Frictionless Authentication System: Security & Privacy Analysis and Potential Solutions

Mustafa A. Mustafa, Aysajan Abidin, and Enrique Argones Rúa

imec-COSIC KU Leuven
Kasteelpark Arenberg 10, B-3001 Leuven, Belgium
Email: {firstname.lastname}@esat.kuleuven.be

Abstract—This paper proposes a frictionless authentication system, provides a comprehensive security analysis of and proposes potential solutions for this system. It first presents a system that allows users to authenticate to services in a frictionless manner, i.e., without the need to perform any particular authentication-related actions. Based on this system model, the paper analyses security problems and potential privacy threats imposed on users, leading to the specification of a set of security and privacy requirements. These requirements can be used as a guidance on designing secure and privacy-friendly frictionless authentication systems. The paper also sketches three potential solutions for such systems and highlights their advantages and disadvantages.

Keywords–Frictionless authentication; Threat analysis; Security and privacy requirements; Threshold signature; Fuzzy extractors.

I. INTRODUCTION

The widespread adoption of mobile and wearable devices by users results in more personal information being stored or accessed using Personal Devices (PDs) such as smartphones. In addition to enhancing user experience, this also creates new opportunities for both users and Service Providers (SPs). However, this also brings with it new security and privacy challenges for both users and SPs [1]. Usually, these PDs and wearable devices, from now on named Dumb Devices (DDs), have limited computational and interaction capabilities. Nevertheless, users expect a frictionless user experience (making minimum effort) when using their PDs or DDs to access services or resources. Since these devices are small, light, and easy to carry, they are susceptible to loss and theft, and easier to break. And the use of context information (such as the user's current location, his typical behaviour, etc.), which can easily be accessed from these devices, also triggers privacy concerns. Taking into account the users' needs and the associated security and privacy risks of using such devices, the way users are authenticated and granted access to a wide range of on-line services and content becomes more challenging [2].

The current authentication systems [3]–[7] do not provide a satisfactory answer to address these (conflicting) needs: (i) users prefer a single password-less solution, (ii) wearable devices do not offer convenient authentication interface for passwords, (iii) strong biometric authentication solutions score low on usability, or are not suited for continuous authentication with minimal interaction with the user, (iv) certain risk-based techniques work well for desktop and laptops (e.g., device fingerprints), but fall short on mobile devices, and (v) smartphones and wearables are more prone to loss and theft. Thus, there is a clear need for solutions that are tailored towards the user, his devices, the context and sensitivity of his assets.

In this paper, we propose a Frictionless Authentication System (FAS) that allows users to authenticate themselves using their devices to third party SPs without intentionally performing any authentication-related specific actions. We also analyse the security and privacy implications of such systems and propose three potential solutions. The main contributions of this paper are three-fold.

- Firstly, it proposes a novel FAS that allows secure, privacy-friendly as well as frictionless user experience when a user authenticates to SPs.

- Secondly, it performs a threat analysis of and specifies a set of security and privacy requirements for the FAS.

- Thirdly, it proposes three potential high level solutions to achieve secure and privacy-friendly FAS.

The remainder of this paper is organised as follows: Section II discusses related work. Section III proposes a frictionless authentication system. Section IV analyses potential security threats and attacks to the proposed system. Section V specifies a set of security and privacy requirements. Section VI provides a high-level overview of three potential solutions for a secure and privacy-friendly FAS. Finally, Section VII concludes the paper.

II. RELATED WORK

In contrast to conventional challenge-response protocols which use a single prover and verifier, collaborative authentication schemes use a challenge-response protocol with multiple collaborating provers and a single verifier. To mitigate the threat of PDs/DDs being stolen or lost as well as to support a dynamic set of devices as users may not always carry the same set, threshold-based cryptography is used. Threshold cryptography allows one to protect a key by sharing it amongst a number of devices in such a way that (i) only a subset of the shares with minimal size (a threshold $t + 1$) can use the key and (ii) having access to t or less shares does not leak any information about the key. Shamir [8] first introduced this concept of secret sharing, which was later extended to verifiable secret sharing by Feldman [9]. Pedersen [10] used this concept to construct the first Distributed Key Generation (DKG) protocol. Shoup [11] showed how to transform a standard signature scheme such as RSA into a threshold-based variant. In 2010, Simoens et al. [12] presented a new DKG protocol which allows devices not capable of securely storing secret shares to be incorporated into threshold signature schemes. Peeters et al. [13] proposed a threshold-based distance bounding protocol which also takes into account the
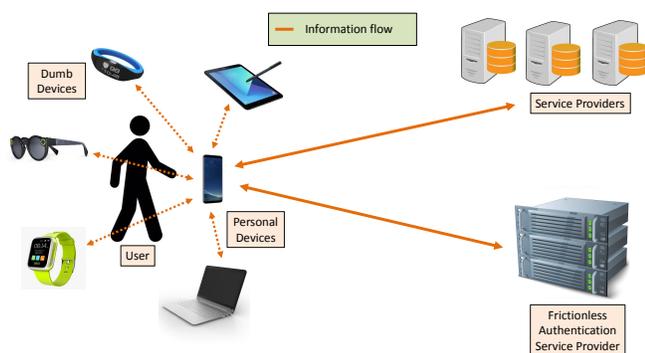
Figure 1. A system model of a FAS.

proximity of devices holding the share to the verifier. An overview of recent developments in continuous authentication schemes is given in [14].

III. FRICTIONLESS AUTHENTICATION SYSTEM

This section details the system model, functional requirements, and interactions amongst entities of a FAS.

A. A System Model

As shown in Figure 1, a system model of a FAS consists of the following entities. A *user* who wants to access various services provided by different *Service Providers (SPs)*. The user also carries or wears a number of personal or dumb devices which she uses to authenticate herself in a frictionless manner, i.e., without intentionally performing any specific authentication-related actions such as entering a password. *Personal Devices (PDs)* are owned by the user and have a secure storage where their owner's secret data such as (parts of) her private key can be stored. The user communicates with SPs via her PDs. *Dump Devices (DDs)* do not have secure storage. They can communicate with PDs, but not necessarily with the SPs. Usually, DDs are wearable which are not paired with the user, and have sensors. Each PD and DD may have one or more *sensors* integrated to measure different data such as location, gait, blood pressure and heart beats. *SPs* are the entities to which users want to authenticate in order to have access to data or services. Usually, this authentication is done by a user digitally signing a challenge sent by the SP. *Frictionless Authentication Service Provider (FASP)* is the SP that assists users in performing a frictionless authentication.

B. Functional Requirements

To be practical and adopted by users, any FAS should be: *frictionless* - the involvement of the user should be minimum while authenticating to various SPs; *adaptive* - the FASP should be able to tailor the multi-modal and -factor authentication scheme to user content data; *collaborative* - the authentication score (AuthScore), i.e., the score which determines how confident the FASP is that the user is who she is claiming to be, should be constructed based on data provided by multiple user's PDs and/or DDs; *flexible* - AuthScore should be constructable using various combinations of user's data collected by user's PDs/DDs; *robust & resilient* - a failure/lack of a single user device should not require any additional effort by the user; and *compatible* - a user should always be able to use conventional authentication methods if desired or needed.

C. Interactions among Entities

Next, we describe the potential message types and interactions among the entities within the FAS.

1) System setup: the FASP performs all the necessary initial steps in order to assist users experience frictionless authentication service. These steps include obtaining the necessary cryptographic keys and certificates.

2) User device setup/registration: the user obtains or generates a public/private key pair and a certificate for the public key. The entire (or part of the) private key is stored in her PDs.

3) User registration: a user provides the SPs with all the necessary information for the service registration such as user identity, public key and certificate.

4) Frictionless authentication: the user proves her identity to a SP without performing any intentional authentication-related actions. It consists of four steps. *Authentication request:* a user informs a SP that she wants to access data or service provided by the SP, or the SP informs the user that she will have to prove her identity. *Identity verification challenge:* the SP sends a challenge to the user to prove her identity. *User AuthScore calculation:* a user's data gathered by the user's PDs and/or DDs are forwarded (via a single user PD) to the FASP which uses these data to compute the AuthScore of the user. Such calculation could be performed on demand (when requested by the SP) or continuously. If the AuthScore is above a certain predefined threshold, the user's private key becomes available for use. Note that the AuthScore can be computed by the FASP on the cloud or locally on the user's PD. See Section IV-D for more details regarding the choice of where the AuthScore is calculated. *Identity verification response:* the user uses her private key to digitally sign the verification challenge and sends the result to the SP. *User identity verification and service access:* the SP checks the user response and if the verification response holds, it grants the user with access to the requested data or services.

IV. THREAT ANALYSIS

We describe the threat model and provide an analysis of the security and privacy threats to the proposed FAS.

A. Threat Model

Users are untrustworthy and malicious. A malicious user might try passively and/or actively to collect and alter the information stored and exchanged within the FAS, in an attempt to gain access to data or services which she does not have permission to access. *PDs are trustworthy (tamper-evident).* We assume that PDs are equipped with security mechanisms to provide access control and protection against data breaches and/or malware. *DDs are untrustworthy.* The data they measure and forward to the FASP might be corrupted. *The FASP is honest-but-curious.* It follows the protocol specification, but it might try to learn and extract unauthorised information about users. *SPs are untrustworthy or even malicious.* They may try to eavesdrop and collect information exchanged within the FAS. Their aim might be to gain access, collect and/or modify information exchanged within a FAS in an attempt to disrupt, and extract confidential information about users, competitors (other SPs) and the FASP itself.

B. Security Analysis

This section analyses the possible security threats to a FAS. The analysis is based on the STRIDE framework [15] which mainly covers security threats.

Spoofing: A malicious entity may attempt to get unauthorised access to services provided by a SP. Such spoofing attacks introduce trust related issues, and may have an economic impact to the SP, especially if the SP provides financial services. Hence, it is important to have thorough user registration procedures and strong mutual authentication.

Tampering with data: A malicious entity may attempt to modify the information stored and/or exchanged within the FAS such as manipulating (i) the data sent from the sensors of a user's devices, (ii) AuthScore and/or (3) user content data such as location. By stating inaccurate information, an adversary may attempt to lower the credibility of users, SPs and the FASP. Therefore, the integrity and authenticity of the data exchanged/stored should be guaranteed.

Information disclosure: A malicious entity may attempt to eavesdrop messages sent within the FAS. By eavesdropping messages one may attempt to retrieve information such as who, when, how often and which services access. Such information is considered as private. Hence, confidentiality of data must be guaranteed. Information disclosure also constitutes a privacy threat to users posing additional risks such as users' profiling.

Repudiation: Disputes may arise when users (do not) access services offered by the SP and claim the opposite. Hence, the non-repudiation of messages exchanged and actions performed by the FAS's entities must be guaranteed, using mechanisms to ensure that disputes are promptly resolved.

Denial-of-Service (DoS): DoS attacks aim to make the FAS inaccessible to specific or all users. An adversary may target a user's PDs/DDs or the FASP in an attempt to make the service unavailable to that specific user or all users, respectively.

Elevation of privilege: An adversary may attempt to gain elevated access to SP resources. For instance, a malicious user may attempt to elevate her privileges from accessing the basic available service to accessing premium service, by, for example, manipulating her AuthScore. Thus, to mitigate these attacks, authorization mechanisms that comply with the principle of least privilege should be deployed.

C. Privacy Analysis

This section analyses the possible privacy threats to a FAS. The analysis is based on the LINDDUN framework [16] which mainly covers privacy threats.

Linkability: An adversary may attempt to distinguish whether two or more Items of Interest (IOI) such as messages, actions and subjects are related to the same user. For instance, an adversary may try to correlate and deduce whether a user has accessed a particular service by a SP at a particular location. Hence, unlikability among IOIs should be guaranteed.

Identifiability: An adversary may attempt to correlate and identify a user from the types of messages exchanged and actions performed within the FAS. For instance, an adversary may try to identify a user by analysing the messages the user exchanges with the SPs. If a user has considerably more PDs/DDs, this may make her more identifiable. Thus, the anonymity and pseudonymity of users should be preserved.

Non-repudiation: In contrast to security, non-repudiation can be used against users' privacy. An adversary may attempt to collect evidence stored and exchanged within the FAS to deduce information about a user. It may deduce whether a user has accessed a particular service at a particular location. Thus, plausible deniability over non-repudiation should be provided.

Detectability: An adversary may try to distinguish the type of IOIs such as messages exchanged amongst FAS entities from a random noise. For instance, an adversary may attempt to identify when a user's PD communicates with a SP. Thus, user undetectability and unobservability should be guaranteed.

Information disclosure: An adversary may eavesdrop and passively collect information exchanged within the FAS aiming at profiling users. For instance, an adversary may attempt to learn the location and availability of a user. Moreover, the user's behaviour may be inferred by a systematic collection of the user's information [17]. For instance, if a SP and/or the FASP collect the data from the user's PDs/DDs and analyse these data, they may infer (i) the user's health related data by collecting their physiological information, (ii) users' activities by analysing the history of service access, and (iii) circles of trust by analysing with whom, when and how often they use the service. Profiling constitutes a high risk for users' privacy. Thus, the confidentiality of information should be guaranteed.

Content Unawareness: A misbehaving FASP may attempt to collect more user information than it is necessary aiming to use such information for unauthorised purposes such as advertisement. For instance, the FASP may only need to know whether a user is eligible to access a service without necessarily the need to identify the user nor the service. Hence, the content awareness of users should be guaranteed.

Policy and Consent Noncompliance: A misbehaving FASP may attempt to collect, store and process users' personal information in contrast to the principles (e.g., data minimisation) described in the European General Data Protection Regulation 2016/680 [18]. For instance, a misbehaving FASP may attempt to (i) collect sensitive information about users such their location, (ii) export users' information to data brokers for revenue without users' consent, and (iii) read users' contacts from their PDs. Thus, privacy policies and consent compliance should be guaranteed.

D. Local versus Cloud-based Frictionless Authentication

The AuthScore, as mentioned earlier, can be computed by the FASP either on the cloud or locally on a PD of a user. The choice will inevitably affect not only the performance of a FAS but also the risk of privacy breaches.

1) Cloud-based AuthScore Calculation: The cloud-based AuthScore calculation requires that all user data gathered by the sensors of the user's PDs/DDs are sent to the cloud where the FASP fuses them to compute the AuthScore of the user. Although outsourcing all the calculations to the cloud should allow the FASP to use more complex fusing algorithms, it also adds an additional risk to users' privacy. As some of these data will be highly user-specific, the confidentiality of these data should be protected. In other words, the communication channels between the user's PD and the FASP servers should be encrypted so that no external entity has access to these data. Also, user's privacy should also be protected from the FASP. Having access to these data may allow the FASP to

extract sensitive information about the user, thus profiling users. Ideally, the FASP should not have access to the user data in the cleartext, but operate only with encrypted data. This could be achieved if the user data are encrypted with a cryptographic scheme that supports homomorphic properties such as the Paillier cryptosystem [19]. Moreover, the FASP should not be able to identify the SP to whom the user authenticates. Otherwise, the FASP would be able to track the user online over the different data/services the user accesses.

2) Locally AuthScore Calculation: In contrast to the cloud-based solution, calculating the AuthScore on the user's PD is more privacy-friendly as no user data leave the PD. However, on one hand, given that the computational resources of PDs are usually much lower than the ones of the cloud, the complexity of the fusion algorithm will be limited. On the other hand, as the user data is not sent to the FASP services, the fusing algorithm running on the user's PD could use much more fine-grained user data. Having access to such data should allow the FASP to use less complex fusion algorithms but yet achieve results comparable to the ones achieved with more complex fusion algorithms used in cloud-based AuthScore calculation.

V. Security and Privacy Requirements

Based on the threat analysis, this section specifies a set of security and privacy requirements for the proposed FAS.

A. Security Requirements

To mitigate the aforementioned security threats, the following security requirements needs to be satisfied.

Entity Authentication assures to an entity that the identity of a second entity is the one that is claiming to be. It aims to mitigate spoofing attacks.

Integrity ensures that the information stored and exchanged within the FAS have not been altered. It aims to mitigate tampering with data attacks. Integrity is achieved with the use of hash functions, MACs and digital signatures.

Confidentiality ensures that only the intended entities are able to read the user data stored and transferred within the FAS. It aims to mitigate information disclosure attacks. Confidentiality can be achieved with the use of encryption schemes, e.g., symmetric, asymmetric and homomorphic encryption schemes.

Non-repudiation is achieved when an entity cannot deny her action or transaction. It aims to mitigate repudiation attacks (disputes). Non-repudiation can be achieved with the use of digital signatures, timestamps and audit trails.

Availability ensures that the resources of the FAS are available to legitimate users. It aims to mitigate DoS attacks. To safeguard availability, network tools such as firewalls, intrusion detection and prevention systems should be used.

Authorisation ensures that an entity has the correct access. It aims to mitigate elevation of privilege attacks. For authorisation, access control mechanisms, e.g., access control lists and role based access control, should be used, following the principle of least privilege for user accounts.

B. Privacy Requirements

To mitigate the specified privacy threats, the following privacy requirements need to be satisfied.

Unlinkability ensures that two or more IOIs such as messages and actions are not linked to the same user [20]. It aims to mitigate linkability attacks. Unlinkability can be achieved with the use of pseudonyms as in [21], anonymous credentials [22] and private information retrieval [23].

Anonymity ensures that messages exchanged and actions performed can not be correlated to a user's identity. It aims to mitigate identifiability attacks. Anonymity can be achieved using Mix-nets [24] and multi-party computation.

Pseudonymity ensures that a pseudonym is used instead of a user's real identity. As anonymity, it aims to mitigate identifiability attacks. It can be achieved by using unique and highly random data strings as pseudonyms.

Plausible deniability over non-repudiation ensures that an adversary cannot prove that a user has performed a specific action and operation. It aims to mitigate non-repudiation privacy threats. However, non-repudiation service should be provided when necessary such as when a user needs to be hold accountable for cheating and/or misbehaving, as in [25].

Undetectability and unobservability ensures that messages exchanged and actions performed by a user cannot be distinguished from others. It aims to mitigate detectability attacks, and can be achieved by using Mix-nets and dummy traffic [24].

Confidentiality is a privacy requirement too (see Sect. V-A).

Content Awareness aims to raise users' awareness by better informing them of the amount and nature of data they provide the FASP. It aims to mitigate the content unawareness threats, and can be achieved with the use of transparency enhancing technologies, e.g., privacy nudges [26] and dashboards [27].

Policy and consent compliance ensures the compliance of the FAS with legislations, e.g., the European General Data Protection Regulation 2016/680 [18]. It aims to mitigate the policy and consent non-compliance privacy threats, and can be achieved with the use of Data Protection Impact Assessments [28] and Privacy Impact Assessments [29] for the FAS.

VI. Potential Solutions

In this section, we propose three possible solutions for a FAS and analyse their pros and cons with respect to their security and privacy properties. The authentication is achieved using a digital signature, wherein the private key is held by the user (i.e., the user device) and the verifier (i.e., the SP) challenges the user to prove that she holds the private key by asking her to sign a challenge. However, the solutions differ from each other in the way the private key is handled.

A. CASE 1: using no Advanced Crypto

1) High-level Description: The first straightforward solution is to password protect the private key. However, this has the obvious drawback of frequent user interaction, as the user has to provide her password every time there is an authentication request. Similarly, protecting the private key using biometrics, e.g., the private key is generated from user biometrics or a local biometric verification is used to grant access to the private key, has the same drawback as the password protected solution. Nevertheless, the user should always be able to authenticate herself using passwords/biometrics. To make it frictionless, one can incorporate behaviometrics/contextual data such as gait, location, or other sensor data. In this case, access to the private key is granted if the behaviometric/contextual data collected from PDs and DDs provide sufficient authentication score; see Figure 2 for a high level description. As can be seen, this solution does not use any advanced cryptographic techniques.
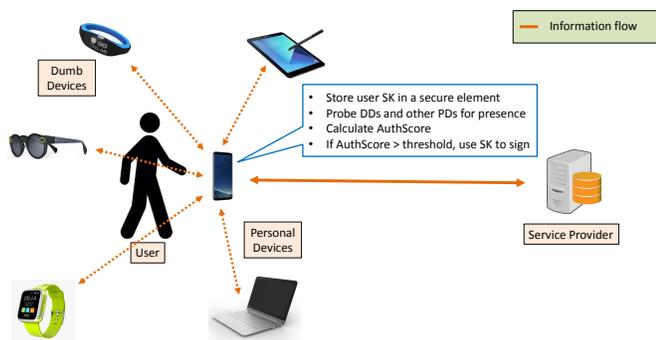
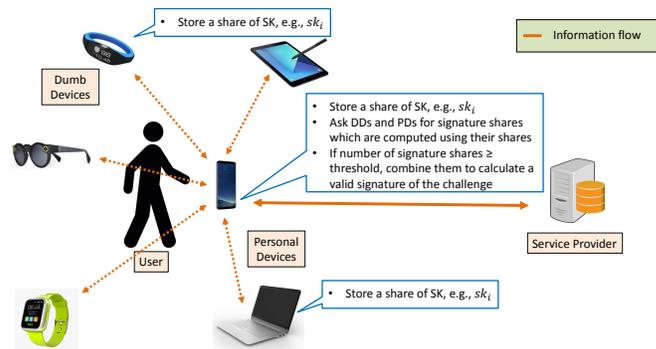Figure 2. CASE 1: FAS using no advanced crypto.

Figure 3. CASE 2: FAS using threshold signature.

2) Advantages: As this solution does not require implementation of any advanced cryptographic algorithms other than the already implemented digital signature algorithm, it is *easy to set-up and implement*. It also has a *simple access control mechanism* as it only requires device presence check and calculation of the AuthScore by matching sensor data.

3) Disadvantages: As the key is stored on a single device, this results in *a single point of failure*. Moreover, there are potentially *higher risks for privacy breach* depending on where the AuthScore is calculated based on the behaviometric/contextual data and whether these data are protected.

B. CASE 2: using Threshold Signature

1) High-level Description: The disadvantages of the previous solution can be addressed by using threshold cryptosystems, in particular, threshold signatures [11], as depicted in Figure 3. In this case, during the enrolment stage, the secret key (i.e., the private key) is shared among the user devices using a threshold secret sharing scheme, so each device stores only a share of the secret key. During the authentication stage, the devices jointly computes a signature on the authentication challenge. In particular, each device computes only one signature share and provides this share to the gateway device, e.g., the user's PD. A valid signature can be computed only if the number of signature shares provided is greater than or equal to a predefined threshold value.

2) Advantages: As the secret key is shared amongst the user devices and never stored as one piece on any user device, *no key is stored as whole*. Furthermore, the key is not even reconstructed. Only if a sufficiently large enough number of shares (more than the predefined threshold) are stolen, then the key can be reconstructed. Also, as the key is not stored in its entirety, this solution has *no single point of failure*.

3) Disadvantages: As threshold signatures are more involved than the traditional digital signatures, they may incur some *performance issues in practice*. In addition, even though the key is never stored as a whole, it can be reconstructed using sufficient number of shares. Therefore, *shares need to be protected*. This might be an issue especially for DDs as they usually do not have the capacity for secure storage, which brings us to our third solution described next.

C. CASE 3: using Threshold Signature and Fuzzy Extractors

1) High-level Description: In the previous solution, shares of the secret key are stored in users' DDs. As these DDs

usually do not have secure storage, storing sensitive data on them (i) might be undesirable and (ii) can pose a threat to security of the FAS, in general. To overcome this limitation, one option is to use Fuzzy Extractors (FEs) to allow DDs to recover their shares of the secret key, thus avoiding the storage of sensitive data on DDs (see Figure 4). FEs use noisy data from a source and Helper Data (HD) to recover a fixed discrete representation. Using mechanisms such as the uncoupling procedure presented in [30], where the binary representation bound in the fuzzy commitment is independent of the fuzzy source, it is possible to make a FE to produce a given key, producing HD which does not disclose any information about the produced key. In our case, each DD uses a FE to obtain its corresponding key share, and the HD are stored in the user's PD. During the enrolment stage, a key share and the associated HD is generated for each DD. The key share is discarded, while the HD is stored in the PD. During the authentication stage, the PD provides the DDs with their corresponding HD. Then, DDs use the collected sensory data and the provided HD to recover the corresponding key share by using the FE. This generated key share is then used to jointly sign the challenge.

2) Advantages: The online generation of the key shares during the authentication stage means that *key shares are not stored* at different devices, thus the security threat associated to their storage simply disappears. In addition, *the stored HD is unlinked with the key shares*, thus avoiding information disclosure and improving the security of the system.

3) Disadvantages: This solution relies on the use of FE, where performance issues and the nature of the stored HD have to be taken into account when evaluating the risks. Although the HD is not linked to the produced key shares, *the stored HD is linked to the biometrics/behaviometrics of the user*, thus providing information about the user's biometric data, which could be used to link the user amongst services, or to obtain information useful for spoofing attacks. Therefore, the HD have to be protected and stored in a secure element in the PD. There might also be some *performance issues* as FEs differ from authentication methods based on fixed factors in the associated uncertainty in their outputs. They are subject to possible errors in genuine attempts (False Rejections) and impostor attempts (False Acceptances). In our case, several DDs will collaborate to generate a response, and $t + 1$ of them need to successfully recover their respective share. These considerations should be kept in mind, when generating the HD, to properly decide the working point for different FEs.
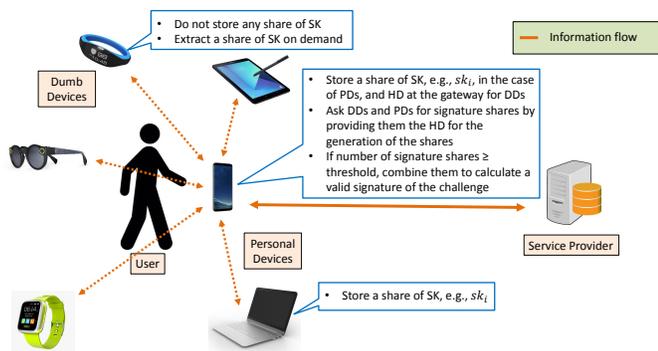
Figure 4. CASE 3: FAS using threshold signature and fuzzy extractors.

VII. Conclusions and Future Work

In this paper we have presented a comprehensive security and privacy analysis of a FAS, starting from a set of functional requirements. Three different approaches for a secure and privacy-friendly FAS have been analysed, integrating possession-based and behavioural authentication factors in a flexible authentication scheme based on threshold signatures. The main advantages and disadvantages of the different approaches have been analysed. Although all the three analysed solutions meet the main security and privacy requirements, we recommend the solution that combines threshold signature with fuzzy extractors, as no key material is stored at user devices. As future work, we will design a concrete protocol for a FAS that combines threshold signature with fuzzy extractors, and evaluate its performance in terms of computational complexity, communication costs, and authentication rates.

Acknowledgment

References

[1] S. Sagiroglu and D. Sinanc, "Big data: A review," in Int. Conf. on Collaboration Technologies and Systems (CTS'13), 2013, pp. 42–47.

[2] T. Van hamme, V. Rimmer, D. Preuveneers, W. Joosen, M. A. Mustafa, A. Abidin, and E. Argones Rúa, "Frictionless authentication systems: Emerging trends, research challenges and opportunities," in the 11th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'17). IARIA, 2017.

[3] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Privacy preserving multi-factor authentication with biometrics," in the 2nd ACM Workshop on Digital Identity Management (DIM'06), 2006, pp. 63–72.

[4] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in IEEE Symposium on Security and Privacy (SP'12), 2012, pp. 553–567.

[5] E. Grosse and M. Upadhyay, "Authentication at scale," IEEE Security Privacy, vol. 11, no. 1, Jan 2013, pp. 15–22.

[6] R. P. Guidorizzi, "Security: Active authentication," IT Professional, vol. 15, no. 4, July 2013, pp. 4–7.

[7] D. Preuveneers and W. Joosen, "SmartAuth: dynamic context fingerprinting for continuous user authentication," in the 30th ACM Symposium on Applied Computing (SAC'15), 2015, pp. 2185–2191.

[8] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, 1979, pp. 612–613.

[9] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in SFCS '87, ser. SFCS '87, 1987, pp. 427–438.

[10] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in CRYPTO'91, ser. LNCS, vol. 576. Springer, 1992, pp. 129–140.

[11] V. Shoup, "Practical threshold signatures," in EUROCRYPT'00, ser. LNCS, vol. 1807. Springer, 2000, pp. 207–220.

[12] K. Simoens, R. Peeters, and B. Preneel, "Increased resilience in threshold cryptography: Sharing a secret with devices that cannot store shares," in International Conference on Pairing-Based Cryptography, ser. LNCS, vol. 6487. Springer, 2010, pp. 116–135.

[13] R. Peeters, D. Singelee, and B. Preneel, "Toward more secure and reliable access control," IEEE Pervasive Computing, vol. 11, no. 3, 2012, pp. 76–83.

[14] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," IEEE Signal Proc. Mag., vol. 33, no. 4, 2016, pp. 49–61.

[15] Microsoft. The STRIDE threat model. Accessed Aug, 2017. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[16] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," Requirements Engineering, vol. 16, no. 1, 2011, pp. 3–32.

[17] Uber. New App Features and Data Show How Uber Can Improve Safety on the Road. Accessed July, 2016. [Online]. Available: https://newsroom.uber.com/safety-on-the-road-july-2016/

[18] Regulation 2016/680 of the European Parliament and of the Council. Accessed Aug, 2017. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG

[19] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in EUROCRYPT'99, ser. LNCS, vol. 1592. Springer, 1999, pp. 223–238.

[20] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (v0.34). tech. rep." pp. 1–98, 2010.

[21] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: An anonymous multi-user protocol," in IEEE Int. Conf. on Smart Grid Communications, 2014, pp. 939–945.

[22] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in CRYPTO'04, ser. LNCS, vol. 3152. Springer, pp. 56–72.

[23] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," Journal of the ACM, vol. 45, no. 6, 1998, pp. 965–981.

[24] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Com. of the ACM, vol. 24, no. 2, 1981, pp. 84–90.

[25] I. Symeonidis, A. Aly, M. A. Mustafa, B. Mennink, S. Dhooghe, and B. Preneel, "Sepcar: A secure and privacy-enhancing protocol for car access provision," in the 22nd European Symposium on Research in Computer Security (ESORICS'17), ser. LNCS, vol. 10493. Springer, 2017, pp. 475–493.

[26] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor, "Privacy nudges for social media: an exploratory facebook study," in the 22nd Int. Conf. on World Wide Web (IW3C2'13), 2013, pp. 763–770.

[27] M. Nebel, J. Buchmann, A. Ronagel, F. Shirazi, H. Simo, and M. Waidner, "Personal information dashboard: Putting the individual back in control," Digital Enlightenment, 2013.

[28] E. Commission. Test phase of the Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Metering Systems. Accessed Aug, 2017. [Online]. Available: http://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems

[29] D. Wright and P. De Hert, Privacy impact assessment. Springer Science & Business Media, 2011, vol. 6.

[30] A. Abidin, E. Argones Rúa, and R. Peeters, "Uncoupling biometrics from templates for secure and privacy-preserving authentication," in the 22nd Symposium on Access Control Models and Technologies (SACMAT'17). ACM, 2017, pp. 21–29.