Computers & Security 132 (2023) 103353

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Privacy-centered authentication: A new framework and analysis

Antonio Robles-González[a], Patricia Arias-Cabarcos[b], Javier Parra-Arnau[a,*]

[a] Department of Telematics Engineering, Universitat Politècnica de Catalunya, C. Jordi Girona 1–3, E-08034 Barcelona, Spain
[b] Human-Centered IT Security, Paderborn University, Germany

ARTICLE INFO

Article history:
Received 4 April 2023
Revised 8 June 2023
Accepted 15 June 2023
Available online 26 June 2023

Keywords:
User authentication
Authentication schemes
Privacy
Behavioural biometrics
Physiological biometrics

ABSTRACT

The usage of authentication schemes is increasing in our daily life with the ubiquitous spreading Internet services. The verification of user's identity is still predominantly password-based, despite being susceptible to various attacks and openly disliked by users. Bonneau et al. presented a framework, based on Usability, Deployability, and Security criteria (UDS), to evaluate authentication schemes and find a replacement for passwords. Although the UDS framework is a mature and comprehensive evaluation framework and has been extended by other authors, it does not analyse privacy aspects in the usage of authentication schemes. In the present work, we extend the UDS framework with a privacy category to allow a more comprehensive evaluation, becoming the UDSP framework. We provide a thorough, rigorous assessment of sample authentication schemes, including the analysis of novel behavioural biometrics. Our work also discusses implementation aspects regarding the new privacy dimension and current gaps to be addressed in the future research.

1. Introduction

Nowadays, Internet services are ubiquitously reaching nearly every daily-life environment and, with it, so does the number of accounts a user must register and manage. We deal with accessing hundreds of services and devices like computers, wearables, smartphone, tablets, and other smart objects. The most used scheme to authenticate towards these services and devices proving the user's identity is still predominantly password-based (Quermann et al., 2018). Passwords are dominant despite being flawed, insecure (Ur et al., 2015; Florencio and Herley, 2007), and openly hated by users. They are susceptible to various attacks, such as dictionary attacks, brute force, shoulder surfing, phishing attacks, key loggers, or video recording attacks (Raza et al., 2012; Wang et al., 2021). These variety of password attacks and the huge amount of accessible password leaks (Veras et al., 2021; Mikalauskas, 2021) 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. (Joseph Bonneau et al., 2012) 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.[1] While the framework presented by Bonneau et al. (Joseph Bonneau et al., 2012) is analysed and extended with additional criteria by Zimmermann et al. (Zimmermann et al., 2018; Zimmermann and Gerber, 2020), 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 (Deng et al., 2010) (see Table 2), e.g. the required compliance with privacy regulations (Deng et al., 2010; Official Journal of the European Union, P 2016).

The main aim of this work 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 3 additionally considers important privacy publications such as (Deng et al., 2010; Pfitzmann and Hansen, 2010; Salmaso, 2022; ULD 2020) privacy-related security benefits (Joseph Bonneau et al., 2012) and includes behavioural biometrics based on machine learning (ML) (Hanisch et al., 2021). The evaluation comprises the authentication schemes of Bonneau et al. (Joseph Bonneau et al., 2012; Joseph Bonneau et al., 2012)

* Corresponding author.
E-mail address: javier.parra@upc.edu (J. Parra-Arnau).

[1] We will use the term privacy benefits for convenience and comparability reasons with Bonneau et al. (Quermann et al., 2018) instead of privacy properties.

https://doi.org/10.1016/j.cose.2023.103353

and extends the biometrics category with behavioural biometrics (Hanisch et al., 2021) 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. (Joseph Bonneau et al., 2012) 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. This work incorporate a privacy benefit[1] category based on well-known and recognized privacy properties.[1] The UDS framework (Joseph Bonneau et al., 2012) covers 35 authentication schemes and we add behavioural biometrics (Hanisch et al., 2021). The survey of privacy-protecting techniques in (Hanisch et al., 2021) contributes to fulfil the privacy benefits of UDSP framework that we defined to gain a more privacy-proofed authentication scheme than web passwords. We evaluate the authentication schemes from the UDS framework (Joseph Bonneau et al., 2012) and including additionally the behavioural biometrics (Hanisch et al., 2021) 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 this work are summarized as follows:

i We extend the framework originally proposed by Bonneau et al. (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012) and additionally the behavioural biometrics from Hanisch et al. (Hanisch et al., 2021) 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 the paper is organized as follows. Section 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 3. The evaluation of the authentication schemes with the UDSP framework is performed in section 4. Section 5 shows our detailed discussion. Finally, in section 6 concluding remarks are given.

2. Background and related work

In this section we review the state of the art and provide the necessary background knowledge on which our contributions are grounded. We review evaluation frameworks for authentication schemes and analyse their limitations (section 2.1), explain the methodology followed to derive privacy benefits (section 2.2) and introduce advances on biometric schemes (section 2.3).

2.1. Frameworks for the evaluation of authentication schemes and their limitations

UDS framework concept and components

Bonneau et al. (Joseph Bonneau et al., 2012) 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. The authors used the framework to evaluate – as reference – the legacy password scheme, and compare 35 additional authentication schemes. They stated that there are no schemes that fulfil all benefits and therefore are not able to replace the password scheme alone. They emphasise that no examined scheme is *perfect - or even comes close to perfect scores*. For understandability, we offer a brief explanation of the UDS framework terminology.

The authors in (Joseph Bonneau et al., 2012) apply the benefit categories of usability, deployability and security, together comprising 25 benefits for the authentication schemes. 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 5. 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. (Mayer et al., 2016) proposed an extension to UDS with 63 sub features (benefits), based on the 25 features used by Bonneau et al. (Joseph Bonneau et al., 2012). 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,[2] the benefit categories UDS include 48 subfeatures. The core function of ACCESS is to offer a decision support platform for developers and decisionmakers, 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.

They include in the biometrics category fingerprint, iris and voice from (Joseph Bonneau et al., 2012), 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 (only with Keystroke Dynamics and password) and Motion-based (only with KinWrite, writing in space a password) combine two categories used in (Joseph Bonneau et al., 2012) in both schemes, thus with eleven remaining categories.

Zimmermann et al. (Zimmermann et al., 2018) 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 (Mayer et al., 2016) adding 10 schemes to (Joseph Bonneau et al., 2012)) 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. (Mayer et al., 2016).

In a further paper (Zimmermann and Gerber, 2020), the authors conducted a rating of 85 authentication schemes with the objective usability, deployability and security of the paper (Joseph Bonneau et al., 2012), with the purpose of being able to compare objective ratings with subjective user perceptions. The authors (Zimmermann and Gerber, 2020) 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 passwords followed by fingerprint authentication. The security as well as the privacy related security benefits applied

[2] access.secuso.org

in UDS (Joseph Bonneau et al., 2012) were still not improved in (Zimmermann and Gerber, 2020) with respect to objective evaluation, but nonetheless the paper also underpins the maturity of the UDS presented in Bonneau et al. (Joseph Bonneau et al., 2012).

In (Alaca and van Oorschot, 2020), Alaca et al. present an evaluation framework that is like UDS and focusing on single signon (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 (Joseph Bonneau et al., 2012), but not so comprehensive as in (Joseph Bonneau et al., 2012). They add a SSO specific category *design properties* in the sense 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 (Joseph Bonneau et al., 2012) – 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 (Joseph Bonneau et al., 2012).

2.2. Other frameworks

Broders et al. (Broders et al., 2020) 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[3]) offers recommendations for digital authentication of users to federal network-based systems targeted at agencies. NIST's special publication 800–63–3 (P.A. Grassi et al., 2017) 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 (P.A. Grassi et al., 2017). The NIST special publication 800–63B (P.A. Grassi et al., 2017) detailing *authentication and lifecycle management* from (P.A. Grassi et al., 2017) generically considers diverse combinations of applicable authentication factors and authenticators such as secrets or biometrics. The privacy considerations in NIST (P.A. Grassi et al., 2017) are informative and comprise privacy controls and in (P.A. Grassi et al., 2017) 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 (P.A. Grassi et al., 2017) references the NIST special publication 800–53 (Joint Task Force 2020) "Security and Privacy for Information Systems and Organizations" document, which provides very generic standard recommendation covering controls and procedural aspects, alike, but not as identically as ISO27001[4] 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 implementers 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 identifiers. 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.

2.3. Comparative overview of frameworks

Table 1 offers a comparative overview of the previously-mentioned and reviewed frameworks (Joseph Bonneau et al., 2012; Zimmermann et al., 2018; Zimmermann and Gerber, 2020; Joseph Bonneau et al., 2012; Mayer et al., 2016; Alaca and van Oorschot, 2020; Broders et al., 2020). The fact that the UDS framework of the seminal paper of Bonneau et al. (Joseph Bonneau et al., 2012; Joseph Bonneau et al., 2012) has been widely applied and extended (Zimmermann et al., 2018; Zimmermann and Gerber, 2020; Mayer et al., 2016) 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 (Joseph Bonneau et al., 2012), and only a very limited number of privacy benefits or criteria.

Furthermore, we observed, and the authors in (Joseph Bonneau et al., 2012; Joseph Bonneau et al., 2012) suggested to extend the benefit list, because e.g., no dedicated privacy category exists. Thus, we introduce a new group with privacy benefits described in section 3 including the existing three privacy benefits considered in the security benefits.

2.4. From privacy properties to privacy benefits

In *LINDDUN: A privacy threat analysis framework* (Deng et al., 2010), Wuyts et al. systematically guides 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. 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 2, the authors present the privacy properties and related privacy threats for hard and soft privacy. We extend the UDS framework including these privacy properties to become the UDSP framework comprising a new privacy category.

The privacy properties of *unlikability, anonymity,* and *pseudonymity* are built on definitions based on the paper by Pfitzmann et al. (Pfitzmann and Hansen, 2010). *Plausible deniability* is defined based on the dissertation of Michael Roe (Roe, 2010). *Undetectability* and *unobservability* are defined on definitions based on the paper of Pfitzmann et al. (Pfitzmann and Hansen, 2010). The definition of *confidentiality* is based on the draft of NIST (NIST Computer Security Division 2009) and is kept up in the corresponding NIST (NIST Computer Security Division 2010) publication. *Content awareness* is summarized in (Deng et al., 2010) 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 (Official Journal of the European Communities 1995) and repealed by REGULATION (EU) 2016/679 (GDPR) (Official Journal of the European Union, P 2016), whereby

[3] www.nist.gov

[4] www.iso.org/isoiec-27001-information-security.html

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

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. (Joseph Bonneau et al., 2012)	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. (Joseph Bonneau et al., 2012)	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. (Mayer et al., 2016)	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 (Quermann et al., 2018), thus the remaining categories are 11 too.
	The Quest to Replace Passwords Revisited Rating Authentication Schemes	Zimmerman et al. (Zimmermann et al., 2018)	2018	25/UDS	10–12/85	Usability, deployability and security benefits are applied for evaluation. Privacy is not considered. Present results in ACCESS[2], 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. (Zimmermann and Gerber, 2020)	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. (Broders et al., 2020)	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. (Alaca and van Oorschot, 2020)	2020	14/UDSP	1/14	The focus is on usability, deployability, security and fewer on privacy aspects.
Our work: UDSP	PRIVACY-CENTRED AUTHENTICATION: A NEW FRAMEWORK AND ANALYSIS	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 2
LINDDUN privacy properties and privacy threats as defined in (Deng et al., 2010).

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

the later will be considered throughout the present paper. Further principals considered by Hansen et al. (ULD 2020) 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 (Salmaso, 2022) in the context of privacy engineering especially adds – besides the security triad (CIA) of *confidentiality, integrity* and *availability* – in the context of privacy *unlinkability, transparency* and *intervenability.* Thus, we propose to address the absence of a privacy benefit category and associated properties based on (Deng et al., 2010; Official Journal of the European Union, P 2016; Pfitzmann and Hansen, 2010; Salmaso, 2022; ULD 2020; NIST Computer Security Division 2009; NIST Computer Security Division 2010; Official Journal of the European Communities 1995).

2.5. Biometric schemes

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 – amongst others – are fingerprint, face, iris, retina, and hand/palm. Furthermore, Hanisch et al. (Hanisch et al., 2021) 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 (Hanisch et al., 2021) machine learning is assumed for attribute extraction from the behavioural biometric data used for user authentication purposes 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 from the behavioural biometrics. They present for the related privacy goals identity and attribute protection different techniques that try to achieve these goals.

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. (Rui and Yan, 2019) stated or based on classical privacy disclosure, e.g. on *shoulder surfing* in the context of behavioural biometrics such as eye gaze (Katsini et al., 2020). Thus, with the privacy benefits we define we will evaluate the physiological biometric recognition of fingerprint as a representative biometric from (Joseph Bonneau et al., 2012). 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 (Hanisch et al., 2021) 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[5] 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. (Mahfouz et al., 2017), 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.

The traditional authentication systems comprise a user identifier (UID) as assumed in (Joseph Bonneau et al., 2012) so that the user proves towards the verifier the claim that he is making with the usage of the UID. The proof of the 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 to protect biometric templates grounded on cryptography to fulfil the following biometric privacy goals are non-invertibility, revocability and diversity. That is the reason why based on the paper of Tran et al. (Tran et al., 2021) and Rui et al. (Rui and Yan, 2019) we additionally consider further criteria that they propose for privacy preservation of biometrics. These biometric privacy benefits, are unlinkability (UL) (Rui and Yan, 2019), non-invertibility (NI) (Rui and Yan, 2019; Tran et al., 2021), revocability (RV) (Rui and Yan, 2019; Tran et al., 2021) and diversity (DV).

2.6. Privacy benefit category for the UDSP framework

In section 3, we extend the UDS framework of Bonneau et al. (Joseph Bonneau et al., 2012) with the privacy benefit category that comprises privacy properties based on LINDDUN from Wuyts et al. (Deng et al., 2010) and underlying properties e.g. defined by Pfitzmann et al. (Pfitzmann and Hansen, 2010), the LIND(D)UN Privacy Threat Tree catalogue (Wuyts et al., 2014), dissertation of Michael Roe (Roe, 2010), the NIST special publication 800–122 (NIST Computer Security Division 2010), GDPR (Official Journal of the European Union, P 2016), project FutureID (Hansen, 2013), *DATA PROTECTION ENGINEERING* from ENISA (Salmaso, 2022) and the ULD SH Standard Data Protection Model (ULD 2020). The privacy benefits of UDSP framework we assembled offer – in contrast to UDS – significantly strengthen evaluation criteria and are shown below in Table 3:

PB1 to PB3 correspond with the security benefits (S) S9 – S11 from (Joseph Bonneau et al., 2012), 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. PB1 – PB4 constitute privacy benefits usable to evaluate every single authentication scheme individually, with enhanced PB1-PB3 (Joseph Bonneau et al., 2012; Joseph Bonneau et al., 2012) benefits and PB4 defined in this paper. 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 (Joseph Bonneau et al., 2012), 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 (Joseph Bonneau et al., 2012):

A The first three privacy benefits – taken from the seminal paper (Joseph Bonneau et al., 2012) – from PB1 to PB7 were strengthen by us, especially PB3.
B The PB4 and PB7 address privacy aspects related with identifiability and PB7 considers impersonation, namely the extreme of identifiability.
C The PB5 and PB6 are mandatory and a compliance requirement for the service or application to be authorized to go online.

2.7. 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. (Joseph Bonneau et al., 2012). 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.

2.8. 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

[5] https://fidoalliance.org/fido2/

Table 3
Privacy benefits gathered for the new UDSP framework presented in this paper.

Privacy Benefit (PB)	PB Name	Definition	Sources[6] for definition or extension
PB1	*No-Trusted-Third-Party*	UDS (Joseph Bonneau et al., 2012)	
PB2	*Requiring-Explicit-Consent*	UDS (Joseph Bonneau et al., 2012)	(Hanisch et al., 2021)
PB3	*Unlinkable*	UDS (Joseph Bonneau et al., 2012)	(Deng et al., 2010), (Hanisch et al., 2021), (Wuyts et al., 2014), (Laperdrix et al., 2020), (Upathilake et al., 2015)
PB4	*Resilient-to-Identifiability*	UDSP[7]	(Deng et al., 2010), (Pfitzmann and Hansen, 2010), (Hanisch et al., 2021), (Wuyts et al., 2014)
PB5	*Intervenability*	UDSP	(Official Journal of the European Union, P 2016), (ULD 2020), (Hansen, 2013), (Hansen et al., 2015)
PB6	*Transparency*	UDSP	(Deng et al., 2010), (Official Journal of the European Union, P 2016), (Salmaso, 2022), (ULD 2020), (Hansen, 2013), (Murmann and Fischer-Hubner, 2017), (Habib et al., 2016), (Fischer-Hübner and Berthold, 2017)
PB7	*Resilient-to-Impersonation*	UDSP	(Joseph Bonneau et al., 2012), (Hanisch et al., 2021), (van Tilberg and Jajodia, 2011)

[6] Privacy related sources additionally considered for the definition or extension of the privacy benefits.
[7] UDSP = UDSP framework presented in the present paper including amongst others the new defined PB 4 – PB7.

might charge a card without user knowledge or consent)." as defined in Bonneau et al. (Joseph Bonneau et al., 2012). 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.

2.9. PB3 unlinkable

Bonneau et al. (Joseph Bonneau et al., 2012) 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 (Laperdrix et al., 2020; Upathilake et al., 2015). We include the linkability threat of entity (Deng et al., 2010; Wuyts et al., 2014) 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 (Hanisch et al., 2021). This equals protecting the true biometrical data, thus avoiding linkability based on true biometric data or a derived biometric template.

2.10. 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 (Pfitzmann and Hansen, 2010) including plausible deniability as defined in (Deng et al., 2010; Wuyts et al., 2014). We consider the identifiability threat of an entity (Deng et al., 2010; Wuyts et al., 2014) 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 MLbased inference of private information, thus protecting the user's identity and attributes (Hanisch et al., 2021). 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.

2.11. 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 (Hansen, 2013)). According to Hansen et al. (ULD 2020; Hansen et al., 2015) and GDPR (Official Journal of the European Union, P 2016) 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 (Official Journal of the European Union, P 2016), otherwise it would not have gained the authorization to go online.

2.12. PB6 transparency

"*Transparency ensures that all personal data processing including the legal, technical and organisational setting can be understood and reconstructed*", according to FutureID (Hansen, 2013). In our context, we stress for transparency the content awareness of the user (Entity) in accordance with Wuyts et al. (Deng et al., 2010), as well as the existence and communication of a privacy policy (compliance) as stated by Wuyts et al. (Deng et al., 2010) with the goal to "inform the data subject about the system's privacy policy". The privacy policy should at least consider the following GDPR (Official Journal of the European Union, P 2016) articles 12, 16, 17, 18, 20 and 22. The principle of transparency is laid down in

Table 4
Grouping of security benefits to sub-benefits of resilient-to-impersonation.

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

article 5 of (Official Journal of the European Union, P 2016) 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 (Murmann and Fischer-Hubner, 2017; Habib et al., 2016; Fischer-Hübner and Berthold, 2017) differentiate between *ex ante transparency* and *ex post transparency* according to the principles and requirements of the GDPR (Official Journal of the European Union, P 2016). 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 (Official Journal of the European Union, P 2016)). Ex ante transparency is granted as offered (fulfilled) if the verifier/service communicates to 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 (Official Journal of the European Union, P 2016), otherwise it would not have received the authorization to go online.

2.13. 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 encyclopaedia of Cryptography and Security Second Edition (van Tilberg and Jajodia, 2011). 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 (van Tilberg and Jajodia, 2011)). The security benefits S1 to S8 (Joseph Bonneau et al., 2012) in sum focus on robustness, and thus we define sub-benefits in Table 4 and ground our evaluation on the results of UDS in (Joseph Bonneau et al., 2012). A sub-benefit is granted as offered (fulfilled) if all included security benefit were rated in (Joseph Bonneau et al., 2012) as *offers the benefit* or *almost offers the benefit*.

Furthermore, the behavioural biometrics in (Hanisch et al., 2021) 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 (Joseph Bonneau et al., 2012). The evaluation of behavioural biometrics with PB7 – thus with S1-S8 – is also assembled in Table 5. 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 (Joseph Bonneau et al., 2012)). **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 (Joseph Bonneau et al., 2012)). 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 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 (Joseph Bonneau et al., 2012)). **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 (Joseph Bonneau et al., 2012)). 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 (Joseph Bonneau et al., 2012)). In accordance with the argumentation in (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012)). 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 (Joseph Bonneau et al., 2012)). 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 (Joseph Bonneau et al., 2012)). An attacker who steals existing biometric data applying ML can infer private information and compromise the identity and attributes of the user.

Table 5
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. (Joseph Bonneau et al., 2012). *"UDSP" = evaluation with UDSP framework* presented in this paper.

		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	-

2.14. Sample evaluation of authentication schemes with the UDSP framework

We evaluate from (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012) (see the motivation for the corresponding authentication scheme in section 4.1 below). We additionally evaluate promising behavioural biometric from (Hanisch et al., 2021), *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. The authors indicate for the different techniques which privacy goals these try to achieve.

We evaluate the sample authentication schemes (Joseph Bonneau et al., 2012) including behavioural biometric (Hanisch et al., 2021) that we introduced with PB1 – PB7. The results are shown in Table 5.

We evaluate **PB1 – PB3** hybrid for the authentication schemes and fingerprint from (Joseph Bonneau et al., 2012), so that the evaluation result from (Joseph Bonneau et al., 2012) is taken and additionally *in contrast* the evaluation is performed with further UDSP criteria that we add and/or previously were disregarded in (Joseph Bonneau et al., 2012). Afterwards, the evaluation with **PB4** is also hybrid, but considering the previous evaluation for PB3, because both privacy benefits hold a close relation. Table 5 summarizes the evaluation with PB1 – PB4 for the sample authentication schemes evaluated in the paper and others we explored.

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 (Official Journal of the European Union, P 2016), otherwise it would not have received the authorization to go online (see the definition of PB5 and PB6 in section 3). Thus, PB5 Intervenability is offered, if the intervenability possibilities in the PB5 definition grounded on (Official Journal of the European Union, P 2016) 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 justifies privacy by design and by default measures has been performed.

PB7 is applied to the sample authentication schemes including fingerprint biometric from (Joseph Bonneau et al., 2012) considering the evaluation for S1 – S8 (Joseph Bonneau et al., 2012). The newly introduced behavioural biometrics (Hanisch et al., 2021) are evaluated by us with S1 – S8 from (Joseph Bonneau et al., 2012) including ML-related aspects that we added with UDSP (see definition PB7 in section 3). Table 5 also summarizes the evaluation with PB7 of the sample authentication schemes evaluated in the paper and others we explored.

The privacy evaluation in section 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. (Joseph Bonneau et al., 2012) in section 4.1.

2.15. Authentication schemes from UDS framework

This section comprises the evaluation of sample authentication schemes from (Joseph Bonneau et al., 2012) for PB1 – PB4. PB7 is undertaken based on the S1 – S8 evaluation in (Joseph Bonneau et al., 2012). PB5 and PB6 are mandatory to be fulfilled before the service goes live, and thus not evaluated.

2.15.1. 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 (Joseph Bonneau et al., 2012).

PB3 Unlinkable is offered, because in (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012) that the IP communication is untrusted and relevant.

PB4 Resilient-toIdentifiability is offered because for PB3 in (Joseph Bonneau et al., 2012) 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.

2.15.2. YubiKey

In the hardware token category, amongst the four best rated in the category of security benefits in (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012). The button must be pressed, so **PB2 Requiring-Explicit-Consent** is offered (Joseph Bonneau et al., 2012). The user has different tokens for each service, so **PB3 Unlinkable** is offered (Joseph Bonneau et al., 2012). 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 (Joseph Bonneau et al., 2012) 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 to 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.

2.15.3. GrIDsure

In the cognitive category, we selected GrIDSure which belongs amongst the best three rated for security benefits in (Joseph Bonneau et al., 2012), 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 (Joseph Bonneau et al., 2012). **PB2 Requiring-Explicit-Consent** is offered because the user must transcribe the one-time password (Joseph Bonneau et al., 2012). The considerations and evaluation results of the legacy password for **PB3 Unlinkable** and **PB4 Resilient-to-identifiability** are applicable to GRIDsure, and therefore 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.

2.15.4. Biometric fingerprint

We selected the physiological biometric fingerprint because it is marginally the best rated for security benefits in (Joseph Bonneau et al., 2012), 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 (Joseph Bonneau et al., 2012). 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 (Joseph Bonneau et al., 2012). 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 (Joseph Bonneau et al., 2012) solely argue that *physical biometrics are also a canonical example of schemes that are not unlinkable,* also linkable to a (pseudo)-identity.

PB4 Resilient-to-identifiability 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 (Wuyts et al., 2014) used. Only the security benefits S1 and S3 are offered, so that for **PB7 Resilient-to-Impersonation** none of the sub-benefits are offered.

2.15.5. Behavioural biometric

Now follows the evaluation of behavioural biometric from (Hanisch et al., 2021) 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 (Hanisch et al., 2021) for behavioural biometrics we assume the privacy threats identity disclosure, and also to link the behavioural data with the user identity, and attribute disclosure of sensitive attributes for the evaluation. The derived privacy goals (Hanisch et al., 2021) of identity protection and attribute protection are in line with the privacy benefits PB3 and PB4.

The applied attacker model (Hanisch et al., 2021) 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 users̍ 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 (Hanisch et al., 2021) 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 (Hanisch et al., 2021) *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 in the evaluation of gait as a representative case. The covert trait-based biometric evaluation of PB7 is given using heartbeat as a representative scheme. Differences are discussed in the corresponding biometric paragraph.

Furthermore, we comment on the scope of the privacy-protecting techniques (Hanisch et al., 2021) in the context of the data-publishing scenario (Hanisch et al., 2021). The privacy-protecting techniques (anonymization methods) privacy goals in (Hanisch et al., 2021) are *identity protection* and *attribute protection* of behavioural biometrics presented in (Hanisch et al., 2021), 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.”* (Hanisch et al., 2021). The approach in (Hanisch et al., 2021) 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.

2.16. Impact of data-publishing related attacker model

The evaluation of the behavioural biometrics based authentication is done primarily conducted based on the data-publishing (Hanisch et al., 2021) 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 (Hanisch et al., 2021), 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.

2.16.1. Voice

In (Joseph Bonneau et al., 2012), 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 (Joseph Bonneau et al., 2012). **PB2 Requiring-Explicit-Consent** is offered because the user must intentionally pronounce the corresponding challenge response phrase (Joseph Bonneau et al., 2012). By contrast following (Hanisch et al., 2021) 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 (Joseph Bonneau et al., 2012) even for time-variant challenge response phrases. **PB3 Unlinkable** is not offered for voice because in (Joseph Bonneau et al., 2012) 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 also are 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 (Hanisch et al., 2021). 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.

2.16.2. Gait

The gait analysis considers the movement of the human limbs in its typical occurrences, namely trotting, walking, or running (Hanisch et al., 2021). **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 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 (Hanisch et al., 2021). The security benefits **S1** 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** is not offered. For **S3** and **S4,** 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** 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** is not offered. Assuming that biometric data captured as a by-product is something like a phishing attack with less effort, **S7** is not offered. Stolen biometric data could be used for identity and attribute disclosure, so that **S8** is not offered. Consequently, for **PB7 Resilient-to-Impersonation** none of the sub-benefit is offered.

The evaluation of behavioural biometric based on overt traits with PB7 mainly considers 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.

2.16.3. Hand motions

Hand motions include a wide variety of movements comprising signature, mouse movement, keyboard stroke and hand gestures (Hanisch et al., 2021). 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 Unlinkable** and **PB4 Resilient-to-Identifiability** 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 (Hanisch et al., 2021). 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).

2.16.4. Eye-Gaze

In Bonneau et al. (Joseph Bonneau et al., 2012) iris (pattern) recognition based on (Daugman, 2007; Daugman, 2004) primarily considers the physiological aspect of the eye, contrary to this in (Hanisch et al., 2021) the *eye-gaze* is analysed including corneal reflection as well as gaze movement, and thus we evaluate eye-gaze independently from the evaluation in (Joseph Bonneau et al., 2012).

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 Unlinkable** and **PB4 Resilient-to-Identifiability** 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 (Hanisch et al., 2021). None of the **PB7 Resilient-to-Impersonation** sub-benefits are offered (see evaluation of gait).

2.16.5. Heartbeat

The capture of electrocardiogram (ECG) in (Hanisch et al., 2021) 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 previously evaluated behavioural biometrics, **PB3 Unlinkable** and **PB4 Resilient-to-Identifiability** 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 (Hanisch et al., 2021). 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 to 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.

2.16.6. Brain activity

The most prominent application of electroencephalography (EEG) is authentication, personalized game experiences for users and brain-controlled interfaces (Hanisch et al., 2021). 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 Unlinkable** and **PB4 Resilient-to-Identifiability** 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 (Hanisch et al., 2021). 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 to S8 for PB7 is the same as for *heartbeat*.

3. 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 5.1. Next, in section 5.2 the privacy benefit criteria of UDSP are parsed for the authentication schemes to correlate the threats and privacy benefits. Finally, section 5.3 concludes with a consideration of implementation approaches for the mitigation of fundamental threats.

3.1. UDS and UDSP based evaluation of all authentication schemes

Table 5 includes an overview of the evaluation of ***PB1-PB4*** for the authentication schemes from (Joseph Bonneau et al., 2012). The evaluation is twofold for PB1-PB4, first based on UDS (Joseph Bonneau et al., 2012) and, second, on the complete UDSP PB criteria that we assembled, indicated at the top of Table 5 with *Bonneau* or UDSP7. The rating of ***PB1*** and ***PB2*** for authentication schemes from the UDS framework (Joseph Bonneau et al., 2012) is confirmed by us. The ***PB3*** rating by UDS framework (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012), we confirm or even further reaffirm with UDSP. Due to the relevance of **PB3** for ***PB4***, if applying the criteria of ***PB3*** in (Joseph Bonneau et al., 2012), the rating for ***PB4*** is the same as for ***PB3***. Our ratings with UDSP for all schemes from (Joseph Bonneau et al., 2012) are then also not offered for ***PB4. PB5*** and ***PB6*** are mandatory preconditions for every authentication scheme from (Joseph Bonneau et al., 2012) including biometrics from Hanisch (Hanisch et al., 2021) 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 5 based on the extended ***S1 to S8*** from (Joseph Bonneau et al., 2012) 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 5 are also discussed in section 5.2 with the parsing of privacy benefit criteria.

The schemes GrIDsure and YubiKey (Joseph Bonneau et al., 2012) are rated based on UDS as equal for PB1 to 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 with the results presented in Table 5 even with PB3 and PB4 limited to the criteria in (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012), 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 – despite not being the best rated in security benefits (Joseph Bonneau et al., 2012) – 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 (Joseph Bonneau et al., 2012) are rated as not offering PB3 and PB4 based on UDS (Joseph Bonneau et al., 2012) criteria, which we reaffirm with our additional privacy UDSP criteria for PB3 - PB4. Thus, they do not offer any of the PB7 sub-benefits. Privacy consideration based on the UDS criteria in (Joseph Bonneau et al., 2012) remains limited for authentication schemes, as can be seen especially for PB3 and PB4 in Table 5.

3.2. Parsing privacy benefit criteria of UDSP for all authentication schemes

PB1 - PB7 (UDSP) defined in section 3 include additional privacy-related criteria and/or alteration of criteria from (Joseph Bonneau et al., 2012) or depreciated criteria in (Joseph Bonneau et al., 2012) or newly added criteria, as undertaken e.g. for PB3 and PB4 with (Deng et al., 2010; Hanisch et al., 2021; Wuyts et al., 2014) and PB7 with (Hanisch et al., 2021) applicable to the underlying security benefit definitions S1 to S8 from (Joseph Bonneau et al., 2012) in section 3. Furthermore, we replenished the biometric category with behavioural biometrics from (Hanisch et al., 2021), which are voice, gait, hand motions, eye-gaze, heartbeat and brain activity, to analyse a novel subset of upcoming authentication mechanisms. 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.

3.3. UDSP privacy benefit criteria focused on authentication schemes from UDS framework

The rating with UDS PB1 and PB2 criteria for authentication schemes from UDS (Joseph Bonneau et al., 2012) remain as in section 4, because with UDSP only ML-related criteria to PB2 were added and for none in UDS (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012) based on PB3 criteria in (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012) in section 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 (Joseph Bonneau et al., 2012), 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 (Official Journal of the European Union, P 2016) to avoid threats, and if not considered vulnerabilities could be used to compromise the user's 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 (Joseph Bonneau et al., 2012) for PB7 are only relevant for machine learning-based behavioural biometric, and thus no alteration of the consideration of PB7 undertaken above in section 5.1 for authentication schemes from UDS (Joseph Bonneau et al., 2012).

Not offered privacy benefits by authentication schemes from UDS framework (Joseph Bonneau et al., 2012) 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 (Joseph Bonneau et al., 2012). 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 5. Biometrics from UDS (Joseph Bonneau et al., 2012) 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 5 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.

3.4. UDSP privacy benefit criteria focused on behavioural biometric

Now we proceed with the behavioural biometrics (Hanisch et al., 2021) evaluated in section 4 with PB1-PB7 (UDSP). As for the authentication schemes in UDS (Joseph Bonneau et al., 2012) in section 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 to PB4 are shown in Table 5.

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, also an internal attacker (Hanisch et al., 2021).

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 5. Not-offered privacy benefits for UDSP in Table 5 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 (Hanisch et al., 2021), which we consider in the context of the implementation approaches in section 5.4, while questions A) to C) remain for future research.

3.5. Specific biometric privacy benefits and aspects

The nature of both the physiological and behavioural biometric 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 be associated with 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 2.3 are as follows and will be detailed in section 5.3:

- Non-invertibility (NI) (Rui and Yan, 2019; Tran et al., 2021)
- Revocability (RV) (Rui and Yan, 2019; Tran et al., 2021)
- Diversity (DV) (Tran et al., 2021)
- Unlinkability (UL) (Rui and Yan, 2019) (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 2.3).

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 5.3 lists revealed threats and section 5.4 presents the corresponding implementation approaches for authentication schemes including biometrics from UDS (Joseph Bonneau et al., 2012) and anonymization methods (privacy-protecting) approaches from (Hanisch et al., 2021), with the latter focused on the data-publishing scenario assumed for behavioural biometrics in (Hanisch et al., 2021).

3.6. Privacy threats of parsed privacy benefits

The parsed privacy benefits in section 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

3.7. 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 (Hanisch et al., 2021) 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 [(P.A. Federal Office for Information Security (German BSI) 2022; P.A. Federal Office for Information Security (German BSI) 2022)] is recommendable and applicable for design and default settings elicitation. Apart from applying TLS in the standard IP communication of the authentication scheme, one further example – in case DNS is used carefully in the context of authentication schemes – is the usage of DNS over TLS (DoT) or DNS over HTTPS (DoH) (Kantas and Dekker, 2022).

User-controlled cookies: Including default settings to be provided by the service or application provider [(P.A. Federal Office for Information Security (German BSI) 2022; P.A. Federal Office for Information Security (German BSI) 2022)] offering privacy settings by default.

Protection against destructive fingerprinting: Browser fingerprinting comprises collecting throughout the web browser (Laperdrix et al., 2020) 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 (Laperdrix et al., 2020) 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 (P.A. Grassi et al., 2017), thus not being forced to use a real name or other personal user information.

Avoid reuse of the 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 (Sakimura et al., 2014), NIST (P.A. Grassi et al., 2017)) 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 (Official Journal of the European Union, P 2016) 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 (Hanisch et al., 2021) present after a survey privacy-protection techniques (methods) for behavioural biometric evaluated in section 4.2 of this paper. The anonymization methods (privacy-protection techniques) (Hanisch et al., 2021) are *continuous conversion, discrete conversion, feature removal, coarsening, noise injection* and *random perturbation*. The data-publishing scenario (Hanisch et al., 2021) 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 (Hanisch et al., 2021) are identity and attribute protection, which – as still mentioned – are in accordance with PB3 and PB4.

The most anonymization methods were found for voice and EEG (heartbeat) (Hanisch et al., 2021), furthermore, for that traits continuous conversion is the most commonly considered followed by noise injection and feature removal (Hanisch et al., 2021). All traits can be used for both identity and attribute inference (Hanisch et al., 2021). 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 (Hanisch et al., 2023). 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 (Hanisch et al., 2021; Hanisch et al., 2023). All traits can be used for identity and attribute inference, and thus to link users to data, identity theft or private attribute (e.g. gender, age, sex, etc.) inference.

The fulfilment of these privacy goals (Hanisch et al., 2021) 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 (Hanisch et al., 2021) 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.

Table 6
Implementation approaches improving privacy benefits.

	PB1	PB2	PB3	PB4	PB5	PB6	PB7
DeC5	X						X
NI			X	X			X
RV				X	X		X
DV			X	X			

Achieve non-invertibility (NI) comprises intentional alteration of biometric data to generate biometric templates so that this transformation is irreversible (Rui and Yan, 2019; Tran et al., 2021).

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 (van Tilberg and Jajodia, 2011) comprising biometric encryption and cancellable biometrics and are related with untraceable biometrics (Cavoukian and Stoianov, 2009).

Achieve diversity (DV) of biometric data templates, so that with different services and application providers the cancellable biometrics used are different, thus avoiding cross template attacks. The cryptographic primitives are from (van Tilberg and Jajodia, 2011; Cavoukian and Stoianov, 2009) (see *achieve revocability*.)

Avoid disclosure (DeC5) 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 5.

The contribution of the biometric privacy (van Tilberg and Jajodia, 2011) methods to each privacy benefit is shown in Table 6.

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 (Johnstone, 2010), which should include the security aspects of S1 to 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 (Hanisch et al., 2021) above in II.−2 are applicable for threats related with PB7 (S1 to S8) grounded on ML.

3.8. Concluding remarks

At a glance, the evaluation results in Table 5 with UDSP for PB3 unlinkabilty and PB4 Resilient-toIdentifiability obviously bring out that none of the authentication schemes from UDS (Joseph Bonneau et al., 2012) and included behavioural biometric (Hanisch et al., 2021) offer out-of-the-box PB3 and PB4. One outcome of the evaluation of authentication schemes from UDS (Joseph Bonneau et al., 2012) and included behavioural biometric (Hanisch et al., 2021) is that privacy is still not comprehensively considered .

For the web password scheme, besides being the worst rated for security with the UDS framework by Bonneau et al. (Joseph Bonneau et al., 2012), our present evaluation with UDSP additionally reveals that it belongs to the worst rated for privacy (see Table 5). Contrary to this, nearly all hardware tokens and most of the phone-based schemes are the best rated with UDSP for privacy (Table 5) and security in (Joseph Bonneau et al., 2012).

Behavioural biometrics rely on usable traits for authentication purposes, which can be used as a single factor or to complement existing authentication schemes with an additional factor. Both cases bring potential to improve the user experience. However, while these usability improvements make behavioural biometrics a promising authentication mechanism, they come with privacy issues that need to be addressed in practical implementations. Ongoing research in this area (Hanisch et al., 2021) has identified anonymization methods to protect against sensitive inferences on behavioural data, as well as generic biometric template protection techniques (Sandhya and Prasad, 2017), though future research is needed on their practicality.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgement

Javier Parra-Arnau is the recipient of a “Ramón y Cajal” fellowship (ref. RYC2021–034256-I) funded by the Spanish Ministry of Science and Innovation and the European Union – “NextGenerationEU”/PRTR (Plan de Recuperación, Transformación y Resiliencia). This work was also supported by the Spanish Government under the project “Enhancing Communication Protocols with Machine Learning while Protecting Sensitive Data (COMPROMISE)” PID2020–113795RB-C31, funded by MCIN/AEI/10.13039/501100011033, and through the project “MOBILYTICS” (TED2021–129782B-I00), funded by MCIN/AEI/10.13039/501100011033 and the European Union “NextGenerationEU”/PRTR.

References

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

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.

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

Raza, M., Iqbal, M., Sharif, M., Haider, W., 2012. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. World Appl. Sci. J. 19 (4), 439–444.

Wang, X., Yan, Z., Zhang, R., Zhang, P., 2021. Attacks and defenses in user authentication systems. A survey. J. Netw. Comput. Appl. 188 (2), 103080.

Veras, R., Collins, C., 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.

Mikalauskas, E., 2021. RockYou2021. Largest password compilation of all time leaked online with 8.4 billion entries. Cybernews Jun. 2021.

Bonneau, Joseph, Herley, Cormac, van Oorschot, Paul C., Stajano, Frank, 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Sympos. Secur. Priv..

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

Zimmermann, V., Gerber, N., 2020. The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. Int. J. Hum. Comput. Stud. 133, 26–44.

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.

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).

Pfitzmann, A., 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.

Salmaso, Alfredo, 2022. Data protection engineering. From Theory to Practice. Eur. Union Agen. Cybersecur. (ENISA).

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).
Hanisch, Simon, Arias-Cabarcos, Patricia, Parra-Arnau, Javier, Strufe, Thorsten, 2021. Privacy-Protecting Techniques for Behavioral Data: A Survey. Priv.-Protect. Tech. Behav..
Bonneau, Joseph, Herley, Cormac, van Oorschot, Paul C., Stajano, Frank, 2012. Extended version: The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes. Tech. Rep..
Mayer, P., Neumann, S., Storck, D., and Volkamer, M. 2016. Supporting Decision Makers in Choosing Suitable Authentication Schemes.
Alaca, F., van Oorschot, P.C., 2020. Comparative Analysis and Framework Evaluating Web Single Sign-on Systems. ACM Comput. Surv. 53 (5), 1–34.
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.
Grassi, P.A., Garcia, M.E., Fenton, J.L., 2017. Digital Identity guidelines. Revision 3. NIST Special Publication 800-63-3. National Institute of Standards and Technology, Gaithersburg, MD.
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., Theofanos, M.F., 2017. Digital Identity guidelines. Authentication and Lifecycle management. NIST Special Publication 800-63B. National Institute of Standards and Technology, Gaithersburg, MD.
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.
Roe, M. 2010 (1997). Cryptography and evidence. Technical Report (May. 2010 (1997)).
NIST Computer Security Division, 2009. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft).
NIST Computer Security Division, 2010. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).
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).
Rui, Z., Yan, Z., 2019. A Survey on Biometric Authentication. Toward Secure and Privacy-Preserving Identification. IEEE Access 7, 5994–6009.
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).
Mahfouz, A., Mahmoud, T.M., Eldin, A.S., 2017. A Survey on Behavioral Biometric Authentication on Smartphones. J. Inform. Secur. Appl. 37 (4), 28–37.
Tran, Q.N., Turnbull, B.P., Hu, J., 2021. Biometrics and Privacy-Preservation. How Do They Evolve? IEEE Open J. Comput. Soc. 2, 179–191.
Kim Wuyts, Riccardo Scandariato, and Wouter Joosen. 2014. LIND(D)UN Privacy Threat Tree Catalog. Version 2.0.
Marit Hansen. 2013. FutureID Privacy Requirements. D22.3 Privacy Requirements. Deliverable D22.3.
Laperdrix, P., Bielova, N., Baudry, B., Avoine, G, 2020. Browser Fingerprinting. ACM Trans. Web 14 (2), 1–33.
Upathilake, Randika, Li, Yingkun, Matrawy, Ashraf, 2015. Class. Web Brows. Fingerprint. Tech. Accessed 16 July 2022.
Marit Hansen, Jensen, M., and Rost, M. 2015. Protection goals for privacy engineering 21 May 2015.
Murmann, P., Fischer-Hubner, S., 2017. Tools for Achieving Usable Ex Post Transparency. A Survey. IEEE Access 5, 22965–22991.
Habib, S.M., Mauw, S., Mühlhäuser, M., Vassileva, J., 2016. IFIP advances in information and communication technology 473. In: Fischer-Hübner, Simone, Angulo, Julio, Karegar, Farzaneh, Pulls, Tobias (Eds.), Trust Management X. 10th IFIP WG 11.11 International Conference, IFIPTM 2016, Darmstadt, Germany, July 18-22, 2016, Proceedings. Springer International Publishing; Imprint: Springer, Cham.
Fischer-Hübner, S., Berthold, S., 2017. Privacy-Enhancing Technologies. In: Vacca, J.R., Fischer-Hbner, Simone, Berthold, Stefan (Eds.), In Computer and Information Security Handbook. Morgan Kaufmann Publishers an imprint of Elsevier, Cambridge MA.
van Tilberg, H.C.A., Jajodia, S., 2011. Encyclopedia of Cryptography and Security. Second Edition. Springer.
Daugman, J., 2007. New methods in iris recognition. IEEE Trans. Syst. Man Cybernet. Part B Cybernet. Pub. IEEE Syst. Man Cybernet. Soc. 37 (5), 1167–1175.
Daugman, J., 2004. How Iris Recognition Works. IEEE Trans. Circuits Syst. Video Technol. 14 (1), 21–30.
Federal Office for Information Security (German BSI). 2022. Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2022-01.
Federal Office for Information Security (German BSI). 2022. Technical Guideline TR-02102-2 – Use of Transport Layer Security (TLS).
Kantas, E., Dekker, M., 2022. Security and privacy of public dns resolvers. Eur. Union Agen. Cybersecur. (ENISA).
Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., Mortimore, C., 2014. Final. OpenID Connect Core 1.0 incorporating errata set 1 Accessed 30 April 2022.
Hanisch, S., Arias-Cabarcos, P., Parra-Arnau, J., Strufe, T., 2023. Privacy-Protecting Techniques for Behavioral Biometric Data. A Survey [cs.CR] 5 Jan 2023.
Cavoukian, A., Stoianov, A., 2009. Chapter 26 Biometric Encryption: The New Breed of Untraceable Biometrics. In Biometrics. Theory, Methods, and Applications.
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.
Sandhya, Mulagala, Prasad, Munaga V.N.K, 2017. Biometric Template Protection. A Systematic Literature Review of Approaches and Modalities. In: Jiang, R., Almadeed, S., Bouridane, A., Crookes, D., Beghdadi, A. (Eds.), Biometric Security and privacy. Opportunities & challenges in the Big Data Era. Springer, Cham, Switzerland Signal processing for security technologies doi:10.1007/978-3-319-47301-7_14.

Antonio Robles-González received the M.S. (Dipl.-Ing.) in Electrical Engineering with emphasis on Telecommunication from the Universität Dortmund (TU Dortmund), Germany, in 1994. Since 1999 he focuses on Information Security. Inter alia he has a large experience in perimeter security, identification and authentication and multiple aspects related with public key infrastructure (PKI). Currently, he is an information security consultant focusing on the area of ISO 27,001, ISO 27,002, GDPR and BSI-IT-Grundschutz. Currently, he is pursuing the Ph.D. degree on information security in telematics engineering in the area of Smart Services for Information Systems and Communication Networks (SISCOM) at the Universitat Politècnica de Catalunya, Barcelona. His-research interests encompass information security and privacy, focusing on private user-centric management of electronic services in smart communities.

Patricia Arias-Cabarcos is professor of IT Security at Paderborn University (UPB). Prior to UPB, she has been researcher at Karlsruhe Institute of Technology (2019–2021), Humboldt Fellow at Universität Mannheim (2017–2019), and Assistant Professor (2013–2018) at University Carlos III of Madrid (Spain), where she got her PhD in Telematic Engineering in 2013. She has also been visiting postdoctoral researcher at TU Darmstadt and intern at NEC Laboratories Europe in Heidelberg. Her research interests lie in the area of human-centred security and privacy, with a special focus on usable authentication, behavioural data protection, and transparency enhancing technologies.

Javier Parra-Arnau is a Ramón y Cajal researcher at the Universitat Politècnica de Catalunya, Spain. He received the M.S. degree in telecommunications engineering from Universitat Politecnica de Catalunya, Spain, in 2004, and the M.S. and Ph.D. degrees in telematics engineering from the same university, in 2009 and 2013, respectively.