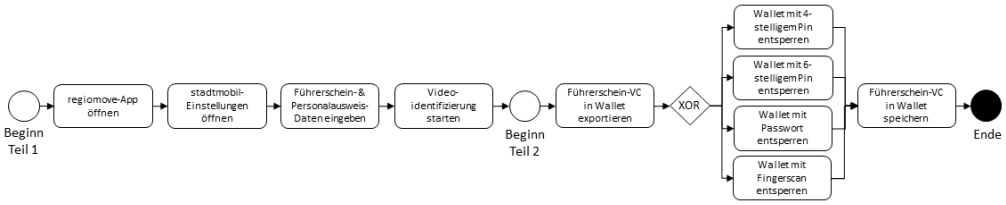


Abbildung 15: Ablauf einer exemplarischen Nutzung des Software-Prototyps. (Sauer u. a., 2025b). Übersetzt aus dem Englischen.

Für die Evaluation des Software-Prototyps waren insgesamt 24 Probanden im Alter von 18 bis 83 Jahren involviert. Es wurden 4 Gruppen mit jeweils 6 Probanden gebildet, die jeweils eine Prototyp-Variante bedienten. Es führten also alle 24 Probanden die gleichen Aktivitäten bis auf die Entsperrung der Wallet mittels unterschiedlichen Authentifizierungsverfahren durch. Es wurde darauf geachtet, dass die Probanden gruppenübergreifend ähnliche demografische Daten besaßen. Hierzu wurden insbesondere Alter, Geschlecht, Deutschkenntnisse, höchster Bildungsabschluss, Vorerfahrung mit Wallets und/oder regiomove, IT-Affinität und Betriebssystem auf dem privaten Smartphone berücksichtigt. Die detaillierten demografischen Daten sind online verfügbar[22].

Am Anfang der Evaluation bekamen alle Probanden einen demografischen Fragebogen und eine Einverständniserklärung zur Datenerhebung vorgelegt. Danach erhielten die Probanden eine Anleitung mit relevanten Informationen zur Evaluation: Die Probanden wurden gebeten, sich in eine fiktive Person namens Robert Glaser hineinzuversetzen. Anstelle eines realen Videoidentifikationsverfahren erschien ein fiktives Standbild einer Person und es gab keine reale Validierung des Führerscheins. Zusätzlich sollten keine persönlichen Daten eingegeben werden. Stattdessen wurden die Daten in den Eingabefeldern automatisch mit den Daten des fiktiven Robert Glaser ausgefüllt. Auch die einzelnen Aufgaben, die von den Probanden zu erfüllen waren, wurden beschrieben. Nun sollten die Probanden mit Teil 1 (siehe Abbildung 15) starten und die entsprechenden Funktionen des Software-Prototyps mithilfe der Anleitung durchführen. Hierzu sollten sie im gesamten Teil 1 Thinking aloud (siehe Abschnitt 5.2.8) anwenden, das heißt, ihre Gedanken während der Bedienung laut äußern, damit UX-Schwächen gesammelt werden konnten. Hierzu wurde der Screen des Smartphones, mit dem der Software-Prototyp bedient wurde, aufgezeichnet. Zusätzlich wurden Mimik, Gestik und Audio aufgenommen. In Teil 2 wurde Eye Tracking (siehe Abschnitt 5.2.12) eingesetzt – zur Aufzeichnung der Augenfixationspunkte auf den einzelnen Screens und schlussendlich zur Prüfung der Eye Tracking-Hypothesen (EH1-7). Die Eye Tracking-Hypothesen wurden im

[22] https://doi.org/10.5281/ZENODO.12785376

Vorfeld gezielt formuliert, um Implikationen zwischen UX und Informationssicherheit zu untersuchen. Die Eye Tracking-Hypothesen lassen sich zukünftig noch erweitern.

EH1: Die Probanden lesen den Informationstext im stadtmobil-Menü zum Export des Führerschein-VC in die Wallet.

EH2: Die Probanden erkennen den Informationsbutton im stadtmobil-Menü zum Export des Führerschein-VC in die Wallet.

EH3: Die Probanden lesen die Informationen im stadtmobil-Menü zum Export des Führerschein-VC in die Wallet linear von oben nach unten.

EH4: Die Probanden erkennen im Dialog der Wallet zur Speicherung des Führerschein-VC, dass der Aussteller des Führerschein-VC nicht verifiziert ist.

EH5: Die Probanden lesen im Dialog der Wallet zur Speicherung des Führerschein-VC den gesamten Informationstext über den Aussteller des Führerschein-VC.

EH6: Die Probanden lesen die Detailinformationen (Claims) des Führerschein-VC im Dialog der Wallet zur Speicherung des Führerschein-VC.

EH7: Die Probanden lesen im Dialog der Wallet zur Speicherung des Führerschein-VC zuerst alle Informationen und drücken dann den Button zur Speicherung des VC.

Zusätzlich wurden die Login-Zeiten gemessen, um die Effizienz der unterschiedlichen Wallet-Authentifizierungsverfahren zu evaluieren.

Nach Durchführung von Teil 2 bekamen die Probanden 2 UX-Fragebögen vorgelegt, die sie ausfüllen sollten. Als Fragebögen wurden UEQ-S (siehe Abschnitt 5.2.13) und SUS (siehe Abschnitt 5.2.13) verwendet.

Nach der UX-Evaluation wurden die Implikationen zwischen UX und Informationssicherheit gesammelt. Dafür wurden die Ergebnisse der UX-Evaluation mit einem wissenschaftlichen Mitarbeiter aus dem Bereich Informationssicherheit, mit 2 wissenschaftlichen Mitarbeitern aus dem Bereich UX und Informationssicherheit sowie mit 2 Wallet-Entwicklern diskutiert und dokumentiert.

Ergebnisse:

Die Ergebnisse des SUS-Fragebogens werden auf einer Skala von 0 bis 100 angegeben. Diese zeigen, dass die Prototyp-Variante mit 6-stelligem Pin am besten abgeschnitten hat (Ø: 75,4). Anschließend folgen die Prototyp-Varianten mit Fingerscan (Ø: 69,2) und 4-stelligem Pin (Ø: 66,9). Am schlechtesten hat die Prototyp-Variante mit Passwort abgeschnitten (Ø: 52,5). Abbildung 16 visualisiert die beschriebenen SUS-Werte.

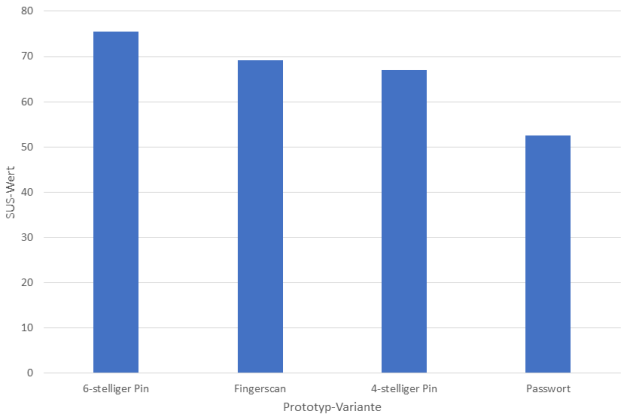


Abbildung 16: SUS-Wert je Prototyp-Variante. (Sauer u. a., 2025b). Übersetzt aus dem Englischen.

Zudem wurde der SUS-Gesamtwert aller Prototyp-Varianten je Altersgruppe berechnet. Es wird deutlich, dass die Probanden unter 20 Jahren den Prototyp am besten bewertet haben (Ø: 79,5). Danach folgen die Werte der Probanden im Alter von 20 bis 29 Jahren (Ø: 68,4), 50 bis 60 Jahren (Ø: 67,5) und 30 bis 49 Jahren (Ø: 58,6). Der SUS-Gesamtwert der Probanden im Alter über 60 Jahren ist am schlechtesten (Ø: 41,3). Abbildung 17 visualisiert die beschriebenen SUS-Gesamtwerte je Altersgruppe.

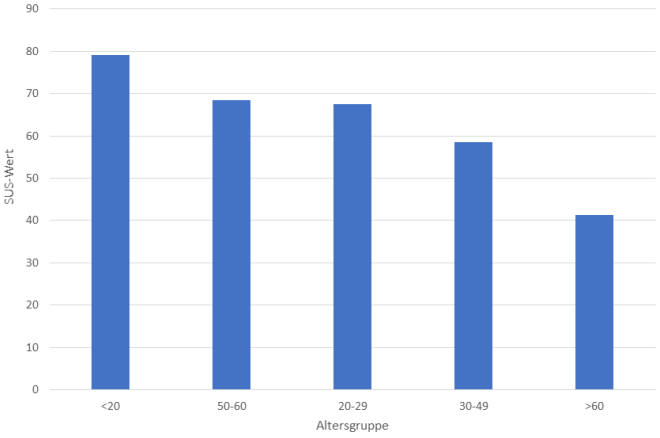


Abbildung 17: SUS-Gesamtwert des Prototyps je Altersgruppe. (Sauer u. a., 2025b). Übersetzt aus dem Englischen.

Die Ergebnisse des UEQ-S-Fragebogens wurden auf einer Skala von -3 bis 3 angegeben. Diese zeigen, dass die Prototyp-Variante mit 4-stelligem Pin am besten abgeschnitten hat (Ø: 0,77). Anschließend folgen die Prototyp-Varianten mit Fingerscan (Ø: 0,52) und 6-stelligem Pin (Ø: 0,42). Die Prototyp-Variante mit Passwort schnitt am schlechtesten ab

(Ø: 0,02), wie auch beim SUS-Fragebogen. Abbildung 18 visualisiert die beschriebenen UEQ-S-Werte der einzelnen Prototyp-Varianten.

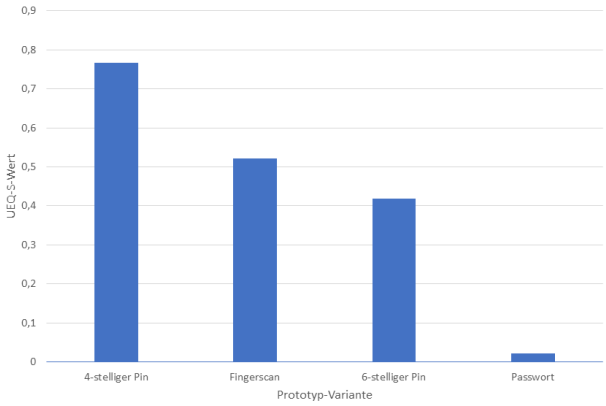


Abbildung 18: UEQ-S-Wert je Prototyp-Variante. (Sauer u. a., 2025b). Übersetzt aus dem Englischen.

Zudem wurde der UEQ-S-Gesamtwert aller Prototyp-Varianten berechnet und nach Altersgruppen kategorisiert. Es wird deutlich, dass die Probanden unter 20 Jahren den Prototyp am besten bewertet haben (Ø: 0,67), wie auch beim SUS-Fragebogen. Danach folgen die Werte der Probanden im Alter von 20 bis 29 Jahren (Ø: 0,57), 50 bis 60 Jahren (Ø: 0,13) und 39 bis 49 Jahren (Ø: 0,02), wie auch beim SUS-Fragebogen. Der UEQ-S-Gesamtwert der Probanden im Alter über 60 Jahren ist am schlechtesten (Ø: -0,03), wie auch beim SUS-Fragebogen. Abbildung 19 visualisiert die beschriebenen UEQ-S-Gesamtwerte je Altersgruppe.

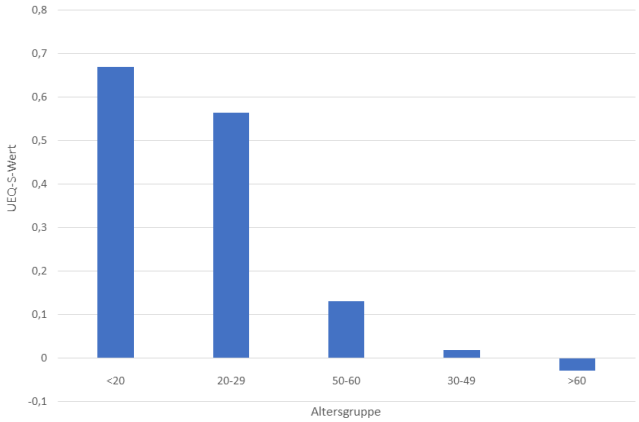


Abbildung 19: UEQ-S-Gesamtwert des Prototyps je Altersgruppe. (Sauer u. a., 2025b). Übersetzt aus dem Englischen.

Des Weiteren wurden die durchschnittlichen Login-Zeiten je Authentifizierungsverfahren gemessen. Die Eingabe des Passworts dauerte durchschnittlich am längsten (Ø: 39 Sekunden). Danach folgte der 6-stellige Pin (Ø: 17,6 Sekunden) und der Fingerscan (Ø: 7,8 Sekunden). Am besten schnitt der 4-stellige Pin ab (Ø: 5,7 Sekunden). Abbildung 20 visualisiert die beschriebenen Login-Zeiten je Authentifizierungsverfahren.

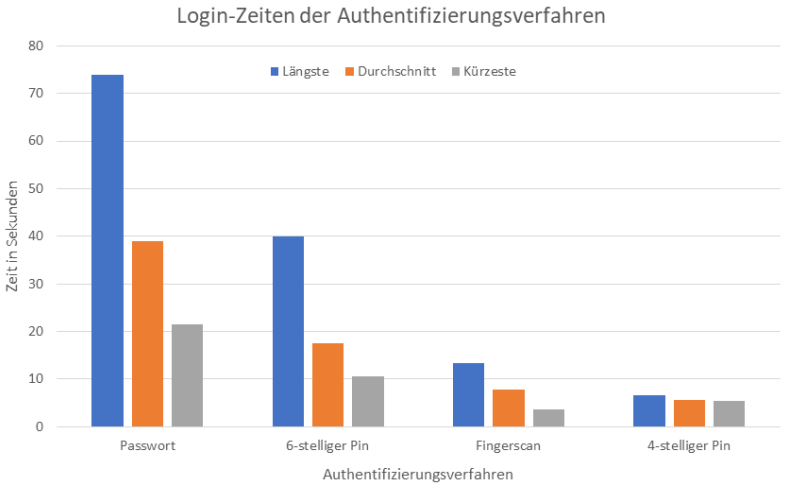


Abbildung 20: Login-Zeiten. (Sauer u. a., 2025b). Übersetzt aus dem Englischen.

Nun wird auf die Eye Tracking-Ergebnisse eingegangen, indem die Untersuchungsergebnisse der zuvor definierten Eye Tracking Hypothesen (EH1 bis EH7) vorgestellt werden.

EH1: 17 der 24 Probanden haben den Informationstext im stadtmobil-Menü zum Exportieren des Führerschein-VC in die Wallet nicht gelesen. Die Heatmap in Abbildung 21 zeigt, dass der Bereich nur leicht grün und gelb eingefärbt ist, was bedeutet, dass dieser Bereich kaum betrachtet wurde. Insbesondere alle Probanden unter 20 Jahren haben den Informationstext nicht gelesen. Die Augenfixierungspunkte und deren Reihenfolge (sogenannter Scanpath) der Probanden in Abbildung 21 zeigen, dass der Informationstext lediglich überflogen wurde. Möglicherweise kennen jüngere Probanden bereits ähnliche Interaktionsmuster von anderen Software-Systemen, wodurch sie dazu neigen, Informationstexte nicht zu lesen und direkt den Export-Button drücken.

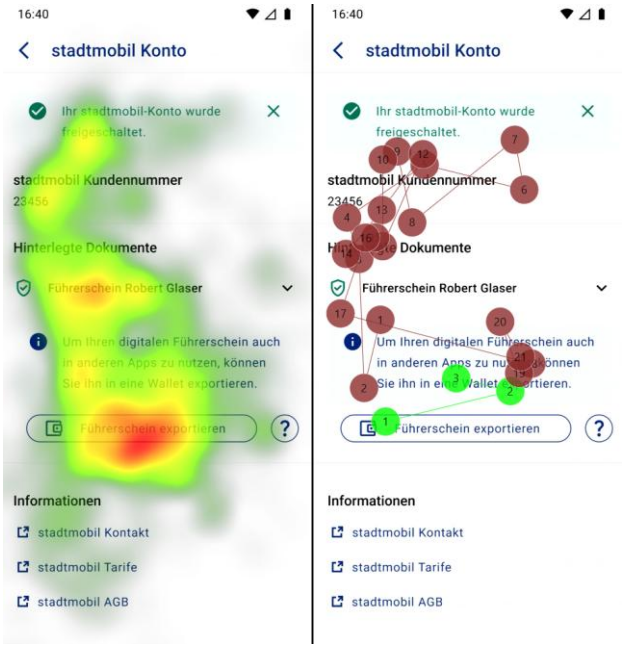


Abbildung 21: Stadtmobil-Konto – Ergebnisse des Eye Tracking. (Sauer u. a., 2025b).

EH2: 18 der 24 Probanden haben den Informations-Button zum Exportieren des Führerschein-VC (mit Fragezeichen-Symbol) nicht bemerkt. Die Heatmap in Abbildung 21 zeigt, dass der Informations-Button kaum eingefärbt ist. Insbesondere Probanden unter 20 Jahren haben diesen nicht bemerkt, was durch den Scanpath in Abbildung 21 deutlich wird, da keine Augenfixierungspunkte auf dem Informations-Button zu sehen sind. Dies könnte erneut (wie bei EH1) ein Hinweis darauf sein, dass jüngere Probanden bereits ähnliche Interaktionsmuster von anderen Software-Systemen kennen, wodurch sie dazu neigen, Informationstexte nicht zu lesen und direkt den Export-Button drücken.

EH3: 12 der 24 Probanden betrachteten zuerst Elemente in der Mitte des stadtmobil-Menüs und 8 Probanden zuerst Elemente am oberen Rand. Von denjenigen Probanden, die in der Mitte begannen, betrachteten 6 Probanden direkt den Export-Button, ohne die restlichen Elemente zu betrachten. Die Mehrzahl von denjenigen, die am oberen Rand begannen, betrachteten zunächst andere Elemente und klickten dann auf den Export-Button. Außerdem neigten Probanden unter 30 Jahren eher dazu, auf den Export-Button zu drücken (anstatt weitere Elemente zu betrachten), als Probanden über 29 Jahren. Dies könnte erneut (wie bei EH1 und EH2) ein Hinweis darauf sein, dass jüngere Probanden bereits ähnliche Interaktionsmuster von anderen Software-Systemen kennen, wodurch sie dazu neigen, Informationstexte nicht zu lesen und direkt den Export-Button drücken.

EH4: 19 der 24 Probanden haben den Sicherheitshinweis beim Speichern des Führerschein-VC in der Wallet nicht wahrgenommen, dass der Aussteller nicht verifiziert ist. In Abbildung 22 ist ein deutlich roter Bereich in der Heatmap erkennbar, was darauf hinweist, dass die Probanden überwiegend dorthin statt auf den Sicherheitshinweis geschaut haben. Außerdem haben Probanden zwischen 20 und 49 Jahren den Sicherheitshinweis eher übersehen, wohingegen Probanden unter 20 und über 50 Jahren den Sicherheitshinweis häufiger betrachtet haben.

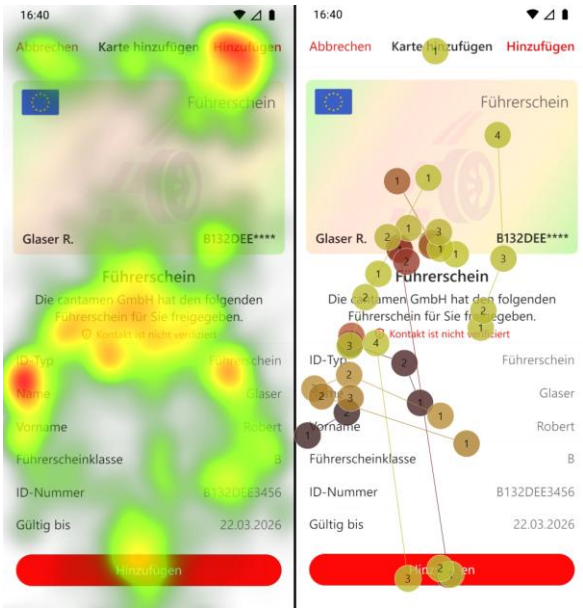


Abbildung 22: VC-Speicherung – Ergebnisse des Eye Tracking. (Sauer u. a., 2025b).

EH5: Mindestens 9 der 24 Probanden haben den Informationstext über den Aussteller nicht vollständig gelesen. Die Heatmap in Abbildung 22 zeigt, dass ein gewisser Teil des Informationstextes leicht rötlich eingefärbt ist, jedoch nicht der gesamte Teil.

EH6: Mindestens 7 der 24 Probanden haben die detaillierten Informationen (wie beispielsweise Name und Vorname) des Führerschein-VC nicht vollständig gelesen. Die Heatmap in Abbildung 22 zeigt, dass nur ein gewisser Teil eingefärbt ist. ID-Typ und Name wurden öfters betrachtet, was die rötere Einfärbung zeigt. Ferner haben alle Probanden über 50 Jahren die detaillierten Informationen des Führerschein-VC betrachtet.

EH7: 2 der 24 Probanden blickten direkt auf den roten „Hinzufügen“-Button des Führerschein-VC zur Wallet, ohne zuvor andere Elemente auf dem Screen zu betrachten. Dies wird im Scanpath in Abbildung 22 deutlich, welcher die anfänglichen Augenfixierungspunkte visualisiert. Die meisten ersten Augenfixierungspunkte liegen im mittleren Be-

reich des Screens und nicht auf dem roten „Hinzufügen“-Button. Außerdem zeigt die Heatmap in Abbildung 22, dass die Probanden eher den „Hinzufügen“-Button in der oberen rechten Ecke fokussiert haben als den größeren „Hinzufügen“-Button im unteren Bereich des Screens.

Mithilfe von Thinking aloud wurden weitere UX-Schwächen (TA1 bis TA7) identifiziert:

(TA1) Am Anfang der Aktivierung von stadtmobil in regiomove haben die Probanden zunächst Informationen über mögliche Aktivierungsverfahren erhalten. Möglich waren (a) der Import eines bereits vorhandenen Führerschein-VC aus der Wallet, (b) die Überprüfung des Führerscheins mittels Videoidentifikationsverfahren und (c) die Überprüfung des Führerscheins vor Ort. Die 3 Möglichkeiten wurden durch 3 verschiedene Icons mit Beschriftung dargestellt. 21 der 24 Probanden interpretierten diese Icons als klickbare Buttons, was zu Verwirrung und Frustration bei den Probanden führte. Die Interaktionsmuster müssen daher angepasst werden.

(TA2) Den Probanden wurde zu Beginn der Evaluation ausdrücklich gesagt, dass sie mit einer Wallet starten, in der keine VC vorhanden sind. Sie sollten das (b) Videoidentifikationsverfahren verwenden und nicht den (a) Import eines bereits vorhandenen Führerschein-VC aus der Wallet. 6 der 24 Probanden versuchten dennoch, VC aus der Wallet zu importieren. Dies bedeutet, dass die Formulierung und die Gestaltung der Funktion verbessert werden sollen, indem stärker betont wird, dass die benötigten VC für einen Import bereits in der Wallet gespeichert sein müssen. Es deutet auch daraufhin, dass die Probanden die Funktionsweise der Wallet nicht richtig verstanden haben oder dass ihre Lernfähigkeit im Umgang mit der Wallet unzureichend ist. Khayretdinova u. a. (2022) zeigten bereits, dass Probanden die Funktionsweise der von ihnen evaluierten Wallet nicht richtig verstanden haben und die Lernfähigkeit unzureichend war. Das bedeutet, dass mehr Hilfsoptionen integriert werden sollen, was auch Sartor u. a. (2022) feststellten. Beispielsweise könnte ein einführendes Tutorial integriert werden, das je nach Erfahrungsstand der Probanden die Grundfunktionalitäten der Wallet erklärt. Zudem haben sich die Probanden generell mehr Erfolgs- und Fehlermeldungen in der Wallet gewünscht, wie beispielsweise Miss-/Erfolgsmeldungen nach dem Teilen und Speichern von VC.

(TA3) Nach erfolgreichem Abschluss des Videoidentifikationsverfahrens erschien ein Dialog, der darauf hinwies, dass das stadtmobil-Konto in wenigen Minuten freigeschaltet wird. 7 von 24 Probanden übersprangen den Dialog, ohne ihn (aufgrund von zu viel Text) zu lesen. Die Probanden kritisierten, dass generell oft zu viel Text auf einmal angezeigt wurde. 2 von 24 Probanden sprachen sich generell für eine stärkere Betonung intuitiver Icons und weniger Textelemente aus. Dieses Ergebnis unterstreicht die Bedeutung eines ausgewogenen Verhältnisses

zwischen Textelementen und Icons, um die UX innerhalb eines komplexen Interaktionsprozesses mit der Wallet zu erhöhen und gleichzeitig die Transparenz im Umgang mit sensiblen Benutzerdaten zu gewährleisten.

(TA4) Nach Aktivierung des stadtmobil-Kontos durch das Videoidentifikationsverfahren konnte das Führerschein-VC in die Wallet exportiert werden. Hierzu konnte ein Export-Button im stadtmobil-Konto gedrückt werden (siehe Abbildung 21). Daraufhin erschien ein Dialog in der Wallet, der Informationen über das zu speichernde Führerschein-VC zeigte, wie beispielsweise Name, Vorname und Führerscheinklasse (siehe Abbildung 22). Zusätzlich beinhaltete dieser Dialog einen roten Sicherheitshinweis „Kontakt ist nicht verifiziert“. Dies bedeutete, dass der Aussteller der VCs nicht verifiziert war und somit das ausgestellte Führerschein-VC unsicher sein konnte. 19 der 24 Testpersonen haben diesen Sicherheitshinweis nicht gelesen, obwohl er in roter Farbe erschien (was auch die Eye Tracking-Ergebnisse zeigen).

(TA5) In der Wallet erschien ein zusätzlicher Dialog, der die Probanden aufforderte, nochmals zu bestätigen, dass das Führerschein-VC in der Wallet gespeichert werden soll. Dies wurde von den Probanden als lästig und unnötig empfunden. Es ist denkbar, dass dieser Dialog nur dann erscheint, wenn der Kontakt nicht verifiziert ist, was diese UX-Schwäche und die beschriebene UX-Schwäche von (TA4) beheben könnte. Außerdem sollte das Design der Buttons zur Bestätigung und Ablehnung des VC-Imports verbessert werden. Das Design sollte nicht dazu verleiten, dass der Button zur Bestätigung gedrückt wird, um das Dark Pattern (siehe Abschnitt 3.4) aufzulösen.

(TA6) Die Wallet verwendet größtenteils rote User Interface-Elemente, was dazu führen kann, dass Probanden manche Elemente als Warnung interpretieren. Denkbar wäre, dass die Wallet andere Farben verwendet und nur Warnhinweise in Rot darstellt (wie beispielsweise ein Hinweis, dass Aussteller und Prüfer nicht verifiziert sind).

(TA7) Probanden forderten außerdem eine Suchfunktion innerhalb der Wallet und regiomove. Dadurch kann die Effizienz der Benutzung gesteigert werden. Dahingegen äußerte ein Proband Bedenken, dass die Nutzung „zu flüssig“ lief, sodass Sicherheitsinformationen übersprungen werden können. Dies unterstreicht die Relevanz des Spannungsfelds von UX und Informationssicherheit und der gemeinsamen Betrachtung beider Aspekte.

Im Folgenden werden die Implikationen von UX und Informationssicherheit diskutiert.

(I1) Wie durch die Ergebnisse von EH4 ersichtlich, haben 19 von 24 Probanden den Sicherheitshinweis nicht gesehen, dass der Aussteller des Führerschein-VC nicht verifiziert ist. Dies eröffnet böswilligen Ausstellern die Möglichkeit, Wallet-

Inhaber dazu zu verleiten, VC in ihrer Wallet zu speichern, in denen falsche Informationen gespeichert sind. Eine mögliche Folge davon könnte sein, dass Wallet-Inhaber für ein VC bezahlen und im Gegenzug keine gültigen VC erhalten. Es sollte möglichst vermieden werden, dass ein Sicherheitshinweis eines nicht verifizierten Ausstellers und Prüfers von VC durch Wallet-Inhaber übersehen wird. Beispielsweise könnte ein zusätzlicher Dialog integriert werden, der nur dann erscheint, wenn nicht verifizierte Aussteller oder Prüfer vorliegen. Wenn der Aussteller sowie Prüfer verifiziert ist und der zusätzliche Dialog trotzdem erscheint, könnte dies die UX mindern, wie in (TA5) beschrieben.

(I2) Ein weiteres Risiko ist das Verstecken von Informationen innerhalb der VC, die für Wallet-Inhaber nicht direkt im User Interface der Wallet ersichtlich sind. Dies könnte unbemerkt bleiben und als verdeckter Kanal für die Kommunikation zwischen kooperierenden, böswilligen Ausstellern und Prüfern dienen. Dadurch wird die Vertraulichkeit der persönlichen Daten des Wallet-Inhabers verletzt und seine Privatsphäre beeinträchtigt, wenn beispielsweise verdeckte Informationen über verpasste oder verspätete Zahlungen enthalten sind. Zudem könnten beispielsweise verdeckte Produktpräferenzen integriert werden. Wenn daraufhin ein Holder seine VC an einen Onlineshop teilt, könnte ungewollte Werbung basierend auf den hinzugefügten Produktpräferenzen erscheinen. In diesem Fall könnte die Wallet von einem Sicherheitshinweis für den Wallet-Inhaber profitieren, dass Daten in der VC enthalten sind, die nicht im User Interface dargestellt werden. Allerdings könnte ein böswilliger Aussteller diese Informationen verschlüsseln, sodass der Wallet-Inhaber keine Rückschlüsse auf den Inhalt ziehen kann, selbst wenn er diese Informationen einsieht.

(I3) Böswillige Prüfer könnten persönlichen Informationen ausspähen, die in der Verifiable Presentation (VP, siehe Abschnitt 2.2) gespeichert sind. Wenn eine VP einen Prüfer erreicht, werden bestimmte Informationen offengelegt. Auch wenn VP die Weitergabe von Informationen der VC einschränken, kann ein böswilliger Prüfer dennoch in den Besitz von Informationen gelangen. Daher sollten die Wallet-Inhaber gewarnt werden, dass ein Prüfer nicht verifiziert ist und dass alle freigegebenen Daten offengelegt werden könnten, wie auch bei nicht verifizierten Ausstellern in (I1).

(I4) Wie in TA2 beschrieben, könnten mehrere Probanden die Funktionsweise der Wallet nicht verstanden haben. Fehlbedienungen durch Wallet-Inhaber können die Informationssicherheit beeinträchtigen. Dies zeigten auch Whitten & Tygar (1999), da nur 3 von 12 Probanden eine E-Mail erfolgreich verschlüsseln und signieren konnten, was auf Bedienungsfehler zurückzuführen ist. Speziell in Bezug auf Wallets könnten Wallet-Inhaber aufgrund der schlechten UX ungewollt VC teilen, worunter die Informationssicherheit leidet, insbesondere die Vertraulichkeit. Außerdem könnten komplizierte Verfahren zur Sicherung von in der

Wallet gespeicherten VC dazu führen, dass Wallet-Inhaber keine Sicherungskopien erstellen, sodass VC bei Verlust des Geräts unwiderruflich verloren gehen.

(I5) Mehrere Probanden wünschten sich mehr Rückmeldungen (beispielsweise Miss-/Erfolgsmeldungen) in der Wallet, wie in (TA2) beschrieben. Wenn die Wallet-Inhaber keine klaren Rückmeldungen darüber erhalten, ob ihre Aktionen erfolgreich waren oder nicht, könnten Wallet-Inhaber in einem unsicheren Zustand verweilen. So könnten sie beispielsweise versehentlich mehrere Transaktionen durchführen, wenn keine Erfolgsmeldung beim Teilen von VC erscheint.

(I6) Die Ergebnisse der Fragebögen SUS und UEQ-S zeigen, dass die Prototyp-Variante mit Passwort die schlechtesten UX-Werte aufweist. Die Prototyp-Varianten mit 4-stelligem und 6-stelligem Pin schnitten am besten ab. Eine PIN mit mehr Ziffern ist in diesem Fall sicherer als eine PIN mit weniger Ziffern. Das Passwort mit mehr Zeichen und einem größeren Alphabet ist die sicherste der 3 Authentifizierungsmethoden. Hier liegt ein offensichtlicher Konflikt zwischen UX und Informationssicherheit vor. Wenn ein 4-stelliger oder 6-stelliger Pin anstatt eines Passworts mit mehr Zeichen und einem größeren Alphabet verwendet wird, erhöht sich die UX und die Informationssicherheit sinkt.

Aufbauend auf den Evaluationsergebnissen aus Abschnitt 5.3 wurden verschiedene UX- und Informationssicherheit-Heuristiken für Wallets entwickelt, die in Abschnitt 5.4 beschrieben werden.

5.4 Ableitung von User Experience- und Informationssicherheit-Heuristiken für Wallets

Sauer u. a. (2025c) entwickelten und evaluierten 12 UX- und 6 Informationssicherheit-Heuristiken für Wallets. Hierzu wurde die Methode von Rusu u. a. (2011) zur Entwicklung von UX-Heuristiken adaptiert, sodass sich auch Informationssicherheit-Heuristiken entwickeln lassen. Das bedeutet konkret, dass jeder Schritt der Methode hinsichtlich UX-Heuristiken auch für die Informationssicherheit-Heuristiken durchgeführt wurde – mit Ausnahme eines Evaluationsschritts (Schritt 9), der im weiteren Verlauf des Abschnitts erläutert wird[23].

[23] Die Entwicklung und Evaluation der Heuristiken erfolgte in Zusammenarbeit mit Sabine Schork, die ihre studentische Abschlussarbeit (Schork, 2023) über das Thema schrieb. Die studentische Abschlussarbeit wurde vom Verfasser dieser Dissertation betreut.

In Schritt 1, der Exploratory stage (dt. Explorationsphase), wurde eine Literaturrecherche durchgeführt, um bereits bestehende Heuristiken und Attribute der UX und Informationssicherheit zu identifizieren. Zusätzlich wurde nach relevanten Informationen über Wallets recherchiert, wie beispielsweise spezifische Funktionen und Vor- und Nachteile einzelner Wallets. Hierzu wurde in den Datenbanken Google Scholar, ResearchGate und ScienceDirect mit folgenden Suchtermen recherchiert:

Suchterm 1: ("digital identity wallet" OR "identity wallet") AND ("UX" OR "user experience" OR "usability" OR "information security" OR "security" OR "heuristics")

Suchterm 2: ("UX" OR "user experience" OR "usability" OR "information security" OR "security") AND "heuristics"

Suchterm 3: ("UX" OR "user experience" OR "usability" OR "information security" OR "security") AND "attributes"

Durch die Datenbanksuche konnten 26 relevante Publikationen identifiziert werden, die in den weiteren Schritten wiederverwendet wurden.

In Schritt 2, der Experimental stage (dt. Experimentelle Phase), sollen Experimente durchgeführt werden, um weitere Heuristiken zu sammeln. Schritt 2 wurde durch Quiñones u. a. (2018) als optional klassifiziert. Da bereits Experimente durchgeführt wurden (siehe Abschnitt 5.3) und Schritt 2 als optional gilt, wurde Schritt 2 nicht erneut durchgeführt, sondern die bereits gewonnenen Erkenntnisse für die weiteren Schritte verwendet.

In Schritt 3, der Descriptive stage (dt. Deskriptive Phase), wurden die erhobenen Informationen aus Schritt 1 und Schritt 2 kategorisiert, priorisiert und selektiert. Als Kategorien dienten (1) Informationen (insbesondere spezifische Funktionen) von Wallets, (2) Attribute der UX, (3) Attribute der Informationssicherheit, (4) Sets an bestehenden Heuristiken der UX und (5) Sets an bestehenden Heuristiken der Informationssicherheit. Nach Kategorisierung aller Informationen wurden die Informationen miteinander verglichen und priorisiert nach „unwichtig", „relativ wichtig" und „sehr wichtig".

Folgende Informationen wurden als „sehr wichtig" priorisiert und für die Weiterverwendung in den folgenden Schritten selektiert:

- Definition einer Wallet nach Podgorelec u. a. (2022)
- Einsatzdomänen von Wallets, wie beispielsweise E-Government, Mobilität und Gesundheit
- Vorteile von Wallets (Atick u. a., 2014)
- Herausforderungen von Wallets (Anke und Richter, 2023)
- Funktionen von Wallets (Cucko u. a., 2022; Krauß u. a., 2023b)

- Attribute der UX (Morville, 2005; Nielsen, 1993)
- Attribute der Informationssicherheit (DIN EN ISO/IEC 27000, 2020)
- Heuristiken nach Nielsen (1994)
- Heuristiken nach Realpe u. a. (2016)
- Heuristiken nach Yeratziotis u. a. (2012)
- Heuristiken nach Gordieiev u. a. (2017)
- Benutzeranforderungen von Wallets (Krauß u. a., 2023a)
- 5 empfohlene und 7 ungeeignete Entwurfsentscheidungen von Wallets (Krauß u. a., 2023b)

In Schritt 4, der Correlational stage (dt. Korrelationsphase), wurden die bereits bestehenden, recherchierten Heuristiken den Wallet-Funktionen und den Attributen der UX und Informationssicherheit zugeordnet.

Tabelle 6 zeigt beispielhaft die Zuordnung einiger Wallet-Funktionen zu den UX-Attributen (siehe Abschnitt 3.1) und den bestehenden Heuristiken. Es wird deutlich, dass keine Heuristik in der Literatur gefunden wurde, welche der Wallet-Funktion der Verwaltung von VC anderer Personen (Krauß u. a., 2023b) zuordenbar ist. Dies bedeutet, dass hierfür eine neue Heuristik in den weiteren Schritten entwickelt werden musste.

Wallet-Funktion	**UX-Attribute**	**Name der bestehenden Heuristik**
Übersicht aller VC (Krauß u. a., 2023b)	Nützlichkeit, Usability, Glaubwürdigkeit (Morville, 2005), Einprägsamkeit, Erlernbarkeit, Zufriedenheit (Nielsen, 1993)	„Recognition rather than recall“ (Nielsen, 1994)
Detailansicht eines VC (Krauß u. a., 2023b)	Nützlichkeit, Usability, Glaubwürdigkeit (Morville, 2005), Einprägsamkeit, Erlernbarkeit, Zufriedenheit (Nielsen, 1993)	„Recognition rather than recall“ (Nielsen, 1994)
Schnellzugriff auf VC (Krauß u. a., 2023b)	Usability, Barrierefreiheit (Morville, 2005), Zufriedenheit, Effizienz (Nielsen, 1993)	„Flexibility and efficiency of use“ (Nielsen, 1994)
Hinweis auf fehlende VC (Krauß u. a., 2023b)	Auffindbarkeit, Usability, Barrierefreiheit (Morville, 2005), Fehleranfälligkeit, Effizienz (Nielsen, 1993)	„Help and documentation“ (Nielsen, 1994)
Verwaltung von VC anderer Personen (Krauß u. a., 2023b)	Nützlichkeit, Usability, Wert (Morville, 2005), Zufriedenheit, Effizienz	-

	(Nielsen, 1993)	

Tabelle 6: Korrelationsphase – Beispiel der UX-Heuristiken. (Sauer u. a., 2025c). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Tabelle 7 zeigt beispielhaft die Zuordnung einiger Wallet-Funktionen zu Informationssicherheit-Attributen und bestehenden Heuristiken. Es wird deutlich, dass in diesem Beispiel nur eine Heuristik der Fehlervermeidung von Fehlbedienung (Gordieiev u. a., 2017) in der Literatur gefunden wurde, die der Wallet-Funktion eines Hinweises auf fehlende VC (Krauß u. a., 2023b) zuordenbar ist. Dies bedeutet, dass hierfür eine neue Heuristik in den weiteren Schritten entwickelt werden muss.

Wallet-Funktion	**Informationssicherheit-Attribute**	**Name der bestehenden Heuristik**
Übersicht aller VC (Krauß u. a., 2023b)	Vertraulichkeit, Integrität, Verfügbarkeit (DIN EN ISO/IEC 27000, 2020)	-
Detailansicht eines VC (Krauß u. a., 2023b)	Vertraulichkeit, Integrität, Verfügbarkeit (DIN EN ISO/IEC 27000, 2020)	-
Schnellzugriff auf VC (Krauß u. a., 2023b)	Vertraulichkeit, Integrität (DIN EN ISO/IEC 27000, 2020)	-
Hinweis auf fehlende VC (Krauß u. a., 2023b)	Verfügbarkeit (DIN EN ISO/IEC 27000, 2020)	„User error protection“ (Gordieiev u. a., 2017)
Verwaltung von VC anderer Personen (Krauß u. a., 2023b)	Vertraulichkeit, Integrität (DIN EN ISO/IEC 27000, 2020)	-

Tabelle 7: Korrelationsphase – Beispiel der Informationssicherheit-Heuristiken. (Sauer u. a., 2025c). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

In Schritt 5, der Selection stage (dt. Selektierungsphase), wurden die jeweils zugeordneten Informationen aus Schritt 4 in die folgenden Kategorien eingeteilt:

(1) Behalten: Die jeweils zugeordneten Informationen sollen unverändert bleiben, da bereits eine passende Heuristik zugeordnet wurde.
(2) Anpassen: Die jeweils zugeordneten Informationen sollen angepasst werden.
(3) Verwerfen: Die Heuristik der jeweils zugeordneten Informationen soll verworfen werden.

In Schritt 6, der Specification stage (dt. Spezifikationsphase), wurden die Heuristiken nun mithilfe einer Standardvoralge anhand der Kategorisierung aus Schritt 5 dokumentiert. Die Standardvorlage besteht aus einer eindeutigen ID, Namen, Definition, Beschreibung, Wallet-Funktion(en), Checkliste, beispielhafte Vorteile, UX-/Informationssicherheit-Attribut(e) und verwandte Heuristiken. So wurden initial insgesamt 14 UX-Heuristiken und 8 Informationssicherheit-Heuristiken erstellt.

In Schritt 7, der First validation stage (dt. Erste Validierungsphase), wurden die erstellten Heuristiken aus Schritt 5 durch Experteninterviews hinsichtlich Verständlichkeit und Vollständigkeit evaluiert. Es wurden insgesamt 8 Experteninterviews durchgeführt, 4 für die UX-Heuristiken und 4 für die Informationssicherheit-Heuristiken. 2 der UX-Experten waren UX-Designer aus der Industrie, die beiden anderen waren wissenschaftliche Mitarbeiter aus dem Bereich UX und Usable Security. 3 der Experten für Informationssicherheit waren wissenschaftliche Mitarbeiter aus dem Bereich Informationssicherheit und ein Experte für Informationssicherheit war wissenschaftlicher Mitarbeiter aus dem Bereich Usable Security. Alle 4 Experten für Informationssicherheit stehen in ständigem Austausch mit der Industrie.

Die Verständlichkeit wurde durch die Experten mittels einer Skala von 1 (nicht verständlich) bis 5 (voll verständlich) bewertet. Tabelle 8 zeigt die Durchschnittswerte der Verständlich je Heuristik.

ID / Name der UX-Heuristik	**Verständlichkeit**	**ID / Name der Informationssicherheit-Heuristik**	**Verständlichkeit**
HU1: Barrierefreiheit	4,5	HI1: Authentifizierung	4,5
HU2: Sichtbarkeit des Systemstatus	4	HI2: Sicherer Datentransfer	3,5
HU3: Transparenz	4,5	HI3: Vermeidung von Fehlbedienungen	4
HU4: Verständliche Systemsprache	3,75	HI4: Passwortrichtlinien	4,5
HU5: Kontrolle und Freiheit der Benutzer	3,5	HI5: Datenverschlüsselung	5
HU6: Konsistenz und Standards	4,5	HI6: Verfügbarkeit	5
HU7: Fehlermeldungen/-prävention	4	HI7: Automatische Updates	5
HU8: Wiedererkennen statt Erinnern	4	HI8: Richtlinien für Smartcards	5
HU9: Flexibilität und Effizienz der Nutzung	4,25		
HU10: Ästhetisches und minimalistisches Design	3,75		

HU11: Hilfe und Dokumentation	3,75		
HU12: Authentifizierung	2,25		
HU13: Interoperabilität	4		
HU14: Verwaltung von Identitäten und VC	3,25		
HU15: Sicherung und Wiederherstellung	3,5		
Durchschnitt	**3,83**	**Durchschnitt**	**4,56**

Tabelle 8: Evaluation der Verständlichkeit der initialen Heuristiken. (Sauer u. a., 2025c). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Hinsichtlich Vollständigkeit wurden die Experten befragt, ob Heuristiken fehlen oder angepasst werden müssen. Ein wesentlicher Punkt war, dass die Heuristiken noch deutlicher voneinander abgegrenzt werden mussten. Ein zweiter wesentlicher Punkt war, dass alle Heuristiken auf ein einheitliches Abstraktionsniveau angeglichen werden mussten, da sie teilweise abstrakter oder spezifischer formuliert waren.

Zudem wurden die Experten befragt, ob sie die Heuristiken in Zukunft für die Evaluation der UX und Informationssicherheit gleicher oder ähnlicher Software-Systeme verwenden würden. Alle 4 UX-Experten antworteten, dass sie die UX-Heuristiken nach Einarbeit ihres Feedbacks in Zukunft verwenden würden. 3 der 4 Experten für Informationssicherheit antworteten, dass sie die Informationssicherheit-Heuristiken zukünftig verwenden würden. Ein Experte für Informationssicherheit kann sich die zukünftige Verwendung zum aktuellen Zeitpunkt noch nicht vorstellen, da die Informationssicherheit-Heuristiken noch an einigen Stellen zu abstrakt seien.

In Schritt 8, der Refinement stage (dt. Überarbeitungsphase), wurden die bisherigen Heuristiken mittels des Feedbacks aus Schritt 7 überarbeitet. Zunächst wurden alle Heuristiken hinsichtlich ihrer Formulierungen geprüft und angepasst. Zudem wurden alle Heuristiken hinsichtlich Abstraktionsniveau und Abgrenzung geprüft und vereinheitlicht. Die ursprünglich 15 UX-Heuristiken wurden auf 12 verfeinerte UX-Heuristiken reduziert. Heuristik HU8 (siehe Tabelle 8) und HU9 wurden zur Heuristik „Transparente Gestaltung“ fusioniert. HU14 und HU15 wurden zur Heuristik „Autonomie und Kontrolle“ fusioniert. HU12 wurde entfernt, da sie bereits durch HU9 abgedeckt ist. Die ursprünglichen 8 Informationssicherheit-Heuristiken wurden auf 6 verfeinerte Informationssicherheit-Heuristiken reduziert. HI4 und HI8 wurden entfernt, da sie laut den Experten aus Schritt 7 für Wallets irrelevant sind.

Die verfeinerten und finalen (da kein Änderungsbedarf in Schritt 9 bestand) UX- und Informationssicherheit-Heuristiken für Wallets sind online verfügbar[24].

Tabelle 9 zeigt beispielhaft eine final entwickelte UX-Heuristik zur verständlichen Systemsprache von Wallets. Hierbei wird der Nutzen der Checkliste deutlich, da die einzelnen Checklisten-Punkte geprüft werden können, inwiefern diese durch eine zu evaluierende Wallet erfüllt werden.

ID	HU4
Name	Verständliche Systemsprache
Definition	Die Wallet sollte eine für Benutzer verständliche und vertraute Sprache verwenden.
Beschreibung	Die in der Wallet verwendeten Begriffe sollten den Benutzern vertraut und nicht zu technisch formuliert sein. Fachbegriffe, die sich nicht vermeiden lassen, sollten den Benutzern erklärt werden. Zudem sollten Benutzer die Möglichkeit haben, aus einer Menge von vorgegebenen Sprachen zu wählen, wobei standardmäßig die Systemsprache eingestellt sein sollte.
Wallet-Funktion(en)	Systemsprache
Checkliste	Die Wallet sollte 1. verständliche und vertraute Begriffe verwenden, 2. Fachbegriffe vermeiden, 3. unvermeidliche Fachbegriffe erklären und 4. Mehrsprachigkeit anbieten.
Beispielhafte Vorteile	Vermeidung von Benutzungsfehler durch verständliche Begriffe.
Anwendungsbeispiele	Die Abkürzung „ID“ wird den Benutzern erklärt.
UX-Attribut(e)	Auffindbarkeit, Barrierefreiheit und Usability
Usability-Attribut(e)	Einprägsamkeit, Lernfähigkeit, Zufriedenstellung, Effizienz, Fehleranfälligkeit
Verwandte Heuristik(en)	Heuristiken von Nielsen (1994)

Tabelle 9: Beispiel einer entwickelten UX-Heuristik. (Sauer u. a., 2025c). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Tabelle 10 zeigt beispielhaft eine final entwickelte Informationssicherheit-Heuristik zur Wallet-Authentifizierung. Auch hier wird deutlich, dass eine Heuristik in mehrere Checklisten-Punkte unterteilt werden sollte, damit die Evaluation erleichtert wird.

[24] https://doi.org/10.5281/ZENODO.10865961

ID	HI1
Name	Authentifizierung
Definition	Benutzer sollten sich bei der Wallet authentisieren müssen und werden daraufhin von der Wallet authentifiziert und autorisiert.
Beschreibung	In der Wallet werden sensible Daten gespeichert. Diese Daten sollten durch mindestens eine Authentifizierungsmethode gesichert werden. Die Authentifizierungsmethode sollte standardisierten, sicheren Regeln entsprechen (wie beispielsweise Fingerscan). Anschließend wird der Benutzer authentifiziert und autorisiert.
Wallet-Funktion(en)	Authentifizierung
Checkliste	1. Die Wallet ist durch eine standardisierte, sichere Authentifizierungsmethode geschützt. 2. Das Gerät und seine IP werden nach ungültigen, nachfolgenden Zugriffsversuchen für eine festzulegende Zeit gesperrt. 3. Die Sitzung wird beim Abmelden beendet und Benutzer müssen sich erneut authentisieren. 4. Aus den kryptografischen Berechnungen dürfen keine Schlüsse auf den Schlüssel gezogen werden können (beispielsweise über den Stromverbrauch). 5. Nach erfolgreicher Authentifizierung werden die Benutzer autorisiert, sodass sie ihre Wallet-Daten einsehen können.
Beispielhafte Vorteile	Unbefugte haben keinen Zugriff auf die in der Wallet gespeicherten, sensiblen Daten.
Anwendungsbeispiele	Beim Öffnen der Wallet müssen sich Benutzer per Fingerscan authentisieren.
Informationssicherheit-Attribut(e)	Vertraulichkeit, Integrität
Verwandte Heuristik(en)	Heuristiken nach Gordieiev u. a. (2017)

Tabelle 10: Beispiel einer entwickelten Informationssicherheit-Heuristik. (Sauer u. a., 2025c). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

In Schritt 9, der Second validation stage (Zweite Validierungsphase), wurden die UX-Heuristiken ein weiteres Mal evaluiert. Da keine vergleichbaren Informationssicherheit-Heuristiken in der Literatur gefunden werden konnten, wurde Schritt 9 nicht für die verfeinerten Informationssicherheit-Heuristiken durchgeführt, sondern nur für die UX-Heuristiken. Es wurden eine Kontroll- und eine Versuchsgruppe gebildet, die jeweils aus 3 UX-Experten bestanden. Die Experten unterschieden sich von denen der ersten Validierungsphase. Es wurde darauf geachtet, dass die Personen in den beiden Gruppen in Bezug auf ihr Fachwissen ausgewogen waren. In jeder Gruppe befanden sich 3 auf UX-Forschung spezialisierte, wissenschaftliche Mitarbeiter, von denen 2 auch Forschung im

Zusammenhang mit Wallets betreiben. Die Experten der Kontrollgruppe führten jeweils eine Heuristische Evaluation (siehe Abschnitt 5.2.2) anhand eines Software-Prototyps unter Verwendung der UX-Heuristiken von Nielsen (1994) durch. Die Experten der Versuchsgruppe führten jeweils eine Heuristische Evaluation anhand desselben Software-Prototyps mithilfe der entwickelten UX-Heuristiken durch. Der Software-Prototyp bildete die Ausstellung eines VC der Meldebescheinigung und die anschließende Ablage des VC in der Wallet ab. Zu diesem Zweck wurde zunächst ein bereits in der Wallet gespeichertes VC des Personalausweises mit der behördlichen Plattform geteilt. Anschließend wurden die gewünschten Daten der Meldebescheingung ausgewählt und das entsprechende VC in der Wallet gespeichert. Die 3 Experten der Kontrollgruppe identifizierten insgesamt 7, 10 und 23 UX-Schwächen des Prototyps (gleichartige, mehrfach beobachtete UX-Schwächen wurden zusammengefasst). Die Experten der Versuchsgruppe konnten unter Verwendung der entwickelten Heuristiken mehr UX-Schwächen des Prototyps identifizieren. Hierbei identifizierten die Experten 24, 37 und 42 UX-Schwächen des Prototyps. Aus der größeren Anzahl von identifizierten UX-Schwächen, die durch die Experten der Versuchsgruppe gefunden wurden, lässt sich annehmen, dass die entwickelten UX-Heuristiken besser geeignet sind, die UX von Wallets zu bewerten als die allgemeinen Heuristiken von Nielsen (1994).

Die einzelnen Evaluationsergebnisse der Versuchsgruppe lassen sich Tabelle 11 entnehmen. Die einzelnen Evaluationsergebnisse der Kontrollgruppe lassen sich Tabelle 12 entnehmen. „E1-3“ stehen für die einzelnen Experten jeder Gruppe. „$E1 \cap E2 \cap E3$“ meint die Schnittmenge identifizierter UX-Schwächen unter den Experten.

ID / Name der Heuristik	**Identifizierte UX-Schwächen**			
	E1	E2	E3	$E1 \cap E2 \cap E3$
HU1: Barrierefreiheit	7	4	5	3
HU2: Sichtbarkeit des Systemstatus	3	3	2	2
HU3: Transparentes Design	5	5	5	1
HU4: Verständliche Systemsprache	2	5	1	1
HU5: Freie Navigation	1	2	1	1
HU6: Konsistenz und Standards	0	0	3	0
HU7: Fehlervermeidung und Fehlertoleranz	6	5	1	1
HU8: Flexibilität, Effizienz und Effektivität der Nutzung	4	4	2	1
HU9: Ästhetisches und minimalistisches Design	5	5	2	0
HU10: Hilfe und Dokumentation	2	2	1	1
HU11: Organisatorische Interoperabilität	0	0	1	0
HU12: Autonomie und Kontrolle	7	7	0	0
Summe	**42**	**37**	**24**	**11**

Tabelle 11: Ergebnisse der heuristischen Evaluation der Versuchsgruppe. (Sauer u. a., 2025c). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Name der Heuristik	**Identifizierte UX-Schwächen**			
	E1	E2	E3	E1 ⋂ E2 ⋂ E3
Sichtbarkeit des Systemstatus	2	2	0	0
Übereinstimmung zwischen System und realer Welt	0	0	2	0
Benutzerkontrolle und -freiheit	2	2	0	0
Konsistenz und Standards	3	6	3	1
Fehlervermeidung	0	4	0	0
Erkennen statt Erinnern	0	3	0	0
Flexibilität und Effizienz der Nutzung	1	2	1	0
Ästhetisches und minimalistisches Design	1	1	0	0
Hilfe für Benutzer bei der Erkennung, Diagnose und Behebung von Fehlern	0	0	0	0
Hilfe und Dokumentation	1	3	1	1
Summe	**10**	**23**	**7**	**2**

Tabelle 12: Ergebnisse der heuristischen Evaluation der Kontrollgruppe. (Sauer u. a., 2025c). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Alle finalen Heuristiken sind online verfügbar[25].

Heuristiken alleine reichen allerdings nicht aus, um den Zusammenhang zwischen UX und Informationssicherheit zu evaluieren, da die Implikationen zwischen den Heuristiken nicht berücksichtigt werden. Zudem wurde kein geeignetes Verfahren identifiziert, mit dem sich der Zusammenhang zwischen UX, insbesondere mit Berücksichtigung weiterer UX-Attribute als Usability, und Informationssicherheit bewerten lässt (siehe Abschnitt 5.2). Daher wurde ein neues Verfahren entwickelt, für das die Ergebnisse aus Kapitel 5 als Grundlage verwendet wurden. Das entwickelte Verfahren wird in Kapitel 6 erläutert.

[25] https://doi.org/10.5281/ZENODO.10865961

6 MEUSec-Methode

Um die UX und Informationssicherheit von Wallets zu evaluieren und Verbesserungsvorschläge zu identifizieren, wurde die MEUSec-Methode auf Basis der Ergebnisse aus Kapitel 5 entwickelt[26]. Diese Methode stellt einen neuartigen Ansatz dar, da sie UX und Informationssicherheit gemeinsam systematisch berücksichtigt und dabei sowohl Experten als auch Endnutzer miteinbezieht.

In (Sauer u. a., 2024b) wird die erste Version der MEUSec-Methode vorgestellt. Nach einer ersten Evaluation, beschrieben in (Sauer u. a., 2025a), wurden Verbesserungsvorschläge eingearbeitet und eine zweite Version entstand. Diese wurde in (Sauer u. a., 2026) evaluiert und die dort identifizierten Verbesserungsvorschläge resultierten letztlich in einer dritten, im Rahmen dieser Arbeit finalen, Version. Abbildung 23 fasst die Entwicklungsschritte der MEUSec-Methode visuell zusammen.

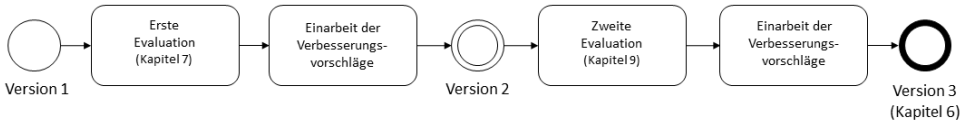


Abbildung 23: Entwicklungsschritte der MEUSec-Methode

Die Evaluationsergebnisse und Verbesserungsvorschläge der ersten und zweiten Version der Methode werden in Kapitel 7 und in Kapitel 9 thematisiert. Mit der dritten Version befasst sich dieses Kapitel. In Abschnitt 6.1 erfolgt die Beschreibung der Methode. Ihre Entwicklung und Begründungen für Entwurfsentscheidungen werden in Abschnitt 6.2 erläutert. Abschnitt 6.3 beschreibt die Beschränkungen und Voraussetzungen der Methode. Danach wird die Methode in Abschnitt 6.4 mit anderen Ansätzen aus der Literatur verglichen.

6.1 Beschreibung der Methode

Im Folgenden wird die dritte Version der MEUSec-Methode beschrieben. Die Beschreibung erfolgt anhand des Modells einer Methode nach Alpers u. a. (2021). Zunächst

[26] Die Entwicklung und Evaluation der zweiten Version der MEUSec-Methode erfolgte im Rahmen einer studentischen Abschlussarbeit (Pfeifer, 2025), die vom Verfasser dieser Dissertation betreut wurde.

werden allgemeine Informationen zur MEUSec-Methode in Abschnitt 6.1.1 gegeben. Anschließend wird das Vorgehensmodell in Abschnitt 6.1.2 erläutert.

6.1.1 Allgemeines

Herausforderung/Problem:

UX und Informationssicherheit können sich gegenseitig beeinflussen. Daher sollten beide Aspekte nicht separat voneinander evaluiert und verbessert werden, sondern gemeinsam betrachtet werden (siehe Abschnitt 5.1).

Ziel/Lösung:

Durch die MEUSec-Methode lassen sich Evaluationsergebnisse der UX und Informationssicherheit mit Berücksichtigung der Beeinflussung von UX und Informationssicherheit von Wallets ermitteln. Die MEUSec-Methode lässt sich im Rahmen des HCD-Prozesses (siehe Abschnitt 3.3) sowohl in der frühen Phase zur Evaluation von Systementwürfen (formative Evaluation) als auch in der späten Phase zur abschließenden Evaluation des fertigen Systems (summative Evaluation) einsetzen. Die Meinungen von Endnutzern und Experten können variieren (Jaspers, 2009), sodass sowohl Endnutzer als auch Experten in die Evaluation miteinbezogen werden. Abschließend lassen sich systematisch Verbesserungsvorschläge für die Wallet sammeln.

Wesentliche Artefakte, die durch die Anwendung der MEUSec-Methode entstehen:

Mithilfe der MEUSec-Methode lassen sich Schwächen der UX und Informationssicherheit durch Endnutzer sowie Experten der UX und Informationssicherheit finden.

UX- und Informationssicherheit-Heurisiken (siehe Abschnitt 5.2.2) lassen sich aus vordefinierten Sammlungen an Heuristiken für die eigene Evaluation auswählen. Zudem lassen sich Heuristiken auf Basis der identifizierten Stärken und Schwächen definieren.

Durch die Bewertung der Erfüllungsgrade aller Heuristiken lassen sich jeweils ein Score für die UX und ein Score für die Informationssicherheit berechnen – inklusive Scores für die Attribute von UX und Informationssicherheit, wie beispielsweise für die Barrierefreiheit (als UX-Attribut) und für die Integrität (als Informationssicherheit-Attribut).

Die Scores der UX und Informationssicherheit können in mehrfachen Anwendungen der MEUSec-Methode wiederverwendet werden, um zu prüfen, inwiefern die identifizierten Verbesserungsvorschläge für eine Wallet zu einer messbaren Verbesserung von weiteren Versionen der Wallet geführt haben.

Zusätzlich lassen sich verschiedene Beeinflussungsarten zwischen Heuristiken (und somit zwischen UX und Informationssicherheit) bestimmen. Die möglichen Beeinflussungsarten zwischen Heuristiken lauten „komplementär“, „konkurrierend“ und „neutral“. Wenn eine Heuristik A komplementär zu einer Heuristik B ist, beeinflusst Heuristik A Heuristik B positiv. Wenn eine Heuristik A konkurrierend zu einer Heuristik B ist, dann beeinflusst Heuristik A Heuristik B negativ. Wenn eine Heuristik A neutral zu einer Heuristik B ist, dann beeinflusst Heuristik A Heuristik B nicht (nennenswert). Die Beeinflussungsarten lassen sich auch in die umgekehrte Richtung festlegen, das heißt, von einer Heuristik B zu einer Heuristik A.

Schließlich lassen sich systematisch Verbesserungsvorschläge der UX und Informationssicherheit mit Berücksichtigung der Beeinflussungsarten identifizieren. Für konkurrierende Heuristiken soll eine Konfliktlösung gefunden werden, das heißt, entweder ein Kompromiss oder eine Priorisierung von UX oder Informationssicherheit. Komplementäre und neutrale Heuristiken können unmittelbar als Basis für die Formulierung von Verbesserungsvorschlägen verwendet werden, da sie sich nicht negativ beeinflussen.

Die gesamten Output-Artefakte – mit Ausnahme der Videoaufnahmen des Thinking aloud – werden bei Durchführung der MEUSec-Methode mit dem entwickelten Software-Tool (siehe Kapitel 8) in einer Datenbank gespeichert. Die Videoaufnahmen des Thinking aloud werden aus Speicherplatzgründen von den Benutzern außerhalb des Software-Tools an einem selbstgewählten Speicherort abgelegt. Erfolgt die Durchführung ohne Tool-Unterstützung, werden die entsprechenden Output-Artefakte stattdessen in einem Dokument festgehalten.

Rollen:

Für die Durchführung der MEUSec-Methode sind unterschiedliche Rollen zu besetzen. Die Durchführung der MEUSec-Methode obliegt einem Methoden-Anwender (engl. Method User, kurz: MU). Dieser arbeitet zusammen mit 2 Experten: einem für UX (engl. UX Expert, kurz: UXE) und einem für Informationssicherheit (engl. Information Security Expert, kurz: ISE). Zusätzlich werden Probanden (engl. Wallet User, kurz: WU) benötigt, welche die Wallet probeweise bedienen. Weder Anzahl noch erforderliche demografische Daten der WU stehen vor Durchführung der Methode fest. Diese werden durch den UXE je nach Evaluationsumfang während der Durchführung definiert.

6.1.2 Vorgehensmodell

Das Vorgehensmodell besteht aus 8 auszuführenden Schritten, die sich jeweils einer der folgenden Kategorien zuordnen lassen:

- die Vorbereitung des Evaluationsobjekts (Schritt 1, siehe Abschnitt 6.1.2.1),
- die benutzerbasierte Evaluation (Schritte 2-4, siehe Abschnitt 6.1.2.2),
- die expertenbasierte Evaluation (Schritte 5-7, siehe Abschnitt 6.1.2.3) und
- die Sammlung von Verbesserungsvorschlägen (Schritt 8, siehe Abschnitt 6.1.2.4).

Das Vorgehen bei erneuter Anwendung der MEUSec-Methode wird in Abschnitt 6.1.2.5 beschrieben.

Die Vorbereitung des Evaluationsobjekts beinhaltet die Definition des Evaluationsobjekts (Schritt 1) – die zu evaluierende Wallet. Danach folgt die benutzerbasierte Evaluation, die sich aufteilt in die Vorbereitung (Schritt 2), Durchführung (Schritt 3) und Auswertung (Schritt 4). Anschließend folgt die expertenbasierte Evaluation, die sich aufteilt in die Vorbereitung (Schritt 5), Durchführung (Schritt 6) und Auswertung (Schritt 7). Zuletzt erfolgt in Schritt 8 das Sammeln von Verbesserungsvorschlägen der UX und Informationssicherheit.

Die beschriebenen 8 Schritte der MEUSec-Methode sind in Abbildung 24 dargestellt.

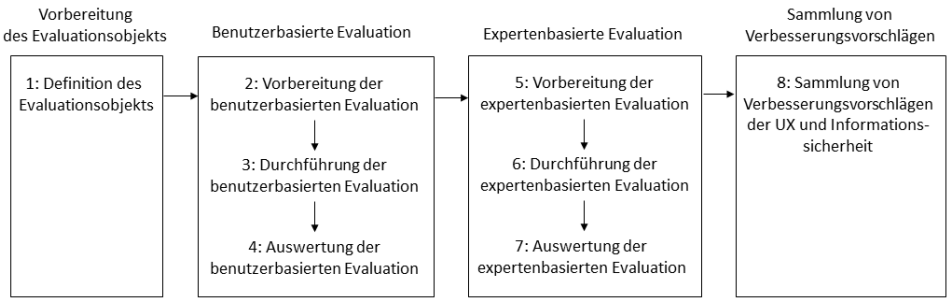


Abbildung 24: 8 Schritte der MEUSec-Methode

Jeder der 8 Schritte beinhaltet verschiedene Aktivitäten, die im Folgenden detailliert beschrieben werden. Die Beschreibung orientiert sich an den 4 Kategorien aus Abbildung 24. Die 4 Kategorien werden mit ihren Schritten und Aktivitäten in den Abschnitten 6.1.2.1 bis 6.1.2.4 erläutert. Das detaillierte Vorgehensmodell ist online verfügbar[27]. Das Vorgehen bei erneuter Anwendung der MEUSec-Methode auf eine verbesserte Version einer Wallet wird in Abschnitt 6.1.2.5 beschrieben.

[27] https://doi.org/10.5281/zenodo.10529247

6.1.2.1 Vorbereitung des Evaluationsobjekts

Die Vorbereitung des Evaluationsobjekts erfolgt in Schritt 1 – der Definition des Evaluationsobjekts (die zu evaluierende Wallet). Zusammenfassend werden die zu evaluierenden Wallet-Funktionen ausgewählt. Außerdem wird der Umfang der Informationssicherheit-Evaluation festgelegt, indem eine Liste an Bedrohungsszenarien erstellt wird.

Schritt 1 – Definition des Evaluationsobjekts:

Input von Schritt 1 ist eine Wallet, die hinsichtlich ihrer UX und Informationssicherheit evaluiert wird, um darauf aufbauend Verbesserungsvorschläge abzuleiten.

Aktivität 1.1: Der MU legt die zu evaluierenden Wallet-Funktionen fest (wie beispielsweise die Teilen- und Speichern-Funktion von VC). Der MU kann für die Auswahl die Liste an Wallet-Funktionen von Krauß u. a. (2023b) verwenden.

Aktivität 1.2: Danach dokumentieren der ISE und der MU mögliche Bedrohungsszenarien für die ausgewählten Wallet-Funktionen aus Aktivität 1.1. Um Bedrohungsszenarien zu definieren, können beispielsweise Bedrohungs- und Risikoanalysen (siehe Abschnitt 4.3.3 und Abschnitt 4.3.4) verwendet werden. Die Bedrohungsszenarien werden mit einer vorgegebenen Vorlage einheitlich dokumentiert. Diese beinhaltet eine Beschreibung, die betroffenen Attribute der Informationssicherheit (wie beispielsweise Vertraulichkeit, Integrität und Verfügbarkeit), die Eintrittswahrscheinlichkeit von 1 (nicht wahrscheinlich) bis 5 (sehr wahrscheinlich) und das Schadensausmaß von 1 (gering) bis 5 (hoch).

Aktivität 1.3: Anschließend legen der ISE und der MU den Umfang der Informationssicherheit-Evaluation fest. Hierzu wählen der ISE und der MU aus, welche der identifizierten Bedrohungsszenarien für den weiteren Verlauf berücksichtigt werden sollen. Für die Auswahl können beispielsweise eine Schutzbedarfsermittlung (siehe Abschnitt 4.3.2) und eine Riskioanalyse (siehe Abschnitt 4.3.4) unter Einbezug der verfügbaren Ressourcen des MU verwendet werden.

Output von Schritt 1 ist das definierte Evaluationsobjekt, das heißt, eine Liste mit den zu evaluierenden Wallet-Funktionen und eine Liste mit Bedrohungsszenarien.

Abbildung 25 visualisiert die beschriebenen Aktivitäten von Schritt 1.

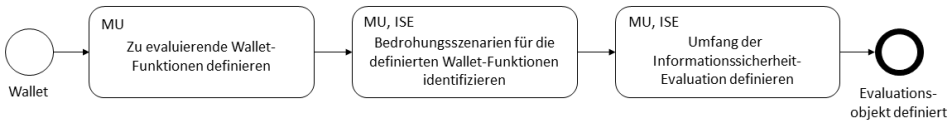


Abbildung 25: Schritt 1 der MEUSec-Methode

6.1.2.2 Benutzerbasierte Evaluation

Im Rahmen der benutzerbasierten Evaluation sollen Evaluationsergebnisse der Wallet durch Thinking aloud (siehe Abschnitt 5.2.8) gewonnen werden. Alternativ käme auch der Einsatz anderer benutzerbasierter Evaluationsverfahren in Betracht. Im Rahmen von früheren Evaluationen (wie etwa die Evaluationen aus Abschnitt 5.3, Abschnitt 7 und Abschnitt 9) hat sich Thinking aloud jedoch als ein besonders effektives und effizientes Verfahren erwiesen. Die benutzerbasierte Evaluation teilt sich auf in Schritt 2 – die Vorbereitung, Schritt 3 – die Durchführung und Schritt 4 – die Auswertung der benutzerbasierten Evaluation. Die benutzerbasierten Evaluationsergebnisse dienen später als Input für die expertenbasierte Evaluation (siehe Abschnitt 6.1.2.3).

Schritt 2 – Vorbereitung der benutzerbasierten Evaluation:

Input von Schritt 2 ist das definierte Evaluationsobjekt, das heißt, eine Liste mit den zu evaluierenden Wallet-Funktionen und eine Liste mit Bedrohungsszenarien.

Aktivität 2.1: Anfangs definieren der MU, der ISE und der UXE die Anforderungen der WU-Selektion im Hinblick darauf, dass später Thinking aloud (siehe Abschnitt 5.2.8) durchgeführt wird. Beispielsweise werden die erforderliche Anzahl der WU und bestimmte demografische Daten definiert, wie beispielsweise verschiedene Altersgruppen und Bildungsabschlüsse. Hierzu kann die Vorgehensweise nach Kujala und Kauppinen (2004) verwendet werden. Es sollten mindestens 5 WU akquiriert werden. Nielsen & Landauer (1993) zeigen in ihrer Untersuchung, dass sich mit 5 repräsentativen Probanden im Durchschnitt 85% der Usability-Probleme identifizieren lassen. Als repräsentativ gelten Probanden, die typische Merkmale der tatsächlichen Zielgruppe besitzen – etwa hinsichtlich ihrer Vorkenntnisse, Nutzungskontexte und Aufgaben. Abhängig vom Umfang der Evaluation kann es jedoch sinnvoll sein, die Anzahl der WU zu erhöhen – insbesondere, wenn gezielt spezifische UX-Aspekte (wie etwa die Wahrnehmung von Elementen des User Interface mit einer Rot-Grün-Schwäche) evaluiert werden sollen.

Aktivität 2.2: Anschließend definieren der MU, der ISE und der UXE Testfälle für die ausgewählten Wallet-Funktionen aus Aktivität 1.1. Jeder Testfall beschreibt eine exemp-

larische Nutzung einer ausgewählten Wallet-Funktion durch die WU. Der MU, der ISE und der UXE erstellen eine Liste mit dem Namen eines Testfalls, der zugehörigen Wallet-Funktion und der Beschreibung. Tabelle 26 zeigt beispielhafte einige Testfälle. Die Testfälle dienen als Grundlage für die Ausarbeitung einer strukturierten Anleitung zur Durchführung des Thinking aloud in Schritt 3. Die Anleitung enthält detailliertere Benutzerinteraktionen, welche die WU während des Thinking aloud in der Wallet ausführen sollen. Eine beispielhafte Anleitung ist online verfügbar[28].

Aktivität 2.3: Daraufhin akquiriert der MU die WU auf Basis der definierten Anforderungen aus Aktivität 2.2.

Aktivität 2.4: Danach richtet der MU die Endgeräte ein, sodass die in Aktivität 2.2 definierten Benutzerinteraktionen auf den Endgeräten durch die WU im Rahmen von Thinking aloud in Schritt 3 ausgeführt werden können.

Output von Schritt 2 ist die vorbereitete benutzerbasierte Evaluation, das heißt, die akquirierten WU, die Liste mit Testfällen, die Anleitung für das Thinking aloud und die eingerichteten Endgeräte für das Thinking aloud.

Schritt 3 – Durchführung der benutzerbasierten Evaluation:

Input von Schritt 3 ist die vorbereitete benutzerbasierte Evaluation, das heißt, die akquirierten WU, die Liste mit Testfällen, die Anleitung für das Thinking aloud und die eingerichteten Endgeräte für das Thinking aloud.

Aktivität 3.1: Anfangs startet der MU die Videoaufnahme des Thinking aloud. Diese umfasst die Aufnahme des Smartphone-Screens, die Aufnahme des Mikrophons und die Aufnahme der Kamera, mit welcher der jeweilige WU gefilmt wird.

Aktivität 3.2: Danach wird das Thinking aloud (siehe Abschnitt 5.2.8) des jeweiligen WU durchgeführt. Die WU bedienen jeweils die Wallet mithilfe der in Aktivität 2.2 erstellten Anleitung und verbalisieren ihre positiven und negativen Eindrücke.

Aktivität 3.3: Anschließend stoppt und sichert der MU die Aufnahmen des Thinking aloud der WU.

Output von Schritt 3 sind die Videoaufnahmen des Thinking aloud und zugehörige Metadaten, die eine Verknüpfung mit den demografischen Daten der WU ermöglichen.

[28] https://doi.org/10.5281/zenodo.15114275, im Dokument „2025_03_31_v1_Thinking_aloud_instruction.pdf“.

Schritt 4 – Auswertung der benutzerbasierten Evaluation:

Input von Schritt 4 sind die Aufnahmen des Thinking aloud der WU.

Aktivität 4.1: Der MU, der ISE und der UXE sammeln Stärken und Schwächen der UX und Informationssicherheit der definierten Wallet-Funktionen, indem sie die Aufnahmen des Thinking aloud der WU aus Schritt 3 betrachten. Es wird empfohlen, dass die Durchführenden der Rollen die Aufnahmen des Thinking aloud separat betrachten (um die Stärken und Schwächen zu dokumentieren), damit sie sich nicht gegenseitig beeinflussen und damit sie die Aufnahmen beliebig vor- und zurückspulen können. Anschließend können die Ergebnisse zusammengeführt werden. Hierzu werden die Stärken und Schwächen durch den MU mithilfe einer Vorlage festgehalten. Die Vorlage beinhaltet die folgenden Inhalte:

- *Identifikator:* ein Identifikator, der die jeweilige Stärke oder Schwäche eindeutig identifiziert.
- *Bezeichnung:* eine Bezeichnung, als Titel der jeweiligen Stärke oder Schwäche.
- *Beschreibung:* eine detaillierte Beschreibung der Stärke oder Schwäche.
- *Stärke/Schwäche:* ob es sich um eine Stärke oder Schwäche handelt.
- *UX/Informationssicherheit:* ob die jeweilige Stärke oder Schwäche die UX oder Informationssicherheit betrifft. Falls es UX und Informationssicherheit betrifft, wird jeweils ein neuer Eintrag aufgenommen.
- *Attribute:* Attribute von UX oder Informationssicherheit, welche die jeweilige Stärke oder Schwäche betreffen. Als Attribute von UX können beispielsweise Nützlichkeit, Auffindbarkeit, Usability, Barrierefreiheit, Glaubwürdigkeit und Wert (siehe Abschnitt 3.1) verwendet werden. Als Attribute der Informationssicherheit können Vertraulichkeit, Integrität und Verfügbarkeit (siehe Abschnitt 4.1) verwendet werden.
- *Wallet-Funktionen:* die jeweiligen betroffenen Wallet-Funktionen, die in Schritt 1 definiert wurden.
- *Schweregrad:* der Schweregrad der identifizierten Schwäche, festgehalten auf einer Skala von 0 (gering) bis 4 (hoch).
- *Häufigkeit:* Häufigkeit des Autretrens der Schwäche.
- *Betroffene WU:* die WU, bei denen die Stärke oder Schwäche aufgetreten ist, um Rückschlüsse auf demografische Daten vorzunehmen.

Output von Schritt 4 ist die Liste der gesammelten Stärken und Schwächen der UX und Informationssicherheit mithilfe der beschriebenen Vorlage. Die Stärken und Schwächen, insbesondere deren Schweregrad und Häufigkeit, können später in der expertenbasierten Evaluation verwendet werden, um die Erfüllungsgrade der UX- und Informationssicherheit-Heuristiken festzulegen.

Abbildung 26 zeigt die beschriebenen Aktivitäten von Schritt 2 bis Schritt 4.

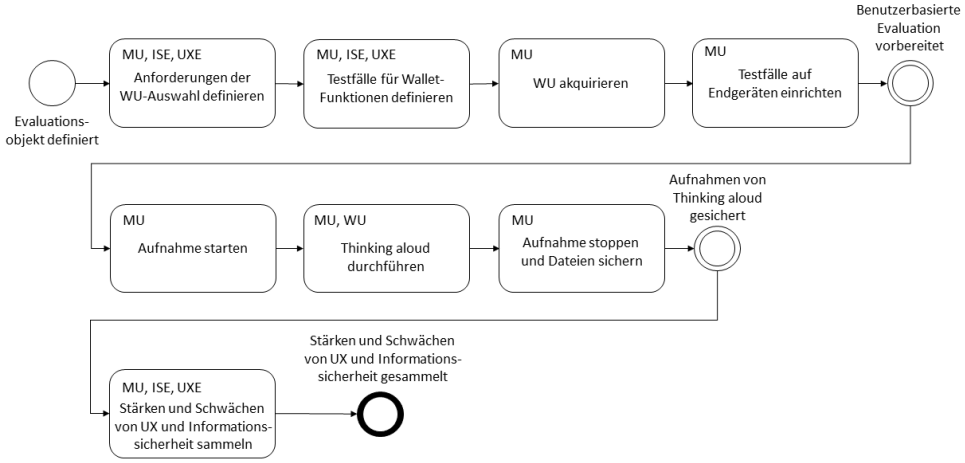


Abbildung 26: Schritt 2 bis 4 der MEUSec-Methode

6.1.2.3 Expertenbasierte Evaluation

Nach der benutzerbasierten Evaluation der Wallet folgt die expertenbasierte Evaluation der Wallet. Grundsätzlich sollen hierbei Evaluationsergebnisse der Wallet durch Heuristische Evaluationen (siehe Abschnitt 5.2.2) gewonnen werden. Zusätzlich sollen die Beeinflussungen zwischen Heuristiken und damit zwischen UX und Informationssicherheit evaluiert werden. Außerdem werden Scores für die UX und Informationssicherheit berechnet. Die benutzerbasierten Evaluationsergebnisse (siehe Abschnitt 6.1.2.2) dienen als Input für die expertenbasierte Evaluation. Die identifizierten Stärken und Schwächen mit deren Schweregrad und Häufigkeit aus der benutzerbasierten Evaluation können für die Festlegung der Erfüllungsgrade der Heuristiken in der expertenbasierten Evaluation verwendet werden. Die expertenbasierte Evaluation teilt sich auf in Schritt 5 – die Vorbereitung, Schritt 6 – die Durchführung und Schritt 7 – die Auswertung.

Schritt 5 – Vorbereitung der expertenbasierten Evaluation:

Input von Schritt 5 ist die Liste der gesammelten Stärken und Schwächen der UX und Informationssicherheit mithilfe der beschriebenen Vorlage aus Schritt 4.

Aktivität 5.1: Anfangs wählen der MU, der ISE und der UXE Heuristiken aus bereits vorhandenen Sammlungen an Heuristiken aus und fügen sie der eigenen Sammlung an Heuristiken hinzu. Als vorhandene Sammlungen an Heuristiken können beispielsweise die Sammlungen von Sauer u. a. (2025c) und von Nielsen (1994) verwendet werden. Für

das Hinzufügen der vorhandenen Heuristiken zur eigenen Sammlung soll die Vorlage der Stärken und Schwächen verwendet werden – ohne die Spalten „Stärke/Schwäche“, „Schweregrad“, „Häufigkeit“ und „Betroffene WU“. Falls noch nicht alle definierten Wallet-Funktionen mit Heuristiken abgedeckt sind, betrachten der MU, der ISE und der UXE die gesammelten Stärken und Schwächen der UX und Informationssicherheit aus Schritt 4 und formulieren weitere Heuristiken.

Aktivität 5.2: Sofern nun noch nicht alle zu evaluierenden Wallet-Funktionen durch Heuristiken abgedeckt sind, sollen der ISE und der UXE eine Literaturrecherche weiterer Heuristiken der UX und Informationssicherheit durchführen.

Aktivität 5.3: Anschließend soll der MU die identifizierten Heuristiken aus der Literaturrecherche der eigenen Sammlung mithilfe der Heuristik-Vorlage hinzufügen. Falls alle Wallet-Funktionen durch Heuristiken abgedeckt sind, können die Aktivitäten 5.2 und 5.3 übersprungen werden.

Aktivität 5.4: Danach soll der ISE die definierten Bedrohungsszenarien aus Schritt 1 gemäß dem Vorgehen aus Aktivität 1.2 aktualisieren, falls sich Bedarf durch die neu hinzugefügten Heuristiken (aus der externen Sammlung oder durch die Literaturrecherche) ergibt.

Aktivität 5.5: Falls neue Bedrohungsszenarien definiert wurden, aktualisieren der MU und der ISE den Umfang der Informationssicherheit-Evaluation gemäß dem Vorgehen aus Aktivität 1.3.

Aktivität 5.6: Abschließend priorisieren der MU, der ISE und der UXE die Heuristiken. Hierzu ordnen sie den Heuristiken ein Gewicht von 1 (nicht relevant) bis 5 (relevant) zu, indem der UX- und der Informationssicherheitsexperte zunächst ein Gewicht für die jeweiligen Heuristiken ihres Fachgebiets vorschlagen. Die endgültige Gewichtung nimmt der Methoden-Anwender unter Abwägung der fachlichen Einschätzungen der Experten vor. Für die Gewichtung der Heuristiken wird die Vorlage der Heuristiken aus Aktivität 5.1 um die Spalte „Gewichtung“ erweitert.

Output von Schritt 5 ist die Liste an gewichteten Heuristiken der UX und Informationssicherheit.

Schritt 6 – Durchführung der expertenbasierten Evaluation:

Input von Schritt 6 ist die Liste an gewichteten Heuristiken der UX und Informationssicherheit aus Schritt 5.

Aktivität 6.1: Anfangs bedienen der ISE und der UXE die definierten Wallet-Funktionen (ohne vorgegebene Aufgaben, das heißt, in einer Freiform-Evaluation). Dabei legen der ISE und UXE je Heuristik einen Erfüllungsgrad von 0 (nicht erfüllt) bis 4 (in vollem Umfang erfüllt) fest. Das heißt, der ISE und der UXE führen eine Heuristische Evaluation (siehe Abschnitt 5.2.2) durch. Für die Bewertung der Erfüllungsgrade der Heuristiken wird die Vorlage der Heuristiken aus Aktivität 5.6 um die Spalten „Score“ und „Begründung“ erweitert.

Aktivität 6.2: Anschließend führen der MU, der ISE und der UXE eine Feedback-Diskussion durch, in der jeder der Beteiligten zunächst während der Heuristischen Evaluation aufgetretene Probleme mit Heuristiken nacheinander benennt. Beispielsweise könnte eine Heuristik zu allgemein oder vage formuliert sein, weshalb sie von den Evaluierenden unterschiedlich interpretiert wird. Die genannten Probleme werden gemeinsam besprochen und dokumentiert, sodass eine Liste entsteht, welche die Heuristiken mit den dazugehörigen Problemen beinhaltet.

Aktivität 6.3: Falls Probleme mit den Heuristiken aufgetreten sind, passen der MU, der ISE und der UXE die Heuristiken an und beginnen erneut mit Schritt 6. Wenn keine Probleme aufgetreten sind, können die Aktivitäten 6.2 und 6.3 übersprungen werden.

Aktivität 6.4: Danach nimmt der MU die Heuristiken in eine Interaktionsmatrix (Nechansky, 2016) auf, in der alle Heuristiken mit ihren Nummern und Bezeichnungen jeweils als Überschriften der Zeilen und Spalten aufgeführt werden.

Aktivität 6.5: Anschließend legen der MU, der ISE und der UXE die Interaktionseigenschaften jeder Heuristik in der Interaktionsmatrix fest. Dabei werden alle Heuristiken paarweise gegenübergestellt, um zu bestimmen, ob zwischen ihnen eine komplementäre, konkurrierende oder neutrale Beeinflussung besteht. Ziel ist es, zu klären, inwiefern sich jeweils 2 Heuristiken gegenseitig beeinflussen. Beispielhaft zeigt Tabelle 13 eine Interaktionsmatrix mit 3 Heuristiken: ausreichende Passwortkomplexität (H1), schneller Login (H2) und ausreichend Hilfshinweise (H3). Es wird deutlich, dass H1 konkurrierend zu H2 ist. Andersherum beeinflusst H1 nicht H2, sodass die Interaktionseigenschaft „neutral“ zugeordnet wurde.

	H1: Passwortkomplexität	H2: Schneller Login	H3: Ausreichend Hilfshinweise
H1: Passwortkomplexität	-	konkurrierend	neutral
H2: Schneller Login	neutral	-	neutral
H3: Ausreichend Hilfshinweise	komplementär	komplementär	-

Tabelle 13: Beispiel einer Interaktionsmatrix

Aktivität 6.6: Nachdem die Interaktionsmatrix vollständig ausgefüllt wurde, fügt der MU die Interaktionseigenschaften der Heuristiken der eigenen Heuristik-Sammlung hinzu, indem er die Vorlage der Heuristiken aus Aktivität 6.1 um die Spalte „Interaktionen“ erweitert. So dokumentiert der MU für jede Heuristik, welche Interaktionseigenschaften zu anderen Heuristiken definiert wurden.

Output von Schritt 6 sind die bewerteten Heuristiken und die Interaktionsmatrix der Heuristiken.

Schritt 7 – Auswertung der expertenbasierten Evaluation:

Input von Schritt 7 sind die bewerteten Heuristiken aus Schritt 6.

Aktivität 7.1: Zunächst aggregiert der MU die Einzelscores aller Heuristiken auf Attributsebene. Der Einzelscore einer Heuristik ergibt sich aus dem Produkt ihres Gewichts und ihres Erfüllungsgrads. Anschließend wird der Gesamtscore (GS) für jedes Attribut berechnet, indem die Einzelscores aller zugehörigen Heuristiken summiert werden. Um den durchschnittlichen Gesamtscore (ØGS) eines Attributs zu ermitteln, wird der GS durch die Anzahl der zugehörigen Heuristiken geteilt. Der maximal mögliche Gesamtscore (MGS) eines Attributs ergibt sich aus dem Produkt des Gewichts und dem maximalen Erfüllungsgrad. Der durchschnittliche maximal mögliche Gesamtscore (ØMGS) wird berechnet, indem der MGS durch die Anzahl der zugehörigen Heuristiken geteilt wird. Anschließend wird das Verhältnis (Ratio) zwischen ØGS und ØMGS ermittelt, das angibt, inwieweit ein Attribut erfüllt ist. Dieses Verhältnis bewegt sich zwischen 0 (nicht erfüllt) und 1 (vollständig erfüllt).

Aktivität 7.2: Danach aggregiert der MU die Scores der einzelnen Attribute, um einen Gesamtscore für die UX und einen Gesamtscore für die Informationssicherheit zu berechnen. Dazu wird zunächst der Durchschnittswert aller MGS der UX-Attribute aus Aktivität 7.1 berechnet. Ebenso wird der Durchschnittswert aller MGS der Informationssicherheit-Attribute berechnet. Anschließend wird der Durchschnittswert aller ØMGS der UX-Attribute berechnet. Ebenso wird der Durchschnittswert aller ØMGS der Informationssicherheit-Attribute berechnet. Danach wird jeweils das Verhältnis beider Werte berechnet, was den Score der UX und den Score der Informationssicherheit ergibt. Die Scores können in einer weiteren Anwendung der MEUSec-Methode auf eine verbesserte Version der Wallet verwendet werden, um zu prüfen, inwiefern die Verbesserungsvorschläge aus Schritt 8 zu messbaren Verbesserungen führen.

Aktivität 7.3: Abschließend fügt der MU die eigene Sammlung an Heuristiken der externen Sammlung an Heuristiken hinzu. So können die erstellten Heuristiken durch weitere

Personen später wiederverwendet werden. Grundsätzlich ist diese Aktivität für die Anwendung der MEUSec-Methode mithilfe des Software-Tools angedacht (siehe Kapitel 9). Das Software-Tool kann genutzt werden, um die eigene Sammlung der Heuristiken mit anderen MU, UXE und ISE zu teilen. Wenn die MEUSec-Methode manuell (ohne Software-Tool) durchgeführt wird, können die Heuristiken anderweitig publiziert werden.

Output von Schritt 7 umfasst einen Score der UX, einen Score der Informationssicherheit und die Veröffentlichung der eigenen Sammlung an Heuristiken, sodass diese unter den externen Sammlungen an Heuristiken verfügbar ist.

Abbildung 27 visualisiert die beschriebenen Aktivitäten von Schritt 5 bis Schritt 7.

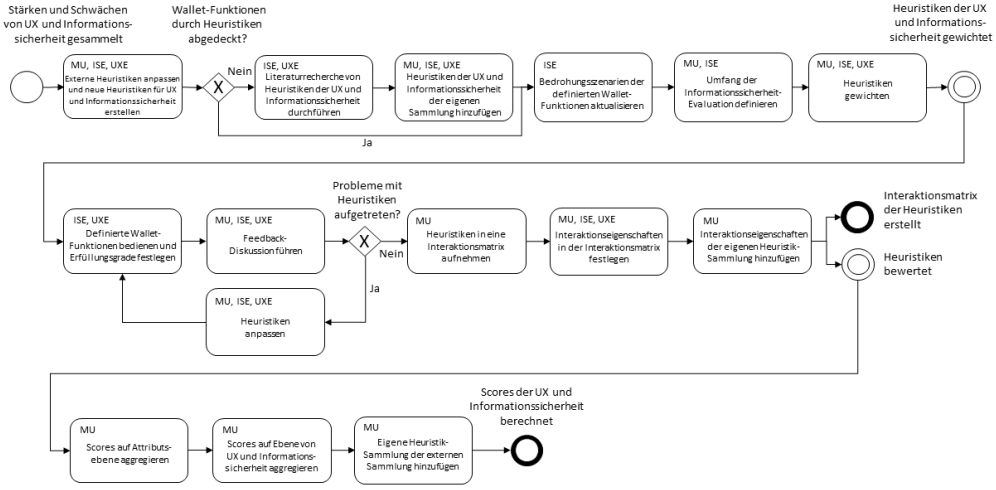


Abbildung 27: Schritt 5 bis 7 der MEUSec-Methode

6.1.2.4 Sammlung von Verbesserungsvorschlägen

Nachdem die Wallet durch Benutzer und Experten evaluiert wurde, folgt in Schritt 8 die Sammlung von Verbesserungsvorschlägen der UX und Informationssicherheit. Grundsätzlich werden die Verbesserungsvorschläge auf Basis der UX- und Informationssicherheit-Heuristiken (siehe Aktivität 5.6 in Abschnitt 6.1.2.3) gesammelt – unter Berücksichtigung der verschiedenen Interaktionseigenschaften zwischen den Heuristiken (siehe Aktivität 6.5 in Abschnitt 6.1.2.3).

Schritt 8 – Sammlung von Verbesserungsvorschlägen der UX und Informationssicherheit:

Input von Schritt 8 ist die Interaktionsmatrix aus Schritt 6.

Aktivität 8.1: Anfangs sammeln der MU, der ISE und der UXE jeweils Verbesserungsvorschläge (Kompromisslösungen) für konkurrierende Heuristiken.

Aktivität 8.2: Falls keine Lösung für einen Konflikt gefunden wird, müssen der MU, der ISE und der UXE entweder UX oder Informationssicherheit priorisieren. Nachdem UX oder Informationssicherheit priorisiert wurde, dient die jeweilige Heuristik von UX oder Informationssicherheit unmittelbar als Verbesserungsvorschlag. Beispielsweise stehen folgende UX- und Informationssicherheit-Heuristiken miteinander in Konflikt: Die Wallet-Pin darf maximal 4 Zeichen lang sein (UX-Heuristik). Die Wallet-Pin muss mindestens 6 Zeichen lang sein (Informationssicherheit-Heuristik). Der MU, der ISE und der UXE definieren, dass die Informationssicherheit priorisiert werden soll. Folglich muss die Wallet entsprechend der Informationssicherheit-Heuristik angepasst werden. Das heißt, die Wallet soll einen 6-stelligen Pin verwenden. Die Entscheidungen werden jeweils durch den MU dokumentiert.

Aktivität 8.3: Anschließend sammeln der MU, der ISE und der UXE Verbesserungsvorschläge für komplementäre und neutrale Heuristiken. Die komplementären und neutralen Heuristiken dienen unmittelbar als Verbesserungsvorschläge, da sie sich nicht negativ beeinflussen. Die Verbesserungsvorschläge werden durch den MU dokumentiert.

Output von Schritt 8 ist die Liste der Verbesserungsvorschläge.

Abbildung 28 visualisiert die beschriebenen Aktivitäten von Schritt 8.

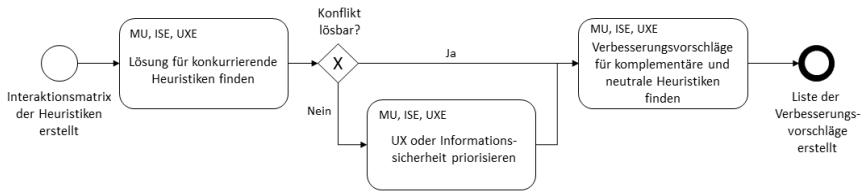


Abbildung 28: Schritt 8 der MEUSec-Methode

Falls Aktivitäten der MEUSec-Methode wiederholt werden, müssen die wiederholten Aktivitäten und die resultierenden Änderungen an Methodenartefakten in einem globalen Änderungsprotokoll festgehalten werden.

6.1.2.5 Vorgehen bei erneuter Anwendung der MEUSec-Methode

Bei einer erneuten Anwendung der MEUSec-Methode auf eine verbesserte Version einer Wallet (die auf Basis der Verbesserungsvorschläge aus der vorherigen Anwendung der MEUSec-Methode verbessert wurde) wird wieder bei Schritt 1 begonnen. Damit sich die Scores der vorherigen Anwendung der MEUSec-Methode mit den Scores der erneuten Anwendung der MEUSec-Methode vergleichen lassen, müssen dieselben zu evaluierenden Wallet-Funktionen und Bedrohungsszenarien verwendet werden. In Schritt 3 muss die benutzerbasierte Evaluation (Thinking aloud) erneut durchgeführt werden. In Schritt 4 müssen die Stärken und Schwächen der angepassten Wallet dokumentiert werden. In Schritt 5 müssen dieselben Heuristiken mit denselben Gewichten aus der vorherigen Anwendung der MEUSec-Methode verwendet werden. Die Erfüllungsgrade der Heuristiken müssen erneut für die angepasste Wallet unter Berücksichtigung der identifizierten Stärken und Schwächen festgelegt werden. Die neuen Scores der UX und Informationssicherheit, die sich aus den Erfüllungsgraden der Heuristiken ergeben, dienen zur Prüfung, ob die Verbesserungsvorschläge aus der vorherigen Anwendung der MEUSec-Methode zu messbaren Verbesserungen geführt haben.

6.2 Entwicklung und Entwurfsentscheidungen der Methode

Die Entwicklung und die Begründungen von Entwurfsentscheidungen der MEUSec-Methode werden im Folgenden beschrieben.

Nach der Gegenüberstellung identifizierter Evaluationsverfahren (siehe Abschnitt 5.2) wurde das Verfahren Heuristic Walkthrough (siehe Abschnitt 5.2.5) adaptiert, sodass nicht nur Experten für UX und Informationssicherheit involviert sind, sondern auch tatsächliche Endanwender. Die Meinungen von Experten und Endanwendern können variieren (Jaspers, 2009), sodass beide Gruppen in die Evaluation miteinbezogen werden sollten. Der erste Teil des Heuristic Walkthrough – Cognitive Walkthrough (siehe Abschnitt 5.2.4) – wurde durch Thinking aloud (siehe Abschnitt 5.2.8) ersetzt, damit tatsächlich Endanwender involviert sind und nicht nur Experten, die sich in Endanwender hineinversetzen. Im zweiten Teil des Heuristic Walkthrough wird eine Heuristische Evaluation (siehe Abschnitt 5.2.2) durchgeführt, indem der Erfüllungsgrad von Heuristiken bewertet wird. Die Ergebnisse des Thinking aloud (Stärken und Schwächen der UX und Informationssicherheit) vom ersten Teil des Heuristic Walkthrough können verwendet werden, um die Erfüllungsgrade der Heuristiken im zweiten Teil des Heuristic Walkthrough – der Heuristische Evaluation – festzulegen.

Rusu u. a. (2011) entwickelten ein Verfahren, mit dem sich Heuristiken der UX und Informationssicherheit entwickeln lassen. Heuristiken alleine reichen allerdings nicht aus, um den Zusammenhang zwischen UX und Informationssicherheit zu evaluieren, da die Beeinflussungen zwischen Heuristiken nicht betrachtet werden. Dennoch sind Heuristiken relevant, um einen Erfüllungsgrad je Heuristik festzulegen. Die von Rusu u. a. (2011) entwickelte Vorlage zur Definition von Heuristiken wurde adaptiert, sodass sich Heuristiken im Rahmen der MEUSec-Methode standardisiert der eigenen Heuristik-Sammlung hinzufügen lassen. Insbesondere wurde die Vorlage so angepasst, dass jeder Heuristik die betroffenen UX-Attribute (siehe Abbildung 6) oder Informationssicherheit-Attribute – die Schutzziele (siehe Abschnitt 4.1) – zugeordnet werden können. Dies ermöglicht die Aggregation der Erfüllungsgrade einzelner Heuristiken zunächst auf Attributsebene und anschließend auf Ebene von UX und Informationssicherheit. Durch die aggregierten Scores können verschiedene Software-Versionen miteinander verglichen werden, um zu prüfen, ob die Verbesserungsvorschläge nach Durchführung der MEUSec-Methode zu messbaren Verbesserungen beigetragen haben. So kann die MEUSec-Methode früh im Entwicklungsstadium eines Software-Systems (beispielsweise auf einen Software-Prototyp) bis hin zum fertigen Produkt angewendet werden.

Sicherheitsrelevante Softwarekomponenten, potenzielle Angreifer und Bedrohungen können stark variieren. Daher wurde in das Vorgehensmodell der MEUSec-Methode eine Aktivität aufgenommen, bei welcher der Experte für Informationssicherheit die sicherheitsrelevanten Softwarekomponenten, potenziellen Angreifer und Bedrohungen identifiziert, priorisiert und damit den Umfang der Informationssicherheit-Evaluation festlegt.

Zudem wurde der Experte für Informationssicherheit in die Aktivität des Thinking aloud integriert, indem er zusätzlich zum UX-Experten auch die Aufnahmen der Probanden betrachtet. So können auch Schwächen und Stärken der Informationssicherheit gesammelt werden, zum Beispiel unverständliche Sicherheitsmeldungen, die zu Informationssicherheit-Schwächen führen können.

Da bereits Heuristiken entwickelt wurden, wie die Heuristiken von Nielsen (1994) und von Sauer u. a. (2025c), wurde die Aktivität 5.1 (siehe Abschnitt 6.1.2.3) in das Vorgehensmodell der MEUSec-Methode aufgenommen, um bestehende Heuristiken zu adaptieren. Die bestehenden Heuristiken können zusätzlich um weitere Heuristiken erweitert werden (beispielsweise auf Basis der identifizierten Stärken und Schwächen), wenn nicht alle definierten Wallet-Funktionen durch Heuristiken abgedeckt sind. Des Weiteren können Heuristiken, die während der Anwendung der MEUSec-Methode ausgewählt wurden, in weiteren Durchführungen der MEUSec-Methode wiederverwendet werden.

Es hat sich bei der Anwendung der MEUSec-Methode gezeigt, dass Heuristiken während der Bewertung der Erfüllungsgrade unverständlich oder zu abstrakt sein können. Daher

wurden Aktivität 6.2 und Aktivität 6.3 (siehe Abschnitt 6.1.2.3) in das Vorgehensmodell der MEUSec-Methode aufgenommen, die nach der Bewertung der Erfüllungsgrade aller Heuristiken durchgeführt werden, um aufgetretene Probleme der Heuristiken zu sammeln und diese zu beheben.

Um die Beeinflussungen zwischen UX und Informationssicherheit zu bewerten, wurden die Aktivitäten 6.4 und 6.5 zur Erstellung einer Interaktionsmatrix (Nechansky, 2016) dem Vorgehensmodell hinzugefügt. In diese Interaktionsmatrix werden alle definierten Heuristiken aufgenommen und Interaktionseigenschaften zwischen den Heuristiken festgelegt. Die Erstellung einer Interaktionsmatrix ist relevant für die Sammlung der Verbesserungsvorschläge für UX und Informationssicherheit. Denn für jede Interaktionseigenschaft sollte ein anderer Ansatz zur Verbesserung gewählt werden. Komplementäre und neutrale Heuristiken dienen unmittelbar als Basis für die Formulierung von Verbesserungsvorschlägen, da sie sich nicht negativ beeinflussen. Für konkurrierende Heuristiken sollte zunächst nach einer Konfliktlösung gesucht werden. Wenn keine gefunden wird, muss entweder UX oder Informationssicherheit priorisiert werden. Wenn beispielsweise UX priorisiert wird, dient die UX-Heuristik als Verbesserungsvorschlag.

Tabelle 14 fasst die Begründungen der MEUSec-Methode zusammen. Es werden jeweils die Erkenntnisse und die daraus abgeleiteten Anpassungen an der MEUSec-Methode erläutert.

Erkenntnisse	**Anpassungen an der MEUSec-Methode**
Meinungen von Experten und tatsächlichen Endanwendern können variieren.	Heuristic Walkthrough wurde angepasst, indem der erste Durchlauf (Cognitive Walkthrough) durch Thinking aloud ersetzt wurde. Auf diese Weise werden tatsächliche Endanwender einbezogen und nicht nur Experten, die sich in Endanwender hineinversetzen.
Die Ergebnisse der benutzerbasierten Evaluation dienen als Input für die expertenbasierte Evaluation, beispielsweise für die Festlegung der Erfüllungsgrade von Heuristiken. Die Kombination von Durchläufen mit vorgegebenen Benutzeraufgaben und Freiformauswertung verringert das Risiko, relevante Schwächen der Wallet zu übersehen.	Die benutzerbasierte Evaluation erfolgt zuerst durch Thinking aloud (mit vordefinierten Benutzeraufgaben) und anschließend durch die expertenbasierte Evaluation mittels Heuristische Evaluation (ohne vordefinierte Benutzeraufgaben).

Eine tiefergreifende Evaluation der Informationssicherheit reicht mit Thinking aloud nicht aus, da damit nur das User Interface evaluiert wird. Dennoch können Implikationen von UX und Informationssicherheit durch Thinking aloud identifiziert werden.	Der Experte für Informationssicherheit ist zusätzlich zum Experten der UX bei Betrachtung der Aufnahmen des Thinking aloud involviert.
Verschiedene Attribute der UX (beispielsweise Zufriedenheit und Effektivität) und Attribute der Informationssicherheit (beispielsweise Integrität und Vertraulichkeit) sollten bei der Bewertung der Erfüllungsgrade der Heuristiken berücksichtigt werden, um eine Aggregation zu ermöglichen.	Es wurde eine Vorlage erstellt, damit die Heuristiken standardisiert formuliert werden können. Insbesondere lassen sich Attribute der UX und Informationssicherheit den Heuristiken zuordnen. So lässt sich für jedes Attribut ein Score berechnen, indem die Erfüllungsgrade der Heuristiken aggregiert werden. Schließlich lassen sich die Scores der Attribute aggregieren, um einen Score für die UX und einen Score für die Informationssicherheit zu berechnen. Die Scores können verwendet werden, um in weiteren Anwendungen der MEUSec-Methode zu vergleichen, ob Verbesserungsvorschläge zu messbaren Verbesserungen geführt haben.
Heuristiken können sich bei der Bewertung der Erfüllungsgrade als unverständlich oder zu abstrakt erweisen.	Nach Bewertung der Erfüllungsgrade wurde eine Aktivität aufgenommen, um Probleme zu sammeln und eine mögliche Wiederholung einzuleiten.
Identifizierte Heuristiken sollten für wiederholte Anwendungen der MEUSec-Methode wiederverwendbar sein, um die Vergleichbarkeit der Ergebnisse und die Bewertung von Verbesserungen zu ermöglichen.	Eine Aktivität wurde integriert, um bestehende Heuristiken zu adaptieren.
Implikationen zwischen UX und Informationssicherheit können nicht alleine durch die Bewertung der Erfüllungsgrade von Heuristiken beurteilt werden. Bei widersprüchlichen Heuristiken, für die keine Lösungen gefunden werden können, muss entschieden werden, ob UX oder Informationssicherheit priorisiert werden soll.	Die Heuristiken werden in eine Interaktionsmatrix aufgenommen und jeweils mit den Interaktionseigenschaften „komplementär“, „konkurrierend“ und „neutral“ bewertet. Basierend auf den Interaktionseigenschaften wird jeweils ein anderer Ansatz zur Erhebung der Verbesserungsvorschläge gewählt.

Tabelle 14: Begründungen der MEUSec-Methode

6.3 Beschränkungen und Voraussetzungen der Methode

Nachfolgend werden die Beschränkungen und Voraussetzungen der MEUSec-Methode erläutert.

Die MEUSec-Methode wurde für die Evaluation und die Formulierung von Verbesserungsvorschlägen der UX und Informationssicherheit von Wallets entwickelt. Die MEUSec-Methode wurde bisher noch nicht auf andere Arten von Software-Systemen (als Wallets) angewendet. Allerdings ist davon auszugehen, dass sich die MEUSec-Methode für die Anwendung auf andere Arten von Software-Systemen adaptieren lässt. Dazu müssten neue UX- und Informationssicherheit-Heuristiken für die jeweilige Art des Software-Systems entwickelt und evaluiert werden. Eine Eignungsprüfung der MEUSec-Methode für andere Arten von Software-Systemen wurde allerdings noch nicht durchgeführt, sodass sich die MEUSec-Methode zunächst auf Wallets beschränkt. Eine entsprechende Untersuchung würde den Rahmen dieser vorliegenden Arbeit überschreiten.

Die MEUSec-Methode wurde nicht für eine tiefgreifende Evaluation der Informationssicherheit entwickelt (wie etwa für die Evaluation von Quellcode), sondern fokussiert auf jene UX- und Sicherheitsaspekte, die sich gegenseitig beeinflussen. Es besteht jedoch die Möglichkeit, auch tiefergreifendere Analysen der Informationssicherheit durchzuführen, indem zusätzliche Evaluationsverfahren (wie Penetrationstests) für die Festlegung der Erfüllungsgrade von Informationssicherheit-Heuristiken verwendet werden. Beispielsweise könnte eine Informationssicherheit-Heuristik lauten: „Die Wallet sollte durch ein angemessenes Authentifizierungsverfahren geschützt sein“. Um den Erfüllungsgrad dieser Informationssicherheit-Heuristik festzulegen, könnte ein Penetrationstest durchgeführt werden.

Die MEUSec-Methode fordert verschiedene Rollen, die besetzt werden müssen. Benötigt werden ein Experte der Informationssicherheit und ein Experte der UX. Außerdem wird ein Anwender der MEUSec-Methode gefordert, der keine Vorerfahrung mit Wallets haben muss, allerdings wäre dies von Vorteil. So könnte der Methoden-Anwender beispielsweise bei der Interpretation der Evaluationsergebnisse gezielter Rückfragen stellen und Kontextinformationen besser einordnen. Außerdem kann Expertise im Wallet-Bereich bei der Ableitung praxisnaher Maßnahmen und bei der Identifikation technischer Einschränkungen hilfreich sein. Zusätzlich werden mindestens 5 Probanden benötigt (siehe Abschnitt 6.1.2.2), welche die Wallet testen. Für die Anwendung der MEUSec-Methode durch die Ausführenden der Rollen sollten ausreichend Ressourcen (Zeit und Kosten) eingeplant werden. Als Vergleichsbasis können die Zeiten und Kosten angesetzt werden, die bei den beiden Anwendungen der MEUSec-Methode (siehe Kapitel 7 und Kapitel 9) gemessen wurden.

6.4 Einordnung der Methode

Nachfolgend wird die MEUSec-Methode mit anderen Ansätzen aus der Literatur verglichen.

Sauer u. a. (2024a) identifizierten verschiedene Verfahren zur Evaluation des Zusammenhangs zwischen UX und Informationssicherheit. Die Verfahren wurden bereits in Abschnitt 5.2 beschrieben. Nun werden die identifizierten Evaluationsverfahren mit der MEUSec-Methode verglichen.

Einige der identifizierten Evaluationsverfahren, wie GOMS (John und Kieras, 1994), SecureUse Score (Dutta u. a., 2016), Eye Tracking (Bojko, 2005) und Fragebögen wie SUS (Brooke, 1996), UEQ (Laugwitz u. a., 2008), UEQS (Schrepp u. a., 2017) und AttrakDiff (Hassenzahl u. a., 2003), sind reine UX-Evaluationsverfahren, die auf unterschiedliche Software-Varianten mit unterschiedlichen Sicherheitsniveaus angewendet werden können, um den Zusammenhang zwischen UX und Informationssicherheit zu evaluieren (siehe Abschnitt 5.2.14). Die mehrfache Anwendung der Evaluationsverfahren auf verschiedene Software-Varianten macht jedoch die Evaluation des Zusammenhangs zwischen UX und Informationssicherheit zeitaufwändig. Mit der MEUSec-Methode lässt sich der Zusammenhang von UX und Informationssicherheit mit nur einer Anwendung evaluieren. Die Heuristiken lassen sich verwenden, um einen Score für UX und einen Score für die Informationssicherheit zu berechnen. Außerdem lassen sich in der Interaktionsmatrix die unterschiedlichen Beeinflussungsarten bzw. Interaktionseigenschaften zwischen Heuristiken und damit zwischen UX und Informationssicherheit bewerten. Die Heuristiken und deren Interaktionseigenschaften können verwendet werden, um Verbesserungsvorschläge systematisch zu definieren.

Bei einer Heuristischen Evaluation (Nielsen und Molich, 1990) können UX- und Informationssicherheit-Heuristiken zur Evaluation von UX und Informationssicherheit verwendet werden, jedoch werden die unterschiedlichen Interaktionseigenschaften zwischen den Heuristiken und damit zwischen UX und Informationssicherheit nicht evaluiert. Im Rahmen der MEUSec-Methode lässt sich die Interaktionsmatrix verwenden, um unterschiedliche Interaktionseigenschaften zwischen den Heuristiken zu bewerten.

Das Ableiten von Heuristiken und das anschließende Formulieren von Verbesserungsvorschlägen auf Basis der Heuristiken und deren Interaktionseigenschaften ist zeit- und kostenintensiver als die direkte Formulierung von Verbesserungsvorschlägen. Allerdings lassen sich die Heuristiken zur Bestimmung eines Scores für UX und Informationssicherheit (sowie für deren Attribute wie Usability und Integrität) verwenden. Zudem lassen sich die Heuristiken einer Interaktionsmatrix hinzufügen, um Interaktionseigenschaften zwischen Heuristiken festzulegen. Die Heuristiken und Scores lassen sich in einer weite-

ren Anwendung der MEUSec-Methode wiederverwenden, um zu überprüfen, ob die Verbesserungsvorschläge zu messbaren Verbesserungen geführt haben – indem die neuen Scores mit den alten verglichen werden.

Des Weiteren beinhaltet die MEUSec-Methode sowohl einen experten- als auch einen benutzerbasierten Ansatz, da sich die Meinungen von Experten und Benutzern stark unterscheiden können (Jaspers, 2009). Zeit und Kosten ließen sich einsparen, wenn entweder nur ein expertenbasierter oder nur ein benutzerbasierter Ansatz verwendet wird. Die Kombination beider Ansätze erhöht jedoch die Qualität der Ergebnisse. Nur eines der identifizierten Evaluationsverfahren – SecureUse Score (Dutta u. a., 2016) – umfasst sowohl einen experten- als auch benutzerbasierten Ansatz. SecureUse Score erfordert jedoch die Evaluation verschiedener Software-Varianten, die unterschiedliche Sicherheitsniveaus haben, um den Zusammenhang zwischen UX und Informationssicherheit zu evaluieren. Alle anderen, identifizierten Evaluationsverfahren basieren entweder auf einem expertenbasierten oder auf einem benutzerbasierten Ansatz.

Eines der identifizierten Evaluationsverfahren, das einem kombinierten experten- und benutzerbasierten Ansatz nahekommt, ist der Heuristic Walkthrough (Sears, 1997). Im Rahmen des Heuristic Walkthrough wird zunächst der Cognitive Walkthrough (Wharton u. a., 1994) und anschließend die Heuristische Evaluation (Nielsen und Molich, 1990) durchgeführt. Beim Cognitive Walkthrough versetzen sich Evaluierende in die Rolle der Benutzer und testen das Software-System anhand vordefinierter Aufgaben. Danach folgt eine freie Evaluation (ohne vorgegebene Aufgaben) im Rahmen der Heuristischen Evaluation. Die MEUSec-Methode basiert auf dem Heuristic Walkthrough, ersetzt jedoch Cognitive Walkthrough durch Thinking aloud (Nielsen, 1993). Der Vorteil davon ist, dass tatsächliche Benutzer in die Evaluation miteinbezogen werden, anstatt sich nur Evaluierende in Benutzer hineinversetzen.

Thinking aloud – als benutzerbasierter Ansatz in der MEUSec-Methode – ist an sich ein reines UX-Evaluationsverfahren (ohne die Betrachtung der Informationssicherheit). Sauer u. a. (2025b) zeigten jedoch, dass Thinking aloud auch zur Evaluation der Implikationen zwischen UX und Informationssicherheit verwendet werden kann. Zum Beispiel haben Benutzer geäußert, dass sie ein Hinweis mit erforderlicher Bestätigung in der Wallet angezeigt bekommen wollen, wenn sicherheitskritische Aktionen durchgeführt werden, wie beispielsweise das Teilen von VC an nicht vertrauenswürdige VC-Prüfer.

7 Evaluation der ersten Version der MEUSec-Methode

Im Rahmen der ersten Evaluation wurde die erste Version der MEUSec-Methode durch Sauer u. a. (2025a) auf die Hidy-Wallet angewendet.

Die erste Version der MEUSec-Methode unterscheidet sich zur finalen Version (siehe Kapitel 6) im Wesentlichen darin, dass zuerst eigene UX- und Informationssicherheit-Heuristiken definiert werden und erst anschließend UX- und Informationssicherheit-Heuristiken aus vorgegebenen Sammlungen von Heuristiken adaptiert werden. Außerdem erfolgt die Feedback-Diskussion der Heuristiken bei der ersten Version der MEUSec-Methode erst nach der Berechnung der UX- und Informationssicherheit-Scores und nicht unmittelbar nach der Bewertung der Erfüllungsgrade der Heuristiken.

Durch die Anwendung der MEUSec-Methode auf die Hidy-Wallet sind grundsätzlich 2 originäre Beiträge entstanden: einerseits die Evaluation der MEUSec-Methode und andererseits die Evaluation der UX und Informationssicherheit der Hidy-Wallet durch die Anwendung der MEUSec-Methode.

Die 2 Evaluationen wurden jeweils als separate Online-Meetings durchgeführt. Im Rahmen der Durchführung der MEUSec-Methode fanden einzelne Schritte und Aktivitäten ebenfalls in getrennten Online-Meetings statt, da jeweils nur bestimmte Rollen beteiligt waren. Der Methoden-Anwender teilte seinen Bildschirm und moderierte durch die einzelnen Schritte und Aktivitäten. Eine Ausnahme bildete Schritt 3 der Methode – die Durchführung des Thinking aloud. Das Thinking aloud wurde in Präsenz im Rahmen einer Laborsituation durchgeführt. Dabei wurden sowohl die Probanden (Video und Ton) als auch der Smartphone-Bildschirm aufgezeichnet.

In Abschnitt 7.1 wird die Vorgehensweise, insbesondere die Evaluationskriterien, der ersten Evaluation beschrieben. Daraufhin werden die Evaluationsergebnisse der Hidy-Wallet in Abschnitt 7.2 erläutert. Danach werden die identifizierten Stärken und Schwächen der Hidy-Wallet mit Stärken und Schwächen anderer Wallets (aus der Literatur) in Abschnitt 7.3 verglichen. Im Anschluss werden die Evaluationsergebnisse der MEUSec-Methode in Abschnitt 7.4 beschrieben. Abschließend werden die Limitationen in Abschnitt 7.5 dargestellt.

7.1 Vorgehensweise

Die Rollen der MEUSec-Methode wurden wie folgt besetzt: Der Methoden-Anwender (MU) war ein wissenschaftlicher Mitarbeiter, der über keine Vorerfahrung mit Wallets verfügte. Diese Auswahl des MU wurde speziell für die Evaluation der MEUSec-Methode getroffen. Es sollte evaluiert werden, ob die Rolle des MU durch eine Person besetzt werden kann, die keine Erfahrung mit Wallets besitzt. Die Erkenntnisse daraus sollten aufzeigen, ob die MEUSec-Methode zukünftig beispielsweise von UX-Dienstleistern genutzt werden kann, ohne dass eine vorherige Einarbeitung in Wallet-spezifische Themen erforderlich ist. Der Informationssicherheit-Experte (ISE) war ein wissenschaftlicher Mitarbeiter, der im Bereich der Informationssicherheit forscht. Der UX-Experte (UXE) war ein wissenschaftlicher Mitarbeiter, der im Bereich der UX forscht. Die Wallet-Benutzer (WU) wurden während der Durchführung der MEUSec-Methode akquiriert und werden daher im Rahmen des zugehörigen Schritts 2 der MEUSec-Methode (siehe Abschnitt 7.2) beschrieben. Die zu evaluierenden Funktionen der Hidy-Wallet werden im Rahmen des zugehörigen Schritts 1 der MEUSec-Methode (siehe Abschnitt 7.2) dargestellt.

Nachfolgend wird die Vorgehensweise der Evaluation der Hidy-Wallet beschrieben. Anschließend wird die Vorgehensweise der Evaluation der MEUSec-Methode erläutert.

Vorgehensweise der Evaluation der Hidy-Wallet:

Die MEUSec-Methode wurde auf die Hidy-Wallet angewendet, um die UX und Informationssicherheit der Hidy-Wallet zu evaluieren und Verbesserungsvorschläge zu finden.

Die Hidy-Wallet wurde als Evaluationsobjekt verwendet, da die Hidy-Wallet Teil des Forschungsprojekts „Schaufenster Sichere Digitale Identitäten Karlsruhe (SDIKA)“[29] war. So war es möglich, sich unkompliziert mit den Entwicklern auszutauschen und Zugang zu Dokumentationen der Hidy-Wallet zu erhalten.

Vorgehensweise der Evaluation der MEUSec-Methode:

Im Rahmen der Evaluation der MEUSec-Methode wurde lediglich die Anwendung der MEUSec-Methode auf die Hidy-Wallet betrachtet, da keine vergleichbaren Evaluationsverfahren identifiziert werden konnten. Der MU, der ISE und der UXE evaluierten die MEUSec-Methode anhand zuvor definierter Evaluationskriterien, indem sie qualitativ die Fragen, die den Evaluationskriterien zugeordnet sind, beantworteten. Zu diesem Zweck

[29] https://sdika.de

machten sich MU, ISE und UXE nach jedem der 8 durchgeführten Schritte Notizen zu den Evaluationskriterien. Zusätzlich war eine außenstehende Person bei der Durchführung der MEUSec-Methode anwesend, die sich ohne aktives Eingreifen Notizen zu den Evaluationskriterien machte. Insbesondere dokumentierte sie die Ausführungszeiten der Schritte. Nach der Anwendung der MEUSec-Methode gab es eine gemeinsame Diskussionsrunde, um zu bewerten, ob die Evaluationskriterien erfüllt, teilweise erfüllt oder nicht erfüllt wurden. Für jedes Evaluationskriterium wurden Argumente für und gegen dessen Erfüllung zusammengetragen. Auf Basis der Argumente wurde eine abschließende Bewertung der Erfüllung getroffen. Da zwischen den Rollen keine Meinungsverschiedenheiten auftraten, waren keine Konfliktlösungen notwendig.

Die definierten Evaluationskriterien lassen sich grundsätzlich der Qualität der Methodenartefakte (E1) und der Durchführbarkeit der Methode (E2) zuordnen. Die Evaluationskriterien (E1.1) Vollständigkeit, (E1.2) Konsistenz, (E1.3) Korrektheit, (E1.4) Nachvollziehbarkeit, (E1.5) Eindeutigkeit und (E1.6) Sachdienlichkeit wurden nach Al-Subaie & Maibaum (2006) festgelegt. Die Evaluationskriterien (E2.1) Effizienz, (E2.2) Effektivität und (E2.3) Akzeptanz wurden nach Kromrey (2001) festgelegt.

Für jedes Evaluationskriterium wurden zunächst Fragen durch den Verfasser dieser vorliegenden Arbeit gesammelt. Diese wurden anschließend durch die Durchführenden der MEUSec-Methode validiert.

Die Evaluationskriterien wurden unter der Annahme der sachgemäßen Durchführung der MEUSec-Methode bewertet. Um eine fehlerhafte Durchführung zu vermeiden, wurde die Durchführung der MEUSec-Methode überwacht. Konkret waren der Verfasser dieser Dissertation und eine außenstehende Person anwesend, um bei einer fehlerhaften Durchführung eingreifen zu können.

(E1) Qualität der Methodenartefakte:

(E1.1) Vollständigkeit: Wurde jede im Rahmen der Anwendung der MEUSec-Methode ausgewählte Wallet-Funktion hinsichtlich UX und Informationssicherheit evaluiert? Gibt es für jede ausgewählte Wallet-Funktion mindestens eine UX-Heuristik und mindestens eine Informationssicherheit-Heuristik, deren Erfüllungsgrad evaluiert wurde? Wurden alle Interaktionseigenschaften einer Heuristik zu anderen Heuristiken festgelegt? Wurde für jede Heuristik, die nicht als erfüllt bewertet wurde, mindestens ein Verbesserungsvorschlag identifiziert, mit Berücksichtigung der Interaktionseigenschaften der Heuristiken?

(E1.2) Konsistenz: Wird ein standardisiertes Bewertungsschema zur Beurteilung der Erfüllungsgrade aller Heuristiken verwendet? Wird ein standardisiertes Bewertungsschema zur Festlegung der Interaktionseigenschaften der Heuristiken (komplementär,

widersprüchlich oder neutral) verwendet? Sind die Verbesserungsvorschläge widerspruchsfrei?

(E1.3) Korrektheit: Wurden die Erfüllungsgrade der Heuristiken sachgemäß bewertet? Wurden die Scores der UX und der Informationssicherheit sachgemäß berechnet? Führen die Verbesserungsvorschläge zu einer messbaren Verbesserung?

(E1.4) Nachvollziehbarkeit: Sind die Erfüllungsgrade und die Interaktionseigenschaften der Heuristiken nachvollziehbar? Ist die Priorisierung von UX oder Informationssicherheit und deren Begründung bei widersprüchlichen Heuristiken nachvollziehbar? Sind die gewonnenen Verbesserungsvorschläge nachvollziehbar?

(E1.5) Eindeutigkeit: Sind die Heuristiken eindeutig formuliert? Sind die Erfüllungsgrade der Heuristiken eindeutig festgelegt? Sind die Interaktionseigenschaften der Heuristiken eindeutig formuliert? Sind die Verbesserungsvorschläge eindeutig formuliert?

(E1.6) Sachdienlichkeit: Dienen die Erfüllungsgrade der Heuristiken als Vergleichsbasis in einer weiteren Durchführung der MEUSec-Methode? Dienen die identifizierten Interaktionseigenschaften der Heuristiken als Basis für die Formulierung von Verbesserungsvorschlägen? Sind die Verbesserungsvorschläge relevant bzw. geeignet, um die identifizierten Schwächen der UX und Informationssicherheit unter Berücksichtigung der Interaktionseigenschaften der Heuristiken zu beheben?

(E2) Durchführbarkeit der Methode:

(E2.1) Effektivität: Lässt sich die MEUSec-Methode zur Evaluation von UX und Informationssicherheit unter Berücksichtigung der Interaktionseigenschaften von Heuristiken verwenden? Lässt sich die MEUSec-Methode zur Identifikation von Verbesserungsvorschlägen für UX und Informationssicherheit unter Berücksichtigung der Interaktionseigenschaften verwenden?

(E2.2) Effizienz: Ist der Ressourcenaufwand (Zeit und Kosten) gerechtfertigt im Verhältnis zu den gewonnenen Artefakten, die durch die Anwendung der MEUSec-Methode entstehen?

(E2.3) Akzeptanz: Wird die MEUSec-Methode vom MU, ISE und UXE akzeptiert? Die Einschätzung hierzu soll unter Einbeziehung der Evaluationsergebnisse aller vorherigen Evaluationskriterien erfolgen.

7.2 Evaluationsergebnisse der Hidy-Wallet

Im Folgenden wird die Evaluation der Hidy-Wallet beschrieben. Es werden jeweils die Input- und Output-Artefakte der 8 Schritte der MEUSec-Methode erläutert.

Schritt 1 – Definition des Evaluationsobjekts:

Input von Schritt 1 war das Evaluationsobjekt, das heißt, die Hidy-Wallet[30].

Schritt 1, Aktivität 1 – Definition der zu evaluierenden Wallet-Funktionen: Der MU definierte die Wallet-Funktionen, die hinsichtlich UX und Informationssicherheit evaluiert werden sollten. Hierzu wählte der MU die zu evaluierenden Wallet-Funktionen aus einer Liste an Wallet-Funktionen von Krauß u. a. (2023b) aus. Die folgenden Wallet-Funktionen wurden durch den MU ausgewählt:

(WF1) Speicherung von VC (siehe Abschnitt 2.2), insbesondere Darstellung und Überprüfung der Vertrauenswürdigkeit des VC-Ausstellers (siehe Abschnitt 2.3).

(WF2) Verwaltung von VC, insbesondere Schnellzugriff auf gespeicherte VC, Löschung von VC und Anzeige von VC.

(WF3) Teilen von VC, insbesondere Darstellung und Überprüfung der Vertrauenswürdigkeit des VC-Prüfers (siehe Abschnitt 2.3) sowie Darstellung und Überprüfung des Verwendungszwecks der zu teilenden VC.

Zusätzlich wurden weitere zu evaluierende Wallet-Funktionen durch den MU definiert:

(WF4) Zahlungsfunktion, insbesondere Anforderung und Ausführung von Zahlungen.

(WF5) Allgemeine Bedienfunktionen, konkret die Navigation zu vorherigen und nachfolgenden Ansichten der Wallet, das Anzeigen von Hilfestellungen, Spracheinstellung, Bestätigungsdialoge, Suche und Filterung.

Schritt 1, Aktivität 2 – Identifizierung sicherheitsrelevanter Softwarekomponenten und potenzieller Angreifer sowie Aktivität 3 – Definition des Umfangs der Informationssicherheitsevaluation: Der ISE identifizierte die sicherheitsrelevanten Softwarekomponenten und potenziellen Angreifer durch Sichtung der Wallet-Dokumentationen und erläuterte diese dem MU. Anschließend legte der MU unter Berücksichtigung der verfügbaren Ressourcen fest, welche der sicherheitsrelevanten Softwarekomponenten und potenziellen Angreifer für die spätere Evaluation berücksichtigt werden sollen. Festgelegt wurde

[30] https://hidy.eu

ein böswilliger VC-Aussteller, der VC erstellen und signieren kann, wodurch die Integrität und Vertraulichkeit beeinträchtigt werden könnte. Zudem könnte ein VC-Aussteller unerwünschte Informationen in einem VC speichern, wie beispielsweise versteckte Gesundheitsdaten. Dadurch könnten VC-Aussteller und VC-Prüfer zusammenarbeiten, was einem böswilligen VC-Prüfer ermöglichen würde, die VC für eigene Zwecke zu missbrauchen. Dies gefährdet sowohl die Vertraulichkeit als auch die Integrität der Informationen.

Output von Schritt 1 war das definierte Evaluationsobjekt, das heißt, eine Liste mit den zu evaluierenden Wallet-Funktionen und eine Liste mit ausgewählten sicherheitsrelevanten Softwarekomponenten sowie potenziellen Angreifern.

Schritt 2 – Vorbereitung der benutzerbasierten Evaluation:

Input von Schritt 2 war das definierte Evaluationsobjekt aus Schritt 1, das heißt, eine Liste mit den zu evaluierenden Wallet-Funktionen und eine Liste mit ausgewählten sicherheitsrelevanten Softwarekomponenten sowie potenziellen Angreifern.

Schritt 2, Aktivität 1 – Definition der Anforderungen an die WU-Auswahl: Der MU, UXE und ISE legten fest, dass 10 WU am Thinking aloud (siehe Abschnitt 5.2.8) teilnehmen sollten. Die Anzahl wurde damit begründet, dass Nielsen & Landauer (1993) zeigten, dass bereits 5 repräsentative Probanden im Durchschnitt 85% der Usability-Probleme identifizieren. Als repräsentativ gelten Probanden, die typische Merkmale der Zielgruppe aufweisen – etwa hinsichtlich ihrer Vorkenntnisse, Nutzungskontexte oder Aufgaben. Aufgrund der verschiedenen Kategorien an demografischen Daten wurde jedoch durch den MU, UXE und ISE beschlossen, die Anzahl der WU von 5 auf 10 zu erhöhen. Die WU sollten sich hinsichtlich der folgenden Kategorien demografischer Daten unterscheiden: Alter, privates mobiles Betriebssystem (zum Beispiel iOS), Vorerfahrung mit Wallets und Kryptowährungen, IT-Affinität, Deutschkenntnisse und körperliche Einschränkungen (zum Beispiel Seheinschränkung).

Schritt 2, Aktivität 2 – Erstellung einer Anleitung für das Thinking aloud: Der MU, UXE und ISE erstellten eine Anleitung für das Thinking aloud. Diese beinhaltet Aufgaben, welche die WU später in Schritt 3 im Rahmen des Thinking aloud in der Hidy-Wallet durchführen sollten:

1. Öffnen Sie die Hidy-Wallet auf dem Startbildschirm.
2. Fordern Sie eine Zahlung von 5000 Satoshi[31] in Ihrer Hidy-Wallet an.

[31] Ein Satoshi entspricht einem Hundertmillionstel eines Bitcoin.

3. Warten Sie, bis die Zahlung eingegangen ist. An dieser Stelle würden Sie Satoshis aus einer externen Anwendung in die Hidy-Wallet übertragen. In diesem Fall ist die Hidy-Wallet bereits mit Satoshis aufgeladen.
4. Sie können die Hidy-Wallet jetzt schließen und erneut öffnen.
5. Fügen Sie „Demo-Shop“ in Ihrer Wallet hinzu.
6. Kaufen Sie ein beliebiges Ticket im Demo-Shop in der Wallet.
7. Öffnen Sie das gekaufte Ticket in der Hidy-Wallet.
8. Ihnen fällt auf, dass Sie das falsche Ticket gekauft haben.
9. Löschen Sie das Ticket aus der Hidy-Wallet.

Schritt 2, Aktivität 3 – Akquise der WU: Die 10 WU wurden durch den MU auf Basis der definierten Anforderungen aus Schritt 2, Aktivität 1 zum Thinking aloud eingeladen. Zur Erhebung der demografischen Daten erhielten die WU einen Fragebogen zum Ausfüllen. Außerdem unterschrieben die WU eine Einverständniserklärung für die Datenerhebung. Die WU erhielten 20€ als Aufwandsentschädigung. Tabelle 15 zeigt die demografischen Daten der 10 WU. Aus Gründen der besseren Lesbarkeit wurde „Betriebssystem“ durch „OS“ abgekürzt.

Geschlecht	**Alter**	**Deutschkenntnisse**	**Job**	**IT-Affinität**	**Privates OS**	**Vorerfahrung**	**Einschränkungen**
Männlich	26-40	Nativ	Wissenschaftler	Medium	iOS	Wallets	-
Weiblich	26-40	Nativ	Manager	Hoch	iOS	Wallets	-
Männlich	26-40	Nativ	-	Hoch	iOS	Wallets	-
Männlich	16-25	Nativ	Wissenschaftler	Hoch	Android	-	-
Weiblich	26-40	Nativ	Eventmanager	Medium	iOS	Wallets	Brille
Männlich	16-25	Fließend	Student	Medium	Android	-	-
Weiblich	16-25	Medium	Student	Medium	Android und iOS	Wallets	-
Weiblich	41-60	Nativ	Assistenz des CEO	Gering	Android	-	Brille
Männlich	41-60	Nativ	IT-Admin	Hoch	Android	Krypto	Brille
Weiblich	61-80	Nativ	Lehrer	Gering	Android	Wallets	Brille

Tabelle 15: Hidy-Wallet – Demografische Daten der Probanden. (Sauer u. a., 2025a). Übersetzt aus dem Englischen.

Schritt 2, Aktivität 4 – Vorbereitung des Endgeräts: Die Hidy-Wallet wurde auf einem iPhone 14 Pro Max installiert. Daher beschränkt sich die Evaluation ausschließlich auf die iOS-Version der Hidy-Wallet. Versionen der Hidy-Wallet für andere Betriebssysteme – wie etwa Android – blieben außerhalb des Evaluationsumfangs und könnten spezifische Abweichungen in Funktion und Interaktion aufweisen. Die Anleitung mit den definierten WU-Aufgaben (siehe Schritt 2, Aktivität 2) wurde ausgedruckt, damit die WU die Anleitung beim späteren Thinking aloud in Schritt 3 nutzen konnten. Auch die Geräte zur Aufzeichnung des Smartphone-Bildschirms und die Geräte für die Bild- und Tonaufzeichnung der WU wurden vorbereitet.

Output von Schritt 2 war die vorbereitete benutzerbasierte Evaluation, das heißt, die akquirierten WU, die Anleitung für das Thinking aloud und das eingerichtete Endgerät für das Thinking aloud.

Schritt 3 – Durchführung der benutzerbasierten Evaluation:

Input von Schritt 3 war die vorbereitete benutzerbasierte Evaluation aus Schritt 2, das heißt, die akquirierten WU, die Anleitung für das Thinking aloud und das eingerichtete Endgerät für das Thinking aloud.

Schritt 3, Aktivität 1 – Start der WU-Aufnahmen, Aktivität 2 – Durchführung des Thinking aloud und Aktivität 3 – Abschluss und Speicherung der WU-Aufnahmen: Zunächst gab der MU jedem WU die ausgedruckte Anleitung mit den Aufgaben, die jeder WU in der Wallet durchführen sollte. Danach startete der MU die Aufnahme des Smartphone-Bildschirms und die Bild- und Tonaufzeichnung des WU. Jeder WU führte Thinking aloud mithilfe der ausgedruckten Anleitung durch. Anschließend stoppte der MU die WU-Aufnahme und archivierte diese. Das Thinking aloud wurde nacheinander je WU durchgeführt (nicht gemeinsam mit allen WU).

Output von Schritt 3 waren die WU-Aufnahmen des Thinking aloud. Die WU-Aufnahmen wurden mittlerweile aus Datenschutzgründen gelöscht und sind somit nicht einsehbar. Allerdings wurden die daraus identifizierten Stärken und Schwächen der Hidy-Wallet dokumentiert (siehe Schritt 4, Aktivität 1).

Schritt 4 – Auswertung der benutzerbasierten Evaluationsergebnisse:

Input von Schritt 4 waren die WU-Aufnahmen des Thinking aloud aus Schritt 3.

Schritt 4, Aktivität 1 – Sammlung von Stärken und Schwächen der UX und Informationssicherheit: Der MU, UXE und ISE sichteten die WU-Aufzeichnungen aus Schritt 3. Dabei dokummentierten sie Stärken und Schwächen der UX und Informationssicherheit der Hidy-Wallet. Der Fokus lag dabei auf der Sammlung von Schwächen – Stärken blieben größtenteils unbeachtet. Sowohl die Stärken als auch die Schwächen wurden mithilfe einer standardisierten Vorlage gemäß der MEUSec-Methode festgehalten. Die Vorlage enthielt eine eindeutige ID, einen Namen, eine Beschreibung, ob es sich um eine Stärke oder Schwäche in Bezug auf UX oder Informationssicherheit handelt, die betroffenen Wallet-Funktionen (die in Schritt 1, Aktivität 1 definiert wurden) und die betroffenen Attribute der UX und Informationssicherheit. Gemäß der MEUSec-Methode wurden für die UX die Attribute nach Morville (2005) verwendet, während für die Informationssicherheit die Schutzziele nach DIN EN ISO/IEC 24760-1 (2022) verwendet wurden.

Insgesamt haben der MU, UXE und ISE 32 UX-Schwächen, 9 Informationssicherheit-Schwächen, 5 UX-Stärken und 2 Informationssicherheit-Stärken identifiziert. Alle identifizierten Schwächen und Stärken lassen sich online einsehen[32].

Beispielsweise ist eine identifizierte Informationssicherheit-Schwäche der Hidy-Wallet, dass in der Detailansicht eines VC nicht alle Informationen des VC den WU angezeigt werden. Dies ermöglicht einen unerwünschten Austausch von Informationen zwischen VC-Ausstellern und VC-Prüfern. Dadurch kann die Verfügbarkeit der Wallet beeinträchtigt werden. Tabelle 16 zeigt die genannte Informationssicherheit-Schwäche, die standardisiert mittels der Vorlage dokumentiert wurde.

ID	26
Name	Nicht alle Informationen sind in der Detailansicht der VC einsehbar.
Beschreibung	In der Detailansicht der VC werden nicht alle gespeicherten Informationen angezeigt, was einen unerwünschten Informationsaustausch zwischen VC-Ausstellern und VC-Prüfern ermöglicht.
Stärke/Schwäche	Schwäche
UX/Informationssicherheit	Informationssicherheit
Attribute	Verfügbarkeit
Wallet-Funktionen	Verwaltung von VC

Tabelle 16: Hidy-Wallet – Beispiel einer Informationssicherheit-Schwäche. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

[32] https://doi.org/10.5281/zenodo.13844612

Ein Beispiel einer UX-Schwäche der Hidy-Wallet ist, dass es kein einführendes Tutorial in der Hidy-Wallet gibt, das den WU die grundsätzliche Funktionsweise der Wallet erklärt. Es zeigte sich, dass die anfängliche Benutzung der Hidy-Wallet für WU herausfordernd ist, insbesondere für weniger technikaffine WU. Tabelle 17 zeigt die genannte UX-Schwäche, die standardisiert mittels der Vorlage dokumentiert wurde.

ID	42
Name	Kein einführendes Tutorial verfügbar
Beschreibung	Es gibt kein einführendes Tutorial in der Wallet. Der Einstieg ist daher schwierig, insbesondere für weniger technikaffine WU.
Stärke/Schwäche	Schwäche
UX/Informationssicherheit	UX
Attribute	Usability
Wallet-Funktionen	Allgemeine Bedienfunktionen

Tabelle 17: Hidy-Wallet – Beispiel einer UX-Schwäche. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Schritt 4, Aktivität 2 – Ableitung von Heuristiken der UX und Informationssicherheit: Basierend auf den identifizierten Stärken und Schwächen der Hidy-Wallet leiteten der MU, UXE und ISE Heuristiken der UX und Informationssicherheit ab. Hierfür betrachteten sie die Liste mit Stärken und Schwächen und formulierten Heuristiken mithilfe einer standardisierten Vorlage. Diese besteht aus: ID, Name, Beschreibung, ob sich die Heuristik auf UX oder Informationssicherheit bezieht, Attribute der UX oder Informationssicherheit und betroffene Wallet-Funktionen.

Insgesamt sammelten der MU, UXE und ISE 18 UX-Heuristiken und 9 Informationssicherheit-Heuristiken in Schritt 4, Aktivität 2. Die Heuristiken sind online verfügbar[33].

Beispielsweise wurde eine UX-Heuristik erstellt, dass alle VC eindeutige Namen haben sollten. Zudem sollten die Namen auf allen Wallet-Screens konsistent verwendet werden. Tabelle 18 zeigt die UX-Heuristik, die standardisiert mittels der Vorlage erstellt wurde.

ID	01
Name	Alle VC sollten eindeutige Namen haben
Beschreibung	Die VC sollten eindeutige Namen und Beschreibungen haben. Zudem sollten die Namen auf allen Wallet-Screens konsistent verwendet werden.
UX/Informationssicherheit	UX
Attribute	Usability, Nützlichkeit, Auffindbarkeit, Begehrlichkeit

[33] https://doi.org/10.5281/zenodo.13844612

	und Wert
Wallet-Funktionen	Speicherung von VC, Verwaltung von VC und Teilen von VC

Tabelle 18: Hidy-Wallet – Beispiel einer UX-Heuristik. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Ein Beispiel einer Informationssicherheit-Heuristik ist, dass Sicherheitshinweise hervorgehoben und verständlich sein sollten. Tabelle 19 zeigt die Informationssicherheit-Heuristik, die standardisiert mittels der Vorlage erstellt wurde.

ID	11
Name	Sicherheitshinweise sollten hervorgehoben werden und verständlich sein
Beschreibung	Sicherheitshinweise sollten den WU auffallen und verständlich sein. Eine ausführliche Erläuterung der Risiken sollte vorhanden sein. Dazu sollten nicht nur Texte, sondern auch Symbole verwendet werden. WU sollten sicherheitsrelevante Handlungen ausdrücklich bestätigen und genehmigen müssen.
UX/Informationssicherheit	Informationssicherheit
Attribute	Vertraulichkeit, Authentizität
Wallet-Funktionen	Speicherung von VC, Verwaltung von VC, Teilen von VC und Zahlungsfunktion

Tabelle 19: Hidy-Wallet – Beispiel einer Informationssicherheit-Heuristik. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Schritt 4, Aktivität 3 – Sammlung der abgeleiteten Heuristiken erstellen: Abschließend erstellte der MU eine einheitliche Sammlung der abgeleiteten Heuristiken. Diese Sammlung an Heuristiken wird in den folgenden Schritten wiederverwendet.

Output von Schritt 4 war die Sammlung von abgeleiteten Heuristiken der UX und Informationssicherheit.

Schritt 5 – Vorbereitung der expertenbasierten Evaluation:

Input von Schritt 5 war die Sammlung von abgeleiteten Heuristiken der UX und Informationssicherheit aus Schritt 4.

Schritt 5, Aktivität 1 – Heuristiken aus einer externen Sammlung auswählen und zur eigenen Sammlung an Heuristiken hinzufügen: Der MU, UXE und ISE haben gemeinsam die externen Heuristik-Sammlungen von Nielsen (1994) und Sauer u. a. (2025c) betrach-

tet, um Heuristiken der eigenen Sammlung hinzuzufügen. Die eigene Sammlung wurde durch die folgenden 5 Heuristiken ergänzt:

1. Die Wallet sollte eine Suchfunktion für VC anbieten (UX-Heuristik).
2. Die Wallet sollte mit anderen Systemen interoperabel sein (UX-Heuristik).
3. Es sollte in der Wallet möglich sein, Profile anzulegen und diesen VC zuzuordnen (UX-Heuristik).
4. Daten sollten verschlüsselt und übertragungssicher sein (Informationssicherheit-Heuristik).
5. Die Wallet sollte WU über verfügbare Updates informieren (Informationssicherheit-Heuristik).

Alle Heuristiken lassen sich in Form der standardisierten Vorlage online einsehen[34].

Schritt 5, Aktivität 2 – Literaturrecherche von Stärken, Schwächen und Heuristiken der UX und Informationssicherheit und Aktivität 3 – Ableitung von Heuristiken der UX und Informationssicherheit und Hinzufügen zur eigenen Sammlung: Diese Aktivitäten sind gemäß der MEUSec-Methode optional. Der MU, UXE und ISE beschlossen, keine Literaturrecherche durchzuführen, da jeder definierten Wallet-Funktion aus Schritt 1, Aktivität 1 eine Heuristik in Schritt 5, Aktivität 1 zugeordnet wurde. Mit dieser Entscheidung entfällt auch Schritt 5, Aktivität 3, Heuristiken aus den Ergebnissen der Literaturrecherche abzuleiten und der eigenen Sammlung an Heuristiken hinzuzufügen. Somit wurden diese Aktivitäten nicht evaluiert.

Schritt 5, Aktivität 4 – Aktualisierung sicherheitsrelevanter Softwarekomponenten und potenzieller Angreifer und Aktivität 5 – Aktualisierung des Umfangs der Informationssicherheitsevaluation: Es wurden 2 neue, potenzielle Angreifer identifiziert. Ein Angreifer könnte sich Zugriff auf den Speicher des Geräts verschaffen. Wenn Backups unverschlüsselt sind, könnten sie vom Angreifer direkt ausgelesen werden. Andernfalls könnten beispielsweise schwache Passwörter der Verschlüsselung der Backups ausgenutzt werden. Ein weiterer Angreifer könnte Schwachstellen der allgemeinen Bedienfunktionen (siehe Schritt 1, Aktivität 1) ausnutzen. Beispielsweise könnten unverständliche Elemente des User Interface dazu verleiten, dass VC ungewollt geteilt werden, wodurch Benutzer versehentlich sensible Daten preisgeben könnten.

Schritt 5, Aktivität 6 – Gewichtung der Heuristiken festlegen: Der MU, UXE und ISE haben den Heuristiken Gewichte durch Diskussion zugeordnet. Im Rahmen der Diskussion schlugen der UXE und ISE ein Gewicht für die jeweiligen Heuristiken ihres Fachgebiets vor. Die endgültige Gewichtung nahm der MU unter Abwägung der fachlichen

[34] https://doi.org/10.5281/zenodo.13844612

Einschätzungen der UXE und ISE vor. Die Gewichte liegen zwischen 1 (nicht wichtig) und 5 (sehr wichtig). Die definierten Gewichte wurden in der eigenen Sammlung an Heuristiken festgehalten. Diese ist online verfügbar[35].

Output von Schritt 5 war die Sammlung von gewichteten Heuristiken der UX und Informationssicherheit.

Schritt 6 – Durchführung der expertenbasierten Evaluation:

Input von Schritt 6 war die Sammlung von gewichteten Heuristiken der UX und Informationssicherheit aus Schritt 5.

Schritt 6, Aktivität 1 – Test der definierten Wallet-Funktionen und Aktivität 2 – Festlegung der Erfüllungsgrade je Heuristik: Der UXE und ISE testeten die definierten Wallet-Funktionen aus Schritt 1, Aktivität 1 und legten für jede Heuristik einen Erfüllungsgrad fest. Dazu verwendeten sie eine Skala von 1 (nicht erfüllt) bis 5 (vollständig erfüllt). Die Erfüllungsgrade fügten sie der eigenen Heuristik-Sammlung hinzu. Diese ist online verfügbar[36]. Die Erfüllungsgrade dienen später für die Berechnung der Scores für UX und Informationssicherheit in Schritt 7.

Schritt 6, Aktivität 3 – Erstellung der Interaktionsmatrix der Heuristiken: Der MU hat eine Interaktionsmatrix (siehe Abschnitt 6.1) mit den Heuristiken angelegt, um später in Schritt 6, Aktivität 4 die Interaktionseigenschaften zwischen den Heuristiken zu bewerten. Gemäß der MEUSec-Methode gibt es 3 mögliche Ausprägungen einer Interaktionseigenschaft: komplementär, konkurrierend und neutral. Wenn die Interaktionseigenschaft zwischen Heuristik A und Heuristik B komplementär ist, bedeutet dies, dass sich die Erfüllung von Heuristik A positiv auf die Erfüllung von Heuristik B auswirkt. Wenn die Interaktionseigenschaft zwischen Heuristik A und Heuristik B konkurrierend ist, bedeutet dies, dass die Erfüllung von Heuristik A einen negativen Einfluss auf die Erfüllung von Heuristik B hat. Wenn die Interaktionseigenschaft neutral ist, bedeutet dies, dass die Erfüllung von Heuristik A keinen (nennenswerten) Einfluss auf die Erfüllung von Heuristik B hat. Die Bewertung der Interaktionseigenschaften aller Heuristiken hätte zu viel Zeit in Anspruch genommen. Da Heuristiken sich gegenseitig beeinflussen können, diese Einflüsse jedoch nicht immer in beide Richtungen wirken (Heuristik A kann Heuristik B beeinflussen, aber nicht unbedingt umgekehrt), entstehen zahlreiche Abhängigkeiten. Deshalb wurden nur die Heuristiken mit einem Gewicht von 5 (sehr wichtig) in die Interaktionsmatrix aufgenommen. Dadurch sank die Anzahl der zu berücksichtigenden

[35] https://doi.org/10.5281/zenodo.13844612
[36] https://doi.org/10.5281/zenodo.13844612

Heuristiken von 32 auf 12. Zudem verringerte sich die Anzahl der zu bewertenden Interaktionseigenschaften von 992 auf 132. Gemäß der ersten Version der MEUSec-Methode war die Selektion der Heuristiken für die Erstellung der Interaktionsmatrix nicht vorgesehen. Allerdings zeigte sich durch die Anwendung der MEUSec-Methode, dass eine Selektion bei einer hohen Anzahl an Heuristiken sinnvoll ist.

Schritt 6, Aktivität 4 – Interaktionsmatrix durch Diskussion ausfüllen: Der MU, UXE und ISE legten die Interaktionseigenschaften der Heuristiken (komplementär, konkurrierend und neutral) durch Diskussion fest. Im Rahmen der Diskussion wurden alle Heuristiken paarweise gegenübergestellt, um zu bestimmen, ob zwischen ihnen eine komplementäre, konkurrierende oder neutrale Beeinflussung besteht. Ziel ist es, zu klären, inwiefern sich jeweils 2 Heuristiken gegenseitig beeinflussen. Es wurden keine widersprüchlichen Heuristiken gefunden, weshalb die Interaktionsmatrix nur neutrale und komplementäre Interaktionseigenschaften enthält. Tabelle 20 zeigt beispielhaft einige Heuristiken mit ihren Interaktionseigenschaften. Jede Zeile stellt die Beeinflussung einer Heuristik auf andere Heuristiken dar, während eine Spalte in der Interaktionsmatrix angibt, wie eine Heuristik von anderen beeinflusst wird. Zum Beispiel ist Heuristik 02 komplementär zu Heuristik 11, da eindeutige Namen der VC die Verständlichkeit von Sicherheitshinweisen verbessern. Umgekehrt verhält sich Heuristik 11 neutral zu Heuristik 02, da verständliche Sicherheitshinweise keinen Einfluss auf eindeutige Namen der VC haben.

	02: Eindeutige Namen der VC	11: Verständliche Sicherheitshinweise	29: Interoperabilität
02: Eindeutige Namen der VC	-	komplementär	neutral
11: Verständliche Sicherheitshinweise	neutral	-	komplementär
29: Interoperabilität	neutral	neutral	-

Tabelle 20: Hidy-Wallet – Ausschnitt der Interaktionsmatrix. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Die gesamte Interaktionsmatrix ist online verfügbar[37].

Schritt 6, Aktivität 5 – Hinzufügen der Interaktionseigenschaften zur Heuristik-Sammlung: Der MU hat die Interaktionseigenschaften jeder Heuristik in die Heuristik-Sammlung mitaufgenommen. Die Heuristik-Sammlung ist online verfügbar[38]. Die Interaktionseigenschaften werden später für die Formulierung der Verbesserungsvorschläge in Schritt 8 verwendet.

[37] https://doi.org/10.5281/zenodo.13844612
[38] https://doi.org/10.5281/zenodo.13844612

Output von Schritt 6 war einerseits die Interaktionsmatrix mit den Interaktionseigenschaften der Heuristiken und andererseits die Heuristik-Sammlung mit den Erfüllungsgraden der Heuristiken.

Schritt 7 – Auswertung und Validierung der expertenbasierten Evaluationsergebnisse:

Input von Schritt 7 war die Heuristik-Sammlung mit den Erfüllungsgraden der Heuristiken aus Schritt 6.

Schritt 7, Aktivität 1 – Aggregation der Heuristik-Scores auf Ebene der UX- und Informationssicherheit-Attribute: Zunächst bestimmte der MU den Einzelscore aller Heuristiken. Der Einzelscore einer Heuristik ist das Produkt aus dem Gewicht und dem Erfüllungsgrad einer Heuristik. Der MU bestimmte dann den Gesamtscore (GS) pro Attribut der UX und Informationssicherheit. Der GS eines Attributs ist die Summe der Einzelscores aller Heuristiken, die diesem Attribut zugeordnet sind. Die GS der UX-Attribute sind in der ersten Zeile von Tabelle 21 dargestellt. Die GS der Informationssicherheit-Attribute sind in der ersten Zeile von Tabelle 22 dargestellt. Um den durchschnittlichen Gesamtscore (ØGE) eines UX- und Informationssicherheit-Attributs zu ermitteln, wurde der Gesamtscore (GS) durch die Anzahl der zugehörigen Heuristiken geteilt. Die ØGE sind in der zweiten Zeile von Tabelle 21 und Tabelle 22 zu finden. Der maximal mögliche Gesamtscore (MGS) eines Attributs ergibt sich aus dem Produkt des Gewichts und dem maximalen Erfüllungsgrad (siehe dritte Zeile von Tabelle 21 und Tabelle 22). Um den durchschnittlichen maximal möglichen Gesamtscore (ØMGS) eines Attributs zu berechnen, wurde der MGS durch die Anzahl der zugehörigen Heuristiken geteilt (siehe vierte Zeile von Tabelle 21 und Tabelle 22). Dann wurde das Verhältnis (Ratio) zwischen dem ØGE und dem ØMGE berechnet. Dieses Verhältnis gibt an, inwieweit ein UX- oder Informationssicherheit-Attribut erfüllt ist – von 0 (nicht erfüllt) bis 1 (vollständig erfüllt). Die Werte der Verhältnisse sind in der fünften Zeile von Tabelle 21 und Tabelle 22 einsehbar.

	UX						
	Nützlichkeit	Begehrlichkeit	Auffindbarkeit	Usability	Barrierefreiheit	Glaubwürdigkeit	Wert
GS	72	40	116	212	49	19	78
ØGE	9	6,67	10,55	10,6	9,8	6,33	9,75
MGS	150	100	200	375	90	55	155
ØMGS	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

Tabelle 21: Hidy-Wallet – Scores der UX-Attribute. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

	Informationssicherheit				
	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Zuverlässigkeit
GS	62	5	33	60	12
ØGE	12,4	5	8,25	15	12
MGS	115	25	90	100	20
ØMGS	23	25	22,5	25	20
Ratio	0,54	0,2	0,37	0,6	0,6

Tabelle 22: Hidy-Wallet – Scores der Informationssicherheit-Attribute. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Schritt 7, Aktivität 2 – Aggregation der Heuristik-Scores auf Ebene von UX und Informationssicherheit: Da für jedes Attribut der UX und Informationssicherheit ein Score in Schritt 7, Aktivität 1 berechnet wurde, war es möglich, einen Score für die UX und Informationssicherheit zu berechnen. Um den Score für die UX zu berechnen, wurde zunächst der Durchschnitt aller MGS der UX-Attribute berechnet (= 8,96). Anschließend wurde der Durchschnitt aller ØMGS der UX-Attribute berechnet (= 18,29). Danach wurde das Verhältnis beider Werte bestimmt (= 0,49), was den Score der UX ergibt. Gleichermaßen wurde bei der Berechnung des Informationssicherheit-Score vorgegangen. Zunächst wurde der Durchschnitt aller MGS der Informationssicherheit-Attribute berechnet (= 10,53). Anschließend wurde der Durchschnitt aller ØMGS der Informationssicherheit-Attribute berechnet (= 23,10). Schließlich wurde das Verhältnis beider Werte bestimmt (= 0,46), was den Score der Informationssicherheit ergibt. Die berechneten Scores der UX und Informationssicherheit können in einer weiteren Anwendung der MEUSec-Methode verwendet werden, um zu überprüfen, ob die Verbesserungsvorschläge aus Schritt 8 zu einer messbaren Verbesserung geführt haben.

Schritt 7, Aktivität 3 – Feedback-Diskussion und Aktivität 4 – Anpassung der Heuristiken: Im Rahmen der Feedback-Diskussion diskutierten der MU, UXE und ISE, ob Probleme mit Heuristiken bei der Festlegung der Erfüllungsgrade der Heuristiken aufgetreten sind. Es sind keine Probleme aufgetreten. So konnte Aktivität 4 – die Anpassung der Heuristiken – übersprungen werden. Diese Aktivität wurde daher nicht evaluiert.

Schritt 7, Aktivität 5 – Eigene Sammlung der Heuristiken zu externer Sammlung der Heuristiken hinzufügen: Grundsätzlich war diese Aktivität für die Anwendung der MEUSec-Methode mithilfe des Software-Tools angedacht (siehe Kapitel 9). Das Software-Tool kann genutzt werden, um die Liste der Heuristiken mit anderen MU, UXE und ISE zu teilen. Da das Software-Tool in der ersten Evaluation nicht verwendet wurde,

wird Aktivität 5 mit der Veröffentlichung der Heuristik-Sammlung[39] als abgeschlossen betrachtet.

Output von Schritt 7 waren die Scores der UX und Informationssicherheit.

Schritt 8 – Verbesserung von UX und Informationssicherheit:

Input von Schritt 8 war die Interaktionsmatrix aus Schritt 6. Die Interaktionsmatrix wurde genutzt, um Verbesserungsvorschläge zu sammeln, da für jede Interaktionseigenschaft der einzelnen Heuristiken ein unterschiedlicher Ansatz erforderlich ist. Bei konkurrierenden Heuristiken muss zunächst geprüft werden, ob eine Lösung für den Konflikt gefunden werden kann. Ist dies nicht möglich, muss entweder die UX oder die Informationssicherheit priorisiert werden. Je nach Priorisierung dient entweder die UX-Heuristik oder die Informationssicherheit-Heuristik als Verbesserungsvorschlag. Neutrale und komplementäre Heuristiken können direkt als Verbesserungsvorschläge verwendet werden, da sie sich nicht negativ beeinflussen.

Schritt 8, Aktivität 1 – Lösungen für konkurrierende Heuristiken finden und Aktivität 2 – UX oder Informationssicherheit priorisieren: Da mithilfe der Interaktionsmatrix keine konkurrierenden Heuristiken ermittelt wurden, konnten Aktivität 1 und Aktivität 2 übersprungen werden. Diese Aktivitäten wurden somit nicht evaluiert.

Schritt 8, Aktivität 3 – Verbesserungsvorschläge auf Basis der komplementären und neutralen Heuristiken formulieren: Da sich komplementäre und neutrale Heuristiken nicht negativ beeinflussen, konnten diese unmittelbar als Verbesserungsvorschläge verwendet werden. Insgesamt wurden 26 Verbesserungsvorschläge in standardisierter Form dokumentiert: ID, Beschreibung und zugehörige Heuristiken. Tabelle 23 zeigt beispielhaft einige der dokumentierten Verbesserungsvorschläge.

Alle 26 Verbesserungsvorschläge sind online einsehbar[40].

ID	Beschreibung	Zugehörige Heuristiken
1	VC sollten aussagekräftige Namen und Beschreibungen haben. Außerdem sollten die Namen und Beschreibungen in der gesamten Wallet konsistent verwendet werden.	01, 02
3	Funktionsnamen sollten konsistent und verständlich sein.	05

[39] https://doi.org/10.5281/zenodo.13844612
[40] https://doi.org/10.5281/zenodo.13844612

9	Sicherheitshinweise sollten den WU auffallen und verständlich sein. Eine ausführliche Erläuterung der Risiken sollte vorhanden sein. Dazu sollten nicht nur Text, sondern auch Symbole verwendet werden. WU sollten sicherheitsrelevante Handlungen ausdrücklich bestätigen und genehmigen müssen. Die Warnung „Anonymer Aussteller“ muss hervorgehoben werden. Das Symbol im Warnhinweis muss ersetzt werden, da „X“ mit „Schließen“ verwechselt werden könnte.	11
14	WU sollten auf die Notwendigkeit von Datensicherungen hingewiesen werden, um den Verlust von VC zu verhindern. Die Wallet sollte eine Sicherungs- und eine Wiederherstellungsfunktion besitzen.	17
20	Sensible Funktionen und Daten sollten nur nach erfolgreicher Authentifizierung zugänglich sein. WU sollten sich nach erneutem Öffnen der App oder beim Teilen und Empfangen von VC erneut authentisieren müssen.	24
22	Die Wallet sollte verschiedene Sprachen anbieten. Außerdem sollte die Wallet „einfache Sprache“ verwenden.	26
23	Die Wallet sollte über eine Such-, Sortier- und Filterfunktion verfügen.	28
25	Es sollte möglich sein, verschiedene WU-Profile zu erstellen, zu bearbeiten, zu gruppieren und zu löschen. Es sollte möglich sein, verschiedene VC in verschiedenen WU-Profilen zu verwalten.	30
26	Sicherheitsupdates sollten automatisch installiert werden. Wenn ein Sicherheitsupdate nicht installiert werden konnte, sollte die Wallet die WU darüber informieren.	32

Tabelle 23: Hidy-Wallet – Ausschnitt der Verbesserungsvorschläge. (Sauer u. a., 2025a). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Output von Schritt 8 waren Verbesserungsvorschläge der UX und Informationssicherheit für die Hidy-Wallet.

7.3 Einordnung der Stärken und Schwächen der Hidy-Wallet

Im Folgenden werden die Evaluationsergebnisse der Hidy-Wallet mit Evaluationsergebnissen anderer Wallets aus der Literatur verglichen. Da der Schwerpunkt der Evaluation der Hidy-Wallet auf der Identifikation von Schwächen lag, wurden vor allem Schwächen dokumentiert, während Stärken weitgehend unberücksichtigt blieben.

Sartor u. a. (2022) zeigen, dass die Terminologie der von ihnen untersuchten Wallet zu technisch ist und von Probanden nicht verstanden wird. Diese Schwäche steht im Zusammenhang mit der Design Guideline „Use of understandable terms“ von Sellung & Kubach (2023). Diese Schwäche wurde auch bei der Durchführung der MEUSec-Methode auf die Hidy-Wallet identifiziert. Beispielsweise haben Probanden nicht verstanden, was mit dem Begriff „Credential“ gemeint ist. Dieses mangelnde Verständnis kann zu weiteren Problemen führen. Zum Beispiel könnten Sicherheitsmechanismen falsch verwendet werden. Darüber hinaus stellt die technische Terminologie eine Barriere für weniger technikaffine Benutzer dar, was die Zugänglichkeit einschränkt.

Des Weiteren verdeutlichen Khayretdinova u. a. (2022), dass Probanden aufgrund der Komplexität der untersuchten Wallet und ihres mangelnden intuitiven Designs Schwierigkeiten bei der Einrichtung und der Verwaltung von VC haben. Sauer u. a. (2025b) und Korir u. a. (2022) zeigen, dass die grundlegende Funktionalität von Wallets oft nicht verstanden wird. Diese Schwäche steht im Zusammenhang mit der Design Guideline „User Onboarding“ von Sellung & Kubach (2023). Durch die Anwendung der MEUSec-Methode auf die Hidy-Wallet wurde festgestellt, dass ein einführendes Tutorial integriert werden sollte, um Benutzern die grundlegende Funktionalität von Wallets zu erklären.

Im Rahmen der Untersuchung von Sauer u. a. (2025b) äußern die Probanden den Wunsch nach mehr Hilfshinweisen in der evaluierten Wallet. Diese Schwäche steht im Zusammenhang mit der Design Guideline „Help & feedback“ von Sellung & Kubach (2023). Auch im Rahmen der Evaluation der Hidy-Wallet zeigte sich, dass Hilfshinweise fehlen. Beispielsweise gibt es keine Erklärungen zum Begriff „App Link“, sodass Probanden nicht verstanden, was mit dem Begriff gemeint ist.

Des Weiteren weisen Sauer u. a. (2025b) darauf hin, dass Informationen in einem VC versteckt sein können, die Benutzern im User Interface nicht angezeigt werden. Auch in der Hidy-Wallet wurden nicht alle im VC gespeicherten Information angezeigt.

Satybaldy (2023) zeigen, dass Fehlermeldungen der evaluierten Wallet durch Probanden nicht verstanden werden. Diese Schwäche steht im Zusammenhang mit der Design Guideline „Error handling“ von Sellung & Kubach (2023). Auch bei der Benutzung der Hidy-Wallet erschienen Fehlermeldungen, die nicht verstanden wurden. Beispielsweise gab die Fehlermeldung „Erstellung fehlgeschlagen“ keinen Hinweis darauf, dass das Problem durch eine fehlende Internetverbindung verursacht wurde. Eine weitere unklare Fehlermeldung „Senden fehlgeschlagen“ erschien nach einem Kauf im Demo-Shop.

Weitere Stärken und Schwächen, die bei der Evaluation der Hidy-Wallet identifiziert wurden, konnten in der Literatur nicht gefunden werden. Allerdings gibt es noch weitere Stärken und Schwächen der Hidy-Wallet, die in Zusammenhang mit den Design Guidelines von Sellung & Kubach (2023) stehen. Diese werden im Folgenden beschrieben.

Die unterschiedlichen Benennungen von Buttons und die unterschiedlichen Währungen im Demo-Shop im Vergleich zu Währungen in weiteren Abschnitten der Hidy-Wallet entsprechen nicht der Design Guideline „Use of consistent terms“ von Sellung & Kubach (2023).

Überlappende Erfolgsmeldungen und Pop-Ups der Hidy-Wallet sind aufgrund ihrer Ähnlichkeit schwer zu unterscheiden und widersprechen der Design Guideline „Simplicity of Use“ von Sellung & Kubach (2023).

VC, die in der Hidy-Wallet gespeichert sind, besitzen keine Namen und keine Beschreibungen. Daher können VC nur anhand ihrer Bilder unterschieden werden. Diese Schwäche widerspricht der Design Guideline „Placement of information“ von Sellung & Kubach (2023).

In der Hidy-Wallet fehlen „Zurück“-Buttons. Zudem lässt sich das erscheinende Tastaturfeld des Smartphones an manchen Stellen nicht schließen. Daher wird die Design Guideline „Operability“ von Sellung & Kubach (2023) nicht vollständig erfüllt.

Die Startseite der Hidy-Wallet entspricht nicht den Erwartungen der Benutzer und die Interaktionsmuster im Demo-Shop weichen von denen der anderen Wallet-Funktionen ab. Es wurde keine Quittung per E-Mail nach Kauf eines Tickets versendet, das Ticket ist nicht erstattbar und das VC des Tickets lässt sich nach Löschung nicht wiederherstellen. Dies widerspricht der Design Guideline „Familiarity and Relatability“ von Sellung & Kubach (2023).

Eine Stärke der Hidy-Wallet ist, dass der Kontostand nicht direkt angezeigt wird. Allerdings kann die Kaufhistorie direkt eingesehen werden, was ebenfalls standardmäßig verborgen sein sollte. Dies widerspricht der Design Guideline „Properly securing the wallet and functions“ von Sellung & Kubach (2023), da alle sensiblen Daten geschützt werden sollten.

Die Startseite der Hidy-Wallet wird als übersichtlich wahrgenommen, was mit der Design Guideline „Minimalistic and simple design“ von Sellung & Kubach (2023) in Verbindung steht. Allerdings gibt es Ladeanzeigen, die nicht als solche erkennbar sind, da die Ladeanzeigen kaum sichtbar sind. Dies verwirrt Benutzer und unterbricht die Fokussierung auf relevante Funktionen.

Neben den in der Literatur identifizierten Stärken und Schwächen von Wallets sowie den Stärken und Schwächen der Hidy-Wallet, die unmittelbar in Bezug zu den Design Guidelines von Sellung & Kubach (2023) stehen, wurden zusätzliche Stärken und Schwächen der Hidy-Wallet festgestellt. Diese werden im Folgenden beschrieben.

Eine Schwäche der Hidy-Wallet ist, dass den Probanden nicht klar kommuniziert wird, dass die Hidy-Wallet neben den grundlegenden Wallet-Funktionen (siehe Abschnitt 2.4) zusätzliche Funktionen bietet, wie beispielsweise den integrierten Demo-Shop. Infolgedessen versuchten Probanden fälschlicherweise den Demo-Shop aus dem App-Store herunterzuladen, da sie annahmen, es handelte sich um eine separate Anwendung.

Eine weitere Schwäche der Hidy-Wallet ist, dass die Hidy-Wallet derzeit nur die deutsche Sprache anbietet. Daher hatten einige Probanden Schwierigkeiten bei der Benutzung der Hidy-Wallet, da sie die deutsche Sprache nicht ausreichend verstanden.

Eine Stärke der Hidy-Wallet ist, dass die Probanden die Hidy-Wallet allein aufgrund ihres Namens problemlos auf der Startseite des Smartphones gefunden haben.

7.4 Evaluationsergebnisse der MEUSec-Methode

Die Evaluation der MEUSec-Methode erfolgte mittels der beschriebenen Vorgehensweise aus Abschnitt 7.1. Im Folgenden werden die Evaluationsergebnisse der MEUSec-Methode je Evaluationskriterium aus Abschnitt 7.1 beschrieben.

(E1) Qualität der Methodenartefakte:

(E1.1) Vollständigkeit:

- Jeder festgelegten Wallet-Funktion konnte mindestens eine UX-Heuristik und mindestens eine Informationssicherheit-Heuristik zugeordnet werden. Außerdem konnte für jede UX-Heuristik und für jede Informationssicherheit-Heuristik ein Erfüllungsgrad festgelegt werden.
- Aufgrund der hohen Anzahl an erstellten Heuristiken und der begrenzten Ressourcen wurde die Interaktionsmatrix nicht mit allen Heuristiken erstellt. Die Interaktionsmatrix wurde lediglich für diejenigen Heuristiken erstellt, denen die höchste Priorität zugeordnet wurde. Für diese Heuristiken konnten in der Interaktionsmatrix alle Interaktionseigenschaften festgelegt werden. Jedoch gehen der Methoden-Anwender (MU), der UX-Experte (UXE) und der Informationssicherheit-Experte (ISE) davon aus, dass die Festlegung der Interaktionseigenschaften auch für die restlichen, nicht betrachteten Heuristiken möglich gewesen wäre.
- Für jede nicht vollständig erfüllte Heuristik konnte mindestens ein Verbesserungsvorschlag gefunden werden. Für die Festlegung der Verbesserungsvorschläge konnten die Interaktionseigenschaften aus der Interaktionsmatrix verwendet werden.
- Insgesamt bewerteten der MU, UXE und ISE das Evaluationskriterium der Vollständigkeit als erfüllt.

(E1.2) Konsistenz:

- Während der Durchführung der MEUSec-Methode wurden keine widersprüchlichen Verbesserungsvorschläge der Hidy-Wallet identifiziert.
- Eine Schwäche der MEUSec-Methode, die der MU, ISE und UXE bei der Anwendung der MEUSec-Methode identifizierten, war das Fehlen einer Vergleichsbasis, die als Grundlage für die Festlegung von Erfüllungsgrade der Heuristiken dient. Bei einer erneuten Durchsicht der Erfüllungsgrade der Heuristiken, nachdem die einzelnen Erfüllungsgrade der Heuristiken festgelegt wurden, änderte sich die Einschätzung häufig, da die Erfüllungsgrade der Heuristiken miteinander in Relation gesetzt werden mussten.
- Des Weiteren betrafen einige identifizierte Schwächen der Hidy-Wallet nur bestimmte Benutzergruppen. Die MEUSec-Methode sollte die Dokumentation davon miteinschließen.
- Insgesamt bewerteten der MU, UXE und ISE das Evaluationskriterium der Konsistenz als teilweise erfüllt.

(E1.3) Korrektheit:

- Insgesamt bewerteten der MU, UXE und ISE die Artefakte der MEUSec-Methode – wie beispielsweise die definierten Heuristiken mit deren Erfüllungsgraden, die Scores der UX und Informationssicherheit, die Interaktionseigenschaften und abschließenden Verbesserungsvorschläge – als plausibel und damit das Evaluationskriterium der Korrektheit als erfüllt.
- Weitere Aussagen zur Korrektheit konnten nicht getroffen werden, da die MEUSec-Methode nur einmal auf die Hidy-Wallet angewendet wurde. Bei einer weiteren Anwendung der MEUSec-Methode auf eine neue Version der Hidy-Wallet müsste anhand der Scores der UX und Informationssicherheit überprüft werden, ob die identifizierten Verbesserungsvorschläge zu einer messbaren Verbesserung der Hidy-Wallet geführt haben.

(E1.4) Nachvollziehbarkeit:

- Die Gewichtung und die Festlegung von Erfüllungsgraden der Heuristiken, die Definition der Interaktionseigenschaften und die Formulierung der Verbesserungsvorschläge erfolgte unmittelbar durch den MU, UXE und ISE. Wenn es dabei Unklarheiten gab, konnten die Unklarheiten durch einen Austausch zwischen dem MU, UXE und ISE gelöst werden.
- Insgesamt bewerteten der MU, UXE und ISE das Evaluationskriterium der Nachvollziehbarkeit als erfüllt.

(E1.5) Eindeutigkeit:

- Der MU, UXE und ISE bewerteten die Heuristiken, deren jeweiligen Gewichte, deren Erfüllungsgrade und deren Interaktionseigenschaften als klar formuliert.
- Die Formulierung der Heuristiken erfolgte durch die Durchführenden der Rollen selbst. Wenn Heuristiken aus der externen Heuristik-Sammlung stammen, die von anderen Personen erstellt wurde, besteht das Risiko, dass Heuristiken nicht klar formuliert sind. Eine Möglichkeit der Bewertung der externen Heuristik-Sammlung könnte dieses Risiko verringern.
- Des Weiteren hatten der MU, UXE und ISE Schwierigkeiten, sicherheitsrelevante Softwarekomponenten und potenzielle Angreifer ohne tiefergehendes Wissen über die Hidy-Wallet zu definieren.
- Zudem war dem MU anfangs nicht bewusst, dass die Interaktionseigenschaften in der Interaktionsmatrix asymmetrisch definiert werden sollen. Beispielsweise wurde zunächst nur die Interaktionseigenschaft von Heuristik A zu Heuristik B berücksichtigt, während die umgekehrte Interaktionseigenschaft von Heuristik B zu Heuristik A nicht definiert wurde. Im weiteren Verlauf der Erstellung der Interaktionsmatrix wurde dieser Fehler korrigiert, sodass die Interaktionseigenschaften für beide Richtungen zwischen den Heuristiken definiert wurden.
- Darüber hinaus war die Bedeutung der berechneten Scores der UX und Informationssicherheit für den MU unklar.
- Zudem fehlte eine klarere Beschreibung der Vorgehensweise zur Berechnung der Scores. Im Laufe der Anwendung der MEUSec-Methode erkannten der ISE und UXE jedoch, dass die Scores verwendet werden können, um zu prüfen, inwiefern die identifizierten Verbesserungsvorschläge in einer weiteren Anwendung der MEUSec-Methode zu messbaren Verbesserungen der Hidy-Wallet geführt haben.
- Insgesamt bewerteten der MU, UXE und ISE das Evaluationskriterium der Eindeutigkeit als teilweise erfüllt.

(E1.6) Sachdienlichkeit:

- Der MU, UXE und ISE bewerteten die Scores der UX und Informationssicherheit als sachdienlich, da die Scores bei weiteren Anwendungen der MEUSec-Methode verwendet werden können, um zu prüfen, ob identifizierte Verbesserungsvorschläge zu messbaren Verbesserungen der Hidy-Wallet geführt haben.
- Außerdem bewerteten der MU, UXE und ISE die identifizierten Interaktionseigenschaften der Heuristiken als relevant, da diese verwendet wurden, um Verbesserungsvorschläge der Hidy-Wallet zu identifizieren.
- Zudem bewerteten der MU, UXE und ISE die identifizierten Verbesserungsvorschläge der Hidy-Wallet als relevant, da diese gezielt die identifizierten Schwächen der Hidy-Wallet aus der experten- und benutzerbasierten Evaluation adressieren.

- Insgesamt bewerteten der MU, UXE und ISE das Evaluationskriterium der Sachdienlichkeit als erfüllt.

(E2) Durchführbarkeit der Methode:

(E2.1) Effektivität:

- Der MU, UXE und ISE verglichen die angestrebten Artefakte mit den gewonnenen Artefakten der MEUSec-Methode.
- Insgesamt wurden 41 Schwächen und 7 Stärken der UX und Informationssicherheit der Hidy-Wallet, 32 Heuristiken und 26 Verbesserungsvorschläge der Hidy-Wallet identifiziert.
- Die Evaluation involvierte sowohl Experten als auch Probanden.
- Für die Heuristiken konnten Erfüllungsgrade festgelegt werden, um schlussendlich einen Score für die UX und einen Score für die Informationssicherheit der Hidy-Wallet zu berechnen.
- Mithilfe der Interaktionsmatrix konnten Interaktionseigenschaften zwischen Heuristiken definiert werden.
- Mittels den Interaktionseigenschaften der Heuristiken konnten Verbesserungsvorschläge der Hidy-Wallet identifiziert werden.
- Dies bedeutet, dass alle angestrebten Artefakte gewonnen wurden. Der MU, UXE und ISE bewerteten das Evaluationskriterium der Effektivität als erfüllt.

(E2.2) Effizienz:

- Um die Effizienz zu bewerten, wurden zunächst die Zeiten für jeden Schritt der MEUSec-Methode und für jeden Durchführenden einer Rolle gemessen. Der MU benötigte insgesamt 1206 Minuten (20,1 Stunden), der UXE benötigte insgesamt 1365 Minuten (22,75 Stunden) und der ISE benötigte insgesamt 1265 Minuten (21,08 Stunden). Die Summe der Zeiten aller Rollen beträgt 3836 Minuten (63,93 Stunden). Die Gesamtdurchführungszeit der MEUSec-Methode (Rollen sind parallel an Schritten beteiligt) beträgt 1576 Minuten (26,27 Stunden). Außerdem waren WU in der benutzerbasierten Evaluation beteiligt. Aufsummiert waren die WU 150 Minuten (2,5 Stunden) involviert. Bei diesen Messungen wurden nur die Zeiten gemessen, die für die Durchführung der Schritte der MEUSec-Methode benötigt wurden. Der zusätzliche Zeitaufwand für die Schulung der Mitarbeiter hinsichtlich der Anwendung der MEUSec-Methode und die Umsetzung der identifizierten Verbesserungsvorschläge wurde nicht berücksichtigt. In Tabelle 24 sind die einzelnen Zeiten aufgeführt. Dabei steht „S“ für „Schritt“ der MEUSec-Methode. Die Tabellenzeile „Max(S[x])“ beinhaltet die Zeiten jedes Schritts der MEUSec-Methode, wobei parallele Ausführungen von Schritten durch verschiedene Rollen berücksichtigt werden.

Die Tabellenzeile „Total“ hingegen summiert die Zeiten der Rollen, ohne parallele Ausführungen von Schritten zu beachten.

	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**Total**
MU	75	122	170	555	158	25	46	55	1206
UXE	-	42	155	555	158	395	5	55	1365
ISE	55	42	-	555	158	395	5	55	1265
Max(S[x])	75	122	170	555	158	395	46	55	**1576**
Total	130	206	325	1665	474	815	56	165	**3836**

Tabelle 24: Hidy-Wallet – Ausführungszeiten der MEUSec-Methode. (Sauer u. a., 2025a).

- Zusätzlich zu den benötigen Zeiten wurden die Kosten berechnet. Für den UXE wurde ein Stundensatz in Höhe von 83€ pro Stunde (für einen UX-Designer), für den ISE ein Stundensatz in Höhe von 101€ pro Stunde (für einen Security-Consultant) und für den MU ein Stundensatz in Höhe von 95€ pro Stunde (für einen IT-Consultant) angesetzt[41]. Pro WU wurden 20€ berechnet, da jeder WU in der benutzerbasierten Evaluation 20€ erhalten hat. So ergaben sich Kosten in Höhe von 1.888,25€ für den UXE, 2.129,08€ für den ISE, 1.909,50€ für den MU und 200€ für die WU. Insgesamt ergaben sich daraus Kosten in Höhe von 6.126,83€.
- Nach Betrachtung der gemessenen Zeiten und berechneten Kosten sollte eine Bewertung der Effizienz mithilfe der Ausprägungen „erfüllt“, „teilweise erfüllt“ und „nicht erfüllt“ vorgenommen werden. Da kein anderes Verfahren als die MEUSec-Methode zur experten- als auch endnutzerbasierten Evaluation der Beeinflussung zwischen UX und Informationssicherheit identifiziert werden konnte (siehe Abschnitt 5.2.14), erfolgte ein subjektiver Vergleich auf Grundlage der Erfahrungswerte des UXE und ISE mit den recherchierten, ähnlichen Evaluationsverfahren (siehe Abschnitt 5.2). Auf Basis dieses Vergleichs bewerteten der UXE und ISE das Evaluationskriterium der Effizienz als erfüllt.
- Mit der MEUSec-Methode konnten Evaluationsergebnisse und Verbesserungsvorschläge durch Experten der UX und Informationssicherheit sowie durch Endnutzer gewonnen werden.
- Die identifizierten Heuristiken können in weiteren Anwendungen der MEUSec-Methode wiederverwendet werden.
- Ferner erwähnten der MU, UXE und ISE, dass die Effizienz der MEUSec-Methode weiter verbessert werden könnte, wenn weitere standardisierte Vorlagen vorgegeben werden. Beispielsweise sollte eine standardisierte Vorlage für die Formulierung von sicherheitsrelevanten Softwarekomponenten und potenziellen Angreifern existieren.

[41] Es handelt sich um durchschnittliche Stundensätze von https://freelancermap.de.

(E2.3) Akzeptanz:

- Insgesamt bewerteten der MU, UXE und ISE das Evaluationskriterium der Akzeptanz als erfüllt, weil sich die MEUSec-Methode für sie als effektiv und effizient erwiesen hat.
- Einzelne Schwachstellen wurden bereits bei den Evaluationsergebnissen der vorangegangenen Evaluationskriterien erläutert.
- Darüber hinaus äußerten der MU, UXE und ISE, dass Schritte der MEUSec-Methode durch ein Software-Tool effizienter durchgeführt werden könnten. Beispielsweise könnte die Interaktionsmatrix mit den Heuristiken automatisiert angelegt werden. Zudem könnte die Berechnung der Scores von UX und Informationssicherheit auf Basis der Erfüllungsgrade automatisiert durch ein Software-Tool erfolgen. Des Weiteren könnten konkurrierende Heuristiken automatisiert hervorgehoben werden, sodass die Formulierung der Verbesserungsvorschläge effizienter erfolgen kann.

Aus den Evaluationsergebnissen der MEUSec-Methode ergaben sich unterschiedliche Verbesserungsvorschläge, die im Folgenden erläutert werden.

1. Die MEUSec-Methode sollte eine Vorauswahl an Angreifermodellen anbieten, die vom ISE adaptiert werden kann.
2. Die MEUSec-Methode sollte eine Vorauswahl an relevanten Eigenschaften der WU für die Akquise der WU anbieten.
3. Die MEUSec-Methode sollte es ermöglichen, dass die Anleitung für das Thinking aloud nach der Einrichtung der Endgeräte angepasst werden kann.
4. Die MEUSec-Methode sollte vorgeben, dass alle Heuristiken nach ihrer Erstellung nochmals im Gesamtzusammenhang geprüft werden, um inhaltliche Überschneidungen zu identifizieren und bei Bedarf Heuristiken zu überarbeiten.
5. Eine hohe Anzahl an Heuristiken erhöht den Zeitaufwand der Durchführung der MEUSec-Methode, da zwischen Heuristiken jeweils Interaktionseigenschaften in der Interaktionsmatrix definiert werden sollen. Die MEUSec-Methode sollte es ermöglich, Heuristiken für die Definition der Interaktionseigenschaften zu filtern. Beispielsweise könnten nur Heuristiken mit einem niedrigen Erfüllungsgrad oder einer hohen Priorität berücksichtigt werden.
6. Die MEUSec-Methode sollte eine weitere Bewertung von Erfüllungsgraden der Heuristiken ermöglichen, nachdem in der ersten Iteration für jede Heuristik ein Erfüllungsgrad festgelegt wurde.
7. Die MEUSec-Methode sollte weitere standardisierte Vorlagen anbieten, wie beispielsweise um sicherheitsrelevante Softwarekomponenten und potenzielle Angreifer zu definieren sowie die Scores von UX und Informationssicherheit automatisiert zu berechnen.

8. Die MEUSec-Methode sollte die Möglichkeit bieten, den Verbesserungsvorschlägen Begründungen zuzuordnen, insbesondere um die Entscheidungsgründe für Priorisierungen von konkurrierenden Heuristiken zu dokumentieren.
9. Die MEUSec-Methode sollte so angepasst werden, dass nach der Festlegung von Erfüllungsgraden der Heuristiken unmittelbar die Feedback-Diskussion erfolgt. Dadurch können auftretende Probleme mit den Heuristiken unmittelbar behoben werden. Außerdem sollten die Feedback-Diskussion und die Anpassung der Heuristiken zusammengelegt werden, da während der Feedback-Diskussion nur aufgetretene Probleme hinsichtlich der Heuristiken gesammelt werden müssen, wodurch diese Diskussion keine eigene Aktivität erfordert.
10. Die Aktivitäten „Testen der Wallet-Funktionen“ und „Bewertung der Heuristiken“ der MEUSec-Methode sollten zu einer Aktivität vereint werden. So werden die Erfüllungsgrade der Heuristiken während des Testens der Wallet-Funktionen festgelegt, damit keine relevanten Aspekte vergessen werden.
11. Die Skala der Erfüllungsgrade von Heuristiken sollte von 1-5 auf 0-4 angepasst werden, damit die Scores für UX und Informationssicherheit im Bereich von 0 bis 1 liegen, anstatt zwischen 0,2 und 1.
12. Es sollte ein Änderungsprotokoll für die Methodenartefakte eingeführt werden, um sicherzustellen, dass Änderungen dokumentiert werden.

7.5 Limitationen

Im Folgenden werden die Limitationen der Evaluation der Hidy-Wallet und der MEUSec-Methode beschrieben.

Die Evaluation der Hidy-Wallet beschränkt sich ausschließlich auf die iOS-Version. Versionen der Hidy-Wallet für andere Betriebssysteme, wie Android, wurden nicht evaluiert und könnten spezifische Abweichungen in Funktion und Interaktion aufweisen.

Des Weiteren wurde das Thinking aloud in einer Labor-Situation durchgeführt. Diese kontrollierte Umgebung könnte zu einem Verhalten der WU geführt haben, das vom alltäglichen Gebrauch abweicht. Zusätzlich könnten die WU durch die Anwesenheit von Beobachtern in ihrer natürlichen Interaktion mit der Hidy-Wallet beeinflusst worden sein.

Zudem wurden keine personenbezogenen Daten der WU in der Hidy-Wallet verarbeitet, sondern ausschließlich Beispieldaten. Dadurch konnten potenzielle Effekte, die sich aus der Verarbeitung realer sensibler Daten ergeben, nicht evaluiert werden. Dies betrifft beispielsweise die Evaluation des Vertrauens in die Hidy-Wallet als auch die wahrgenommene Sicherheit.

Das UX-Attribut Barrierefreiheit kann nicht als ausreichend evaluiert betrachtet werden, da in der benutzerbasierten Evaluation nicht ausreichend Probanden mit unterschiedlichen Einschränkungen, wie beispielsweise einer Rot-Grün-Schwäche und Blindheit, involviert waren.

Nun werden die Limitationen der Evaluation der MEUSec-Methode erläutert.

Es wurden nur Heuristiken der UX und Informationssicherheit identifiziert, die entweder komplementär oder neutral zueinander sind, jedoch nicht in konkurrierender Beziehung zueinanderstehen. Dadurch wurden die Aktivitäten, Konfliktlösungen zu identifizieren und UX oder Informationssicherheit zu priorisieren, in Schritt 8 übersprungen und somit nicht evaluiert.

Um die Effektivität ausführlicher zu bewerten, wäre es notwendig gewesen, die gewonnenen Verbesserungsvorschläge in die Hidy-Wallet einzuarbeiten und die MEUSec-Methode erneut auf die angepasste Version der Hidy-Wallet anzuwenden. Dadurch wäre es möglich gewesen, mithilfe der UX- und Informationssicherheit-Scores zu prüfen, inwiefern die Verbesserungsvorschläge zu messbaren Verbesserungen der UX und Informationssicherheit beigetragen haben. Dies konnte durch die einmalige Anwendung der MEUSec-Methode auf die Hidy-Wallet nicht untersucht werden.

Des Weiteren deckten die adaptierten und selbstformulierten Heuristiken der UX und Informationssicherheit die definierten Wallet-Funktionen ab. Somit wurden in Schritt 5 die Aktivitäten, eine Literaturrecherche durchzuführen und Heuristiken abzuleiten, übersprungen und somit nicht evaluiert.

Aufgrund der hohen Anzahl an identifizierten Heuristiken entschieden sich der MU, UXE und ISE nur die Interaktionseigenschaften für Heuristiken zu definieren, denen die höchste Priorität zugeordnet wurde. Heuristiken mit niedrigerer Priorität wurden nicht in der Evaluation berücksichtigt, was die umfassende Evaluation einschränkt. So wurden lediglich 12 von 32 Heuristiken in der Interaktionsmatrix berücksichtigt, was die Anzahl der Interaktionseigenschaften von 992 auf 132 reduzierte. Für die Definition von 132 Interaktionseigenschaften benötigten der MU, UXE und ISE 210 Minuten (= 3,5 Stunden). Das heißt, für die Definition von 992 Interaktionseigenschaften hätten der MU, UXE und ISE ungefähr 1580 Minuten (= 26,33 Stunden) benötigt.

Des Weiteren wurden die Rollen der MEUSec-Methode mit Personen aus dem näheren Projektumfeld besetzt. Dies birgt das Risiko einer unbewussten Verzerrung der Ergebnisse, da persönliche Beziehungen die Objektivität und Neutralität der Beteiligten beeinflussen könnten. So könnten beispielsweise kritische Aspekte weniger stark hinterfragt oder abweichende Meinungen zurückgehalten werden, um Konflikte zu vermeiden.

8 Software-Tool

Um die Anwendung der MEUSec-Methode zu verbessern, wurde ein originäres Software-Tool entwickelt[42], mit dem sich alle 8 Schritte der Methode ausführen lassen.

Zielgruppe des Software-Tools sind Personen, die Wallets hinsichtlich ihrer UX und Informationssicherheit evaluieren und Verbesserungsvorschläge finden wollen, wie beispielsweise Wallet-Anbieter. Darüber hinaus wurde das Software-Tool so entwickelt, dass es erweiterbar und für andere Arten von Software-Systemen einsetzbar ist, sofern geeignete Heuristiken für die jeweilige Art des Software-Systems im Software-Tool hinterlegt werden. Zur Durchführung der MEUSec-Methode mithilfe des Software-Tools müssen ein Experte der UX und ein Experte der Informationssicherheit beteiligt sein. Die Person, die bei Verwendung des Software-Tools die Rolle des Methoden-Anwenders übernimmt, muss keine Expertise im Wallet-Bereich besitzen, allerdings wäre dies von Vorteil. So könnte der Methoden-Anwender beispielsweise bei der Interpretation der Evaluationsergebnisse gezielter Rückfragen stellen und Kontextinformationen besser einordnen. Außerdem kann Expertise im Wallet-Bereich bei der Ableitung praxisnaher Maßnahmen und bei der Identifikation technischer Einschränkungen hilfreich sein.

Das Software-Tool ist als plattformunabhängige, JavaScript-basierte Web-Anwendung realisiert und kann daher über den Browser unabhängig vom Betriebssystem verwendet werden. Das User Interface wurde allerdings speziell für die Desktop-Verwendung entwickelt. Zwar ist der Zugriff auf das Software-Tool über mobile Endgeräte möglich, allerdings wurde auf eine spezifische Anpassung des User Interface für mobile Endgeräte aus Gründen fehlender Ressourcen verzichtet. Zudem wird die Verwendung auf einem Desktop-Gerät aus inhaltlichen Gründen empfohlen – etwa bei der Darstellung der Interaktionsmatrix, die aufgrund ihres Umfangs und ihrer Struktur auf größeren Bildschirmen übersichtlicher und effektiver bedienbar ist. Vor Beginn der Entwicklung wurde nach ähnlichen, bereits entwickelten Software-Tools recherchiert. Es konnte kein Software-Tool gefunden werden, mit dem sich UX und Informationssicherheit gemeinsam evaluieren lassen. Daraus ergab sich der Bedarf zur Neuentwicklung. Besondere Herausforderungen waren die Entwicklung des Datenmodells über alle 8 Schritte der MEUSec-

[42] Die erste Version des Software-Tools wurde im Rahmen einer studentischen Abschlussarbeit (Pfeifer, 2025) entwickelt, die vom Verfasser dieser Dissertation betreut wurde.

Methode hinweg, die automatisierte Berechnung der Scores von UX und Informationssicherheit auf Basis der Erfüllungsgrade der Heuristiken und die Schieberegler zur Einstellung jeweils eines angestrebten Scores der UX und der Informationssicherheit zur Ausgabe von Verbesserungsvorschlägen.

Zuerst wird die Vorgehensweise der Entwicklung in Abschnitt 8.1 beschrieben. Danach wird die Anforderungserhebung in Abschnitt 8.2 erläutert. Anschließend wird der Entwurf in Abschnitt 8.3 dargestellt. Abschließend folgt die Funktionsbeschreibung in Abschnitt 8.4.

8.1 Vorgehensweise der Entwicklung

Für die Entwicklung des Software-Tools wurde eine Vorgehensweise gewählt, die sich an den Prinzipien der iterativen und inkrementellen Softwareentwicklung (Larman und Basili, 2003) orientiert, unter Berücksichtigung des Human-Centered Design – kurz HCD (DIN EN ISO 9241-210:2020-03, 2020). So wurden die Anforderungen und die Entwürfe in enger Abstimmung mit Benutzern validiert und weiterentwickelt. Die Umsetzung des Software-Tools erfolgte in Form funktionaler Module, die iterativ und inkrementell entwickelt sowie getestet wurden. Durch diese Vorgehensweise konnte das Software-Tool gezielt zur Unterstützung der Anwendung der MEUSec-Methode entwickelt werden. Die einzelnen Module orientierten sich an den in der Anforderungserhebung (siehe Abschnitt 8.2) erhobenen Funktionskategorien des Software-Tools. Dazu zählen die Heuristiken, die Interaktionsmatrix, die Festlegung von Erfüllungsgraden der Heuristiken, die benutzerbasierte Evaluation, die Evaluation der Informationssicherheit und allgemeine Funktionen des Software-Tools, wie die Registrierung, Login und Änderung des Passworts. Ergänzt wurde diese inkrementelle und iterative Vorgehensweise durch das HCD, da die kontinuierliche Einbindung von Benutzern dazu beiträgt, dass das Software-Tool die Anforderungen der Benutzer erfüllt. Diese kombinierte Vorgehensweise ist in Abbildung 29 dargestellt und wird im Folgenden detaillierter beschrieben:

Durch die initiale Anwendung der MEUSec-Methode ohne Einsatz eines unterstützenden Software-Tools (siehe Kapitel 7) wurde ein Verständnis des Nutzungskontexts aufgebaut. Es konnten erste Erkenntnisse darüber gewonnen werden, wie ein Software-Tool die methodische Anwendung künftig unterstützen könnte (erste Phase des HCD-Prozesses).

Anschließend wurde die *Anforderungserhebung* für das Software-Tool durchgeführt. Die Anforderungen wurden auf Basis der praktischen Anwendung der MEUSec-Methode (siehe Kapitel 7) gesammelt und kategorisiert. Anschließend wurden die Anforderungen durch den Methoden-Anwender (MU), den UX-Experten (UXE) und den Informationssicherheit-Experten (ISE) der ersten Anwendung der MEUSec-Methode (siehe Kapitel 7)

validiert (zweite Phase des HCD-Prozesses). Die Anforderungserhebung wird in Abschnitt 8.2 thematisiert.

Nach der Anforderungserhebung folgte der *Entwurf*. Zunächst wurde das *Architekturmodell* entworfen. Danach wurden *Wireframes des User Interface* auf einem Miro-Board[43] erstellt. Wireframes vermitteln die grundlegende Struktur, Hierarchie und Funktionalität eines User Interface (Almani und Alrwais, 2024). Die Wireframes wurden zur Validierung mit dem MU, dem UXE und dem ISE der ersten Anwendung der MEUSec-Methode (siehe Kapitel 7) diskutiert und iterativ verbessert. Anschließend wurde das Datenmodell für das Software-Tool entworfen. Damit wurde die dritte Phase des HCD-Prozesses – die „Erarbeitung des Systementwurfs“ – abgedeckt. Der gesamte Entwurf wird in Abschnitt 8.3 erläutert.

Auf Basis des Entwurfs begann die *Programmierung* des Software-Tools. Das Software-Tool wurde in funktionale Module unterteilt, die unabhängig voneinander entwickelt, getestet und verbessert werden konnten. Diese inkrementelle, iterative Vorgehensweise ermöglichte eine flexible Weiterentwicklung der einzelnen Komponenten und unterstützte die Anpassung an neue oder veränderte Anforderungen, die im Verlauf der Entwicklung auftraten. Die Programmierung lässt sich auch der dritten Phase des HCD-Prozesses zuordnen. Die Beschreibung der wichtigsten Funktionen des Software-Tools erfolgt in Abschnitt 8.4.

Zum Schluss folgte die *Evaluation* des Software-Tools (vierte Phase des HCD-Prozesses). Die Evaluation wird in Abschnitt 9.5 beschrieben.

Abbildung 29 visualisiert die beschriebene Vorgehensweise der Entwicklung.

[43] Miro ist ein digitales Whiteboard-Tool, das kollaboratives Arbeiten ermöglicht. https://miro.com.

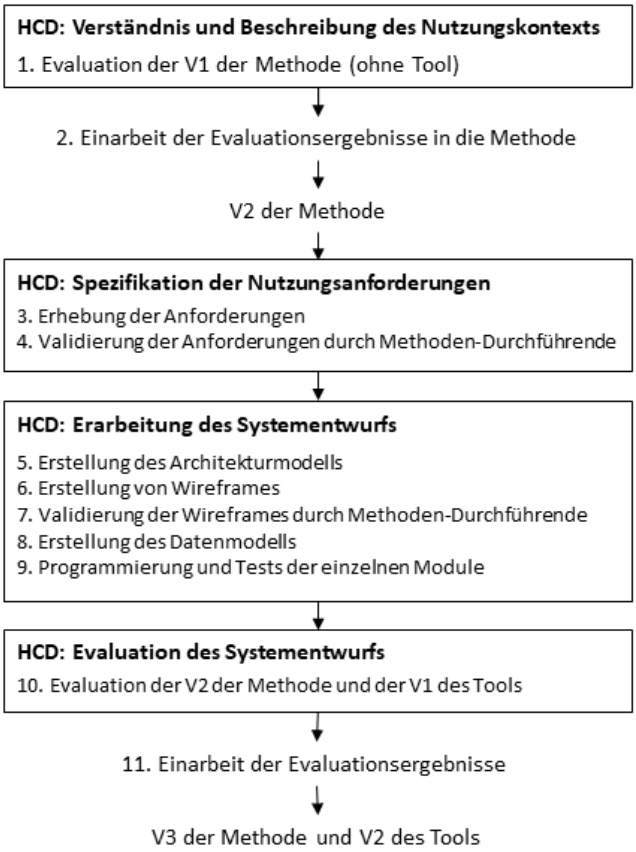


Abbildung 29: Vorgehensweise der Entwicklung des Software-Tools

8.2 Anforderungserhebung

Nach der ersten Anwendung der MEUSec-Methode auf die Hidy-Wallet (siehe Kapitel 7) sammelten Sauer u. a. (2026) Anforderungen an das Software-Tool. Diese Anforderungen wurden von den Personen geprüft, angepasst und erweitert, die bei der ersten Anwendung der MEUSec-Methode (siehe Kapitel 7) die jeweiligen Rollen übernommen hatten. Die validierten 72 Anforderungen wurden verschiedenen Kategorien zugeordnet, darunter „Heuristiken“, „Interaktionsmatrix“, „Festlegung von Erfüllungsgraden der Heuristiken“, „Benutzerbasierte Evaluation“, „Evaluation der Informationssicherheit“ und „Allgemeine Funktionen des Software-Tools“. Diese Kategorien wurden mit dem

Ziel gewählt, eine unabhängige Umsetzung der Anforderungen zu erleichtern. Die Anforderungen wurden in funktionale und nicht-funktionale Anforderungen unterteilt.

Im Folgenden wird eine Zusammenfassung der erhobenen Anforderungen gegeben. Die gesamte Liste aller 72 Anforderungen ist online verfügbar[44].

Zunächst werden die Anforderungen, die der Kategorie „Heuristiken“ zugeordnet wurden, zusammengefasst:

Funktional:

- Erstellung, Bearbeitung und Löschung von Heuristiken
- Verwaltung benutzerspezifischer Heuristik-Sammlungen
- Übersichtsseite, auf der externe Heuristik-Sammlungen (wie beispielsweise die Heuristiken von Nielsen (1994) und von Sauer u. a. (2025c)) aufgelistet, bewertbar und zum Hinzufügen zu den benutzerspezifischen Heuristik-Sammlungen auswählbar sind

Nicht-funktional:

- Übersichtliche Darstellung und leichte Auffindbarkeit von Heuristiken
- Heuristik-Sammlungen sind jederzeit aufrufbar

Nun werden die Anforderungen, die der Kategorie „Interaktionsmatrix“ zugeordnet wurden, zusammengefasst:

Funktional:

- Erstellung, Bearbeitung, Filterung und Löschung von Interaktionsmatrizen
- Festlegung von Interaktionseigenschaften (komplementär, konkurrierend oder neutral) in der Interaktionsmatrix
- Anzeige und Priorisierung konkurrierender Heuristiken
- Dokumentation von Verbesserungsvorschlägen der Wallet

Nicht-funktional: -

[44] https://doi.org/10.5281/zenodo.14917300

Nachfolgend werden die Anforderungen, die der Kategorie „Festlegung von Erfüllungsgraden der Heuristiken“ zugeordnet wurden, zusammengefasst:

Funktional:

- Benutzerverwaltung für Rollen der MEUSec-Methode
- Rollenspezifische Festlegung, Bearbeitung und Auswertung von Erfüllungsgraden der Heuristiken
- Schieberegler zur Einstellung jeweils eines Scores der UX und Informationssicherheit, um zugehörige Verbesserungsvorschläge zu erhalten

Nicht-funktional:

- Evaluationsergebnisse werden für alle Benutzer im Software-Tool verständlich dargestellt

Nun werden die Anforderungen, die der Kategorie „Benutzerbasierte Evaluation“ zugeordnet wurden, zusammengefasst:

Funktional:

- Verwaltung von Probanden (WU) und von zugehörigen Informationen, wie beispielsweise demografische Informationen der WU
- Dokumentation textueller Anleitungen für WU zur Durchführung des Thinking aloud
- Benachrichtigungsfunktion bei Ablauf von Löschfristen der Aufnahmen des Thinking aloud

Nicht-funktional:

- Stärken, Schwächen und Heuristiken werden für alle Benutzer im Software-Tool verständlich dargestellt

Nachfolgend werden die Anforderungen, die der Kategorie „Evaluation der Informationssicherheit“ zugeordnet wurden, zusammengefasst:

Funktional:

- Verwaltung und Verknüpfung von sicherheitsrelevanten Softwarekomponenten, Wallet-Funktionen, Angreifern und Bedrohungen

- Überprüfung, ob jede Wallet-Funktion einer Heuristik zugeordnet wurde

Nicht-funktional:

- Sicherheitsrelevante Softwarekomponenten, Wallet-Funktionen, Angreifer und Bedrohungen werden für alle Benutzer im Software-Tool verständlich dargestellt

Nun werden die Anforderungen, die der Kategorie „Allgemeine Funktionen“ zugeordnet wurden, zusammengefasst:

Funktional:

- Fortschrittsanzeige der Methoden-Durchführung
- Rollen- und Projektverwaltung
- Erstellung von Evaluationsberichten
- Authentifizierung und Zugriffskontrolle

Nicht-funktional:

- Alle Funktionen sollen ohne Anleitung verständlich und problemlos nutzbar sein

8.3 Entwurf

Nach der Anforderungserhebung folgte der Entwurf des Software-Tools. Zunächst erfolgte der Entwurf des Architekturmodells. Danach wurden Wireframes des User Interface entworfen. Anschließend folgte der Entwurf des Datenmodells.

Entwurf des Architekturmodells:

Das Architekturmodell teilt sich grundsätzlich in das Frontend und das Backend auf. Die Trennung ermöglicht es, dass sich das Frontend unabhängig vom Backend entwickeln und anpassen lässt. Zudem unterstützt diese Entkopplung eine verbesserte Skalierbarkeit, da Frontend und Backend separat betrieben und bei Bedarf eigenständig erweitert oder ausgelagert werden können.

Das Backend beinhaltet eine relationale MySQL[45]-Datenbank, einen Server und eine API. Die Wahl einer relationalen MySQL-Datenbank beruht darauf, dass die Anwendung auf einem strukturierten Datenmodell basiert, bei dem Entitäten in logischen Beziehungen zueinanderstehen. MySQL bietet eine performante Lösung mit zuverlässiger Transaktionsverwaltung. Außerdem lässt sich MySQL einfach in bestehende Serverumgebungen integrieren. Die MySQL-Datenbank speichert alle relevanten Daten, während der Server und die API für die Verarbeitung der Anfragen aus dem Frontend verantwortlich sind. Dabei werden SQL-Abfragen genutzt, um Daten abzurufen und zu speichern. Die API bildet die Schnittstelle zwischen Frontend und Backend und ermöglicht eine strukturierte Kommunikation über standardisierte HTTP-Anfragen. Sie wurde als eigenständige Komponente implementiert, um die verschiedenen Systemschichten voneinander zu entkoppeln. Diese Trennung erhöht die Flexibilität, da das Frontend unabhängig vom Backend weiterentwickelt oder durch andere Clients ersetzt werden kann. Gleichzeitig dient die API als zentrale Kontrollinstanz, über die sämtliche Datenoperationen laufen, was die Sicherheit und die Nachvollziehbarkeit verbessert. Der Server verarbeitet die API-Abfragen und führt die SQL-Abfragen in der MySQL-Datenbank aus. Dadurch wird sichergestellt, dass das Frontend keinen direkten Zugriff auf sensible Daten erhält.

Das Frontend umfasst eine Web-Applikation[46], die mit der JavaScript-Bibliothek React[47] umgesetzt wurde. React ermöglicht eine modulare und komponentenbasierte Entwicklung und bietet eine breite Unterstützung externer Bibliotheken, wie Material UI[48], für responsives Design. Dadurch ließ sich ein modernes, anpassungsfähiges User Interface effizient umsetzen. Die Web-Applikation ist in 2 Hauptbereiche unterteilt: die Homepage und das MEUSec-Tool. Die Homepage gliedert sich in mehrere Seiten, darunter die Startseite, wissenschaftliche Grundlagen, Kontakt, Datenschutz und das Impressum. Das MEUSec-Tool beinhaltet alle relevanten Seiten zur Durchführung der MEUSec-Methode. Es gibt eine Projekt-Übersicht, in der sich alle Evaluationsprojekte einsehen lassen. Ein Evaluationsprojekt beinhaltet eine Übersicht der Schritte der MEUSec-Methode mit deren Fortschrittsanzeige. Von dieser Übersicht lässt sich zu den einzelnen Seiten der 8 Schritte der MEUSec-Methode navigieren. Zusätzlich umfasst das MEUSec-Tool verschiedene Seiten zur Anmeldung, Registrierung, Passwortrücksetzung, Support und Einstellungen.

Abbildung 30 visualisiert das beschriebene Architekturmodell.

[45] https://mysql.com
[46] www.meusec.de
[47] https://react.dev
[48] https://mui.com/material-ui

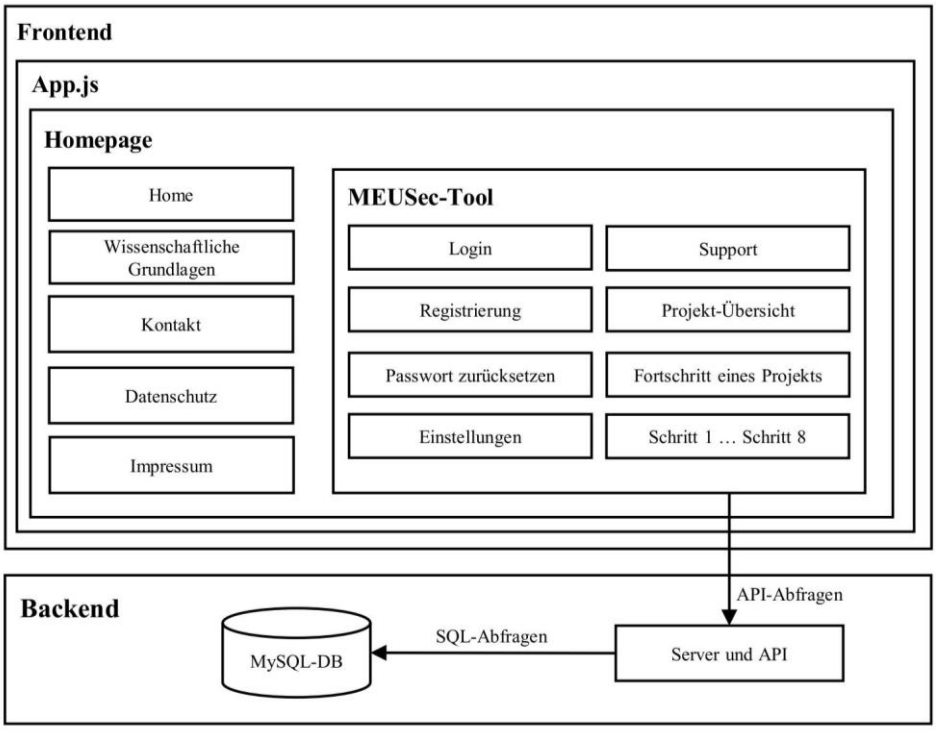


Abbildung 30: Architekturmodell des Software-Tools

Entwurf des User Interface:

Im Rahmen des Entwurfs des User Interface wurden Wireframes der einzelnen Seiten erstellt. Benutzer erreichen zunächst über www.meusec.de eine Startseite mit den Unterseiten „Wissenschaftliche Grundlagen“, „MEUSec-Tool“, „Kontakt“, „Impressum“ und „Datenschutz“. Die Unterseite „MEUSec-Tool“ beinhaltet alle Seiten zur Durchführung der MEUSec-Methode. Hierüber erreichen Benutzer zunächst eine Seite zum Login und zur Registrierung. Danach erreichen Benutzer eine Übersicht aller Evaluationsprojekte. Sobald ein Evaluationsprojekt ausgewählt wird, erscheint die Übersicht aller Schritte der MEUSec-Methode mit deren Fortschrittsanzeige. Von dort aus können Benutzer zu den Seiten der einzelnen Schritte der MEUSec-Methode navigieren. Am Anfang jedes Schritts erscheint eine Seite, welche die Aktivitäten jedes Schritts aufzeigt. Am Ende jedes Schritts erscheint eine Seite, auf der die Namen aller gewonnenen Output-Artefakte in textueller Form aufgelistet sind. Zusätzlich gibt es eine Seite, auf der Einstellungen vorgenommen werden können, wie etwa das Ändern des Passworts und der E-Mail-

Adresse sowie das Löschen des Accounts. Des Weiteren steht eine Seite mit Hilfestellungen zur Verfügung, die ein FAQ-Bereich und Kontaktadressen beinhaltet.

Alle Wireframes sind im Detail online einsehbar[49]. Die wichtigsten Funktionen der Seiten werden in Abschnitt 8.4 zusammengefasst.

Entwurf des Datenmodells:

Im Rahmen des Entwurfs des Datenmodells wurde zunächst ein Entity-Relationship-Modell (ER-Modell) erstellt. Hierzu wurden auf Basis der erhobenen Anforderungen (siehe Abschnitt 8.2) und der Beschreibung der MEUSec-Methode, einschließlich der beteiligten Rollen, zunächst die Entitätstypen definiert. Anschließend wurden die Attributstypen, die Beziehungstypen und die Kardinalitäten definiert.

Das ER-Modell beinhaltet 12 Entitätstypen: „Benutzer“, „Projekt“, „Sammlung“, „Heuristik“, „Stärke/Schwäche“, „Interaktion“, „Verbesserungsvorschlag“, „Funktion“, „Bedrohungsszenario“, „Testfall“, „Wallet-Benutzer“ und „Zu akquirierender Wallet-Benutzer“.

„Benutzer“ meint einen Benutzer des Software-Tools, der eine E-Mail-Adresse, ein Passwort, einen Namen und einen Status („aktiv“ oder „inaktiv“) besitzt. Ein „Benutzer“ kann Zugriff zu keinem Projekt, einem Projekt oder mehreren Projekten (Entitätstyp „Projekt“) haben. Außerdem kann ein „Benutzer“ Inhaber von keinem Projekt, einem Projekt oder mehreren Projekten (Entitätstyp „Projekt“) sein.

„Projekt“ meint ein Evaluationsprojekt, das einen Namen, das Datum der letzten Aktualisierung, den Status („erstellt“, „in Bearbeitung“ und „abgeschlossen“), den aktuellen Schritt mit der aktuellen Aktivität, das Datum der Erstellung und die Anleitung für das Thinking aloud besitzt. Ein Projekt kann keinen Entitätstyp, einen Entitätstyp oder mehrere der folgenden Entitätstypen haben: „Zu akquirierender Wallet-Benutzer“, „Wallet-Benutzer“, „Testfall“, „Funktion“ und „Sammlung“.

Ein „Zu akquirierender Wallet-Benutzer“ meint einen zu akquirierenden Probanden mit dessen Attributstypen „Name“ und „Daten“ (Liste an demografischen Daten).

Ein „Wallet-Benutzer“ meint den akquirierten Probanden mit den Attributstypen „Name“, „Daten“ (Liste an demografischen Daten), „Status“ („erstellt“, „eingeladen“ und „aufgezeichnet“), „Pfad der Aufnahme“, „Datum der Aufnahme“, „Notizen“, „Erhoben”

[49] https://doi.org/10.5281/zenodo.14917062

(Status, ob die Aufnahme des Thinking aloud des Probanden ausgewertet wurde und die daraus abgeleiteten Stärken und Schwächen der Wallet dokumentiert wurden) und „Löschdatum“ (Datum aus der Einwilligungserklärung des Probanden, an dem die Aufnahme des Probanden gelöscht werden soll).

Ein „Testfall“ beschreibt eine exemplarische Nutzung einer ausgewählten Wallet-Funktion durch die WU und dient als Grundlage zur Formulierung der Anleitung des Thinking aloud. Ein „Testfall“ hat die Attributstypen „Name“, „Betroffene Funktionen“ (Wallet-Funktionen, die durch den Testfall abgedeckt sind), „Beschreibung“ (textuell beschriebene, exemplarische Nutzung von mindestens einer ausgewählten Wallet-Funktion durch die WU, wie beispielsweise: „Der WU erstellt ein Backup, setzt die Wallet zurück und stellt das Backup wieder her.“) und „Einrichtungsstatus“ (Status, ob der Testfall für die Wallet vorbereitet wurde).

Eine „Funktion“ meint die zu evaluierende Wallet-Funktion mit den Attributstypen „Name“ und „Beschreibung“. Eine „Funktion“ kann kein Bedrohungsszenario, ein Bedrohungsszenario oder mehrere Bedrohungsszenarien haben (Entitätstyp „Bedrohungsszenario“).

Ein „Bedrohungsszenario“ hat die Attributstypen „Beschreibung”, „Attribute” (Attribute der Informationssicherheit, das meint, Integrität, Vertraulichkeit und Verfügbarkeit), „Schadensausmaß“ (von 1 „geringes Ausmaß“ bis 5 „hohes Ausmaß“), „Eintrittswahrscheinlichkeit“ (1 „unwahrscheinlich“ bis 5 „sehr wahrscheinlich“) und „Inkludiert“ (Status, ob das jeweilige „Bedrohungsszenario in der Evaluation berücksichtigt wird).

Eine „Sammlung“ meint eine Sammlung an Heuristiken der UX und Informationssicherheit. Eine „Sammlung“ hat die Attributstypen „Name“, „Erstelldatum“, „Autor“, „Kontakt”, „Verwendung” (Anwendungsdomäne der jeweiligen Sammlung an Heuristiken) und „Ist öffentlich“ (Status, ob es sich um die eigene Sammlung oder um eine externe Sammlung an Heuristiken handelt). Eine „Sammlung“ kann keine Heuristik, eine Heuristik oder mehrere Heuristiken beinhalten (Entitätstyp „Heuristik“).

Eine „Heuristik“ hat die Attributstypen „Name“, „Beschreibung“, „UX/Informationssicherheit“ (ob die Heuristik die UX oder Informationssicherheit betrifft), „Wallet-Funktion“ (betroffene Wallet-Funktionen), „Gewicht“ (Priorisierung), „Score“ (Erfüllungsgrad), „Begründung“ (Begründung für einen Erfüllungsgrad), „Interaktionen“ (Liste an Interaktionen zu anderen Heuristiken) und „In Matrix“ (ob die Heuristik der Interaktionsmatrix hinzugefügt wurde). Eine „Heuristik“ kann keine, eine oder mehrere Stärke(n) oder Schwäche(n) besitzen (Entitätstyp „Stärke/Schwäche“). Eine „Heuristik“ kann keine Interaktion, eine Interaktion oder mehrere Interaktionen zu anderen Heuristiken haben (Entitätstyp „Interaktionen“). Eine „Heuristik“ kann ein Verbesserungsvorschlag oder mehrere Verbesserungsvorschläge haben (Entitätstyp „Verbesserungsvorschlag“).

Eine „Stärke/Schwäche“ hat die Attributstypen „Typ“ (ob es sich um eine Stärke oder eine Schwäche handelt), „Name“, „Beschreibung“ (beliebiger Text), „Wallet-Funktionen“ (betroffene Wallet-Funktionen), „UX/Informationssicherheit“ (ob es UX oder Informationssicherheit betrifft) und „Attribute“ (betroffene Attribute von UX oder Informationssicherheit).

Eine „Interaktion“ hat die Attributstypen „Typ“ (Interaktionseigenschaft, das meint, „komplementär“, „konkurrierend“ oder „neutral“) und eine „Begründung“ (Begründung eines Erfüllungsgrads).

Ein „Verbesserungsvorschlag“ hat die Attributstypen „Beschreibung“, „Begründung“ (Begründung für die Erstellung des Verbesserungsvorschlags) und „Betroffene Heuristiken“ (betroffene Heuristiken auf Basis derer der Verbesserungsvorschlag erstellt wurde).

Abbildung 31 visualisiert das beschriebene ER-Modell mit den Entitäts- und Beziehungstypen.

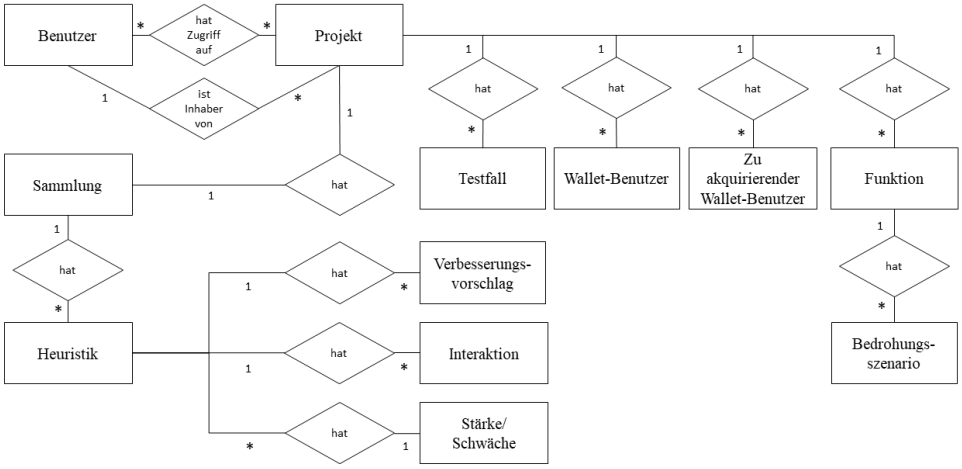


Abbildung 31: Entity-Relationship-Modell des Software-Tools. Zusammengefasst auf Basis des detaillierten, online verfügbaren Modells[50].

Anschließend wurde ein logisches Datenmodell erstellt, das die Datenbanktabellen mit deren Namen, Attributen, Datentypen und Primär- sowie Fremdschlüsseln beinhaltet. Insgesamt wurden 25 Datenbanktabellen erstellt. Das logische Datenmodell ist online verfügbar[51].

[50] https://doi.org/10.5281/zenodo.14917062
[51] https://doi.org/10.5281/zenodo.14917062

8.4 Funktionsbeschreibung

Im Folgenden werden die wichtigsten Funktionen des Software-Tools zusammengefasst und relevante Stellen des Quellcodes erläutert. Das User Interface des Software-Tools wurde anhand der entworfenen Wireframes (siehe Abschnitt 8.3) programmiert.

Übersicht der Evaluationsprojekte: Das Software-Tool zeigt anfangs eine Übersicht aller Evaluationsprojekte eines Benutzers mit den relevanten Daten, wie Name, aktueller Schritt und aktuelle Aktivität, Erstellungsdatum und Status, ob das Projekt in Bearbeitung oder abgeschlossen ist. Zudem kann ein Evaluationsprojekt mit anderen Personen geteilt werden, sodass die jeweiligen Personen Zugriff auf das Evaluationsprojekt erhalten. Außerdem können Evaluationsprojekte gelöscht und dupliziert werden, wenn beispielsweise eine weitere Anwendung der MEUSec-Methode auf ein verbessertes Evaluationsobjekt durchgeführt werden soll. Sobald ein Evaluationsprojekt ausgewählt wird, erscheint die Übersicht der Schritte und Aktivitäten des Evaluationsprojekts.

Übersicht der Schritte und Aktivitäten eines Evaluationsprojekts: Auf dieser Seite können Benutzer einsehen, welche Schritte und Aktivitäten ausstehend, in Bearbeitung und abgeschlossen sind. Zudem lässt sich zu den Schritten und Aktivitäten navigieren.

Schritte und Aktivitäten: Für jeden der 8 Schritte der MEUSec-Methode lässt sich anfangs eine Seite mit den Aktivitäten des jeweiligen Schritts einsehen. Am Ende jedes Schritts erscheint eine Seite mit den gewonnenen Artefakten des Schritts.

Nachfolgend werden die zentralen Funktionen der Schritte zusammengefasst.

In *Schritt 1* lassen sich die zu evaluierenden Wallet-Funktionen auswählen. Hierzu bietet das Software-Tool eine Liste mit vordefinierten Wallet-Funktionen nach Krauß u. a. (2023b) an, die für die Evaluation ausgewählt werden können. Zudem lassen sich Bedrohungsszenarien mit deren Eintrittswahrscheinlichkeit und Schadensausmaß (siehe Abschnitt 6.1.2.1) festlegen.

In *Schritt 2* lassen sich die zu akquirierenden Probanden mit Kategorien und Ausprägungen an demografischen Daten dokumentieren, wie beispielsweise die Kategorie „Alter“ mit den Ausprägungen „14-17“, „18-30“, „31-45“, „46-59“ und „60-99“. Außerdem können Testfälle angelegt und den ausgewählten Wallet-Funktionen zugeordnet werden. Zusätzlich lässt sich die Anleitung des Thinking aloud für die Probanden erstellen und als PDF-Datei exportieren.

In *Schritt 3* lassen sich die akquirierten Probanden verwalten. Die in Schritt 2 definierten Kategorien der demografischen Daten mit deren Ausprägungen lassen sich den Probanden zuordnen. Der Status der Thinking aloud-Aufnahmen kann dokumentiert werden und

relevante Informationen zu den Thinking aloud-Aufnahmen (wie der Pfad zur Datei der Aufnahme oder das Datum der Aufnahme) können festgehalten werden.

In *Schritt 4* lassen sich die durch das Thinking aloud identifizierten Stärken und Schwächen der Wallet dokumentieren. Hierzu können den jeweiligen Stärken und Schwächen vordefinierte Attribute der UX und Informationssicherheit sowie die definierten Wallet-Funktionen zugeordnet werden.

In *Schritt 5* lassen sich UX- und Informationssicherheit-Heuristiken aus vordefinierten Sammlungen an Heuristiken auswählen und der eigenen Sammlung an Heuristiken hinzufügen. Die hinzugefügten Heuristiken können anschließend um eigene Heuristiken, die auf Basis der identifizierten Stärken und Schwächen aus Schritt 4 erstellt werden, erweitert werden. Das Software-Tool zeigt prozentual an, ob den definierten Wallet-Funktionen mindestens eine UX- und eine Informationssicherheits-Heuristik zugeordnet wurde. Zudem werden die fehlenden Heuristiken und die zugehörigen Wallet-Funktionen angezeigt. Die Rückgabe-Werte der zugehörigen Funktion sind wie folgt strukturiert:

1) Wallet-Funktionen, denen entweder die Heuristik der UX oder die Heuristik der Informationssicherheit fehlen:
   - Wallet-Funktion: Übersicht der gespeicherten VC, Heuristik der UX fehlt
   - Wallet-Funktion: Detailansicht der gespeicherten VC, Heuristik der UX fehlt
   - Wallet-Funktion: Teilen von VC, Heuristik der Informationssicherheit fehlt
   - Wallet-Funktion: Speichern von VC, Heuristik der UX und Heuristik der Informationssicherheit fehlen
2) Prozentwert der Wallet-Funktionen, denen sowohl eine Heuristik der UX als auch eine Heuristik der Informationssicherheit zugeordnet wurden: 76,67 %

In *Schritt 6* lässt sich den Heuristiken ein Erfüllungsgrad zuordnen. Die Heuristiken werden automatisiert in eine Interaktionsmatrix eingefügt. In der Interaktionsmatrix können den Heuristiken dann die Interaktionseigenschaften (komplementär, konkurrierend und neutral) zugeordnet werden.

In *Schritt 7* werden die Scores der UX und Informationssicherheit automatisiert (nach der Vorgehensweise aus Abschnitt 6.1) berechnet.

Außerdem lässt sich die eigene Sammlung an Heuristiken veröffentlichen, sodass diese anderen Personen unter den externen Sammlungen an Heuristiken zur Verfügung steht.

In *Schritt 8* werden zunächst die konkurrierenden Heuristiken angezeigt. Wenn sich für diese Konfliktlösungen finden lassen, können die entsprechenden Verbesserungsvorschläge angelegt werden. Wenn sich keine Konfliktlösungen finden lassen, kann entweder die UX-Heuristik oder die Informationssicherheit-Heuristik priorisiert und der ent-

sprechende Verbesserungsvorschlag festgehalten werden. Des Weiteren lassen sich die Verbesserungsvorschläge für komplementäre und neutrale Heuristiken anlegen.

Anschließend werden 2 Schieberegler angezeigt, mit denen die gewünschten Scores für UX und Informationssicherheit festgelegt werden können. Die Schieberegler lassen sich bis zu einem bestimmten Wert anpassen, solange die maximale Summe aller Erfüllungsgrade der komplementären und neutralen Heuristiken nicht überschritten wird. Sobald dieser Punkt erreicht ist, hat die Anpassung des Scores der UX oder Informationssicherheit negative Auswirkungen auf den Score des jeweiligen anderen, sodass sich die Schieberegler anpassen. Für die jeweilige Einstellung der Schieberegler wird die Anzeige der zugehörigen Heuristiken in Echtzeit aktualisiert, deren Erfüllungsgrad verbessert werden muss, um die eingestellten Scores der UX und Informationssicherheit zu erreichen. Die angezeigten Heuristiken können dann verwendet werden, um daraus die zugehörigen Verbesserungsvorschläge anzulegen.

Abbildung 32 beschreibt die Logik des UX-Schiebereglers zur Auswahl von Heuristiken, deren Erfüllungsgrade verbessert werden müssen, um den eingestellten UX-Score mit dem angepassten Informationssicherheit-Score zu erreichen.

Input sind:

- die neutralen und komplementären UX-Heuristiken: „not_conflicting_ux_heuristics“
- die konkurrierenden UX-Heuristiken: „conflicting_ux_heuristics“
- der mit dem UX-Schieberegler neu eingestellte UX-Score: „newUXScore“
- der ursprüngliche UX-Score: „initialUXScore“
- der maximal mögliche UX-Score (Summe der maximalen Erfüllungsgrade aller UX-Heuristiken): „maxUXScore“
- der maximal mögliche UX-Score, bei dessen Überschreitung die UX die Informationssicherheit negativ beeinflusst (Summe der maximalen Erfüllungsgrade aller komplementären und neutralen Heuristiken): „maxUXScoreNotConfl“

Output sind:

- die neutralen und komplementären Heuristiken und
- die konkurrierenden Heuristiken, die zur Erreichung des eingestellten UX-Scores auf ihre maximalen Erfüllungsgrade verbessert werden müssen

In der ersten foreach-Schleife (Zeile 1 bis 9) wird zunächst geprüft, ob sich der eingestellte UX-Score durch die Maximierung der Erfüllungsgrade der komplementären und neutralen Heuristiken erreichen lässt. Je Iteration wird der Erfüllungsgrad der jeweiligen Heuristiken auf „initialUXScore“ addiert (Zeile 3). Zusätzlich wird je Iteration die Eigenschaft „heuristic_included“ der jeweiligen Heuristik auf „true“ gesetzt (Zeile 4). Es

wird solange iteriert bis „initialUXScore“ den „newUXScore“ erreicht hat. Die Eigenschaft „heuristic_included“ der übrigen komplementären und neutralen Heuristiken wird auf „false“ gesetzt. Wenn „initialUXScore“ den „newUXScore“ nicht erreicht, werden die konkurrierenden Heuristiken in der zweiten foreach-Schleife mit der gleichen Vorgehensweise der ersten foreach-Schleife iteriert (Zeile 10 bis 18). Anschließend erfolgt in Zeile 19 die Aktualisierung des UX-Sliders, indem der neue Wert von „newUXScore“ gesetzt wird. Danach muss der Score des Informationssicherheit-Sliders namens „SliderISScore“ angepasst werden, falls die Einstellung des UX-Scores den Informationssicherheit-Score negativ beeinflusst hat. Hierzu wird in Zeile 20 geprüft, ob „maxUXScoreNotConfl“ kleiner als „newUXScore“ ist. Wenn ja, wird zunächst die Differenz aus „newUXScore“ und „maxUXScoreNotConfl“ in Zeile 21 berechnet. In Zeile 22 wird daraufhin der Wert von „SliderISScore“ um die Differenz von „newUXScore“ und „maxUSScoreNotConfl“ verringert. Falls nein, werden Zeile 21 und Zeile 22 übersprungen.

```
   Input: not_conflicting_ux_heuristics, conflicting_ux_heuristics,
          newUXScore, initialUXScore, maxUXScore,
          maxUXScoreNotConfl
 1 foreach heuristic ∈ not_conflicting_ux_heuristics do
 2 |  if initialUXScore < newUXScore then
 3 |  |  initialUXScore ←
   |  |   initialUXScore + heuristic.heuristic_score_diff;
 4 |  |  heuristic.heuristic_included ← true;
 5 |  end
 6 |  else
 7 |  |  heuristic.heuristic_included ← false;
 8 |  end
 9 end
10 foreach heuristic ∈ conflicting_ux_heuristics do
11 |  if initialUXScore < newUXScore then
12 |  |  initialUXScore ←
   |  |   initialUXScore + heuristic.heuristic_score_diff;
13 |  |  heuristic.heuristic_included ← true;
14 |  end
15 |  else
16 |  |  heuristic.heuristic_included ← false;
17 |  end
18 end
19 setSliderUXScore(newUXScore);
20 if maxUXScoreNotConfl < newUXScore then
21 |  diff ← newUXScore − maxUXScoreNotConfl;
22 |  recudeISScore(diff);
23 end
   Output: all heuristics h ∈ not_conflicting_ux_heuristics and h ∈
           conflicting_ux_heuristics with h.included = true
```

Abbildung 32: Software-Tool – Schieberegler-Funktion. Der dargestellte Pseudocode wurde auf Grundlage des online verfügbaren Quellcodes[52] erstellt.

[52] https://github.com/fzi-forschungszentrum-informatik/meusec

Auf der letzten Seite des Software-Tools lässt sich ein Bericht generieren, der alle relevanten Ergebnisse der Evaluation und der Verbesserungsvorschläge beinhaltet. Ein Beispiel eines generierten Berichts ist online verfügbar[53].

Der gesamte Quellcode des Software-Tools ist online einsehbar[54]. Das Software-Tool lässt sich online verwenden[55].

[53] https://doi.org/10.5281/zenodo.15114275
[54] https://github.com/fzi-forschungszentrum-informatik/meusec
[55] www.meusec.de

9 Evaluation der zweiten Version der MEUSec-Methode und der ersten Version des Software-Tools

Nach der ersten Evaluation (siehe Kapitel 7) wurde die MEUSec-Methode auf Basis der Evaluationsergebnisse (siehe Abschnitt 7.4) verbessert. Diese zweite, verbesserte Version unterscheidet sich von der dritten, finalen Version (siehe Kapitel 6) im Wesentlichen darin, dass zuerst eigene UX- und Informationssicherheit-Heuristiken definiert und anschließend UX- und Informationssicherheit-Heuristiken aus vorgegebenen Sammlungen ausgewählt werden.

Die zweite Version der MEUSec-Methode wurde auf die Lissi-Wallet[56] angewendet[57]. Zur Unterstützung der Anwendung der MEUSec-Methode wurde das entwickelte Software-Tool (siehe Kapitel 8) verwendet. Dadurch sind grundsätzlich 3 Beiträge entstanden: die Evaluation der MEUSec-Methode, die Evaluation des Software-Tools und die Evaluation der UX und Informationssicherheit der Lissi-Wallet. Nach der zweiten Evaluation wurden die Verbesserungvorschläge in die Methode und in das Software-Tool eingearbeitet, sodass im Rahmen dieser Arbeit eine finale dritte Version der Methode und eine finale zweite Version des Software-Tools entstanden sind.

Abbildung 33 fasst den Entwicklungsprozess der MEUSec-Methode und des Software-Tools zusammen.

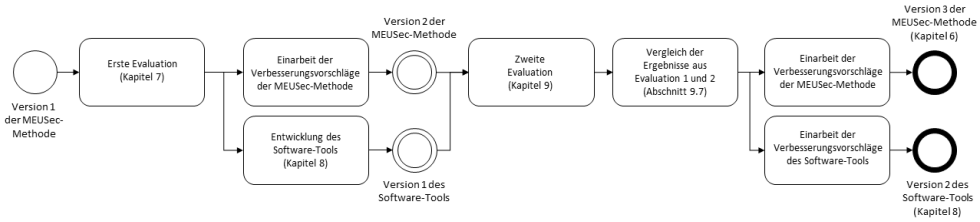


Abbildung 33: Entwicklungsprozess von MEUSec-Methode und Software-Tool.

[56] https://lissi.id/de

[57] Die zweite Evaluation wurde im Rahmen einer studentischen Abschlussarbeit (Pfeifer, 2025) durchgeführt, die vom Verfasser dieser Dissertation betreut wurde.

In Abschnitt 9.1 wird die Vorgehensweise der zweiten Evaluation beschrieben. Daraufhin werden die Evaluationsergebnisse der Lissi-Wallet in Abschnitt 9.2 dargestellt und in Abschnitt 9.3 mit Evaluationsergebnissen anderer Wallets aus der Literatur verglichen. Die Evaluationsergebnisse der MEUSec-Methode werden in Abschnitt 9.4 ausgeführt. Die Evaluationsergebnisse des Software-Tools werden in Abschnitt 9.5 erläutert. Die Limitationen werden in Abschnitt 9.6 beschrieben. Abschließend werden die Ergebnisse der zweiten Evaluation mit denen der ersten Evaluation in Abschnitt 9.7 verglichen.

9.1 Vorgehensweise

Die im Rahmen der ersten Evaluation identifizierten Verbesserungsvorschläge der ersten Version der MEUSec-Methode (siehe Kapitel 7) wurden in die MEUSec-Methode eingearbeitet. So entstand die zweite Version der MEUsec-Methode. Das überarbeitete Vorgehensmodell der zweiten Version ist online verfügbar[58]. Die zweite Version wurde evaluiert, indem diese auf die Lissi-Wallet[59] angewendet wurde. Hierzu wurde das entwickelte Software-Tool (siehe Kapitel 8) verwendet, das die Anwendung der MEUSec-Methode unterstützt. Dadurch entstanden grundsätzlich 3 Beiträge: die Evaluation der Lissi-Wallet, die Evaluation der zweiten Version der MEUSec-Methode und die Evaluation des Software-Tools.

Die kombinierte Evaluation der Lissi-Wallet, der MEUSec-Methode und des Software-Tools kann die Unabhängigkeit der einzelnen Evaluationen beeinträchtigen. Beispielsweise könnte sich ein ineffizienter Schritt der MEUSec-Methode auf die Evaluation der Effizienz des Software-Tools auswirken. Um dieser Herausforderung entgegenzuwirken, wurden Maßnahmen ergriffen: Die Anwendung der MEUSec-Methode mithilfe des Software-Tools wurde durch 2 außenstehende Personen begleitet, die sicherstellten, dass alle Aktivitäten sachgemäß durchgeführt wurden. Auf diese Weise sollte verhindert werden, dass Anwendungsfehler die Ergebnisse der Evaluationen verfälschen. Des Weiteren wurden zur Evaluation der MEUSec-Methode und des Software-Tools voneinander getrennte Evaluationskriterien verwendet. Außerdem wurden die Personen, die im Rahmen ihrer Rollen die jeweiligen Evaluationskriterien bewerteten, unmittelbar vor der Bewertung ausdrücklich darauf hingewiesen, Schwächen der MEUSec-Methode und des Software-Tools zu berücksichtigen und die Evaluationskriterien unabhängig voneinander zu bewerten. Ziel war es, eine möglichst klare Trennung zwischen den Evaluationen der Methode, des Tools und der Wallet zu erreichen.

[58] https://doi.org/10.5281/zenodo.14384065
[59] https://lissi.id/de

Die 3 Evaluationen wurden jeweils als separate Online-Meetings durchgeführt. Im Rahmen der Durchführung der MEUSec-Methode fanden einzelne Schritte und Aktivitäten ebenfalls in getrennten Online-Meetings statt, da jeweils nur bestimmte Rollen beteiligt waren. Die beteiligten Rollen hatten dabei jeweils das Software-Tool geöffnet, während der Methoden-Anwender seinen Bildschirm teilte und durch die einzelnen Schritte und Aktivitäten im Software-Tool moderierte. Eine Ausnahme bildete Schritt 3 der Methode – die Durchführung des Thinking aloud. Schritt 3 wurde in Präsenz im Rahmen einer Laborsituation durchgeführt. Dabei wurden sowohl die Probanden (Video und Ton) als auch der Smartphone-Bildschirm aufgezeichnet.

Die Lissi-Wallet wurde verwendet, da die Lissi GmbH[60] Teil des gemeinsamen Forschungsprojekts „Sichere und Selbstbestimmte Digitale Identitäten im E-Commerce (SDI4ECom)“[61] war. Dadurch stand die API-Dokumentation zur Verfügung und Fragen konnten einfach mit den Mitarbeitenden der Lissi GmbH diskutiert werden.

Vorgehensweise der Evaluation der Lissi-Wallet:

Die Anwendung der MEUSec-Methode erfordert vier Rollen, die zu besetzen sind: der Methoden-Anwender (MU), der UX-Experte (UXE), der Informationssicherheit-Experte (ISE) und Probanden (WU). Der MU wurde durch einen wissenschaftlichen Mitarbeiter besetzt, der noch keine Erfahrung mit Wallets hatte. Diese Auswahl des MU wurde speziell getroffen, um zu evaluieren, ob die Rolle des MU durch eine Person besetzt werden kann, die keine Erfahrung mit Wallets besitzt. Die Erkenntnisse daraus sollten aufzeigen, ob die MEUSec-Methode und das Software-Tool zukünftig beispielsweise von UX-Dienstleistern genutzt werden können, ohne dass eine vorherige Einarbeitung in Wallet-spezifische Themen erforderlich ist. Der ISE war ein wissenschaftlicher Mitarbeiter, der im Bereich Informationssicherheit forscht. Der UXE war ein akademischer Mitarbeiter, der im Bereich UX forscht. Die WU wurden während der Anwendung der MEUSec-Methode akquiriert. Diese werden im zugehörigen Abschnitt 9.2 beschrieben. Die Lissi-Wallet wird in Abschnitt 9.2 erläutert.

Vorgehensweise der Evaluation der MEUSec-Methode:

Zur Evaluation der zweiten Version der MEUSec-Methode wurden dieselben Evaluationskriterien der ersten Version verwendet (siehe Abschnitt 7.1).

Nach jedem der 8 Schritte der MEUSec-Methode dokumentierten der MU, UXE und ISE ihre Beobachtungen bezüglich der Evaluationskriterien. Zusätzlich nahmen 2 externe Beobachter an der Anwendung der MEUSec-Methode teil, um ohne einzugreifen Notizen

[60] https://www.lissi.id
[61] https://sdi4ecom.de

zu den Evaluationskriterien festzuhalten. Beispielsweise dokumentierten sie die Zeiten der einzelnen Schritte der MEUSec-Methode. Abschließend fand eine gemeinsame Diskussionsrunde statt, um zu bewerten, ob die Evaluationskriterien erfüllt, teilweise erfüllt oder nicht erfüllt wurden. Im Rahmen der Diskussionsrunde erfolgte eine Gegenüberstellung von Argumenten für und gegen die Erfüllung jedes einzelnen Evaluationskriteriums. Auf Basis der Argumente wurde eine abschließende Bewertung der Erfüllungsgrade getroffen. Da zwischen den Rollen keine Meinungsverschiedenheiten auftraten, waren keine Konfliktlösungen notwendig.

Die Evaluationskriterien der MEUSec-Methode wurden unter der Annahme der sachgemäßen Durchführung der MEUSec-Methode bewertet. Um Fehler durch eine unsachgemäße Durchführung zu vermeiden, wurde die Durchführung der MEUSec-Methode überwacht. Konkret waren der Verfasser dieser Dissertation und eine außenstehende Person anwesend, um bei einer fehlerhaften Durchführung eingreifen zu können.

Vorgehensweise der Evaluation des Software-Tools:

Für die Evaluation des Software-Tools wurden die folgenden Evaluationskriterien anhand der Software-Qualitätsmerkmale nach ISO/IEC 25010 (2023) verwendet. Für jedes Evaluationskriterium wurden zunächst Fragen durch den Verfasser dieser Dissertation gesammelt. Diese wurden anschließend durch die Durchführenden der MEUSec-Methode validiert.

(ET1) Funktionalität des Software-Tools:

(ET1.1) Vollständigkeit: Lassen sich alle 8 Schritte der MEUSec-Methode mithilfe des Software-Tools ausführen? Lassen sich alle definierten Wallet-Funktionen mithilfe des Software-Tools evaluieren? Lassen sich UX- und Informationssicherheit-Heuristiken sowie Interaktionseigenschaften der Heuristiken im Software-Tool dokumentieren? Lassen sich UX- und Informationssicherheit-Heuristiken im Software-Tool auswählen und wiederverwenden? Werden jeweils ein Score für UX und ein Score für die Informationssicherheit durch das Software-Tool berechnet? Lassen sich Verbesserungsvorschläge für UX und Informationssicherheit basierend auf den definierten Interaktionseigenschaften der Heuristiken im Software-Tool erstellen? Lassen sich Verbesserungsvorschläge über einen Schieberegler für verschiedene Scores der UX und Informationssicherheit ausgeben? Lässt sich nach der Durchführung ein Evaluationsbericht mithilfe des Software-Tools generieren? Lassen sich Projekte für unterschiedliche Evaluationen erstellen? Lassen sich Projekte gezielt für Benutzer freigegeben?

(ET1.2) Korrektheit: Berechnet das Software-Tool die Scores der UX und Informationssicherheit korrekt? Unterstützt das Software-Tool die Formulierung plausibler Verbesserungsvorschläge?

(ET1.3) Angemessenheit: Unterstützt das Software-Tool die zweckmäßige Durchführung aller 8 Schritte der MEUSec-Methode?

(ET2) UX und Usability:

(ET2.1) Selbstbeschreibungsfähigkeit: Lässt sich das Software-Tool intuitiv bedienen? Sind das User Interface und dessen Elemente logisch strukturiert? Werden die gewonnenen Artefakte (wie beispielsweise Erfüllungsgrade von Heuristiken, Interaktionseigenschaften und Verbesserungsvorschläge) verständlich angezeigt?

(ET2.2) Effizienz: Reduziert das Software-Tool den Zeit- und Ressourcenaufwand im Vergleich zu einer manuellen Durchführung der MEUSec-Methode?

(ET2.3) Fehlervermeidung: Unterstützt das Software-Tool, Eingabefehler zu verhindern? Werden Warnungen oder Hilfestellungen bei fehlerhaften Eingaben bereitgestellt?

(ET2.4) Akzeptanz: Wird das Software-Tool von den verschiedenen Rollen (UXE, ISE und MU) akzeptiert? Erfüllt das Software-Tool die Anforderungen und Erwartungen dieser Rollen?

Analog zur Vorgehensweise der Evaluation der MEUSec-Methode haben der MU, UXE und ISE während der Durchführung Notizen zu den Evaluationskriterien des Software-Tools festgehalten. Abschließend fand eine gemeinsame Diskussionsrunde statt, um zu bewerten, ob die Evaluationskriterien erfüllt, teilweise erfüllt oder nicht erfüllt wurden. In der Diskussionsrunde erfolgte eine Gegenüberstellung von Argumenten für und gegen die Erfüllung jedes einzelnen Evaluationskriteriums. Auf Basis der Argumente wurde eine abschließende Bewertung der Erfüllung getroffen. Da zwischen den Rollen keine Meinungsverschiedenheiten auftraten, waren keine Konfliktlösungen notwendig.

Zusätzlich prüften der MU, der UXE und der ISE, ob die definierten Anforderungen des Software-Tools (siehe Abschnitt 8.2) erfüllt wurden.

9.2 Evaluationsergebnisse der Lissi-Wallet

Im Folgenden wird die Evaluation der Lissi-Wallet beschrieben. Es werden jeweils die Artefakte der 8 Schritte der MEUSec-Methode erläutert. Mit Ausnahme der Aufnahmen des Thinking aloud wurden alle gewonnenen Artefakte in der Datenbank des Software-Tools gespeichert. Die Aufnahmen des Thinking aloud wurden aus Speicherplatzgründen von den Benutzern außerhalb des Software-Tools an einem selbstgewählten Speicherort abgelegt. Die Speicherorte wurden im Software-Tool dokumentiert.

Schritt 1 – Definition des Evaluationsobjekts:

Input von Schritt 1 war das Evaluationsobjekt, das heißt, die Lissi-Wallet[62].

Schritt 1, Aktivität 1 – Definition der zu evaluierenden Wallet-Funktionen: Zu Beginn wählte der MU die zu evaluierenden Wallet-Funktionen aus einer Liste an Wallet-Funktionen von Krauß u. a. (2023b) aus. Die folgenden Wallet-Funktionen (WF1-15) wurden ausgewählt:

(WF1) Übersicht gespeicherter VC (siehe Abschnitt 2.2)

(WF2) Detailansicht gespeicherter VC

(WF3) Zurücksetzen der Wallet

(WF4) Erstellung eines Backups

(WF5) Wiederherstellung eines Backups

(WF6) Suche nach VC und deren Ausstellern und Prüfern

(WF7) Automatische Vorauswahl von zu teilenden VC

(WF8) Wallet-Schutz

(WF9) Löschen von VC

(WF10) Übersicht von Kontakten (Aussteller und Prüfer)

(WF11) Kontakte löschen

(WF12) PIN ändern

(WF13) Sprache ändern

(WF14) Speicherung von VC

(WF15) Teilen von VC

Schritt 1, Aktivität 2 – Identifizierung von Bedrohungsszenarien und Aktivität 3 – Definition des Umfangs der Informationssicherheitsevaluation: Der ISE und der MU betrachteten die ausgewählten Wallet-Funktionen aus Aktivität 1.1 und dokumentierten mögliche

[62] https://lissi.id/de

Bedrohungsszenarien. Die Dokumentation erfolgte mit einer Vorlage, welche die folgenden Attribute besaß: die eindeutige ID, die Beschreibung des Bedrohungsszenarios, die betroffenen Attribute der Informationssicherheit (Vertraulichkeit, Integrität oder Verfügbarkeit), das Schadensausmaß von 1 (geringe Auswirkung) bis 5 (hohe Auswirkung), die Eintrittswahrscheinlichkeit von 1 (unwahrscheinlich) bis 5 (sehr wahrscheinlich) und die betroffenen Wallet-Funktionen. Anschließend wählte der MU in Abstimmung mit dem ISE diejenigen Bedrohungsszenarien aus, die später in der Evaluation berücksichtigt werden sollten. Die Auswahl erfolgte durch den MU unter Berücksichtigung der durch den ISE vorgenommenen Risikobewertung. Diese basierte auf Schadensausmaß und Eintrittswahrscheinlichkeit. Ergänzend flossen in die Entscheidungsfindung die verfügbaren Ressourcen des MU ein. Tabelle 25 zeigt die ausgewählten Bedrohungsszenarien. Aus Gründen der besseren Lesbarkeit wurden Schadensausmaß mit (SA) und Eintrittswahrscheinlichkeit mit (EW) abgekürzt.

Beschreibung	**Attribute**	**SA**	**EW**	**Wallet-Funktion**
Falls das Smartphone entsperrt ist, kann ein Angreifer ohne zusätzliche Authentifizierung auf Daten in der Wallet zugreifen.	Vertraulichkeit	5	2	Wallet-Schutz, Übersicht von Kontakten
Ein VC könnte Daten beinhalten, die für Benutzer nicht sichtbar sind. So könnte ein versteckter Datenaustausch zwischen dem Aussteller und dem Prüfer stattfinden.	Vertraulichkeit	3	3	Detailansicht gespeicherter VC
Falls VC ausschließlich auf dem Smartphone gespeichert sind, könnte der Benutzer nicht wissen, dass diese nach dem Zurücksetzen der Wallet unwiderruflich verloren gehen.	Verfügbarkeit	5	3	Zurücksetzen der Wallet, Löschen von VC
Falls keine zusätzliche Authentifizierung für das Zurücksetzen der Wallet erforderlich ist, könnte die Wallet versehentlich zurückgesetzt werden.	Verfügbarkeit	5	2	Zurücksetzen der Wallet, Löschen von VC und Kontakten
Falls ein Angreifer Zugriff auf das Smartphone hat, könnte er vollständigen Zugriff auf die VC haben, wenn die Wallet keine Authentifizierung erfordert oder wenn dieselbe Authentifizierung des Smartphones verwendet wird.	Vertraulichkeit, Verfügbarkeit, Integrität	5	2	Wallet-Schutz

Falls Kontakte ausschließlich auf dem Smartphone gespeichert sind, könnte der Benutzer nicht wissen, dass sie nach dem Zurücksetzen der Wallet unwiderruflich verloren gehen.	Verfügbarkeit	5	3	Löschen von Kontakten
Die Wallet könnte es erlauben, dass Benutzer eine zu schwache PIN der Wallet festlegen dürfen.	Vertraulichkeit, Verfügbarkeit, Integrität	5	1	Pin ändern
Während der Wiederherstellung eines Backups könnte der kopierte Backup-Schlüssel unbeabsichtigt über die Zwischenablage an andere Anwendungen weitergegeben werden.	Vertraulichkeit	3	3	Wiederherstellung eines Backups

Tabelle 25: Lissi-Wallet – Bedrohungsszenarien. (Sauer u. a., 2026). Übersetzt aus dem Englischen.

Output von Schritt 1 war das definierte Evaluationsobjekt, das heißt, eine Liste mit den zu evaluierenden Wallet-Funktionen und eine Liste mit ausgewählten Bedrohungsszenarien.

Schritt 2 – Vorbereitung der benutzerbasierten Evaluation:

Input von Schritt 2 war das definierte Evaluationsobjekt, das heißt, eine Liste mit den zu evaluierenden Wallet-Funktionen und eine Liste mit ausgewählten Bedrohungsszenarien.

Schritt 2, Aktivität 1 – Definition der Anforderungen an die WU-Auswahl: Der MU, ISE und UXE definierten 8 Anforderungskategorien mit ihren Ausprägungen für die anschließende Akquise von WU: Die Anforderungskategorie „Alter“ umfasst die Ausprägungen „14-17 Jahre“, „18-30 Jahre“, „31-40 Jahre“, „41-50 Jahre“, „51-60 Jahre“ und „61-99 Jahre“. Die Anforderungskategorie „Geschlecht“ hat die Ausprägungen „weiblich“, „männlich“ und „divers“. Die Anforderungskategorie „Familienstand“ umfasst die Ausprägungen „ledig“, „verheiratet“, „geschieden“ und „verwitwet“. Die Anforderungskategorie „Kinder“ gibt an, ob eine Person Kinder hat (Ausprägungen: „ja“ oder „nein“). Die Anforderungskategorie „Bildungsabschluss“ hat die Ausprägungen „Schulabschluss“ (Hauptschulabschluss, Realschulabschluss, Abitur), „Berufsabschluss“ und „Hochschulabschluss“ (Bachelor, Master, Promotion). Die Anforderungskategorie „technische Affinität“ wird anhand der Ausprägungen „keine Kenntnisse“, „geringe Kenntnisse“, „grundlegende Kenntnisse“, „solide Kenntnisse“, „gute Kenntnisse“ und „fortgeschrittene Kenntnisse“ bewertet. Die Anforderungskategorie „Vorerfahrung“ mit Wallets wird in

die Ausprägungen „ja“, „nein, aber bekannt“ und „nein, unbekannt“ unterteilt. Schließlich gibt die Anforderungskategorie „Datenschutzbedenken“ an, inwieweit Personen um ihre Privatsphäre besorgt sind. Die Ausprägungen sind „keine Bedenken“, „geringe Bedenken“, „wesentliche Bedenken“, „hohe Bedenken“ und „ernsthafte Bedenken“.

Schritt 2, Aktivität 2 – Definition von Testfällen der Wallet-Funktionen: Der MU, UXE und ISE definierten die Testfälle der Lissi-Wallet mit dem Namen, den betroffenen Wallet-Funktionen und der Beschreibung (siehe Tabelle 26). Jeder Testfall beschreibt eine exemplarische Nutzung einer ausgewählten Wallet-Funktion durch die WU. Die Testfälle dienten als Grundlage für die Ausarbeitung einer strukturierten Anleitung zur Durchführung des Thinking aloud in Schritt 3.

Name	**Betroffene Wallet-Funktionen**	**Beschreibung**
Login der Wallet	Wallet-Schutz	Der WU öffnet die Wallet und authentisiert sich.
Speichern eines VC in der Wallet nach Einkauf in Online-Shop A	Übersicht gespeicherter VC, Speicherung von VC	Der WU kauft in Online-Shop A ein und speichert das VC der Shoppingdaten in der Wallet. Der WU prüft, ob das gespeicherte VC in der VC-Übersicht der Wallet erscheint.
WU prüft gespeichertes VC in der Wallet	Übersicht gespeicherter VC, Detailansicht gespeicherter VC, Suche	Der WU prüft in der Detailansicht des VC, ob die Daten des VC korrekt sind.
WU teilt VC aus der Wallet an Online-Shop B	Automatische Vorauswahl von zu teilenden VC, Teilen von VC	Der WU teilt das gespeicherte VC mit Online-Shop B.
Einstellungen in der Wallet ändern	Sprache ändern, PIN ändern	Der WU ändert die PIN und die Sprache der Wallet.
Backup der Wallet	Zurücksetzen der Wallet, Erstellung eines Backups, Wiederherstellung eines Backups	Der WU erstellt ein Backup, setzt die Wallet zurück und stellt das Backup wieder her.

WU löscht VC und Kontakte in der Wallet	Löschen von VC, Löschen von Kontakten, Übersicht von Kontakten, Übersicht gespeicherter VC, Detailansicht gespeicherter VC	Der WU löscht den Kontakt (Online-Shop A und B) und das VC.

Tabelle 26: Lissi-Wallet – Testfälle der Wallet. (Sauer u. a., 2026). Übersetzt aus dem Englischen.

Schritt 2, Aktivität 3 – Akquise der WU: Die 13 WU wurden durch den MU anhand der definierten Anforderungen aus Schritt 2, Aktivität 1 zum Thinking aloud eingeladen. Zur Erhebung der demografischen Daten erhielten die WU einen Fragebogen zum Ausfüllen. Außerdem mussten die WU eine Einverständniserklärung für die Datenerhebung unterschreiben. Tabelle 24 beinhaltet die demografischen Daten der 13 WU anhand der definierten Anforderungskategorien und Ausprägungen von Aktivität 2.1.

Alter	**Geschlecht**	**Familienstand**	**Kind**	**Höchster Bildungsabschluss**	**Technik-Affinität**	**Vorerfahrung**	**Datenschutzbedenken**
31-40	Weiblich	Verheiratet	Nein	Hochschulabschluss	Solide	Ja	Wesentliche Bedenken
51-60	Männlich	Verheiratet	Ja	Hochschulabschluss	Fortgeschritten	Nein, unbekannt	Wesentliche Bedenken
31-40	Weiblich	Ledig	Nein	Hochschulabschluss	Solide	Nein, aber bekannt	Geringe Bedenken
31-40	Weiblich	Ledig	Nein	Hochschulabschluss	Gut	Ja	Wesentliche Bedenken
41-50	Weiblich	Ledig	Ja	Hochschulabschluss	Gut	Nein, aber bekannt	Geringe Bedenken
18-30	Männlich	Ledig	Nein	Hochschulabschluss	Fortgeschritten	Nein, aber bekannt	Geringe Bedenken
41-50	Weiblich	Ledig	Nein	Berufsabschluss	Keine	Nein, aber bekannt	Hohe Bedenken
51-60	Weiblich	Verheiratet	Ja	Berufsabschluss	Gering	Nein, unbekannt	Keine Bedenken
18-30	Weiblich	Ledig	Nein	Hochschulab-	Solide	Nein, aber	Geringe Bedenken

				schluss		bekannt	
14-17	Männlich	Ledig	Nein	Schulab-schluss	Grund-legend	Nein, unbe-kannt	Geringe Bedenken
14-17	Weiblich	Ledig	Nein	Schulab-schluss	Grund-legend	Nein, unbe-kannt	Keine Bedenken
61-99	Weiblich	Verhei-ratet	Ja	Hoch-schulab-schluss	Grund-legend	Nein, aber bekannt	Geringe Bedenken
61-99	Männlich	Verhei-ratet	Ja	Schulab-schluss	Grund-legend	Nein, unbe-kannt	Geringe Bedenken

Tabelle 27: Lissi-Wallet – Demografische Daten der Probanden. (Sauer u. a., 2026). Übersetzt aus dem Englischen.

Schritt 2, Aktivität 4 – Einrichten von Testfällen auf dem Endgerät: Der MU, ISE und UXE erstellten eine Anleitung für die WU um später Thinking aloud (siehe Abschnitt 5.2.8) durchzuführen. Eine Zusammenfassung der Anleitung wird nachfolgend dargestellt. Die detaillierte Anleitung ist online verfügbar[63].

1. Wallet-Login: Öffnen Sie die Lissi-Wallet auf Ihrem Smartphone und loggen Sie sich mit der PIN „112233“ ein.

2. Einkaufen im Online-Shop A: Kaufen Sie Weihnachtsprodukte im Online-Shop A und exportieren Sie die Shoppingdaten in die Wallet, indem Sie den QR-Code mit der Lissi-Wallet scannen.

3. Datenteilung für Online-Shop B: Besuchen Sie Online-Shop B und scannen Sie den QR-Code mit der Lissi-Wallet. Teilen Sie die Daten aus der Wallet mit Online-Shop B. Laden Sie die Seite von Online-Shop B neu und prüfen Sie, ob personalisierte Angebote basierend auf den geteilten Daten angezeigt werden.

4. Einstellungen der Wallet ändern: (a) PIN ändern: Navigieren Sie zu den Einstellungen, geben Sie die PIN „112233“ ein und ändern Sie die PIN zu „223344“. (b) Backup erstellen: Speichern Sie die Backup-Datei und notieren Sie den Wiederherstellungsschlüssel. (c) Anmeldeinformationen und Kontakte löschen: Löschen Sie die Kontakte der Online-Shops und die Shoppingdaten in der Wallet. (d) Sprache ändern: Stellen Sie die Wallet-Sprache in den Einstellungen auf Englisch um. (e) Wallet wiederherstellen: Verwenden

[63] https://doi.org/10.5281/zenodo.15114275

Sie das zuvor gespeicherte Backup, um die Wallet wiederherzustellen und prüfen Sie, ob alle ursprünglichen Daten wiederhergestellt wurden.

Der MU bereitete das Endgerät gemäß der Thinking aloud-Anleitung vor. Dazu installierte der MU die Lissi-Wallet auf einem iPhone 14 Pro. Die Evaluation der Lissi-Wallet beschränkt sich damit ausschließlich auf die iOS-Version. Versionen der Lissi-Wallet für andere Betriebssysteme – wie etwa Android – blieben außerhalb des Evaluationsumfangs und könnten spezifische Abweichungen in Funktion oder Interaktion aufweisen. Darüber hinaus richtete der MU den Demo-Shop auf einem Computer ein.

Output von Schritt 2 war die vorbereitete benutzerbasierte Evaluation, das heißt, die akquirierten WU, die Liste der Testfälle, die Anleitung für das Thinking aloud und das eingerichtete Endgerät für das Thinking aloud.

Schritt 3 – Durchführung der benutzerbasierten Evaluation:

Input von Schritt 3 war die vorbereitete benutzerbasierte Evaluation, das heißt, die akquirierten WU, die Liste der Testfälle, die Anleitung für das Thinking aloud und das eingerichtete Endgerät für das Thinking aloud.

Schritt 3, Aktivität 1 – Start der WU-Aufnahmen, Aktivität 2 – Durchführung des Thinking aloud und Aktivität 3 – Abschluss und Speicherung der WU-Aufnahmen: Zu Beginn gab der MU jedem WU die ausgedruckte Thinking aloud-Anleitung mit den Aufgaben, die jeder WU in der Wallet durchführen sollte. Danach startete der MU die Aufnahme des Smartphone-Bildschirms und die Bild- und Tonaufzeichnung des WU. Jeder WU führte Thinking aloud mithilfe der ausgedruckten Thinking aloud-Anleitung durch. Anschließend stoppte der MU die WU-Aufnahme und archivierte diese mit einem Verweis auf die demografischen Daten.

Output von Schritt 3 waren die WU-Aufnahmen des Thinking aloud. Die WU-Aufnahmen wurden mittlerweile aus Datenschutzgründen gelöscht und sind somit nicht einsehbar. Allerdings wurden die daraus identifizierten Stärken und Schwächen der Lissi-Wallet dokumentiert (siehe Schritt 4, Aktivität 1).

Schritt 4 – Auswertung der benutzerbasierten Evaluationsergebnisse:

Input von Schritt 4 waren die WU-Aufnahmen des Thinking aloud aus Schritt 3.

Schritt 4, Aktivität 1 – Sammlung von Stärken und Schwächen der UX und Informationssicherheit: Der MU, UXE and ISE sichteten die WU-Aufnahmen des Thinking aloud.

Dabei dokumentierten sie Stärken und Schwächen der UX und Informationssicherheit der Lissi-Wallet. Der Fokus lag dabei auf der Sammlung von Schwächen – Stärken blieben größtenteils unbeachtet. Für die Dokumentation nutzten sie eine Vorlage: ID, Name, Beschreibung, ob es eine Stärke oder Schwäche ist, ob es UX oder Informationssicherheit betrifft, die betroffenen Attribute der UX oder Informationssicherheit und die betroffenen Wallet-Funktionen. So wurden 10 UX-Stärken, 3 Informationssicherheit-Stärken, 40 UX-Schwächen und 12 Informationssicherheit-Schwächen identifiziert. Tabelle 28 zeigt ein Beispiel einer Informationssicherheit-Schwäche. Tabelle 29 zeigt ein Beispiel einer UX-Schwäche. Alle identifizierten Stärken und Schwächen der UX und Informationssicherheit sind online verfügbar[64].

ID	27
Name	Fehlender Hinweis, dass andere Applikationen auf die Zwischenablage zugreifen könnten.
Beschreibung	WU könnten sich nicht bewusst sein, dass andere Applikationen auf die Zwischenablage zugreifen könnten. Dies ist beispielsweise kritisch, wenn der Backup-Schlüssel in die Zwischenablage kopiert wird.
Stärke/Schwäche	Schwäche
UX/Informationssicherheit	Informationssicherheit
Attribute	Vertraulichkeit
Wallet-Funktionen	Erstellung eines Backups

Tabelle 28: Lissi-Wallet – Beispiel einer Informationssicherheit-Schwäche. (Sauer u. a., 2026). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

ID	60
Name	Die Navigationsleiste ist nicht intuitiv
Beschreibung	Die Übersicht der gespeicherten VC wurde in der Lissi-Wallet nicht gefunden, vermutlich aufgrund des Namens „Wallet“ anstatt beispielsweise „Nachweise“. Zusätzlich wurde die Navigationsleiste nicht als Navigationsleiste identifiziert.
Stärke/Schwäche	Schwäche
UX/Informationssicherheit	UX
Attribute	Nützlichkeit, Auffindbarkeit, Usability
Wallet-Funktionen	Übersicht gespeicherter VC, Übersicht von Kontakten, Suche

Tabelle 29: Lissi-Wallet – Beispiel einer UX-Schwäche. (Sauer u. a., 2026). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

[64] https://doi.org/10.5281/zenodo.15114275

Schritt 4, Aktivität 2 – Ableitung und Zusammenfassung von Heuristiken der UX und Informationssicherheit: Der MU, UXE und ISE formulierten 6 UX- und 9 Informationssicherheit-Heuristiken auf Basis der identifizierten Stärken und Schwächen der Lissi-Wallet aus Aktivität 4.1. Die UX- und Informationssicherheit-Heuristiken wurden mit einer Vorlage erstellt: ID, Name, Beschreibung, ob UX oder Informationssicherheit betroffen ist, die betroffenen Attribute von UX oder Informationssicherheit und die betroffenen Wallet-Funktionen. Tabelle 30 zeigt beispielhaft eine Informationssicherheit-Heuristik. Tabelle 31 zeigt beispielhaft eine UX-Heuristik. Alle UX- und Informationssicherheit-Heuristiken sind online verfügbar[65].

ID	158
Name	Alle in einem VC gespeicherten Daten sollten für WU sichtbar sein
Beschreibung	Wenn nicht alle Daten eines VC für WU sichtbar sind, ist ein verdeckter Informationsaustausch (Sneaking als eine Art eines Dark Pattern, siehe Abschnitt 3.4) zwischen Aussteller und Prüfer von VC möglich.
UX/Informationssicherheit	Informationssicherheit
Attribute	Verfügbarkeit
Wallet-Funktionen	Speicherung von VC, Teilen von VC, Detailansicht gespeicherter VC

Tabelle 30: Lissi-Wallet – Beispiel einer Informationssicherheit-Heuristik. (Sauer u. a., 2026). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

ID	120
Name	Hilfe und Anleitung
Beschreibung	WU sollten einen einfachen Zugang zu strukturierten Hilfefunktionen und Anleitungen haben, um das Verständnis der Wallet zu erhöhen. Eine Suchfunktion sollte vorhanden sein. Hilfstexte sollten verständlich bereitgestellt werden.
UX/Informationssicherheit	UX
Attribute	Nützlichkeit, Auffindbarkeit, Usability, Barrierefreiheit, Glaubwürdigkeit

[65] https://doi.org/10.5281/zenodo.15114275

Wallet-Funktionen	Übersicht gespeicherter VC, Detailansicht gespeicherter VC, Zurücksetzen der Wallet, Erstellung von Backups, Wiederherstellung von Backups, Suche, Automatische Vorauswahl von zu teilenden VC, Löschen von VC, Löschen von Kontakten, Übersicht von Kontakten, Speicherung von VC, Teilen von VC

Tabelle 31: Lissi-Wallet – Beispiel einer UX-Heuristik. (Sauer u. a., 2026). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Schritt 4, Aktivität 3 – Sammlung der abgeleiteten Heuristiken erstellen: Diese Aktivität wurde automatisiert durch das Software-Tool während Aktivität 4.2 ausgeführt.

Output von Schritt 4 war die Sammlung von abgeleiteten Heuristiken der UX und Informationssicherheit.

Schritt 5 – Vorbereitung der expertenbasierten Evaluation:

Input von Schritt 5 war die Sammlung von abgeleiteten Heuristiken der UX und Informationssicherheit.

Schritt 5, Aktivität 1 – Heuristiken aus einer externen Sammlung auswählen und zur eigenen Sammlung an Heuristiken hinzufügen: Nach der Erstellung der Heuristiken (Aktivität 4.2) auf Basis der identifizierten Stärken und Schwächen (Aktivität 4.1) adaptierten MU, UXE und ISE weitere Heuristiken aus 3 Sammlungen externer Heuristiken von Nielsen (1994), von Sauer u. a. (2025c) und von Sauer u. a. (2025a). Dabei wurden 4 neue UX-Heuristiken hinzugefügt. Außerdem wurde eine Informationssicherheit-Heuristik um die Wiederherstellung von Backups erweitert. Somit bestanden nach der Erweiterung der eigenen Heuristiken um die externen Heuristiken 10 UX- und 9 Informationssicherheit-Heuristiken. Die detaillierten Heuristiken sind online verfügbar[66].

Schritt 5, Aktivität 2 – Literaturrecherche von Stärken, Schwächen und Heuristiken der UX und Informationssicherheit und Aktivität 3 – Ableitung von Heuristiken der UX und Informationssicherheit und Hinzufügen zur eigenen Sammlung: Diese beiden Aktivitäten sind optional und sollten nur durchgeführt werden, wenn nicht alle definierten Wallet-Funktionen durch UX- und Informationssicherheit-Heuristiken abgedeckt sind. Da dies nicht gegeben war, wurden beide Aktivitäten übersprungen und damit nicht evaluiert.

[66] https://doi.org/10.5281/zenodo.15114275

Schritt 5, Aktivität 4 – Aktualisierung sicherheitsrelevanter Softwarekomponenten und potenzieller Angreifer und Aktivität 5 – Aktualisierung des Umfangs der Informationssicherheitsevaluation: Auf Basis der Adaption der Heuristiken aus Aktivität 5.1 aktualisierten der MU und ISE die potenziellen Angreifer und den Umfang der Informationssicherheitsevaluation gemäß Schritt 1, Aktivität 2 und Aktivität 3. Der MU und ISE fügten hinzu, dass der kopierte Backup-Schlüssel versehentlich über die Zwischenablage an andere Anwendungen weitergegeben werden könnte.

Schritt 5, Aktivität 6 – Gewichtung der Heuristiken festlegen: Der MU, UXE und ISE haben den Heuristiken Gewichte durch Diskussion zugeordnet. Hierzu schlugen der UXE und ISE ein Gewicht für die jeweiligen Heuristiken ihres Fachgebiets vor. Die endgültige Gewichtung nahm der MU unter Abwägung der fachlichen Einschätzungen des UXE und ISE vor. Die Gewichte liegen zwischen 1 (nicht wichtig) und 5 (sehr wichtig). Die definierten Gewichte wurden in der eigenen Sammlung an Heuristiken festgehalten. Diese ist online verfügbar[67].

Output von Schritt 5 war die Sammlung von gewichteten Heuristiken der UX und Informationssicherheit.

Schritt 6 – Durchführung der expertenbasierten Evaluation:

Input von Schritt 6 war die Sammlung von gewichteten Heuristiken der UX und Informationssicherheit.

Schritt 6, Aktivität 1 – Test der definierten Wallet-Funktionen und Festlegung der Erfüllungsgrade je Heuristik: Der UXE und ISE führten eine Heuristische Evaluation (siehe Abschnitt 5.2.2) durch. Das heißt, sie bedienten die ausgewählten Wallet-Funktionen und legten für jede UX- und Informationssicherheit-Heuristik einen Erfüllungsgrad von 0 (nicht erfüllt) bis 5 (voll erfüllt) fest. Die UX- und Informationssicherheit-Heuristiken mit deren Erfüllungsgraden sind online verfügbar[68]. Die Erfüllungsgrade dienen später für die Berechnung der Scores für UX und Informationssicherheit in Schritt 7.

Schritt 6, Aktivität 2 – Feedback-Diskussion und Aktivität 3 – Anpassung der Heuristiken: Der MU, UXE und ISE besprachen, ob bei der Heuristischen Evaluation Probleme mit den Heuristiken aufgetreten sind. Es traten keine Probleme auf, sodass die Aktivität 6.3 übersprungen und damit nicht evaluiert wurde.

[67] https://doi.org/10.5281/zenodo.15114275
[68] https://doi.org/10.5281/zenodo.15114275

Schritt 6, Aktivität 4 – Erstellung der Interaktionsmatrix der Heuristiken: In der Interaktionsmatrix (siehe Abschnitt 6.1) wurden Interaktionseigenschaften (komplementär, konkurrierend und neutral) zwischen Heuristiken festgehalten. Eine Heuristik A ist komplementär zu einer Heuristik B, wenn Heuristik A Heuristik B positiv beeinflusst. Eine Heuristik B ist konkurrierend zu einer Heuristik B, wenn Heuristik A Heuristik B negativ beeinflusst. Eine Heuristik A ist neutral zu einer Heuristik B, wenn Heuristik A Heuristik B nicht (nennenswert) beeinflusst. Der MU, UXE und ISE fügten zunächst Heuristiken ohne Interaktionseigenschaften der Interaktionsmatrix hinzu. Aufgrund der hohen Anzahl an Heuristiken wurde eine Vorauswahl der Heuristiken getroffen, sodass nur konkurrierende Heuristiken in die Interaktionsmatrix aufgenommen wurden, da für konkurrierende Heuristiken später Konfliktlösungen identifiziert werden mussten. Komplementäre und neutrale Heuristiken dienen später unmittelbar als Basis für die Definition von Verbesserungsvorschlägen, da sie sich nicht negativ beeinflussen. Insgesamt wurden 8 der 19 Heuristiken in die Interaktionsmatrix aufgenommen. Tabelle 32 zeigt einen Ausschnitt der Interaktionsmatrix (bereits mit den Interaktionseigenschaften, die in der nächsten Aktivität zugeordnet wurden). Die gesamte Interaktionsmatrix ist online verfügbar[69].

Schritt 6, Aktivität 5 – Interaktionsmatrix durch Diskussion ausfüllen: Der MU, UXE und ISE legten die Interaktionseigenschaften der 8 ausgewählten Heuristiken aus Aktivität 6.4 zu den jeweiligen anderen Heuristiken durch Diskussion fest. Dabei wurden alle Heuristiken paarweise gegenübergestellt, um zu bestimmen, ob zwischen ihnen eine komplementäre, konkurrierende oder neutrale Beeinflussung besteht. Ziel ist es, zu klären, inwiefern sich 2 Heuristiken gegenseitig beeinflussen. So wurden insgesamt 11 konkurrierende Heuristiken, 22 komplementäre Heuristiken und 23 neutrale Heuristiken identifiziert. Tabelle 32 zeigt einen Ausschnitt der Interaktionsmatrix. Die gesamte Interaktionsmatrix ist online verfügbar[70]. Jede Zeile stellt die Beeinflussung einer Heuristik auf andere Heuristiken dar, während eine Spalte angibt, wie eine Heuristik von anderen Heuristiken beeinflusst wird. Zum Beispiel hat Heuristik 151 „Authentifizierung“ negative Auswirkungen auf Heuristik 123 „Effiziente und intuitive Interaktion“. Das bedeutet, dass Heuristik 151 konkurrierend zu Heuristik 123 ist, da Authentifizierungsmechanismen verschiedene Interaktionen des Benutzers unterbrechen können. Heuristik 123 „Effiziente und intuitive Interaktion“ hat keinen (nennenswerten) Einfluss auf Heuristik 151 „Authentifizierung“. Das heißt, Heuristik 123 ist neutral zu Heuristik 151, da effiziente und intuitive Interaktionen keinen (nennenswerten) Einfluss auf den Schutz der Wallet durch Authentifizierung haben. Heuristik 151 „Authentifizierung“ hat einen positiven Einfluss auf Heuristik 152 „Verhinderung von sicherheitskritischen Aktionen“.

[69] https://doi.org/10.5281/zenodo.15114275
[70] https://doi.org/10.5281/zenodo.15114275

Das heißt, Heuristik 151 ist komplementär zu Heuristik 152, da sicherheitskritische Aktionen durch Authentifizierung verhindert werden können.

	123: Effiziente und intuitive Interaktion	151: Authentifizierung	152: Verhinderung von sicherheitskritischen Aktionen
123: Effiziente und intuitive Interaktion	-	Neutral	Neutral
151: Authentifizierung	Konkurrierend	-	Komplementär
152: Verhinderung von sicherheitskritischen Aktionen	Konkurrierend	Komplementär	-

Tabelle 32: Lissi-Wallet – Ausschnitt der Interaktionsmatrix. (Sauer u. a., 2026). Übersetzt aus dem Englischen.

Schritt 6, Aktivität 6 – Hinzufügen der Interaktionseigenschaften zur Heuristik-Sammlung: Das Software-Tool fügte die Interaktionseigenschaften automatisiert der eigenen Sammlung an Heuristiken hinzu.

Output von Schritt 6 war einerseits die Interaktionsmatrix mit den Interaktionseigenschaften der Heuristiken und andererseits die Heuristiken mit deren Erfüllungsgraden.

Schritt 7 – Auswertung der expertenbasierten Evaluationsergebnisse:

Input von Schritt 7 waren die Heuristiken mit deren Erfüllungsgraden.

Schritt 7, Aktivität 1 – Aggregation der Heuristik-Scores auf Ebene der UX- und Informationssicherheit-Attribute: Zunächst bestimmte der MU den Einzelscore aller Heuristiken. Der Einzelscore einer Heuristik ist das Produkt aus dem Gewicht und dem Erfüllungsgrad einer Heuristik. Der MU bestimmte als nächstes den Gesamtscore (GS) pro Attribut der UX und Informationssicherheit. Der GS eines Attributs ist die Summe der Einzelscores aller Heuristiken, die diesem Attribut zugeordnet sind. Die GS der UX-Attribute sind in der ersten Zeile von Tabelle 33 einsehbar. Die GS der Informationssicherheit-Attribute sind in der ersten Zeile von Tabelle 34 einsehbar. Um den durchschnittlichen Gesamtscore (ØGE) eines UX- und Informationssicherheit-Attributs zu ermitteln, wurde der Gesamtscore (GS) durch die Anzahl der zugehörigen Heuristiken geteilt. Die ØGE sind in der zweiten Zeile von Tabelle 33 und Tabelle 34 zu finden. Der maximal mögliche Gesamtscore (MGS) eines Attributs ergibt sich aus dem Produkt des Gewichts und dem maximalen Erfüllungsgrad (siehe dritte Zeile von Tabelle 33 und Tabelle 34). Abschließend wurde das Verhältnis (Ratio) zwischen dem ØGE und dem ØMGE berechnet. Dieses

Verhältnis gibt an, inwieweit ein UX- oder Informationssicherheit-Attribut erfüllt ist – von 0 (nicht erfüllt) bis 1 (vollständig erfüllt). Die Werte der Verhältnisse sind in der fünften Zeile von Tabelle 33 und Tabelle 34 einsehbar.

	UX						
	Nützlichkeit	Begehrlichkeit	Auffindbarkeit	Usability	Barrierefreiheit	Glaubwürdigkeit	Wert
GS	93	47	45	102	69	55	23
ØGE	10,33	9,4	9	10,2	9,86	11	11,5
MGS	160	88	84	172	128	84	36
ØMGS	17,78	17,6	16,8	17,2	18,29	16,8	18
Ratio	0,58	0,53	0,54	0,59	0,54	0,65	0,64

Tabelle 33: Lissi-Wallet – Scores der UX-Attribute. (Sauer u. a., 2026). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

	Informationssicherheit		
	Vertraulichkeit	Integrität	Verfügbarkeit
GS	65	47	27
ØGE	10,83	15,67	13,5
MGS	108	52	36
ØMGS	18	17,33	18
Ratio	0,60	0,9	0,75

Tabelle 34: Lissi-Wallet – Scores der Informationssicherheit-Attribute. (Sauer u. a., 2026). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Schritt 7, Aktivität 2 – Aggregation der Heuristik-Scores auf Ebene von UX und Informationssicherheit: Da für jedes Attribut der UX und Informationssicherheit ein Score in Schritt 7, Aktivität 1 berechnet wurde, war es möglich, einen Score für die UX und Informationssicherheit zu berechnen. Um den Score für die UX zu berechnen, wurde zunächst der Durchschnitt aller MGS der UX-Attribute berechnet (= 10,2). Anschließend wurde der Durchschnitt aller ØMGS der UX-Attribute berechnet (= 17,2). Danach wurde das Verhältnis beider Werte bestimmt (= 0,59), was den Score der UX ergibt. Gleichermaßen wurde bei der Berechnung des Informationssicherheit-Score vorgegangen. Zunächst wurde der Durchschnitt aller MGS der Informationssicherheit-Attribute berechnet (= 11,56). Anschließend wurde der Durchschnitt aller ØMGS der Informationssicherheit-Attribute berechnet (= 17,33). Schließlich wurde das Verhältnis beider Werte bestimmt (= 0,67), was den Score der Informationssicherheit ergibt. Die berechneten Scores der UX und Informationssicherheit können in einer weiteren Anwendung der MEUSec-Methode verwendet werden, um zu überprüfen, ob die Verbesserungsvorschläge aus Schritt 8 zu messbaren Verbesserungen der Wallet geführt haben.

Schritt 7, Aktivität 3 – Eigene Sammlung der Heuristiken zu externer Sammlung der Heuristiken hinzufügen: Der MU hat die Heuristiken im Software-Tool veröffentlicht, sodass sie in der externen Heuristik-Sammlung im Software-Tool verfügbar sind (für andere Personen und für weitere Iterationen der MEUSec-Methode).

Output von Schritt 7 waren die Scores der UX und Informationssicherheit. Die eigene Heuristik-Sammlung wurde in der externen Sammlung im Software-Tool veröffentlicht.

Schritt 8 – Verbesserung von UX und Informationssicherheit:

Input von Schritt 8 war die Interaktionsmatrix aus Schritt 6.

Schritt 8, Aktivität 1 – Lösungen für konkurrierende Heuristiken finden und Aktivität 2 – UX oder Informationssicherheit priorisieren: Der MU, ISE und UXE suchten zunächst nach Konfliktlösungen für die 11 konkurrierenden Heuristiken aus Aktivität 6.5. Als Konfliktlösungen wurden für 4 der 11 konkurrierenden Heuristiken entweder die UX-Heuristik oder die Informationssicherheit-Heuristiken priorisiert. Zum Beispiel kann die Informationssicherheit-Heuristik 135 „Benutzer sollten darauf hingewiesen werden, dass der Inhalt der Zwischenablage von anderen Anwendungen gelesen werden kann“ die UX-Heuristik 131 „Ästhetisches und minimalistisches Design“ negativ beeinflussen. Der MU, ISE und UXE haben die Informationssicherheit-Heuristik 135 priorisiert. Somit diente die Informationssicherheit-Heuristik 135 als Grundlage für die Formulierung des zugehörigen Verbesserungsvorschlags. Als Konfliktlösungen wurden für 7 der 11 konkurrierenden Heuristiken Kompromisslösungen festgelegt. Zum Beispiel kann Heuristik 120 „Hilfe und Anleitung“ die Heuristik 131 „Ästhetisches und minimalistisches Design“ negativ beeinflussen, wenn zu viele Hilfshinweise in der Lissi-Wallet erscheinen. Als Kompromisslösung sollte die Lissi-Wallet nur relevante Hilfshinweise anzeigen, um das User Interface übersichtlich zu halten. Die 11 Konfliktlösungen dienen als Verbesserungsvorschläge für die Lissi-Wallet.

Die gesamten 11 Verbesserungsvorschläge sind online verfügbar[71].

Schritt 8, Aktivität 3 – Verbesserungsvorschläge auf Basis der komplementären und neutralen Heuristiken formulieren: Die 22 komplementären Heuristiken und die 23 neutralen Heuristiken aus Aktivität 6.5 konnten unmittelbar als Grundlage für die Formulierung der Verbesserungsvorschläge verwendet werden, da sie sich nicht gegenseitig negativ beeinflussen.

[71] https://doi.org/10.5281/zenodo.15114275

Insgesamt formulierten der MU, ISE und UXE 25 Verbesserungsvorschläge (einschließlich der 11 Verbesserungsvorschläge aus Aktivität 8.2).

Tabelle 35 zeigt einige der Verbesserungsvorschläge mit den zugehörigen Heuristiken, auf deren Basis die Verbesserungsvorschläge formuliert wurden. Die gesamten 25 Verbesserungsvorschläge sind online verfügbar[72].

ID	Beschreibung	Zugehörige Heuristiken
18	Nach der Ausführung von Wallet-Funktionen sollten Benutzer entsprechendes Feedback erhalten, beispielsweise nach der Freigabe von Anmeldedaten oder der PIN-Änderung.	123, 139
21	Die Bezeichnung des Navigationstabs „Wallet“ sollte präziser gewählt werden, etwa durch eine eindeutigere Formulierung wie „Nachweise“.	123
25	Das Abbrechen von Benutzer-Aktionen sollte immer möglich sein. Zudem sollten Hinweise zum Abbrechen von Benutzer-Aktionen verständlich formuliert sein, wie beispielsweise beim Abbrechen einer Backup-Erstellung.	124, 138
26	Fehlermeldungen sollten aussagekräftig sein und Lösungen anbieten, beispielsweise wenn gespeicherte VC ablaufen und abgelaufen sind.	125
28	Der Verifizierungsstatus der Aussteller und Prüfer von VC sollte visuell ersichtlicher sein. Außerdem sollten weitere Informationen zum Verifizierungsstatus geboten werden.	128
30	Benutzer sollten eine Warnmeldung erhalten, die sie bestätigen müssen, bevor sie Aktionen mit weitreichenden Folgen durchführen, wie die Änderung der Spracheinstellungen.	139
31	Die Wallet sollte eine einheitliche Terminologie verwenden.	140
33	Benachrichtigungen über sicherheitsrelevante Aktionen sollten angezeigt werden, wie über regelmäßige Backups und zeitnah ablaufende VC.	153
34	Benutzer sollten informiert werden, welche Daten beim Erstellen eines Backups gesichert werden. Zudem sollten die zu sichernden Daten auswählbar sein.	153

Tabelle 35: Lissi-Wallet – Ausschnitt der Verbesserungsvorschläge. (Sauer u. a., 2026). Übersetzt aus dem Englischen und begrifflich angepasst an die in dieser Arbeit verwendeten Notationen.

Zusätzlich verwendeten der MU, ISE und UXE den optionalen Schieberegler im Software-Tool, um einen gewünschten UX- und Informationssicherheit-Score einzustellen, um entsprechende Verbesserungsvorschläge zu erhalten. Die UX- und Informationssi-

[72] https://doi.org/10.5281/zenodo.15114275

cherheit-Scores können mithilfe des Schiebereglers beliebig angepasst werden, bis die maximalen Erfüllungsgrade der komplementären und neutralen Heuristiken erreicht sind. Von dort an sinkt der jeweils andere Score (UX oder Informationssicherheit). Der MU, ISE und UXE legten 92% für UX und 89% für Informationssicherheit fest. Als Ergebnis schlug das Software-Tool 28 Heuristiken vor, die als Verbesserungsvorschläge dienen. Das heißt, die Erfüllungsgrade der ausgegebenen Heuristiken müssen maximiert werden, um die eingestellten UX- und Informationssicherheit-Scores zu erreichen. Bei anderen eingestellten Prozentzahlen wären entsprechend andere Heuristiken ausgegeben worden. Das Verfahren zur Ermittlung der entsprechenden Heuristiken auf Basis der eingestellten UX- und Informationssicherheit-Scores wurde bereits in Abschnitt 8.4 beschrieben und in Abbildung 32 visualisiert.

Die Liste der 28 Verbesserungsvorschläge ist online verfügbar[73].

Output von Schritt 8 waren die Verbesserungsvorschläge der UX und Informationssicherheit für die Lissi-Wallet.

9.3 Einordnung der Stärken und Schwächen der Lissi-Wallet

Im Folgenden werden die identifizierten Stärken und Schwächen der Lissi-Wallet mit denen anderer Wallets verglichen, darunter auch mit denen der Hidy-Wallet aus Abschnitt 7.2. Da der Schwerpunkt der Evaluation der Lissi-Wallet und der Hidy-Wallet auf der Identifikation von Schwächen lag, wurden vor allem Schwächen dokumentiert, während Stärken weitgehend unberücksichtigt blieben.

Unverständliche und inkonsistente Begriffe sind nicht nur in der Hidy-Wallet, sondern auch in der Lissi-Wallet zu finden. Beispielsweise wird in der Lissi-Wallet der Begriff „Wallet“ als Bezeichnung für die VC-Übersicht in der Navigationsleiste verwendet, während in der Hidy-Wallet der Begriff „Lightning Wallet“ genutzt wird. Darüber hinaus stellten Sartor u. a. (2022) und Sauer u. a. (2025b) fest, dass einige in den evaluierten Wallets verwendeten Begriffe durch Benutzer nicht verstanden wurden. Dies lag vor allem an einer zu technisch geprägten Sprache. Unverständliche und inkonsistente Begriffe stehen im Widerspruch zu den Design Guidelines „Use of understandable terms“ und „Use of consistent terms“ für Wallets von Sellung & Kubach (2023). Unverständliche und inkonsistente Begriffe in Wallets können dazu führen, dass Benutzer Sicherheitsfunktionen falsch interpretieren und ungewollt sicherheitskritische Aktionen durchführen.

[73] https://doi.org/10.5281/zenodo.15114275

Außerdem leidet die Barrierefreiheit der Wallet aufgrund der Verwendung von zu technischen Begriffen, da die Benutzung für weniger technikaffine Personen erschwert wird.

Sowohl die Lissi-Wallet als auch die Hidy-Wallet gaben im Fehlerfall oft keine aussagekräftigen Rückmeldungen. Beispielsweise erschien in der Lissi-Wallet die Fehlermeldung „Ein Fehler ist aufgetreten“ beim Einsehen der Interaktionen mit VC-Ausstellern und VC-Prüfern. In der Hidy-Wallet erschien beispielsweise die Fehlermeldung „Erstellung fehlgeschlagen“ bei der Anforderung einer Zahlung, wenn keine Internetverbindung bestand. Nicht aussagekräftige Fehlermeldungen widersprechen der Design Guideline „Error handling“ von Sellung & Kubach (2023).

Wie bereits bei der Hidy-Wallet wurde auch bei der Lissi-Wallet deutlich, dass die grundsätzliche Funktionsweise der Wallet für einige Probanden nicht verständlich war. Bei beiden Wallets fehlten Hilfshinweise, wie beispielsweise ein einführendes Tutorial. Auch Probanden von Korir u. a. (2022) und Sauer u. a. (2025b) haben die grundsätzliche Funktionsweise der Wallet nicht verstanden. Diese Schwäche widerspricht der Design Guideline „User Onboarding“ von Sellung & Kubach (2023).

Sowohl in der Lissi-Wallet als auch in der Hidy-Wallet wurden den Probanden in der Detailansicht von VC nicht alle gespeicherten Daten angezeigt. Dies ermöglicht einen verdeckten Datenaustausch zwischen Ausstellern und Prüfern von VC. Auch Sauer u. a. (2025b) identifizierten die gleiche Schwäche im Rahmen einer Wallet-Evaluation. Diese Schwäche widerspricht der Design Guideline „Transparent information on data storage“ von Sellung & Kubach (2023).

Wie sich im Rahmen der Evaluation der Lissi-Wallet zeigte, hatten auch Probanden von Satybaldy (2023) Probleme mit der Erstellung des Wallet-Backups aufgrund der zu hohen Komplexität. Diese Schwächen widersprechen den Design Guidelines „User friendly and transparent backup options”, „Simplicity of use” und „Visible reminders to back up data” von Sellung & Kubach (2023).

Die Lissi-Wallet verfügte zwar über eine Suchfunktion für VC, jedoch nicht über eine Suchfunktion innerhalb der Einstellungen. Diese Schwäche widerspricht der Design Guideline „Search & filter“ von Sellung & Kubach (2023).

In der Lissi-Wallet gelang es den Probanden – ebenso wie zuvor in der Hidy-Wallet –, verschiedene Funktionen ohne Schwierigkeiten zu finden. So wurden beispielsweise in der Hidy-Wallet die Seite zum Zahlungen tätigen, die Seite zum Ändern der PIN und die Seite zum Ändern der Sprache problemlos gefunden. Diese Stärke steht im Einklang mit der Design Guideline „Simplicity of Use“ von Sellung & Kubach (2023).

9.4 Evaluationsergebnisse der MEUSec-Methode

Im Folgenden werden die Evaluationsergebnisse der MEUSec-Methode beschrieben. Zunächst werden die Evaluationsergebnisse anhand der Evaluationskriterien aus Abschnitt 7.1 erläutert. Anschließend werden die aus den Evaluationsergebnissen abgeleiteten Verbesserungsvorschläge im Einzelnen erläutert.

(E1) Qualität der Methodenartefakte:

(E1.1) Vollständigkeit:

- Alle Wallet-Funktionen wurden hinsichtlich UX und Informationssicherheit evaluiert. Allerdings wurde nicht jeder Wallet-Funktion eine UX- und Informationssicherheit-Heuristik zugeordnet. Dies liegt daran, dass es Wallet-Funktionen gab, bei denen UX oder Informationssicherheit nicht sinnvoll bewertet werden konnten, wie beispielsweise die Informationssicherheit der Suchfunktion (die stattdessen nur hinsichtlich UX evaluiert wurde).
- Alle Interaktionseigenschaften von Heuristiken konnten festgelegt werden.
- Für jede nicht erfüllte Heuristik konnte mindestens ein Verbesserungsvorschlag unter Berücksichtigung der Interaktionseigenschaften identifiziert werden.
- Insgesamt bewerteten der UXE, ISE und MU das Evaluationskriterium der Vollständigkeit als erfüllt.

(E1.2) Konsistenz:

- Mithilfe eines standardisierten Bewertungsschemas konnten der Erfüllungsgrad aller definierten Heuristiken und deren Interaktionseigenschaften bewertet werden.
- Es wurden keine widersprüchlichen Verbesserungsvorschläge formuliert.
- Insgesamt bewerteten der UXE, ISE und MU das Evaluationskriterium der Konsistenz als erfüllt.

(E1.3) Korrektheit:

- Die Korrektheit der Methodenartefakte konnte nicht ausreichend bewertet werden, da die MEUSec-Methode nicht auf die verbesserte Wallet angewendet wurde. So konnte anhand der UX- und Informationssicherheit-Scores nicht geprüft werden, ob die Verbesserungsvorschläge zu messbaren Verbesserungen geführt haben.
- Die Verbesserungsvorschläge der Lissi-Wallet wurden jedoch systematisch auf Basis der identifizierten Schwächen und der Heuristiken mit ihren Interaktionseigenschaften formuliert. Daher gehen der UXE, ISE und MU davon aus, dass die Verbesserungsvorschläge plausibel sind.

(E1.4) Nachvollziehbarkeit:

- Der Rechenweg der UX- und Informationssicherheit-Scores wurde durch den UXE, ISE und MU als nachvollziehbar bewertet.
- Die Priorisierung der konkurrierenden Heuristiken und deren Begründungen sind nachvollziehbar.
- Die identifizierten Verbesserungsvorschläge sind nachvollziehbar.
- Insgesamt bewerteten der UXE, ISE und MU das Evaluationskriterium der Nachvollziehbarkeit als erfüllt.

(E1.5) Eindeutigkeit:

- Die Heuristiken, ihre Interaktionseigenschaften und die Verbesserungsvorschläge wurden aufgrund der vorgegebenen Vorlage eindeutig formuliert.
- Insgesamt bewerteten der UXE, ISE und MU das Evaluationskriterium der Eindeutigkeit als erfüllt.

(E1.6) Sachdienlichkeit:

- Die UX- und Informationssicherheit-Scores können für eine weitere Iteration der MEUSec-Methode verwendet werden, um zu prüfen, ob die Verbesserungsvorschläge zu messbaren Verbesserungen geführt haben.
- Die Heuristiken und ihre Interaktionseigenschaften dienten zur systematichen Formulierung von Verbesserungsvorschlägen.
- Insgesamt bewerteten der UXE, ISE und MU das Evaluationskriterium der Sachdienlichkeit als erfüllt.

(E2) Durchführbarkeit der Methode:

(E2.1) Effektivität:

- Der MU, UXE und ISE verglichen die angestrebten Artefakte mit den gewonnenen Artefakten der MEUSec-Methode.
- Insgesamt wurden 52 Schwächen und 13 Stärken der UX und Informationssicherheit der Lissi-Wallet identifiziert, wobei der Fokus auf den Schwächen anstatt auf den Stärken lag. Außerdem wurden 10 UX-Heuristiken, 9 Informationssicherheit-Heuristiken und 35 Verbesserungsvorschläge der Lissi-Wallet ermittelt.
- Die Evaluation involvierte sowohl Experten als auch Probanden.
- Für die Heuristiken konnten Erfüllungsgrade festgelegt werden, um schlussendlich einen Score für die UX und einen Score für die Informationssicherheit der Lissi-Wallet zu berechnen.

- Mithilfe der Interaktionsmatrix konnten Interaktionseigenschaften zwischen Heuristiken definiert werden.
- Mittels den Interaktionseigenschaften der Heuristiken konnten Verbesserungsvorschläge der Lissi-Wallet identifiziert werden.
- Dies bedeutet, dass alle angestrebten Artefakte gewonnen wurden. Der MU, UXE und ISE bewerteten das Evaluationskriterium der Effektivität als erfüllt.

(E2.2) Effizienz:

- Zur Evaluation der Effizienz der MEUSec-Methode wurden zunächst die von den Durchführenden der Rollen benötigten Zeiten je Schritt gemessen. Insgesamt benötigten der ISE 1564 Minuten (26,07 Stunden), der UXE 1392 Minuten (23,2 Stunden) und der MU 2131 Minuten (35,52 Stunden). Die Summe der Einzelzeiten von ISE, UXE und MU beträgt also 5087 Minuten (84,78 Stunden). Die Gesamtausführungszeit der MEUSec-Methode (da Rollen gemeinsam an Schritten beteiligt sind) beträgt 2241 Minuten (37,35 Stunden). Die Zeit für die WU (in Schritt 3 enthalten) beträgt 334 Minuten (5,57 Stunden). Die gemessenen Zeiten beziehen sich ausschließlich auf die Ausführung der einzelnen Schritte der MEUSec-Methode. Die gemessenen Zeiten umfassen nicht Zeiten für Schulungen der Durchführenden zur Anwendung der MEUSec-Methode und nicht Zeiten zur Umsetzung der identifizierten Verbesserungsvorschläge der Lissi-Wallet. In Tabelle 36 sind die gemessenen Zeiten aufgeführt. Dabei steht „S“ für „Schritt“ der MEUSec-Methode. Die Tabellenzeile „Max(S[x])“ beinhaltet die Zeiten jedes Schritts der MEUSec-Methode, wobei simultane Ausführungen von Schritten durch verschiedene Rollen berücksichtigt werden. Die Tabellenzeile „Total“ hingegen summiert die Zeiten der Rollen, ohne simultane Ausführungen von Schritten zu beachten.

	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**Total**
MU	137	303	464	721	119	150	16	221	2131
UXE	-	104	-	721	71	260	15	221	1392
ISE	124	104	-	721	119	260	15	221	1564
Max(S[x])	137	303	464	721	119	260	16	221	**2241**
Total	261	511	464	2163	309	760	46	663	**5087**

Tabelle 36: Lissi-Wallet – Ausführungszeiten der MEUSec-Methode. (Sauer u. a., 2026).

- Zusätzlich zu den benötigen Zeiten wurden die Kosten berechnet. Für den UXE wurde ein Stundensatz in Höhe von 83€ pro Stunde (für einen UX-Designer), für den ISE ein Stundensatz in Höhe von 101€ pro Stunde (für einen Security-Consultant) und für den MU ein Stundensatz in Höhe von 95€ pro Stunde (für einen IT-

Consultant) angesetzt[74]. Pro WU wurden 20€ berechnet, da jeder WU in der benutzerbasierten Evaluation 20€ erhalten hat. So ergeben sich Kosten in Höhe von 1.929,60€ für den UXE, 2.631,07€ für den ISE, 3.374,08€ für den MU und 260€ für die WU. Insgesamt ergeben sich daraus Kosten in Höhe von 8.194,75€.

- Nach Betrachtung der gemessenen Zeiten und berechneten Kosten sollte eine Bewertung der Effizienz mithilfe der Ausprägungen „erfüllt", „teilweise erfüllt" und „nicht erfüllt" vorgenommen werden. Da kein anderes Verfahren als die MEUSec-Methode zur sowohl experten- als auch endnutzerbasierten Evaluation der Beeinflussung zwischen UX und Informationssicherheit identifiziert werden konnte (siehe Abschnitt 5.2.145.2), erfolgte ein subjektiver Vergleich auf Grundlage der Erfahrungswerte des UXE und ISE mit den recherchierten, ähnlichen Evaluationsverfahren (siehe Abschnitt 5.2). Auf Basis dieses Vergleichs bewerteten der UXE und ISE das Evaluationskriterium der Effizienz als erfüllt.
- Ferner schlugen sie vor, dass zunächst Heuristiken aus den externen Sammlungen von Heuristiken ausgewählt und dann eigene Heuristiken formuliert werden sollten (und nicht umgekehrt). Dies wird die Effizienz weiter erhöhen.

(E2.3) Akzeptanz:

- Insgesamt bewerteten der MU, UXE und ISE das Evaluationskriterium der Akzeptanz als erfüllt, weil sich die MEUSec-Methode für sie als effektiv und effizient erwiesen hat.
- Einzelne Schwachstellen wurden bereits in den Evaluationsergebnissen der vorangegangenen Evaluationskriterien erläutert.

Aus den Evaluationsergebnissen ergaben sich verschiedene Verbesserungsvorschläge der MEUSec-Methode, die im Folgenden beschrieben werden.

1. In den Aktivitäten 1 und 2 von Schritt 8 der MEUSec-Methode sollten Beispiele von Konfliktlösungen gegeben werden, insbesondere um den Detaillierungsgrad der Konfliktlösung vorzugeben. Außerdem sollte der Unterschied zwischen Beschreibung und Argumentation eines Verbesserungsvorschlags verdeutlicht werden.
2. In Aktivität 1 von Schritt 4 sollte es möglich sein, den Stärken und Schwächen einen Schwere- und Häufigkeitsscore zuzuordnen. Diese Scores dienen als Grundlage für die Bewertung der Erfüllungsgrade der Heuristiken und können auch zur Priorisierung der Verbesserungsvorschläge verwendet werden.

[74] Es handelt sich um durchschnittliche Stundensätze von https://freelancermap.de.

3. In Aktivität 1 von Schritt 4 sollte es möglich sein, die ausgewählten WU den Stärken und Schwächen zuzuordnen, um Aussagen über den Zusammenhang zwischen Stärken und Schwächen und bestimmten Benutzergruppen treffen zu können.
4. In Aktivität 1 von Schritt 4 sollten der UXE und ISE die Aufzeichnungen des Thinking aloud jedes WU getrennt betrachten und Stärken sowie Schwächen sammeln, damit sich UXE und ISE nicht gegenseitig beeinflussen. Im Anschluss daran sollte eine gemeinsame Abstimmungsrunde erfolgen, in der Dubletten der erfassten Stärken und Schwächen aufgehoben werden. Output-Artefakt ist eine Liste an Stärken und Schwächen der Wallet.
5. Die Auswahl bestehender Heuristiken aus den externen Sammlungen an Heuristiken sollte erfolgen, bevor eigene Heuristiken auf der Grundlage der ermittelten Stärken und Schwächen definiert werden. Dies bringt Effizienzvorteile und trägt dazu bei, dass die Heuristiken auf einem ähnlichen Abstraktionsniveau formuliert werden. Außerdem wurden die externen Heuristiken bereits evaluiert.
6. Zu Beginn der Durchführung der MEUSec-Methode sollte darauf hingewiesen werden, dass die Schritte und Aktivitäten der MEUSec-Methode möglichst ohne längere Pausen durchgeführt werden, da sonst Informationen vergessen und erneut nachgeschlagen werden müssen, was die Effizienz verringert.

9.5 Evaluationsergebnisse des Software-Tools

Im Folgenden werden die Evaluationsergebnisse des Software-Tools beschrieben. Zunächst werden die Evaluationsergebnisse anhand der Evaluationskriterien aus Abschnitt 9.1 erläutert. Anschließend wird auf die Erfüllung der erhobenen Anforderungen der Anforderungserhebung (siehe Abschnitt 8.2) eingegangen. Danach werden die Verbesserungsvorschläge ausgeführt.

Die Durchführenden der Rollen haben das Software-Tool mithilfe der Evaluationskriterien aus Abschnitt 9.1 bewertet. Die Evaluationsergebnisse werden nun erläutert.

(ET1) Funktionalität des Software-Tools:

(ET1.1) Vollständigkeit:

- Der Experte der Informationssicherheit (ISE), der Experte der UX (UXE) und der Methoden-Anwender (MU) konnten mit dem Software-Tool alle ausgewählten Wallet-Funktionen evaluieren.
- Außerdem konnten der ISE, UXE und MU im Software-Tool bestehende UX- und Informationssicherheit-Heuristiken für den eigenen Gebrauch auswählen.

- Das Software-Tool hat automatisiert Scores für UX und Informationssicherheit auf Basis der Erfüllungsgrade der Heuristiken berechnet. Zur Validierung wurden die Scores manuell – ohne Verwendung des Software-Tools – berechnet.
- Der ISE, UXE und MU konnten das Software-Tool verwenden, um Verbesserungsvorschläge basierend auf den Interaktionseigenschaften zu formulieren. Das Software-Tool zeigte die konkurrierenden Heuristiken nacheinander an, sodass entweder Kompromisslösungen oder Prioritäten zwischen UX und Informationssicherheit dokumentiert werden konnten. Ergänzend dazu wurden komplementäre und neutrale Heuristiken angezeigt, die als eigenständige Verbesserungsvorschläge dokumentiert werden konnten. Des Weiteren moderierte der Methoden-Anwender die Formulierung der Verbesserungsvorschläge und teilte seinen Bildschirm. Auf diese Weise ließ sich das Risiko doppelter Verbesserungsvorschläge reduzieren.
- Zusätzlich ließen sich mithilfe eines Schiebereglers zum Einstellen eines Scores der UX und Informationssicherheit Verbesserungsvorschläge anzeigen.
- Außerdem konnten der ISE, UXE und MU einen Evaluationsbericht generieren und anderen Benutzern Zugriff auf das Evaluationsprojekt gewähren.
- Insgesamt bewerteten der ISE, UXE und MU das Evaluationskriterium der Vollständigkeit als erfüllt.

(ET1.2) Korrektheit:

- Der ISE, UXE und MU bewerteten, dass das Software-Tool die Scores der UX und Informationssicherheit korrekt berechnet. Hierzu wurden die Scores manuell – ohne Verwendung des Software-Tools – berechnet und mit den Ergebnissen des Software-Tools verglichen.
- Außerdem bewerteten der ISE, UXE und MU, dass das Software-Tool dabei unterstützt, systematisch plausible Verbesserungsvorschläge zu formulieren.
- Insgesamt bewerteten der ISE, UXE und MU das Evaluationskriterium der Korrektheit als erfüllt.

(ET1.3) Angemessenheit:

- Der ISE, der UXE und der MU bewerteten, dass das Software-Tool dazu verwendet werden kann, verschiedene Wallet-Funktionen hinsichtlich UX und Informationssicherheit experten- und endnutzerbasiert zu evaluieren und zugehörige Verbesserungsvorschläge zu finden.
- Im Software-Tool lassen sich Heuristiken wiederverwenden und neu hinzufügen.
- Im Software-Tool lassen sich Interaktionseigenschaften für Heuristiken hinzufügen.
- Insgesamt bewerteten der ISE, UXE und MU das Evaluationskriterium der Angemessenheit als erfüllt.

(ET2) UX und Usability:

(ET2.1) Selbstbeschreibungsfähigkeit:

- Die Informationstexte wurden durch den ISE, UXE und MU als teilweise unverständlich bewertet.
- Die Elemente des User Interface waren intuitiv, allerdings wurde teilweise nicht deutlich, welche Aktivitäten der MEUSec-Methode durchgeführt werden sollen.
- Der ISE, der UXE und der MU bewerteten, dass das Software-Tool Artefakte der MEUSec-Methode (wie beispielsweise Verbesserungsvorschläge) übersichtlich darstellt, aber dass die Bedeutung der UX- und Informationssicherheit-Scores fehlt und dass die Interaktionseigenschaften grafisch besser dargestellt werden können.
- Insgesamt bewerteten der ISE, UXE und MU das Evaluationskriterium der Selbstbeschreibbarkeit als teilweise erfüllt.

(ET2.2) Effizienz:

- Das Software-Tool konnte den Zeit- und Ressourcenaufwand im Vergleich zur manuellen Anwendung der MEUSec-Methode ohne Software-Tool (siehe Abschnitt 7.4) reduzieren. So wurden etwa die Scores der UX und Informationssicherheit automatisch berechnet, die Interaktionsmatrix wurde automatisch erstellt (ohne die Interaktionseigenschaften) und es konnten vordefinierte Heuristiken für die eigene Verwendung ausgewählt werden. Die Zeiten der Schritte und Aktivitäten werden in Abschnitt 9.7 diskutiert und mit den Zeiten der manuellen Anwendung der MEUSec-Methode ohne Software-Tool verglichen.
- Insgesamt bewerteten der ISE, UXE und MU das Evaluationskriterium der Effizienz als erfüllt.

(ET2.3) Fehlervermeidung:

- Der ISE, der UXE und der MU bewerteten, dass das Software-Tool dabei hilft, Fehler bei der Eingabe und bei der Anwendung der MEUSec-Methode zu vermeiden. Beispielsweise erschien eine Warnung beim Einfügen von mehreren Wallet-Funktionen, die nicht durch Kommas separiert wurden.
- Insgesamt bewerteten der ISE, UXE und MU das Evaluationskriterium der Fehlervermeidung als erfüllt.

(ET2.4) Akzeptanz:

- Insgesamt bewerteten der ISE, UXE und MU das Evaluationskriterium der Akzeptanz als erfüllt. Grundlage dieser Einschätzung waren die Ergebnisse der 6 zuvor bewerteten Kriterien, von denen 5 als erfüllt und eines als teilweise erfüllt eingestuft

wurden. Da somit ein positives Gesamtbild vorliegt und keine gravierenden Mängel identifiziert wurden, konnte das Kriterium der Akzeptanz als erfüllt bewertet werden.

Zusätzlich bewerteten die Durchführenden der Rollen, welche der erhobenen Anforderungen aus der Anforderungserhebung (siehe Abschnitt 8.2) erfüllt wurden. Insgesamt wurden 50 Anforderungen erfüllt, 4 Anforderungen wurden teilweise erfüllt, 14 Anforderungen wurden nicht erfüllt und 4 Anforderungen konnten nicht bewertet werden.

Nicht erfüllte Anforderungen:

1. Mit dem Software-Tool sollen sich verschiedene Statistiken generieren lassen, wie beispielsweise von Bedrohungsszenarien, deren Eintrittswahrscheinlichkeiten und Schadensausmaße.
2. Im Software-Tool sollen sich Attribute der UX und Informationssicherheit erstellen, bearbeiten und löschen lassen.
3. Im Software-Tool sollen sich externe Sammlungen von Heuristiken bewerten lassen.
4. Im Software-Tool sollen sich Interaktionseigenschaften grafisch darstellen lassen.
5. Das Software-Tool soll konkurrierende Heuristiken grafisch hervorheben.
6. Im Software-Tool sollen sich Rollen erstellen, bearbeiten und löschen lassen.
7. Im Software-Tool soll der Experte der UX und der Experte der Informationssicherheit separat Erfüllungsgrade der Heuristiken festlegen können.
8. Im Software-Tool sollen die separat durch die Experten der UX und Informationssicherheit bewerteten Erfüllungsgrade der Heuristiken ausgewertet werden können.
9. Im Software-Tool sollen die Experten der UX und Informationssicherheit gegenseitig keinen Zugriff auf die Bewertungsfunktion der Erfüllungsgrade von Heuristiken haben.
10. Das Software-Tool soll ein Beispiel zur Auswahl der Anforderungen der Probanden anzeigen.
11. Das Software-Tool soll darüber informieren, wenn das festgelegte Datum zum Löschen personenbezogener Daten, insbesondere von Aufnahmen des Thinking aloud, erreicht wurde.
12. Im Software-Tool sollen sich Statistiken über Probanden generieren lassen.
13. Das Software-Tool soll die Erstellung von demografischen Fragebögen ermöglichen.
14. Das Software-Tool soll auf die DSGVO hinweisen.

Teilweise erfüllte Anforderungen:

1. Das Software-Tool soll es ermöglichen, Schritte zu wiederholen und eine Begründung zu dokumentieren. Es lassen sich zwar Schritte wiederholen, allerdings keine Begründungen dokumentieren.

2. Das User Interface des Software-Tools soll benutzerfreundlich sein. Es wurden Verbesserungsvorschläge hinsichtlich des Designs geäußert, die später bei den Verbesserungsvorschlägen erläutert werden.
3. Das Software-Tool soll einen Schieberegler für den UX-Score und für den Informationssicherheit-Score haben, um Verbesserungsvorschläge für die eingestellten Scores zu bekommen. Es lassen sich ein Score der UX und Informationssicherheit beliebig bis zum Maximum der Erfüllungsgrade komplementärer und neutraler Heuristiken einstellen. Ab diesen Maxima verringert sich der jeweilige andere Score um einen Prozentpunkt. Die negative Beeinflussung könnte zukünftig noch präziser bestimmt werden.
4. Grafische Darstellungen von Evaluationsergebnissen im Software-Tool sollen leicht verständlich und aussagekräftig sein. Beispielsweise war den Durchführenden der Rollen nicht klar, dass die Scores der UX und Informationssicherheit dazu verwendet werden können, um bei erneuter Anwendung der MEUSec-Methode zu prüfen, inwiefern identifizierte Verbesserungsvorschläge zu messbaren Verbesserungen der Wallet geführt haben.

Nicht bewertete Anforderungen:

1. Im Software-Tool sollen Benutzer anderen Benutzern in verschiedenen Evaluationsprojekten Rollen zuweisen können.
2. Im Software-Tool sollen Benutzer Evaluationsprojekte exportieren und importieren können.
3. Im Software-Tool sollen Benutzer Wallet-Funktionen, Stärken, Schwächen und Heuristiken zwischen Projekten importieren und exportieren können.
4. Das Software-Tool sollte Datenschutz-Hinweise anzeigen.

Alle Anforderungen mit deren Erfüllungsstatus sind online verfügbar[75].

Aus den Evaluationsergebnissen und den nicht erfüllten sowie teilweise erfüllten Anforderungen des Software-Tools ergaben sich 21 Verbesserungsvorschläge, die nun vorgestellt werden.

1. Jeder Screen des Software-Tools sollte Verlinkungen zu allen anderen relevanten Screens enthalten, die weiterführende Informationen für die Funktionen und Inhalte des jeweiligen Screens bereitstellen. Beispielsweise sollte auf dem Screen zur Formulierung von Verbesserungsvorschlägen für die Wallet der Screen zur Verwaltung

[75] https://doi.org/10.5281/zenodo.15114275

der Stärken und Schwächen der Wallet verlinkt sein. Die Verlinkung könnte beispielsweise durch einen Button umgesetzt werden, mit dem sich der jeweilige andere Screen in einem neuen Tab oder einem Pop-Up öffnen lässt.

2. Sichten von Tabellen sollten gespeichert werden, wie beispielsweise gefilterte Datensätze.
3. Informationstexte sollten überarbeitet werden: (a) Es sollte eine Anleitung zur Durchführung des Thinking aloud gegeben werden. Zusätzlich sollte ein Beispiel einer Anleitung für Probanden zur Durchführung des Thinking aloud gezeigt werden. (b) Es sollte erläutert werden, was der Begriff „Heuristik" bedeutet und wie sich die Gewichtung einer Heuristik auf den weiteren Verlauf der Evaluation auswirkt. (c) Es sollte ein Beispiel einer Konfliktlösung für konkurrierende Heuristiken gegeben werden. (d) Bei der Auswahl der Heuristiken zur Erstellung der Interaktionsmatrix sollte die Anzahl der ausgewählten Heuristiken geringgehalten werden (maximal 10 Heuristiken). (e) Fehlermeldungen sollten klar formuliert sein. (f) Es sollte verdeutlicht werden, wofür die Bedrohungsszenarien im weiteren Verlauf der Durchführung verwendet werden können. (g) Es sollte auf die DSGVO hingewiesen werden.
4. In Schritt 2 der MEUSec-Methode sollte es möglich sein, nicht nur eine Anleitung für die Probanden des Thinking aloud zu dokumentieren, sondern auch relevante Informationen für den Methoden-Anwender festzuhalten, wie beispielsweise, dass die Wallet nach jedem Thinking aloud eines Probanden zurückgesetzt wird.
5. Externe Sammlungen von Heuristiken sollten bewertbar sein. Außerdem sollten externe Sammlungen von Heuristiken nach Bewertung geordnet, gefiltert und durchsucht werden können.
6. Die Auswahl möglicher Sicherheitsattribute (wie Integrität, Verfügbarkeit und Vertraulichkeit) sollte erweitertbar sein, beispielsweise um Authentizität und Zuverlässigkeit.
7. Manche Eingabefelder sollten größer und erweiterbar sein, wie beispielsweise das Feld der Beschreibung einer Heuristik.
8. Verschiedene Design-Verbesserungen sollten vorgenommen werden: (a) Primäre und sekundäre Buttons sollten visuell eindeutig voneinander unterscheidbar sein. (b) Abstände zwischen Buttons sollten größer sein, um eine bessere visuelle Trennung zu gewährleisten. (c) In der Liste der Wallet-Funktionen sollten die ausgewählten, vorgeschlagenen Wallet-Funktionen kenntlich gemacht werden, sodass erkennbar ist, welche Wallet-Funktionen aus der vorgeschlagenen Liste ausgewählt und welche zusätzlich hinzugefügt wurden.
9. Die Reihenfolge einiger Funktionen sollte angepasst werden, wie beispielsweise, dass zuerst Heuristiken zur Erstellung der Matrix ausgewählt werden, bevor die leere Matrix erscheint.
10. Auf dem Screen der ermittelten Scores der UX und Informationssicherheit sollte klargestellt werden, dass die Scores für weitere Anwendungen der MEUSec-

Methode verwendet werden können, um zu prüfen, inwiefern Verbesserungsvorschläge zu messbaren Verbesserungen der Wallet geführt haben.

11. Die Fortschrittsanzeige sollte nicht nur die 8 Schritte der MEUSec-Methode, sondern auch die Aktivitäten je Schritt auflisten. Zudem sollte es möglich sein, zu den entsprechenden Screens der Aktivitäten zu navigieren, indem man diese anklickt.
12. Das Feld „Betroffene Heuristiken“ bei der Formulierung von Verbesserungsvorschlägen sollte automatisch ausgefüllt und dann erweitert werden können.
13. Das Wording sollte einheitlich und verständlich sein. In Pop-Ups sollten „Abbrechen“-Buttons anstelle von „Schließen“-Buttons implementiert werden.
14. Die Schieberegler der UX- und Informationssicherheit-Scores sollten kontrastreicher dargestellt werden. Außerdem sollten die Schieberegler mit den aktuellen UX- und Informationssicherheit-Scores initialisiert werden.
15. Wenn Aktivitäten wiederholt werden und Daten geändert werden, sollten die Änderungen automatisiert durch das Software-Tool dokumentiert werden.
16. Im Rahmen der Aktivitäten 1 und 2 in Schritt 8 wird nicht deutlich, welche Konflikte bereits gelöst wurden. Die verbleibenden Konflikte sollten farblich hervorgehoben werden. Konfliktlösungen sollten in Schritt 8, Aktivität 1, editierbar sein.
17. Die Bedrohungsszenarien sollten kopiert und bearbeitet werden können. Es sollte möglich sein, Begründungen für festgelegte Eintrittswahrscheinlichkeiten und Schadenausmaße dokumentieren zu können.
18. Es sollten weitere Informationen bereitgestellt werden. Beispielsweise sollte in der Tabelle der Bedrohungsszenarien zusätzlich zum Namen auch die Beschreibung der betroffenen Wallet Funktionen dargestellt werden.
19. Stärken und Schwächen der Wallet sollten Heuristiken und Verbesserungsvorschlägen zugeordnet werden können. Zudem sollte es möglich sein, Stärken und Schwächen der Wallet abzuhaken, wenn diese Heuristiken und Verbesserungsvorschlägen zugeordnet wurden.
20. Auf allen Screens der jeweiligen Schritte und Aktivitäten der MEUSec-Methode sollte jeweils ersichtlich sein, welche Rollen gefordert werden.
21. Im generierten Evaluationsbericht sollten Hyperlinks implementiert werden, beispielsweise bei den Heuristik-IDs der Verbesserungsvorschläge, um eine direkte Navigation zur jeweils referenzierten Heuristik zu ermöglichen.

In der zweiten, im Rahmen dieser Arbeit finalen Version des Software-Tools (siehe Kapitel 8) wurden nahezu alle Verbesserungsvorschläge umgesetzt. Die Verbesserungsvorschläge 11, 15 und 21 wurden nicht umgesetzt, da der Aufwand für ihre Umsetzung im Vergleich zum Nutzen im Rahmen dieser Arbeit als zu hoch eingestuft wurde.

9.6 Limitationen

Im Folgenden werden die Limitationen der Evaluation der Lissi-Wallet, der MEUSec-Methode und des Software-Tools beschrieben.

Die Evaluation der Lissi-Wallet beschränkt sich ausschließlich auf die iOS-Version. Versionen der Lissi-Wallet für andere Betriebssysteme, wie Android, wurden nicht evaluiert und könnten spezifische Abweichungen in Funktion und Interaktion aufweisen.

Des Weiteren wurde das Thinking aloud in einer Labor-Situation durchgeführt. Diese kontrollierte Umgebung könnte das Verhalten der WU verändert haben, da sich die WU möglicherweise anders verhalten haben als beim alltäglichen Gebrauch. Zusätzlich könnten die WU durch die Anwesenheit von Beobachtern in ihrer natürlichen Interaktion mit der Lissi-Wallet beeinflusst worden sein.

Zudem wurden keine personenbezogenen Daten der WU in der Lissi-Wallet verarbeitet, sondern ausschließlich Beispieldaten. Dadurch konnten potenzielle Effekte, die sich aus der Verarbeitung realer sensibler Daten ergeben, nicht evaluiert werden. Dies betrifft beispielsweise die Evaluation des Vertrauens in die Lissi-Wallet als auch die wahrgenommene Sicherheit.

Das UX-Attribut Barrierefreiheit kann nicht als ausreichend evaluiert betrachtet werden, da in der benutzerbasierten Evaluation nicht ausreichend Probanden mit unterschiedlichen Einschränkungen, wie beispielsweise einer Rot-Grün-Schwäche und Blindheit, involviert waren.

Die Rollen der MEUSec-Methode wurden von Personen aus dem näheren Umfeld besetzt. Persönliche Beziehungen oder gruppendynamische Effekte können die Objektivität der Personen beeinträchtigen. Dadurch kann es zu einer milderen Einschätzung von Schwachstellen oder zu einer Bestätigung bestehender Annahmen kommen, anstatt einer neutralen Bewertung der MEUSec-Methode und des Software-Tools.

Zur weiteren Evaluation der Korrektheit der Methodenartefakte ist es notwendig, die MEUSec-Methode auf die verbesserte Version der Lissi-Wallet anzuwenden. So kann anhand der Scores der UX und Informationssicherheit geprüft werden, ob die Verbesserungsvorschläge zu messbaren Verbesserungen beigetragen haben.

Die Literaturrecherche und die Ableitung zusätzlicher Heuristiken (Schritt 5, Aktivitäten 2 und 3) wurden im Rahmen der Anwendung der MEUSec-Methode nicht durchgeführt, da alle betrachteten Wallet-Funktionen bereits durch bestehende Heuristiken abgedeckt waren. Auch eine Anpassung der Heuristiken (Schritt 6, Aktivität 3) war nicht erforderlich, da keine inhaltlichen Konflikte oder Unklarheiten auftraten. Diese Aktivitäten

wurden folglich nicht evaluiert, sind jedoch gemäß MEUSec-Methode ohnehin als optional vorgesehen.

9.7 Vergleich und Diskussion der Evaluationsergebnisse

Die Evaluationsergebnisse der Hidy- und Lissi-Wallet wurden bereits in Abschnitt 9.3 mit Evaluationsergebnissen anderer Wallets verglichen. In diesem Abschnitt werden die Ergebnisse der ersten Evaluation der MEUSec-Methode ohne Software-Tool (siehe Kapitel 7) mit den Ergebnissen der zweiten Evaluation der MEUSec-Methode mit Software-Tool verglichen und diskutiert. Insbesondere wird diskutiert, inwiefern das Software-Tool die Anwendung der MEUSec-Methode verbessert.

Von den 12 Verbesserungsvorschlägen aus der ersten Evaluation kamen in der zweiten Evaluation 2 Verbesserungsvorschläge erneut auf.

1. Die MEUSec-Methode sollte weitere standardisierte Vorlagen anbieten. Nach der ersten Evaluation wurden weitere Vorlagen implementiert, wie beispielsweise eine Vorlage für einen Score der Eintrittswahrscheinlichkeit und einen Score des Schadensausmaßes für die Bedrohungsszenarien. Allerdings wurden in der zweiten Evaluation nochmals weitere standardisierte Vorlagen gefordert, wie beispielsweise vordefinierte, potenzielle Angreifer.
2. Es sollte ein Änderungsprotokoll für wiederholte Aktivitäten der MEUSec-Methode und für resultierende Änderungen an Methodenartefakten eingeführt werden, um sicherzustellen, dass Änderungen dokumentiert werden. Die Begründungen und Beschreibungen, die im Rahmen der Aktivitäten der MEUSec-Methode dokumentiert wurden, reichen nicht aus, da beispielsweise Aktivitäten wiederholt werden können und somit ein globales Änderungsprotokoll notwendig ist.

Im Rahmen der ersten Evaluation der MEUSec-Methode kam das Software-Tool nicht zum Einsatz, während es in der zweiten Evaluation verwendet wurde. So lässt sich bewerten, inwiefern das Software-Tool die Anwendung der MEUSec-Methode verbessert. Allerdings sind die gemessenen Zeiten je Schritt der MEUSec-Methode nicht unmittelbar vergleichbar, da sich beispielsweise die Anzahl der evaluierten Wallet-Funktionen und die Anzahl der verwendeten Heuristiken unterscheiden. Zudem wurden Aktivitäten einzelner Schritte der MEUSec-Methode zusammengefasst oder verschoben. Zeiten einzelner Aktivitäten lassen sich jedoch vergleichen.

1. In der ersten Evaluation der MEUSec-Methode dauerte es etwa 30 Minuten, die Interaktionsmatrix mittels der Heuristiken (ohne Interaktionseigenschaften) zu erstel-

len. In der zweiten Evaluation mussten die Heuristiken im Software-Tool lediglich per Checkbox ausgewählt werden, woraufhin die Interaktionsmatrix automatisch erstellt wurde. Dies dauerte nur etwa 5 Minuten. Allerdings wurden im Rahmen der ersten Evaluation 12 Heuristiken in die Interaktionsmatrix einbezogen, im Vergleich zu 8 Heuristiken im Rahmen der zweiten Evaluation. Selbst bei einer proportionalen Anpassung der Zeit auf 8 Heuristiken ergibt sich eine Dauer von etwa 20 Minuten.

2. Im Rahmen der zweiten Evaluation berechnete das Software-Tool die UX- und Informationssicherheit-Scores automatisch, was die Zeit von 41 Minuten auf eine Berechnung per Button-Klick innerhalb von Millisekunden reduzierte.
3. Im Rahmen der ersten Evaluation mussten die Interaktionseigenschaften händisch der Sammlung an Heuristiken hinzugefügt werden. Im Rahmen der zweiten Evaluation konnten die Interaktionseigenschaften auf Knopfdruck der eigenen Sammlung an Heuristiken hinzugefügt werden. Dadurch wurde die Zeit von 77 Minuten auf Millisekunden reduziert.

Zusammenfassend lässt sich sagen, dass die Evaluationen wertvolle Erkenntnisse über die Durchführbarkeit der MEUSec-Methode, über die Qualität der Methodenartefakte, über die Funktionalität des Software-Tools und über UX und Usability des Software-Tools erbrachten.

Die MEUSec-Methode erwies sich als geeignet, um die UX und Informationssicherheit von Wallets systematisch mit Berücksichtigung des Zusammenhangs von UX und Informationssicherheit zu evaluieren und Verbesserungsvorschläge abzuleiten. Besonders hervorzuheben ist die Kombination der beiden Perspektiven von Endnutzern und Experten der UX und Informationssicherheit, die eine ganzheitliche Evaluation von Wallets ermöglichen. Es wurde wertvolles Verbesserungspotenzial identifiziert, wie beispielsweise, dass zuerst Heuristiken aus der externen Sammlung der Heuristiken ausgewählt werden, bevor eigene Heuristiken auf Basis der identifizierten Stärken und Schwächen der Wallet formuliert werden. So konnte die Effizienz gesteigert werden. Außerdem wurden die externen Heuristiken bereits evaluiert und bieten Beispiele, falls die zu evaluierenden Wallet-Funktionen nicht mit den externen Heuristiken abgedeckt sind und eigene Heuristiken formuliert werden müssen.

Das Software-Tool ermöglicht eine effizientere Durchführung der MEUSec-Methode. Besonders hervorzuheben ist, dass einige Aktivitäten der MEUSec-Methode automatisiert ausgeführt werden, wie beispielsweise die Berechnung der UX- und Informationssicherheit-Scores, die Erstellung der Interaktionsmatrix mit ausgewählten Heuristiken (ohne deren Interaktionseigenschaften) und das Hinzufügen der festgelegten Interaktionseigenschaften zur eigenen Sammlung der Heuristiken. Zusätzlich zu betonen sind die externen Sammlungen an Heuristiken aus denen Heuristiken für den eigenen Gebrauch

ausgewählt werden können. Außerdem zu erwähnen sind die Schieberegler, mit denen sich jeweils ein Score für die UX und die Informationssicherheit einstellen lassen, worauf sich Verbesserungsvorschläge für die eingestellten Scores ausgeben lassen.

10 Fazit und Ausblick

In diesem Kapitel werden zunächst in Abschnitt 10.1 die zentralen Resultate der Arbeit zusammengefasst. Zum Abschluss erfolgt in Abschnitt 10.2 ein Ausblick auf mögliche weiterführende Forschungsarbeiten.

10.1 Fazit

Wallets ermöglichen das Speichern, Verwalten und Teilen von digitalen Nachweisen in einer einzigen digitalen Applikation. Wallet-Benutzer können dadurch selbstbestimmt entscheiden, mit wem sie welche Nachweise teilen möchten.

Bestehende Wallets besitzen jedoch mehrere Schwächen der UX und Informationssicherheit. Dies ist insbesondere deshalb problematisch, da jeder EU-Mitgliedsstaat bis Ende 2026 verpflichtet ist, seinen Bürgern eine Wallet zur Verfügung zu stellen (Europäische Union, 2024). Zusätzlich zu den Schwächen der UX und Informationssicherheit von Wallets können sich beide Aspekte gegenseitig negativ oder positiv beeinflussen. Daher ist es wichtig, dass UX und Informationssicherheit von Wallets nicht separat voneinander evaluiert und verbessert werden, sondern gemeinsam betrachtet werden.

Ziel der Arbeit war es, den Zusammenhang zwischen UX und Informationssicherheit von Wallets bewertbar zu machen und Verbesserungsvorschläge der UX und Informationssicherheit zu finden. Hierzu sollte eine Methode entwickelt und ein Software-Tool für die Anwendung der Methode bereitgestellt werden.

Zusammenfassend lässt sich feststellen, dass das Ziel erreicht wurde.

Anfangs wurde eine systematische Literaturrecherche durchgeführt, um bestehende Verfahren zur Evaluation des Zusammenhangs von UX und Informationssicherheit zu identifizieren. Die 22 identifizierten Evaluationsverfahren (inklusive 10 Fragebögen) wurden bewertet, diskutiert und einander gegenübergestellt.

Anschließend wurden einige dieser Evaluationsverfahren auf eine Wallet angewendet, um einerseits Erkenntnisse über die Wallet und andererseits Erkenntnisse über die Evaluationsverfahren zu gewinnen. Hinsichtlich der Wallet konnte beispielsweise durch Eye Tracking gezeigt werden, dass 19 von 24 Probanden einen in rot gefärbten Sicherheitshinweis beim Speichern eines digitalen Nachweises nicht sahen, sodass die Informationssicherheit gefährdet war. Hinsichtlich der Evaluationsverfahren zeigte sich zum Beispiel,

dass die Meinungen von Experten und Probanden stark voneinander abweichen können, sodass ein Evaluationsverfahren sowohl Experten als auch Probanden miteinbeziehen sollte.

Anschließend wurden 12 UX- und 6 Informationssicherheit-Heuristiken entwickelt. Die entwickelten Heuristiken wurden durch Interviews mit Experten aus den Bereichen UX, Informationssicherheit und Wallets aus der Praxis und der Wissenschaft evaluiert und verbessert. Außerdem wurden eine Versuchsgruppe und eine Kontrollgruppe gebildet. Die Versuchsgruppe führte Heuristische Evaluationen (Nielsen und Molich, 1990) mit den entwickelten UX-Heuristiken durch, die Kontrollgruppe Heuristische Evaluationen mit den Heuristiken von Nielsen (1994). Anschließend wurden die Ergebnisse miteinander verglichen und es zeigte sich, dass mehr UX-Schwächen mit den entwickelten UX-Heuristiken identifiziert wurden.

Anschließend wurden einige der identifizierten Evaluationsverfahren adaptiert, um die MEUSec-Methode zu entwickeln. Mit der MEUSec-Methode lassen sich UX und Informationssicherheit, insbesondere mit Berücksichtigung der Implikationen zwischen UX und Informationssicherheit, von Wallets evaluieren und systematisch Verbesserungsvorschläge finden. Außerdem vereint die MEUSec-Methode eine benutzerbasierte Evaluation mit einer expertenbasierten Evaluation.

Danach wurde die MEUSec-Methode ein erstes Mal evaluiert, indem diese auf die Hidy-Wallet angewendet wurde. Dadurch ergaben sich grundsätzlich 2 Beiträge: die Evaluation der Hidy-Wallet und die Evaluation der MEUSec-Methode. Insgesamt konnten 41 Schwächen der UX und Informationssicherheit der Hidy-Wallet identifiziert werden. Außerdem wurden 32 UX- und Informationssicherheit-Heuristiken und 26 Verbesserungsvorschläge der Hidy-Wallet gewonnen. Die MEUSec-Methode wurde anhand verschiedener Kriterien evaluiert. Auf Basis der Evaluationsergebnisse wurden 12 Verbesserungsvorschläge der MEUSec-Methode identifiziert, die anschließend in die MEUSec-Methode eingearbeitet wurden.

Danach wurde ein Software-Tool zur Unterstützung der Anwendung der MEUSec-Methode entwickelt. Zunächst wurde eine Anforderungserhebung durchgeführt. Anschließend folgte der Entwurf des Architekturmodells, des User Interface und des Datenmodells.

Anschließend wurden die MEUSec-Methode mithilfe des Software-Tools auf die Lissi-Wallet angewendet. Dadurch entstanden grundsätzlich 3 Beiträge: die Evaluation der Lissi-Wallet, die Evaluation der MEUSec-Methode und die Evaluation des Software-Tools. Insgesamt konnten 52 Schwächen der UX und Informationssicherheit der Lissi-Wallet identifiziert werden. Des Weiteren wurden 19 Heuristiken der UX und Informationssicherheit sowie 26 Verbesserungsvorschläge der Lissi-Wallet gewonnen.

Für die Evaluation der MEUSec-Methode wurden dieselben Evaluationskriterien wie in der ersten Evaluation verwendet. Für die Evaluation des Software-Tools wurden weitere Evaluationskriterien verwendet und die erhobenen Anforderungen auf Erfüllung geprüft. Zusätzlich wurden die Ergebnisse der ersten Evaluation mit denen der zweiten Evaluation verglichen. Es zeigte sich, dass das Software-Tool die Effizienz der MEUSec-Methode erhöht. Die identifizierten Verbesserungsvorschläge der MEUSec-Methode und des Software-Tools wurden in die Methode und in das Software-Tool eingearbeitet. So entstanden die dritte, im Rahmen des Promotionsvorhabens finale Version der MEUSec-Methode und die zweite Version des Software-Tools.

10.2 Ausblick

Das Thema dieser Arbeit bietet weitere Fragestellungen und Potenziale, die im Rahmen zukünftiger Forschungsarbeiten betrachtet werden können.

Die Heuristischen Evaluationen (siehe Abschnitt 5.4) beschränkten sich auf die entwickelten UX-Heuristiken, da keine vergleichbaren Informationssicherheit-Heuristiken identifiziert werden konnten. Allerdings wäre denkbar, dass die Ergebnisse von Heuristischen Evaluationen unter Einsatz der entwickelten Informationssicherheit-Heuristiken mit Ergebnissen anderer Evaluationsverfahren der Informationssicherheit verglichen werden könnten.

Des Weiteren wurden bei den Heuristischen Evaluationen (siehe Abschnitt 5.4) lediglich die Anzahl und nicht der Schweregrad der identifizierten UX-Schwächen betrachtet. Dadurch konnte nicht vollständig untersucht werden, ob eine höhere Anzahl identifizierter UX-Schwächen tatsächlich auf eine effektivere Erkennung von UX-Schwächen durch die entwickelten UX-Heuristiken hindeutet oder ob vor allem weniger gravierende UX-Schwächen mit den entwickelten Heuristiken erfasst wurden. In einer weiterführenden Untersuchung könnten daher die entwickelten UX-Heuristiken und die Heuristiken von Nielsen (1994) nicht nur hinsichtlich der Anzahl der gefundenen Schwächen miteinander verglichen, sondern auch deren Schwergrad in den Vergleich miteinbezogen werden.

Ferner wurden die UX- und Informationssicherheit-Heuristiken unmittelbar für Wallets entwickelt. Wallets können für das Empfangen von digitalen Nachweisen von Ausstellern und für das Teilen von digitalen Nachweisen an Prüfer verwendet werden. Da sich UX- und Informationssicherheit-Schwächen der Software-Systeme von Ausstellern und Prüfern digitaler Nachweise auch auf die UX und Informationssicherheit von Wallets auswirken können, werden für diese zukünftig auch UX- und Informationssicherheit-Heuristiken entwickelt. Beispielsweise könnte ein einführendes Tutorial seitens des Ausstellers digitaler Nachweise bereits Wallet-Benutzern die grundlegende Funktions-

weise von Wallets verdeutlichen. Dadurch könnte zusätzlich das Risiko von Fehlbedienungen reduziert werden, sodass sich die Informationssicherheit erhöht.

Das Software-Tool automatisiert bereits einzelne Aktivitäten der MEUSec-Methode. Zukünftig soll untersucht werden, inwiefern weitere Aktivitäten der MEUSec-Methode automatisiert werden können. Hierzu könnten unterschiedliche Technologien, insbesondere aus dem Bereich der Künstlichen Intelligenz (KI), verwendet werden, um die UX und Informationssicherheit von Wallets zu evaluieren und Verbesserungsvorschläge zu finden. Einige mögliche Beispiele werden im Folgenden erläutert.

Die MEUSec-Methode verwendet das Evaluationsverfahren Thinking aloud (Nielsen, 1993). Hierbei testen Probanden die Wallet und verbalisieren ihre positiven und negativen Gedanken über die Wallet. Diese Aufnahmen bieten wertvolle Einblicke in die Wahrnehmung und das Verhalten der Probanden. Mithilfe von Natural Language Processing und Spracherkennungstechnologien könnte das Software-Tool die verbalen Äußerungen der Probanden auf relevante UX- und Informationssicherheit-Schwächen untersuchen. Beispielsweise könnte die KI nach bestimmten Schlüsselwörtern suchen, die auf Stärken oder Schwächen hinweisen, wie etwa „einfach“, „schwierig“ oder „verwirrend“. Dadurch könnten die Effizienz und die Effektivität der Evaluation erhöht werden.

Denkbar wäre auch, dass die Probanden durch KI-Modelle ersetzt werden könnten. Die Akquise von Probanden und die Durchführung einer UX-Evaluation mit Probanden stellt sich oft als zeit- und kostenaufwändig dar. Um diese Aufwände zu reduzieren, könnte KI eingesetzt werden. In zukünftigen Untersuchungen soll ermittelt werden, inwieweit unterschiedliche KI-Modelle die Leistung von menschlichen Probanden bei der Durchführung von UX-Evaluationen ersetzen oder sogar übertreffen können. Ein entscheidender Vorteil des Einsatzes von KI in der UX-Evaluation könnte darin liegen, dass KI-Modelle in der Lage sind, eine Vielzahl von unterschiedlichen Personas zu simulieren. Dadurch könnten insbesondere Personas mit spezifischen Bedürfnissen hinsichtlich Barrierefreiheitsaspekten, wie körperlichen oder kognitiven Einschränkungen, in der UX-Evaluation berücksichtigt werden. Diese bleiben in bisherigen UX-Evaluationen oft unberücksichtigt.

Hinsichtlich der expertenbasierten Evaluation inkludiert die MEUSec-Methode das Evaluationsverfahren der Heuristischen Evaluation. Dazu werden ein UX- und Informationssicherheit-Experte benötigt, welche die Erfüllungsgrade der Heuristiken bewerten, was zeit- und kostenintensiv ist. Ein KI-Modell könnte die UX- und Informationssicherheit-Experten bei der Bewertung der Erfüllungsgrade unterstützen oder sogar ersetzen. Die geplante Untersuchung zielt darauf ab, zu ermitteln, inwieweit KI-Modelle menschliche Experten bei der Heuristischen Evaluation unterstützen oder ersetzen können. Für die Bewertung der Erfüllungsgrade der Informationssicherheit-Heuristiken könnten weitere

Evaluationsverfahren automatisiert angewendet werden. Beispielsweise könnte ein Wallet-Betreiber den Quellcode der Wallet automatisiert auf Schwächen untersuchen lassen. Zum Beispiel könnte überprüft werden, ob Passwörter im Klartext gespeichert werden, ob Verschlüsselungsmechanismen korrekt implementiert sind oder ob der Quellcode gegen potenzielle Angriffe resistent ist. Zusätzlich könnten Penetrationstests automatisiert durchgeführt werden, um Angriffe auf die Wallet zu simulieren, sodass Schwachstellen aus der Perspektive eines Angreifers identifiziert werden.

Des Weiteren könnten die Interaktionseigenschaften zwischen den Heuristiken automatisiert bewertet und auf dieser Basis automatisiert Verbesserungsvorschläge der UX und Informationssicherheit für die Wallet generiert werden. Für die Bewertung der Interaktionseigenschaften könnte auf Vergangenheitsdaten aufgebaut werden, die bereits durch vergangene Untersuchungen erhoben wurden. So müssten die Interaktionseigenschaften für verschiedene Aspekte der UX und Informationssicherheit von bestimmten Wallet-Funktionen nicht erneut bewertet werden. Zudem könnten die Beeinflussungen zwischen UX und Informationssicherheit nicht nur qualitativ erfasst werden, sondern auch quantitativ. Ein quantitativer Score könnte dabei von KI-Modellen vergeben werden, um anzugeben, inwieweit eine Veränderung der UX die Informationssicherheit beeinflusst und umgekehrt. Bisher lässt sich der Schieberegler bis zum maximalen Score neutraler und komplementärer Heuristiken ohne die Abnahme des Scores des jeweiligen anderen Qualitätsattributs (UX oder Informationssicherheit) einstellen. Ab dann wird für jede Erhöhung des Scores der UX oder Informationssicherheit um einen Prozentpunkt, ein Prozentpunkt beim Score des jeweiligen anderen Qualitätsattributs abgezogen. Zukünftig könnte das Software-Tool durch eine präzisere quantitative Bewertung der Beeinflussungen zwischen UX und Informationssicherheit nach dem Einstellen der gewünschten Scores für UX und Informationssicherheit durch den Schieberegler präzisere Verbesserungsvorschläge generieren.

Der Einsatz von KI-Modellen im Rahmen von UX-Evaluationen ist nicht nur mit Chancen, sondern auch mit Herausforderungen verbunden. Beispielsweise können die kreative Vielfalt im Entwurfsprozess eingeschränkt und Innovationspotenziale reduziert werden, wenn KI-Modelle Artefakte auf Basis bestehender Muster generieren und dadurch insbesondere bewährtere, aber weniger originelle Entwurfsansätze berücksichtigen (Doshi und Hauser, 2024). Des Weiteren können Trainingsdaten von KI-Modellen Vorurteile enthalten, wodurch beispielsweise diskriminierende Entwurfsempfehlungen generiert werden können (Abdul u. a., 2018). Zudem mangelt es KI-Modellen an Transparenz ihrer Entscheidungsfindung, wodurch Rückschlüsse auf die Herkunft von Empfehlungen erschwert werden. Dies behindert die kritische Überprüfung und mindert die Nachvollziehbarkeit (Papenmeier u. a., 2022). Die Herausforderungen von KI-Modellen sollten in zukünftigen Untersuchungen berücksichtigt werden.

Die MEUSec-Methode und das Software-Tool wurden bisher nach einer Anwendung auf eine Wallet nicht ein zweites Mal auf die gleiche Wallet angewendet. Eine weiterführende Untersuchung könnte darin bestehen, die Methode und das Tool erneut auf die gleiche Wallet, jedoch mit den eingearbeiteten Verbesserungsvorschlägen, anzuwenden. Ziel wäre es, zu überprüfen, ob die zuvor identifizierten Verbesserungsvorschläge zu messbaren Verbesserungen der Wallet geführt haben.

Ferner wurden die MEUSec-Methode und das Software-Tool bisher lediglich auf Wallets angewendet. Denkbar wäre eine Anwendung auf andere Arten von Software-Systemen. Eine entsprechende Eignungsprüfung steht noch aus und würde den Rahmen der vorliegenden Arbeit überschreiten. Perspektivisch ist zunächst eine Anwendung der Methode und des Tools auf weitere Wallet-Arten – wie etwa die Google Wallet oder die Apple Wallet – vorgesehen. In einem weiteren Schritt sollen die Methode und das Tool auf andere Software-Systeme als Wallets angewendet werden.

Literaturverzeichnis

Abdul, Vermeulen, Wang, Lim und Kankanhalli (2018). *Trends and Trajectories for Explainable, Accountable and Intelligible Systems: An HCI Research Agenda*. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '18)*.

Abrams (2010). *Quantitative business valuation: a mathematical approach for today's professionals*.

Abu-Salma, Krol, Parkin, Koh, Kwan, Mahboob, Traboulsi und Sasse (2017). *The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram*. In: *Proceedings of the 2nd European Workshop on Usable Security (EuroUSEC '17)*.

Adams und Sasse (1999). *Users are not the enemy*. In: *Journal of Communications of the ACM*, S. 40-46.

Alarifi, Alsaleh und Alomar (2017). *A model for evaluating the security and usability of e-banking platforms*. In: *Journal of Computing*, S. 519-535.

Almani und Alrwais (2024). *The Role of Wireframes in Enhancing User Interface Design*. In: *Journal of Innovations in Engineering and Technology*, S. 134-140.

Alpers, Karle, Schreiber, Schönthaler und Oberweis (2021). *Process Mining bei hybriden Vorgehensmodellen zur Umsetzung von Unternehmenssoftware*. In: *Informatik Spektrum*, S. 178-189.

Al-Subaie und Maibaum (2006). *Evaluating the Effectiveness of a Goal-Oriented Requirements Engineering Method*. In: *4th International Workshop on Comparative Evaluation in Requirements Engineering (CERE '06)*, S. 8-19.

Anderson (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*.

Anke und Richter (2023). *Digitale Identitäten: Status Quo und Perspektiven*. In: *HMD Praxis der Wirtschaftsinformatik*, S. 261-282.

Apple Inc. (2024). *Wallet*. *Apple*. Verfügbar unter: https://www.apple.com/wallet.

Atick, Gelb, Pahlavooni, Gasol und Safdar (2014). *Digital identity toolkit: a guide for stakeholders in Africa*. *World Bank Group*. Verfügbar unter: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa.

Bader, Schön und Thomaschewski (2017). *Heuristics Considering UX and Quality Criteria for Heuristics*. In: *Journal of Interactive Multimedia and Artificial Intelligence*, S. 48-53.

Bojko (2005). *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 `05)*.

Bosnjak und Brumen (2019). *Examining Security and Usability Aspects of Knowledge-based Authentication Methods*. In: *Proceedings of the 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO '19)*.

Braun, Sauer, Sürmeli und Thessen (2024). *Selbstbestimmte Identitäten im E-Commerce: Die Zukunft des personalisierten Online-Shoppings*. In: *HMD Praxis der Wirtschaftsinformatik*.

Braz, Seffah und M'Raihi (2007). *Designing a Trade-Off Between Usability and Security: A Metrics Based-Model*. In: Baranauskas, Palanque, Abascal und Barbosa (Hrsg.), *Human-Computer Interaction (INTERACT '07)*, S. 114-126.

Brooke (1996). *SUS: A quick and dirty usability scale*. In: Jordan, Thomas, Weerdmeester und McClelland (Hrsg.), *Usability Evaluation In Industry*, S. 189-194.

Bundesamt für Sicherheit in der Informationstechnik (2017). *BSI-Standard 200-2. IT-Grundschutz-Methodik.* Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html.

Bundesamt für Sicherheit in der Informationstechnik (2020). *Elementare Gefährdungen*. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/Elementare_Gefaehrdungen.pdf.

Bundesministerium des Innern und für Heimat (2023). *Der Personalausweis*. *Bundesministerium des Innern und für Heimat*. Verfügbar unter: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/der-personalausweis-node.html.

Bundesministerium für Wirtschaft und Klimaschutz (2020). *Schaufenster Sichere Digitale Identitäten*. *Schaufenster Sichere Digitale Identitäten*. Verfügbar unter: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html.

Chadwick, Laborde, Oglaza, Venant, Wazan und Nijjar (2019). *Improved Identity Management with Verifiable Credentials and FIDO*. In: *Journal of IEEE Communications Standards Magazine*, S. 14-20.

Chin, Diehl und Norman (1988). *Development of an instrument measuring user satisfaction of the human-computer interface*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '88)*, S. 213-218.

Cirucci und Pruchniewska (2022). *UX Research Methods for Media and Communication Studies: An Introduction to Contemporary Qualitative Methods*.

Cucko, Becirovic, Kamisalic, Mrdovic und Turkanovic (2022). *Towards the Classification of Self-Sovereign Identity Properties*. In: *Journal of IEEE Access*.

Darwish und Bataineh (2012). *Eye tracking analysis of browser security indicators*. In: *Proceedings of the International Conference on Computer Systems and Industrial Informatics 2012*, S. 1-6.

DIN EN ISO 9241-11:2018-11 (2018). *DIN EN ISO 9241-11:2018-11, Ergonomie der Mensch-System-Interaktion- Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte (ISO 9241-11:2018);* Verfügbar unter: https://www.beuth.de/de/-/-/279590417.

DIN EN ISO 9241-110:2020-10 (2020). *DIN EN ISO 9241-110:2020-10, Ergonomie der Mensch-System-Interaktion - Teil 110: Interaktionsprinzipien (ISO 9241-110:2020);* Verfügbar unter: https://www.beuth.de/de/-/-/320862700.

DIN EN ISO 9241-210:2020-03 (2020). *DIN EN ISO 9241-210:2020-03, Ergonomie der Mensch-System-Interaktion - Teil 210: Menschzentrierte Gestaltung interaktiver Systeme (ISO 9241-210:2019);* Verfügbar unter: https://www.beuth.de/de/-/-/313017070.

DIN EN ISO/IEC 24760-1:2022 (2022). *IT-Sicherheit und Datenschutz - Rahmenwerk für Identitätsmanagement - Teil 1: Terminologie und Konzept (ISO/IEC 24760-1:2022)*.

DIN EN ISO/IEC 27000 (2020). *DIN EN ISO/IEC 27000:2020, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie*.

Doshi und Hauser (2024). *Generative AI enhances individual creativity but reduces the collective diversity of novel content*. In: *Journal of Science Advances*.

Dutta, Madnick und Joyce (2016). *SecureUse: Balancing Security and Usability Within System Design*. In: Stephanidis (Hrsg.), *HCI International 2016 – Posters' Extended Abstracts*, S. 471-475.

Eckert (2012). *IT-Sicherheit: Konzepte - Verfahren - Protokolle*.

Ehrlich, Richter, Meisel und Anke (2021). *Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten*. In: *HMD Praxis der Wirtschaftsinformatik*, S. 247-270.

Europäische Kommission (2023). *Pilotimplementierung der EU-Brieftasche für digitale Identität*. Verfügbar unter: https://digital-strategy.ec.europa.eu/de/policies/eudi-wallet-implementation.

Europäische Union (2024). *Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt*. Verfügbar unter: http://data.europa.eu/eli/reg/2024/1183/oj.

Fanelle, Karimi, Shah, Subramanian und Das (2020). *Blind and Human: Exploring More Usable Audio CAPTCHA Designs*. In: *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS '20)*, S. 111-125.

Furnell, Jusoh und Katsabas (2006). *The challenges of understanding and using security: A survey of end-users*. In: *Journal of Computers & Security*, S. 27-35.

Gartner Inc. (2024). *Gartner Predicts At Least 500 Million Smartphone Users Will Be Using a Digital Identity Wallet by 2026*. *Gartner*. Verfügbar unter: https://www.gartner.com/en/newsroom/press-releases/2024-09-24-gartner-predicts-at-least-500-million-smartphone-users-will-be-using-a-digital-identity-wallet-by-2026.

Gonzalez, Martin, Munoz-Arteaga, alvarez-Rodriguez und Garcia-Ruiz (2009). *A measurement model for secure and usable e-commerce websites*. In:

Proceedings of the Canadian Conference on Electrical and Computer Engineering, S. 77-82.

Google LLC (2024). *Alles Wichtige auf dem Smartphone aufbewahren und bequem per Smartphone bezahlen*. *Google Wallet: Carry more with Google Wallet*. Verfügbar unter: https://wallet.google/intl/de_de.

Gordieiev, Kharchenko und Vereshchak (2017). *Usable Security Versus Secure Usability: an Assessment of Attributes Interaction*. In: *Proceedings of the International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications*.

Grassi, Garcia und Fenton (2017). *Digital identity guidelines: revision 3*. Verfügbar unter: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Gray, Kou, Battles, Hoggatt und Toombs (2018). *The Dark (Patterns) Side of UX Design*. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '18)*, S. 1-14.

Hassenzahl (2008). *User experience (UX): towards an experiential perspective on product quality*. In: *Proceedings of the 20th Conference on l'Interaction Homme-Machine (IHM '08)*, S. 11-15.

Hassenzahl, Burmester und Koller (2003). *AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität*. In: Szwillus und Ziegler (Hrsg.), *Mensch & Computer 2003*, S. 187-196.

Herzog und Shahmehri (2007). *Usability and Security of Personal Firewalls*. In: Venter, Eloff, Labuschagne, Eloff und von Solms (Hrsg.), *New Approaches for Security, Privacy and Trust in Complex Environments*, S. 37-48.

Hornung (2005). *Die digitale Identität: Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren*.

ISO/IEC 25010:2023-11 (2023). *ISO/IEC 25010:2023-11, System- und Software-Engineering - Qualitätskriterien und Bewertung von System und Softwareprodukten (SQuaRE) - Produktqualitätsmodell*.

Jaspers (2009). *A comparison of usability methods for testing interactive health technologies: Methodological aspects and empirical evidence*. In: *Journal of Medical Informatics*, S. 340-353.

John und Kieras (1994). *The GOMS Family of Analysis Techniques: Tools for Design and Evaluation*. In: *Journal of ACM Transactions on Computer-Human Interaction (TOCHI)*.

Johnston, Eloff und Labuschagne (2003). *Security and human computer interfaces*. In: *Journal of Computers & Security*, S. 675-684.

Khayretdinova, Kubach, Sellung und Roßnagel (2022). *Conducting a Usability Evaluation of Decentralized Identity Management Solutions*. In: Friedewald, Kreutzer und Hansen (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz*, S. 389-406.

Korir, Parkin und Dunphy (2022). *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 '22)*, S. 195-211.

Krauß, Kostic und Sellung (2023a). *A more User-Friendly Digital Wallet? User Scenarios of a Future Wallet*. In: *Open Identity Summit 2023*, S. 73-84.

Krauß, Sellung und Kostic (2023b). *Ist das die Wallet der Zukunft?: Ein Blick durch die Nutzendenbrille beim Einsatz von digitalen Identitäten*. In: *HMD Praxis der Wirtschaftsinformatik*, S. 344-365.

Kromrey (2001). *Evaluation - ein vielschichtiges Konzept: Begriff und Methodik von Evaluierung und Evaluationsforschung ; Empfehlungen für die Praxis*. In: *Sozialwissenschaften und Berufspraxis*.

Krueger und Casey (2015). *Focus groups: a practical guide for applied research*.

Kujala und Kauppinen (2004). *Identifying and selecting users for user-centered design*. In: *Proceedings of the 3rd Nordic conference on Human-computer interaction (NordiCH '04)*, S. 297-303.

Kulyk, Neumann, Budurushi und Volkamer (2017). *Nothing Comes for Free: How Much Usability Can You Sacrifice for Security?* In: *Journal of IEEE Security & Privacy*, S. 24-29.

Kwon, Shin und Na (2014). *Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected*. In: *Journal of IEEE Transactions on Systems, Man, and Cybernetics: Systems*, S. 716-727.

Lallemand und Koenig (2017). *Lab testing beyond usability: challenges and recommendations for assessing user experiences*. In: *Journal of Usability Studies*, S. 133-154.

Larman und Basili (2003). *Iterative and incremental developments. a brief history*. In: *Journal of IEEE Computer*, S. 47-56.

Laugwitz, Held und Schrepp (2008). *Construction and Evaluation of a User Experience Questionnaire*. In: Holzinger (Hrsg.), *HCI and Usability for Education and Work*, S. 63-76.

Lewis (1991). *Psychometric evaluation of an after-scenario questionnaire for computer usability studies: The ASQ*. In: *Journal of ACM SIGCHI Bulletin*, S. 78-81.

Lewis (1995). *IBM computer usability satisfaction questionnaires: Psychometric evaluation and instructions for use*. In: *Journal of Human-Computer Interaction*, S. 57-78.

Lund (2001). *Measuring Usability with the USE Questionnaire*. In: *Usability and User Experience Newsletter. Usability Interface.*, S. 3-6.

Ma und Feng (2011). *Evaluating Usability of Three Authentication Methods in Web-Based Application*. In: *Proceeding of the 9th International Conference on Software Engineering Research, Management and Applications*, S. 81-88.

Mare, Baker und Gummeson (2016). *A study of authentication in daily life*. In: *Proceedings of the 12th USENIX Conference on Usable Privacy and Security (SOUPS '16)*, S. 189-206.

Marky, Schmitz, Zimmermann, Herbers, Kunze und Mühlhäuser (2020a). *3D-Auth: Two-Factor Authentication with Personalized 3D-Printed Items*. In: *Proceedings of the CHI Conference on Human Factors in Computing Systems 2020*, S. 1-12.

Marky, Zimmermann, Funk, Daubert, Bleck und Mühlhäuser (2020b). *Improving the Usability and UX of the Swiss Internet Voting Interface*. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, S. 1-13.

Marky, Zollinger, Roenne, Ryan, Grube und Kunze (2021). *Investigating Usability and User Experience of Individually Verifiable Internet Voting Schemes*. In: *ACM Transactions on Computer-Human Interaction*.

Mathur, Acar, Friedman, Lucherini, Mayer, Chetty und Narayanan (2019). *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. In: *Proceedings of the ACM on Human-Computer Interaction*, S. 1-32.

Molich und Nielsen (1990). *Improving a human-computer dialogue*. In: *Journal of Communications of the ACM*, S. 338-348.

Morville (2005). *Experience design unplugged*. In: *Proceedings of the ACM SIGGRAPH 2005 Web program on (SIGGRAPH '05)*.

Nechansky (2016). *The interaction matrix: from individual goal-setting to the four modes of coexistence*. In: *Journal of Kybernetes*, S. 87-106.

Nieles, Dempsey und Pillitteri (2017). *NIST Special Publication 800-12: An introduction to information security*.

Nielsen (1993). *Usability engineering*.

Nielsen (1994). *Enhancing the explanatory power of usability heuristics*. In: *Proceedings of the SIGCHI conference on Human factors in computing systems celebrating interdependence (CHI '94)*, S. 152-158.

Nielsen und Landauer (1993). *A mathematical model of the finding of usability problems*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '93)*.

Nielsen und Molich (1990). *Heuristic evaluation of user interfaces*. In: *Proceedings of the SIGCHI conference on Human factors in computing systems Empowering people (CHI '90)*, S. 249-256.

Papenmeier, Kern, Englebienne und Seifert (2022). *It's Complicated: The Relationship between User Trust, Model Accuracy and Explanations in AI*. In: *Journal of ACM Transactions on Computer-Human Interaction*.

Pfeifer (2025). *Adaption einer Methode und Entwicklung eines Software-Tools zur Verbesserung der Informationssicherheit und User Experience von Digital Identity Wallets. Masterarbeit.*

Podgorelec, Alber und Zefferer (2022). *What is a (Digital) Identity Wallet? A Systematic Literature Review*. In: *Proceedings of the IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC '22)*, S. 809-818.

Pohl (2004). *Taxonomie und Modellbildung in der Informationssicherheit*. In: *DuD - Datenschutz und Datensicherheit*, S. 678-685.

Pohlmann (2022). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*.

Preukschat und Reed (2021). *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*.

Quiñones, Rusu, Arancibia, González und Saavedra (2020). *SNUXH: A Set of Social Network User Experience Heuristics*. In: *Journal of Applied Sciences*.

Quiñones, Rusu und Rusu (2018). *A methodology to develop usability/user experience heuristics*. In: *Journal of Computer Standards & Interfaces*, S. 109-129.

Realpe, Collazos, Hurtado und Granollers (2016). *A Set of Heuristics for Usable Security and User Authentication*. In: *Proceedings of the 17th International Conference on Human Computer Interaction (Interacción '16)*, S. 1-8.

Reese, Trevor, Dutson, Armknecht, Cameron und Seamons (2019). *A Usability Study of Five Two-Factor Authentication Methods*. In: *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS '19)*, S. 357-370.

Rosenbaum, Glenton und Cracknell (2008). *User experiences of evidence-based online resources for health professionals: User testing of The Cochrane Library*. In: *Journal of BMC Medical Informatics and Decision Making*.

Rusu, Roncagliolo, Rusu und Collazos (2011). *A Methodology to establish usability heuristics*. In: *Proceedings of the 4th International Conference on Advances in Computer-Human Interactions (ACHI '11)*.

Sartor, Sedlmeir, Rieger und Roth (2022). *Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets*. In: *Proceedings of the 30th European Conference on Information Systems (ECIS '22)*.

Sasse, Brostoff und Weirich (2001). *Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security*. In: *Journal of BT Technology*, S. 122-131.

Satybaldy (2023). *Usability Evaluation of SSI Digital Wallets*. In: Bieker, Meyer, Pape, Schiering und Weich (Hrsg.), *Privacy and Identity Management*, S. 101-117.

Sauer, Alpers und Becker (2024a). *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), S. 8-16.

Sauer, Becker, Kneis, Oberweis, Pfeifer, Stark und Sürmeli (2025a). *A case study of the MEUSec method to enhance user experience and information security of digital identity wallets*. In: *Journal of Interactive Media (i-com)*, S. 125-143.

Sauer, Becker, Oberweis, Pfeifer, Stark und Sürmeli (2025b). *User Experience and Information Security Implications of Digital Identity Wallets*. In: *Proceedings of the 14th International Conference on Information Communication and Management (ICICM '24)*, S. 36-45.

Sauer, Becker, Oberweis, Pfeifer und Sürmeli (2024b). *MEUSec – Method for Enhancing User Experience and Information Security*. In: Delir Haghighi, Fedushko, Kotsis und Khalil (Hrsg.), *Advances in Mobile Computing and Multimedia Intelligence*, S. 39-53.

Sauer, Becker, Oberweis, Schork und Sürmeli (2025c). *User Experience and Information Security Heuristics for Digital Identity Wallets*. In: Plácido Da Silva und Cipresso (Hrsg.), *Computer-Human Interaction Research and Applications*, S. 339-361.

Sauer, Braun, Oberweis, Pfeifer, Stark, Sürmeli, Take und Thessen (2026). *Refining the MEUSec Method: A Follow-Up Case Study on Improving User Experience and Information Security of Digital Identity Wallets*. In: *Proceedings of the 28th International Conference on Human-Computer Interaction (HCII '26)*. *Im Druck.*

Sauer, Pfeifer, Sürmeli, Siebert und Woytal (2024c). *User-friendly Integration of Identity Wallets and Mobility Platforms: A User Experience Study Conducted in the SDIKA Project*.

Sauro und Dumas (2009). *Comparison of three one-question, post-task usability questionnaires*. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*, S. 1599-1608.

Schork (2023). *Benutzererfahrung und Informationssicherheit von digitalen Identitäts-Wallets. Masterarbeit.*

Schrepp, Hinderks und Thomaschewski (2017). *Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S)*. In: *Journal of Interactive Multimedia and Artificial Intelligence*, S. 103-108.

Sears (1997). *Heuristic Walkthroughs: Finding the Problems Without the Noise*. In: *Journal of Human-Computer Interaction*, S. 213-234.

Seffah, Donyaee, Kline und Padda (2006). *Usability measurement and metrics: A consolidated model*. In: *Journal of Software Quality*, S. 159-178.

Sellung und Kubach (2023). *Research on User Experience for Digital IdentityWallets: State-of-the-Art and Recommendations*. In: *Open Identity Summit 2023*.

Skierka (2022). *Digitale Identitäten*. In: Klenk, Nullmeier und Wewer (Hrsg.), *Handbuch Digitalisierung in Staat und Verwaltung*, S. 1-12.

Sporny, Amy, Sabadello und Reed (2022). *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations*. Verfügbar unter: https://www.w3.org/TR/did-core.

Suratkar, Shirole und Bhirud (2020). *Cryptocurrency Wallet: A Review*. In: *Proceedings of the 4th International Conference on Computer, Communication and Signal Processing (ICCCSP '20)*, S. 1-7.

Watson und Webster (2020). *Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0*. In: *Journal of Decision Systems*, S. 129-147.

West, Mayhorn, Hardee und Mendel (2008). *The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions*. In: Gupta und Sharman (Hrsg.), *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, S. 43-60.

Wharton, Rieman, Lewis, Polson, Nielsen und Mack (1994). *The cognitive walkthrough method: a practitioner's guide*. In: *Usability inspection methods*, S. 105–140.

Whitten und Tygar (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. In: *Proceedings of the 8th conference on USENIX Security Symposium (SSYM '99)*.

Yáñez Gómez, Cascado Caballero und Sevillano (2014). *Heuristic Evaluation on Mobile Interfaces: A New Checklist*. In: *Journal of The Scientific World*.

Yeratziotis, Pottas und Greunen (2012). *A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm*. In: *Journal of Human-computer Interaction*.

Zhang, Guo, Guo und Shao (2021). *Does the layout of the Android unlock pattern affect the security and usability of the password?* In: *Journal of Information Security and Applications*.

Zimmermann, Henhapl, Volkamer und Vogt (2017). *Ende-zu-Ende sichere E-Mail-Kommunikation*. In: *DuD - Datenschutz und Datensicherheit*, S. 308-313.