UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Private user-centric management of electronic services in smart communities

Antonio Robles González

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

PhD Dissertation

PRIVATE USER-CENTRIC MANAGEMENT OF ELECTRONIC SERVICES IN SMART COMMUNITIES

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF TELEMATICS ENGINEERING
AND THE COMMITTEE ON GRADUATE STUDIES
OF THE UNIVERSITAT POLITÈCNICA DE CATALUNYA
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Doctoral thesis by:

Antonio Robles González

Thesis advisor:

Dr. Javier Parra Arnau

Thesis co-advisor:

Prof. Dr. Patricia Arias Cabarcos

SISCOM (Smart Services for Information Systems and Communication Networks)
Department of Network Engineering

28 June 2023

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

_____

Javier Parra Arnau
(Thesis Advisor)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

_____

Patricia Arias Cabarcos
(Thesis Co-Advisor)

Approved for the University Committee on Graduate Studies.

A Lisa y nuestros hijos.
Gracias a mis padres por
haber abierto nuevos
horizontes.

Abstract

Smart community services are reaching nearly every area of our daily life, often requiring private information from their users. The scope of all contributors to these services is to collaboratively share information for the benefit of all stakeholders, including citizens (user), organizations, schools, and governing institutions. User contribution can be participatory – hence intentionally given – or smart community services can gather information opportunistically from user sensors and/or APIs nearly automatically or with less user influence. The present dissertation focuses on participatory user contribution.

The participatory user contribution increasingly demanded by smart community services is undertaken actively and consciously towards an accessed service, almost always requiring a user verification procedure performed predominantly through a login, based on an identification and authentication process. Throughout this process, the user usually first makes a claim by means of the presented user identity – regardless of whether the real user identity is required or not – and corroborates it performing the login. The verification process is associated with immanent privacy threats to users. The user can contribute with tagging, posting, or uploading information demanded by the smart community service, which may need reliability guarantees linked to the trustworthiness of the users. Nowadays becoming more aware about their privacy and right to self-determine, users are not so willing to contribute as demanded by the smart community service, leading to a conflict between user privacy and smart community service requirements.

The verification process of users to login and contribute to smart community services as well as their contributions to smart community services imply user privacy threats. Chapter 3 and Chapter 4 of this dissertation focus on the privacy threat analysis (PTA) of the user verification process and Chapter 5 on user self-determined privacy aware contributions to the smart community service.

Chapter 3 focuses on the PTA of the verification process in the modelling phase. The scientifically grounded LINDDUN PTA framework provides a methodology to model privacy relevant threats in software-based systems. Thus, we extend the LINDDUN PTA framework to be used systematically for modelling the verification process to perform a user login. Our contribution includes modelling the identification (I) and authentication (A) processes, considering IA methods, the extension of the trust boundary concept, and extensively extends the privacy threat mapping table. Our contributions are assembled in a systematic and reproducible step-by-step guide intended for privacy auditors including knowledge and decision support, whereby the

results do not depend on the knowledge of the auditor or his intuition. The results provide the requirements for the authentication schemes to be implemented or selected.

Chapter 4 focuses on the PTA of the verification process of realized authentication schemes. Bonneau et al. proposed a comparison framework to extensively evaluate authentication schemes for usability (U), deployability (D) and security (S), namely, the UDS framework. We extend it with a new defined privacy (P) category to become the UDSP framework. Our evaluation of the 38 authentication schemes including biometrics with UDSP reveals inter alia fundamental privacy threats, for which we propose guidelines for more secure implementations.

Chapter 5 focuses on user self-determined and user accepted revocable privacy. The contributing user in particular is exposed to privacy threats when he contributes to a critical or non-critical incident of a smart community service that requires evidence and trustworthiness for the contribution. That is the reason why we propose a taxonomy concept for classifying the criticality of incidents, including a mapping to enhanced privacy requirements and the cryptographic primitives that would support their realization in a privacy preserving fashion. Chapter 5 presents this taxonomy concept for user self-determination comprising enforceable graded revocable privacy, which is nonetheless partially applicable to the right to be forgotten. The taxonomy concept is exemplified for two proofs-of-concepts applying cryptographic primitives alike, namely blacklistable anonymous credentials and group signatures with distributed management.

Acknowledgements

Aprovecho estas líneas para agradecerle a las personas, que cada una a su manera me han apoyado en el desarrollo de la tesis doctoral.

En primer lugar, a mis dos directores de tesis Javi y Patricia por haberme dado la oportunidad de poder trabajar con dos científicos excelentes, de los que he aprendido mucho. En momentos difíciles me han escuchado y animado. Ha sido un honor para mí, gracias.

Este recorrido no hubiera sido posible sin mi tutor Jordi, también un científico excelente, que en todo momento ha estado también disponible para escucharme y orientarme. Le agradezco haberme dado la oportunidad poder realizar mi tesis en el entorno de seguridad y privacidad del departamento de telemática de la UPC. Gracias por creer en mí.

Gracias a los familiares y amigos que me han acompañado en este camino. Cada una de estas personas ha puesto de su parte para que pueda llevar a cabo este desafiante y a su vez encantador proyecto.

Gracias a mis padres por haber abierto nuevos horizontes. Y por muchos que fueran los obstáculos para superar en el camino es importante recordar, “Caminante no hay camino, se hace camino al andar …” y siempre en mente la hermosa frase que me acompaña desde mi más tierna adolescencia y aprendí de mi madre “¡El no ya lo tienes, solo puedes encontrar el sí!”.
Gracias, madre.

Y por supuesto le doy las gracias a “mi” Lisa, un sueño hecho realidad, que siempre ha creído en mí y en todo momento me ha animado y apoyado sin precedente igual. Y a nuestros hijos que con una sonrisa inocente en todo momento me han acariciado y animado para todo.
Gracias a Lisa y nuestros hijos.

Contents

List of tables

List of Figures

Chapter I

1 Introduction

The rapidly increasing number of internet services are ubiquitously reaching every area of everyday life and the diffusion is still rising and growing. The services can be used by the user either personalized or not, both being building blocks of how users (smart citizens) can contribute individually or collaboratively to smart communities. The activity area of a smart community can comprise a local area such as a city, whole country, continent or the whole earth in the sense that different stakeholders including citizens, organizations, schools, and governing institutions cooperate. The stakeholders collaborate as partners in partnership to achieve the best results in the use of information and communication technologies [1].

Collaborative users can contribute participatory [2] (intentionally) by actively passing information, e.g. posting, tagging, uploading, or allowing, e.g. the usage of the general positioning sensor (GPS) of a mobile phone or other devices or sensors. Users' information contribution can also be opportunistically [2] based on automatically (with less influence by the user) provided information by further sensors of his devices or gathered by APIs, e.g. the browser that the user uses facilitating a malicious service to generate related destructive fingerprinting [3, 4] based on the information disclosure through user device hardware (HW), software, personal configurations, and other settings. Smart communities comprise contributing users being part of a virtual group without consciously joining a group. On the one hand, services opportunistically use e.g. a mobile phone GPS sensor to detect traffic jams or warning apps use Bluetooth for contact tracing of persons infected with COVID-19 or use the number of logged-in mobile phones in a radio cell to detect crowds and predict their movement. On the other hand, user participatory actively contributes from various devices with e.g. uploads, comments, posts or tagging. Participatory user contribution is in the focus of the present dissertation.

Like all other internet services, services in smart communities can be categorised into those requiring an explicit user login to verify the user claim with the presented user identity and those

that do not require an explicit user login. Predominantly smart services require a user login independent of whether the real user identity is required or not, so that the contribution of the user to the smart community is reliable and trustworthy as far as required by the respective service. At this point, we want to stress that services in smart communities not only comprise the so-called smart services often equipped with diverse sophisticated sensors (e.g. a traffic regulation service for adaptive traffic light switching, the usage of emergency mobile cell broadcasts or information about accessible electric car charging stations), but also ordinary services such as mail providers, online shops, or home banking. Smart services as well as so-called ordinary services are interlinked, with one simple example being that a user sets an agent that determines actual traffic load for a certain route on an online car route planner and then sends a mail to the user once an acceptable traffic flow without congestion is expected. Of course, even the smart service route planner will probably also be related with the user mail for administration purposes. In smart communities and coming along smart services of course reliable and trustworthy machine to machine communication (M2M) with the coming along identification and authentication between the machines is required and still in operation, but not in our focus because we focus on user authentication schemes.

In the context of users contributing to smart community services, the focus of this dissertation is twofold: on the one hand, the verification process that a user must pass for proving the claim by presenting a user identity (UID) [5] to log in; and on the other hand, the user contribution to the smart community service including demanded reliable evidence and user trustworthiness. Smart community services have stringent requirements towards the user contribution, so that from their perspective in the best case the user always contributes with all available information to the smart community service regardless of whether the user privacy is compromised. This verification process requires passing an identification (I) and authentication (A) process [6] towards the service to successfully perform a login. The user login can be based on different authentication schemes using one or more of the three authentication factors to provide evidence, namely knowledge (something you know), possession (something you have) or being someone (something you are, biometric) [7, 8]. The privacy of the user can be jeopardized by diverse privacy threats focusing on the implemented authentication scheme when performing the login to access a service and through the user contribution. The privacy of the user must be safeguarded. Consequently, the focus is placed on analysing the immanent privacy threats to the verification process of the user login and contribution to analyse the modelling of the identification and authentication process and authentication schemes, as well as the rising conflict between the stringent smart community service requirements for contributions and the user right of self-determination.

A feasible recommendation is that of the European Union for a privacy impact assessment framework (PIAF) [9]. A PIAF starts with a privacy threat analysis (PTA), which is the basis for the following privacy impact assessment. Handbooks and guides to perform a privacy impact assessment (PIA) [10–12] as well as the PIAF require a high degree of intuition by the auditor realizing the PIA, who is not always an expert and the PIA lacks special PTA support. According to an ENISA privacy report [13], existing privacy risk analysis methods are based on adopted security analysis methods, e.g. EBIOS [14] or STRIDE [15]. In different scientific publications, the LINDDUN privacy threat analysis framework [16] – which is based on STRIDE– is referenced and proposed e.g. for health systems [17, 18] or the architecture and development of national identification systems [19]. To the best of our knowledge, LINDDUN is the only systematic and scientifically proven PTA framework.

A PIA of the verification process for user login based on an identification and authentication process also requires a previous PTA. In the absence of a systematic and reproducible methodology to perform such a PTA we take the LINDDUN privacy threat analysis framework and extend it to be usable for the verification process of user login, hence for the underlying identification and authentication process. The application of the LINDDUN framework focuses on the analysis of generic modelled scenarios still in process to be determined, and thus we tailor it for modelling the identification and authentication process and components, so that afterwards the results are usable to determine or improve the necessary authentication scheme. LINDDUN[1] is an acronym of the underlying privacy threats that threaten the corresponding privacy properties.

A privacy-centered analysis of authentication schemes, ready to be introduced to realize the verification process for user login additionally requires evaluating its usability, deployability and security, which hold interest for the user as well the service. Independent of the LINDDUN framework-based contribution, diverse frameworks [20–23] focus on the evaluation of usability experiences for the user, deployability and security of the authentication scheme. Among them, the most comprehensive evaluation framework considering usability (U), deployability (D) and security (S) for the most extensive number of authentication schemes including three biometrics is developed by Bonneau et al. [20]. Like others [20–23], the UDS framework [20] only considers privacy to be subliminal, thus without an explicit privacy (P) category. Here is where we tie in and extend the UDS framework of Bonneau et al. [20] to become UDSP framework and facilitate additionally performing a privacy evaluation of authentication schemes. The cycle is initiated with the LINDDUN-based PTA analysis for the verification process for login to elicit the most

[1] **L**inkability, **I**dentifiability, **N**on-repudiation, **D**etectability, **D**isclosure of information, content **U**nawarness, policy and consent **N**oncompliance.

suitable scheme for the modelled scenario, and once a concrete authentication scheme is realized it can be closed with a further privacy threat analysis performed with the extended UDSP framework. Naturally, the extended UDSP framework can be applied without previously having applied the extended LINDDUN framework.

The machine learning (ML)-based behavioural biometrics from [24] are also included and evaluated with the extended UDSP framework. The privacy benefits[2] (PB) introduced to the privacy category of the UDSP framework comprise PB1 - PB7[3] partially focusing on traditional authentication schemes mainly based on passwords, tokens, or cognitive authenticators and biometrics. ML-based feature extraction of behavioural biometrics [24], voice, gait, hand motions, eye-gaze, heartbeat and brain activity includes the privacy threats of identity disclosure and attribute disclosure, and therefore with ML it is possible to infer users' personal information from the behavioural biometric data. The user only consented to the usage of his behavioural biometric data by the service for authentication purposes, and hence it is not to be used to infer personal information. In [24], the authors survey privacy-protecting technologies to mitigate this privacy threat, therefore trying to achieve the privacy goals identity protection and attribute protection (which are in line with the PB3 and PB4 introduced to the extended UDSP framework) even for a data-publishing scenario towards the service. The data-publishing scenario comprises, that the service has full access to the biometric data. The authors in [24] assume a malicious service. A further important aspect arising with the consideration of the behavioural biometrics is that they can be based on covert or overt traits, with the latter challenging the realization of the authentication scheme to be resistant to threats based on captured biometric data as a by-product.

The stringent, all-encompassing user information, requirements of the smart community service for the demanded user contribution and the user right of self-determination anchored in [25] comprising stated or inferred rights such as the right to be asked for consent, the right to have privacy and the right to be forgotten are in conflict. This area of tension is in the focus of this dissertation. The motivation of informed and privacy-aware users to be willing to contribute depends on how his right of self-determination is guaranteed by the smart community service. The contribution as demanded by the smart community service endangers the user's self-determination and privacy because the possibility for the user to self-determine and enforce his privacy demand is lacking. Simply relying on the smart community service compliance is insufficient. This is the reason why the last part of the thesis focuses on the user's right to be

[2] We will use the term privacy benefits for convenience and comparability reasons with Bonneau et. al [1] instead of privacy properties.
[3] PB1 No-Trusted-Third-Party, PB2 Requiring-Explicit-Consent, PB3 Unlinkable, PB4 Resilient-to-Identifiability, PB5 Intervenability, PB6 Transparency and PB7 Resilient-to-Impersonation.

asked for consent and the right to have privacy extended with a user-accepted gradation and revocation of privacy, depending on the criticality requirements of the incident to which he contributes. The enforcement, gradation and revocability of privacy are e.g. realizable based on appropriate cryptographic primitives comprising anonymous credentials and group signatures. The presented taxonomy concept facilitates the user to accept (give consent) the extent to which his privacy is revocable in case he misbehaves during the contribution to the smart community service. The user will be informed if the stakeholders involved detect a misuse case and proceed with the revocation of his privacy, so that he is then anonymously blocked or additionally in coordination with the openers his identity is revealed to be prosecuted.

1.1 Objectives

The objectives across the dissertation are threefold and focus on the verification process for user login and the user contribution to smart community services. On the one hand, the modelling phase of the underlying login scenario as well as the implemented authentication scheme are subjected to separate privacy threat analysis, both of which are systematically-reproducible. On the other hand, the user privacy requirements for user contributions are detailed to achieve user-driven self-determination with revocable privacy. The resulting three objectives of the dissertation are as follows:

- **Privacy Threat Analysis of the verification process in the modelling phase**

The realization of the privacy threat analysis (PTA) of the verification process of a user login scenario requires a systematic scenario modelling phase to elicit the requirements. The modelling phase must facilitate the PTA of the identification and authentication process of the user login in the concrete scenario. The modelling and PTA result should be usable to contribute to the design and implementation of the appropriate authentication scheme for the modelled scenario. In contrast to existing PTAs the result should not depend on the knowledge of the auditor or its intuition. Especially for the modelling and PTA of the identification and authentication process, the aim is to tailor a systematic step-by-step guide through the modelling of the IA process and PTA including knowledge to support the auditor for reproducibility purposes.

- **Privacy Threat Analysis of the verification process of realized authentication schemes**

A designated or implemented authentication scheme should be subject to further privacy-centered threat analysis focusing on the whole authentication scheme. The usability, deployability and security of authentication schemes are extensively evaluated but privacy is neither addressed systematically nor in an explicit privacy category. Thus, it is required to investigate how to realize

a privacy-centered analysis of the authentication schemes, systematically relate not offered privacy criteria with corresponding privacy threats and mitigate fundamental privacy threats.

- **Revocable Privacy – Enhanced user privacy requirements for user-driven self-determination**

The conflict between the stringent smart community service requirements that demand as much information as possible about the user and his contribution, and the right of the user to have privacy is the starting point. The contributing user in particular is exposed to privacy threats when he contributes to whatever type of incident to a smart community service, especially for critical incidents that require evidence and trustworthiness from the user for the contribution. A taxonomy concept for the classification of the criticality of the incidents, enhanced user privacy requirements and a high-level description of the flow for the use case of a user contributing to a smart community service is required. The focus is to work out a concept for user self-determination comprising enforceable graded revocable privacy, which at present is partially applicable to the right to be forgotten.

1.2 Summary of Contributions

We proceed with an overview of the most significant contributions of this dissertation.

Privacy Threat Analysis of the verification process in the modelling phase

The realization of Privacy Impact assessment (PIA) is undertaken to determine the privacy objectives of a system and in Europe the PIAF (Privacy impact Assessment Framework) [9] research project recommends in a deliverable the application of the created “A Privacy Impact Assessment Framework for data protection and privacy rights.” The starting point of a PIA is a privacy threat analysis (PTA), which neither the PIAF nor existing privacy risk analysis methods based on adapted security analysis methods e.g. EBIOS [14] and STRIDE [15] address. The only promising PTA framework for privacy threat analysis is *LINDDUN: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements [16]* based on STRIDE and globally addressing software-based systems.

The verification process of a user login based on an identification and authentication process must be subject to a PIA and consequently to a PTA to safeguard the user’s privacy. In the absence of a systematic PTA methodology, we take up the LINDDUN PTA framework [16] and extend the corresponding problem space to be applicable to modelling the identification and authentication process. For this purpose, we extend the existing *trust boundary/change of privileges* concept, and we categorize to cover centralized, decentralized up to delegated user identification and/or authentication. The results are recorded usable for an auditor in identification and authentication

(IA) methods tables, dataflow diagram (DFD)-drawings depicting trust boundaries and in an extensively extended table for DFD elements to privacy threat mapping, all focusing on the modelling of the identification and authentication process to perform a PTA. We apply and discuss the extension of LINDDUN in a two-fold proof-of-concept (PoC) scenario, one with a password a second with smartcard authentication. This first contribution is in [26].

The realization of the privacy impact assessment (PIA) requires intuition and knowledge by the auditor to perform a PIA even more to perform a privacy threat analysis (PTA). The consequence is that the result of a PTA depends on the auditor, and thus it is not reproducible. This is the reason why we assemble a systematic procedure guide to apply our enhancement of the problem space of the LINDDUN PTA framework [16] for modelling the IA process. Our guide scrutinizes the extension of the LINDDUN PTA framework [16] so that the auditor profit from the knowledge included by us and we also combine it with the decision support that we added. This second contribution is also in [26].

Privacy Threat Analysis of the verification process of realized authentication schemes

Authentication schemes are analysed extensively from different perspectives that comprise criteria related with the usability (U), deployability (D) and security (S). The privacy-related criteria are not addressed explicitly if only with less importance. The literature review brings out the widely applied UDS framework from Bonneau et al. [20] as the one that applies most criteria from UDS categories to the most authentication schemes, namely 35. An integral view of the authentication schemes also makes it indispensable to perform a privacy threat analysis.

We extend the UDS framework [20] with a privacy benefit category, thus becoming the UDSP framework, and add behavioural biometrics from [24], whereby the UDSP framework comprises 38 authentication schemes. The privacy category comprises benefits related to authentication schemes as well as machine learning-based behavioural biometrics to protect biometric data captured for authentication purposes. We perform an evaluation with the extended UDSP framework of sample authentication schemes. This third contribution is in [27].

Our extension of UDS framework [20] yields to the UDSP framework for the analysis of the privacy of authentication schemes, which includes a privacy category with new privacy benefits (properties). Additionally, we consider the existing security benefit category in the seminal paper of the UDS framework to define the privacy benefit PB7 with sub-benefits based on these security benefits. We evaluate the authentication schemes with the resulting UDSP framework, and thus fundamental privacy threats for the authentication schemes and security related privacy sub-benefits are revealed. Afterwards, we propose implementation approaches to mitigate these fundamental privacy threats. This contribution is necessary to ensure that fundamental avoidable

privacy threats affecting most of the schemes are mitigated. This fourth contribution is also in [27].

Revocable Privacy – Enhanced user privacy requirements for user-driven self-determination

The smart community service demands user contributions for the services offered, e.g. emergency management services (e.g. 112 and 911). The smart community service requires user contributions with evidence and trustworthiness because the contributions could set off a laborious, time-consuming, and costly flow for a smart community service, e.g. the roll out of emergency teams such as the fire brigade and/or emergency ambulance including medical staff, policeman or other rescuers. The most prominent examples are traffic accidents, house fires, people drowning or other emergency incidents. The other extreme is that of user contributions to social networks about trivial themes, e.g. sunny weather preferences or personal, non-offensive opinions. Thus, the contribution to the emergency management service for a critical service requires a more trustworthy contribution with evidence than the mentioned social network contribution about weather preferences. Especially the critical services that require evidence-based trustworthy contributions could keep users from contributing to critical services because they worry about their privacy.

We take up this conflict between the legitimate claim for user privacy and smart community service requirements to propose a user-centered solution, so that users are more willing to contribute because their privacy is respected based on self-determination. Our contribution includes a taxonomy concept for the classification of the criticality of services, so that the smart community service requirements for the trustworthiness of the contributions and the evidence are scalable. We enhance the user privacy requirements in accordance with the European GDPR [25] to achieve self-determination comprising enforceable graded revocable privacy while being partially applicable to the right to be forgotten. The enforcement, gradation and revocability of privacy are e.g. realizable based on appropriate cryptographic primitives comprising anonymous credentials and group signatures. The user can now contribute by applying *revocable privacy*. This means that depending on the criticality of the service, the contributions are made in a self-determined manner by the user with the required level of trustworthiness and evidence. This implies that the user privacy is maintained, so that no one knows who made the contribution as long as the user did not misuse the service. A misuse, e.g. could be to report an accident with injured people whereas nothing happened. In this case, and depending on the severity of the misuse and the criticality of the service, the graded revocable privacy is applied to reveal the responsible of the misuse. This fifth contribution is in [28].

1.3 Related publications

The thesis results are mainly published, in process of being peer reviewed in a journal or submitted to a conference.

JCR Journal Publications:

1. Robles-González, A., Parra-Arnau, J., and Forné, J. 2020. A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes. Computers & Security, Vol. 94 no. 101755. DOI: https://doi.org/10.1016/j.cose.2020.101755. Impact factor (2020): 4.438. [26]
2. Robles-González, A., Arias-Cabarcos, P., and Parra-Arnau, J. 2023. Privacy-Centered Authentication: a new Framework and Analysis. Computers & Security. Available online 26 June 2023, 103353, DOI: https://doi.org/10.1016/j.cose.2023.103353. Impact factor (2021): 5.105. [27]

Conference:

3. Robles-González, A., Arias-Cabarcos, P., and Parra-Arnau, J. Revocable Privacy – Enhanced user privacy requirements for user-driven self-determination. Submitted to the International Conference on Networked Systems (NetSys23) in June 2023. [28]

1.4 Outline of the thesis

The structure of this dissertation is based according to the research objectives defined in section 1.1 as follows:

Chapter 2 presents the background and preliminaries. Chapter 3 focuses on the privacy threat analysis-oriented modelling of the verification process of user login. The results rely on the given background and state of the art for privacy impact assessment (PIA), the LINDDUN framework [16] in Chapter 2 as well as the identification and authentication background in section 3.2. The contributions in section 3.3 are two-fold. On the one hand, the LINDDUN framework [16] is extended for identification and authentication schemes, mainly based on the consideration of diverse I- and A-methods, the subdivision of the verification process and conceptualization of the trust boundaries. On the other hand, the modelling of the LINDDUN framework is systematized in a step-by-step guide that guides the auditor through the corresponding extended LINDDUN framework steps. Section 3.4 presents the application of the extended LINDDUN framework to a proof-of-concept scenario for evaluation purposes and a discussion, including a related work review to emphasize the value and novelty of the contributions. Conclusions and future work outlook are given in section 3.5.

Chapter 4 focuses on the privacy-centered analysis of authentication schemes. The contributions are grounded on the background provided in section 2.2 for evaluation frameworks for authentication schemes, and privacy and biometric schemes in section 4.2. Section 4.3 presents the extension of the UDS framework that becomes the extended UDSP framework including the privacy category[3] that we assembled. Section 4.4 presents the evaluation of the sample authentication schemes with the extended UDSP framework (see Table 10). Section 0 discusses the evaluation and offers implementation approaches to mitigate fundamental privacy threats. Concluding remarks with future work and prospect of a future authentication scheme are given in section 4.6.

In Chapter 5, the revocable privacy taxonomy concept to facilitate user self-determination is presented. The required background is presented in section 5.2, before section 5.3 presents the stringent smart community service requirements for a user contribution. In section 5.4, the User's right of self-determination for enhanced revocable privacy as the basis for the taxonomy concept is given and applied in section 5.5 to the stringent SCS requirements for a user contribution from section 5.3. Section 5.6 presents proofs-of-concepts including applicable cryptographic primitives. The chapter concludes with the discussion and conclusion in section 5.7.

Finally, Chapter 6 offers in section 6.1 an individual conclusion for each of the three objectives and concludes with overarching conclusions, before finally section 6.2 provides an overview of future work.

Chapter 2

2 Background and preliminaries

2.1 Privacy Impact Assessment and Threat Analysis

We review the background and state of the art of related technologies. We start with PIA and PTA. Existing PTA approaches are derived from security threat analysis (STA) solutions but do not tackle PTA from a sufficiently systematic perspective. As far as we know, LINDDUN is the one scientifically substantiated systematic methodology exclusively used for PTA.

2.1.1 Privacy Impact Assessment

A PIA [13] is performed to determine the privacy objectives of a system. In Europe, the PIA Framework recommendation was created in the project entitled "A Privacy Impact Assessment Framework for data protection and privacy rights" (PIAF) [9]. Generally, it is recommended that a PIA initially should be conducted in a short version, and then if necessary in an extended version. After the review of handbooks, guides or other formal descriptions of how to perform a PIA, e.g. [29], [11], [12], the conclusion is the same as for the PIAF project. All present a widespread set of recommendations, procedure descriptions and/or check lists, etc., and all require a high degree of intuition by the person realizing the PIA. This person is not always the necessary expert for a substantiated PTA and the PIA procedure does not offer special PTA support to guide the person realizing the PIA. A PTA is the starting point to perform a PIA. According to the ENISA Privacy Report [13], existing privacy risk analysis methods use adopted security analysis methods, e.g. EBIOS [14] and STRIDE [15].

In the specific context of RFID, one PIA is proposed by the European Commission [30] and another by the BSI [31]. The PIA guideline [31] for RFID created by the BSI considering the European Privacy and data protection Impact Assessment Framework for RFID applications [30] is usable for dedicated RFID-based scenarios and offers solid guideline. The European PIA Guideline [30] is based on BSI and guides through three RFID-based scenarios from the retail, public transportation and automotive environments.

The "Conducting PIA" of the UK information Commissioner's office [12] describes the process to carry out a PIA and a guide to identify the privacy-related risk at a very high level without explicitly referring to privacy threats.

In the context of Chapter 3, we will focus on PTA, as the indispensable fundament for every convincing PIA. A systematic approach for PTA is required to make it easier for the auditor to perform a reliable PIA.

2.1.2 Privacy Threat Analysis

A PTA is the starting point to perform a PIA. According to the ENISA Privacy Report 2014 [13], the only existing privacy risk analysis methods adopt security risk analysis methods, e.g. EBIOS [14] and STRIDE [15]. The former focuses more on the methodology for privacy risk management, considers threats at a high abstraction level and tackles security needs such as confidentiality, integrity and availability [32]. On the other hand, the STRIDE methodology is the initial point to develop LINDDUN. As explained in the next subsection, LINDDUN is a specialized PTA framework that instructs the pertinent staff performing the PTA on how to make a system model and provides a list of threat types for this purpose. Moreover, it instructs how to map them to elements on the system model. Next, we elaborate more on this framework.

2.1.3 LINDDUN Framework: A Systematic Approach for Privacy Threat Analysis

Throughout different scientific documents, LINDDUN[4] is referenced as one applicable PTA methodology and/or is used to analyse concrete scenarios, e.g. in health systems [17, 18]. To the best of our knowledge, LINDDUN is the only promising PTA framework that is systematically and scientifically proven.

The LINDDUN methodology offers a systematic procedure for eliciting and fulfilling privacy requirements and is based on STRIDE [15], an approach for security threat modelling. The LINDDUN framework was first presented in [16] and – according to their authors – the primary contribution is a systematic methodology to model privacy-specific threats. A further important contribution is that it provides an extensive catalogue of privacy-specific threat tree patterns [33] and defines a mapping of most commonly known privacy enhancing technologies (PET) to identified privacy threats.

One of the authors of LINDDUN evaluated the framework in [34] and provided some improvements. A contribution of [34] that we would like to stress at this point is the extension of

[4] LINDDUN is an acronym of these privacy threat categories: linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, noncompliance.

the “LINDDUN privacy threat catalog.” Another contribution to be highlighted is the reduction of interaction between LINDDUN and STRIDE.

The improvement of the LINDDUN framework proposed in [34] leads to the improved LIND(D)UN methodology, which is described in the tutorial [35] and the corresponding updated “LIND(D)UN privacy threat tree catalog” [33]. We will use LINDDUN throughout the thesis, since we will consider the information disclosure threat.

The LINDDUN framework is divided into two phases, namely the “PROBLEM SPACE” and the latter the “SOLUTION SPACE”, as shown in Figure 1 (original figure taken and identically redrawn by ourselves).

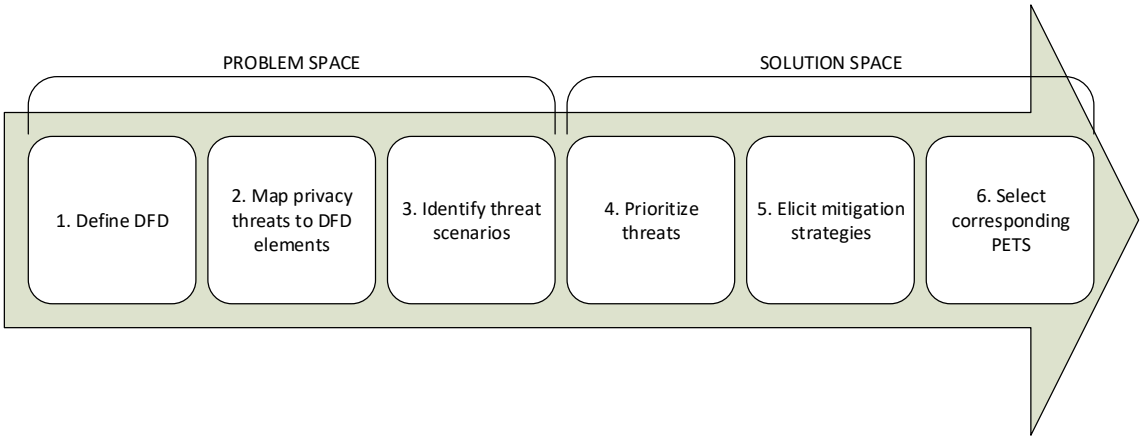


Figure 1. Formalized LINDDUN steps [1].

The emphasis throughout Chapter 3 is placed on the PTA, and for this reason the focus will be on the “PROBLEM SPACE” of the LINDDUN framework (see Figure 14 in Appendix B), and hence on steps 1 and 2. The problem-oriented steps of LINDDUN rely on [35], [33], [36] and [37].

2.1.3.1 Recent review of LINDDUN related work

As rapidly as the number of internet services increases and ubiquitously reaches nearly every area of daily life, the related technology evolves at a similar pace. Especially for the LINDDUN PTA Framework [16], a brief overview of the most recent and relevant publications is given with a focus on the application scenarios of LINDDUN or its extension.

In 2021, the LINDDUN privacy threat modeling framework was included to the National Institute of Standards and Technology (NIST) [38] as a Guidance/Tool resource in the Privacy Framework section.

The publication [39] from April 2022 presents systematization approaches to guide the auditor from the threat tree node to the most suitable countermeasure with a focus on hard privacy. One of the authors is Kim Wuyts who also published the LINDDUN seminal paper [16]. In [39], the

authors address the problem "*However, when moving from the problem space into the solution space, typically some details of the identified threats are lost and the problem space knowledge is abstracted and not used to its full potential when selecting the most suitable mitigation solution.*" The authors introduce a knowledge-enriched solution-space methodology and apply it to the LINDDUN threat trees to support the user in the selection, and thus they present flowcharts providing help questions for the user to be guided.

As reminder, in our LINDDUN-related publication [27] we created a step-by-step guide for the auditor to support him in modelling the identification and authentication process. We also include knowledge combined with the decision support that we added.

The following extract is to emphasize the ongoing dissemination of the LINDDUN PTA framework gathered from scientific publications.

LINNDUN is proposed in 2022 for the privacy threat modelling [19] of the identity management of a National Identification System.

The publication [40] in 2022 investigates and shows how the LINDDUN PTA framework is applied for the privacy analysis of a mobility-as-a-service system.

In 2022, the authors of [41] applied the LINDDUN PTA framework mapping the LINDDUN threats to the modelled autonomous car system (ACS) as well as relating the LINDDUN threats to the GDPR principles. In an overview table, LINDDUN is rated high for maturity, thus further corroborating our selection.

The authors in [42] from 2022 reported an empirical study of 27 mental health apps aimed at systematically identifying and understanding data privacy. The authors apply LINDDUN to elicit privacy threats.

2.2 Frameworks for the evaluation of authentication schemes and their limitations

In this section, we review evaluation frameworks for authentication schemes and analyse their limitations.

UDS framework concept and components

Bonneau et al. [20] presented the UDS framework to evaluate authentication schemes and apply three benefit groups of usability, deployability and security for this purpose. The benefits comprise eight usability benefits, six deployability benefits and eleven security benefits, with the latter including three privacy benefits. This, the UDS framework allows a comprehensive assessment. The authors used the framework to evaluate – as a reference – the legacy password

scheme, and compare 35 additional authentication schemes. They stated that there are no schemes that fulfil all benefits and therefore not able to replace the password scheme alone. It depends on the scope where the scheme is used to determine which benefit group is considered with higher weight. They emphasise that no examined scheme is *perfect - or even comes close to perfect scores*. The authors [20] explicitly highlighted that the presented benefit list is not complete and could be extended, whereby they explicitly mentioned privacy. For understandability, we offer a brief explanation of the UDS framework terminology.

The authors in [20] apply the benefit categories of usability, deployability and security, together comprising 25 benefits for the authentication schemes. Usually we talk about privacy properties, but due to compatibility and readability we also use the term benefit. The authors evaluate the authentication schemes grouped into categories and we add the behavioural biometric category we introduced, as can be seen in the first two columns of our Table 10. The UDS framework benefits are evaluated as *offers the benefit*, *almost offers the benefit,* or *does not offer the benefit*. Additionally, they give a comparison to the reference password scheme indicating whether the evaluated scheme is better or worse than passwords or without any change.

UDS framework extensions

Mayer et al. [21] proposed an extension to UDS with 63 sub features (benefits), based on the 25 features used by Bonneau et al. [20]. They introduced granularity by terms of complementary evaluation options like *fulfilled-benefit* or *non-fulfilled-ben*efit and for certain benefits additional (differentiation) characteristics, albeit none of them related to privacy. In ACCESS[5], the benefit categories UDS include 48 sub-features. The core function of ACCESS is to offer a decision support platform for developers and decision-makers, which after selecting the necessary UDS benefit requirements with the possibility to indicate hard-constraints returns a rated list of authentication scheme candidates. The central benefit groups remain as in UDS, and no further privacy-related benefits were added into the security benefit group.

The main contribution of the paper is the construction of a feasibility analysis using an analytic hierarchy process based on reusable expert knowledge and offer a decision support system as a collaborative platform, which they presented in their work with ACCESS. They include in the biometrics category fingerprint, iris and voice from [20], PalmVeins, Face, Hand Geometrics, Retina Scan, Face Recognition, 2D Gesture, 3D gesture, Keystroke Dynamics, Signature Dynamics, Hand vein Triangulation and Knuckle Shape, as listed in ACCESS. The authors in ACCESS grouped the authentication schemes into thirteen categories, but the categories 2FA

[5] access.secuso.org [21]

(only with Keystroke Dynamics and Password) and Motion-based (only with KinWrite, writing in space a password) combine two categories used in [20] in both schemes, thus with eleven remaining categories.

Zimmermann et al. [43] proposed an extension of UDS to "*revisit the rating process and describes the application of an extended version of the original framework to an additional 40 authentication schemes identified in a literature review*." A further step was to rate the 85 (including the 45 schemes resulting from [21] adding 10 schemes to [20]) schemes according to 63 sub features derived from the initial original UDS features (the so-called benefits) and specified in the technical report of Mayer et al. [21].

In a further paper [44], the authors conducted a rating of 85 authentication schemes with the objective usability, deployability and security of the paper [20], with the purpose of being able to compare objective ratings with subjective user perceptions. The authors [44] arrive at the conclusion that despite the lower score for objective criteria compared to the other schemes, password and the fingerprint schemes, are the most preferred by the participants. The subjective user perceptions favour password followed by fingerprint. The security as well as the privacy related security benefits applied in UDS [20] were still not improved in [44] with respect to objective evaluation, but nonetheless the paper also underpins the maturity of the UDS presented in Bonneau et al. [20].

In [22], Alaca et al. present an evaluation framework that is like UDS and focusing on single sign-on (SSO) systems. The authors evaluate fourteen web SSO systems. The applied core benefits of usability, deployability and security are similar to those of the UDS framework [20], but not so comprehensive as in [20]. They add a SSO specific category of *design properties* in that they interrelate the identity provider (IdP), service provider (SP), user, user identity, IdP authentication type and the user devices involved. A further core benefit is privacy, with three benefits, all of them related with the SSO environment. The UDS framework [20] – beside SSO – schemes covers a total of ten categories (password manager, proxy, federated SSO, graphical, cognitive, paper tokens, visual crypto, hardware tokens, phones and biometric). Thus, it offers a wider range of applicability, and thus we proceed with [20].

Other frameworks

Broders et al. [23] focus on complementary modelling techniques, so that the categories usability and security of authentication schemes can be analysed together. The modelling is based on tasks to depict the *quantity and complexity of the work that users have to perform to complete an authentication*. Security is evaluated based on attack trees considering eavesdropping (key logging, video recording, shoulder surfing), phishing and brute force related to the tasks, summing

up five criteria. Usability is evaluated based on workload and time performance for the tasks of the authentication schemes. The goal of the paper is to analyse jointly usability and security. The workload is measured for perceptive, cognitive, and motor tasks, thus involving four criteria for the evaluation of usability. The evaluated authentication schemes are Google 2 Step and Firefox Password Manager. The framework covers a very limited number of authentication schemes and categories without addressing privacy.

The National Institute of Standards and Technology (NIST[6]) offers recommendations for digital authentication of users to federal network-based systems targeted at agencies. NIST's special publication 800-63-3 [45] as a framework includes aspects of *enrolment and identity proofing*, *authentication and lifecycle management* and *federation and assertions*. Suggestions are given to use e.g. pseudonymous identifier or pairwise pseudonymous identifier and for authentication it makes references to [46]. The NIST special publication 800-63B [46] detailing *authentication and lifecycle management* from [45] generically considers diverse combinations of applicable authentication factors and authenticators such as secrets or biometrics. The privacy considerations in NIST [46] are informative and comprise privacy controls and in [46] consider legal and compliance aspects related to personal identifiable information (PII), as well as the associated risk processing the PII.

NIST's special publication 800-63B [46] references the NIST special publication 800-53 [47] "Security and Privacy for Information Systems and Organizations" document, which provides very generical standard recommendation covering controls and procedural aspects, alike, but not as identically as ISO27001[7] [48] for establishing an information security management system. Summing up, NIST offers a broad range of aspects as well as controls to consider e.g. in the context of authentication and related privacy, but at a very high level intended to be used by organizations or system implementors to be guided throughout the establishment of related processes and common controls. We state that at a high level NIST offers recommendations for the usage of authenticators and their combinations or suggestions of how to achieve pseudonymous usage of user identifier. They define for a limited number of authenticators guidelines how they can be assembled to become authentication schemes offering a required assurance level. This restricts the evaluation to authentication schemes based on the considered authenticators, while no privacy-focused evaluation of authentication schemes is given.

Comparative overview of frameworks

[6] www.nist.gov
[7] www.iso.org/isoiec-27001-information-security.html

Table 1 offers a comparative overview of the previously-mentioned and reviewed frameworks [20–23, 43, 44, 49]. The fact that the UDS framework of the seminal paper of Bonneau et al. [20, 49] has been widely applied and extended [21, 43, 44] underpins the general maturity of the UDS framework. We observe that all reviewed frameworks comprehensively consider benefits in the usability, deployability, and security categories, as in [20], and only a very limited number of privacy benefits or criteria.

Framework	Title	Author(s) and Ref.	Year	(sub-) benefits (criteria)/categories	Authentication categories/schemes	Results
UDS	Paper: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes	Bonneau et al. [8]	2012	25/UDS	10/9 (35)	Usability, deployability and security benefits are applied for evaluation. Fewer security benefits with privacy aspect are considered. In the published paper nine authentication categories are considered.
	EXTENDED Version: Technical Report: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes	Bonneau et al. [17]	2012	25/UDS	10/35	See comment above. In the EXTENDED Version 35 Authentication schemes are evaluated .
UDS extension	Supporting Decision Makers in Choosing Suitable Authentication Schemes	Mayer et al. [18]	2016	63/UDS	11/45	The authors in ACCESS offer an expert based knowledge decision support system. They group the authentication schemes into thirteen categories, but the categories 2FA (only with Keystroke Dynamics and Password) and motion-based (only with KinWrite, writing in space a password) combine in both schemes two categories used in Bonneau [1], thus the remaining categories are 11 too.
	The Quest to Replace Passwords Revisited Rating Authentication Schemes	Zimmerman et al. [9]	2018	25/UDS	10-12/85	Usability, deployability and security benefits are applied for evaluation. Privacy is not considered. Present results in ACCESS[5], an online assess tool for authentiction scheme with extended UDS benefits.
	The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes	Zimmerman et al. [10]	2020	48/UDS	5/12	Focused on usability, deployability and security evalaution. Privacy is not considered.
Other related frameworks	Generic Multimodels-Based Approach for the Analysis of Usability and Security of Authentication Mechanisms	Broders et al. [20]	2020	9/US	2/2	Model-based on user tasks extended with threats and effects on the tasks. The focus is on security and usability. Privacy is not considered.
	Comparative Analysis and Framework Evaluating Web Single Sign-on Systems	Alaca et al. [19]	2020	14/UDSP	1/14	The focus is on usability, deployability, security and fewer on privacy aspects.
Our work: UDSP	PRIVACY-CENTERED ANALYSIS OF AUTHENTICATION SCHEMES: THE NEXT QUEST TO REPLACE PASSWORDS	UDSP framework	2022	32/UDSP	11/38	The UDS framwork is extended with privacy benefits, the biomtrics are extended and a privacy-based evaluation is done.

Table 1: Comparison of evaluation frameworks for authentication schemes with the UDSP framework.

Furthermore, we observed and the authors suggested to extend the benefit list, because e.g. no dedicated privacy category exists. We pick up the suggestions of the authors in [20, 49] and extend the benefit groups. Thus, we introduce a new group with privacy benefits including the existing three privacy benefits considered in the security benefits. The privacy benefits that we introduce are described in section 4.3.

Chapter 3

3 Privacy Threat Analysis of verification process in the modelling phase

3.1 Introduction

Emerging smart communities and social networks demand increasingly more user interaction to perform identification (I) and authentication (A) procedures. Users usually carry out an IA process, send personal, sensitive information to a service provider that might not be fully trusted, or this service provider might want to share this information with other providers and third parties. Therefore, an IA process embracing different domains of responsibilities could result in unwanted information disclosure and/or linkability, and ultimately jeopardize user privacy. Although user IA processes are present in a large variety of procedures and supported by heterogeneous software and hardware, the simultaneous protection of user privacy is an open problem and the focus of Chapter 3.

From a legal perspective, the European Union legislation requires protecting the processing of personal data throughout the whole IA procedure. Among others, privacy objectives are identified by performing a privacy impact assessment (PIA), for which several recommendations are offered by governments, the European Union itself and scientists. All of them demand to perform a privacy threat analysis (PTA) as one pillar for a reliable PIA. However, the recommendations on how to conduct a PIA predominantly focus on describing the procedure to follow, albeit without neither guiding the auditor through the necessary PTA nor providing specialized systematic tools or methods for a reliable PTA.

To the best of our knowledge, LINDDUN [16] is the most promising systematic PTA framework, using an information-flow-oriented system representation and relying on a data flow diagram (DFD) methodology. Nonetheless LINDDUN is a generic framework in the sense that it has not been originally conceived for the IA procedures tackled in Chapter 3. The fact that IA procedures

focus solely on authenticity and non-repudiation and do not aim to safeguard user privacy motivates the development and study of more systematic PTA methodologies and frameworks that are applicable to user IA processes.

The purpose of Chapter 3 is to investigate an extension of LINDDUN that allows performing a reliable and systematically-reproducible PTA of user IA processes, and thus to contribute to one of the pillars of a reliable PIA. The realization of a high-level description of the whole verification (IA) process, the creation of a systematic modelling framework and the improvement of the LINDDUN PTA framework are crucial, while further aspects are investigated in Chapter 3. Moreover, from an instructional-guidance perspective, our work aims to provide step-by-step instructions for auditors to systematically apply the proposed methodology. The ultimate objective of Chapter 3 is to provide them with a comprehensive tool-set to analyse their environment.

We would like to stress – in the context of Chapter 3 – the relevance of LINDDUN, whose usage is predominant when tackling threat modelling problems. However, it is important to emphasize that LINDDUN largely addresses general privacy threat modelling and currently cannot be applied directly to identification and authentication processes.

More specifically, the main contributions of Chapter 3 are described as follows:

I. We propose a high-level description of the IA verification process, which we illustrate with an UML use case. We describe the process of a user demanding access to a service, including the *user demand – service login – user verification – service access* sequence. The creation of the UML is accompanied by the categorization of the IA processes into centralized and decentralized, and the definition of whether they are realized as one or two components (unit/threat).

II. We develop an identification and authentication modelling framework and provide a generic overview of possible combinations of IA methods. We extend the modelling of user verification, introducing – among others – the DFD representation, a user data repository, DFD-related trust boundaries, the concept of centralized and decentralized and local and external authentication.

III. We propose an extension of two critical steps of the LINDDUN scheme (specifically steps 1 and 2) with the previously created DFD-based IA modelling framework, and further develop the trust boundary concept applied in the original LINDDUN framework.

IV. We propose a systematic methodology aimed to help auditors to apply the proposed improvements to the LINDDUN steps 1 and 2, so that they can continue with step 3 of the original LINDDUN framework.

The remainder of Chapter 3 is organized as follows. Section 3.2 presents the background, state of the art of PIA as well as PTA, and the LINDDUN framework. The developed IA modelling framework, the extended LINDDUN methodology and one-page instructions list are presented in Section 3.3. Subsequently, a proof-of-concept with two variants is evaluated in Section 3.4. Finally, conclusions are drawn in Section 3.5.

3.2 Background on Identification and Authentication

In the present section, a basic background for I and A processes is provided to be used in Section 3.3.2.

Throughout the present chapter, the definition used for identity is: "An identity is any subset of attribute of an individual person which sufficiently identifies this individual person within any set of persons. So usually there is no such thing as "the identity", but several of them" [5].

An identity required for the use of a certain service represents a "partial identity" [5], also *"*a subset of attribute values of a complete identity" of an individual person and "where a complete identity is the union of all attribute values of all identities of this person." Throughout the present chapter we will use the term *identity* representing a *partial identity* of all attributes related to one user (person).

The concept of identity mentioned in [5] comprises a subset or all identity attributes that a service can require to be proved by the user passing an IA process.

In accordance with [50], we use following the definitions for I and A: "Identification is the process of using claimed or observed attributes of an entity to deduce who the entity is." "Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence." In this context, we would like to highlight that for an auditor, identification is sometimes used as a synonym of authentication [6].

Authentication factors are used by the user to provide evidence of their claim made by presenting the identity. The authentication factors are grouped in three recognized categories as follows. The user can give evidence by demonstrating to know a knowledge (something you know), have something in his possession (something you have) or being someone (something you are, biometric) [7, 8].

3.3 IA Modelling Framework Development and Application to the Enhanced LINDDUN Framework

In this section, we propose an IA modelling framework suitable to extend the subsequent privacy-aware analysis and illustrate its application with a use case. We start in Section 3.2 with the presentation of a preliminary background for I and A. More specifically, in Section 3.3.1 the high-level description of the IA verification process for the use case of a user demanding service access is shown with UML notation. The IA modelling framework is developed in Section 3.3.2. During the development, common IA methods are gathered and presented in Table 2 and 3. The IA methods are modelled using the DFD, sub-phases are defined, and trust boundaries are considered. The extension of the LINDDUN framework – shown in Section 3.3.3 – is contrived to perform PTA on IA methods. The LINDDUN privacy threats are mapped to the DFD-based IA modelling framework and the trust boundary concept of the LINDDUN framework is tailored. A straightforward usable procedure (instructions) of how to use the previously worked-out contributions is presented in Section 3.3.4.

3.3.1 Use Case of User Demanding Service Access

The generic use case *service provision* for a user demanding service access is presented for modelling purposes using UML in Figure 2. The steps of *service demand*, *service login*, *user verification* and *service usage* represent at an overview the steps of the process to be passed by the user.

Depending on the user interaction throughout the *user verification,* we introduce the categorization into *centralized user verification* (user only communicates with the service) and *decentralized user verification* (user communicates with service and I / A components).

We assume that the I and A components can be realized together as one component (IA) or in two different components (I)-(A), so real circumstances can be considered. I and A components can be realized as hardware or software artefacts. The arrows interconnecting the categories and components below *user verification* indicate common combinations.

Depending on whether the service to be used and the components (IA), (I), (A) belong to the same or different domains, the user verification is determined as local or external authentication. Further details will be given in the context of trust boundary consideration in Section 3.3.2.5.

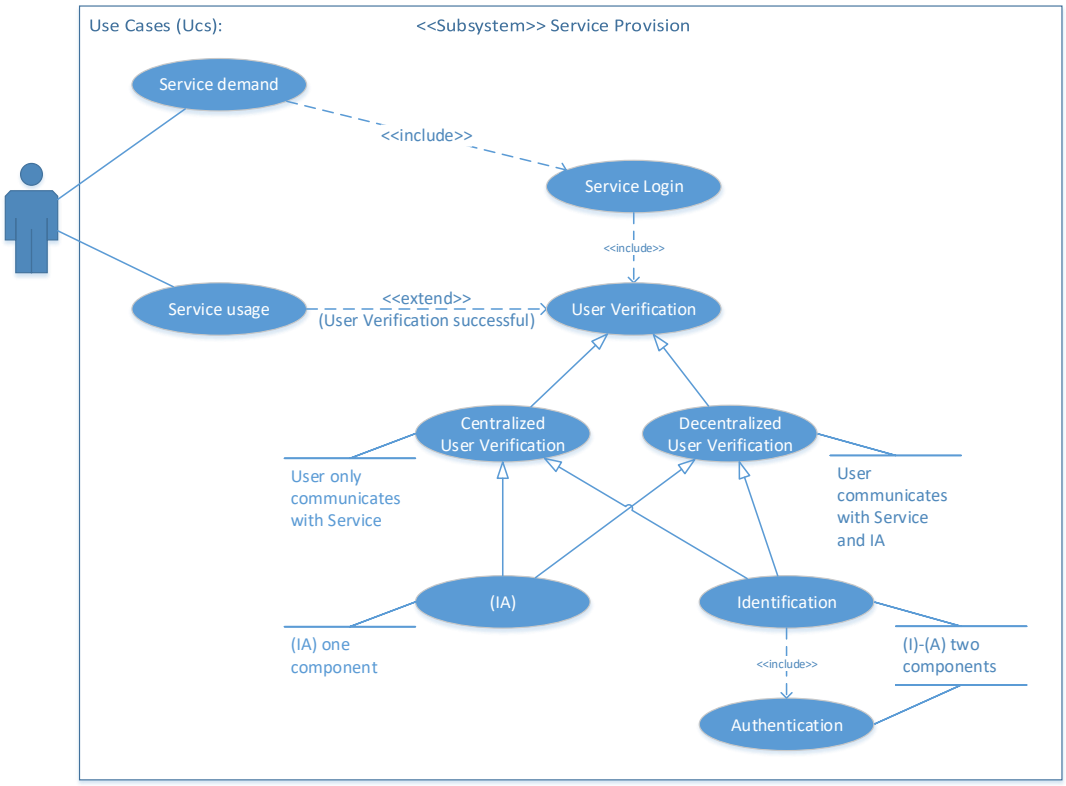


Figure 2. UML use case of user demanding service access.

3.3.2 Identification and Authentication Modelling Framework

In Section 3.3.2.1, the three-step I and A process is defined. Section 3.3.2.2 presents tables with IA methods and possible combinations. Section 3.3.2.3 introduces the DFD for modelling purposes. The phases and sub-phases regarding the scope of the identification and authentication process are outlined in Section 3.3.2.4. Section 3.3.2.5 relates the concept of trust boundaries with the characteristics of identification and authentication methods.

3.3.2.1 Three-Step Identification and Authentication Process

Our starting point considers the definition of identification and authentication [50], namely as a two-step process. We parse the two steps I and A as follows into three steps of *identity presentation*, *identification* and *authentication*. Now, before defining the three-step I and A processes we want to point out authenticable and not-authenticable attributes.

Authenticable and Not-Authenticable Attributes

Theoretically, the provision of information by the user can be undertaken during the whole IA process and will depend on the service requirements and IA methods used. We categorize the information that a user can provide into *authenticable attributes* and *not-authenticable attributes*.

Authenticable attributes require that the user on his part can prove towards the service provider the correctness and/or legitimate usage of the presented attributes, which belong to one identity or partial identity of the user.

Not-authenticable attributes are passed to the service provider without any direct proof of correctness or whether the user is legitimated to use it. These can be grouped into *free collected attributes* by the service provider or the user's additionally *voluntary given attributes*. Based on the applied *transitivity of trust,* the service provider assumes that the additionally voluntary given attributes are true, and therefore, they are called *trust-based attributes*.

We would like to highlight the arising risk of privacy threats when the user – in addition to proving authenticable attributes – gives trust-based attributes. The consideration of all given user information holds major interest for an integral PTA, which lies beyond the scope of the present chapter. The scope of the present chapter is the PTA for authenticable attributes in the context of IA methods.

Accordingly, we define the three IA process steps of *identity presentation*, *identification* and *authentication* (IIA). In a two-step IA process, step 1 is usually included in step 2. We describe these three steps next:

- Step 1: Identity presentation is the consideration of how a subset of identity attributes are presented by the user. The user presents the required subset of identity attributes to a service, so that the user claims to be someone (or something), e.g. presenting a user ID, username or other attributes. In step 1, we only consider attributes that are required to pass the (I)IA process, and therefore to be proved. The introduction of step 1 *identity presentation* was chosen to cover – if necessary – all possibly existing technical realization of IA methods.
- Step 2: Identification in the present context is defined as the verification of the plausibility of the presented "subset of" (identity) "attributes" [5]. The plausibility verification can comprise the verification of the technical correctness (e.g. syntax, format, length, etc.), but can include the semantical verification of plausibility (e.g. age in realistic range, age minimum is given, etc.) before proceeding with the proof of the presented attributes.
- Step 3: Authentication is the proof of the claim made by the user with the presentation of the subset of identity attributes in step 1 and/or 2, and therefore to confirm the legitimate usage and/or correctness of the presented identity attributes. This step in the best case is undertaken in a self-determined manner by the user, e.g. introducing a password or personal identification number (PIN).

3.3.2.2 IA Methods: Creation of Tables for I-Methods and A-Methods

The three steps of "identity presentation", "I" and "A" (IIA) defined in Section 3.3.2.1 require a technical basis. For this purpose, technical IA methods and authentication factors and protocols are used to create IA methods tables.

Identity Presentation in the Context of Identification and Authentication

Identification methods comprises the procedure and technical components that the user applies to present his identity to the service. The selected identification method facilitates the user to manually or electronically pass the required attribute to the service, whereby the user manually types in the required details of the identifier or electronically passes the information in a technology-based manner, e.g. on a barcode, magnetic strip, NFC and/or a smartcard.

Furthermore, recall that the acronym IA implies that "I" includes the identity presentation and identification (II) and "A" is the abbreviation of authentication. In the remaining part of the subsection, the compilation of the I-method in Table 2 including the most common methods for realizing step 1 identity presentation, step 2 identification and gathering the provided attributes used is undertaken. We show in Table 3 the compilation of A-methods including the most common methods for step 3 authentication. Table 3 also depicts part of the possible combination of IA methods.

Next, we describe the manual and electronic identity presentation methods.

The categorization of identification methods is conducted depending on the provision method applied to pass the required user attributes (e.g. loginID, username, name, etc.) to the service, which can take place manually and electronically.

- *Manually*: The user types in the required attributes, e.g. his loginID, which he knows or is printed on a smartcard, magnetic card or similar plastic card.
  Access (protection) to the attributes is "free", whereby the access to the attribute, e.g. printed on the card is without any restriction.
- *Electronically*: The user presents a smartcard, magnetic card or another similar card that is electronically readable using at least one of the following methods: optically (barcode, machine readable zone), magnetic strip card, smartcard with contact or by proximity using NFC (e.g. NFC smartcard or RFID tag).
  Access (protection) to the attributes is "free," as the attribute is accessible without any restriction (barcode, RFID, smartcard), "restricted," as the identity/attribute can only be read by (authorized) terminals (RFID, smartcard readable only with, e.g. a cryptographic key), or "auth," whereby the identity/attribute can only be read or verified by (authorized) terminals

after additional user authorization with e.g. a password/pin and are called *authenticable attributes*.

- We introduce the *user information storage/user data repository* in the context of identity presentation methods for the user environment towards a more reliable and systematic user centric analysis, which implies the presence of a storage/database usable by the user and could be his brain for accessing the username or another identifier or medium, e.g. smartcard, smartphone or capability he possesses to access the cloud.[8]

Table 2 shows identity presentation methods including one group of rows for authenticable attributes, therefore, to be proved by the user and a group of rows for trust-based attributes provided voluntarily by the user without additional proof (for more details, see non-authenticable attributes in Section 3.3.2.1). The *user ID* is one possible attribute of the identity of the user and for which an authentication proof ("authenticable attribute") could be required, whereby the proof of more than one attribute could be demanded.

The input row in Table 2 describes how the trust-based attributes will be passed to the system, therefore typed in, by a barcode, with a MRZ, contact reader or proximity (NFC) reader. The row storage describes where the attributes are stored, e.g. on an optical readable barcode, smart card or NFC tag. We add to these storages the user memory and named it as being known to user. In Table 2, the identity presentation method properties of the presented authenticable attributes can be gathered, as well as which trust-based attributes (see Section 3.3.2.1) are additionally provided by the user.

[8] There are still ideas and first realization of IA solutions based on attributes stored in the cloud.

Identity Presentation/ Identification Method (ID-M)	ID-M properties			Authenticable (A) Attributes				Input method can vary from that used for A-Attributes	Trust Based (TB) Attributes given by user during IA process or afterwards		
ID-Method-Name	Storage	Input	Access (protection)	A-Attr1 e.g. User ID	Au-Attr 2 e.g. address	Au-Attr 3 e.g. adult	...	Input	TB-Attri1 e.g. hobby	TB-Attr2 e.g. name	...
Manually											
M-user	Known to user	Typed in	Free								
M-card	Printed on a card	Typed in	Free								
Electronically											
E-barcode	Optical readable	barcode	free								
E-MRZ	Optical readable	machine readable zone (MRZ)	free								
RFID-Tag	NFC-Tag	proximity	free								
RFID-Tag	NFC-Tag	proximity	restricted								
RFID-Tag	NFC-Tag	proximity	auth								
E-magnetic	Magnetic card	Reader	free								
E-contact-SC	Contact smart card (SC)	Reader	free								
E-contact-SC	Contact smart card (SC)	Reader	restricted								
E-contact-SC	Contact smart card (SC)	Reader	auth								
E-NFC-SC	NFC smart card	proximity	free								
E-NFC-SC	NFC smart card	proximity	restricted								
E-NFC-SC	NFC smart card	proximity	auth								

Table 2 Identity presentation methods.

Compilation of I- and A-Methods Combination

In Table 3, we assemble A-methods, authentication factors, general recognized procedures (protocols) and requirements for securing user authentication:

Multi-Factor Authentication: Usage of two or more authentication factors. A verification process using more than one authentication factor is called multi-factor authentication [7].

Challenge Response (CR)-Based Authentication Procedure: An entity (claimant) proves his identity to another entity (verifier) by demonstrating knowledge of a secret, without revealing the secret itself to the verifier during the protocol [6]. Known variants of CR-based authentication [6] could rely on techniques like a “one-time password”, “symmetric keys” or a “public key.” A special CR-based procedure is the zero-knowledge procedure [7].

Challenge Response Procedure (each authentication with a new password/credential): A one-time password-based (e.g. S/Key (Lesli Lampert), OTP (RFC2289), Symmetric cryptosystem, Asymmetric cryptosystem. Zero-knowledge procedure (special CR procedure [7]), randomly asking for a subset of available credentials.

Strong Authentication: The definition is ambiguous and could mean that multiple answers have been requested (CR Zero-Knowledge), it must be based on a challenge response protocol or the verification may not be accomplished by sending the secret. In the following consideration, we will use the definition of strong authentication (see [7]), and therefore the method based on challenge response (CR) and without sending the secret.

In Table 3, the A factors can be used in combination with different authentication procedures (protocols) that are ordered from weak to strong and e.g. for which *secret not revealed* are marked with (X), indicates that in the meantime it is an accepted and recognized and indispensable practice. The authenticable attributes are either provided during the identity presentation step (see in Table 3 in column *attributes* the cell with the text "Table 2") or implicitly with the authentication method (see in Table 3 in column *attributes* the cell with the text *Amethod*). When considering Table 3 for a PTA in Section 3.3.3 with the LINDDUN framework, the (X) will indicate that it is (quasi) mandatory to fulfil this requirement. Table 3 is a template for gathering information of the system to be analysed. Systems using whatever IA methods could require (and is recommendable) to apply in their realization the procedure of "mutual authentication and secure communication channel" (secure channel).

As explained in Section 3.3.2.5, the concept of trust boundary and trusted third party (TTP) related authentication, local authentication (inside the same domain) and external authentication (cross domain) is also used throughout diverse IA methods. Both concepts are used to expand Table 3 with two more categories at the end, namely "mutual authentication and secure communication channel" and "trust boundary and trusted third party (TTP)-related authentication".

Table 3 for identification-methods (I-methods) and authentication-methods (A-methods) shows a few of the possible and commonly used combinations of I-methods and A-methods. Each combination is a generic IA Type. Table 3 will serve as a template to guide the auditor to elicit the analysed IA environment for applying LINDDUN [16]. Table 3 has embedded in the center an *authentication method* table.

The output of the present section is a set of tables related with IA methods usable as part of a tool set by the auditor for gathering the actual status of the environment and model it afterwards. To our best knowledge we did not find similar tables for I- and A-methods.

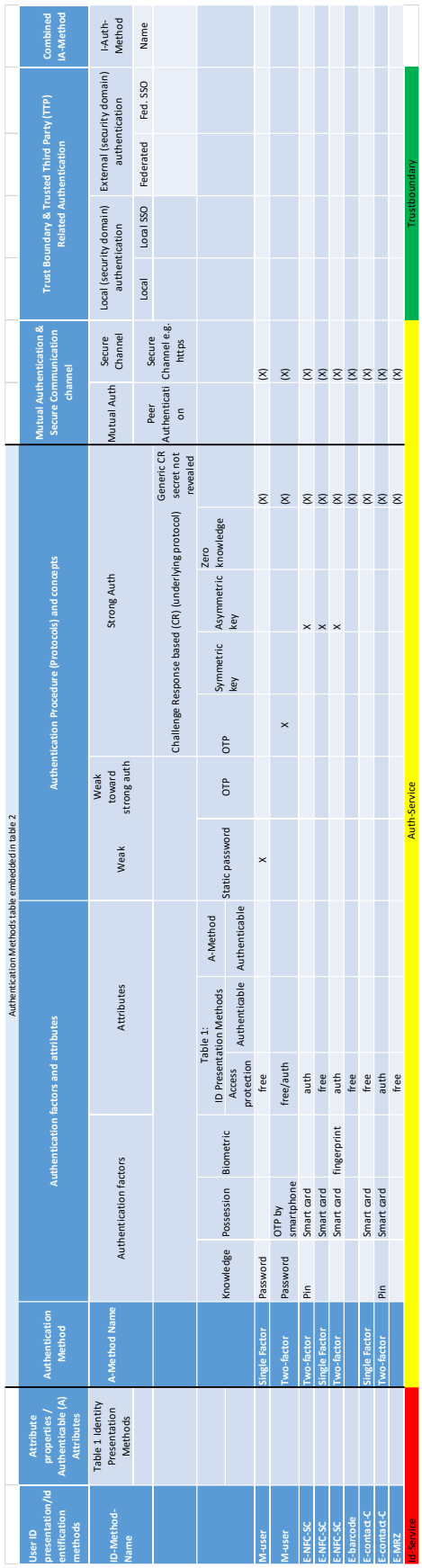


Table 3: A-methods, combinations of I-methods and A-methods and trust boundary.

3.3.2.3 Data Flow Diagram

The application of the LINDDUN framework [16, 34] is based on a DFD describing the environment to analyse. The core components required for identification and authentication are user, identification service, authentication service and (application) service provision and for each component one database/data store is assumed. To illustrate the application of the LINDDUN framework, we present a generic DFD for the identification and authentication environment (Figure 3).

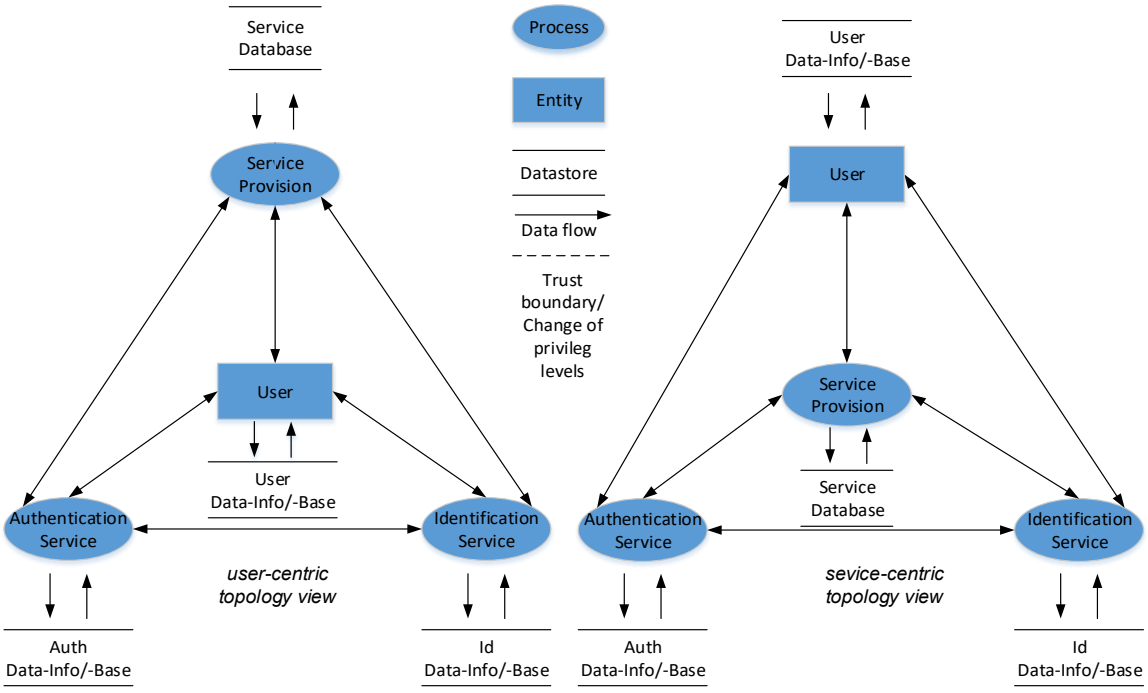


Figure 3. Generic DFD of the identification and authentication processes (user- or service-centric topology view).

In contrast to the DFD presented in the LINDDUN paper [16], we introduce a *user data-info/-base (repository)* that can be used for a more detailed analysis of IA methods. An example for the location of a user data-info/base could be a device brought along by the user to provide or confirm required attributes, therefore for proving the claim, while the attributes could also be stored in the cloud. Further details are provided later in Section 3.3.2.2.

An arrow with two arrowheads between two components indicates that in principle a communication in both directions is possible and could be subdivided into two arrows with opposite head directions. The detailed communication to be considered will ultimately depend on the IA methods implemented.

The DFD elements of Figure 3 are:

Entity: User U; Processes: identification (I) ≙ (I)-P, authentication (A) ≙ (A)-P, service provision (S) ≙ S-P, identification-authentication (IA) ≙ (IA)-P; data Store: user data-/info-base ≙ U-DB,

identification database ≙ (I)-DB, authentication database ≙ (A)-DB, identification-authentication database (IA)-DB, service provision database ≙ S-DB; data flow: "bidirectional arrows" ≙ "⇔", "unidirectional arrows" ≙ "→" or "←".

User or service centric representation:
In Figure 3, both views are given, namely the service-centric as well the user-centric view. It is possible to gain different benefits for the LINDDUN analyses depending on which of both views have been used, namely the user- or service-centric representation.

Applying the DFD-IA model user- or service-centric only offers an advantage in the visualization, which can be useful when the components depending on the real implementation belong to different domains and differ from the user domain and must be grouped together. Another conceivable visualization of the content could be a three-dimensional figure offering different perspectives. In this present chapter, we consider the service-centric DFD element arrangement as depicted in Figure 3.

3.3.2.4 Process Phases P1 – P4 and Sub-Phases

In the present section, the IA phases and sub-phases are investigated. The derived extended generic DFD including the (sub-)phases, is shown in Figure 4. The user access process to the service is divided in four phases P1 to P4, as explained below.

Figure 4 shows four phases in which the user, service provider and IA service can be involved, and the details depend on the IA system to be analysed. Here, it is assumed that the user in P1 demands the usage of the service. The identification and authentication process are carried out in phases P2 and P3. Phase P4 represents the authorization to use the service after successful authentication.

The sub-phases P1 to P4 and the resulting phase diagram for a complete identification and authentication processes will depend on the system to be analysed, so that only P1 and P4 are detailed and the rectangle for P2 and P3 will be replenished later by the auditor depending on the real system to be examined. The auditor can use Figure 4 as a template for this purpose and gather for the place holders *Auditor verifies for P2 to P3 range of influence* which components and/or user of the analysed system are participating in each of these sub-phases.

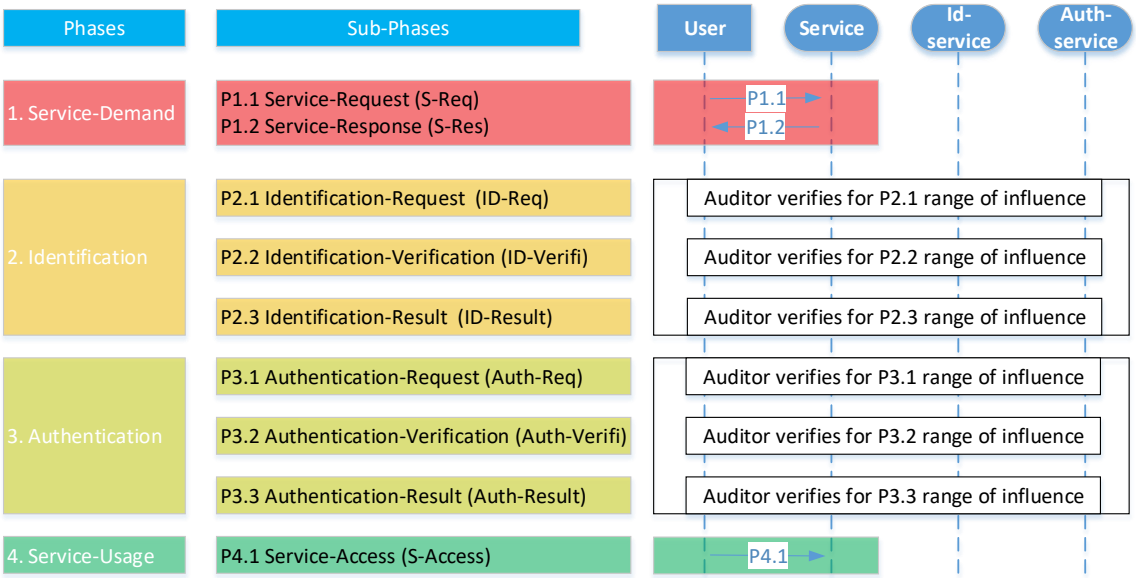


Figure 4. Extended DFD with (sub-)phases P1 to P4.

3.3.2.5 Trust Boundaries

In the present subsection we introduce the concept of centralized and decentralized user verification, local and external authentication and mutual authentication and secure channel.

Centralized and Decentralized User Verification

The categories of *centralized user verification* (user only communicates with the service) and *decentralized user verification* (user communicates with service and I/A components) introduced in Section 3.2 are depicted in Figure 5, including the trust boundaries given by the domain borders and used for further explanation.

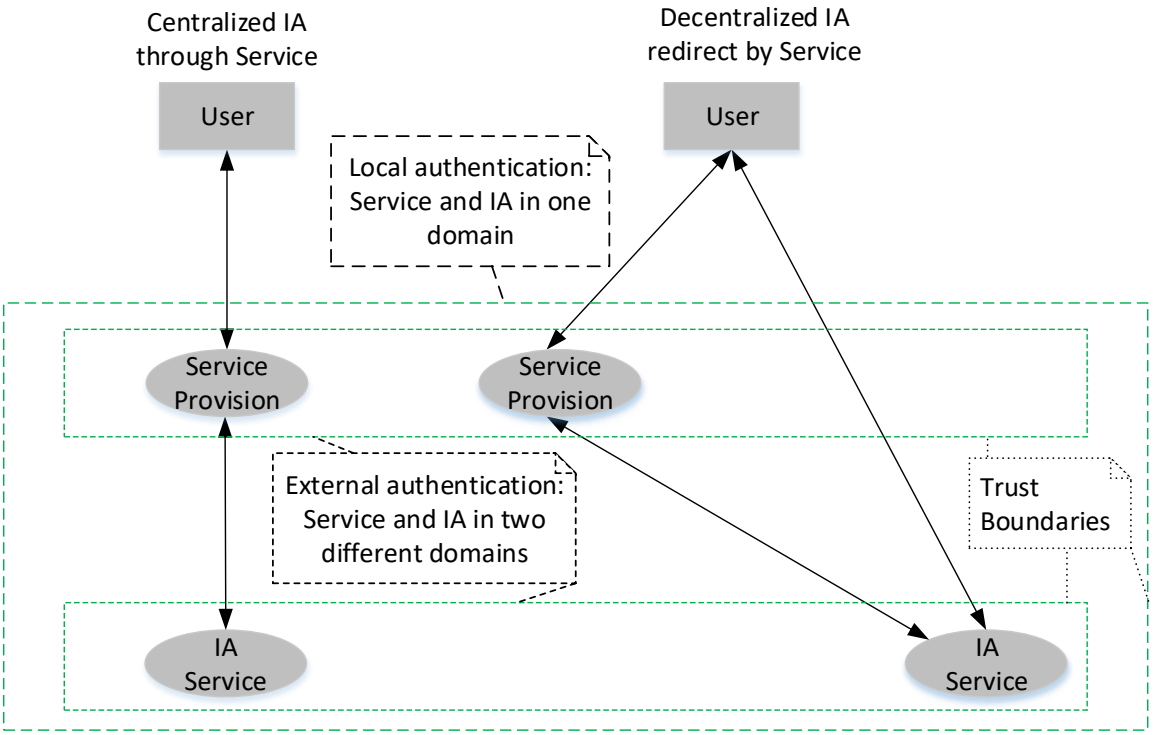


Figure 5. Trust boundaries centralized and decentralized user verification.

Local and External Authentication

The categorization into *local authentication* and *external authentication* (see Table 4 and Figure 5) refers to the domain in which the authentication is performed, and therefore whether in the local domain (where the service reside) or an external domain. We assume that the identification is conducted together in the same domain with the authentication. The presented model and concept could be applied for the case that the identification is performed locally and only the pure authentication is also undertaken through the external domain. The definition of what is to be considered local or external depends on the trust relation between the components, the environment, and the user, and therefore the course of trust boundaries.

Local authentication (inside one domain):

The service (S) provider receives the service request and will perform the identification and authentication processes in a centralized or decentralized manner, only communicating with the IA service (TTP) in the own local domain (see Figure 5).

As depicted in Figure 6, the service *n* in domain 1 to be accessed by a user of domain 1 (D1) will contact within his own local domain 1 an instance, e.g. called IA service domain1, for performing the IA of the user. The user accesses to all other services of domain 1 will rely on the same IA service of domain1.

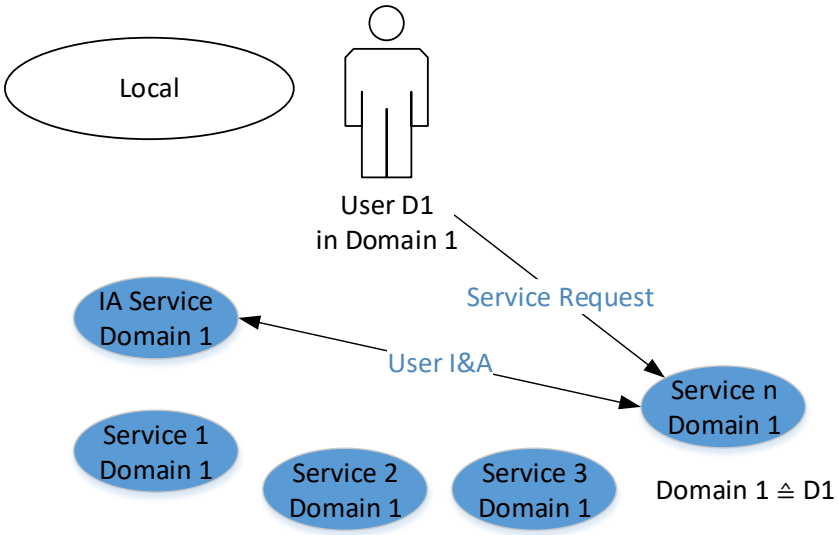


Figure 6. Local authentication (within one domain).

External authentication (cross domain):

The service (S) provider receives the service request and will perform the identification and authentication processes in a centralized or decentralized manner, contacting an IA service (TTP) of an external domain (see Figure 5).

The concept of external authentication is often named delegated. As depicted in Figure 7, the services in domain n to be accessed by a user of domain 1 will contact an instance, e.g. called IA service domain 1, of the external domain 1 for performing the IA of the user of domain 1.

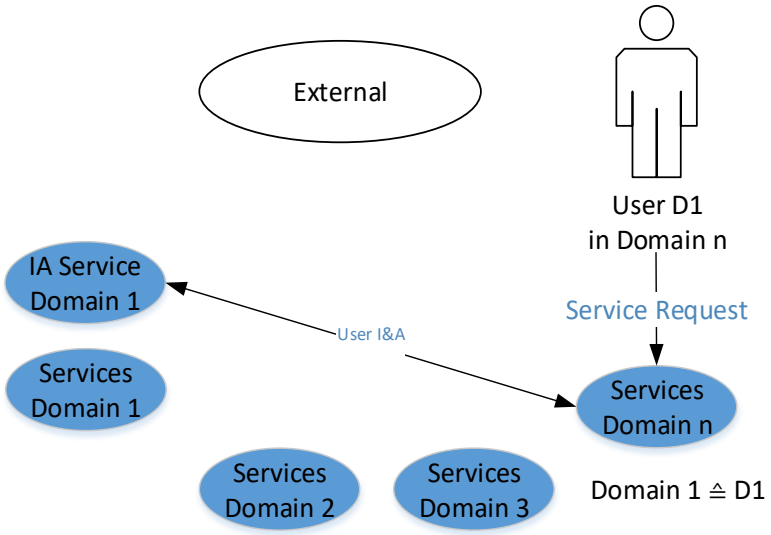


Figure 7. External authentication (cross domain).

Single sign on (SSO) for local and external authentication:

Regardless of whether the user successfully passes the IA service in the local or external context, SSO is determined as follows:

SSO is defined as the possibility of a user to access continuously after passing the IA service (successful authentication) for a period t one or more services in the domain(s) for which the initial authentication was performed. The validity period t and SSO domain together constitute the auth-result presented in Table 4 in Section 3.3.2.5. Table 4 is a further instrument for the auditor to elicit the environment to be analysed.

In Table 4, regardless of whether the IA process is realized locally or externally or with centralized and decentralized IA, different combinations with possible realizations of IA processes – therefore, as one server (unit/threat) (IA) service or two server (units/threats) (I)-(A) service – are presented.

IA-Service		Centralized		Decentralized				Authentication in Security Domain		Auth-Result Validity	Auth-Result SSO
		A1	A2	B1	B2	C1	C2	Local (LD)	External (ED)	Time	Domain(s)
One component	(IA)	(IA)		(IA)	(IA)						
Two component	(I)-(A)		(I)-(A)			(I)-(A)	(I)-(A)				
Auth-Result-to-S	S	S	S	S			S				
Auth-Result-to-U	U				U	U					

Table 4 Authentication results in the context of centralized and decentralized IA processes, trust boundaries and SSO.

In Table 4, the rows labelled *authentication in security domain* including the options *local domain (LD)* and *external domain (ED)* and *auth-result* including the options *validity* and *SSO* in particular expand the possibility to note more precisely the details of the real system.

Mutual Authentication and Secure Channel

Mutual authentication in Table 3 is related with the underlying communication channel, such as *https* or *TLS layer* used between the server and client independent of the possible mutual authentication at the level of user identification and authentication. According to [8], mutual authentication is “When both the client and the server must be authenticated, the process is known as mutual authentication.” The server identifies himself with a certificate towards the client and if required by the server the client can be requested to authenticate himself towards the server with one’s own client certificate. Therefore, mutual authentication at the communication channel level holds interest for fulfilling security requirements but reduces the possibility of the user to maintain his privacy, e.g. it can be possible to determine more easily if a user is accessing independently from the IP address from the same client device. Client certificates could belong to the operating system or application, e.g. a browser for surfing environment, and therefore the corresponding store can vary and reveal more information as intended about the changing user environment.

Secure channel communication, e.g. https and TLS layer [7] are for granting the confidentiality on the communication channel, and therefore observers cannot access the encrypted content in the communication.

Mutual authentication and *secure channel communication* nowadays have become – as highlighted in Table 3 – indispensable from the security perspective but can contribute to compromised user privacy.

3.3.3 Extension of LINDDUN Framework

In Section 3.3.3, we apply the PROBLEM SPACE of the LINDDUN framework (see Section 2.1.3) to the previously developed DFD-based IA modelling framework. The mapping of LINDDUN privacy threats to the IA DFD model is specified in Section 3.3.3.1 and the extension of the LINDDUN trust boundary concept and application to IA DFD is shown in Section 3.3.3.2.

3.3.3.1 LINDDUN Privacy Threats Mapping to DFD IA Modelling Framework

The LINDDUN privacy threats [16] and related privacy properties are shown in Table 5, which is borrowed (but drawn by ourselves) from the LINDDUN framework to explain the terminology definition presented by their authors and used in this dissertation.

	Privacy properties	Privacy threats
HARD	Unlinkability	**L**inkability
	Anonymity & Pseudonymity	**I**dentifiability
	Plausible deniability	**N**on-repudiation
	Undetectability& Unobservability	**D**etectability
	Confidentiality	**D**isclosure of information
SOFT	Content awarness	content **U**nawarness
	Policy and sonsent compliance	policy and consent **N**oncompliance

Table 5. In the LINDDUN framework [16] privacy properties and the corresponding privacy threats are categorized as hard and soft privacy.

The LINDDUN framework differentiates (as shown in Table 5) between hard privacy as data minimization, and soft privacy where the data controller (entity getting user information) obtaining the information (should) honestly preserve the data privacy as agreed.

The service-centric topology view of Figure 3 is used to map the DFD elements to LINDDUN privacy threats and thus we obtain

Table 6, considering that the pure IA process could be implemented centralized as one component (IA) one server (unit/threat) or decentralized as two servers (as two units/threats) (I)-(A).

Table 6 can be used as a template to determine the susceptible LINDDUN privacy threats of the system during the analysis, e.g. as in the proof-of-concept scenarios in Section 3.4.

DFD Elements of the Identification and Authentication model				Mapping LINDDUN privacy threats to DFD elements of the Identification and Authentication model						
		I-A on two server								
		IA on one server								
				L	**I**	**N**	**D**	**D**	**U**	**N**
Entity			L	X	X				X	
	User	U		X	X				X	
Process			L	X	X	X	X	X		X
	Identification (I)	I-P		X	X	X	X	X		X
	Authentication (A)	A-P		X	X	X	X	X		X
	Service Provision (S)	Service-P		X	X	X	X	X		X
	Identifi-Authent (IA)	IA-P		X	X	X	X	X		X
Data Store			L	X	X	X	X	X		X
	User Data-/Info-Base	U-DB		X	X	X	X	X		X
	Identification Database	I-DB		X	X	X	X	X		X
	Authentication Database	A-DB		X	X	X	X	X		X
	Identifi-Authent Database	IA-DB		X	X	X	X	X		X
	Service Provision Database	Service-DB		X	X	X	X	X		X
Data Flow			L	X	X	X	X	X		X
	User data stream	with {U-DB, I-P, A-P, Service-P}								
		U- I-P		X	X	X	X	X		X
		U- A-P		X	X	X	X	X		X
		U- IA-P		X	X	X	X	X		X
		U- Service-P		X	X	X	X	X		X
		U- U-DB		X	X	X	X	X		X
	Service data stream	with { Service-DB, U, I-P, A-P}								
		Service-P U		X	X	X	X	X		X
		Service-P I-P		X	X	X	X	X		X
		Service-P A-P		X	X	X	X	X		X
		Service-P IA-P		X	X	X	X	X		X
		Service-P Service-DB		X	X	X	X	X		X
	Identification data stream	with {I-DB, U, A-P, Service-P}								
		I-P U		X	X	X	X	X		X
		I-P A-P		X	X	X	X	X		X
		I-P Service-P		X	X	X	X	X		X
		I-P I-DB		X	X	X	X	X		X
	Authentication data stream	with {A-DB, U, I-P, Service-P}								
		A-P U		X	X	X	X	X		X
		A-P I-P		X	X	X	X	X		X
		A-P Service-P		X	X	X	X	X		X
		A-P A-DB		X	X	X	X	X		X
	Identifi-Authent data stream	with {IA-DB, U, IA-P, Service-P}								
		IA-P U		X	X	X	X	X		X
		IA-P Service-P		X	X	X	X	X		X
		IA-P IA-DB		X	X	X	X	X		X

Table 6: DFD elements of IA modelling framework mapping to LINDDUN privacy threats distinguishing (IA) and (I)-(A).

Table 6 will be the pattern (template) to be used when applying LINDDUN for IA process analysis regardless of whether it is realized on one or different (two or more) servers (units/threats), e.g. (IA)-P stands for identification and authentication on one server and (I)-P and (A)-P are identification and authentication on two (or more) servers. We have highlighted in different shadows of grey IA components combinations that usually will be considered together or disregarded together depending on the realization, and therefore they are mutually exclusive.

3.3.3.2 Trust Boundary Concept Extension and Application to IA Data Flow Diagram

In the further development the term trust boundary (in LINDDUN [16] called trust boundaries/change of privileges) will be employed and extended for IA processes. A description of how the trust boundary should be considered in the required interaction of the user and the components of the IA model environment will be provided and is illustrated referring to Figure 3. Trust boundaries are illustrated by broken closed lines imbedding within the components or entities trusting each other and will imply that the connecting data flow arrow between two components are not crossed by any trust boundary.

The smallest unit surrounded completely by a trust boundary comprises a component or entity and the accompanying database/information storage, so that the communication between these two parties is considered trustworthy. The database (information store) of the components and entity will be detailed in a latter step together with the IA methods considered.

The requirements of the possible realizations of IA systems result in the necessity to concretize the trust types to apply, since the trust boundaries delimit changes of competence and the possibility to take influence in the further handling of user and communication information.

We introduce three concepts of trust, namely *Exclusive-Trust*, *Non-Exclusive-Trust* and *Enclosed-Exclusive-Trust*. The terminology is applied according to the DFD introduced in Section 3.3.2.3 and in addition brackets "(", ")" and "[", "]" are used to depict which components are within one trust boundary and distinguish different overlapping trust boundaries. Furthermore, the three concepts of trust are defined and applied to the IA DFD presented in Section 3.3.2.3. Additionally for *Exclusive-Trust Trust Boundary DFD-(U)(S)(I)(A)* Figure 8 and for *Non-Exclusive-Trust/Overlapping Trust Boundary [U ({I A}] S)* Figure 9 are exemplarily presented. Of course, for the other trust concepts, analogous figures could be derived.

Exclusive-Trust Trust Boundary

Definition of "Exclusive-Trust Trust Boundary"

Entity, components and data flows grouped together are only imbedded within a single trust boundary, and therefore there are no overlapping trust boundaries.

3.3.3.2.1.1 DFD-(U) (S) (I) (A)

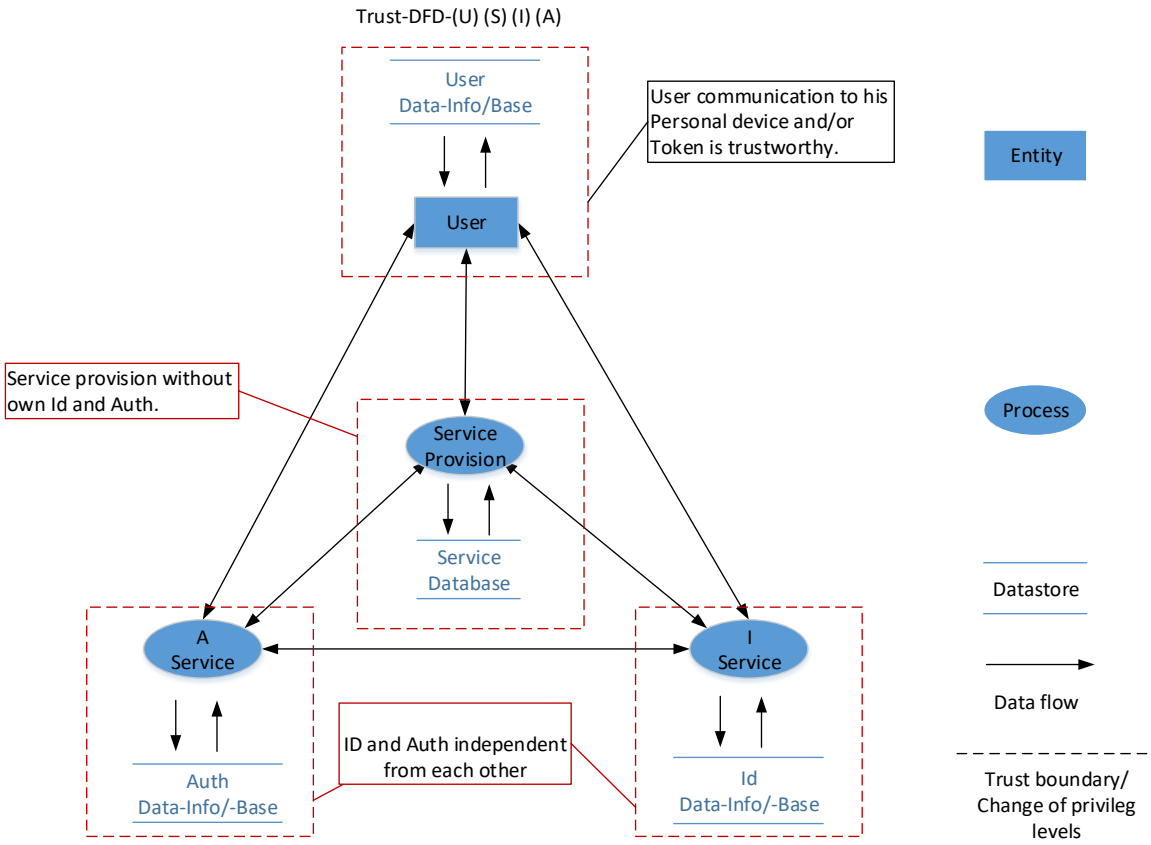
Each component only trusts its own database/information store imbedded by the broken line for trust boundary including the accompanying component and there is no further trust between the other components (see Figure 8).

One example can be a service delegating the identification to an I service, which involves an A service to perform the authentication and afterwards the authorization confirmation could be provided by the I service or A service.

3.3.3.2.1.2 DFD-(U) (S) (I A)

Each component trusts its own database/information store imbedded by the broken line for trust boundary including the component. The identification (I) and authentication (A) service are within one broken trust boundary line, and therefore these are the only components trusting each other. Thus, additionally to Figure 8 one more broken trust boundary line including the I and A service would be added to the DFD.

One example can be a service delegating the IA process to an external IA service (e.g. LDAP, RADIUS) located outside one's own domain of responsibility, e.g. authentication in the environment of EDUROAM[9] access at universities. Another example could be that of a faculty service offered at a university and the faculty service server contacts an identification and authentication service offered by the computation centre within the local university campus domain.



[9] User roaming in the education and research area, www.eduroam.org

Figure 8. Exclusive Trust-DFD-(U) (S) (I) (A).

3.3.3.2.1.3 DFD-(U) (S I A)

Each component trusts its own database/information store imbedded by the broken line for the trust boundary including the component. The service provision (S), the identification (I) and authentication (A) service are within one broken trust boundary line, and therefore these are the components trusting each other. Thus, additionally to Figure 8 one more broken trust boundary line including the S, I and A service would be added to the DFD.

One example can be a service with its own IA service, e.g. a company applying LDAP and authenticating the users using his own user DB.

3.3.3.2.1.4 DFD-(U S I A)

Each component trusts its own database/information store imbedded by the broken line for the trust boundary including the components. The service provision (S), the identification (I) and authentication (A) service and user (U) are all within one broken trust boundary line, and therefore these components and user trust each other.

This constellation could be an environment where the user uses all hardware provided by one operator, e.g. an employee using a computer (without any other physical access possibility, despite the keyboard and mouse) within the company with a company account. The computer could be a fixed PC (especially hardened) only configurable by the company system administrator. This constellation would require an "hermetic" isolation towards the outer "world" of all domain communication and is depreciated because nowadays it is not a realistic constellation.

Non-Exclusive-Trust/Overlapping Trust Boundary [U ({I A}] S)

Definition of "Non-Exclusive-Trust/Overlapping Trust Boundary"

Entity, components, and data flows grouped together can be imbedded within several overlapping trust boundaries.

One common example of the Non-Exclusive-Trust/Overlapping Trust Boundary concept is that of a user possessing a trusted third party-issued IA method set who presents it to a service provider that on his part is trusting the same trusted third party issuing the IA method set of the user (see Figure 9).

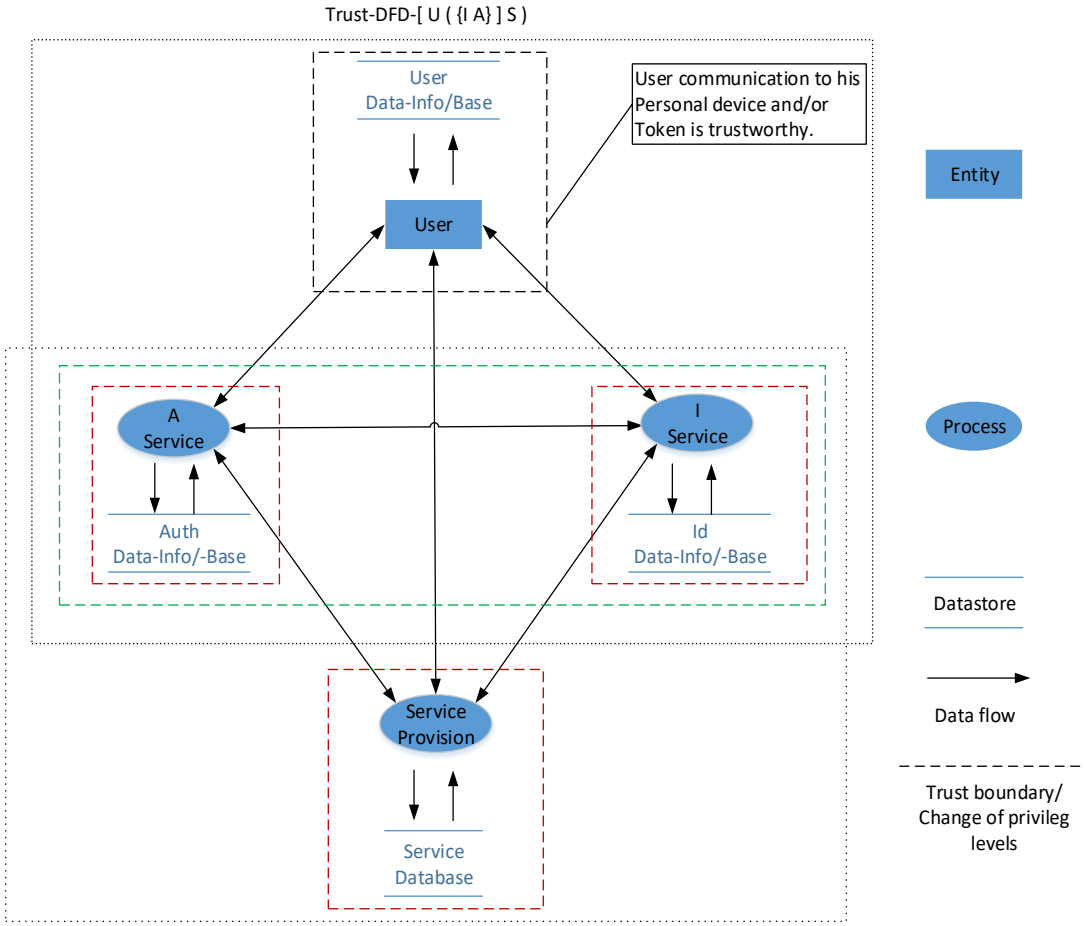


Figure 9. Non-Exclusive-Trust/Overlapping Trust Boundary [U ({I A}] S).

One concrete example can be a trusted third party issuing, e.g. an electronic ID (eID) (e.g. national identity (smart)card, etc.) and providing the necessary infrastructure for offering the identification and authentication service. One realization could be e.g. authentication as a service based on an external TTP system that has the trust of the service provider company and the user possessing an eID issued by this TTP.

Enclosed-Exclusive-Trust Trust Boundary: DFD- U [S (I A)]

Definition “Enclosed-Exclusive-Trust Trust Boundary”

Entity, components, and data flows grouped together are imbedded inside a single trust boundary (Exclusive-Trust) and a further surrounding outer trust boundary (Enclosed-Trust) encloses such a group and further individual elements, without an overlap of the existing trust boundaries.

This constellation could be the trust concept 3.3.3.2.1.2 DFD-(U) (S) (I A) replenished with one additional broken line for trust that imbeds the S, I and A service.

3.3.4 Procedure (Instructions) to Apply Enhanced LINDDUN Step 1 and Step 2 for Analysing IA Modelling Framework-Based Systems

Before proceeding with the present section, the auditor should first pick up from Section 3.3.1 the use case depicted in Figure 2.

LINDDUN Step 1: Define DFD

0. Replenish the tables (see Section 3.3.2.2):
   Table 2: Identity Presentation Methods
   Table 3: Authentication methods, combinations of I-methods and A-methods
1. DFD (see Section 3.3.2.3)
2. Process Phases (see Section 3.3.2.4)
   Consider DFD in context of sub-phases, see Figure 4, and
   Categorize the IA process of your system.
   Note down in Table 2 and Table 3 the phases when the attributes are provided.

3.1 a) Is your I A system (see Section 3.3.2.5):
   Centralized U->S
   Or
   Decentralized U->S and U-> I A
   b) Verify if your system uses (IA) on one server or (I)-(A) on two servers
   c) Determine if the S and I A are in one or two domains

} Use *Figure 5* to categorize

3.2 Using Figure 5 and Table 4 is for determining which of the constellations from A1 to C2 could be applicable to your system (see Section 3.3.2.5):
   which combinations {A1, A2, B1, B2, C1, C2} describes the system
   -> {A1, B1, B2} for (IA) on one server
   -> {A2, C1, C2} for (I)-(A) on two servers
   Determining if the system is centralized
   -> {A1} on one server for centralized or
   -> {B1, B2} on one server for decentralized
   or decentralized
   -> {A2} on two servers for centralized or
   -> {C1, C2} on two servers for decentralized

3.3 -> Draw the DFD for the analysed system considering as a guide Section 3.3.3.2 with the accompanying figures

LINDDUN Step 2: Map Privacy Threats to DFD Elements

4. With the details of step 3.3.2 above in LINDDUN step 1 and Table 6, choose whether to consider the cells for (IA) on one server or the cells for (I)-(A) on two servers.
5. Reduce the table you selected in the previous step by disregarding (removing) the lines not corresponding to your choice (real system).
6. Verify, if your IA is realized as Local authentication (see Figure 6) or
   External authentication (see Figure 7)

Step 6 is to determine a further trust boundary and apply it to the resulting table in step 5 above. At this point, the auditor has finished step 2 of the LINDDUN framework depicted in Figure 14 (see Appendix B), applying the contributions of the present chapter and must now continue with step 3 of the LINDDUN framework [16].

3.4 Evaluation

In this section we conduct an evaluation in conjunction with a proof-of-concept. Recall that the central contributions of the present chapter are the creation of a tool set and procedure description of how to model and analyse a system for identification and authentication of user identity attributes. The presented identification and authentication methods (see Section 3.3.2) enables numerous combinations. For this reason, only a limited selection could be presented exemplarily for describing the application of the procedure summarized in Section 3.3.4. The proof-of-concept scenario (see Section 3.4.1) considers a user login (authentication) with a username and password, as well as the user authentication with a pin-protected smartcard, in both cases towards the university library service. In Section 3.4.2, the application of the procedure summarized in Section 3.3.4 is presented. In Section 3.4.3, we discuss the application of the proposed framework to the proof-of-concept scenario of Section 3.4.1.

3.4.1 Proof-of-Concept Scenario

A state university with the accompanying information technology (IT) infrastructure including all services usually provided to members is chosen for the proof-of-concept of the IA modelling framework developed and enhancement of the steps 1 and 2 of the LINNDDUN framework. The scenario is based on a user – member of the state university – having access to diverse university IT infrastructure services. For the proof-of-concept, a user accesses from outside of the University to the library service on the one hand, to reserve e.g. a printed book, and on the other hand e.g. to pay the lending fee.

The state university issues smart cards including chip-based authentication using a personal identification number (PIN), chip-based cash, a barcode for the library with an associated password, associated university user account (username/password) and printed on the smartcard are the user identity number, first name and surname, photo and validity of the smartcard.

In the context of the state university, for a user there are many constellations conceivable that require the user identification and authentication, e.g. VPN to the university campus, login at the server of different faculties and usage of trust relationship through EDUROAM.[9] The user of the state university has at least two possibilities for user verification (login) purpose: on the one hand, the username/password combination, and on the other hand, a PIN protected smartcard with an access protected public key infrastructure (PKI) private key. The selected proof-of-concept depicts a username and password-based login to the university library service, as well as a smart card-based authentication for electronic payment of the lending fee (see Figure 10).

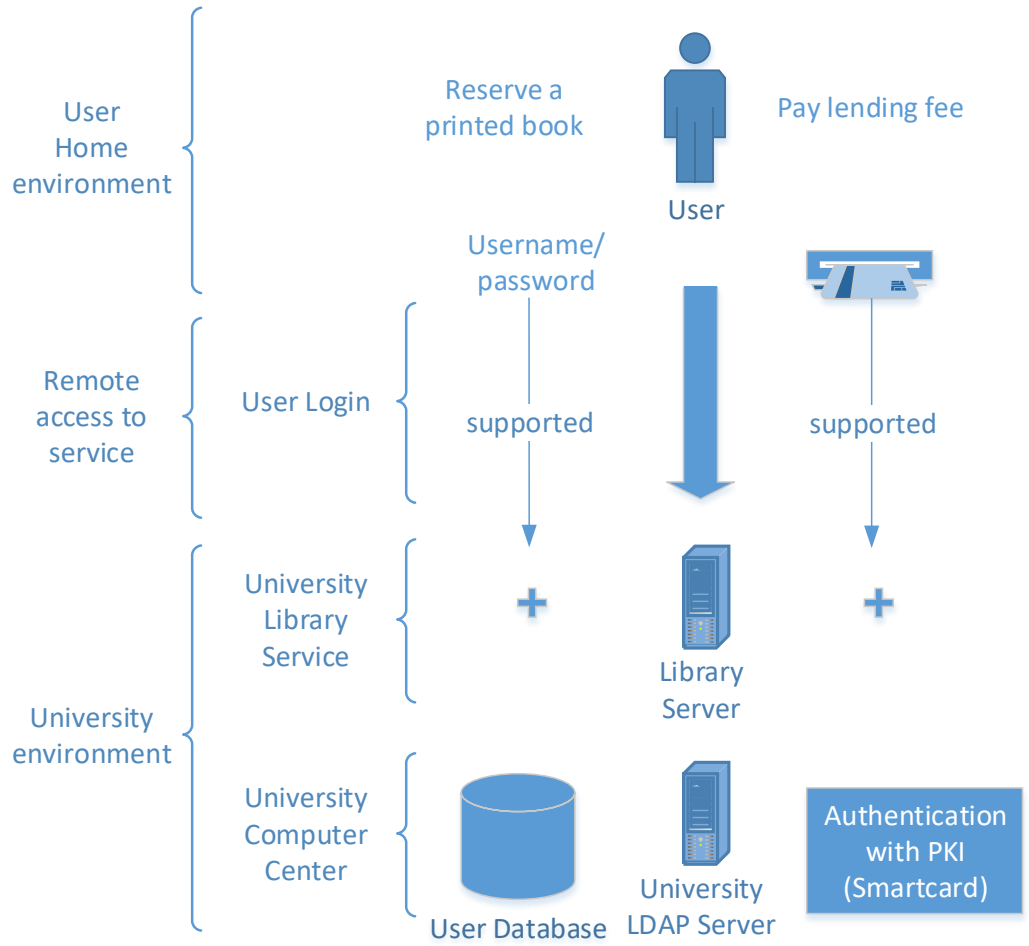


Figure 10. Proof-of-concept: user reserves a book or pays a lending fee at the university library server.

3.4.2 Application of the Proposed Framework

In Section 3.4.2, we apply the contributions of Section 3.3 to the two variants of the proof-of-concept scenario depicted in Section 3.4.1. The first variant uses a username/password, and the second variant a smartcard-based user identification and authentication.

Username and Password-Based Login to the University Library Service

The scenario in Figure 10 is scrutinized based on Section 3.3. First consider the use case depiction in Figure 2 from Section 3.3.1 for visualizing the service access process.

According to Sections 3.3.2.1 and 3.3.2.2, the identity – the attribute username – presentation is done manually and is authenticable. The user has no other information storage than his memory. From Section 3.3.2.3, the service-centric DFD representation from Figure 3 will be taken. Following Section 3.3.2.4, phase 2, the identification is undertaken through the library server, therefore centralized by contacting the University LDAP server, and phase 3, the authentication, is also conducted centralized. It depends on the realization of IA, namely whether it is on one or

two servers, and therefore if the LDAP has its own user database or contacts an external one for performing the authentication. The present proof-of-concept assumes an LDAP with its own user database, and thus one server (IA). Considering Figure 5 and 6 in 3.3.2.5, the verification of the legitimate usage of the username is determined as local authentication. The user is not giving further attributes.

Table 6 in Section 3.3.3.1 presents the global table of DFD elements IA mapped to LINDDUN privacy threats for (IA) and (I) (A). Based on Section 3.3.3.2, the scenario presents the Exclusive-Trust (U) (S) (I A) property and obeys the DFD example 3.4.2.2 in Section 3.3.3.2. As commented in Section 3.3.2.5, the recommended secure channel communication between the user client and server is given accessing the university servers by using https. Mutual authentication between the user client and server is not used and no SSO with the authentication is offered.

The considerations made lead to the left light grey components of the DFD shown in Figure 11 and considering from

Table 6 the cells for (IA) on one server. At this point of the selected proof-of-concept variation, the auditor would have to continue with step 3 of the LINDDUN framework [16].

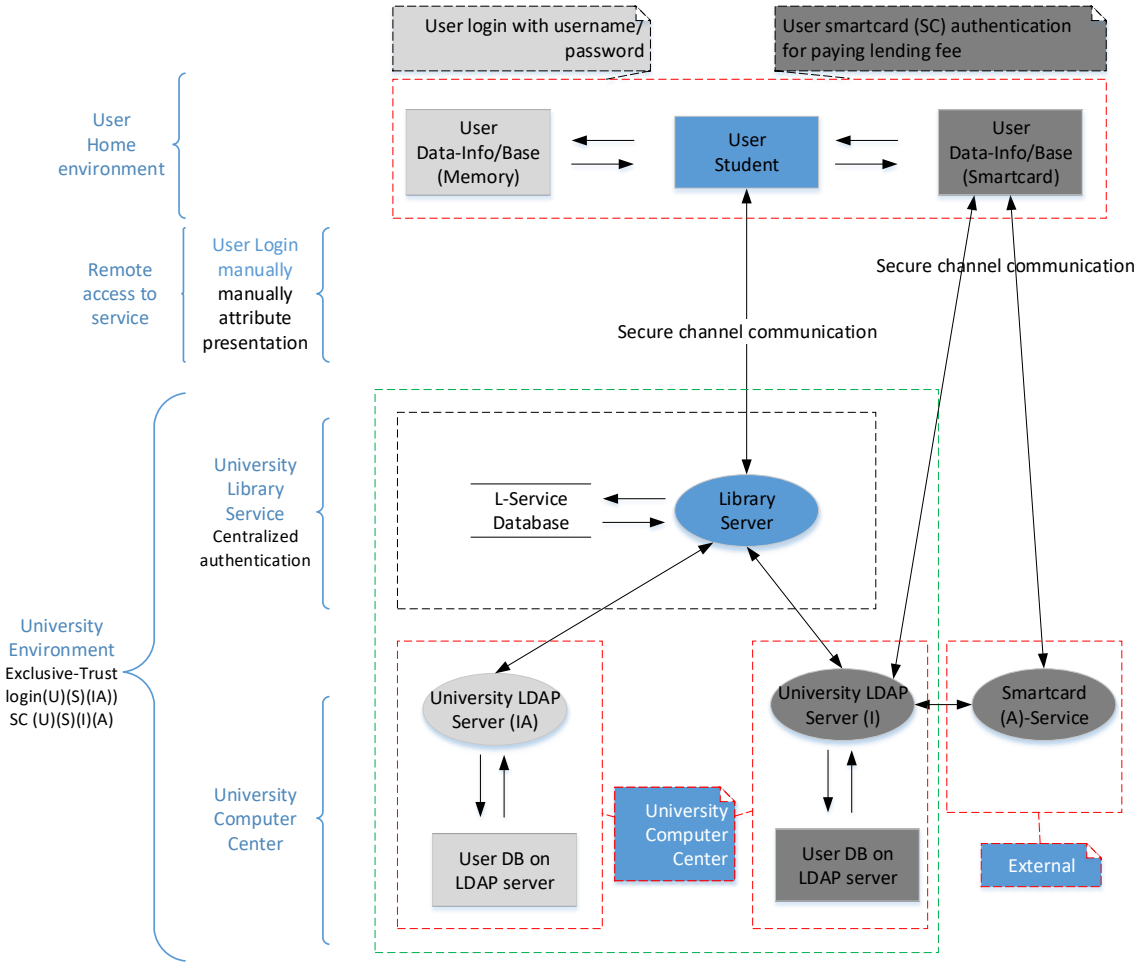


Figure 11. DFD for proof-of-concept: User/password login and smartcard-based authentication.

Smart-Card-Based Authentication for Electronic Payment of Lending Fee at University Library Service

Consider again as in the beginning of Section 3.4.2 the use case in Figure 2 from Section 3.3.1 for visualizing the whole service access process.

According to Sections 3.3.2.1 and 3.3.2.2, the identity – the attribute username – presentation now is conducted electronically and is authenticable. The user brings along the information storage in the smartcard. From Section 3.3.2.3, the service-centric DFD representation from Figure 3 will be taken. Following Section 3.3.2.4, phase 2, the identification, is done through the library server contacting the university LDAP server, and phase 3, the authentication, is undertaken directly between the user device and the external smartcard authentication server, and therefore decentralized. Assuming for the present proof-of-concept variation that the identification is conducted by the university LDAP server and the authentication is delegated to the external smartcard authentication server, the present subsystem is based on two servers, (I)

(A). Considering Figure 5 and 7 in 3.3.2.5, the verification of the legitimate usage of the username is determined as external authentication. The user is not giving further attributes.

Table 6 in Section 3.3.3.1 presents the global table of DFD elements IA mapped to LINDDUN privacy threats for (IA) and (I) (A). Based on Section 3.3.3.2, the scenario presents the Exclusive-Trust (U) (S) (I) (A) property and obeys the DFD example 3.3.3.2.1.2 in Section 3.3.3.2. As commented in Section 3.3.2.5, the recommended secure channel communication between the user client smartcard reader and smartcard authentication server is given by using TLS. Mutual authentication between the user client smartcard reader and the smartcard authentication server is used and no SSO with the authentication is offered.

The considerations result in the right dark grey components of the DFD shown in Figure 11 and considering from

Table 6 the cells for (I)-(A) on two servers. At this point of the selected proof-of-concept variation, the auditor would have to continue with step 3 of the LINDDUN framework [16].

3.4.3 Discussion

This section discusses several aspects of our contributions, particularly regarding the application of the two use cases of user authentication described in the previous subsections.

In Section 3.3.1, Figure 2 offers a high-level entry point into the system analysis for the general use case of *user demanding service access*. The presented subdivision facilitates the auditor a first assignment of parts of their system to the general use case. At this stage, for both proof-of-concept variants (two uses cases of user authentication) in Section 3.4.2, we would like to stress the different specificity of (i) the user login with a username and password, and (ii) user authentication with a smartcard. These two variants could be regarded as *centralized user verification* or *decentralized user verification*.

On the other hand, Section 3.3.2 provides the auditor with a tool set to break down the user verification process in their system. Sections 3.3.2.1 and 3.3.2.2 facilitate the auditor to itemize their identification and authentication methods used with Table 2 and 3. For both uses cases of user authentication, the core findings are:

- In the first use case with a username and password login, no additional user data base (repository) is present. Phase 2, the identification, and phase 3, the authentication, are conducted on the same server including a user DB. The verification of the legitimate usage

of the username is determined as local authentication and is a centralized verification based on one server (IA).

- Per contra, in the second use case with smartcard authentication, an additional user data base (repository) is present. Phase 2, the identification, is carried out through one server, and phase 3, the authentication, is performed directly between the user device and a second external smartcard-authentication server. The verification of the legitimate usage of the username is given by an external authentication and is a decentralized verification based on two servers (I) (A).

A comparison of the two use cases shows that the results can vary largely depending on the assumptions made. Concerning the centralized and decentralized user verification on the one hand, and on the other hand, the one (IA) or two (I)(A) server solution for identification and authentication, we notice that the results could be switched. This means that the first use case with a username and password login could be conducted in a decentralized manner, and therefore on two (I)-(A) servers, e.g. using a separate user database server. Consequently, the second use case with smartcard authentication could take place in a centralized environment and therefore carried out on one (IA) server. In this case, a smartcard authentication service would be integrated in the university LDAP server.

To our best knowledge, for the first time a set of tables of user identification and authentication methods are introduced. Likewise, our work is the first to introduce – in combination with the aforementioned tables – a user data base store (repository) to the DFD representation. Furthermore, we have extended the verification process representation and trust boundary concept. A remaining limitation is the lack of further adaptation of the LINDDUN framework for more environments.

The relevance of our work also lies in the practical applicability of the proposed solution. In particular, auditors can easily map the LINDDUN privacy threats to the DFD IA model created in Section 3.3.2. More specifically,

Table 6 in Section 3.3.3.1 presents the IA DFD elements mapped to the LINDDUN privacy threats for one server (IA) and two server (I)-(A) solutions. In this manner, the most suitable trust boundary concept can be selected. For both proofs-of-concepts, the most important remarks are described next:

- In the first use case (with username and password login), from
- Table 6 the cells for (IA) on one server are considered and the scenario presents the Exclusive-Trust (U) (S) (I A) property.

- In the second use case (with smartcard authentication), from
- Table 6 the cells for (I)(A) on two servers are contemplated and the scenario shows the Exclusive-Trust (U) (S) (I) (A) property.

The combination of both remarks highlight that the auditor is supported in eliciting trust boundaries and that they should be aware of the fact that the cell groups for one server (IA) and two server (I)-(A) solution in

Table 6 are mutually exclusive.

Nonetheless, the most important aspect of our proposal is the adaptation of the LINDDUN framework to allow identification and authentication processes. The extension and application of the trust boundary concept to LINDDUN are undoubtedly a major advance in the systematic modeling of privacy threats in the context of those two processes. However, one of the limitations of such an adaptation is that our solution is constrained to the assumptions made after step 2, and that the extension is obviously tailored for IA processes. We elaborate further in the section on *Emphasizing our contribution* that one important challenge is to extend the application of LINDDUN to more environments.

Finally, we would like to emphasize that with the user data repository (user data-info/-base), we proposed a more precise modelling of the location of attributes and authentication factors. This permits analysing more specific privacy threats.

Emphasizing our contribution

This section reviews the state of the art relevant to Chapter 3 and emphasizes the value and novelty of our contributions. We proceed first by stressing the relevance of LINDDUN, the privacy threat analysis framework that we build upon.

The usage of LINDDUN is predominant in the context of threat modelling methodologies. However, we would like to emphasize that the focus is largely on security threat modelling, where LINDDUN is mentioned as one systematic modelling framework focusing on privacy threat analysis. This is specifically stated in [51], where a systematic literature review of threat modelling is conducted based on more than 100 works. In the cited paper, the authors contemplate that LINDDUN can address security threats in the environment of software application with a focus on privacy.

The usage of LINDDUN is also suggested in [52] as central threat modelling methodology in the context of privacy by design, to directly achieve privacy guaranteeing systems. In that paper, the authors utilize LINDDUN as the core threat modelling methodology and propose the usage of LINDDUN in an iterative way.

A further recent paper [53] offers a summary of available methods for threat modelling associated with twelve threat modelling methods that tackle most security services. Particularly only for LINDDUN, the authors emphasize its relevance on privacy. Most of the proposed threat modelling methods are based on a data flow diagram (DFD) to describe the system to be analysed. In [54], the threat methodologies STRIDE and LINDDUN are shown to be susceptible to certain threat explosion vulnerabilities, which the authors attempt to mitigate by first applying the PASTA threat methodology and afterwards LINDDUN. The authors claim that *PASTA also mitigates the threat explosion weaknesses of STRIDE and LINDDUN by utilizing risk and impact analysis*. In the context of threat explosion, [55] proposes a refinement of LINDDUN to mitigate its vulnerabilities.

We agree with the authors of [54] to use LINDDUN for threat modelling with a focus on privacy. However, we do not completely agree with previously applying PASTA to mitigate the threat explosion weaknesses of LINDDUN. We believe that at that stage, possible relevant threats might be disregarded. In the cited paper, the authors evaluate LINDDUN based on the core categorizations of *Strengths and Weaknesses and Tailorability* and conclude that its level of maturity is sufficient high and that no consistent results could be achieved. As for tailorability, [11] states that *since none of these methods were designed with a specific type of system in mind, all may be applied to any kind of system*.

On the one hand, we agree with [11] that LINDDUN has achieved a high level of maturity, and on the other hand, we acknowledge the previously mentioned weaknesses and limitations as far as tailorability is concerned. In this dissertation, we aimed to achieve consistent results to increase the reproducibility of the application of LINDDUN, e.g. a more detailed and systematic approach to create the DFD of a system. One further contribution of the present chapter is a step-by-step guide to be used by analysts. This last step additionally guarantees a higher reproducibility, since the guided DFD creation depends less on the knowledge of the analyst.

Our focus on LINDDUN and therefore the relevance of our contributions are then justified by the extensive literature succinctly reviewed above. The adaptation of the LINDDUN framework for the specific services of identification and authentication may not need justification. Identification and authentication are essential and nearly ubiquitous security services nowadays.

Now we discuss different aspects related to privacy in the context of identification and authentication.

In privacy enhanced authentication systems (e.g. attribute-based credentials [56]), we find systematic analyses of privacy threats based on system-related weaknesses. The authors of the cited work offer an example: “Even though an attribute may be anonymous, the ‘leaking’ of

information from another level in the infrastructure, such as an IP address, could make the attribute pseudonymous or even fully identifying…". A further example of privacy threats in IA is given in [57], where a privacy vulnerability of OpenID was found.

The vulnerabilities mentioned in [56] and [57] can be analysed systematically with our extended LINDDUN methodology, which we enhance to contemplate IA process modelling components. Our work supports the systematic development of privacy-by-default fulfilling systems, which guarantee a higher reproducibility based on our LINDDUN methodology.

In the review of LINDDUN-related papers in [58], the authors propose a further improvement of LINDDUN comprising the so-called *Interaction-Based Privacy Threat Elicitation* which – as the authors acknowledge – is also associated with threat explosion. Similar to this approach, we have independently introduced the subdivision of Process Phases P1-P2 and Sub-Phases in the context of systematically describing more detailed identification and authentication processes. Our subdivision of IA processes is to perform a reproducible, reusable, and detailed segregation of the subphases of identification and authentication.

Finally, to stress the novelty and relevance of our versatile contributions to the DFD-based modelling, and for the sake of completeness we would like to briefly comment on [59]. In this paper, the authors mention the privacy knowledge for threat elicitation, list six different knowledge bases including LINDDUN and assume for all of them a common underlying DFD modelling of the system. From this standpoint, our enhanced DFD modelling methodology could be used across all these so-called knowledge bases for privacy knowledge for threat elicitation.

3.5 Conclusion

Systematic approaches for PTA are a central pillar for a reliable PIA, but this task is in general not carried out systematically. The LINDDUN framework has become a promising approach for a systematic PTA framework, as we stated in related work.

- Our first main contribution is a novel modelling framework for an identification (I) and authentication (A) process that is usable with LINDDUN framework [16, 33–37]. To our best knowledge, the proposed novel DFD based I and A modelling framework provides a compilation of tables including I- and A-methods linked with well-known procedures for the first time.
- Our second main contribution applies the privacy threat mapping of the LINDDUN framework to our data flow diagram (DFD)-based IA modelling framework. More specifically, we have extended the LINDDUN trust boundary concept to the developed DFD-based IA modelling framework. We have also adapted steps 1 and 2 of the LINDDUN

framework to be usable for PTA of the I and A process. This contribution facilitates a generic mapping of the DFD elements of the IA modelling framework to LINDDUN privacy threats. It distinguishes the realization of the process as one component (IA) and two components (I)-(A) and is furthermore usable as a generic template by the auditor.

- The third contribution is the generic UML drawing in Figure 2 (see 3.3.1) which serves as an entry point for the auditor for a first categorization of the system.
- The fourth contribution is the compilation of straightforward instructions, (see Section 3.3.4) which guides the auditor through the application of the contributions of the present chapter.
- Finally, with the fifth contribution we have introduced a more detailed modelling of the user data repository called user data-info/-base to the DFD applied in LINDDUN. The user data-info/-base makes possible a more precise representation of the location where user attributes are stored, e.g. in the user memory, smartcard or the cloud. This is a major further step towards the analysis and realization of user self-determination.

The specific objectives for the design of the PTA framework are described next:

- Rely on a mature and widely used privacy threat analysis framework.
- Satisfy upcoming demands stated in the literature such as privacy by default, adequate reduction of threat explosion weakness, reproducibility and adaptability.
- Capable of being extended to encompass identification and authentication, which are core processes to guarantee trustworthiness.
- Create a DFD-based system modelling method applicable with different privacy knowledge bases for threat elicitation.

As future research, we intend to extend our results to more environments (apart from that of I and A), develop more modelling procedures and hence systematic PTA methodologies focusing on specific user requirements.

Chapter 4

4 Privacy Threat Analysis of the verification process of realized authentication schemes

4.1 Introduction

The most commonly used authentication scheme to authenticate towards the ubiquitously present internet and smart community services and devices for proving the user's identity is still predominantly password-based [60]. Passwords are dominant despite being flawed, insecure [61, 62], and openly disliked by users. They are susceptible to various attacks, such as dictionary attacks, brute force, shoulder surfing, phishing attacks, key loggers, or video recording attacks [63, 64]. These variety of password attacks and the huge amount of accessible password leaks [65, 66] make it indispensable to find alternatives that are more reliable.

One arising challenge is to find an appropriate authentication scheme to cover the wide range of desirable requirements that are frequently in tension with each other. Bonneau et al. [20] made a fundamental contribution in this direction by proposing a comparative framework called UDS, comprising 25 criteria belonging to three benefit categories of usability (U), deployability (D) and security (S). The security benefits only intrinsically comprise three privacy benefits[2] (properties). While the framework presented by Bonneau et al. [20] is analysed and extended with additional criteria by Zimmermann et al [43, 44], the privacy dimension remains limited. User privacy in authentication schemes is still a challenge and comprises aspects of hard privacy, e.g. enforcing technical measures, and soft privacy [16] (see Table 7), e.g. the required compliance with privacy regulations [16, 25].

The main aim of Chapter 4 is to extend UDS with a privacy (P) benefit category. The UDSP framework introduces the privacy benefits *PB1 No-Trusted-Third-Party*, *PB2 Requiring-Explicit-Consent*, *PB3 Unlinkable*, *PB4 Resilient-to-Identifiability*, *PB5 Intervenability*, *PB6 Transparency* and *PB7 Resilient-to-Impersonation*. Thus, the UDSP framework in section 4.3

additionally considers important privacy publications such as [5, 16, 67, 68] privacy-related security benefits [20] and includes behavioural biometric based on machine learning (ML) [24]. The evaluation comprises the authentication schemes of Bonneau et al. [20, 49] and extends the biometrics category with behavioural biometrics [24] voice, gait, hand motions, eye-gaze, heartbeat and brain activity chosen by the authors to present *privacy-protecting techniques for data of behavioural biometrics* that they surveyed.

To the best of our knowledge, Bonneau et al. [20] is the most promising framework for a comprehensive evaluation of usability, deployability and security benefits of authentication schemes, including biometrics. Nonetheless, it lacks a privacy category to facilitate the evaluation of privacy benefits. Chapter 4 incorporate a privacy benefit[2] category based on well-known and recognized privacy properties.[1] The UDS framework [20] covers 35 authentication schemes and we add behavioural biometrics [24]. The survey of privacy-protecting techniques in [24] contributes to fulfil the UDSP framework privacy benefits that we defined to gain a more privacy-proofed authentication scheme than web passwords. We evaluate the authentication schemes from the UDS framework [20] and including additionally the behavioural biometrics [24] with the UDSP framework that we presented. Our evaluation reveal privacy threats for which we propose implementation approaches, including established standard cryptographic technologies for biometric data protection.

More specifically, the main contributions of Chapter 4 are summarized as follows:

I. We extend the framework originally proposed by Bonneau et al. [20] to comprise a privacy category, including the following privacy benefits: *PB1* No-Trusted-Third-Party, *PB2* Requiring-Explicit-Consent, *PB3* Unlinkable, *PB4* Resilient-to-Identifiability, *PB5* Intervenability, *PB6* Transparency and *PB7* Resilient-to-Impersonation.
II. With the new UDSP framework we evaluate the authentication schemes analysed in [20] and additionally the behavioural biometrics from Hanisch et al. [24] that we included.
III. We elicit the privacy threats and categorise them by the asset they bear on and provide the description of the cause.
IV. We propose implementation approaches to mitigate fundamental privacy threats of authentication schemes.

The remainder of Chapter 4 is organized as follows. Section 4.2 presents the background and related work of evaluation frameworks, privacy properties and biometric schemes. The privacy benefit category of the new UDSP framework is worked out in section 4.3. The evaluation of the authentication schemes with the UDSP framework is performed in section 4.4. Section 0 shows

our detailed discussion. Finally, in section 4.6 concluding remarks are given, and we sketch a conceivable multi factor authentication scheme without a password including a behavioural biometric. The prospect for the behavioural biometric is to become a single-factor authentication scheme and in the best case with continuous authentication.

4.2 Background and related work

In section 4.2.1 we explain the methodology followed to derive the privacy benefits of section 4.3 and introduce advances on biometric schemes in section 4.2.2.

4.2.1 From privacy properties to privacy benefits

In *LINDDUN: A privacy threat analysis framework* [16], Wuyts et al. systematically guide an analyst to make a privacy threat analysis (PTA), so that the associated privacy properties (benefits) are fulfilled. To the best of our knowledge, LINDDUN is the only promising PTA framework that is systematically and scientifically proven. The underlying privacy properties in LINDDUN are defined and grouped into hard and soft privacy. Accordingly, hard privacy as written in [16] "*...refers to data minimization, based on the assumption that personal data is not divulged to third parties.*" Furthermore, the authors write that: "*Soft privacy, on the contrary, is based on the assumption that data subject lost control of personal data and has to trust the honesty and competence of data controllers.*" Summing up, hard privacy focuses on avoiding disclosing personal data and soft privacy focuses on the demanded obligation towards data controllers, which obtain the information. In Table 7, the authors present the privacy properties and related privacy threats for the categories hard and soft privacy. In the present dissertation, Table 7 with its underlying privacy properties is the starting point to extend the UDS framework with a privacy category to achieve the UDSP framework and are derived as follows.

	Privacy properties	Privacy threats
HARD	Unlinkability	**L**inkability
	Anonymity & Pseudonymity	**I**dentifiability
	Plausible deniability	**N**on-repudiation
	Undetectability& Unobservability	**D**etectability
	Confidentiality	**D**isclosure of information
SOFT	Content awarness	Content **U**nawarness
	Policy and consent compliance	Policy and consent **N**on-compliance

Table 7: LINDDUN privacy properties and privacy threats as defined in [16].

The privacy properties of *unlikability*, *anonymity,* and *pseudonymity* are built on definitions based on the paper by Pfitzmann et. al [5]. *Plausible deniability* is defined based on the dissertation of Michael Roe [69]. *Undetectability* and *unobservability* are defined on definitions based on the paper of Pfitzmann et. al [5]. The definition of *confidentiality* is based on the draft of NIST [70]

and is kept up in the corresponding NIST [71] publication. *Content awareness* is summarized in [16] with "the content awareness property focuses on the user's consciousness regarding his own data" and *policy and consent compliance* is defined essentially according to [72] and repealed by REGULATION (EU) 2016/679 [25], whereby the later will be considered throughout Chapter 4 and this dissertation. Further principals considered by Hansen et al. [68] from the *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH)* are privacy default settings comprising data minimization and intervenability. Finally, we stress that the document *DATA PROTECTION ENGINEERING* from ENISA [67] in the context of privacy engineering especially add – besides the security triad (CIA) of *confidentiality*, *integrity* and *availability* – for privacy *unlinkability*, *transparency* and *intervenability.* Thus, we propose to address the absence of a privacy benefit category and associated properties based on [5, 16, 25, 67, 68, 70–72]. For better readability with respect to [20], we will use the term privacy benefit[2] (PB) instead of the common term privacy properties.

4.2.2 Biometric schemes

As stated in section 2.2, the UDS framework to evaluate authentication schemes is extended by Zimmermann et. al. [43, 44]. In section 4.2.1, we present the basis to extend the evaluation criteria of [20] insofar that we introduce an additional category, namely privacy benefit (see section 4.3), preserving the privacy related benefits organized as part of the security benefits of the seminal work of Bonneau et. al [20]. UDS has the further limitation of considering only three biometrics, namely fingerprint, iris and voice recognition, all belonging to the physiological (and partially to the behavioural) category.

Physiological and especially behavioural biometrics are emerging, because increasingly more manageable sensors are capable of capturing detailed and accurate biometric related information for authentication purposes. Physiological biometrics – among others – are fingerprint, face, iris, retina, and hand/palm. Furthermore, Hanisch et al. [24] give in their survey a representative overview of emerging behavioural biometrics, namely voice, gait, hands motion, eye-gaze, heartbeat and brain activity. The authors assume for the biometric data a data-publishing scenario, so that once the biometric data are privacy protected this data is voluntary published or shared with a service or application. Involuntary publication comprises somehow leaked biometric templates from authentication schemes.

In [24] machine learning is assumed for attribute extraction from the behavioural biometric data used for user authentication purpose at the application or service side. The service or application provider trusted by the user is assumed to be malicious and tries to infer ML-based personal

information beyond that needed for the authentication of the user. The authors survey anonymization methods that they identified in the literature analysis to mitigate the two main identified privacy threats, namely identity disclosure to identify the user in another scenario and attribute disclosure to derive sensitive attributes form the behavioural biometrics. They give in the actualized paper version [73] of [24] an overview table indicating for the related privacy goals identity and attribute protection the different techniques that try to achieve these goals.

One challenge in the context of the usage of biometrics is the preservation of user privacy. Privacy disclosure can happen on the *biometric itself*, e.g. "disclose their biological information at any time in real life, such as the fingerprints left after touching some objects … " as Rui et al. [74] stated, or based on classical privacy disclosure, e.g. on *shoulder surfing* in the context of behavioural biometrics such as eye gaze [75]. Thus, with the privacy benefits we define, we will evaluate the physiological biometric recognition of fingerprint as a representative biometric from [20]. The evaluation of promising behavioural biometrics with the privacy benefits that we elicited is conducted for *voice*, *gait*, *hand motions*, *eye-gaze*, *heartbeat* and *brain activity* from [24] used by the authors to describe the surveyed privacy-protecting techniques for behavioural data. Especially the fast-emerging behavioural biometrics and its rich stream of information can leak privacy sensitive user-related attributes, especially in the assumed data-publishing scenario.

One promising biometric model assume a decentralized structure as proposed by FIDO Alliance[10] [76] in such a way that the biometric feature templates are stored directly at the sensor side where they have been extracted, using something like a secure element. The basic capture of the biometric trait can be undertaken as depicted by Mahfouz et al. [77], which involves starting at the user located sensor with *Data Acquisition -> Feature Extraction (elicit user specific characteristics) -> Feature Templates (storage of user specific characteristics)* **->** so that the feature template or a still modified probe is then compared with the feature extracted during the authentication of the user in real time.

Actual biometric based authentication systems usually rely on existing traditional authentication schemes so that the biometrics following the multifactor authentication options (*something the user knows*, *something the user has* and *something the user is*) [78] e.g. support the user to introduce a second authentication factor based on *something the user is* or e.g. used as single factor, both at the beginning of the session. The traditional authentication systems comprise a user identifier (UID) as assumed in [20] so that the user proves towards the verifier the claim that he is making with the usage of the UID, hence to be legitimated to use the UID. The proof of the

[10] fidoalliance.org/fido2/

claim is made based on the usage of, e.g. the fingerprint to directly login to the PC or service or authorizing the usage of a HW token as second factor with e.g. his fingerprint. The most widespread method to use biometrics is the creation of a biometric template that in the best case is only in possession of the data owner, the user. Established procedures protect biometric templates grounded on cryptography to fulfil the following biometric privacy goals that are non-invertibility, revocability and diversity. This is the reason why based on the paper of Tran et al. [79] and Rui et al. [74] we additionally consider further criteria that they propose for privacy preservation of biometrics. These biometric privacy benefits are unlinkability (UL) [74], non-invertibility (NI) [74, 79], revocability (RV) [74, 79] and diversity (DV).

4.3 Privacy Benefit Category for the UDSP Framework

In section 4.3, we extend the UDS framework of Bonneau et al. [20] with the privacy benefit category that comprises privacy properties based on LINDDUN from Wuyts et al. [16] and underlying properties e.g. defined by Pfitzmann et. al [5], the LIND(D)UN Privacy Threat Tree Catalog [80], dissertation of Michael Roe [69], the NIST special publication 800-122 [71], REGULATION (EU) 2016/ 679 OF THE (EU-GDPR) [25], project FutureID [81], *DATA PROTECTION ENGINEERING* from ENISA [67] and the ULD SH Standard Data Protection Model [68]. We want to remember that in the literature the term *privacy property* is normally used, but due to readability and for compatibility reasons with the terminology of Bonneau et al. [20] we will use the term *privacy benefit (PB)* (*see section 4.2.1*).

The privacy benefits of the UDSP framework we assembled offer – in contrast to UDS – significantly strengthen evaluation criteria and are shown in Table 8.

PB1 - PB3 correspond with the security benefits (S) S9 – S11 from [20], which we take over and where appropriate extend them with further criteria, and PB4 – PB7 are assembled by us. In sum, the PB can be structured as follows.

The privacy benefits that we assembled are based on:

Privacy Benefit (PB)	PB Name	Definition	Sources[11] for definition or extension
PB1	No-Trusted-Third-Party	UDS [20]	
PB2	Requiring-Explicit-Consent	UDS [20]	[24]
PB3	Unlinkable	UDS [20]	[16],[24],[80],[3],[4]
PB4	Resilient-to-Identifiability	UDSP[12]	[16],[5],[24],[80]
PB5	Intervenability	UDSP	[25],[68],[81],[82]
PB6	Transparency	UDSP	[16],[25],[67],[68],[81],[83],[84],[85]
PB7	Resilient-to-Impersonation	UDSP	[20],[24],[78]

Table 8: Privacy benefits gathered for the UDSP framework presented in Chapter 4.

PB1 - PB4 constitute privacy benefits usable to evaluate every single authentication scheme individually, with enhanced PB1 - PB3 [20, 49] benefits and PB4 defined in Chapter 4. Furthermore, PB5 – PB6 constitute privacy benefits that are mandatory in the same manner for all authentication schemes and necessary for being compliant with legal standards, thus only then the service or application provider can go live. Finally, PB7 reflects the privacy relevance of security benefits [20], which we enhance in the definition of PB7 and apply to the authentication schemes.

Summing up we want to foreground – before presenting the privacy benefits and the subsequently undertaken evaluation of authentication schemes – that the evaluation criteria of our UDSP framework are significantly strengthen with respect to UDS framework criteria [8]:

- The first three privacy benefits – taken from the seminal paper [8] – from PB1 – PB7 were strengthen by us, especially PB3.
- The PB4 and PB7 address privacy aspects related with identifiability and PB7 considers impersonation, namely the extreme of identifiability.
- The PB5 and PB6 are mandatory and a compliance requirement for the service to be authorized to go online.

[11] Privacy-related sources additionally considered for the definition or extension of the privacy benefits.
[12] UDSP = UDSP framework presented in the Chapter 4 including among others the new defined PB 4 – PB7.

4.3.1 PB1 No-Trusted-Third-Party:

"*The scheme does not rely on a trusted third party (other than the prover and the verifier) who could, upon being attacked or otherwise becoming untrustworthy, compromise the prover's security or privacy.*" as defined in Bonneau et al. [20]. In the context of biometrics, the definition comprises biometric user-centred devices capturing the biometric traits that then are processed, e.g. ML-based. In the best case afterwards, it is privacy protected before being used for the verification process towards the verifier, whereby only the prover and verifier are involved.

4.3.2 PB2 Requiring-Explicit-Consent:

"*The authentication process cannot be started without the explicit consent of the user. This is both a security and a privacy feature (a rogue wireless RFID-based credit card reader embedded in a sofa might charge a card without user knowledge or consent).*" as defined in Bonneau et al. [20]. Neither an automatic reuse of a still undertaken authentication is possible, nor a new authentication can be performed without the consent of the user. The usage of biometric data without user consent for authentication – regardless of whether it is based on an overt trait captured as a by-product or leaked or stolen biometric template – must be avoided.

4.3.3 PB3 Unlinkable:

Bonneau et al. [20] define unlinkable as follows: *"Colluding verifiers cannot determine, from the authenticator alone, whether the same user is authenticating to both. This is a privacy feature. To rate this benefit, we disregard linkability introduced by other mechanisms (same user ID, same IP address, etc)."* Furthermore, we consider linkability based on information gathered throughout the web browser, e.g. grounded on cookies or destructive fingerprinting [3, 4]. We include the linkability threat of entity [16, 80] for log-in using insufficient protected network communication (untrusted communication, hence not fully protected network communication and no or insufficient anonymised communication), and thus personal identifiable information (PII) (e.g. IP address, computer ID, identifier/biometrics, session ID or temporary ID) is linkable, or login with a certificate or a reused fix login, the last two also PII. Biometric data used must be protected against ML-based inference of private information, thus protecting the user's identity and attributes [24]. This equals protecting the true biometrical data, thus here avoiding linkability based on true biometric data or a derived biometric template.

4.3.4 PB4 Resilient-to-Identifiability:

The privacy benefit of being Resilient-to-Identifiability addresses privacy aspects that are not associated with impersonation, and thus we focus on anonymity and pseudonymity as defined in

[5] including plausible deniability as defined in [16, 80]. We consider the identifiability threat of an entity [16, 80] for log-in using insufficient protected network communication (untrusted communication, hence not fully protected network communication and no or insufficient anonymised communication) e.g. with a certificate, an identity, pseudo-identity based on a pseudonym, token or biometric as log-in or if a secret used could be related with the user. Biometric data used must be protected against ML-based inference of private information, thus protecting the user's identity and attributes [24]. This equals protecting the true biometric data, thus here avoiding identifiability based on true biometric data or a derived biometric template. The mere impersonation is evaluated in PB7 Resilient-to-Impersonation, the extreme of identifiability.

4.3.5 PB5 Intervenability:

"*The protection goal of intervenability aims at the possibility for parties involved in any personal data processing to interfere with the ongoing or planned data processing. The objective of intervenability is the application of corrective measures and counterbalances where necessary.*" (see FutureID Privacy Requirements Deliverable D22.3 [81]). According to Hansen et al. [68, 82] and REGULATION (EU) 2016/ 679 OF THE (EU-GDPR) [25] articles 12, 16, 17, 18 and 22, with our focus on authentication schemes-related data we choose the following intervenability possibilities (based on tools) to take into consideration: possibility of rectification of data, erasure of data, restriction of processing of data and possibility of intervention in processes of automated decisions. In other words, intervenability comprises especially technically enforceable user rights and is established in law. PB5 Intervenability is granted as offered (fulfilled) if the user can make use of the above-mentioned intervenability possibilities with the method of choice for the user, in our opinion a web browser. The verifiability of whether the services offer the demanded intervenability is not viable for general purposes, and even less for each of the authentication schemes. Thus, PB5 intervenability is considered mandatory (M) and we assume that the service or application provider is compliant with the requirements from [25], otherwise it would not have gained the authorization to go online.

4.3.6 PB6 Transparency:

"*Transparency ensures that all personal data processing including the legal, technical and organisational setting can be understood and reconstructed*", according to FutureID [81]. In our context, we stress for transparency the content awareness of the user (Entity) in accordance with Wuyts et al. [16], as well as the existence and communication of a privacy policy (compliance) as stated by Wuyts et al. [16] with the goal to "*inform the data subject about the system's privacy policy.*" The privacy policy should at least consider the following REGULATION (EU) 2016/

679 OF THE (EU-GDPR) [25] articles 12, 16, 17, 18, 20 and 22. The principle of transparency is laid down in article 5 of [25] and especially article 12 addresses transparency, demanding "transparent information, communication, and modalities for the exercise of the rights of the data subject."

The authors Fischer-Hübner et al. in [83–85] differentiate between *ex ante transparency* and *ex post transparency* according to the principles and requirements of the EU-GDPR [25]. As they wrote, *ex ante transparency* enables the anticipation of consequences before data are disclosed and *ex post transparency* informs about consequences if data already have been revealed.

In ex ante transparency, we consider availability of the system's privacy policy, their previous communication to all relevant parties and provision with privacy by design and by default, the latter is in article 25 of [25]). Ex ante transparency is granted as offered (fulfilled) if the verifier/service communicates the user an existing privacy policy and justifies precautionary measures to provide privacy by design and by default.

Ex post transparency comprises providing the possibility to execute all communicated user rights such as rectification, erasure, and others, based on *PB 5 intervenability* by the user and related to all information that is still disclosed. Ex post transparency is granted as offered (fulfilled) if this possibility is provided to the user.

The verifiability of whether services offer the demanded intervenability is not viable for general purpose, even less for each of the authentication schemes. Thus, PB6 transparency is considered mandatory (M), and we assume that the service or application provider is compliant with the requirements from [25], otherwise it would not have received the authorization to go online.

4.3.7 PB7 Resilient-to-Impersonation:

"*An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol,*" as defined by Carlisle Adams in van Tilberg *Encyclopedia of Cryptography and Security Second Edition* [78]. In the following we focus on assuming a user identity in a system. PB7 Resilient-to-Impersonation addresses the mere taking over of an user identity (see [78]). The security benefits S1 - S8 [20] in sum focus on robustness, and thus we define sub-benefits in Table 9 and ground our evaluation on the results of UDS in [20]. A sub-benefit is granted as offered (fulfilled) if all included security benefit were rated in [20] as *offers the benefit* or *almost offers the benefit*.

Grouping of Security Benefits S1 to S8 into: sub-benefit(s) of Resilient-to-Impersonation				
observation	guessing	external verifier leakage	phishing	loss of possession
S1, S2, S5	S3, S4	S6	S7	S8

Table 9: Grouping of security benefits to sub-benefits of resilient-to-impersonation.

Furthermore, the behavioural biometrics in [24] are evaluated with the security benefits S1 – S8, too, so that for this purpose the security benefits where reasonable are replenished (extended) with ML-related aspects to evaluate behavioural biometrics that otherwise remain as in [20]. The evaluation of behavioural biometric with PB7 – thus with S1 - S8 – is also assembled in Table 10. The resulting S1 – S8 are as follows:

S1 Resilient-to-Physical-Observation: "An attacker cannot impersonate a user after observing them authenticate one or more times" (see [20]). S2 Resilient-to-Targeted-Impersonation: "It is not possible for an acquaintance (or skilled investigator) to impersonate a specific user by exploiting knowledge of personal details (birth date, names of relatives etc.)" (see [20]). The considered behavioural biometric for S1 and S2 in general we consider susceptible to attacks focusing on physical observation or targeted impersonation based on machine learning analysis of behavioural data captured e.g. as a by-product, so that with inferred private information user identity and attributes can be compromised.

S3 Resilient-to-Throttled-Guessing: "*An attacker whose rate of guessing is constrained by the verifier cannot successfully guess the secrets of a significant fraction of users*" (see [20]). S4 Resilient-to-Unthrottled-Guessing: "*An attacker whose rate of guessing is constrained only by available computing resources cannot successfully guess the secrets of a significant fraction of users*" (see [20]). S3 as well as S4 are not offered in the context of ML assuming an external attacker with access to biometric data (e.g. biometric template) from a leak or captured as a by-product can infer private information and compromise the identity and attributes of the user.

S5 Resilient-to-Internal-Observation: "*An attacker cannot impersonate a user by intercepting the user's input from inside the user's device (e.g. by keylogging malware) or eavesdropping on the cleartext communication between prover and verifier (we assume that the attacker can also defeat TLS if it is used, perhaps through the CA)*" (see [20]). In accordance with the argumentation in [20] for RSA SecurID, we assume for behavioural biometrics that *dedicated devices can resist malware infiltration* (secure software and hardware development are assumed) and the other

aspects are not in the scope for the evaluation of the behavioural biometric, and thus we assume S5 offered for all authentication schemes.

S6 Resilient-to-Leaks-from-Other-Verifiers: "*Nothing that a verifier could possibly leak can help an attacker impersonate the user to another verifier*" (see [20]). If leaked, the biometric templates of an authentication system could be used by an attacker applying ML to infer private information and compromise the identity and attributes of the user.

S7 Resilient-to-Phishing: "*An attacker who simulates a valid verifier (including by DNS manipulation) cannot collect credentials that can later be used to impersonate the user to the actual verifier*", (see [20]). Biometric data captured as a by-product – with less effort than for a sophisticated phishing attack – is comparable to phishing biometric data, and thus we rate S7 as S3 and S4, not offered in the context of ML.

S8 Resilient-to-Theft: "*If the scheme uses a physical object for authentication, the object cannot be used for authentication by another person who gains possession of it*" (see [20]). An attacker who steals existing biometric data applying ML can infer private information and compromise the identity and attributes of the user.

4.4 Sample evaluation of authentication schemes with the UDSP Framework

We evaluate from [20] sample authentication schemes from the most established categories, also *YubiKey (HW Token)*, *GrIDsure (Cognitive)*, and *fingerprint (physiological biometric)*, and incumbent *legacy password* as reference. Our selection is grounded on the evaluation of the security benefits, usability benefits and/or deployability benefits in [20] (see the motivation for the corresponding authentication scheme in section 4.4.1 below). We additionally evaluate promising behavioural biometric from [24], *voice, gait, hands motion, eye-gaze, heartbeat and brain activity,* which the authors presented with the anonymization methods that they surveyed to protect behavioural biometric traits. The authors grounded their work on "*two main privacy threats that apply to behavioural data collected/processed by a third party"*, *identity disclosure* and *attribute disclosure*, which are in line with the PB3 Unlinkable and PB4 Resilient-to-Identifiability that we defined. In the actualized paper version [73], the authors provide an overview table indicating the privacy goals that the different techniques try to achieve.

We evaluate the sample authentication schemes [20] including behavioural biometrics [24] that we introduced with PB1 – PB7. The results are shown in Table 10.

		UDSP Privacy Benefits (PB1 to PB7)														
		PB1		PB2		PB3		PB4		PB5/PB6	PB7					
		No-Trusted-Third-Party		Requiring-Explicit-Consent		Unlinkable		Resilient-to-Identifiability		Intervenability/ Transparency	sub-benefits of Resilient-to-Impersonation					
											observation	guessing	external verifier leakage	phishing	loss of possession
Category	Scheme	UDS	UDSP	UDS	UDSP	UDS	UDSP	UDS	UDSP	Mandatory	S1, S2, S5	S3,S4	S6	S7	S8
(Incumbent)	Web passwords	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-a-	--	-	-	x
Password Manager	Firefox	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	aa-	--	-	x	x
	LastPass	NB	NB	● OB	● OB	● OB	NB	● OB	NB	M	aa-	aa	a	x	x
Proxy	URRSA	NB	NB	● OB	● OB	● OB	NB	● OB	NB	M	-aa	--	-	x	w
	Impostor	NB	NB	NB	NB	● OB	NB	● OB	NB	M	xaa	--	-	x	x
Federated	OpenID	NB	NB	● OB	● OB	NB	NB	NB	NB	M	aa-	aa	x	-	x
	Microsoft Passport	NB	NB	● OB	● OB	NB	NB	NB	NB	M	aa-	aa	x	-	x
	Facebook Connect	NB	NB	NB	NB	NB	NB	NB	NB	M	aa-	aa	x	-	x
	OTP over email	NB	NB	● OB	● OB	NB	NB	NB	NB	M	aa-	aa	x	x	x
Graphical	PCCP	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-x-	a-	x	x	x
	PassGo	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-x-	--	-	-	x
Cognitive	GrIDsure (original)	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-x-	--	-	-	x
	Weinshall	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	ax-	--	x	x	x
	Hopper Blum	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	ax-	--	x	x	x
	Word Association	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-w-	--	-	-	x
Paper tokens	OTPW	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-xx	xx	x	x	x
	S/KEY	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-xx	xx	x	a	w
	PIN+TAN	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-xx	xx	x	x	a
Visual crypto	PassWindow	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	axa	xx	x	x	w
Hardware tokens	RSA SecurID	NB	NB	● OB	● OB	● OB	NB	● OB	NB	M	xxx	xx	x	x	x
	YubiKey	NB	NB	● OB	● OB	● OB	NB	● OB	NB	M	xxx	xx	x	x	x
	IronKey	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	xaa	--	-	x	x
	CAP reader	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	xxx	xx	x	x	x
	Pico	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	xxx	xx	x	x	a
Phone-based	Phoolproof	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	xxa	xx	x	x	x
	Cronto	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	xxa	xx	x	x	x
	MP-Auth	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	-a-	--	-	x	x
	OTP over SMS	NB	NB	● OB	● OB	● OB	NB	● OB	NB	M	xxa	xx	x	x	x
	Google 2-Step	● OB	● OB	● OB	● OB	● OB	NB	● OB	NB	M	aa-	xx	x	x	x
Biometric	Fingerprint	● OB	● OB	● OB	● OB	NB	NB	NB	NB	M	xw-	x-	-	-	w
	Iris	● OB	● OB	● OB	● OB	NB	NB	NB	NB	M	xw-	x-	-	-	w
	Voice	● OB	● OB	● OB	● OB	NB	NB	NB	NB	M	xw-	a-	-	-	w
Behavioural Biometric	Voice	● OB	● OB	● OB	NB	NB	NB	NB	NB	M	--x	--	-	-	-
	Gait		● OB		NB		NB		NB	M	--x	--	-	-	-
	Hand motions		● OB		NB		NB		NB	M	--x	--	-	-	-
	eye-gaze		● OB		NB		NB		NB	M	--x	--	-	-	-
	Heartbeat		● OB		● OB		NB		NB	M	xxx	--	-	x	-
	Brain activity		● OB		● OB		NB		NB	M	xxx	--	-	x	-

Table 10: UDSP Evaluation for PB1 to PB4 (with ● OB = offer benefit, NB = not offered benefit); for PB5 and PB6 are mandatory = M for all; for sub-benefits of privacy benefit PB7 Resilient-to-Impersonation based on security benefits S1 – S8 (With X = offer benefit, a = almost offers benefit, - = not offered benefit, w = worse than web password). *"UDS" = evaluation with UDS framework of Bonneau et al. [20]. "UDSP" = evaluation with UDSP framework* presented in Chapter 4.

We evaluate PB1 – PB3 hybrid for the authentication schemes and fingerprint from [20], so that the evaluation result from [20] is taken and additionally *in contrast* the evaluation is performed with further UDSP criteria that we add and/or previously were disregarded in [20]. Afterwards, the evaluation with PB4 is also hybrid, but considering the previous evaluation for PB3, because both privacy benefits hold a close relation. Table 10 summarizes the evaluation with PB1 – PB4 for the sample authentication schemes.

PB5 and PB6 are mandatory for all authentication schemes and we assume that the service or application provider is compliant with the legal requirements from [25], otherwise it would not have received the authorization to go online (see the definition of PB5 and PB6 in section 4.3). Thus, PB5 Intervenability is offered if the intervenability possibilities in the PB5 definition grounded on [25] are provided by the service, and therefore PB6 transparency for ex post transparency is also offered. PB6 transparency for ex ante transparency is offered if an existing privacy policy is previously communicated to the user pointing to the PB5 details and the service justify privacy by design and by default measures has been performed.

PB7 is applied to the sample authentication schemes including fingerprint biometric from [20] considering the evaluation for S1 – S8 [20]. The newly introduced behavioural biometrics [24] are evaluated by us with S1 – S8 from [20] including ML-related aspects that we added with UDSP (see definition PB7 in section 4.3). Table 10 also summarizes the evaluation with PB7 of the sample authentication schemes.

The privacy evaluation in section 4.4.2 of authentication schemes using behavioural biometrics will be limited to the mere biometric data of the trait in the assumed data-publishing scenario considering associated technologies. Such aspects that can be related e.g. with user ID, underlying IP communication, etc. are not considered again because these are considered with the evaluation of the authentication schemes from Bonneau et al. [20] in section 4.4.1.

4.4.1 Authentication Schemes from UDS framework

This section comprises the evaluation of sample authentication schemes from [20] for PB1 – PB4. PB7 is undertaken based on the S1 – S8 evaluation in [20]. PB5 and PB6 are mandatory to be fulfilled before the service goes live, and thus not evaluated.

4.4.1.1 Legacy password:

PB1 No-Trusted-Third-Party is offered, because no TTP is involved, as well as PB2 Requiring-Explicit-Consent because the user must actively assent to login, so that no automatic reuse of a previous authentication is possible, as argued in [20].

PB3 Unlinkable is offered because in [20] linkability by the same user ID, same IP address and other mechanisms are disregarded and assume correctly salted passwords resulting in different authenticators for different services. By contrast, PB3 Unlinkable is not offered if information could be retrieved from cookies or browser fingerprinting, or the same user ID is used at different services. Further, we assume contrary to [20] that the IP communication is untrusted and relevant.

PB4 Resilient-to-Identifiability is offered because for PB3 in [20] the underlying IP communication, same user ID and other mechanisms are disregarded. By contrast, PB4 is not offered if contrary to their assumption the password authenticator can be related with the user, and/or an identity if a real name mail address is used, so no pseudonym is really used, and we assume that the IP communication is untrusted and relevant.

PB7 Resilient-to-Impersonation for legacy password is not fulfilled for the sub-benefits observation, guessing, external verifier leakage and phishing. Only the sub-benefit loss of possession is fulfilled. Only security benefit 8 resilient-to-theft is offered, and security benefit 2 resilient-to-targeted-impersonation is almost offered.

4.4.1.2 YubiKey

In the hardware token category, among the four best rated in the category of security benefits in [20] we selected YubiKey because it is much more accessible and mature than Pico, despite the fact that Pico is rated better for usability benefits.

PB1 No-Trusted-Third-Party is not offered, because in default mode every verifier relies on Yubico servers [20]. The button must be pressed, so PB2 Requiring-Explicit-Consent is offered [20]. The user has different tokens for each service, so PB3 Unlinkable is offered [20]. By contrast, PB3 Unlinkable is not offered if information could be retrieved from cookies or browser fingerprinting and assume the IP communication is also untrusted and relevant. Furthermore, the reuse of a token – hence the corresponding YubiKey pseudonym string at different services by a user – is more than probably due to the cost per token, which is a further reason why PB3 would not be offered.

PB4 Resilient-to-Identifiability is offered in accordance with the PB3 assumptions in [20] and it is assumed that the token software is implemented secure or the token hardware is physically secure. By contrast, PB4 Resilient-to-Identifiability is not offered for the mentioned reuse of the token and assume the IP communication is also untrusted and relevant. The security benefits S1 - S8 are all offered, so that for PB7 Resilient-to-Impersonation all sub-benefits observation, guessing, external verifier leakage, phishing and loss of possession are offered.

4.4.1.3 GrIDsure

In the cognitive category, we selected GrIDSure which belongs among the best three rated for security benefits in [20], because it offers much better usability than Weinshall and Hopper Blum.

PB1 No-Trusted-Third-Party is offered, because only the prover and verifier are involved [20]. PB2 Requiring-Explicit-Consent is offered because the user must transcribe the one-time password [20]. The considerations and evaluation results of the legacy password for PB3 Unlinkable and PB4 Resilient-to-Identifiability are applicable to GRIDsure, and therefore assigned the same rating. The security benefits S2 and S8 are offered, so that for PB7 Resilient-to-Impersonation only the sub-benefit loss of possession is offered.

4.4.1.4 Biometric fingerprint

We selected the physiological biometric fingerprint because it is marginally the best rated for security benefits in [20], whereby all biometrics are rated identically for usability and it belongs to the best rated for deployability.

PB1 No-Trusted-Third-Party is offered, because no TTP is involved [20]. We underline this, if e.g. a built-in fingerprint reader in a user device is autonomous from any other system outside.

The user must actively place their finger on the reader, so that PB2 Requiring-Explicit-Consent is offered [20]. We agree because an unintended or unperceived usage of the biometric fingerprint in the presence of the user is not feasible. PB3 Unlinkable is not offered because the authors in [20] solely argue that *physical biometrics are also a canonical example of schemes that are not unlinkable,* also linkable to a (pseudo)-identity.

PB4 is not offered based on the argumentation of PB3, and with the usage of real name mail addresses the biometric data could also be linked back to the (pseudo)-identity [80] used. Only the security benefits S1 and S3 are offered, so that for PB7 Resilient-to-Impersonation none of the sub-benefits are offered.

4.4.2 Behavioural biometric

Now follows the evaluation of behavioural biometric from [24] with UDSP PB1 – PB4 and PB7, whereby the latter is applied based on S1 – S8 replenished with ML-related aspects. PB5 and PB6 are mandatory to be fulfilled before the service goes live, and thus not evaluated here.

In accordance with [24] for behavioural biometrics we assume the privacy threats identity disclosure, and thus to link the behavioural data with the user identity, and attribute disclosure of sensitive attributes for the evaluation. The derived privacy goals [24] of identity protection and attribute protection are in line with the privacy benefits PB3 and PB4.

The applied attacker model [24] in the context of the considered data-publishing scenario assumes a malicious service or application provider that the user trusts, having full access to the behavioural biometric data, so the provider or application provider can freely apply inference techniques with machine learning. The identity disclosure attacker scope is to re-identify the user across accounts, assuming that he can link behavioural data to the user´s identity. The attribute disclosure attacker scope is *to derive sensitive attributes included within the available behavioural data that the user did not intend to disclose, such as gender, age, or mental state*. The behavioural biometric data is analysed based on machine learning to infer private information of the user [24] and compromise the privacy goals. The service or application provider authenticates the user with the behavioural biometric data, extracting user-related attributes with machine learning, having the unhindered possibility to extract further attributes that are neither required for authentication nor consented by the user.

The behavioural biometric [24] *voice, gait, hands motion* and *eye-gaze* are overt traits, and *heartbeat* and *brain activity* are covert traits. Overt traits can be captured as a by-product without user consent, e.g. the gait with cameras, and covert traits cannot be captured as a by-product, e.g. brain activity requires placing head contacts, which requires user consent.

The detailed evaluation for all overt trait-based biometrics for PB7 sub-benefits is given on behalf for all in the evaluation of gait. The covert trait-based biometric evaluation of PB7 is given on behalf for all in that for heartbeat. Differences are commented in the corresponding biometric paragraph.

Furthermore, we comment the scope of the privacy-protecting techniques [24] in the context of the data-publishing scenario [24]. The privacy-protecting techniques (anonymization methods) privacy goals in [24] are *identity protection* and *attribute protection* of behavioural biometrics presented in [24], which we consider here for the biometric-based user authentication use case (utility). These anonymization methods are intended for the use in a data-publishing scenario for authentication purposes, so that behavioural data collected by the user is treated in a privacy protective manner and then published or shared with a service or application. *"This also includes involuntary publication, which for example can occur when the biometric templates of an authentication system are leaked"* [24]. The approach in [24] has in scope that not only the data owner (the user) learns anything from the data, contrary to the most widespread method to restrict access to biometric data or a biometric template.

An aspect that is not treated throughout the following evaluation is how to distinguish for overt traits if the presented biometric data to the service or application was really captured by the owner and not as a by-product, or a leaked or stolen biometric template is presented on behalf of the real owner by an attacker. This interesting and challenging consideration is beyond our scope being part of future research.

4.4.2.1 Impact of Data-publishing related attacker model

The evaluation of the behavioural biometric-based authentication is done primarily conducted based on the data-publishing [24] approach, also biometric data presented towards the service or application provider.

I. The service and application provider are assumed to be malicious being the central attack we scope on [24], so that they try to infer from the passed biometric data by the user, e.g. a biometric template private information not required for the mere authentication process.
II. Biometric templates could be leaked or stolen, and thus the malicious service or application provider and others can also use them to infer private information. Extended view of the central attack scope also affecting PB7-related security benefits 1-8.
III. Overt trait-based biometrics could be captured as a by-product by anyone and presented to the service or application provider without user consent and of course infer whatever available private information. Considerable in the PB7-related security benefits 1-8.

4.4.2.2 Voice

In [20], time-variant challenge response phrases are assumed to avoid trivial record-and-replay attacks. PB1 No-Trusted-Third-Party is offered, because no TTP is involved [20]. PB2 Requiring-Explicit-Consent is offered because the user must intentionally pronounce the corresponding challenge response phrase [20]. By contrast, following [24] with a created fake record, audio samples and secret records the user consent can be circumvented, and thus PB2 would not be offered because generative attacks with ML are possible [20] even for time-variant challenge response phrases. PB3 Unlinkable is not offered for voice because in [20] they argue it is comparable to fingerprint. We refer for the further argumentation for PB4 to biometric fingerprinting, and thus PB4 Resilient-to-Identifiability is also not offered. Additionally, we point out that PB3 and PB4 are also not offered because the malicious service or application provider could infer private information beyond that required for authentication revealing sensitive attributes and identify the user in another scenario based on biometric data [24]. None of the PB7 Resilient-to-Impersonation sub-benefits are offered (see evaluation of gait). In contrast to the PB7 evaluation for gait, the voice by-product can be captured with a voice recorder.

4.4.2.3 Gait

The gait analysis considers the movement of the human limbs in its typical occurrences, namely trotting, walking, or running [24]. PB1 No-Trusted-Third-Party is offered, because only the verifier and prover are involved. PB2 Requiring-Explicit-Consent is not offered, because without user consent a simple camera capture as a by-product inferring private information could be presented to the service and application provider. Additionally, we point out that PB3 and PB4 are also not offered, because the malicious service or application provider could infer private information beyond that required for authentication revealing sensitive attributes and identify the user in another scenario based on biometric data [24]. The security benefits S1 Resilient-to-Physical-Observation is not offered, because with observation as a by-product a capture with a camera could be made. Once biometric data are collected as a by-product ML-based attributes could be inferred, and thus S2 Resilient-to-Targeted-Impersonation is not offered. For S3 Resilient-to-Throttled-Guessing and S4 Resilient-to-Unthrottled-Guessing**,** an attacker has no constraint to apply ML to infer attributes from biometric data collected as a by-product, and thus both are not offered. S5 Resilient-to-Internal-Observation is offered, assuming secure software and hardware development for the biometric device. Leaked biometric data due to an inference attack could be used for identity and attribute disclosure, and thus S6 Resilient-to-Leaks-from-Other-Verifiers is not offered. Assuming that biometric data captured as a by-product is something like a phishing attack with less effort, S7 Resilient-to-Phishing is not offered. Stolen

biometric data could be used for identity and attribute disclosure, so that S8 Resilient-to-Theft is not offered. Consequently, for PB7 Resilient-to-Impersonation none of the sub-benefits are offered.

The evaluation of behavioural biometric based on overt traits with PB7 mainly consider throughout the security benefits S1 – S8 data captured as a by-product, because it is the easiest way to obtain biometric data to infer private information to compromise the user identity and special attributes with ML.

4.4.2.4 Hand Motions

Hand motions include a wide variety of movements comprising signature, mouse movement, keyboard stroke and hand gestures [24]. In relation with the user authentication, keystroke, online handwriting, and hand gestures are the most suitable hand motions.

PB1 No-Trusted-Third-Party is offered, because only the verifier and prover are involved. PB2 Requiring-Explicit-Consent is not offered, because without user consent, e.g. hand gestures – which are becoming popular with the rise of smartphones – could be captured in daily life with a camera or through keystrokes and presented to the service and application provider. PB3 and PB4 are also not offered, because the malicious service or application provider could infer private information beyond that required for authentication revealing sensitive attributes and identify the user in another scenario based on biometric data [24]. Furthermore, for PB3 and PB4, beside being captured directly, keystrokes could be recognised based on network latency side-channel attacks. None of the PB7 Resilient-to-Impersonation sub-benefits are offered (see evaluation of gait).

4.4.2.5 Eye-Gaze

In Bonneau et al. [20] iris (pattern) recognition based on [86, 87] primarily considers the physiological aspect of the eye, contrary to this in [24] the *eye-gaze* is analysed including corneal reflection as well as gaze movement, and thus we evaluate eye-gaze independently from the evaluation in [20].

PB1 No-Trusted-Third-Party is offered, because no TTP is involved. PB2 Requiring-Explicit-Consent is not offered, because without user consent simply a camera capture as a by-product inferring private information could be presented to the service and application provider.

Additionally, we point out that PB3 and PB4 are also not offered because the service could infer private information beyond that required for authentication revealing sensitive attributes and identify the user in another scenario based on biometric data [24]. None of the PB7 Resilient-to-Impersonation sub-benefits are offered (see evaluation of gait).

4.4.2.6 Heartbeat

The capture of electrocardiogram (ECG) in [24] for whatever purpose assumes trusted wearables or devices in or close to the patient (user) and the external entity (service) receiving the ECG data can be assumed to be trusted, but can be partially trusted or fully untrusted. Thus, especially in the latter two cases the access must be restricted to only authorized persons. As for other covert trait-based biometrics, biometric data cannot be captured as a by-product.

PB1 No-Trusted-Third-Party is offered, because no TTP is involved. PB2 Requiring-Explicit-Consent is offered because the wearables and other devices capturing the ECG data require user consent to place them, so that the ECG data cannot be captured as a by-product. As for the previous evaluated behavioural biometrics, PB3 and PB4 are also not offered, because the service or application provider could infer private information beyond that required for authentication revealing sensitive attributes and identify the user in another scenario based on biometric data [24]. The security benefits S1, S2, S5 and S7 are offered, so that for heartbeat biometric the PB 7 Resilient-to-Impersonation sub-benefits observation and phishing are offered. The following evaluation of S1 - S8 for PB7 is also applicable to biometric *brain activity*. We rate the *heartbeat biometric* offering S1 Resilient-to-Physical-Observation because wearables and other devices capturing the ECG data require user consent to be placed, and thus it is not possible to capture biometric data as a by-product. S2 Resilient-to-Targeted-Impersonation is also rated as offered because no capture as a by-product is possible. S3 Resilient-to-Throttled-Guessing and S4 Resilient-to-Unthrottled-Guessing are rated as not offered, because an external attacker with access to a biometric template, e.g. from a leak, can infer private information. **S5** Resilient-to-Internal-Observation is offered assuming secure software and hardware development for the biometric device (see definition of S5 in PB7). We rate **S6** Resilient-to-Leaks-from-Other-Verifiers as not offered because biometric templates of an authentication system – if leaked – could be used to infer private information. **S7** Resilient-to-Phishing is rated as offered because no capture as a by-product is possible. At this point, we disregard e.g. the possibility of an attacker trying to outwit the user with a malicious wearable or other device, and thus using software and hardware developed secure (see definition of S5 in PB7). S8 Resilient-to-Theft is rated as not offered because an attacker who steals biometric data – e.g. a biometric template – can use it to infer private information.

4.4.2.7 Brain Activity

The most prominent application of electroencephalography (EEG) is authentication, personalized game experiences for users and brain-controlled interfaces [24]. As with other covert trait-based biometric, data cannot be captured as a by-product.

PB1 No-Trusted-Third-Party is offered, because no TTP is involved. PB2 Requiring-Explicit-Consent is offered because user consent to place the EEG capturing devices on the user scalp is required. Additionally, we point out that PB3 and PB4 are also not offered because the service or application provider could infer private information beyond that required for authentication revealing sensitive attributes and identify the user in another scenario based on biometric data [24]. The security benefits S1, S2, S5 and S7 are offered, so that for brain activity the PB 7 Resilient-to-Impersonation sub-benefits observation and phishing are offered. The detailed evaluation of S1 - S8 for PB7 is the same as for *heartbeat*.

4.5 Discussion

The evaluation conducted for authentication schemes based on the UDS framework criteria and the evaluation with the extension to UDSP framework based on PB1 – PB7 is now expounded. First, we present the UDS and UDSP based evaluation of all schemes in section 4.5.1. Next, in section 4.5.2 the privacy benefit criteria of UDSP are parsed for the authentication schemes to correlate the threats and privacy benefits. Finally, section 4.5.3 concludes with a consideration of implementation approaches for the mitigation of fundamental threats.

4.5.1 UDS and UDSP based evaluation of all authentication schemes

Table 10 includes an overview of the evaluation of *PB1* - *PB4* for the authentication schemes from [20]. The evaluation where indicated is twofold for PB1 - PB4, one based on UDS [20] and the other on the complete UDSP PB criteria that we assembled, indicated at the top of Table 10 with *Bonneau* or UDSP[12]. The rating of *PB1* and *PB2* for authentication schemes from the UDS framework [20] is confirmed by us. The *PB3* rating by UDS framework [20] where offered is not confirmed by us, because based on further UDSP criteria our rating is not offered. In case *PB3* is considered as not offered by [20], we confirm or even further reaffirm with UDSP. Due to the relevance of PB3 for *PB4*, if applying the criteria of *PB3* in [20], the rating for *PB4* is the same as for *PB3*. Our ratings with UDSP for all schemes from [20] are then also not offered for *PB4*. *PB5* and *PB6* are mandatory preconditions for every authentication scheme from [20] including biometrics from Hanisch [24] to fulfil legal standards and thus a service or application provider to be allowed to go live, whereby both are marked with *M* (mandatory). The *PB7* evaluation overview in Table 10 based on the extended S1 - S8 from [20] depicts the resilience of the authentication schemes against related security threats, and thus which sub-benefits of *PB7* are offered to avoid impersonation, namely the extreme of identifiability. The details of PB7 evaluation from Table 10 are also discussed in section 4.5.2 with the parsing of privacy benefit criteria.

The schemes GrIDsure and YubiKey [20] are rated based on UDS as equal for PB1 - PB4 as web password, except YubiKey for PB1, but only YubiKey is rated better and best for PB7. Fingerprint only offers PB1 and PB2. Web password as GrIDsure only offers the PB7 sub-benefit loss of possession, while fingerprint do not offer any of the PB7 sub-benefits and YubiKey offers all PB7 sub-benefits.

The sample evaluation of web password, GrIDsure, Yubikey and fingerprint in section 4.4 with the results presented in Table 10 even with PB3 and PB4 limited to the criteria in [20] shows that web password is the worst rated scheme for PB7 based on security benefits S1 - S8.

Nevertheless, the web password is still the most commonly used authentication scheme, whereby the only reason can be that it offers all deployability benefits and most of the usability benefits in [20], including being easy-to-learn and easy-recovery-from-loss, as well as offering low-cost and in general user-friendly usage. At this point, we want to emphasize and admit that our choice for GrIDsure in section 4.4 – despite not being the best rated in security benefits [20] – is grounded to be the best rated for usability of the cognitive category schemes without being the best for security. This is in line with the existing trade-off between usability, deployability and security benefits, which results in the predominance of web passwords despite being rated worst for security.

All authentication schemes including biometrics in [20] are rated as not offering PB3 and PB4 based on UDS [20] criteria, which we reaffirm with our additional privacy UDSP criteria for PB3 and PB4. Thus, they do not offer any of the PB7 sub-benefits. Privacy consideration based on the UDS criteria in [20] remains limited for authentication schemes, as can be seen especially for PB3 and PB4 in Table 10.

4.5.2 Parsing privacy benefit criteria of UDSP for all authentication schemes

PB1 - PB7 (UDSP) defined in section 4.3 include additional privacy-related criteria and/or alteration of criteria from [20] or depreciated criteria in [20] or newly added criteria, as undertaken e.g. for PB3 and PB4 with [16, 24, 80] and PB7 with [24] applicable to the underlying security benefit definitions S1 - S8 from [20] in section 4.3. Furthermore, we replenished the biometric category with behavioural biometrics from [24], which are voice, gait, hand motions, eye-gaze, heartbeat and brain activity to foster to realize the expectations coming up with this promising behavioural biometrics. Now we bring out the reasons for not offered privacy benefits throughout the evaluation with UDSP of authentication schemes, so we parse them and finish considering specific aspects of biometrics.

4.5.2.1 *UDSP privacy benefit criteria focused on authentication schemes from UDS framework*

The rating with UDS PB1 and PB2 criteria for authentication schemes from UDS [20] remain as in section 4.4, because with UDSP only ML-related criteria were added to PB2 and for none in UDS [20] ML is explicitly assumed.

The rating related with PB3 and PB4 including all criteria is not offered, regardless of whether they are initially rated as offered. We want to stress here that for PB4 – introduced by us – we gave an initial rating based on the rating of UDS framework [20] based on PB3 criteria in [20] because the criteria are closely related with PB4 and thus applicable.

The UDSP evaluation of legacy password, YubiKey, GrIDsure and fingerprint authentication schemes from UDS [20] in section 4.4 for PB3 and PB4 share being rated as not offered. For PB3, they share the reasons for this rating, namely that beside the usage of untrusted IP communication are threats arising from non-user-controlled cookies, destructive browser fingerprinting, or the same user ID used at different services. YubiKey additionally has the threat caused by token reuse, which is similar to using the same user ID at different services.

Related to PB4, they further share that the authenticator could be related to the user and/or identity and e.g. real name mail addresses are used instead of pseudonyms. Analogue to the authenticator argumentation (e.g. to use salt passwords) in UDS [20], the threat exists to relate a user based on a used biometric template (see e.g. fingerprint). The Yubikey – as the whole HW Token category – additionally requires secure software and hardware development [25] to avoid threats, and if not considered vulnerabilities could be used to compromise the user privacy. The secure software and hardware development is assumed to be fulfilled, as can be seen in the definition of S5 for PB7.

The UDSP criteria added to the security benefits 1 – 8 from [20] for PB7 are only relevant for machine learning-based behavioural biometric, and thus no alteration of the consideration of PB7 is undertaken above in section 4.5.1 for authentication schemes from UDS [20].

Not offered privacy benefits by authentication schemes from UDS framework [20] for UDSP framework reveal threats for privacy benefits:

Threats for PB3:

- Usage of untrusted IP communication
- Non-user-controlled cookies
- Application of destructive browser fingerprinting
- Insufficient pseudonymization

- Reuse of same user ID or HW token at different services

Threats for PB4:

- Secure software and hardware development (we assume here fulfilled, see S5 in PB7)
- Compromise biometric template and/or identify them across services

The sub-benefits of PB7 can be considered for all authentication schemes in [20]. The authentication schemes either offer all PB7 sub-benefits such as YubiKey or up to only the PB7 sub-benefit loss of possession such as GrIDsure and web passwords, all being a representative cross-section for their category of the authentication schemes in Table 10. Biometrics from UDS [20] do not offer any PB7 sub-benefits. Independent of whether the PB7 sub-benefits are offered by the authentication schemes, it is indispensable to mitigate the threats related with PB3 and PB4. Additionally, the not-offered PB7 sub-benefits assembled in Table 10 indicate that threats apparently related with security benefits impact on privacy, which must be mitigated. Nonetheless, for authentication schemes regardless of whether they include biometrics, an accompanying security assessment is recommended to mitigate the threats related with S1 – S8.

4.5.2.2 UDSP privacy benefit criteria focused on behavioural biometric

Now we proceed with the behavioural biometrics [24] evaluated in section 4.4 with PB1 - PB7 (UDSP). As for the authentication schemes in UDS [20] in section 4.5.1, the PB5 and PB6 are also mandatory for authentication schemes based on behavioural biometric and a perquisite for the service or application provider to be allowed to go live. The evaluation results for PB1 - PB4 are shown in Table 10.

PB1 is offered by all behavioural biometric in the authentication scenario. PB2 is only offered by the covert trait of biometric heartbeat and brain activity for the data-publishing scenario. The overt trait behavioural biometric voice, gait, hand motions and eye-gaze are susceptible to be captured as a by-product, and thus rated as not offered.

All behavioural biometrics are rated for PB3 and PB4 as not offered because due to the applied ML technology biometric data can be exploited for identity and attribute disclosure by anyone and everyone in possession of biometric data. This attack can be performed by external attacker with a data capture as a by-product and by the service or application provider (verifier), which must have access to biometric data for authentication purpose in the context of a data-publishing scenario, in the latter assuming that the provider or application provider are malicious, thus an internal attacker [24].

The behavioural biometrics once again can be distinguished depending on whether they are based on covert or overt trait. None of the overt trait behavioural biometrics offer any of the sub-benefits

of PB7, contrary to that the covert trait heartbeat and brain activity biometric offer for PB7 Resilient-to-Impersonation the sub-benefits observation and phishing. The PB7 sub-benefit observation and phishing – not relevant for the data-publishing scenario – are offered for covert trait-based behavioural biometrics because capturing biometric data as a by-product is not possible and we assume for S5 secure software and hardware development. The PB7 sub-benefits guessing, verifier leakage and loss of possession are relevant for the data-publishing scenario and rated as not offered, as shown in Table 10. Not-offered privacy benefits for UDSP in Table 10 reveal the underlying threat for data-publishing scenario, leaked or stolen biometric templates and biometric data captured as a by-product:

Threat for PB2, PB3, PB4 and PB7:

- Identity and attribute disclosure with machine learning inference techniques

Regardless of whether overt or covert based biometric data is passed by the user as in the data-publishing scenario, through a leaked or stolen (from a verifier or user) biometric template or captured as a by-product by whomsoever, an attacker can try to infer personal information, thus compromising the privacy goal identity protection and attribute protection. In the context of authentication, overt traits are susceptible to impersonation attacks based on inferred personal information, especially captured as a by-product. Therefore, we point out that these aspects raise the following questions:

A. Are overt biometric traits usable as the only authentication factor?
B. Are covert biometric traits usable as the only authentication factor?
C. How can impersonation (authentication) based on overt trait data captured as a by-product be avoided?
D. How can biometric data – regardless of whether from a covert or overt trait – be protected against inference of personal information?

Question D) is in the scope of the anonymization methods that aim for protecting biometric data in the data-publishing scenario [24], which we consider in the context of the implementation approaches in section 4.5.4, while questions A) to C) remain for future research.

4.5.2.3 Specific biometric privacy benefits and aspects

The nature of both the physiological and behavioural biometrics can be categorised into overt and covert trait-based. Once a biometric data template for usage is captured with user consent, all biometrics – regardless of whether overt or covert – must be protected against different threats.

Well-known threats considered now are not originated in the data-publishing scenario, and are invertibility of the biometric data template, thus to reveal or link the user identity. Another threat is that stolen, leaked, or lost biometric data can cause the uselessness of the compromised

biometric data template, and thus the biometric user data cannot be used anymore. The last threat mentioned is if biometric data templates can be used across different services to link users. The resulting biometric privacy benefits to offer and still presented in section 4.2.2 are as follows and will be detailed in section 4.5.3:

- Non-invertibility (NI) [74, 79]
- Revocability (RV) [74, 79]
- Diversity (DV) [79]
- Unlinkability (UL) [74] (listed for completeness, but is still considered intrinsically in PB3)

Additionally, the mitigation of threats caused by lost, leaked, or stolen biometric data template can also be supported, applying e.g. a decentralized structure as proposed by FIDO Alliance (see section 4.2.2).

The aforementioned privacy benefits NI, RV, DV and UL are close related to the disclosure of a biometric data template, and thus we anticipate here for mitigation the decentralized structure to capture the biometric data (see FIDO Alliance) where the user resides and to use sealed storage for the captured biometric data in e.g. a secure element (SE) storage device. The SE offers access protection and is only usable after explicit user authenticated consent.

The next section 4.5.3 lists revealed threats and section 4.5.4 presents the corresponding implementation approaches for authentication schemes including biometrics from UDS [20] and anonymization methods (privacy-protecting) approaches from [24], with the latter focused on the data-publishing scenario assumed for behavioural biometrics in [24].

4.5.3 Privacy threats of parsed privacy benefits

The parsed privacy benefits in section 4.5.2 reveal related privacy threats that are categorizable into primarily *affecting as a whole authentication schemes*, affecting the included *biometrics* and *security originated privacy threats affecting authentication schemes and included biometrics*.

I.-1 Privacy threats affecting as a whole authentication schemes:

- Usage of untrusted IP communication
- Non-user-controlled cookies
- Application of destructive browser fingerprinting
- Insufficient pseudonymization
- Reuse of same user ID or HW token at different services
- Insecure software and hardware development

- Compromise and/or identify biometric template across services

II.-1 Privacy threats affecting included biometrics:

- Identity and attribute disclosure by means of machine learning inference techniques
- Invertibility of biometric data templates
- Uselessness of compromised original biometric data
- Cross linkable biometric data
- Caused by lost, leaked, or stolen biometric data

III.-1 Security originated privacy threats affecting authentication schemes and included biometrics:

- Non-fulfilled security benefits S1 – S8
    - Identity and attribute disclosure by means of machine learning inference techniques

4.5.4 Implementation approaches for mitigation

Reviewing the privacy threats, a comprehensive mitigation of fundamental threats can be achieved based on implementation approaches and applying privacy-protection techniques [24] not only applicable to behavioural biometrics. An accompanying extensive security assessment to mitigate further security threats related with S1 - S8 and still not detected threats is reasonable.

I.-2 Implementation approaches contribute to mitigate the threats in I.: Privacy threats affecting as a whole authentication schemes

Usage of trusted IP communication: The application of technical recommendations for encryption and TLS by the *Federal Office for Information Security in Germany* [88, 89] is recommendable and applicable for design and default settings elicitation.

User-controlled cookies: Including default settings to be provided by the service or application provider [88, 89] offering privacy settings by default.

Protection against destructive fingerprinting: Browser fingerprinting comprises collecting throughout the web browser [3] user information spanning from hardware, operating system to application and software, including configuration details. Thus, the user is tracked and could be attacked by terms of detected vulnerabilities. Defence techniques [3] to avoid destructive fingerprinting at a high level intend to increase the device diversity (alter the fingerprint) or present a homogeneous fingerprint (e.g. using a Tor Browser) or decrease the surface of a browser API, hence reducing the information collectable through the browser API.

Pseudonymization: Allowing the user e.g. to freely select an user identifier [45], thus not being forced to use a real name or other personal user information.

Avoid reuse of same user ID or HW token at different services: One approach is that given for pseudonymization. Another approach is to facilitate the user especially in federated single sign on (SSO) environment the application of a *pairwise pseudonymous identifier (PPID)* (e.g. see OpenID specs [90], NIST [45]) per service, resulting in an *Unlinkable* user identifier in federated environments. In case of usage of biometric data with a hardware token, the linkability of biometric data can be avoided based on offering diversity for biometric data (see below for details). Thus, the threat *compromise and/or identify biometric template across services* is also mitigated.

Avoid insecure software and hardware development: Required in [25] for all components regardless of whether belonging to authentication schemes, included device (hardware) for biometric data, or client personal computer or notebook.

II.-2 Implementation approaches (and privacy-protection techniques) contribute to mitigate the threats in II.: Privacy threats affecting included biometrics

Avoid inference of identity and attributes with machine learning techniques: The authors in [24] present after a survey privacy-protection techniques (methods) for behavioural biometric evaluated in section 4.4.2. The anonymization methods (privacy-protection techniques) [24] are *continuous conversion*, *discrete conversion*, *feature removal*, *coarsening*, *noise injection* and *random perturbation*. The data-publishing scenario [24] aims to protect behavioural biometric data published, leaked or stolen against inference of private information usable for identity and attribute disclosure. Consequently, the privacy goals of the privacy-protection techniques [24] are identity and attribute protection, which – as still mentioned – are in accordance with PB3 and PB4.

In [73] the extended version 2 of [24] the authors sum up their survey with an overview in two tables. One table provides *an overview of all found methods classified by trait and method*, while a second table offers *an overview over which privacy goals the different techniques try to achieve*. The most anonymization methods were found for voice and EEG (heartbeat) [24]. Furthermore, for that traits continuous conversion is the most commonly considered followed by noise injection and feature removal [24]. All traits can be used for both identity and attribute inference [24]. Of interest in this context is the fact that these three most commonly considered anonymization methods (continuous conversion, noise injection and feature removal) have the highest simultaneous applicability for both, identity and attribute inference at the same trait.

Summarized, the privacy goals can be described as follows. The identity protection comprises transformation of behavioural biometric data so that a person cannot be linked to the data. This includes pseudonymization and anonymization in relation to the identity [73]. The attribute protection comprises transformation of behavioural biometric data to protect specific private attributes, up to template protection, which is then still usable for authentication [24, 73]. All traits can be used for identity and attribute inference, and thus to link user to data, identity theft or private attribute (e.g. gender, age, sex, etc.) inference.

The fulfilment of these privacy goals [24] in a mitigation strategy including one or more of the anonymization methods for authentication schemes including biometrics would contribute to offer PB3, PB4 and PB7, thus avoiding or significantly reducing linkability, identifiability and impersonation.

Almost all of the following implementation approaches – e.g. for non-invertibility, revocability and diversity – are mentioned in the survey [24] as criteria to be necessary or implicitly given in the context of the anonymization methods, so that they are addressed here explicitly if not done in the context of the anonymization methods thus underlying the indispensability for all kind of biometrics.

Achieve non-invertibility (NI) comprises intentional alteration of biometric data to generate biometric templates so that this transformation is irreversible [74, 79].

Achieve revocability (RV) of biometric data template for the case it is compromised, so that the original biometric does not become useless. The underlying cryptographic primitives belong to biometric privacy [78] comprising biometric encryption and cancellable biometrics and are related with untraceable biometrics [91].

Achieve diversity (DV) of biometric data templates, so that with different services and application provider the cancellable biometrics used are different, thus avoiding cross template attacks. The cryptographic primitives are from [78, 91] (see *achieve revocability)*.

Avoid disclosure (DeC[10]***)*** of biometric data and biometric templates. Contrary to the assumed data-publishing scenario, in case of not intended data-publishing the disclosure of biometric template can be avoided using a decentralized secure element, e.g. see FIDO Alliance[10].

The contribution of the biometric privacy [78] methods to each privacy benefit is shown in Table 11.

	PB1	PB2	PB3	PB4	PB5	PB6	PB7
DeC[10]	X						X
NI			X	X			X
RV				X	X		X
DV			X	X			

Table 11: Implementation approaches improving privacy benefits.

III.-2 Implementation approaches contribute to mitigate the threats in III.: Security originated privacy threats affecting authentication schemes and included biometric

Fulfilment of known security benefits S1 – S8 and further elicited security benefits can be achieved with an extensive accompanying security analysis for authentication schemes and biometrics, e.g. based on STRIDE [15], which should include the security aspects of S1 - S8 and elicit upcoming or not-considered particular use case relevant security threats negatively affecting privacy.

Avoid inference of identity and attributes with machine learning techniques: the mentioned privacy-protection techniques [24] above in II.-2 are applicable for threats related with PB7 (including S1 - S8) grounded on ML.

4.6 Concluding remarks and prospect of a future user authentication scheme

At a glance, the evaluation results in Table 10 with UDSP for PB3 unlinkabilty and PB4 Resilient-to-Identifiability obviously bring out that none of the authentication schemes from UDS [20] and included behavioural biometric [24] offer out-of-the-box PB3 and PB4. One outcome of the evaluation of authentication schemes from UDS [20] and included behavioural biometric [24] is that privacy still is not considered sufficiently comprehensively.

For the web password scheme, besides being the worst rated for security with the UDS framework by Bonneau et al. [20], our present evaluation with UDSP additionally reveals that it belong to the worst rated for privacy (see Table 10). Contrary to this nearly all hardware tokens and most of the phone-based schemes are the best rated with UDSP for privacy (Table 10) and security in [20].

The promising behavioural biometrics from [24] extend the basis of usable traits for authentication purposes whether to complement existing authentication schemes with a further factor or to be the unique reliable factor, in both cases with the potential to increase the user

usability experience. The use of the strong emerging ML with behavioural biometrics is an advantage with respect to the expected reliability of the user authentication, and it is also applicable to compromise the privacy of the behavioural biometric.

Hanisch et al. [24, 73] present upcoming anonymization methods to protect the privacy goals identity protection and attribute protection for ML-based behavioural biometrics. The most promising anonymization methods still in process of research are continuous conversion, noise injection and feature removal, and they are applicable to all behavioural biometrics [24, 73].

The protection of the behavioural biometric with the anonymization methods comprises protecting in the data-publishing scenario data voluntary published to a service as well as any involuntary leaked biometric template against inference of private information, regardless of whether they are based on overt or covert traits.

The anonymization methods presented by Hanisch et al. [24, 73] still require future research to be applicable for privacy safeguarding the authentication in the data-publishing scenario.

One remaining gap that requires future research is the unavoidable capture of overt traits as a by-product, which raises the issue of how to avoid the usage of this biometric data for impersonation by an attacker in an authentication process, and being able to use overt traits as a unique single factor in an authentication process, which in fact seems to be more feasible with covert traits.

Finally, based on our results we sketch the roadmap towards a conceivable multi-factor authentication scheme, focusing on becoming a single-factor authentication scheme based on behavioural biometrics. *First***,** we combine a behavioural biometric with the password scheme or a possession-based authentication factor applying established cryptographic technologies (see section 4.2.2) avoiding publishing biometric data. Anonymization methods [24] are applied to the behavioural biometric, regardless of not being published. *Second*, we apply data-publishing for behavioural biometric, maintaining the second factor for two reasons. The first reason to maintain the second factor is to maintain the required security level until the anonymization methods are sufficiently reliable to protect the privacy goals of biometric templates in the data publishing scenario against inference of private information. The second reason is to protect behavioural biometric-based authentication if based on overt trait against the threat based on data capture as a by-product, an issue not arising for covert traits. *Third* – at this moment not really tangible – is to only use a behavioural biometric in a data-publishing scenario as the only factor and in the best case offering continuous authentication.

Chapter 5

5 Revocable Privacy – Enhanced user privacy requirements for user-driven self-determination

5.1 Introduction

In Chapter 3 and Chapter 4 of the dissertation, we investigated the privacy threat analysis of the user verification process in the modelling phase and for realized authentication schemes. The smart community service requirements demands stringent unconditional evidence and trustworthiness for the user contribution, which conflicts with the legitimate user right to self-determined maintain his privacy, whereby we thus now investigate this conflict.

Occurrences can be classified into non-critical incidents (NCI) or critical incidents (CI), for which the smart community service (SCS) demands all available information about the incident and the contributing user. This brings up the conflicting interests between the understandable stringent smart community service requirements and the central user right of self-determination stated in REGULATION (EU) 2016/679 [25] to maintain his privacy. The user rights as stated by ENISA [92] lack technical enforceability. Furthermore, beside the stated right of self-determination there are stated others or inferred from [25] that comprise but are not limited to the right to be asked for consent (RTC), the right to have privacy (RTHP), and the right to be forgotten (RTBF).

Our objective is primarily to strengthen the self-determination, thus the associated right to be asked for consent (RTC) and right to have privacy (RTHP). Our results are partially applicable to the right to be forgotten (RTBF) of a user contributing to a smart community service, but RTBF is not in the scope of the present dissertation.

The aim is to empower the user to execute in connection with the contribution his right of self-determination in accordance with the rights RTC and RTHP. The user must be able to enforce (*enforceable*) privacy comprising his desired gradation (*graded)* and accepted detail of revocation

(*revocable)*, whereby the latter is a user accepted concession to the SCS in case the user perpetrates a misuse.

The present chapter focuses on the consideration of the user self-determination, so he knows and can decide to accept the conditions for which the user privacy could be revoked when contributing to a smart community service, and being informed of possible consequences in case of misuse. In the context of smart community services, these often require participatory voluntary user contributions for critical incidents, e.g. to emergency management services (e.g. 112 and 911), responsible e.g. for traffic jams, traffic accident, house fires, natural disasters, etc., as well as for non-critical incidents, so that the smart community service can initiate earlier and more effective countermeasures.

The arising challenge for the smart community service is twofold. On the one hand, the user must be convinced to contribute to an incident in a privacy-preserving manner information. On the other hand, the smart community service must be able to unequivocally discern a user in case the user perpetrates a misuse when reporting information for an incident. This SCS requirements and the legal user right of self-determination [25] bring up the mentioned conflict. Therefore, in the context of a user contributing to a smart community service, we define a taxonomy concept for revocable privacy.

This *taxonomy* concept provides a classification and action system, so that the user can identify if an occurrence is an incident, classify the related criticality of the incident, he is informed about the required trustworthiness for the incident and the associated gradation of revocable privacy in case he perpetrates a misuse. Thus, the user is enabled to contribute to an incident by means of reported information and at the same time maintains his privacy as long as the user did not misbehave. The user is transparently informed about the associated possibility of revocable privacy, so he can freely accept revocable privacy in case of misuse or reject. In the latter case, it depends on the smart community service whether there are incidents for which he wants a user contribution without user-accepted revocable privacy. The presented approach of revocable privacy can convince honest users to contribute to smart community service accepting revocable privacy and ensure that the user privacy is technically enforced and maintained if the user behaves honestly.

More specifically, the contributions of this chapter comprise the following aspects:

I. Assort as a starting point the stringent SCS requirements for contributing users
II. Definition of revocable privacy taxonomy concept grounded on the user right of self-determination
III. Application of revocable privacy taxonomy concept to stringent SCS requirements
IV. Proofs-of-concepts for revocable privacy

The remainder of the chapter is organized as follows. In section 5.2, the background for revocable privacy is presented. Section 5.3 gathers the stringent smart community service requirements and section 5.4 presents the basis for a revocable privacy taxonomy concept based on the user right of self-determination. Section 5.5 shows the application of revocable privacy for stringent SCS requirements. A proof-of-concept for the application of revocable privacy for user contributions to SCS is given in section 5.6, including examples of applicable cryptographic primitives. The chapter concludes with a discussion and conclusion in section 5.7.

5.2 Background

The concept of revocable privacy presented by authors Galindo et al. [93] is defined as "a *system implements revocable privacy if the architecture of the system guarantees that personal data are revealed only if a predefined rule has been violated.*" The details of the user are revealed automatically if a rule is violated without any user-side possibility to interact.

Lueks et al. [94] extend this definition as follows: "*A system implements revocable privacy if the architecture of the system guarantees a predefined level of anonymity for a participant as long as she does not violate a predefined rule*." The authors introduce a predefined level of anonymity depending on the defined rules, but do not demand that the user knows the defined rules. Contrary to this, our taxonomy concept for revocable privacy is fully transparent to the user about when and under what circumstances revocable privacy is applied. Once applied, these decision rules comprise exemplary applicable cryptographic primitives such as blacklistable anonymous credentials (BLACR) and group signatures with distributed management (GSDM). An applicable BLACR approach is presented in [95]. In Chaums [96], the basics of group signatures are presented and in [97] how several parties together can reveal the identity of a group signer in case of misuse. In section 5.6, the cryptographic primitives BLACR as well as GSDM are considered for the proofs-of-concepts, so that a misbehaving user can be blocked anonymously based on the application of BLACR and if required the identity with that the user signed a contribution based on GSDM could be revealed. Depending on the severity of the misuse, this enables smart community services to anonymously block and if required reveal the user identity to prosecute him.

Anonymous credentials are not linkable and neither the verifier nor the issuer can relate it with the user that used it [98, 99], and thus the user is unlinkable throughout different sessions at the same service. Predestined are e.g. subscription services or other similar services, but it is conceivable that services requiring knowing the real user identity can alternatively offer for certain sub-services the possibility to use anonymous authentication with anonymous credentials. The applied anonymous credential method [98] allows the user to determine the conditions under which the anonymity could be revoked or *choose unconditional anonymity* [98], therefore self-determined. In [100] as in [98] the user once registered at a smart community service in step 1 with a real known user identity and obtained anonymous credentials in step 2, comes back with them to anonymously authenticate towards the same smart community service in step 3. The SCS would only know the real identity of the user in case the user misbehave according to the conditions accepted by him.

5.3 Smart Community Service stringent requirements

The present section defines the use case and stringent smart community service requirements for a user who contributes in a participatory manner to the smart community service. The user contribution is considered initially from the perspective of the smart community service requirements, which need users to report detected incidents and replenish as much as possible information. The contribution to the SCS can be for a critical or non-critical incident. The smart community service demands a contribution with evidence for the incident and trustworthiness for the user. The legitimate interest of a smart community service motivates him to demand regarding the user trustworthiness and contributed evidence to decide who contributes and have all available user related information, thus to have always (and permanent) unrestricted access to the user identity. Based on this comprehensible smart community service demand, we proceed with further definitions and assumptions related with the demanded user contribution. The user contribution to the SCS can be for critical as well as non-critical incidents.

The definitions of critical incident and non-critical incident are as follows.

Critical incident (CI) are given when any error or defective function can entail strong negative consequences such as reputation lost, significant reputation lost, financial loss and/or human safety endangering. Non-critical incidents (NCI) are all other incidents not classified as critical incidents. The classification of incident types into CI and NCI by the smart community service could have more than these two levels, and can therefore be more scaled or specific, and can be in the scope of future work to apply our presented *revocable privacy taxonomy* concept to more scaled or detailed incident types.

Incident types:

- Critical incident (CI)
- Non-critical incident (NCI)

Evidence and trustworthiness: smart community service requirements for the user contribution

The smart community service has two central requirements towards the user contribution. The first requirement is to obtain reliable evidence (E) that proves an incident. The second requirement is to obtain a trustworthiness (T) proof of the contributing user to substantiate the evidence and associated incident. Therefore, the user contribution (UC) is composed of an evidence proof and a trustworthiness proof, thus defined as the user contribution [E, T] = UC [E, T].

User contribution :

- User contribution [E, T] = UC [E, T]

The user contribution participatory provided on a per incident basis by the user in the best case is composed of two parts, namely evidence of the incident and a trustworthiness of the user. Thus, we define:

Evidence (E) proof:

The evidence proof can be e.g. an uploaded photo, video, voice message, or whatever available evidence for the incident. Another kind of evidence proof – but not in the scope of the present considerations – could be the information of the user's device sensors that he participatorily passes on per incident basis to the smart community service, e.g. location, temperature, altitude, detected gas, combined with surrounding area sensors in the range of the SCS. The evidence (E) can be replenished with a comment (C) to reaffirm an evidence proof or provide a first incident notification, thus being a written and/or a voice message. The further explanations will consider evidence (E) without mention explicitly the comment.

Trustworthiness (T) proof:

Trustworthiness refer to the reliability of the evidence provided by the user, so that for the contribution the **smart community service** has as much as possible information about the user who contributes. The trustworthiness can be provided by the user e.g. by proving the legitimate usage of a trusted user identity (TUID).

A TUID is an identity in which the smart community service trusts. We now provide a brief – but not exclusive – overview of the different origins that a trusted user identity (TUID) can have. The TUID used could be e.g. a social network ID (SNID) or an electronic ID (eID) from a government or company, brought along by the user, or a smart community service (SCS) user id (UID) issued by the SCS itself, thus being an SCSUID. The trustworthiness could be replenished considering e.g. user devices and/or dedicated installed SCS applications, which are not in the scope of the

present thesis. In this context, we stress that for our presented taxonym concept it does not matter whether the user contribution is done by a dedicated application installed on a user device or browser based. A representative overview of applicable trustworthy user identities (TUIDs) to provide trustworthiness is given in Table 12.

Trustworthy user IDs	TUID
Social network ID	SNID
Electronic ID	eID
Smart community service ID	SCSUID
Other identities	…

Table 12: Representative overview of applicable trustworthy user identities (TUIDs).

The user can perpetrate a misuse with the contribution to the SCS, and thus the basic underlying misuse cases considered are as follows.

Definition of basic misuse cases for user contributions:

The SCS is interested in knowing whether a user perpetrates a misuse case by means of reporting a non-existing incident or contributing false information to an existing incident.

- A.) Report a non-existing incident, hence a false report
- B.) Report false information (not true details) for an existing incident.

The SCS requirements described thus far are now compiled in an overview table:

SCS requirements	
Incident types	Critical incident (CI)
	Non-critical incident (NCI)
User contribution	Evidence (E)
	Trustworthiness (T)
Trustworthy user identity	Social network identity (SNID)
	Electronic identity (eID)
	Smart community service user identity (SCSUID)
Misuse cases	Reported not existing incident (RNI)
	False information to existing incident (FII)

Table 13: SCS requirements in the context of user contribution to SCS related incidents.

Generic process flow of a user contribution to a smart community service

The SCS requirements embedded in a process flow that describes the actions starting with the classification of an incident by the user, followed by the user contribution to the SCS, the

evaluation of the UC by the SCS and ending – if happened – with the misuse detection are detailed in Figure 12.

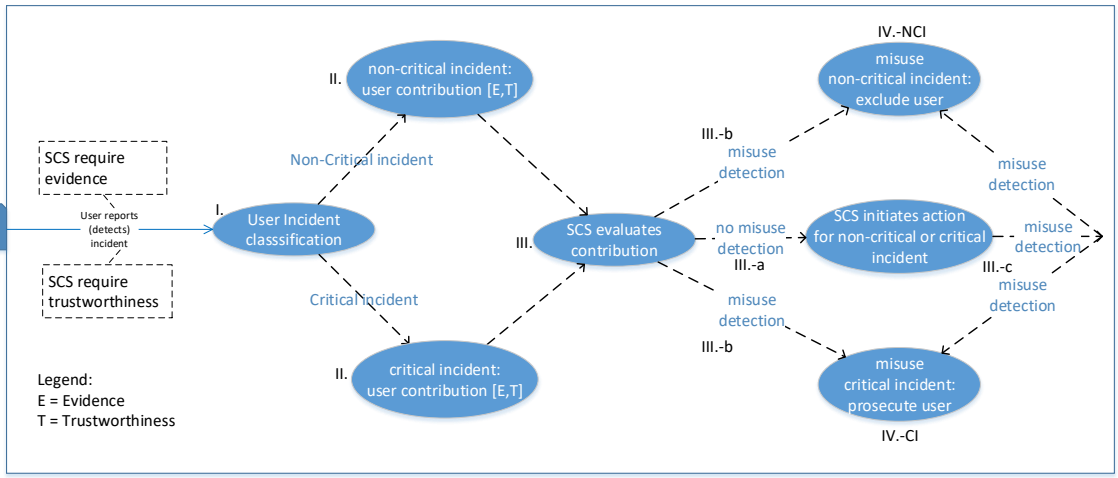


Figure 12: Generic process flow of a user contribution to a smart community service.

After phase I. and II., having received the user contribution, the smart community service evaluates in phase III. the UC [E, T], and acts as depicted in Figure 12:

- III.-a) no misuse detection –> the SCS will initiate normal action in accordance with the reported incident type
- III.-b) misuse detection –> SCS acts in phase V. according to the criticality of the incident, e.g.
    - IV.-NCI) exclude (block) the user, thus the user cannot contribute anymore
      or
    - IV.-CI) the SCS can exclude (block) the user and additionally prosecute the user after user identity disclosure
- III.-c) in case of detecting the misuse after initiation (rollout) the action for the corresponding incident type, the SCS will afterwards exclude or prosecute the misbehaving user, thus see IV.-NCI or IV.-CI.

The described process flow represents the optimal roll out for the use case from the perspective of the smart community service, therefore providing as much as possible user-related information to the SCS without no user option to opt-out once he has contributed. The only option granted to the user is to decide to contribute or not to contribute to the smart community service with information to report an incident.

The smart community service demands for the user contribution to fulfil the stringent SCS requirements, and thus the user cannot execute his right of self-determination and cannot realise his right to preserve his privacy. We take up this arising conflict and propose a taxonomy concept

to facilitate the user a classification and action system to completely self-determined decide whether at all to contribute and what eventually necessary privacy limitations he is willing to assume.

User privacy threats immanent to SCS requirements

In Table 14, an overview of the stringent SCS requirements and upcoming privacy threats is provided. The mentioned stringent smart community service use case requirements described in section 5.3 threaten the user privacy and entail – depending on their details – different privacy threats. The stringent SCS requirements demand obtaining as much information as possible from the contributing user substantiated with the provided evidence and trustworthiness proofs, which leads to the privacy threats shown in Table 14.

	Privacy Threats	SCS requirements for user contributions
1.	Profiling	the possibility to recognize a user
2.	Identification	obligation to include a real user identity (UID)
3.	Non-repudiation	obligation to include a user identity (ID) to the contribution (and smart community service demands non-repudiation)
4.	No self-determination applicable by the user	user obligation to include an identity (ID)

Table 14: Stringent smart community service requirements and related privacy threats.

The privacy threats in Table 14 show that the user cannot execute fundamental legitimate rights stated or inferred from REGULATION (EU) 2016/679 [25] related with his right of self-determination that – beside others – comprises the right to be forgotten, rectification of data, object profiling, privacy and have constant explicit right to execute, rethink and rectify consent.

The user contribution usually must provide a reliable evidence and trustworthiness to the smart community service, thus arising the conflict between the smart community service requirements and the user right to have privacy, which we investigate accordingly. The aim is to facilitate the user to contribute in a self-determined manner, so that the user must not accept to waive his privacy and further associated rights. Therefore, we present a taxonomy concept for user-consented enforceable graded revocable privacy.

5.4 User's right of self-determination for enhanced revocable privacy

This section shows the basis for the realization of enhanced revocable privacy by means of user right of self-determination.

Origins of revocable privacy (RPr)

Revocable privacy mentioned by Galindo et al. [93] does not actively involve the user in the decision process whether (given) privacy should be revocable or not, and thus the user was not able to give his consent or rather to disagree with the application of revocable privacy. This definition implies that the user is neither informed about observation, nor about the fact that in case of misuse the given level of anonymity could be revoked. One prominent example in [93] is that of the detection of truck canvas cutters when they repeatedly enter highway parking spaces by car during a defined time period, so that then their numberplate is deanonymized.

Lueks et al. [94] extend the definition as follows: "*A system implements revocable privacy if the architecture of the system guarantees a predefined level of anonymity for a participant as long as she does not violate a predefined rule*." The authors comment that the user must not be informed about the rules that determine the predefined level of anonymity. We extend revocable privacy to become user-consented enforceable graded revocable privacy and in contrast to [94] the user can decide whether and to what extent he accepts and assumes revocable privacy.

Enhancement and further development of revocable privacy

We take up the definition [94] and concretise it for the use case of a contributing user to a smart community service, insofar that we concretise *participant* with user, *predefined level* with graded, and *does not violate a predefined rule* with user-consented (admitted) revocability (revocable) for the demanded privacy, here the desired anonymity or pseudonymity.

User-consented comprises the notion that the user accepts to make his contribution with revocable privacy in case of misuse. *Graded* comprises the possibility for the user to accept the range of the revocation. The revocation can include being recognised anonymously or pseudonymously as a returning user or can include being unequivocally identified by terms of one of his trustworthy user IDs (TUID), and thus revocable privacy is accepted. The execution of revocable privacy is undertaken in accordance with predefined rules and the identification by means of the TUID by authorized decision-makers.

Decision-makers about revocation:
Decision-makers – the so-called opener – can comprise a single party or several parties together, which can decide to reveal the identity of the user in case the SCS requests the disclosure related with a misuse. These stakeholders also stipulate the rules for automatic blocking and corresponding thresholds for blocking user without identity disclosure. A list of possibly involved stakeholders acting as openers to revoke user privacy by disclosing the user identity or stipulating automatic blocking rules is provided below:

I. User and smart community service together
II. Trusted third party that is involved
III. t parties of n participating parties
    - Participating parties can be the user, smart community service, governmental entity or trusted third party. A positive in passing effect is the possibility to avoid or detect a misbehaving smart community service.
IV. Automatic blocking of user, based on the rules stipulated by the openers (see III. above), without required active interaction of anyone after a threshold of infraction or misbehave is reached. However, the user must be informed and still give his consent when contributing to the smart community service.

The right of self-determination [25] in the context of the contributing user comprises stated or inferred rights, namely the right to be asked for consent (RTC), the right to have privacy (RTHP), and the right to be forgotten (RTBF), and are defined as follows:

Right to be asked for consent (RTC) comprises for the user for whatever action related with his contribution to the smart community service to have the right and capability to *authorize* (allow), *disallow* and *revoke given authorization*. In other words, RTC comprises the constant explicit right to execute, rethink and rectify a given consent [25].

Right to have privacy (RTHP) comprises for the user to having the possibility related with the contribution to decide which personal identifiable information the user discloses towards the smart community service. RTHP is an inferred right from REGULATION (EU) 2016/679 [25].

Right to be forgotten (RTBF) is the user's right to demand from the data controller (here the smart community service) the erasure of personal data [25].

The smart community service can guarantee the user rights RTC, RTHP and RTBF being compliant or providing the user with technical measures to ensure the realization of the user rights. Our scope is to present a taxonomy concept to empower the user to enforce revocable privacy in the context of RTC and RTHP. RTBF is beyond the scope of the present thesis.

Detailing of RTHP for enforcing, graded and revocable:

We consider for the user the ability to *enforce (Enforceable)* the execution of RTHP considering RTC and simultaneously demand the desired *gradation (Graded)* and accepted detail of *revocation* (*Revocable*). Regardless of the intermeshed nature, we offer individual initial definitions for *Enforceable*, *Graded* and *Revocable* as follows:

Enforceable is defined as the user capability to be able to ensure enforcement for his rights, irrespective of whether if it initially depends on the smart community service compliance or a technical implementation.

Graded is defined as the user capability to decide which of the possible shades he admits, independent of compliance or technical implementation guaranteeing the gradation.

Revocable is defined as the capability to have the possibility to revoke privacy. Revocation is then performed automatically user-consented to block user or upon explicit request, by the user and the smart community service, trusted third party or a group of these stakeholders to reveal the user identity.

We consider for the right to have privacy (RTHP) the possibility, that the user can enforce *(Enforceable)* privacy indicating his desired gradation *(Graded)* for the privacy and how far the user accepts revocability *(Revocable)* of his privacy. The right to be asked for consent (RTC) as defined in the present section is included corresponding to the requirements of RTHP. We call the resulting extension of right to have privacy including the right to be asked for consent:

- *User-consented enforceable graded revocable privacy*

In this context, we stress that the detailed consideration of the more far-reaching right to be forgotten (RTBF) is beyond our actual scope, but the contribution to the right to have privacy (RTHP) by means of enforceable and graded could be included thus far and tailored later for the RTBF after a detailed review of the corresponding requirements of article 17 in REGULATION (EU) 2016/679 [25] in conjunction with the SCS stringent requirements in section 5.3. Section 5.5 presents the application of the revocable privacy taxonomy concept to a user contribution to an SCS.

5.5 Application of Revocable Privacy to stringent SCS requirements for user contribution

The considerations in section 5.4 related with the user right of self-determination for revocable privacy (RPr) are applied to the user contribution considering the stringent SCS requirements from section 5.3, so we concretise the misuse cases and define related criticality levels for the incident types including the possible gradation.

A misuse case is given if a contribution is obviously malicious. Malicious is e.g. to report an incident such as a traffic accident whereas no accident actually happened. Another example can be reporting clearly incorrect information for an accident that actually happened. The following are in our opinion the two basic misuse categories: A.) reporting a non-existing incident, thus a false report or B.) reporting false information (not true details) for an existing incident, in both cases to the smart community service. The granularity of these two misuse categories are sufficient for our use case conceptualisation and the intended proofs-of-concepts. Later, for a more far-reaching realization in the future, the then-required granularity could be determined. Furthermore, additionally it is important to consider whether the misuse categories are affecting a non-critical or critical incident.

Examples of possible non-critical and critical incidents are:

- A concrete non-critical incident e.g. could be the contribution to traffic congestion that requires correct information, but if the contribution is in whatever form not appropriate or a false report, the consequences are manageable and usually with less impact on cost and/or reputation.
- A concrete critical incident e.g. could be the contribution to a traffic accident that requires correct information but in the case that the contribution is not appropriate, or it is a false report, the consequences are not so easily manageable because the impact can endanger human safety, being associated with high costs and/or reputation loss.

The *level of trustworthiness* required for the critical and non-critical incident will determine the necessary gradation for the *revocable privacy* action and e.g. are as follows:

- The non-critical incident e.g. (only) requires that the smart community service can anonymously or pseudonymously recognize a coming back user, without any possibility to reveal the user identity behind the pseudonym. The misbehaving returning user can be blocked.

- The critical incident e.g. requires that the smart community service can anonymously or pseudonymously recognize a returning user and unequivocally identify (discern) a user. The identification depends on the gravity of the underlying misuse and how far-reaching the consequences are, so that for a pseudonym the trustworthy user id (TUID) could be revealed.

For the sake of completeness, we point out, that the revocable privacy actions in Table 15 can be tied additionally to the circumstance if a countermeasure for the related incident still was initiated or not, so the SCS can additionally prioritise if he initiated a costly rollout in vain and thus consider this factor in the definition of the criticality levels. This can be part of future work to apply the revocable privacy taxonomy concept to a more detailed SCS use case for a user contribution.

For now, we continue presenting the resulting combinations in Table 15:

Misuse categories	Incident types			
	non-critical		critical	
	C level	Revocable Privacy action	C level	Revocable Privacy action
Report a non-existing incident (false report)	C1	Anonymous recognition + increment count for threshold before blocking	C3	Anonymous recognition + direct blocking (+ optional revealing TUID)
Report false information for existing incident	C2	Anonymous recognition + direct blocking	C4	Anonymous recognition + direct blocking + revealing TUID

Table 15: Misuse cases, criticality levels increasing from C1 to C4 and revocable privacy action for incident types.

The *misuse triggers* can alert before the smart community service initiated an incident related roll out of a countermeasure or after the smart community service initiated the roll out of a countermeasure (see Figure 12). The smart community service can detect a contribution, either being a false report or false information for an existing incident. Depending on the gravity, based on the applied criticality levels from Table 15, consented by the user, the contributing user can be recognized anonymously followed by the execution of previously user-consented actions up to be identified by means of the revelation of his TUID.

The criticality level increasing from C1 to C4 are defined as follows:

C1: User reports non-existing non-critical incident: A detected misuse led to tagging the anonymous user and blocking after n times of misuse.

- The smart community service can define together with other stakeholders, so that the user is blocked after n times of misuse for criticality level C1. Thus, to increase a counter towards a defined threshold after each detected misuse.

C2: User reports false information for existing non-critical incident: A detected misuse led to tagging the anonymous user and direct blocking of the user.

- The smart community service can include here to consider the number of misuses related with criticality level C1 or block the anonymous user directly as assumed in Table 15.

C3: User reports non-existing critical incident: A detected misuse led to tagging and blocking of the anonymous user and to optionally reveal the user identity (TUID).

- The smart community service can consequently block the user and optionally initiate to reveal the TUID of the user.

C4: User reports false information for existing critical incident: A detected misuse led to tagging and blocking of the anonymous user and in any case to reveal the user identity (TUID).

- The smart community service can consequently block the user and in any case initiate to reveal the TUID of the user.

The section concludes with the visualization of the taxonomy concept for revocable privacy in Figure 13 for a user contribution to a SCS for an incident based on the considerations thus far, consequently including the user right of self-determination, the stringent SCS requirements and Figure 12.

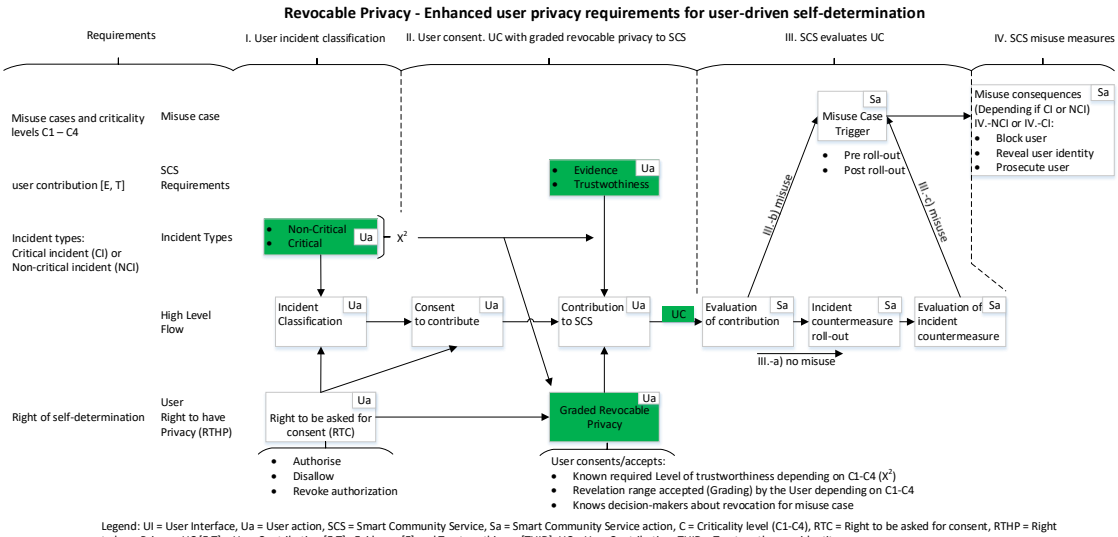


Figure 13: Taxonomy concept for revocable privacy in the context of a user contribution to a smart community service.

Next, we present two proofs-of-concepts including cryptographic primitives for the implementation of the taxonomy concept for user-consented enforceable graded revocable privacy

5.6 Proofs-of-concepts

The proofs-of-concepts presented here are two-fold, namely involving a user misuse that comprises a false report of a non-existing incident, and a user misuse reporting false information of an existing incident. The realization of the revocable privacy action in Table 15 is undertaken for the present use case of a user contribution to a SCS based on the cryptographic primitives BLACR[13] and GSDM[14] (for more details, see section 5.2). The resulting Table 16 shows the exemplary realization of the revocable privacy concept with these cryptographic primitives.

Misuse categories	Incident types			
	Non-critical		Critical	
	C level	Revocable Privacy action	C level	Revocable Privacy action
Report a non-existing incident (false report)	C1	BLACR[13] + increment count for threshold before blocking	C3	BLACR + direct blocking (+ optional reveal TUID with GSDM[14])
Report false information for existing incident	C2	BLACR + direct blocking	C4	BLACR + direct blocking + reveal TUID with GSDM

Table 16: Revocable privacy action of Table 15 with cryptographic primitives BLACR and GSDM.

Proof-of-concept for a user reporting a non-existing traffic congestion:

A user classifies in phase I. (see Figure 12 and 13) the incident based on smart community service guidelines as a non-critical incident (NCI). In phase II. the user accepts the criticality level C1 according to Table 15 or rather Table 16, hence using blacklistable anonymous credentials (BLACR) [94] for the authentication when contributing to the smart community service and reports a traffic congestion. The smart community service in phase III. evaluates the user contribution and immediately detects, that it is a false report of a traffic congestion, because the smart community service has further information e.g. based on GPS, other sensors and cameras positioned along the streets allowing to verify that there is no traffic congestion. Therefore,

[13] Cryptographic primitive: Blacklistable Anonymous Credentials
[14] Cryptographic primitive: Group Signature system with Distributed Management

afterwards in phase IV.-NCI the smart community service based on the applied BLACR [94] can increment the count for a threshold belonging to the private key used in the present misuse and is blocked once having reached the threshold.

Proof-of-concept for a user reporting false information for a traffic accident:

A user classifies in phase I. (see Figure 12 and 13) the incident based on smart community service guidelines as a critical incident (CI). In phase II. the user accepts the criticality level C4 according to Table 15 or rather Table 16, hence using blacklistable anonymous credentials (BLACR) [94] for the authentication when contributing to the smart community service and signs the contribution based on a group signature system with distributed management (GSDM). The user reports the traffic accident including e.g. photos of the cars, injured people, and further details. In phase III., the smart community service starts immediately the roll-out to assist the accidented people to avoid further harm of persons and objects. Detected during the initiated roll-out and corroborated afterwards, the smart community service knows that the contributing user perpetrates a misuse for whatever reason. Therefore, afterwards in phase IV.-CI, based on the applied BLACR [94] the smart community service can immediately block the user from further anonymous authentication regardless of whether the initially set threshold was reached. In addition, depending on the possible damage, the smart community service additionally initiate to reveal the TUID used of the user by means of the applied GSDM to prosecute him. Next, we conclude with the discussion and conclusion of Chapter 5.

5.7 Discussion and conclusions

Starting with the central user right of *self-determination* demanded in *REGULATION (EU) 2016/679* [25], we take up explicitly stated or inferred user rights, which are – among others – the right to be asked for consent (RTC),[15] the right to have Privacy (RTHP),[15] and right to be forgotten (RTBF).[15] The regulation in [25] demands from services to provide related with the user rights compliance as well as technically enforce user rights. RTC – the necessary user consent – is one of the key issues[16] of [25] defined in article 4 and concretised throughout several articles, among others in art. 6 -7. The RTHP to guarantee privacy is in the scope of the key issues[17,18] and concretised throughout the related articles in [25]. Finally, the RTBF is one key issue[19] and explicitly addressed in article 17, but we excluded it from our present detailed consideration

[15] We chose the wording and acronyms for the right to be asked for consent (RTC) and right to have privacy (RTHP). The wording and acronym for the right to be forgotten (RTBF) are commonly used.
[16] https://gdpr-info.eu/issues/consent/
[17] https://gdpr-info.eu/issues/privacy-by-design/
[18] https://gdpr-info.eu/issues/privacy-impact-assessment/
[19] https://gdpr-info.eu/issues/right-to-be-forgotten/

because it addresses a more extensive and partially different focus than the right to have privacy. The results for revocable privacy nonetheless are partially applicable to RTBF, although our focus is on RTC and RTHP.

Users nowadays are becoming increasingly aware about their rights and in particular the importance of their privacy, and thus they are not willing to contribute unconditionally to a smart community service, much less to accept stringed smart community service requirements. In this area of tension, we define a taxonomy concept that obviously facilitates *user enforceable graded revocable privacy* and offers an incentive to be willing to contribute, but nonetheless at the same time to fill the stringent requirements of a smart community service. The developed taxonomy concept considers RTC and RTHP as being anchored in the right of self-determination [25] and we additionally define *enforceable*, *graded* and *revocable* in the context of *user privacy*.

The definition of enforceable, graded and revocable in section 5.4 comprises the fulfilment of the user right to have privacy and for this purpose in section 5.6 the cryptographic primitives blacklistable anonymous credentials (BLACR) and group signatures with distributed management (GSDM) are considered exemplified, thus showing that there are already available cryptographic primitives to realise these basic proofs-of-concepts of enforceable graded revocable privacy scenario. A more granular and sophisticated enforceable graded revocable privacy scenario would require a wider review of existing relevant cryptographic primitives to realize this scenario. For completeness, we point out that there are divers realizations for anonymous authentication [98, 99] using anonymous credentials that offer the user to decide if they want to use unconditional anonymity or not.

The taxonomy concept presented in this chapter facilitates the smart community service in case of misbehaving users by means of e.g. reporting non existing incidents or contributing false information to an existing incident to block the user up to reveal its identity. The presented taxonomy concept developed in the sections 5.4 and 5.5 to harmonise the SCS stringent requirements in section 5.3 and user right of self-determination [25] provides the basis for further investigation of revocable privacy for user contributions to SCS.

The presented taxonomy concept is fullly transparent to the user, so he knows when and under which circumstances revocable privacy is applied. Consequently, to convince user to contribute, their self-determination is guaranteed insofar that they can freely decide to give their consent and if they contribute their privacy is respected. Only in case of misuse if at all the smart community service will anonymously block the user or know the TUID in accordance with the opener's appraisal, regardless of whether the smart community service himself provides the service to issue anonymous credentials or pseudonymous private keys based on the user TUID.

As future research, an outstanding issue is to increase the granularity of the misuse cases and criticality levels defined in Table 15 in section 5.5 or rather Table 16 in section 5.6 and associated with the application of further cryptographic primitives allowing to enforce more granular the realization of graded and revocability for privacy. We stress that besides the mentioned improvement of the mere realization there are further challenges to be addressed in parallel, e.g. to avoid several registrations of the same user using apparently different identities and reduce or eliminate the necessity of a TTP. Of further interest is to investigate how far a user should be able to withdraw a previously-made contribution, e.g. to a critical incident that endangers human safety or camouflage a user misuse. Finally, a systematic PIA and associated PTA of the revocable privacy taxonomy concept and cryptographic approach are indispensable.

Chapter 6

6 Conclusion and Future Work

Users who contribute to smart community services as well as other internet services predominantly perform a user login to pass the verification process towards the service to prove the legitimate usage of the claimed user identity. The protection of the user privacy against privacy threats throughout the verification process and due to the user contribution are – as presented in the introduction Chapter 1 and concretised in the definition of the objectives in section 1.1 – fundamental and require further improvement. This leads to the three-folded objectives of the dissertation related with the PTA of the user verification process in the modelling phase and for realized authentication schemes and how to protect the right of user self-determination with focus on privacy when contributing to a smart community service. Next, we present in chapter 6.1 the conclusions for the main results of the three objectives and finish with overarching conclusions. The chapter concludes with section 6.2 with identified future work.

6.1 Conclusions

The section is organized in accordance with the three main objectives of the dissertation. Section 6.1.1 focuses on the extension of the LINDDUN PTA framework for the modelling of the verification process in Chapter 3, section 6.1.2 on the extended UDSP framework for the evaluation of authentication schemes in Chapter 4 and section 6.1.3 on the presented taxonomy concept to realize a user self-determined revocable privacy approach in Chapter 5, followed by overarching conclusions in section 6.1.4.

6.1.1 Extended LINDDUN framework-based Privacy Threat Analysis of the verification process in the modelling phase

The verification process is analysed in the modelling of the scenario to determine privacy threats before implementing an authentication scheme for login purpose.

Specifically for the verification process, we extend LINDDUN [16], the most promising systematic PTA framework, which uses an information-flow-oriented system representation using data flow diagram (DFD).

Thus, we model the user login verification process as a four-phase process (service demand, identification, authentication, service access). Embedding the three-step identification and authentication process that we defined, thus the identification comprises identity presentation and subsequently the plausibility verification of the presented identity, before the authentication step to prove the user claim is performed. In tables, we gather IA methods combination comprising authentication factors, authentication protocols and conceptualize trust boundaries (see section 3.3). Next, we extend the trust boundary concept from LINDDUN [16] with the conceptualized trust boundaries to elicit the relationship between the single DFD elements, the user and domains involved.

All of this culminated in the extension for identification and authentication process of LINDDUN PTA modelling framework and further we contribute DFD template drawings considering domain trust boundaries to support the modelling and threat mapping process, so we conclude by extending the privacy threat mapping table significantly to be applicable to IA processes.

A systematic-reproducible step-by-step guide to facilitate to perform based on the extended LINDDUN framework a PTA of the modelled verification process assembled by us is applicable by the auditor.

We create a step-by-step guide for the auditor to systematically and reproducibly apply the extended LINDDUN framework for identification and authentication process. The PROBLEM SPACE[20] of LINDDUN [16] framework is composed of three steps, *1. Define DFD*, *2. Map privacy threats to DFD elements* and *3. Identify threat scenarios*, which build on one another. Our extensions of LINDDUN framework are in steps 1 and 2 starting with the modelling of IA and concluding in the DFD diagrams and extended privacy threat mapping table.

Once the replenished LINDDUN framework steps 1 and 2 are realized with the systematic step-by-step guide, the auditor has the basis to proceed with the regular step 3 of the LINDDUN framework.

[20] Figure 1. The formalized LINDDUN steps

Summing up, with the extended LINDDUN PTA framework a privacy corresponding authentication scheme can be modelled for a concrete scenario for the identification and authentication process, thus afterwards designed or selected and then implemented. The modelling of the authentication process with our extended LINDDUN framework and realization of the PTA is guided with our step-by-step- guide to apply adequate our included knowledge offering decision support that we added.

6.1.2 UDSP framework-based: Privacy Threat Analysis of the verification process of realized authentication schemes

The authentication scheme to realize the user verification process – once known and thus developed, or selected – can be subject to a further different or initial PTA independent from the previous presented considerations for the extension of the LINDDUN framework.

In the context of evaluation frameworks for authentication schemes, the concept of Bonneau et al. [20] analysing usability (U), deployability (D) and security (S) stands out as being scientifically proven in further publications, e.g. in [43, 44]. We extend the UDS evaluation framework [20] for authentication schemes from Bonneau et al. [20] with a privacy category (P) to close the gap and become the UDSP evaluation framework. The privacy category in a first step comprises privacy benefits covering traditional hard and soft privacy benefits. Only three biometrics are considered in [20], and thus we add machine learning-based behavioural biometrics from the survey of Hanisch et al. [24]. Accordingly, in a second step we extend the new privacy category with ML-related privacy benefits.

Therefore, the resulting privacy category covers traditional hard and soft privacy benefits related with the authentication schemes, as well as ML-related privacy benefits in the context of behavioural biometrics (e.g. to avoid ML-based inference of additional personal information from the biometric data, originally envisaged only for authentication).

Implementation approaches applicable to authentication schemes to mitigate the revealed privacy threats.

The PTA of authentication schemes including all types of biometrics (see Table 10) with the extended UDSP framework reveals – inter alia – not-offered fundamental privacy benefits, and thus we group the privacy threats by the affected targets (section 4.5.3), namely authentication schemes, biometrics (especially behavioural biometric with ML-based feature extraction) and security category of the original UDS framework, with the latter being relevant for the privacy of both authentication schemes as a whole and the included biometrics. We gathered implementation approaches across the three targets to mitigate

fundamental privacy threats for authentication schemes including machine learning-based privacy threats of biometrics.

Summing up, the extended UDSP framework facilitates additionally performing a detailed PTA considering a new defined privacy benefit category including previous results of the UDS framework. Consequently we propose implementation approaches for the mitigation of fundamental privacy threats. The associated implementation approaches of our UDSP framework constitute an extension of the LINDDUN SOLUTION SPACE[22] comprising three steps, 4. Prioritize threats, 5. Elicit mitigation strategies and 6. Select corresponding PETs[21].

6.1.3 Revocable Privacy

The user contribution to a smart community service especially for critical incidents can be undertaken in a self-determined manner by the user, so that depending on the criticality level he accepts in case he perpetrates a misuse revocable privacy.

The taxonomy concept applied to achieve revocable privacy comprises the composition of the user contribution, the definition of the criticality level of the incident and a first proposal for a realization with cryptographic primitives based on blacklistable anonymous credentials (BLACR) and group signatures with distributed management (GSDM). The cryptographic primitives supports the contributing user to self-determined decide to what incident type and criticality level – hence graded – he wants to contribute and if he is willing to accept in case he perpetrates a misuse revocable privacy. The revocation of the privacy can comprise the user being blocked anonymously or pseudonymously and the additional revelation of his TUID. Applying the process flow depicted in Figure 13, our taxonomy concept is exemplified for the two central main misuse case categories, namely misuse based on reporting a non-existing incident or based on reporting false information of a real existing incident. The smart community service in principle can issue based on the user presented TUID the necessary anonymous credentials or pseudonymous private keys for BLACR and GSDM without compromising the privacy of the taxonomy concept.

Summing up, we present a taxonomy concept suitable for describing the integral parts of a user self-determined revocable privacy-aware solution whose process flow is detailed in Figure 13 of section 5.5 and exemplified with two proofs-of-concepts in section 5.6. The smart community service can issue based on the user TUID the required anonymous credentials for BLACR or pseudonymous private keys for GSDM.

[21] Privacy Enhancing Technologies

6.1.4 Overarching Conclusions

The contributions throughout the dissertation constitute an integral approach to safeguard the privacy of the user passing the verification process for login purposes and contributing to a smart community service.

The view towards the verification process is from the development or design point of view based on the extended LINDDUN PTA framework [16], and thus privacy is considered systematically from the beginning to fulfil privacy-by-default development as demanded in article 25 of REGULATION (EU) 2016/ 679 OF THE (EU-GDPR) [25].

On the other hand, the further view is after selecting or implementing an authentication scheme, and thus the fulfilment of privacy in the authentication scheme is verified with the extended UDSP PTA framework for authentication schemes [20].

In Chapter 3 with the extended LINDDUN PTA framework two proof-of-concept scenarios are modelled, one based on login with a username and password, while the other is a smart-card-based authentication. The basic difference between the two is that for password *local authentication and a centralized verification based on one server (IA)* is assumed and for smartcard *external authentication and a decentralized verification based on two servers (I)-(A) is assumed.* These assumptions result from the proofs-of-concepts scenario description. A comparison of the two use cases show that if the assumptions are interchanged, the modelling results are mutually interchangeable, so that the results vary largely depending on the assumptions. That is the point where our contribution beside of guiding the modelling facilitates additional knowledge to the auditor for realistic assumptions.

The IA process extended LINDDUN PTA framework in Chapter 3 and the extended UDSP framework in Chapter 4 can be used sequentially for scenarios that are in the definition stage to initially determine the relevant privacy threats for the verification process with the LINDDUN PTA framework. After determining the appropriate authentication scheme, the UDSP framework is independently applicable to corroborate the fulfilment of the elicited privacy requirements.

The extended UDSP framework can naturally be applied to existing authentication schemes realizations to verify their privacy benefit conformity, without previous application of the extended LINDDUN framework.

The modelling of identification and authentication methods in the extended LINDDUN PTA framework considers electronic and manual user identity presentation methods and for authentication factors *knowledge*, *possession* or *being someone* representative realizations. The UDSP PTA framework considers both methods of presenting (inserting) the user identity,

manually by the user or electronically passed e.g. with a token. Furthermore, the precursor of the extended UDSP PTA framework originally considers additional knowledge-based authentication factors based on graphical and cognitive user abilities as well as passwords, too. In this context, we stress that the UDSP PTA framework considerably contributes to the consideration of the authentication factor *being someone* through the multiple behavioural biometrics that we included from [24, 73]. Additionally, we point out that the UDSP framework further contributes to the authentication factor *being someone* with covert or overt trait-based behavioural biometrics from [24] using machine learning. The overt trait behavioural biometrics are prone to be liable to not avoidable capture of biometric data as a by-product e.g. possible with cameras or microphones, and thus are still susceptible to inference of private information with ML.

The UDSP framework offers implementation approaches to mitigate detected fundamental privacy threats. We group the privacy threats by the affected targets, which are authentication schemes including biometrics and security benefits. Thus, we point out that this contributes to the LINDDUN SOLUTION SPACE (see Figure 1) with concrete privacy enhancing technologies or standard measures to consider.

The sequential application of the extended LINDDUN PTA framework and extended UDSP framework constitutes a connection between both frameworks that we will pick up in future work to investigate a systematic combined approach of both.

The evaluation of authentication schemes in Chapter 4 with the extended UDSP framework including the new privacy category emphasizes the evaluation results of the original UDS framework towards the legacy password scheme. Legacy passwords belong to the worst rated for security with UDS, and additionally the evaluation with UDSP reveal it belongs to the worst rated for privacy. Furthermore, the UDSP framework additionally reveals in the evaluation that privacy benefits are not offered due to not-offered security benefits, because we considered the UDS framework security benefit evaluated in [20] additionally in the UDSP framework. The results of the evaluation with UDS [20] and evaluation with UDSP framework in Chapter 4 do not point out what is the best authentication scheme, but both independently conclude that the password authentication scheme belongs to the worst rated for security or rather privacy. The only reasonable explanation why it is still the most commonly used is due to being best rated for deployability and offering an acceptable usability.

The user contribution to the smart community service with information for critical incidents fulfilling the stringent smart community service requirements conflicts with the user privacy requirements. Our proposed taxonomy concept facilitates the contributing user to self-determined decide up to what grade he is willing to accept revocable privacy in case his contribution

constitutes a misuse. Revocable privacy comprises that the user privacy is guaranteed based on cryptographic primitives and only revealed if a misuse is detected. Our taxonomy concept for a contribution with revocable privacy is open for whatever cryptographic primitives are required for the defined proof-of-concept or criticality levels included in the future for more sophisticated definition of critical incidents. The user TUID can be used by a smart community service itself or another trusted service to issue anonymous credentials, apply blacklistable anonymous credentials, or to issue private keys to apply group signatures with distributed management.

Finally, a holistic view of the contributions is given. The PTA with the extended LINDDUN framework is applicable in the modelling of the verification process (identification and authentication process) to afterwards design or select an authentication scheme. The UDSP framework including our extensions is applicable to authentication schemes irrespective if the authentication scheme was previously selected based on the extended PTA LINDDUN framework in the modelling phase of the verification process. In case the authentication scheme was previously selected or implemented based on the extended PTA LINDDUN framework, the posterior evaluation with the extended UDSP PTA framework equals the corroboration of previously elicited requirements. At least we emphasize that the privacy evaluated authentication schemes can be used for a more privacy compliant login to whatever internet or smart community service requiring to know the real user identity, although it can also be used in the context of anonymous credential-based authentication services or group signatures e.g. with distributed management. Thus, the user can use the privacy conform authentication scheme to obtain anonymous authentication tokens or private key for the use with group signatures from issuing trusted services or the smart community service itself, and afterwards use them for contributions with enforceable graded revocable privacy. Next, we proceed and conclude with an outlook to future research lines.

6.2 Future Work

In the present section, we present possible further research lines that we detected, which are based on upcoming ideas or constitute a continuation of results presented in the dissertation.

The UDSP PTA framework from Chapter 4 is applicable to existing authentication schemes. It is already possible to apply the extended LINDDUN PTA framework from Chapter 3 to elicit relevant privacy threats for authentication schemes to be selected or implemented, and afterwards apply the UDSP PTA framework to the resulting authentication scheme. This facilitates corroborating the realization of requirements elicited during the modelling of the identification and authentication process.

- Thus, the intuitive sequential application of the extended LINDDUN and extended UDSP framework could be systemized through further research, so that both frameworks are mutually extended and systematically build on one another.

The extended UDSP PTA framework considers machine learning-based behavioural biometrics using covert or overt traits and the privacy threats arising from inference of private information derived from the biometric data used for authentication purpose. The work [24, 73] considered in Chapter 4 presents a survey of privacy-protecting technologies to protect behavioural biometric data for authentication purpose against ML-based inference of personal information, especially threaten by a malicious service. The authors assume a biometric data-publishing scenario. Overt trait-based behavioural biometrics are susceptible to be captured inevitably as a by-product.

- Thus, it is reasonable to research how to avoid the usage of overt trait-based biometric captured as a by-product for authentication purposes.

The password authentication scheme belongs to the worst rated for privacy with the extended UDSP PTA framework in Chapter 4 and worst rated for security based on the UDS framework [20]. Our evaluation with our extended UDSP PTA framework for privacy corroborates the appraisal that a password scheme alternative is indicated. Overall, the password scheme is compared worse for security and privacy, but offering the best deployability and predominantly offering the best usability.

- Thus, the prospect of a future authentication scheme (see section 4.6) capable of substituting the password scheme is needed, so that security and privacy are offered without affecting or reducing usability and deployability.

The presented taxonomy concept for *Revocable Privacy* facilitates the user to self-determined accept the grade of revocation of his privacy he is willing to assume in case he misbehaves in the context of the contribution to an incident. In two representative proofs-of-concepts, one for a misuse due to reporting a non-existing incident and a further for reporting false information of an existing incident, we verified our taxonomy concept comprising a basic definition of the criticality levels of critical incidents. In the POCs, the cryptographic primitives blacklistable anonymous credentials (BLACR) and group signatures with distributed management (GSDM) are applied.

- Thus, for a more graded revocable privacy a more granular definition of criticality levels can be defined by smart community services, consequently cryptographic primitives supporting them will be elicited and applied.
- Concluding, as mentioned in section 5.7 further challenges must be addressed in parallel, e.g. to avoid several registrations of the same user using apparently different identities

and reduce or eliminate the necessity of a TTP. The evaluation of how far a user should be able to withdraw a contribution to a critical incident that endangers human safety or to camouflage a user misuse

Appendices

Appendix A

Acronyms

A	Authentication
AS	Authentication Scheme
API	Application Programming Interface
AppID	SmartPhone app SCS installation ID
BLACR	Blacklistable anonymous credentials
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
C1	Criticality level 1
C2	Criticality level 2
C3	Criticality level 3
C4	Criticality level 4
CR	Challenge response
D	Deployability
DB	Data Base
DFD	Data Flow Diagram
E	Evidence
ED	External Domain
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité – Expression of needs and identification of security objectives
eID	Electronic identity
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
GSDM	Group signature system with distributed management
HW	Hardware
I	Identification
ID	Identity

IA	Identification and authentication
ID	Identifier
LD	Local Domain
loginID	Login Identity
M	Mandatory
MRZ	Machine Readable Zone
NFC	Near Field Communication
P	Privacy
PB	Privacy Benefit
PIAF	A Privacy Impact Assessment Framework for data protection and privacy rights (project name)
PII	Personal Identifiable Information
PET	Privacy Enhancing Technologies
PKI	Public Key Infrastructure
PIA	Privacy Impact Assessment
Proof-of-concept	PoC
PTA	Privacy Threat Analysis
RFID	Radio-Frequency Identification
RTBF	Right to be forgotten
RTC	Right to be asked for consent
RTHO	Right to have privacy
S	Service
SC	Smartcard
SCS	Smart community service
SCSUID	Smart community service user identity
SNID	Social network identity
SSO	Single Sign On
S/SP	Service Provision

STRIDE	An acronym for Spoofing identity, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
SW	Software
TTP	Trusted Third Party
TUID	Trustworthy user identity
U	Usability
UDS	Usability Deployability Security
ULD SH	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UML	Universal Markup Language

Table 17: List of acronyms.

Appendix B

LINDDUN Framework in Chapter 3: A step-by-step overview of the LINDDUN framework example

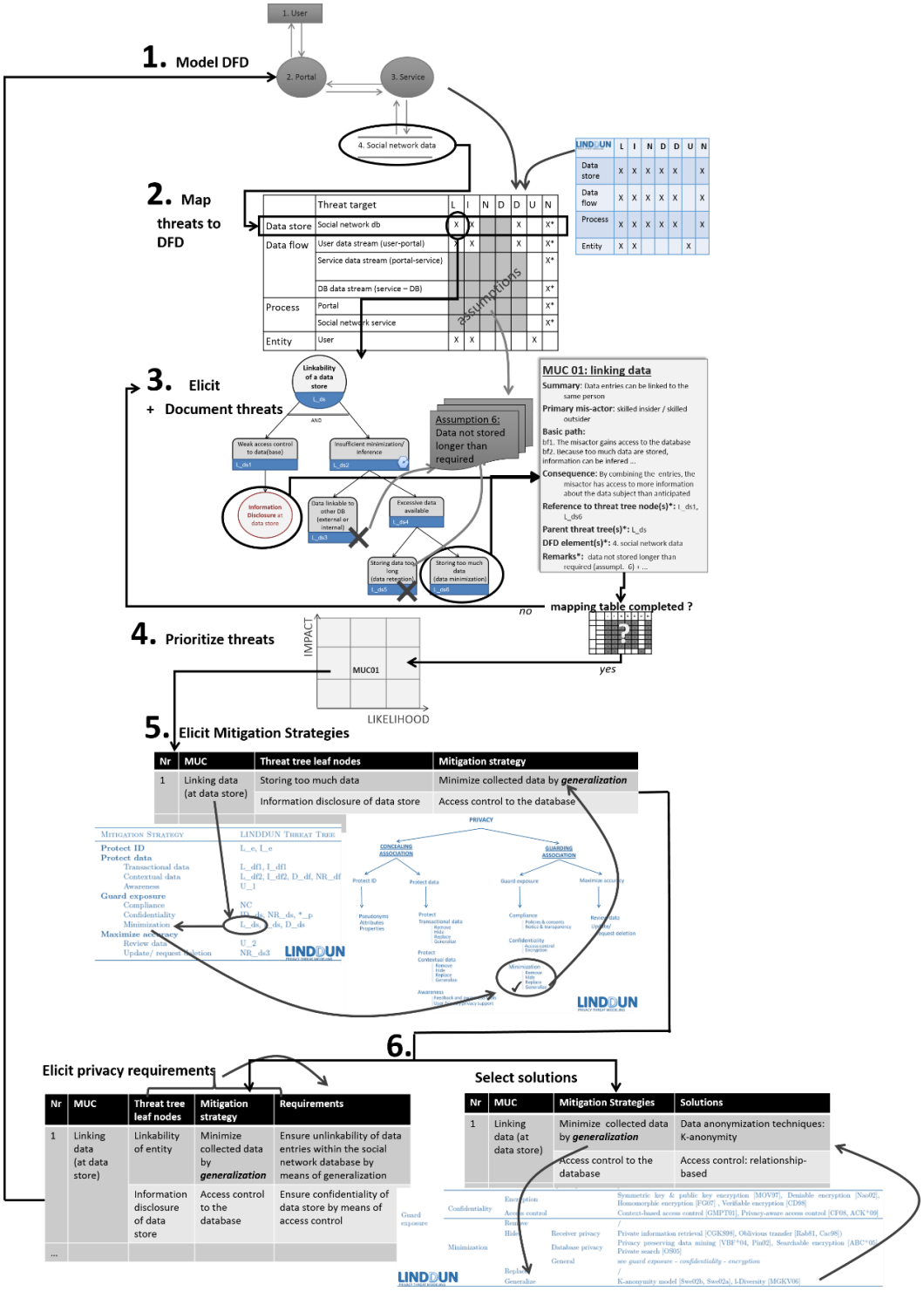


Figure 14. A step-by-step overview of the LINDDUN framework using a simple social network system as running example[22].

[22] https://distrinet.cs.kuleuven.be/software/linddun/linddun.php

Appendix C

Functional description of UDS Authentication Schemes of Chapter 4

Password Manager

Firefox PWM

The user identifier can be a real name or pseudonym and is inserted manually as well as the password-based user credential (called password). After using the account details for the first time – if the user agree to store them – the Firefox PWM remember them. The access to all encrypted accounts in the Firefox PWM is protected with a master password and inserted only one time for each Web Browser session.

LastPass

LastPass is a commercial and proprietary password manager that integrates with a variety of web browsers (through plug-ins) and provides cloud storage and syncing of encrypted passwords. Saved passwords are protected by a master password, as with Firefox, but LastPass also allows cross-browser syncing, even with browsers on smartphones. The program also generates strong passwords. User account details are decrypted at client side.

Proxy

URSSA

The user identifier can be a real name or pseudonym and is inserted manually as well as the used one-time codes. The proxy-based scheme (acting as reverse-proxy) places a man-in-the-middle between the prover and verifier, and after the initial registration of services at the proxy the user gets the encrypted password, and thus the ciphertext e.g. thirty times with as much different keys per service (see [20]) printed on a paper sheet. The proxy only stores the corresponding keys. To login, the user accesses the proxy, indicates the site to visit with the corresponding user identifier and is then asked by the proxy to insert one of the not-used codes (the printed ciphertext), so that the proxy (reverse-proxy) only decrypts the ciphertext replacing the ciphertext with the password, see [101].

Impostor

The AS Impostor proxy-based solution named by the author [102] pseudo-SSO system, strictly speaking is not a SSO system because it is not reusing a still done authentication at a service A once visiting service C. From our point of view, it is more a password manger which requires instead of a master password a one-time authentication mechanism to give access to use the stored accounts using long-term credentials. Once the session to the proxy by the user is authenticated with one-time

authentication, the user is automatically logged-in to the subsequently used services [102] if the account details are stored in Impostor. The user authenticates with a random N character long subset of a shared passphrase with the proxy. The shared passphrase at least has eight characters, but it is recommendable to set 30, 50 or more characters. The user inserts N randomly challenged characters from the passphrase to authenticate.

Federated

OpenID

The user identifier can be a real name or pseudonym. The user identifier and the password-based user credential are inserted manually. Bonneau et al. [20] note, that in practise identity provider will continue using passwords with OpenID despite that the protocol supports the usage of stronger authentication schemes. The difference in comparison with legacy password is that the verification of the claim, hence the mere authentication step, is done towards the OpenID identity provider (IdP). The initial request is sent by the user to the verifier service (relying party (RP)), which redirects the user to the OpenID (IdP) and after the successful authentication towards the OpenID (IdP) the user is coming back (redirected) to the verifier service (RP), and thus presenting the cryptographic proof (token) gotten by the OpenID (IdP). Profile data to be released towards the verifier service (RP) by the user by means of the OpenID protocol are beyond the scope of the evaluation done in Chapter 4.

Microsoft Passport

Meanwhile Microsoft Passport is Microsoft account (MSA) and is accessible with MSA and still being centralized with only trusting authentication server from a Microsoft environment.

Facebook Connect

Facebook Connect is a SSO scheme being the only identity provider and being very similar to OpenID [49]. The user when accessing a service is redirected to Facebook for authentication purpose to e.g. type in the credentials. In case of still being authenticated by Facebook Connect the user is automatically logged in accessing another service.

SAW (OTP over email)

The manually inserted user identifier can be a real name or pseudonym. As described in [103], with Simple Authentication for the Web (SAW) the user inserts the user identifier, in this case his email to the service to be accessed. The service sets a *user auth token* at the user's browser (cookie) and sent a one-time *email auth token* to the user by email. Once the user gets the *email auth token* the authentication can be completed by means of returning both tokens to the service to be used. In case of non-availability of the primary email provider a secondary email is settable.

Graphical

PCCP (Persuasive Cued Clickpoints)

The user identifier can be a real name or pseudonym and is inserted manually. The extension of a website with the Persuasive Cued Click-Points (PCCP) selection in a sequence of five images collects the *PCCP password* – as Chiasson et al. [104] writes – and is passed afterwards to the original website that perform the authentication. The user proves with PCCP his secret knowledge about the initially selected click points.

PassGo

The user e.g. on a 9 x 9 grid of dots doodles a sequence with his finger, mouse, or stylus. The user to authenticate inserts the user identifier and afterwards the user recalls a previously defined sequence.

Cognitive

GrIDsure

The user identifier can be a real name or pseudonym and is inserted manually. The extension of a website with the GrIDsure introduces an underlying one-time password (OTP) authentication scheme where the OTPs are calculated based on the fix pattern defined by the user, and for that the values of the selected fix cells vary between two authentication attempts. The user proves with GrIDSure his secret knowledge of the initially selected pattern.

Weinshall

The user identifier can be a real name or pseudonym and is inserted manually. The authentication scheme require to memorize 30 pictures before using it (see [105]). The login presents the user 80 pictures as a grid of 8 X 10 pictures. Starting from the upper left picture the user steps down or to the right depending on if the picture below belongs to the 30 memorized pictures. The reached picture at the right side indicates a number to be entered for login. The average is eleven times to pass this query.

Hopper Blum

The user identifier can be a real name or pseudonym and is inserted manually. The authentication scheme requires the user and server to share a N-bit secret with N = 120. The authentication starts with a N-bit challenge and the user must calculate the 1-bit inner product and returns the correct answer. This is repeated up to 20 times to authenticate the user.

Word Association

The user identifier can be a real name or pseudonym and is inserted manually. The user defines e.g. 20-word pairs and share them with the server. The authentication requires that the user for one or more word pairs answers with the second word to the related first word of the pair.

Paper tokens

OTPW

The user identifier can be a real name or pseudonym and is inserted manually. The extension of a website with the OTPW paper list is a one-time password (OTP)-based authentication scheme. Each authentication requires to insert manually a prefix password and one of the OTPW for that the user is prompted.

S/Key

The user identifier can be a real name or pseudonym and is inserted manually. The user identifier is as for other schemes. Starting with a secret S a hash function is applied to the initial secret n times resulting in n one-time passwords. The authentication can be done manually or as usual with a pluggable login module.

PIN+TAN

The user identifier can be a real name or pseudonym and is inserted manually. The AS is used in bank environments, and thus the bank sends the user a sheet of printed codes so that for authentication purposes the user can be queried for a random set of codes.

Visual crypto

PassWindow

The user identifier can be a real name or pseudonym and is inserted manually. The user gets a card looking like a bank credit card with a little transparent rectangular area that once positioned on the display of a smart device or monitor displays digit by digit the secret to be transcribed by the user to the login form.

Hardware tokens

RSA SecurID

The user identifier can be a real name or pseudonym and is inserted manually. The extension of a website with the RSA SecurID is a one-time password (OTP)-based authentication scheme by means of a hardware token. Each authentication requires to insert manually a prefix password and the displayed OTP.

YubiKey

The user identifier is a fixed string sent concatenated with the one-time code. The USB-based YubiKey device is plugged to the PC/NB and the user insert a PIN or password, and thus the user sets for login the cursor scope to the YubiKey input box and press the only button. Next the Yubikey device passes concatenated fixed identity string and one time code to authenticate the user.

IronKey

The user identifier can be a real name or pseudonym and is inserted manually. The user carry with him a bootable USB device including an encrypted storage accessible once the user inserts the password. The USB offers – once booted – a harden and secured execution environment for running the Web Browser for login to the bank whose URL is included into the secure environment. The user then proceeds to login with the bank account composed of a user identifier and password.

CAP reader

The user identifier can be a real name or pseudonym and is inserted manually. The user inserts in the CAP (Chip Authentication Program) reader the EMV (Europay International, MasterCard and VISA) bank card and types in the card PIN into the CAP reader, and afterwards the CAP reader displays a one-time 8-digit code. The user transcribes this one-time code to the login form of the bank site.

Pico

The user identifier is as for other schemes. Pico is a hardware device capable to interact via a 2 D camera with visual information presented at the PC screen [106]. The Pico token is cryptographically paired with the Pico app on the PC and Picosiblings (small objects chosen for the property that the user *"... will wear them practically all the time: glasses, belt, wallet, various items of jewellery—even piercings, wigs, dentures and subcutaneous implants*" [49]). The usual user identifier and password login form is augmented with a visual code, and by pointing with the camera to this visual code and pressing the button *main* on Pico the authentication is performed based on pre-established credentials [106]. Depending on the Picosiblings [106] in the proximity of the Pico near the PC continuous authentication is performed.

Phone-based

Phoolproof

The user identifier can be a real name or pseudonym and is inserted manually as well as the password-based user credential. Phoolproof uses a mobile phone to establish a secured TLS connection with mutual authentication to whitelisted destinations (e.g. bank), and over this secured connection the banking website is opened to introduce the user identifier and password.

Cronto

The user identifier can be a real name or pseudonym and is inserted manually. Cronto is based on a camera phone [20, 49]. The bank login web page shows a cryptogram and after the user gets it with the phone camera an on-time password is shown that must then be passed to the web page login form. The phone uses a bank application using a per-device key shared with the bank.

MP-Auth

The user identifier can be a real name or pseudonym and is inserted manually. The phone based AS is used as trusted endpoint that is connected to the PC with e.g. wire-line or Bluetooth [107]. The

user connects to the bank webpage based on a symmetric key-based SSL connection with the password the user provides, that is not stored on the phone but introduced by means of the phone. Next, a challenge response sequence is performed between the phone and the PC and afterwards the success or failure of the authentication is displayed.

OTP over SMS

The user identifier can be a real name or pseudonym and is inserted manually. The user accesses the login form of the webpage to access with his user identifier and that trigger sending him an SMS with a one-time password.

Google 2-Step

The user identifier can be a real name or pseudonym and is inserted manually. The AS combines the traditional legacy password with one-time codes. The OTP code to be transcribed by the user can be transmitted to him over an SMS, voice call or is generated on a mobile phone application (Google Authenticator) holding the secret. The user can accept cookies on the Web Browser, so that within the next 30 days the user do not need to use the phone to authenticate again. The evaluation done by Bonneau et all rate the variant without the Google Authenticator.

Bibliography

[1] Lindskog, H. SMART COMMUNITIES - EUROPEAN AND AMERICAN INITIATIVES. *Proceedings of the 3rd ISOneWorld Conference, 2004*.

[2] Ganti, R. K., Ye, F., and Lei, H. Mobile Crowdsensing: Current State and Future Challenges. *IEEE Communications Magazine* November 2011.

[3] Laperdrix, P., Bielova, N., Baudry, B., and Avoine, G. 2020. Browser Fingerprinting. *ACM Trans. Web* 14, 2, 1–33.

[4] Randika Upathilake, Yingkun Li, and Ashraf Matrawy. 2015. *A Classification of Web Browser Fingerprinting Techniques*. Accessed 16 July 2022.

[5] Pfitzmann, A. and Hansen, M. 2010. *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. *Anon_Terminology_v0.34.pdf*.

[6] Menezes, A. J., Vanstone, S. A., and Van Oorschot, Paul C. 1997. *Handbook of applied cryptology*. CRC Press series on discrete mathematics and its applications. CRC, [S.l.].

[7] Eckert, C. 2013. *IT-Sicherheit*. *Konzepte - Verfahren - Protokolle*. 8. aktualisierte und korrigierte Auflage. Oldenbourg, München.

[8] Robert Havighurst. 2007. User Identification and Authentication Concepts. In *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*, D. Todorov, Ed.

[9] Kloza, D. 2012. A Privacy Impact Assessment Framework for data protection and privacy rights. Recommendations for a privacy impact assessment framework for the European Union. Microsoft Word - PIAF D3 recommendations v4.2 pr clean.docx.

[10] Wright, D. and Hert, P. d. 2012. *Privacy impact assessment*. Law, governance and technology series v.6. Springer, Dordrecht, New York.

[11] Oetzel, M. C. and Spiekermann, S. 2013. A systematic methodology for privacy impact assessments: a design science approach. *Eur J Inf Syst* 23, 2, 126–150.

[12] Christopher, G. and Information Commissioners Office. 2014. Conducting privacy impact assessments. code of practice. pia-code-of-practice.

[13] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., and Schiffner, S. 2014. *Privacy and Data Protection by Design – from policy to engineering*. *ENISA*.

[14] CNIL - French Data protection Authority. É d i t i o n 2 0 1 2. Methodology for Privacy Risk Management - English version. How to implement the Data Protection Act (É d i t i o n 2 0 1 2).

[15] Michael N. Johnstone. 2010. Threat Modelling with Stride and UML. *Originally published in the Proceedings of the 8th Australian Information Security Mangement Conferencee, Edith Cowan University, Perth Western*.

[16] Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W. 2010. LINDDUN: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements.

[17] Prasser, F., Kohlmayer, F., Spengler, H., and Kuhn, K. 2017. A scalable and pragmatic method for the safe sharing of high-quality health data. *IEEE journal of biomedical and health informatics*.

[18] Brandizi, M., Melnichuk, O., Bild, R., Kohlmayer, F., Rodriguez-Castro, B., Spengler, H., Kuhn, K. A., Kuchinke, W., Ohmann, C., Mustonen, T., Linden, M., Nyronen, T., Lappalainen, I., Brazma, A., and Sarkans, U. 2017. Orchestrating differential data access for translational research. A pilot implementation. *BMC medical informatics and decision making* 17, 1, 30.

[19] Livinus Obiora Nweke, Mohamed Abomhara, Sule Yildirim Yayilgan, Debora Comparin, Olivier Heurtier, and Calum Bunney. A LINDDUN-Based Privacy Threat Modelling for National Identification Systems. *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*.

[20] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *IEEE Symposium on Security and Privacy*.

[21] Mayer, P., Neumann, S., Storck, D., and Volkamer, M. 2016. Supporting Decision Makers in Choosing Suitable Authentication Schemes.

[22] Alaca, F. and van Oorschot, P. C. 2020. Comparative Analysis and Framework Evaluating Web Single Sign-on Systems. *ACM Comput. Surv.* 53, 5, 1–34.

[23] Broders, N., Martinie, C., Palanque, P., Winckler, M., and Halunen, K. 2020. A Generic Multimodels-Based Approach for the Analysis of Usability and Security of Authentication Mechanisms.

[24] Simon Hanisch, Patricia Arias-Cabarcos, Javier Parra-Arnau, and Thorsten Strufe. 2021. Privacy-Protecting Techniques for Behavioral Data: A Survey. *Privacy-Protecting Techniques for Behavioral*.

[25] Official Journal of the European Union, P. 2016. REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection

of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) (Apr. 2016).

[26] Robles-González, A., Parra-Arnau, J., and Forné, J. 2020. A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes. *Computers & Security,* Vol. 94 no. 101755. https://doi.org/10.1016/j.cose.2020.101755.

[27] Robles-González, A., Arias-Cabarcos, P., and Parra-Arnau, J. 2023. Privacy-Centered Authentication: a new Framework and Analysis. *Computers & Security,* available online 26 June 2023, 103353. https://doi.org/10.1016/j.cose.2023.103353.

[28] Robles-González, A., Arias-Cabarcos, P., and Parra-Arnau, J. Revocable Privacy – Enhanced user privacy requirements for user-driven self-determination. *Submitted to the International Conference on Networked Systems (NetSys) in June 2023*.

[29] Wright, D. and Hert, P. d. 2012. PRIVACY IMPACT ASSESSMENT. *Law, Governance and Technology Series,* VOLUME 6.

[30] European Commission. 2011. *Privacy and Data Protection Impact Assessment Framework for RFID Applications*. Accessed 1 October 2015.

[31] (BSI) Bundesamt für Sicherheit in der Informationstechnik. 2011. Privacy Impact Assessment Guideline for RFID Applications.

[32] CNIL - Commission Nationale de l'informatique et des libertés. 2015. PIA, METHODOLOGY. PRIVACY IMPACT ASSESSMENT (PIA) Methodology (how to carry out a PIA) (Jun. 2015).

[33] Wuyts, K., Joosen, W., and Scandariato, R. 2014. LIND(D)UN privacy threat tree catalog (Sep. 2014).

[34] Wuyts, K. 2015. Privacy Threats in Software Architectures. PhD (Jan. 2015).

[35] Wuyts, K. and Joosen, W. 2015. LINDDUN privacy threat modelling: a tuorial (Jul. 2015).

[36] LINDDUN - DistriNet Research Group. 2014. *LINDDUN in a nutshell*. https:// distrinet.cs.kuleuven.be/software/linddun/linddun.php. Accessed 2 June 2016.

[37] Wuyts, K. 2015. LINDDUN 2.0. Privacy knowledge (tables) (Jul. 2015).

[38] NIST. 2021. *NIST Privacy Framework Guidance/Tool*. *LINDDUN privacy threat modeling framework*. https://www.nist.gov/privacy-framework/linddun-privacy-threat-modeling-framework.

[39] Al-Momani, A.'a., Bösch, C., Wuyts, K., Sion, L., Joosen, W., and Kargl, F. 2022. Mitigation lost in translation. In *The 37th Annual ACM Symposium on Applied Computing*. *Virtual, April 25 - April 29, 2022*. Association for Computing Machinery, New York, NY, United States, 1236–1247. DOI=10.1145/3477314.3507107.

[40] Omitola, T., Tsakalakis, N., Wills, G., Gomer, R., Waterson, B., Cherret, T., and STALLA-BOURDILLON, S. 2022. User Configurable Privacy Requirements Elicitation in Cyber-Physical Systems. In *UMAP '22*. *Adjunct proceedings of the 30th ACM Conference on User*

Modeling, Adaptation and Personalization : 4-7 July 2022, Barcelona, Spain. The Association for Computing Machinery, New York, New York, 109–119. DOI=10.1145/3511047.3537683.

[41] Azam, N., Michala, L., Ansari, S., and Truong, N. B. 2022. Data Privacy Threat Modelling for Autonomous Systems. A Survey from the GDPR's Perspective. *IEEE Trans. Big Data*, 1–27.

[42] Iwaya, L. H., Babar, M. A., Rashid, A., and Wijayarathna, C. 2023. On the Privacy of Mental Health Apps. An Empirical Investigation and its Implications for Apps Development. *Empir Software Eng* 28, 1, e15654.

[43] Zimmermann, V., Gerber, N., Kleboth, M., and von Preuschen, A. 2018. The Quest to Replace Passwords Revisited – Rating Authentication Schemes (Aug. 2018).

[44] Zimmermann, V. and Gerber, N. 2020. The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies* 133, 26–44.

[45] Grassi, P. A., Garcia, M. E., and Fenton, J. L. 2017. *Digital identity guidelines*. *Revision 3*. NIST Special Publication 800-63-3. National Institute of Standards and Technology, Gaithersburg, MD.

[46] Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., and Theofanos, M. F. 2017. *Digital identity guidelines*. *Authentication and lifecycle management*. NIST Special Publication 800-63B. National Institute of Standards and Technology, Gaithersburg, MD.

[47] Joint Task Force. 2020. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Revision 5. National Institute of Standards and Technology.

[48] ISO. 2022. *ISO/IEC 27001 Standard – Information Security Management Systems*. *Actual version 2022*. https://www.iso.org/standard/27001. Accessed 11 May 2023.

[49] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano. 2012. EXTENDED Version: The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes. Technical Report.

[50] Modinis IDM Study Team. 2005. Modinis Study on Identity Management in eGovernment. Modinis Workshop Discussion Paper (Nov. 2005).

[51] Xiong, W. and Lagerström, R. 2019. Threat modeling – A systematic literature review. *Computers & Security* 84, 53–69.

[52] Veseli, F., Olvera, J. S., Pulls, T., and Rannenberg, K. Engineering privacy by design. In *Hung (Hg.) 2019 – The 34th Annual ACM Symposium*, 1475–1483. DOI=10.1145/3297280.3297429.

[53] Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., and Woody, C. 2018. Threat Modeling: A Summary of Available Methods.

[54] Nataliya Shevchenko, Frye, B. R., and Woody, C. 2018. THREAT MODELING FOR CYBER-PHYSICAL SYSTEM-OF-SYSTEMS: METHODS EVALUATION.

[55] Wuyts, K., Van Landuyt, D., Hovsepyan, A., and Joosen, W. Effective and efficient privacy threat modeling through domain refinements. In *Haddad, Computing (Hg.) 2018 – The 33rd Annual ACM Symposium*, 1175–1178. DOI=10.1145/3167132.3167414.

[56] Koning, M., Korenhof, P., Alpár, G., and Hoepman, J.-H. The ABC of ABC. - An Analysis of Attribute-Based Credentials in the Light of Data Protection, Privacy and Identity - 2014.

[57] Urueña, M., Muñoz, A., and Larrabeiti, D. 2014. Analysis of privacy vulnerabilities in single sign-on mechanisms for multimedia websites. *Multimed Tools Appl* 68, 1, 159–176.

[58] Sion, L., Wuyts, K., Yskout, K., Van Landuyt, D., and Joosen, W. 2018. Interaction-Based Privacy Threat Elicitation. In *3rd IEEE European Symposium on Security and Privacy Workshops*. *Proceedings : 24-26 April 2018, London, United Kingdom*. Conference Publishing Services, IEEE Computer Society, Los Alamitos, California, 79–86. DOI=10.1109/EuroSPW.2018.00017.

[59] Wuyts, K., Sion, L., Van Landuyt, D., and Joosen, W. IEEE 2019. Knowledge is Power: Systematic Reuse of Privacy Knowledge for Threat Elicitation (IEEE 2019).

[60] Quermann, N., Harbach, M., and Dürmuth, M. 2018. *The State of User Authentication in the Wild*. https://wayworkshop.org/2018/papers/way2018-quermann.pdf. Accessed 27 August 2021.

[61] Ur, B., Noma, F., Bees, J., Segreti, S. M., and Shay, R. 2015. "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab.

[62] Florencio, D. and Herley, C. 2007. A LargeScale Study of Web Password Habits. *Proceedings of the 16th international conference on World Wide Web*.

[63] Raza, M., Iqbal, M., Sharif, M., and Haider, W. 2012. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal,* 19 (4), 439–444.

[64] Wang, X., Yan, Z., Zhang, R., and Zhang, P. 2021. Attacks and defenses in user authentication systems. A survey. *Journal of Network and Computer Applications* 188, 2, 103080.

[65] Veras, R., Collins, C., and Thorpe, J. 2021. A Large-Scale Analysis of the Semantic Password Model and Linguistic Patterns in Passwords. *ACM Trans. Priv. Secur.* 24, 3, 1–21.

[66] Mikalauskas, E. 2021. RockYou2021. Largest password compilation of all time leaked online with 8.4 billion entries. *Cybernews* (Jun. 2021).

[67] Alfredo Salmaso. 2022. DATA PROTECTION ENGINEERING. From Theory to Practice. *European union agency for cybersecurity (ENISA)*.

[68] ULD. 2020. ULD Standard Data Protection Model. A method for Data Protection advising and controlling on the basis of uniform protection goals. Version 2.0b (english version).

[69] Roe, M. 2010 (1997). Cryptography and evidence. Technical Report (May. 2010 (1997)).

[70] NIST Computer Security Division. 2009. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft).

[71] NIST Computer Security Division. 2010. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

[72] Official Journal of the European Communities. 1995. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 (Oct. 1995).

[73] Hanisch, S., Arias-Cabarcos, P., Parra-Arnau, J., and Strufe, T. 2023. *Privacy-Protecting Techniques for Behavioral Biometric Data*. *A Survey*. arXiv:2109.04120v2 [cs.CR] 5 Jan 2023.

[74] Rui, Z. and Yan, Z. 2019. A Survey on Biometric Authentication. Toward Secure and Privacy-Preserving Identification. *IEEE Access* 7, 5994–6009.

[75] Christina Katsini, Yasmeen Abdrabou, George Raptis, Mohamed Khamis, Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Apr. 2020).

[76] FIDO Alliance. 2022. *FIDO2 - FIDO Alliance*. *FIDO Authentication. A Passwordless Vision.* https://fidoalliance.org/fido2/. Accessed 11 May 2023.

[77] Mahfouz, A., Mahmoud, T. M., and Eldin, A. S. 2017. A Survey on Behavioral Biometric Authentication on Smartphones. *Journal of Information Security and Applications* 37, 4, 28–37.

[78] van Tilberg, H. C.A. and Jajodia, S., Eds. 2011. *Encyclopedia of Cryptography and Security*. *Second Edition*. Springer.

[79] Tran, Q. N., Turnbull, B. P., and Hu, J. 2021. Biometrics and Privacy-Preservation. How Do They Evolve? *IEEE Open J. Comput. Soc.* 2, 179–191.

[80] Kim Wuyts, Riccardo Scandariato, and Wouter Joosen. 2014. LIND(D)UN Privacy Threat Tree Catalog. Version 2.0.

[81] Marit Hansen. 2013. FutureID Privacy Requirements. D22.3 Privacy Requirements. Deliverable D22.3.

[82] Marit Hansen, Jensen, M., and Rost, M. 2015. PROTECTION GOALS FOR PRIVACY ENGINEERING 21 May 2015.

[83] Murmann, P. and Fischer-Hubner, S. 2017. Tools for Achieving Usable Ex Post Transparency. A Survey. *IEEE Access* 5, 22965–22991.

[84] Habib, S. M., Mauw, S., Mühlhäuser, M., Vassileva, J., Simone Fischer-Hübner, Julio Angulo, Farzaneh Karegar, and Tobias Pulls, Eds. 2016. *Trust Management X. 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings*. IFIP advances in information and communication technology 473. Springer International Publishing; Imprint: Springer, Cham.

[85] Fischer-Hübner, S. and Berthold, S. 2017. Privacy-Enhancing Technologies. In *Computer and information security handbook*, J. R. Vacca, Simone Fischer-Hbner and Stefan Berthold, Eds. Morgan Kaufmann Publishers an imprint of Elsevier, Cambridge MA.

[86] Daugman, J. 2007. New methods in iris recognition. *IEEE transactions on systems, man, and cybernetics. Part B, Cybernetics : a publication of the IEEE Systems, Man, and Cybernetics Society* 37, 5, 1167–1175.

[87] Daugman, J. 2004. How Iris Recognition Works. *IEEE Trans. Circuits Syst. Video Technol.* 14, 1, 21–30.

[88] Federal Office for Information Security (German BSI). 2022. Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2022-01.

[89] Federal Office for Information Security (German BSI). 2022. Technical Guideline TR-02102-2 – Use of Transport Layer Security (TLS).

[90] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and Mortimore, C. 2014. *Final*. *OpenID Connect Core 1.0 incorporating errata set 1*. Accessed 30 April 2022.

[91] Cavoukian, A. and Stoianov, A. Chapter 26 Biometric Encryption: The New Breed of Untraceable Biometrics. In *Biometrics*. *Theory, Methods, and Applications* 2009.

[92] ENISA. 2016. *Privacy and Security in Personal Data Clouds*. *FINAL REPORT PUBLIC NOVEMBER 2016*.

[93] Galindo, D. and Hoepman, J.-H. 2011. Non-interactive Distributed Encryption: A New Primitive for Revocable Privacy. *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, 81–91.

[94] Lueks, W., Everts, M. H., and Hoepman, J.-H. 2016. Revocable Privacy. Principles, Use Cases, and Technologies. In *Privacy technologies and policy*. *Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers*, B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer and S. Schiffner, Eds. Lecture notes in computer science 9484. Springer, [Cham], 124–143. DOI=10.1007/978-3-319-31456-3_7.

[95] Tsang, P. P., Au, M. H., Kapadia, A., and Smith, S. W. 2007. Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*. *Alexandria, Virginia, USA, October 29 - November 2, 2007*, S. de Di Capitani Vimercati, Ed. ACM, New York, NY.

[96] Chaum, D. and van Heyst, E. 1991. Group Signatures. In *Advances in cryptology - EUROCRYPT '91*. *Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, April 8 - 11, 1991 ; proceedings*, D. W. Davies, Ed. Lecture notes in computer science 547. Springer, Berlin.

[97] Ghadafi, E. 2015. Efficient Distributed Tag-Based Encryption and Its Application to Group Signatures with Efficient Distributed Traceability. In *Progress in Cryptology - LATINCRYPT 2014*, D. F. Aranha and A. Menezes, Eds. 8895. Springer International Publishing, Cham.

[98] Camenisch, J. and Lysyanskaya, A. 2001. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. X. In *Advances in Cryptology -- EUROCRYPT 2001*. *X*. Springer Berlin Heidelberg, Berlin, Heidelberg, 93–118.

[99] Yanjiang, Y., Xuhua, Dingy, Haibing, Luz, and Jian, W. 2013. Self-blindable Credential: Towards LightWeight Anonymous Entity Authentication.

[100] Lindell, A. Y. 2009. *studying the technical aspects of anonymous Internet connections and anonymous authenticati*. https://www.blackhat.com/presentations/bh-usa-07/Lindell/Whitepaper/bh-usa-07-lindell-WP.pdf. Accessed 12 June 2022.

[101] Florencio, D. and Herley, C. ISC 2008: Information Security. One-Time Password Access to Any Server without Changing the Server. In *Information Security*, W. Tzong-Chen, L. Chin-Laung, R. Vincent and L. Der-Tsai, Eds. International Conference on Information Security.

[102] A. Pashalidis and C.J. Mitchell. 2004. Impostor: A Single Sign-On System for Use from Untrusted Devices. IEEE Global Telecommunications Conference : Emerging technologies, applications and services : [conference record] : 29 November-3 December, 2004, Dallas, Texas, Hyatt Regency Dallas at Reunion Hotel.

[103] van der Horst, T. W. and Seamons, K. E. 2007. Simple Authentication for the Web.

[104] Chiasson, S., Stobert, E., Forget, A., Biddle, R., and van Oorschot, P. C. Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism.

[105] Weinshall, D. 2006. Cognitive authentication schemes safe against spyware.

[106] Stajano, F. Pico: No more passwords! *Proc. Security Protocols Workshop 2011, Springer LNCS* Aug 2011.

[107] Mannan, M. and van Oorschot, P. C. 2010. Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers.