Project no. 826278

SERUMS

Research & Innovation Action (RIA)

SECURING MEDICAL DATA IN SMART-PATIENT HEALTHCARE SYSTEMS

Initial Report on Security Metrics and Authentication Policies D5.1

Due date of deliverable: 30th June 2019

Start date of project: 1st January 2019

Type: Deliverable
WP number: WP5

Responsible Institution: UCY
Editor and editor's address: Marios Belk (belk@cs.ucy.ac.cy)
Partners Contributing: ZMC, SOPRA, FCRB

Approved by:
Reviewers: David Vidal (FCRB)
Euan Blackledge (SOPRA)

Version 1.0

Project co-founded by the European Commission within the Horizon H2020 Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Release History

Release No.	Date	Author(s)	Release Description/Changes made
V0.01	07/01/2019	Marios Belk (UCY), Andreas Pitsillides (UCY)	Defined TOC and added initial Executive Summary
V0.02	08/03/2019	Marios Belk (UCY), Christos Fidas (UCY), Elias Athanasopoulos UCY), Andreas Pitsillides (UCY)	Added initial literature review on state-of-the-art user authentication schemes
V0.03	18/03/2019	Marios Belk (UCY), Christos Fidas (UCY), Andreas Pitsillides (UCY)	Added literature review on personalization approach in user authentication
V0.04	29/03/2019	Marios Belk (UCY), Christos Fidas (UCY)	Extended the literature review with user authentication healthcare systems
V0.05	19/04/2019	Marios Belk (UCY), Christos Fidas (UCY), Andreas Pitsillides (UCY)	Report on security and usability metrics
V0.1	30/04/2019	Marios Belk (UCY), Christos Fidas (UCY), Andreas Pitsillides (UCY)	Finalize literature review analysis on user authentication and metrics
V0.2	15/05/2019	Marios Belk (UCY), Christos Fidas (UCY)	Report of results of the semi-structured interviews for Organization 1
V0.3	24/05/2019	Marios Belk (UCY), Christos Fidas (UCY)	Report of results of the semi-structured interviews for Organization 2
V0.4	31/05/2019	Marios Belk (UCY), Christos Fidas (UCY)	Report of results of the semi-structured interviews for Organization 3
V0.5	04/06/2019	Marios Belk (UCY), Christos Fidas (UCY), Elias Athanasopoulos UCY), Andreas Pitsillides (UCY)	First draft of the deliverable
V0.6	20/06/2019	Marios Belk (UCY), Christos Fidas (UCY), Elias Athanasopoulos UCY), Andreas Pitsillides (UCY)	Beta version of the deliverable
V0.7	27/06/2019	David Vidal (FCRB) Euan Blackledge (SOPRA)	Version after partners' comments
V0.8	28/06/2019	Marios Belk (UCY), Christos Fidas (UCY), Andreas Pitsillides (UCY)	Pre-final version for final check
V1.0	29/06/2019	Marios Belk (UCY), Christos Fidas (UCY), Andreas Pitsillides (UCY)	Release candidate

SERUMS Consortium

Partner 1	**University of St Andrews**
Contact Person	Name: Vladimir Janjic, Juliana Bowles Email: vj32@st-andrews.ac.uk, jkfb@st-andrews.ac.uk
Partner 2	**Zuyderland Medisch Centrum**
Contact Person	Name: Cindy Wings Email: c.wings@zuyderland.nl
Partner 3	**Accenture B.V.**
Contact Person	Name: Bram Elshof, Wanting Huang Email: bram.elshof@accenture.com, wanting.huang@accenture.com
Partner 4	**IBM Israel Science & Technology Ltd.**
Contact Person	Name: Michael Vinov Email: vinov@il.ibm.com
Partner 5	**Sopra-Steria**
Contact Person	Name: Andre Vermeulen Email: andreas.vermeulen@soprasteria.com
Partner 6	**Université Catholique de Louvain**
Contact Person	Name: Axel Legay Email: axel.legay@uclouvian.be
Partner 7	**Software Competence Centre Hagenberg**
Contact Person	Name: Michael Rossbory Email: michael.rossbory@scch.at
Partner 8	**University of Cyprus**
Contact Person	Andreas Pitsillides Email: andreas.pitsillides@ucy.ac.cy
Partner 9	**Fundació Clínic per a la Recerca Biomèdica**
Contact Person	Name: Santiago Iriso Email: siriso@clinic.cat

Table of Contents

Executive Summary

Securing Medical Data in Smart Patient-Centric Healthcare Systems (SERUMS) is a research project supported by the European Commission (EC) under the Horizon 2020 program. This is the first deliverable of *Work Package 5: "Authentication and Trust"*. The leader of this work package is UCY, with involvement from the following partners: ZMC, IBM, SOPRA, UCL, and FCRB. The objective of this work package is focused on designing and developing a user-centric authentication system aiming to deliver a secure, personalized and usable authentication mechanism to each user's preference and interaction device, in order to preserve security and improve usability. The primary goals are to: *i)* provide high levels of security to confirm the identity of each user and accordingly authorize access to certain parts of personal and/or medical data in the system; and *ii)* improve the usability levels of the user authentication mechanisms by increasing memorability of selected secrets and task execution efficiency and effectiveness.

This deliverable, entitled *"D5.1. Initial Report on Security Metrics and Authentication Policies"* describes the outcome and overall methodology that has been applied for the analysis, elicitation, validation and documentation of the security measurements, metrics and policies of the Serums user authentication system. The Serums user authentication system is designed and developed following a User-Centered Design (UCD) cycle [ISO 9241-210]. The deliverable starts with a literature review on state-of-the-art research in the area of user authentication. The literature review was focused on knowledge-based, token-based, biometric-based authentication systems, and their combination within multi-factor authentication systems, important security metrics and authentication policies aiming to derive current best practices and guidelines in user authentication. We further conducted an analysis of existing works on human-centered approaches in user authentication as well as related works focused on user authentication within healthcare systems in order to identify the peculiarities of user authentication in this domain.

The deliverable further describes the methodology, analysis and main findings of a series of semi-structured interviews that were conducted with various stakeholders at the three end-user organizations aiming to identify current user authentication practices, policies and procedures followed at large-scale healthcare organizations in Europe. Nine (9) stakeholders with various backgrounds and roles (Chief Information Security Officers, Enterprise Architects, Department Managers) from three (3) different countries participated in the semi-structured interviews. The interviews were focused around two main topics related to user authentication policies and procedures applied at each end-user organization, and security and technical aspects of the user authentication scheme.

The aforementioned tasks helped us to specify the initial evaluation measurements, metrics and authentication policy of the Serums user authentication system as well as initial personas and use-case scenarios. In the deliverable, we describe the initial personas of typical end-users of the Serums system that were derived from the discussions in the semi-structured interviews, as well as preliminary use-case scenarios based on the proposed user authentication paradigm. We further present the security and usability measurements and metrics, the proposed adaptive and adaptable authentication policy, as well as how the metrics affect the Success Indicators (SI) and Key Performance Indicators (KPI) of the project.

1 Introduction

1.1 Role of the Deliverable

The role of this deliverable is threefold: *i)* to conduct a thorough literature review analysis on user authentication focusing on knowledge-, token- and biometric-based user authentication systems, as well as state-of-the-art security and usability metrics; *ii)* to identify the current policies, practices and procedures followed at the three end-user organizations; and *iii)* to identify and define the security and usability metrics, and policy of the Serums user authentication system. The outcome of the deliverable constitutes the basis for the design, development and evaluation of the Serums authentication system.

1.2 Relationship to Other SERUMS Deliverables

Deliverable	**Relation**
D2.2: Initial Software for Storage, Access, Blockchain and metadata Extraction for Smart Patient Health Records	The defined metrics of D5.1 will be used as input in the Smart Patient Health Records
D2.3: Report on Refined Specification of Smart Patient Health Record Format	The defined metrics of D5.1 will be used as input in the refined specification of the Smart Patient Health Records
D5.2: Software on the Initial Verified User Authentication System	The outcome of D5.1 will be used as an essential first step towards an iterative software development cycle of the user authentication scheme.
D5.3: Software on the Refined Verified User Authentication Scheme	D5.3 will include the refined security metrics and user authentication policies. Hence, the outcome of D5.1 will be used as a basis for the refined security metrics and policies of the user authentication scheme
D6.1: Report on Initial Smart Health Centre System Software	The outcome of D5.1 will be used as input for the integrated smart healthcare system software
D7.1: Initial Requirements Analysis and Success Metrics	The security and usability metrics defined in D5.1 are utilized as part of D7.1 Key Performance Indicators.
D7.2: Report on Serums Change Plan	The outcome of D5.1 is determined and affects the project's change plan.
D7.3: Initial Report on Use Cases and Evaluation	The security and usability metrics defined in D5.1 are essential for the use cases and evaluation studies.

1.3 Structure of this Document

Following the current introductory chapter, the rest of the document is structured as follows: *Chapter 2* provides an overview of user authentication and the main tasks involved in a typical user authentication workflow. *Chapter 3* describes a thorough literature review on state-of-the-art research in user authentication covering its three main categories (knowledge-, token-, biometric-based). *Chapter 4* describes state-of-the-art security and usability metrics in user authentication. *Chapter 5* describes existing user authentication practices in healthcare, as well as the method and results of a series of semi-structured interviews performed at the three healthcare end-user organizations of the

Serums consortium aiming to identify the current policies, practices and procedures of user authentication. *Chapter 6* lists the suggested user authentication types, an initial conceptual design of the proposed user authentication system that will be utilized in Serums as well as initial personas and use-case scenarios with typical end-users of the Serums user authentication system. Furthermore, Chapter 6 describes the initial security and usability metrics for measuring the validity of the approach along with the suggested Serums adaptive and adaptable user authentication policy. *Chapter 7* concludes the deliverable.

2 User Authentication Overview and Workflow

User authentication is a cornerstone of security in today's interactive systems [70]. Derived from the Greek word *αὐθεντικός*; meaning real or genuine, user authentication is the act of confirming that a person interacting with a service is who she or he claims to be. The term relates to human-computer interactions and differentiates from machine authentication which entails processes to authenticate machines. During an authentication task, users are required to provide specific information in order to prove their identity. This can either be a secret password, a specific object such as a credit card, or biometric information of the user such as fingerprints. User authentication is currently achieved primarily with the use of text-based passwords [71, 76, 86] in which users typically provide a username and secret password which entails a sequence of alphanumeric characters only known to the user.

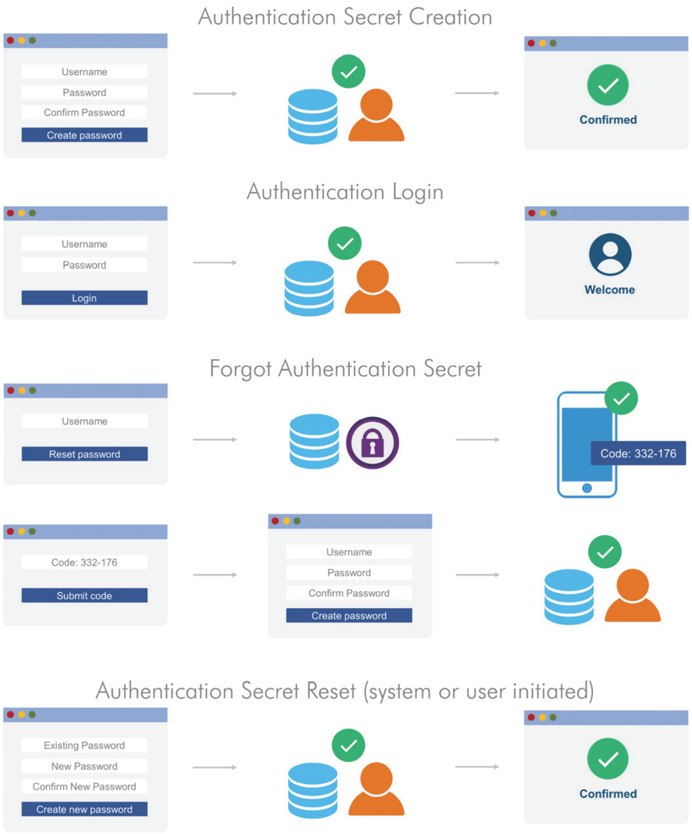


Figure 1. Main processes for user authentication.

A user authentication system consists of four main processes (Figure 1): *a) authentication secret creation* in which users create their main secret key that will be used for authentication (*i.e.*, secret password, pattern, fingerprint scan, etc.); *b) authentication login* in which users need to provide the created authentication factor in order to prove their identity and eventually access sensitive information; *c) forgot authentication secret* which is a process initiated by users after they have forgotten or lost their authentication secret. In this case, users need to provide specific information to identify themselves in order to proceed with the authentication factor reset process; and *d) authentication secret reset* which is a process to recreate the users' authentication factor. The process can be initiated either by the system (*e.g.*, after a specific period of time -30 days- to increase the security of the system), or initiated by the user.

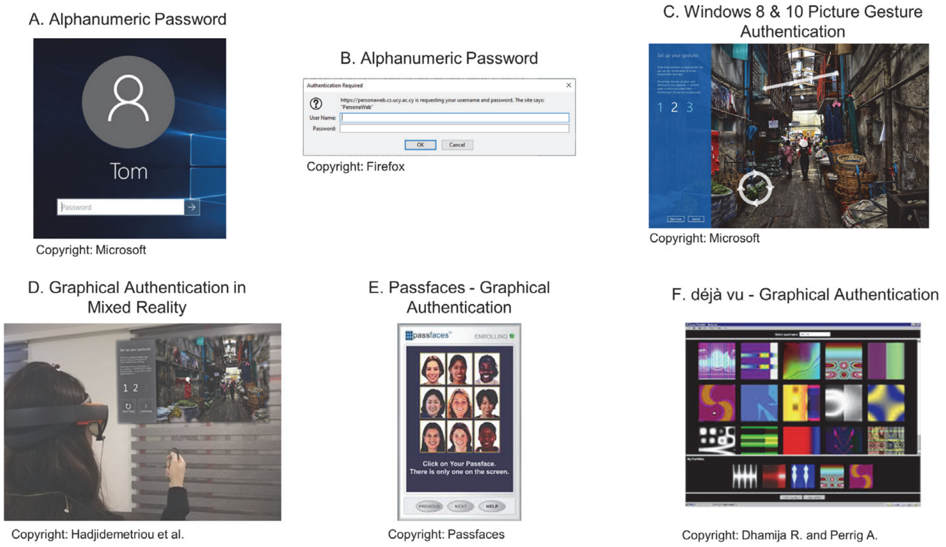
3 State-of-the-art Research in User Authentication

Numerous user authentication schemes are currently deployed which can be classified into *knowledge-based* (*what the user knows*, *e.g.*, secret passwords, pictorial keys, sketches) [71], *token-based* (*what the user has*, *e.g.*, credit cards) [72], and *biometric-based* (*what the user is*, *e.g.*, fingerprint, interaction behavior) [73]. Knowledge-based authentication schemes are widely used today since: *a)* they are easy, fast and inexpensive to implement [71]; and *b)* they don't entail the security and privacy flaws found in tokens (*e.g.*, loss or theft of credit card [74]) and in biometrics (*e.g.*, users' fingerprints can be extracted from the objects they touch [75]). Multi-factor authentication is an authentication method to prove the authenticity of the user by combining different factors (*i.e.*, knowledge, token, biometric).

3.1 Knowledge-based Authentication Mechanisms

Knowledge-based authentication mechanisms require from the user to memorize specific information (*e.g.*, password, passphrase, PIN code, sequence of images, etc.). Figure 2 and Figure 3 illustrate examples of knowledge-based user authentication mechanisms. Text-based passwords are the dominant means for authentication and are currently utilized in most computing systems worldwide since they are familiar to most of the users, and easy and inexpensive to implement [76, 80]. Nevertheless, passwords have always been criticized about their security flaws [81]. Various studies have been reported that underpin the necessity for secure and usable authentication mechanisms [82-87]. The literature reveals many proposals for improving password security, such as educating and influencing users to create more secure passwords [88, 89, 90], improving existing recall-based password approaches with recognition of text [91], enforcing the creation of secure passwords through password policies [83, 85, 92], automatically generating secure passwords and mnemonic passphrases [93, 94], providing guidance and feedback during password creation [95], and assisting users to create memorable passwords, *e.g.*, through image-based mnemonic techniques [96]. Furthermore, password managers [97, 98] have been proposed to minimize users' cognitive load.

A great amount of research on knowledge-based authentication mechanisms has focused on the design and implementation of graphical authentication schemes (see [71] for a comprehensive review). This is further strengthened by the technological shift of current computing systems toward touch-based devices in which entering textual information (in this case, text-based passwords) on touch-based keyboards is a demanding task [99]. In addition, graphical authentication mechanisms claim to preserve security and improve usability and memorability of user authentication as they leverage the vast capacity and capabilities of the human visual memory system [71, 100, 101] and are memorable over extended periods of time [102]. Principally, graphical authentication mechanisms require from a user to enter an authentication key represented by images in a specific sequence. Graphical authentication schemes can be classified into three categories according to the memory task involved in remembering and entering the authentication key; *recall-based*, *cued-recall-based* and *recognition-based authentication*.



A. Alphanumeric Password

Copyright: Microsoft

B. Alphanumeric Password

Copyright: Firefox

C. Windows 8 & 10 Picture Gesture Authentication

Copyright: Microsoft

D. Graphical Authentication in Mixed Reality

Copyright: Hadjidemetriou et al.

E. Passfaces - Graphical Authentication

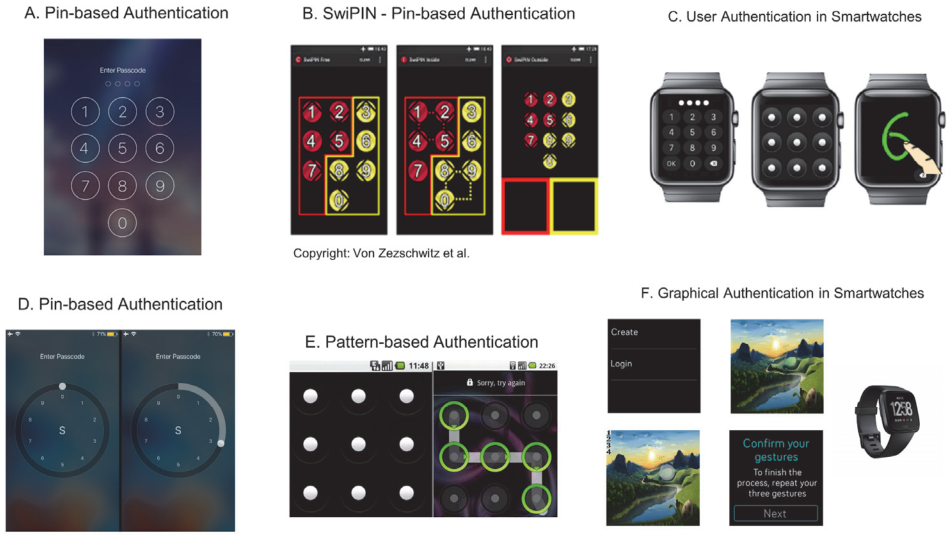
Copyright: Passfaces

F. déjà vu - Graphical Authentication

Copyright: Dhamija R. and Perrig A.

Figure 2. Knowledge-based user authentication mechanisms.

Recall-based graphical authentication mechanisms require that users remember information and reproduce a secret drawing on a static image as their authentication key. The first recall-based authentication mechanism proposed was Draw-a-Secret (DAS) [103] where users draw their authentication key on a two-dimensional grid. Variations of the first DAS system that aimed to improve some of its usability issues include BDAS [104] which added background images to the existing DAS to encourage the creation of stronger authentication keys, YAGP (Yet Another Graphical Password) [105] that modified DAS to accept approximately correct drawings, Passdoodle [106] that added additional factors, such as, pen color, number of pen strokes, drawing speed for the matching process to add variability of drawings, Pass-Go [107] where users draw their authentication key using grid intersection points, as well as commercial applications of Pass-Go, like Google Android mobile phones for unlocking screens by drawing an authentication key on a 3x3 grid.



A. Pin-based Authentication

B. SwiPIN - Pin-based Authentication

Copyright: Von Zezschwitz et al.

C. User Authentication in Smartwatches

D. Pin-based Authentication

E. Pattern-based Authentication

F. Graphical Authentication in Smartwatches

Figure 3. Knowledge-based user authentication mechanisms.

Cued-recall graphical authentication mechanisms require users to identify specific locations on a static image and are intended to reduce the memory load on users since specific cues are utilized in order to assist the recall of information. The dominant cued-recall authentication system is PassPoints [108] and its variations [71]. In PassPoints, users click anywhere on a picture, with a tolerance metric defined around each click-point to avoid the need for pixel-perfect entries in the future. Variations include Persuasive Cued Click Points [109] that assists users to select random authentication keys by highlighting a random part of the picture where the click must occur. Recently, Bulling et al. [110] have proposed a gaze-based authentication scheme that supports users in selecting secure gaze-based graphical passwords. In particular, the proposed authentication scheme uses saliency maps to mask out those areas of the image most likely to attract visual attention with the aim to increase the security of gaze-based cued-recall graphical authentication mechanisms.

Recognition-based graphical authentication mechanisms require that the user creates an authentication key by selecting and memorizing specific images, and then recognize the images among decoys to authenticate. The most popular and extensively researched recognition-based graphical authentication system to date is Passfaces [78] that uses human faces as part of the authentication key. Variations have been proposed that use different content in images, like the Story system [111] that uses everyday objects, places and people as the authentication key, and ImagePass [112] that utilizes single-object images as the authentication key. Another recent work proposed the Tiles system [113] in which users are assigned a target image and subsequently asked to select segments of that image with the aim to help mitigate the threat from verbal sharing and observation attacks.

To this end, knowledge-based user authentication mechanisms, and more specifically text-based passwords and graphical authentication mechanisms entail various design features. Based on the aforementioned analysis, we categorize important and widely used features as follows: *i)* Design type (*e.g.*, text-based, picture-based); *ii)* interaction design type (*e.g.*, selecting images/text *vs.* typing text *vs.* touching visual images/text objects *vs.* drawing patterns); *iii)* image type (faces, abstract or single-object); *iv)* number of user-selected images/characters for the authentication key; *v)* number of decoy images illustrated during graphical authentication; *vi)* the policy of the authentication key (*e.g.*, allow or not using the same image multiple times in a single key); and *vii)* the procedure for graphical authentication (*e.g.*, showing more decoy images in one screen *vs.* showing less decoy images in multiple screens) [118].

3.2 Token-based Authentication Mechanisms

A plethora of authentication materials (*e.g.*, ATM cards, RSA token, corporate badge, etc.) is utilized by many people for accessing services and environments that require high level of assurance in their daily lives (*e.g.*, bank accounts, corporate environments, etc.) [8, 9, 13]. These materials are typically used in two-factor authentication (2FA) [10-12] as a factor that the user *has* in possession, which is coupled with a factor that the user *knows* (*e.g.*, PIN or password) or a factor that the user is (*e.g.*, fingerprint) [5, 9]. Numerous solutions have been proposed in the literature, which can be broadly categorized as *traditional* or *hybrid* [5]. Figure 4 illustrates examples of token-based user authentication mechanisms.

Traditional Solutions

The traditional solutions rely either on hardware devices that are used for a single-purpose (*i.e.*, identification) or on unique user's characteristics (*i.e.*, a biometric) [5]. Examples include the One-Time

Password (OTP) tokens, the Challenge/Response tokens, and the Public Key Infrastructure (PKI) tokens.

OTP Tokens. OTP tokens are devices that generate passwords intended for single-use, often composed of up to 10 digits. They come in two types: *i)* event-based, which generate a new password at the press of a button on the device; and *ii)* time-based, which generate a new password that is valid only for a certain amount of time (*e.g.*, for 30 seconds). Their operation relies on the principles of symmetric cryptography; a secret is stored in the device securely, which is also known on the server that validates users when they attempt to login. Examples of OTP tokens include: VASCO Digipass [1], RSA SecurID [2], and Feitian OTP Tokens [3].

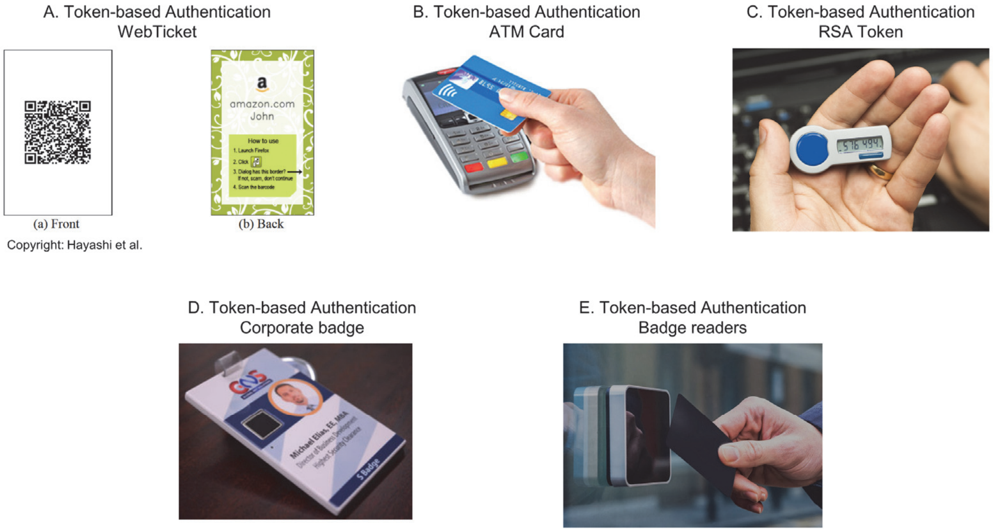

A. Token-based Authentication
WebTicket
(a) Front
(b) Back
amazon.com
John
How to use
Copyright: Hayashi et al.
B. Token-based Authentication
ATM Card
C. Token-based Authentication
RSA Token
D. Token-based Authentication
Corporate badge
E. Token-based Authentication
Badge readers

Figure 4. Token-based user authentication mechanisms.

Challenge/Response Tokens. Similar to OTP tokens, the operation of Challenge/Response tokens relies on symmetric cryptography. Unlike OTP tokens that are mainly used for simple authentication, the main use of the challenge/response tokens is to authenticate transactions (*e.g.*, to approve money transfer). This is achieved by assigning to the user a "challenge" (*i.e.*, to enter some sequences of digits on the token), and then using these as input parameter to a cryptographic algorithm that generates the "response" (*i.e.*, another sequence of digits). The user is then requested to return a valid response to the authentication party in order to be authenticated. Examples of challenge/response tokens include VASCO Digipass [1], SafeNet SafeWord GOLD [4] and Feitian OTP Tokens [3].

PKI Tokens. Unlike OTP and Challenge/Response tokens, the PKI tokens rely on the principles of public key cryptography. Almost all PKI tokens rely on a smart card integrated circuit with an on-board co-processor capable of performing public key cryptography operations. The most common forms of hardware PKI tokens are the smart cards and the USB dongles. The authentication process relies on challenge/response protocols that aim to prove that the user owns the private key that belongs to its corresponding public key which is usually stored in an X.509 certificate [5].

Hybrid Solutions

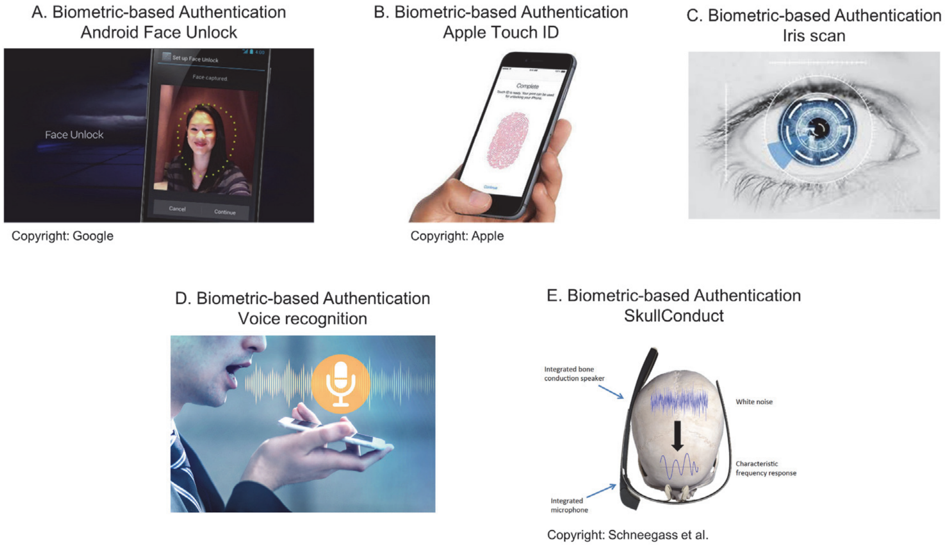
The hybrid solutions rely on devices owned by the user that are used for non-single purpose and are usually combined with software running on these devices [5]. Examples include the SMS OTP and OTP applications.

SMS OTP. In the modern world, the fact that the vast majority of people have a mobile phone capable of SMS allowed SMS OTP to become a superior yet cost-effective method for 2FA. The first authentication factor is commonly the traditional username/password. The second authentication factor is an OTP generated by the authentication server and sent to the user's mobile phone as an SMS text message. The user is requested to first enter the correct login credentials, and then provide additional proof of identity through the SMS OTP. However, it is not evident whether SMS OTP is a real two-factor authentication [6, 7], considering that a (temporary) theft of user's mobile phone is a concern given that the SMS is displayed even if the device is locked.

OTP Applications. Another technology advancement is the emergence of OTP mobile applications. These applications run on modern smartphones and serve the purpose of the traditional OTP tokens. However, the secret resides and is processed in software on the smartphone. Nowadays, most OTP token manufacturers provide also an application version of their tokens which is interfaced with the same authentication server that is used for the hardware tokens.

3.3 Biometric-based Authentication Mechanisms

Biometric authentication is the security process that aims to automatically recognize individuals based on their unique physiological (*e.g.*, fingerprint, face, iris etc.) or behavioral (*e.g.*, voice, signature, gait etc.) attributes [14, 15]. A biometric system performs a one-to-one comparison of a captured biometric data with the confirmed authentic data that is stored in a database and if both samples match then the authentication is confirmed. Numerous biometric modalities have been proposed in the literature [16]. Figure 5 illustrates examples of biometric-based user authentication mechanisms.



A. Biometric-based Authentication
Android Face Unlock

Copyright: Google

B. Biometric-based Authentication
Apple Touch ID

Copyright: Apple

C. Biometric-based Authentication
Iris scan

D. Biometric-based Authentication
Voice recognition

E. Biometric-based Authentication
SkullConduct

Copyright: Schneegass et al.

Face Unlock
Integrated bone conduction speaker
White noise
Characteristic frequency response
Integrated microphone

Figure 5. Biometric-based user authentication mechanisms.

Voice Biometrics

Today's smart electronic devices include a microphone, which enables voice recognition to be used as a factor for Multi-Factor Authentication (MFA) [17, 18]. Voice relies on both physiological and behavioral characteristics for the synthesis of the produced sound. Although the physiological characteristics remain unchanged over time, the behavioral characteristics may change due to various factors (*e.g.*, aging, changes in emotional states and health conditions) [38]. Furthermore, technological advancements may allow systems to recognize speakers, as well as mimic their voices, suggesting that voice might be an inappropriate primary means of authentication [19, 20].

Facial Recognition

Facial recognition is considered the most natural method of biometric identification [54] and refers to the technique that automatically identifies or verifies an individual from a digital image [27]. The initial steps of facial recognition technologies relied on the landmark picture analysis [21]. Then, the three-dimensional face recognition has been introduced, which requested the individual to move the head in specific ways during the process of authentication [22, 23]. Recent advancements of the technology allowed for the recognition of the actual expressions of the individual [24]. However, to support facial recognition technology, the system must be equipped with an output device and a camera [25]. Moreover, recent works revealed that state-of-the-art face recognition systems can be fooled by transformed images printed on paper [55, 56].

Ocular-Based Methodology

The complex texture of the iris contains distinctive information that can be used for personal recognition [14]. The iris recognition is based on mathematical pattern-recognition techniques that analyze video images of one or both irises [26], without requiring the person to be close to the capture device. Another technique that falls under this methodology is retina analysis, which is based on the unique pattern that is formed by the blood vessels at the back of the eye [27]. The currently deployed iris-based recognition systems exhibit sufficient accuracy and speed of processing [14], however, for the deployment of such methodologies, the systems must be equipped with high quality capture devices and accurate mathematical recognition techniques [28].

Hand Geometry

Hand geometry refers to the biometric that identifies users based on the analysis of the physical shape of their hands [9] and is commonly used for access control and employee attendance. In the early days of hand geometry, pegs were used to capture the image of the hand, however, such methods suffer from poor usability [29]. Technological advancements allowed for better user experience through the use of flatbed scanners [30] and conventional cameras [31], capable of capturing the image without requiring the user to place the hand at a certain position. This is performed through the hand geometry reader devices that can capture and process an individual's hand geometry and then produce a biometric template which is used to verify identity.

Vein Recognition

Vein Recognition is another method of biometric authentication which relies on pattern-recognition techniques of the finger vein picture [32]. Hand vein geometry is another approach that leverages on vein matching and is based on the fact that the vein pattern can be distinguishable for various individuals [27]. More advanced and complex devices allow for contactless palm vein recognition by considering hand movements [33, 34]. However, recent works revealed that vein recognition approaches are still prone to spoofing attacks [35, 36].

Fingerprint-based Recognition

Fingerprint-based Recognition is the most extensively studied and widely deployed method of biometric authentication [37], and it is based on capturing and comparing the impression of the friction ridges of all or any part of the finger [27]. Despite the ease of use and speed of operation, the general public exhibited medium acceptability to acquisition of fingerprint solutions [38] mainly due to insufficient recognition accuracy [37], as well as security and privacy concerns [9, 37, 39]. In general, despite the high potential of integration of these methods [42], it is recommended to avoid using them as a standalone means of authentication since fingerprints can be easily fabricated [40, 41].

Thermal Image Recognition

Thermal Image Recognition techniques rely on the infrared (IR) thermal imaging, which utilizes IR thermal sensors capable of capturing images based on either the IR reflectance or the IR radiation emittance [43]. High resolution thermal images can capture anatomical and physiological face information (*e.g.*, blood flow, facial vascular network), which can be used as a unique biometric feature [43, 44, 45]. However, such authentication solutions suffer from limitations mainly due to user conditions that could influence the perceived images [46, 47].

3.4 Additional Factors for User Authentication

Geographical Location

Location-based authentication leverages on device's and user's geographical location for deciding whether access to a service could be granted [48, 49, 50]. Considering the importance of location information within various security solutions, prior works proposed location-aware authentication and access control approaches [57, 58, 59]. In the context of authentication, location information can be used as either a factor in a multi-factor authentication process or as a security policy [60]. Most location-based authentication systems rely on the Global Positioning System (GPS) signals for the detection of location, however, such an approach is susceptible to various types of attacks (*e.g.*, GPS jamming, GPS spoofing) [51]. Therefore, it is recommended to use multiple location sources (*e.g.*, GPS in combination with the wireless network cell ID) [52]. Furthermore, prior work has shown that GPS is not only susceptible to hardware attacks, but also on GPS devices at the data level [53].

Behavior Detection

Behavior recognition refers to the techniques that identify users based on behavioral characteristics. Recent works have shown the feasibility of such an identification by considering the tapping on the smartphone screen [61, 62]. Since the typing pattern is unique for each individual [63-65], such a solution can be easily integrated into any text-input authentication method. Other works investigated the use of accelerometer data captured from handheld and wearable devices [66, 67]. For example, accelerometer data could be used for identifying an individual based on the gait pattern which is considered almost impossible to be faked by other individuals [68]. A recent work in [69] has shown the feasibility of authenticating users based on a personalized model of users' movements during gait periods. Behavior detection could also be used for in-vehicle authentication through monitoring of the following driver-related features [143, 144]: *i) vehicle-specific behavior* such as speed sensor, brake pressure sensor, etc. [145, 146]; and *ii) human factors* such as calls made, music played, etc. [147].

Beam-Forming Techniques

Beam-forming refers to the techniques used in signal processing that allow signals to be transmitted or received in a directional way [148, 149]. In the context of telecommunication, the most widely adopted techniques are the Radio-frequency Identification (RFID) and Near-Field Communication (NFC) [150]. Recent works in physical-layer security suggested using wireless Multiple-Input Multiple-Output (MIMO) solutions for locating the source of signal, which might be an important advancement for the validation of the token on user body [151-153].

Electrocardiographic (ECG) Recognition

ECG recognition is an emerging biometric modality which utilizes electrocardiograms (*i.e.*, recordings of the electrical activity of the heart) for the identification and authentication of individuals [154]. ECG data could be collected through ECG sensors (*e.g.*, embedded in smartwatch or activity trackers) in non-intrusive ways [155]. The use of ECG for authentication purposes has two main benefits: *i)* ECG signals are difficult to counterfeit, and *ii)* ECG signals exist in all living individuals [154]. However, for the deployment of ECG in biometric systems there are several issues that need to be addressed first, such as heart rate variability, changes in emotional states and health conditions, sensor placement, and time-varying nature of the ECG signal [156].

Electroencephalographic (EEG) Recognition

EEG recognition is another emerging technique in the context of biometric systems which utilizes electroencephalograms (*i.e.*, recordings of the electrical activity of the brain) for the identification and authentication of individuals [157, 158]. In the early days of EEG, the data capturing was performed only in clinical settings using invasive probes under the skull. Today, it is possible to collect data using headset devices [159]. Using EEG data as a biometric modality has the advantages of being difficult to mimic, impossible to observe, unique, and non-intrusive [157, 160]. However, there are still open issues and challenges for the deployment of brainwave authentication, such as changes in emotional states and health conditions, usability, electrode placement paradigm, multimodality, and customization of EEG device [161].

Deoxyribonucleic acid (DNA) Recognition

Human cell lines have been extensively studied in the literature, mostly in reverse genetic approaches and vitro disease models [162]. Although they could be used as a source of unique DNA fingerprinting information [40], the process is time-consuming and expensive. Furthermore, DNA contains sensitive data, therefore, privacy concerns may arise [14]. However, DNA-based solutions may be used for pre-authorizing users' access in facilities that require high security, in combination with other authentication factors [9].

3.5 Human-centered Approaches in User Authentication

A recent streamline of research has focused on the influence of specific human, technology and design factors affecting knowledge-based user authentication task performance. Main aim of these works is to understand human-computer interactions in such realms, and further apply that knowledge in designing personalized and usable authentication mechanisms. Table 1 summarizes some state-of-the-art research works that investigated the effects of several factors (human, technology, design) on user authentication.

An early study of Brostoff and Sasse [123] has investigated the usability of traditional password schemes and graphical authentication (Passfaces). Results of the study have shown that overall, graphical authentication needs more time to complete, however graphical authentication has higher success rate compared to text-based and users authenticate less frequently on graphical authentication than text-based passwords. In Wiedenbeck et al. [108], a longitudinal study was run aiming to investigate the usability of traditional passwords and a new graphical authentication scheme (PassPoints). Results have shown that users created the graphical key faster and with less difficulties than the password key during system registration. However, login times and failed attempts with the graphical authentication scheme were higher than the password scheme.

Nicholson et al. [114] suggested personalizing the user authentication type based on age differences. In particular, this research work investigated age differences (young users and older adults) in various user authentication types (*i.e.*, personal identification number (PIN) and graphical authentication), regarding the number of attempts needed to authenticate. Results revealed that young users need fewer attempts to authenticate than older adults on both graphical and PIN. Furthermore, young users do not have significant differences in number of attempts between graphical and PIN, whereas older adults need fewer attempts on graphical compared to PIN.

Belk et al. [115, 116] investigated how users' cognitive styles (Verbal and Imager) and cognitive processing abilities' (limited and enhanced) affect task completion performance between text-based and graphical authentication mechanisms. In particular, results revealed that overall, users authenticate faster with text-based passwords compared to graphical authentication, with Verbal users being faster than Imager users, whereas Imager users perform more efficiently in graphical authentication mechanisms, compared to Verbal users. Furthermore, users with enhanced cognitive processing abilities authenticate faster and need fewer attempts in graphical authentication than users with limited abilities, whereas in text-based passwords, no significant differences exist between limited and enhanced cognitive abilities' groups. Such results suggest personalizing user authentication tasks by adapting the type of user authentication (textual or graphical) based on the users' cognitive processing styles and abilities.

Katsini et al. [117] investigated how different visual behaviors of individuals with varying cognitive strategies affect the security aspects of graphical user authentication across device types. Results revealed differences on key strength and complexity, as well as on gaze-based entropies between users with different cognitive strategies, which can be used for the design of user-adaptive graphical user authentication schemes.

Ma et al. [118] investigated how cognitive disabilities of users (users with Down syndrome *vs.* neuro-typical users) affect task performance and user preference of text-based passwords and graphical authentication mechanisms. Results revealed that overall, text-based passwords are completed faster and with less attempts than graphical authentication. Users with Down syndrome need more time to create and enter a username and password than neuro-typical users. Furthermore, persons with Down syndrome are able to quickly learn and memorize the graphical authentication key suggesting that graphical authentication mechanisms could be a valid alternative for users with Down syndrome. In addition, the research suggests that Web service providers should offer personalized authentication functions that allow the users to select their preferred authentication types.

In a similar approach, Forget et al. [119] proposed a work-in-progress authentication scheme for enabling users to choose the preferred user authentication mechanism (*e.g.*, text or graphical) instead of providing a one-size-fits-all user authentication type.

From the technology perspective, recent research investigated how several technology factors affect user authentication task performance and user behavior, such as device type, interaction design and virtual keyboard layout [120, 121]. The main findings of the studies suggest that user authentication mechanisms should be personalized based on the interaction device type. In particular, von Zezschwitz et al. [120] recently investigated the effect of device type (desktop computers, tablets, smartphones) on password entry performance, users' password choice and users' security behavior. Results revealed that password input in mobile devices is slower than desktop computers and that users choose easy and fast to enter passwords for mobile devices com-pared to desktop computers. Schlöglhofer et al. [121] compared also different authentication types (PIN, text-based passwords and graphical authentication) regarding device unlock function duration on smartphones. Results suggest that PINs are the fastest to enter, graphical authentication is considered as usable as PINs and passwords are the least usable in terms of time to authenticate on smartphones. Schaub et al. [122] compared different virtual key-board layouts (iOS, Android, Windows Phone, Symbian, MeeGo) regarding password entry performance and composition. Significant differences were observed between different virtual keyboards in password entry time and error rates, with Windows Phone and iOS virtual keyboards being the most usable (fast password entry times and high typing accuracy).

Table 1. Factors affecting the user experience in knowledge-based user authentication.

Human	**Technology**	**Design**	**Ref.**
-	-	Password *vs.* graphical	[123]
-	-	Password *vs.* graphical	[108]
Age differences (younger *vs.* older adults)	-	PIN & graphical	[114]
Cognitive styles (Verbal *vs.* Imager)	-	Password & graphical	[115]
Cognitive processing abilities (limited *vs.* enhanced)	-	Password & graphical	[116]
Field dependence-independence cognitive styles	-	Graphical	[117]
Cognitive disabilities (Down syndrome *vs.* neuro-typical)	-	Password & graphical	[118]
User preference	-	Any user authentication type	[119]
-	Device type (desktop, tablet, smartphone)	Password	[120]
-	Smartphone	PIN, text-based passwords and graphical authentication	[121]
-	Smartphone	Virtual keyboard layout (iOS, Android, Windows Phone, Symbian, MeeGo)	[122]

4 State-of-the-art Security and Usability Metrics in User Authentication

Design and development of user authentication represents a typical example of a cross-roads priority problem, between security and usability, which emerge from contradictory requirements posed by different stakeholders. Security experts increase continuously the security levels of user authentication policies, end-users demand transparent, adaptable and user-friendly solutions, and service providers are trying, together with user experience experts, to find a viable equilibrium among security and usability.

Hence, security and usability aspects are two important quality dimensions of an effective user authentication scheme. The security level determines its strength against adversary attacks, whereas usability levels are commonly determined by memorability of selected secrets and task completion efficiency and effectiveness [71]. The literature reveals that various user authentication schemes entail different security strengths and weaknesses [124, 71], since in each case different factors exist that affect the security of the authentication mechanisms. Recent reviews on state-of-the-art security and usability metrics are reported in [71, 127]. Next, we describe types of threats in user authentication followed by an analysis of security and usability metrics utilized in knowledge-based, token-based and biometric-based authentication systems.

4.1 Types of threats

According to Biddle et al. [71], attacks can be classified in two broad categories; *guessing attacks* or *capture attacks*. *Guessing attacks* are considered an important threat in knowledge-based user authentication where the goal of the attacker is to guess the authentication key by trying guesses repeatedly. The consequences of a successful attack would affect thousands of users and would have an impact on the provider's credibility. Guessing attacks are either performed online in which the attacker guesses and enters the authentication key through the live login interface or performed offline in which the attacker first gains full access to the system's database that contains verifiable authentication keys (*e.g.*, cryptographic hashes). Offline attacks are harder to deal with since the attacker does not have time limitation other than the computational power of the device. Brute force attack is a widely used offline attack also known as exhaustive key search which entails systematically testing all possible authentication keys until the correct one is found. For user chosen passwords, search optimizations have been proposed such as dictionary attacks and intelligent brute force [128, 129]. Offline guessing attacks are prevented by processing the authentication key through a hash function in case the attacker gains full access to the authentication keys. Thus, the attacker is required to check if an authentication key attempt is correct by first hashing the guessed key and then compare it to the value stored in the database. Accordingly, the theoretical space of an authentication key is vital for preventing offline guessing attacks. Thus, in both text-based and graphical authentication mechanisms, the number and type of images has a significant effect on guessing attacks [83, 71].

Capture attacks aim to acquire the authentication key by either capturing data while the user enters the authentication key during login, or by stealing the users' secret key. Most common capture attacks include: *i) Shoulder surfing attacks* in which the attacker visually observes the user entering the authentication key; *ii) social engineering* using social manipulation of the user to convince them to divulge confidential information (either willingly or through phishing); *iii) malware attacks* (malicious software) to gather sensitive information; *iv) on touch screen device smudge attacks* with attackers aiming to discern the password pattern; *v) stealing* the user's device that is used for authentication; and *vi) data spoofing* in which an individual or software masquerades as another by falsifying data, to gain access to the system. A high number of research works have focused on minimizing threats of shoulder surfing attacks, such as De Luca et al. [125] that proposed an approach using fake cursors in on-screen password mechanisms and Winkler et al. [126] that proposed a hybrid approach for preventing shoulder surfing attacks on smartphones by leveraging a private near-eye display (*i.e.*, Google Glass). Researchers have also focused to prevent social engineering by assisting users to create secure and memorable passwords [96, 91] as well as investigating the type of image used in graphical authentication mechanisms [112].

4.2 Security metrics

Security concerns both the users and the service providers for different reasons and using secure authentication mechanisms is of major importance for both, as attackers may be targeting either side [127]. Users are rather concerned with capture attacks while providers are mainly concerned with protecting their services from guessing attacks both online and offline. Security is communicated to the users through strict authentication key policies, which ensure the created passwords meet a minimum-security level. There are a number of security metrics that enable the comparison between the different authentication policies such as *password strength*, *guessability* and *entropy* [127].

Focusing on knowledge-based authentication keys, *guess numbers*, *password strength meters* and *entropy* are three common approaches for measuring the security level [127]. *Guess numbers* refer to how many guesses it would take for a cracking algorithm with a given training set up to guess a password [130]. This approach refers to parameterized password guessability which aims to model real-world attackers and provide strength estimates per password. Despite recent research favoring guessability and guess numbers as a new more modern and accurate metric for measuring security [131-135], this approach's effectiveness depends on the selected algorithm and on the training data. Its value lies in providing a per password estimation meaning it can be used for security audits and for providing feedback to the user when creating passwords, through strength meters.

A *password strength meter* refers to checking the created password against a set of rules before submitting it to the system and providing feedback to the user through a word qualifying password strength (*e.g.*, weak, medium, strong, very strong). The accuracy of many deployed password checkers is low because they are often too simple to capture the complexity of passwords [131, 136]. Combining this with the fact that password distribution may be significantly different for different sites (*e.g.*, due to language differences), means there is no global password checker available that can be applied to all Websites. On the other hand, password strength meters allow for quick check of the created password for patterns (*e.g.*, dictionary words, repeats or sequences) and some providers restrict the use of such patterns while others only inform the users for the strength of the chosen password.

Entropy is another important security metric per policy. Shannon introduced entropy as a measure of uncertainty of choices [137]. In terms of authentication, entropy refers to how random users select passwords from a given *key space*, it relates to how difficult attackers can guess a password [138] and it is enforced through a password policy. The password key space (K_p) refers to the range of all possible values of key combinations and is governed by the character pool and the key length. Entropy is measured in bits and is calculated using the following equation [139]:

$$H_{max} = log_2 K_p \ [bits]$$

Users tend to select memorable passwords rather than random. This password selection strategy results in a non-uniform distribution of the key space, making the entropy lower. To describe this phenomenon, researchers distinguish between *theoretical entropy* and the *practical entropy* which stands for the entropy resulting from the non-random selection of passwords by users. The practical entropy is difficult to measure, mainly due to users' being skeptical in disclosing information regarding their password creation strategy and the inability of accessing raw password data. To confront this problem, providers have introduced dictionary checks, where common words and character combinations are not allowed to be used as passwords. The NIST Electronic Authentication Guideline SP-800-63 allows for calculating and estimate practical entropy based on Shannon's estimation of the entropy of each successive character of the English alphabet [138]. To this end, the discussed metrics and research work have been mostly applied in knowledge-based text-based authentication mechanisms. Nonetheless, these metrics can be applied to graphical authentication mechanisms with minor adjustments. Rass et al. proposed a methodology for calculating the theoretical entropy for a graphical authentication mechanism based on unordered image selection from a given pool [140]. It should be noted that when using images instead of text, random selection of authentication keys becomes more viable [141]. Kayem provides a comparison of the vulnerability to guessing between text-based authentication keys and recall-based graphical authentications keys and suggests that the latter outperform in terms of security [142]. Davis et al., conducted a large scale empirical study on user choices in graphical authentication mechanisms and concluded that user choices are far from random and depend on gender and race [111], which suggests that a strength meter could also serve as a security metric for graphical authentication schemes just as for passwords.

With regards to token-based authentication schemes, common evaluation metrics for security relate to resistance to data spoofing, transmission security, and social engineering [152]. Other evaluation metrics for token-based schemes include: *i) probabilistic behavior* which can be assessed through False Acceptance Rate (FAR), False Reject Rate (FRR), Failure To Enroll (FTE), Failure to Acquire (FTA) [152]; *ii) integration* which can be assessed based on hardware compatibility, software compatibility, systems interoperability, vendor independency, access to source code [152]; *iii) robustness* which can be assessed through resistance against noise, input device quality, reliability [152]; and *iv) privacy* which can be assessed through resistance against known attacks, investigation of potential attacks, template protection [152].

With regards to biometric-based authentication schemes, the resistance to the following attacks can be used: faking the sensor, resubmitting biometric signals, network attacks on servers [151]. Common approaches classify the security of biometrics as: *i) High*, if a soundproof security solution has been proposed; *ii) Medium*, if the biometric system contains a security characteristic that makes it difficult to attack; and *iii) Low*, if the biometric feature is not secure or there are a few studies on the particular security issue [151]. *Accuracy* is another important measurement which can be assessed through False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), Authentication Accuracy [151]. Finally, one important factor in biometric-based systems relates to user privacy. To assess the privacy of a biometric system, the following aspects can be used: Mission Success Rate, Noninvertibility, Revocability, Unlinkability [151].

4.3 Usability Metrics

The Computer Security community has come to understand the critical importance of *usable security*, which is primarily focused on *designing secure systems that people can use*. In this section we describe the terms *usability* and *user experience* and identify the main metrics that are used within user authentication schemes.

The International Standard Organization (ISO 9241-11) [154] identifies three aspects of *usability*, defining it as *"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use"*. A variety of methods have been proposed to ensure that the interface of the final product is effective, efficient, and satisfying to use. This includes heuristics and guidelines, expert reviews, and user-centered design methods. The idea of user-centered design (UCD) is to place the user, at the center of the design process. Users are involved in the development process in very early phases of the software development and in fact throughout the complete development lifecycle. Involving users from the beginning can help to discover their ideas and expectations about the system (*i.e.*, mental model). Moreover, it can help to identify and analyze tasks, workflows and goals, and in general to validate the developers' assumptions about the users. As usability and UCD methods focus on cognitive and ergonomic factors (*i.e.*, perception, memory, etc.) they are important for the design of user authentication systems.

Recent research on Human-Computer Interaction (HCI) extends traditional task-based analysis and evaluation (*e.g.*, usability evaluation), but rather focuses on hedonic and affective (*e.g.*, surprise, diversion, intimacy) aspects of HCI design and evaluation. In this context, *user experience (UX)* has gained momentum in the field of HCI and interaction design, that is a countermovement to the dominant, task- and work-related usability paradigm. Some people distinguish between the terms usability and user experience. Usability is usually considered the ability of the user to use the system to carry out a task successfully, whereas user experience takes a broader view, looking at the individual's entire interaction with the system, as well as the thoughts, feelings, and perceptions that result from that interaction. ISO 9241-210 [155] defines UX as *"a person's perceptions and responses that result from the use or anticipated use of a product, system or service"*. Effective HCI design and evaluation involves two important qualities: *i)* usability (*i.e.*, traditional HCI), and *ii)* hedonic, beauty and affective [153].

A number of research works have investigated the usability of various user authentication schemes. The most prominent usability dimensions being measured are *task efficiency*, *task effectiveness*, *user preference*, *memory time*, and *user experience* which can be measured as *perceived usability, memorability,* and *security*.

Task Efficiency. Task efficiency refers to the resources expended in relation to the accuracy and completeness with which users achieve goals [154]. In user authentication, task efficiency is measured as time to create the user authentication key and time to login. Biometric-based systems additionally include the following aspects: time spent for data collection, data processing, feature extraction, and authentication decision [151].

Task Effectiveness. Task effectiveness refers to the accuracy and completeness with which users achieve specified goals [154]. In user authentication, task effectiveness is commonly measured as the number of attempts required to create the user authentication key and the number of attempts required to login.

User Preference. User preference is typically measured through Likert-type questionnaires in which users indicate for example whether they prefer a particular authentication scheme over another (*e.g.*, textual *vs.* graphical).

Memorability. Memorability is typically measured through: *i) memory time* that refers to the greatest length of time between a password creation and a successful password login using the same password [156]; and *ii) number of password resets* when users forget their authentication keys.

User Experience. User experience is typically measured through validated questionnaires aiming to elicit the users' perceptions about the user authentication scheme with regards to usability, memorability and security. User experience is further measured through interviews, semi-structured interviews and focus groups.

Usability of Biometric-based System. To assess the usability of a biometric system, the following aspects can be used: universality, uniqueness, permanence, need for extra equipment [151].

5 Inspection of Current State of User Authentication Practices in Healthcare Environments

We applied a two-fold method aiming to investigate and validate the current state of user authentication practices in healthcare environments as follow: *i)* we conducted a literature review on state-of-the-art user authentication practices in healthcare environments aiming to reveal which of the abovementioned practices and schemes are applied nowadays within this domain; and subsequently *ii)* we conducted a qualitative study with healthcare institutions of our consortium in order to validate results and manifest the current literature and evaluation criteria.

5.1 Literature Review of User Authentication in Healthcare Environments

Advancements in computer and communication technology enabled the rapid growth of E-Health services [143], which can nowadays provide various electronic methods (*e.g.*, obtaining online consent, exchanging health data) [144]. Considering the sensitive nature of health data, such electronic methods are susceptible to various threats [145] and may lead to ethical issues [144]. Therefore, there is an increased need for providing security that takes into consideration not only the technical aspects, but also the ethical aspects within electronic healthcare systems [144]. The confidentiality of patients' data, which are exchanged by healthcare professionals through network-based technologies, is of major importance since any disclosure could violate patients' privacy. To protect such sensitive data from unauthorized access, effective authentication mechanisms must be utilized [145]. However, the importance of authentication mechanisms is often underrated in healthcare services [146]. Although most healthcare providers often employ the traditional text-based password solutions [144], which can be compromised by adversaries [145], biometric technologies are getting market share aiming to reduce fraud and to provide increased security and usability for accessing medical records without compromising patients' privacy [145, 147, 148]. Today, some healthcare providers adopt biometric solutions [149] which offer a convenient alternative authentication mechanism, especially for elderly adults or individuals with cognitive impairments [145]. Nevertheless, despite its ease of use, biometric technology is not yet the reliable solution to all security concerns [144, 145, 150].

Kogetsu et al. [144] underpin the importance of adopting a secure authentication scheme and the impact of compromising the authentication scheme would have on a patient's data. Their analysis indicates that the authentication method that is utilized by most of current medical research is the traditional textual password approach, although other examples exist that utilize alternative authentication methods. For example, in RUDY, which is a study that targets rare diseases of human bones, joints and blood vessels, during registration, patients must provide information regarding their healthcare institutions or doctors. Then researchers make inquiries in order to check the validity of the request. An alternative way for patients to be authenticated in RUDY, is by uploading a medical certificate or sharing their medical records with the institutions' researchers. Finally, Kogetsu et al. elaborate that two-factor authentication schemes are the most viable alternative, since the username and password combination is not completely secure as is. By combining knowledge- and token-based authentication schemes, greater security can be achieved that can be further tuned according to the context of use. For example, for accessing simple patient data such as blood pressure, simple two-factor authentication can be used, whereas for accessing more sensitive data, a biometric factor can be used, in order to achieve three-factor authentication. Li et al. [146] similarly report the importance of authentication mechanisms for achieving patient's privacy of health and personal information, and how conventional textual passwords can be easily compromised. In addition, their analysis indicates how biometric-based authentication schemes can be a viable alternative to current authentication schemes, since they offer easier and more secure access to data by both the patients and physicians, and that they have already been adopted by many healthcare organizations. Also, their work dictates new studies that target other biometric modalities which offer dynamic user authentication that could further enhance security. Marohn [147] states the importance of biometric-based authentication schemes in order to help prevent fraud and identity theft, without compromising the security and users' privacy. The research analysis does so by giving examples of three healthcare systems across the world (Texas, South Africa, Australia) where biometric-based authentication has been applied to help with accurately identifying the user and administrating each corresponding treatment. Krawczyk and Jain [148] discuss around alternative user authentication approaches for protecting patients' privacy, suggesting that biometric-based authentication schemes are promising alternatives to current textual authentication practices. Moreover, they propose a new biometric-based authentication scheme that combines online signatures and voice biometrics in order to achieve a desired security threshold. Silva et al. [149] review current and widely applied biometric-based user authentication solutions and further introduce a framework for continuous authentication by using ECG signals. Win et al. [161] analyze widely applied user authentication mechanisms in healthcare systems and how alternative authentication schemes could achieve better security and usability. Based on their analysis, the most widely applied authentication scheme is a combination of a user identifier and a textual password. Other applied schemes include combining a key card and a PIN code, together with biometric-based authentication. Finally, their research work states that the next level of authentication security is the implementation of cryptographic mechanisms within smart cards. Finally, Santangelo et al. [162] argue how currently deployed textual password authentication schemes are antiquated and not secure enough within healthcare organizations and propose that two-factor authentication should be used in order to add additional layers of protection.

Recently, several EU-funded research projects have proposed and evaluated novel user authentication schemes within the healthcare domain, among other domains. A recent EU-funded research project in the frame of Horizon 2020, namely CREDENTIAL - Secure Cloud Identity Wallet (#653454) [164] proposed, developed, tested and showcased innovative cloud-based services for storing, managing, and sharing digital identity information and other critical personal data. The security of these services relies on the combination of hardware-based multi-factor authentication with end-to-end encryption. An ongoing Horizon 2020 project, namely SILENSE - (ultra)Sound Interfaces and Low Energy iNtegrated SEnsors (#737487) [165] proposes among others a behavioral biometrics authentication scheme based on gestural input that can be applied in various contexts such as E-Health [165]. Another ongoing Horizon 2020 project, namely ACTIVAGE - ACTivating InnoVative IoT smart living environments for AGEing well (#732679) [166] aims to build the first European IoT ecosystem, reusing and scaling up underlying open and proprietary IoT platforms, technologies and standards within the Active and Healthy Ageing domain. An important objective of the project is to build a modular and open-source user authentication hub based on a multi-factor authentication approach, *i.e.*, using a physical key, fingerprint and/or Near Field Communication (NFC) tags. Another past EU project that was funded in the frame of the 7th Framework Programme for Research and Technological Development, namely PCAS - Personalised Centralized Authentication System (#610713) [163] proposed a Secured Personal Device (SPD), enabling users to securely store their data, to share it with trusted applications, and to easily and securely authenticate them. The SPD recognizes its users utilizing multiple biometric sensors, including a stress level sensor to detect coercion. The proposed authentication system was evaluated within electronic health and university campus access control contexts.

To this end, table 2 summarizes the aforementioned works, focusing on the user authentication schemes that are currently applied within the healthcare domain, and the proposed alternative user authentication schemes. Accordingly, a generic conclusion that can be derived from the state-of-the-art research and practice is that: *a)* the majority of current healthcare organizations apply the traditional textual user authentication scheme; *b)* studies and analyses indicate that textual password within the healthcare domain are not adequate due to know security and usability issues; and *c)* a high number of research projects and works propose new alternative user authentication solutions that embrace multiple factors for authentication (beyond traditional knowledge-, token-, and biometric-based solutions) such as innovative personal devices [163], behavioral biometrics (*e.g.*, gestures) [165], human biometrics (*e.g.*, stress) [163].

Table 2. Currently applied and proposed alternative user authentication schemes for healthcare environments based on existing practices and literature work analyses.

Currently applied user authentication	**Proposed user authentication**	**Ref.**
Textual passwords	Two-factor authentication	144
Textual passwords	Biometric-based authentication	146
Biometric-based authentication	-	147
-	Biometric-based authentication	148
Biometric-based authentication	ECG continuous authentication	149
Multi-factor authentication: Textual password, key card, PIN, biometrics	Cryptographic mechanisms within tokens	161
Textual passwords	Two-factor authentication	162
Textual passwords	Multi-factor authentication, combining token-based with biometrics sensors	163
Textual passwords	Hardware-based multi-factor authentication	164
Textual passwords	Behavioral biometric authentication	165
Textual passwords	Multi-factor authentication using physical keys, fingerprint, NFC tags	166

5.2 Qualitative Study on User Authentication Practices at End-user Organizations

Based on the analysis of the literature review we formed the main research topics which were further validated based on a mixed evaluation method that embraced mini focus groups and semi-structured interviews with the partners of the consortium. In a nutshell, the partners verified that current approaches entail knowledge-based and token-based approaches, and follow practices based on industry standards. Next, we describe in detail the responses of the participants and analyze the results. For privacy and security concerns, we anonymized the responses of the interviews reported in the deliverable which are however available within the consortium. The Annex lists the interview schedules, the main questions of each topic (Topic 1 and Topic 2), and a copy of the participants' consent form. The Annex also includes a draft list of questions (Topic 3) for eliciting the end-users' behaviors, opinions and practices with regards to the user authentication of their organization. These questions have not been utilized in the current qualitative study, however these will be used as a basis for *D5.3 - Software on the Refined Verified User Authentication Scheme*, as well as the baseline evaluation measurements of the user authentications schemes of the three end-user organizations in *WP7*.

Method of Study

A series of semi-structured interviews were conducted at the three end-user organizations aiming to identify current user authentication practices, policies and procedures followed at large healthcare organizations in Europe. Each interview took approximately 45 minutes including one to two participants in each session. Participation in the interviews was voluntary and could be cancelled at any time.

The interviews were split in two parts. In *Part A*, participants were initially guided to an online consent form and each one read and agreed to participate. Participants were then introduced to the project and purpose of the interviews. In *Part B*, we conducted an initial profiling (approx. 5 min) of the participants asking questions that relate to the participant's background and position in the company. The purpose was to understand the background of the interviewee and the context of his/her answers. Then we discussed around two topics: *Topic 1 - User Authentication Policy* (approx. 20 min) was focused on eliciting details about the user authentication policy and procedures of the organization (*e.g.*, how the policy was derived, since when the policy is valid, etc.); and *Topic 2 - Technical Details and Workflows* (approx. 20 min) was focused on eliciting details with regards to technical and security matters of the currently applied user authentication scheme and policy (*e.g.*, what is the current password complexity of the applied authentication policy, which is the maximum number of days a password may be used, etc.).

Participants

A total of 9 stakeholders participated (1 female, 8 male) in the semi-structured interviews. We recruited participants with various roles such as Chief Information Security Officers, Enterprise Architects, IT Department Managers, Security Experts, Project Managers, etc.

Analysis of Results

In this section, we present the analysis of results for the three organizations.

Organization 1 (O1). Organization 1 based their user authentication policy on EU standards and primarily apply textual password authentication. The policy has been active for three years, in particular:

"*Policy has been defined for let's say 5 years and it is implemented let's say 3 years ago when we implemented one active directory in our organization*" ~ *U1*

The main policy is based on a widely applied password policy, *i.e.*, a textual password has to be of minimum length of 8 characters containing no part of the user's real name or username, and including minimum one uppercase, one lowercase, one symbol and one digit symbol. When resetting their password, users are restricted from using any one of their past 20 passwords. Maximum 5 login attempts are allowed with no penalty time between attempts and each password must be changed every 90 days. When a user's login attempt results to a failure, no penalty time between attempts is activated. After five unsuccessful login attempts, the user's account is disabled for 15 minutes.

Passwords are hashed using hashing algorithms that are based on Microsoft Azure services.

"Active directory is your first line of defense so that's why when you are internally it's ok and you login with your badge, so your badge is your second factor. If you are outside of the hospital that's also possible, you can get a remote reader at home, so you get an SMS or via the Microsoft app, you can authenticate and get your session." ~ U2

The organization also uses multi-factor authentication for accessing the patient database to achieve higher security. The authentication can be token-based (RFID badge), combined with a 4-digit PIN code and at the moment *"this works well"* (*U2*) as stated by the interviewee.

The organization applies variations in the policy depending on the role of the user as well as the context of use. For example, exceptions for policies can be requested by general users to be applied only for them. Also, multi-factor authentication is enforced when users access their accounts remotely.

"People can request exceptions on a policy and then we look at the case and decide whether we can change the policy" ~ U1

Currently, there is no scheduled plan by the organization to upgrade the current policy, however the active directory will be updated to the Microsoft Azure active directory system and there is no need for the policy to be changed for now. The company is integrating as many applications to one active directory so that with a single sign in several applications can be accessed.

With regards to biometric authentication:

"*I have considered it but this moment we are migrating to Microsoft multi-factor authentication and within that scheme as far as I know at this moment I did not study it elaborately, you are able to choose your multi-factor so it is multi-factor authentication but the way, the means with which you authenticate are not yet fully established*" *~ U1*

Furthermore, another participant reported that biometric methods have been considered before, however entailed usability problems. For instance, facial recognition was given a trial, however there were problems in some cases:

"The problem is that if you go a little away from the screen, or two persons are standing, one person is close and one is standing behind the screen, the system did not know which one is the user" ~ U2

With regards to user complains, *U1* stated that users expressed some complaints on the authentication policy:

"There are complaints about the complexity of the passwords, the amount of passwords they have to used, changing the passwords, so it's not a very nice picture" ~ U1

With regards to threats and attacks on the user authentication system:

"No we never had signals of anything like that happened but that doesn't mean that it didn't happen, that means we don't know" ~ U1

One of the vulnerabilities of the current scheme and policy relate to password reuse from users. The organization is currently applying introduction programs to information security and privacy, security awareness, guidelines, etc. aiming to spread the awareness to the employees of the organization.

Regarding security attacks, none have been reported so far. Specifically, one interviewee stated:

"Not that I am aware of in the last few years that I am here for regarding user authentication. Of course, we always have some vulnerabilities and threats regarding ICT but not on behalf of user authentication." ~ U3

Prior to applying the current policy, the organization has outsourced another security expert firm for taking benchmarks for the former user authentication policy. The firm performed an ethical brute force attack attempting to crack passwords aiming to measure the amount of difficulty needed to guess the passwords. From the 5314 users, there were 4695 unique NTLM hashes (New Technology LAN Manager), in which 1000 unique passwords were cracked within a couple of seconds. This was the motivating factor for implementing two-factor authentication and more strict policies on the single textual password. NTLM passwords are not used anymore as it is considered an old technology by the organization. A new penetration test with the current policy was not yet performed.

For newcomers to the system, their manager requests a User ID for them, which is sent via email, along with a one-time-password (OTP). Then, the user is requested to login using that information, and they must change their password. When trying to access the network remotely, the user must enter a 4-digit PIN number in order to receive an SMS code, as a two-factor authentication method, which is then entered in the system. After that, the normal textual password process in required. In case of requesting a password reset, no password reset tool is in existence so far, and the users need to contact the helpdesk and after answering several questions which verify the user's identity, the password is reset. Although, no complaints have been made so far from the users regarding the authentication process, but within the next few months an alternative remote login method is going to be applied that will make the process more user friendly. As stated by the participant:

"No, people are too happy they can work from outside and they understand the security as a tight topic. But we are in the process to make it a little bit more user friendly" ~ U2

This method will require from a user to enter their credentials and then an automated confirmation call will be executed from Microsoft, that will provide a confirmation code that will have to be typed in, in order to authenticate the user. For accessing the systems, users use all sorts of devices, such as smartphones, tablets, laptops and desktop computers. In addition to the aforementioned authentication methods, a two-factor authentication may also be applied, where the user can swipe their badge (token-based) on a badge reader and then enter their four-digit PIN (knowledge-based) that they specified for themselves when obtaining the badge.

When asked to provide details about the *"perfect authentication schemes"* and a wish list for *"better passwords"* the participant responded:

"I would really like to leave our employees free and choosing what mechanism they want, the only concern is the level of security and it's usability" ~ U1

"In the past there was token authentication using banking cards, but it was discontinued because of the cost of this system. Picture passwords is a difficult method to be integrated at the moment because of interoperability issues. The specifications of the system make the use of picture passwords difficult. More specifically, Windows 7 with virtualization is used and there are no touch screens for interaction. 95% of the infrastructure is based on virtual workspace sessions" ~ U1

Another participant stated that currently there are no plans for applying a user-centered authentication system. The participant did not have any wish list for better passwords as the company relies on industry standards and Microsoft's recommendations and best practices. With regards to alternative authentication a participant stated that he/she is aware of picture-based passwords, however, the organization would not want to experiment with new authentication methods, as their main focus is to deliver care to their patients:

“Login accounts should not be traceable to a physical person. It should be an unpersonalized user ID” ~ U2

“We standardize on the Windows platform so everything is Windows so then it’s not very bright I think to use user authentication from other vendor … Also most of the users are used to windows” ~ U2

“If it is not supported by Microsoft we don’t implement it. As a concept: I don’t see any problems with the approach now” ~ U2

Organization 2 (O2). Organization 2 authentication policy was derived based on SAP system’s standards and policies which was first applied in the organization in 2003. According to one interviewee, *“this policy is active from 2003” (U3)* and has not been changed since then. The user authentication method is primarily based on textual passwords which are stored in the database using the SHA-1 hashing algorithm. According to the policy, users are required to enter passwords of minimum length 8 characters with main restriction that there must be at least 1 character different from the previous password. No restrictions on uppercase or lowercase letters, nor on special characters and numbers are applied. In addition, the password cannot contain the user’s username, however, dictionary words are allowed to be used within the password. Passwords expire every 90 days and must be changed. An alternative authentication method is applied for specific doctors accessing emergency rooms that have the option to use an RFID card to login.

The organization is currently working on a new policy that will be deployed within the next few months which will require from users to enter at least one number, one uppercase letter and one special character. Primary focus of the implementation is to increase its security levels rather than usability.

“The focus is only on security. Trying to increase the security always has a contradiction with the users but primarily our focus is to try to increase the security” ~ U4

Furthermore, in case of 5 consecutive unsuccessful logins with no waiting time between the attempts, the user’s account is locked. Once the account is locked, users can follow two options to unlock their account: *i)* contact the helpdesk for recovery of the password by answering specific security questions related to the user; and *ii)* at the end of the same day (midnight) the account was locked, the account is automatically unlocked. There is no waiting time between unsuccessful logins.

“We are working on a system based on a web application where the user can access and they are asked for special questions that only the user knows and then if you answered correctly all of the questions the system allow you to reset the password and send you via email or phone number” ~ U4

Furthermore, the organization does not have different types and policies of authentication depending on the context of use and the passwords used from both remote and within access are the same. There is only need for connection to the VPN of the organization when the user is in an external network.

Currently, no multifactor authentication is applied, but a version is in testing environments, where the users will accept push notifications on their smartphones, after attempting to login, which will validate their login attempt.

"We are testing now but it is not in production environment ... using your mobile phone, to accept in your authenticator app, for example your google authenticator app or your Microsoft authenticator app to accept a validation for connecting for example to your email in the office" ~ U4

In terms of benchmarking and measuring the strength of the current policy, no benchmarks are used and no quantification of the security strength has been made. Moreover, some usage data are recorded, such as time to login, number of failed attempts, the time of the account lock, the reason for the account lock and the date a user changed their password, but they are primarily collected in case there is a security issue so they can search for the cause.

"The time to login, the number of failed attempts, the time the user account is locked, the reason for user account lock and the date the user changed the password. [We keep these data] Only in case of problems. But we cannot evaluate these data everyday." ~ U5

Furthermore, the organization has not taken into consideration the usability of the passwords and no benchmarks of user authentication usability and security metrics. The organization has not used any brute force attacks to measure the strength of the policy, nor did they receive any security threats. In addition, no profiling or user categorization is applied before the authentication process, however some authorization is applied, after the authentication, that enables you to access sensitive data.

With regards to security threats, until now there were no security threats faced in the organization and this is primarily because of the restricted access to the system only from people in the network or from an external network connected to the VPN of the organization.

With regards to user complaints, the main reported problem is that the users easily forget their passwords, either due to holidays or due to the frequent password changing, so there is often the need to reset them via the helpdesk.

"They have problems to remember and sometimes they have to put the password in a post-it and the password is not hidden from the public when they are working in their desk" ~ U5

Finally, an interviewee stated that he/she would like to improve the security of the organization, however the main concern is the trade-off between password security and usability. There was also expressed a lot of interest in two-way authentication methods like Google's authenticator or SMS authentication. Another interviewee is very interested in the integration of alternative and usable authentication schemes, however the main concern is related to the increased complexity and costs of applying new policies and systems in the organization's production line.

"There are many procedures in order to make small changes. It is very difficult to implement. We are now testing another user authentication but this takes a lot of time and it will take as much time to implement it." ~ U6

Organization 3 (O3). Organization 3 user authentication policy is based on widely used industry standards. The primary means for authentication is based on textual passwords requiring from users to enter a minimum length of 8 characters, including minimum one uppercase character, one special character and one digit. Dictionary words are allowed to be included in the password. A password reset is required every 60 days.

The policy does not consider the user's context of use, hence the same policy is applied for all users. The main interaction devices used within the organization, are laptops and desktop computers, along with minor usage of smartphones. In addition, user accessibility is not taken into account, but it is sufficient for the most part of the users that have access to the system.

“Laptop. I have a smartphone for email and calendar but nothing else.” ~ U7

In case users forget their password, the password can be reset only by contacting the helpdesk by answering specific security questions known only by the user. An alternative method applies, which is rarely used, where users can visit a Web-based service desk and request a password reset.

“It involves phoning an IT helpdesk which will normally take between 15 and 20 minutes” ~ U8

Several users of the organization must remember and use more than one password, a factor that renders the authentication process harder to complete. In addition, the Web browser of these systems do not allow saving the password for the organization.

“It feels like quite a large number. I would say at least 10.” ~ U8

With regards to user complaints, users in general feel like they are putting a lot of efforts to remember passwords and need to login several times per day. One stakeholder stated that end-user are more than willing to change their current authentication scheme, as long as it applies across multiple systems and it is not too complicated to use.

“I certainly will be willing to change as long as it was applied across multiple systems. But if it’s a new authentication type that’s different for each system then that would cause problems.” ~ U8

Summary of Main Findings

In Table 3 we summarize and compare the authentication policies of the three organizations.

Table 3. Summary of policy and security aspects of the user authentication mechanisms at the three organizations.

	Organization 1	**Organization 2**	**Organization 3**
Main user authentication type	Textual password	Textual password	Textual password
Minimum length	8	8	8
Dictionary check	Dictionary words are not allowed on username	No check	No check
Policy within the network	Textual password, length>=8 characters, at least 1 lowercase letter, 1 uppercase letter, 1 number, 1 special character	Textual password, length>=8 characters, no restriction applied	Textual password, length>=8 characters, at least 1 lowercase letter, 1 uppercase letter, 1 number, 1 special character
Policy outside the network	VPN connection, Two-factor authentication (Password+OTP)	VPN connection, Same policy as within	VPN connection, Same policy as within
Alternative Authentication	4-digit PIN + RFID badge	RFID badge for doctors in emergency rooms only	N/A
Main devices used	Desktop, Laptop	Desktop, Laptop, Mobile, Tablet	Desktop
Password hashing algorithm	Microsoft’s Azure Services	SHA-1	N/A
Waiting time between failed login attempts	No waiting time	No waiting time	N/A

Maximum login attempts	5 attempts	5 attempts	5 attempts
Authentication process logging	No	Yes	N/A
Security benchmarks	No	No	N/A
Action taken after exceeding the maximum allowed login attempts	Account disabled for 15 minutes	Account disabled and helpdesk has to be contacted for recovery	N/A
Password life	90 days	90 days	60 days
Password reset method	Contact helpdesk	Contact helpdesk Working on: Textual secret questions/answers	Contact helpdesk or Request through service desk Website
Authentication wish list	As secure as possible, practical and easy to remember	Flexible passwords, not complicated, secure, and has low cost	Flexible passwords as long it is not complicated and secure

6 Proposed Authentication Approach, Initial Evaluation Metrics, Policy and Personas of the Serums User Authentication Scheme

In this section we describe the proposed user authentication approach, the identified personas and use-case scenarios, as well as the initial evaluation measurement and metrics, and policy for the Serums user authentication scheme. We also relate each evaluation metric with the Success Indicators (SIs) and Key Performance Indicators (KPIs) of the project that are defined in *D7.1 - Initial Requirements Analysis and Success Metrics*.

6.1 Proposed User Authentication Approach

Based on the aforementioned state-of-the-art analyses, we conclude that despite the fact that textual passwords entail several security and usability concerns, they are currently still the most widely applied user authentication approach in the healthcare domain. In addition, research indicates that knowledge-based approaches will continue to prevail in the next decade [76], even in combination with other approaches (*e.g.*, token, biometric). Nonetheless, several research attempts exist that work towards finding alternative authentication solutions such as graphical passwords, two-factor authentication approaches with tokens, novel authentication devices, biometrics, etc.

From an end-user perspective, evidence has shown that user preference and task performance in knowledge-based authentication vary significantly depending on the user and the context of use, suggesting that any specific solution might not please everyone. Thus, bearing in mind that: *a)* users prefer and perform differently in various authentication schemes; and *b)* nowadays user authentication is performed on multiple heterogeneous devices, one of the major objectives related to the user authentication approach that will be adopted in the Serums project is to provide a viable and flexible solution that is based on state-of-the-art practices in the healthcare domain, and in parallel applicable within the consortium’s end-user organizations. Therefore, we suggest adopting a personalized and adaptable multi-factor user authentication scheme which will be based on a flexible user authentication paradigm [157-160], along with token-based user authentication utilizing push notifications on smartphones and smartwatches. Our work is primarily driven by our vision to combine textual and graphical password schemes based on a new flexible user authentication paradigm, which allows us to move from current generic *"one-size-fits-all"* authentication systems to flexible, user-adaptable authentication systems.

Main aim is to leverage on the benefits of each approach (knowledge-based and token-based). On the one hand, we believe that knowledge-based approaches can still be viable in today's interaction contexts since they are easy and inexpensive to implement compared to token-based and biometric-based that require additional hardware to work, they are familiar to the majority of users, they don't entail privacy concerns raised by biometrics, and they allow adapting and personalizing the authentication scheme to the characteristics and preference of each user. For adding an additional security layer to the authentication solution, we combine knowledge-based authentication with push notifications through SMS passcodes and mobile application passcodes that will allow users to approve push notifications to verify their identity.

A first conceptual design of the proposed flexible user authentication paradigm is depicted in Figure 6. Our approach attempts to provide a new user authentication paradigm that leverages upon theories in Cognitive Psychology (dual coding, episodic and semantic memory), which suggest that humans' episodic and semantic memories, represented as verbal and visual information, can be transformed into memorable and personal authentication secrets. Such secrets can be semantically similarly reflected on both textual and graphical password keys, and accordingly used complimentary based on user preference and individual characteristics (Figure 6). Hence, the paradigm relies on a single, open-ended, user-selected secret that can be reflected as a textual key and a graphical key. *The suggested paradigm will be further analyzed and designed in the forthcoming deliverable D5.2 - Software on the Initial Verified User Authentication System.*

Consider a password creation scenario in which a user chooses a secret derived from his episodic memory, *e.g.*, *"Places that we visited in Europe"*. In this scenario, the textual password key is based on the articulation of the secret, *e.g.*, the system will generate a textual password key *"PlacesThatWeVisitedInEurope"*. For the creation of the graphical password key, the user chooses pictures illustrating relevant images through search in Web engines. Other related images from the image search default to decoy images (in the case of recognition-based graphical authentication). Both user-selected and decoy images are finally assigned to the user's profile to be used for login. Users will also be able to choose a single background image and then draw secret gestures on the image that will be based on the chosen single secret. Hence, the FlexPass paradigm extends existing works in knowledge-based user authentication based on theories of human cognition with the aim: *a)* to enhance memorability through ownership, and prior experience and knowledge of each single user; and *b)* to support user authentication adaptability since users can choose their preferred way to login based on their needs and context of use. For example, users that are on the move and interact on their smartphone might prefer to login with a graphical password, instead of entering text on a virtual keyboard which is considered a demanding and time-consuming task [99, 120]. The same user however, in a different context, *e.g.*, while at home working on the desktop computer, can chose to login through his textual password key. Note that in both cases, the user is only required to recall the same single secret, which can be reflected differently based on the user's preference. Similarly, older adults might prefer to always login with a graphical password since they find it easier than textual passwords, as opposed to younger adults that instead, prefer traditional textual passwords [113, 114].

Nevertheless, the dual nature of FlexPass embraces new vulnerabilities related to security that need closer attention, *i.e.*, a brute-force algorithm could use the additional information provided by the graphical representation to break the textual key. In addition, FlexPass introduces a new kind of observational attack; adversaries know the format of the password and they can see the set of pictures. Accordingly, aiming to add an additional layer of security to the proposed approach, we use a second factor for authentication through push notifications as a first step before proceeding to login. In particular, at a first stage users will be required to approve a push notification that will be realized as an SMS notification including an OTP, and a mobile application notification. After verifying their identity, users will login through their preferred user authentication type based on the FlexPass paradigm. Furthermore, in order to prevent revealing at the front-end system the unique identities of the images stored in the database, we will implement a one-time authentication process for graphical authentication. In particular, a random hashed number will be assigned to each image and the relation between the image and the hashed number will be stored in a temporary record in the database that will be valid for a short period of time.

Furthermore, the open-ended nature of the suggested paradigm might affect users towards misuse strategies. To assure that users will not create semantically insecure (predictable) grids of images, automated image tagging technologies (*e.g.*, IBM Watson Visual Recognition, Google Vision API, Amazon Rekognition, etc.) and policies need to be investigated to prevent users' unsafe coping strategies. These will be further investigated and reported in *D5.2 - Software on the Initial Verified User Authentication System.*

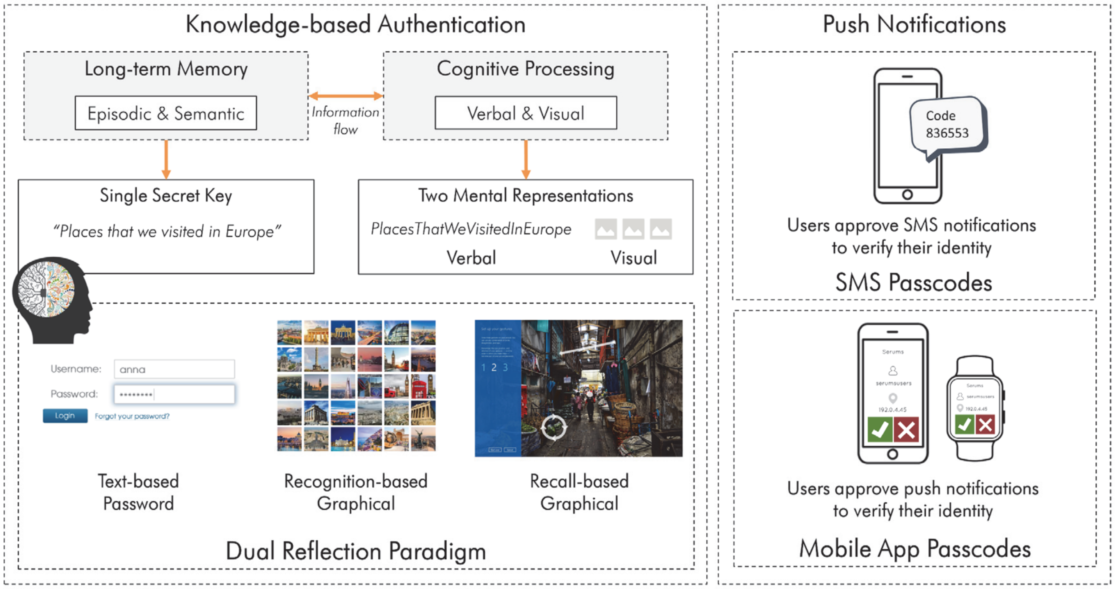
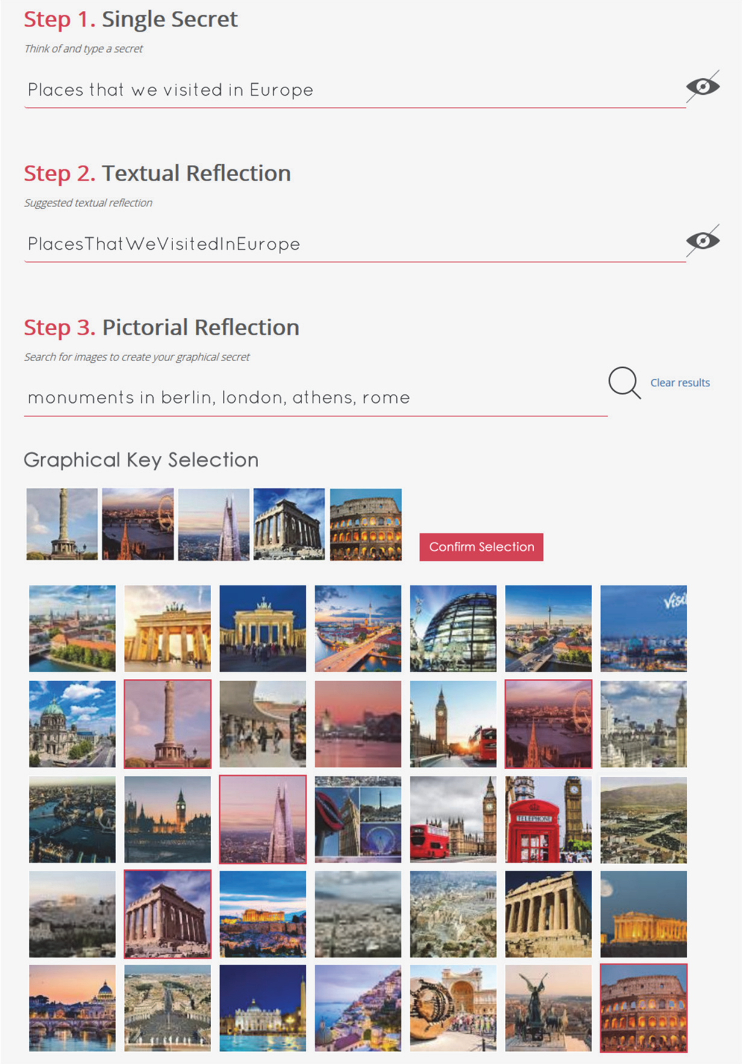


Figure 6. The Flexible user authentication concept.

6.2 Use-case Scenario

The FlexPass paradigm will be realized as two main processes: *i)* creation of the single secret and its two reflections; and *ii)* user-adaptable authentication. We next describe a use-case scenario of the two main processes.

Creation of the Single Secret and its Two Reflections. The user enrolment/registration phase is split in three main steps (Figure 7): *i)* users type a unique username and further choose and type a single secret they wish, *e.g.*, *"Places that I visited in Europe in my childhood"*; *ii)* the system generates a textual password key based on the single secret, *e.g.*, *"PlacesThatIVisitedInEuropeInMyChildhood"*, in which users are free to slightly modify the text, *e.g.*, change upper- to lower-case letters, include special characters, etc.; and *iii)* users create a graphical password key. For the creation of the graphical key, FlexPass provides an image grid manager that can be filled with pictures related to the chosen secret. Through communication with several APIs (*e.g.*, Google Custom Search, Facebook, Instagram, etc.), FlexPass enables users to include existing pictures through search in Web-based engines and their social networking profiles. The users then select and create the graphical password key, either by selecting a set of images among decoys (for the recognition-based approach), or by drawing gestures on the selected image (for the recall-based approach). Finally, users confirm their passwords which are further assigned to profile in the FlexPass database.



Step 1. Single Secret

Think of and type a secret

Places that we visited in Europe

Step 2. Textual Reflection

Suggested textual reflection

PlacesThatWeVisitedInEurope

Step 3. Pictorial Reflection

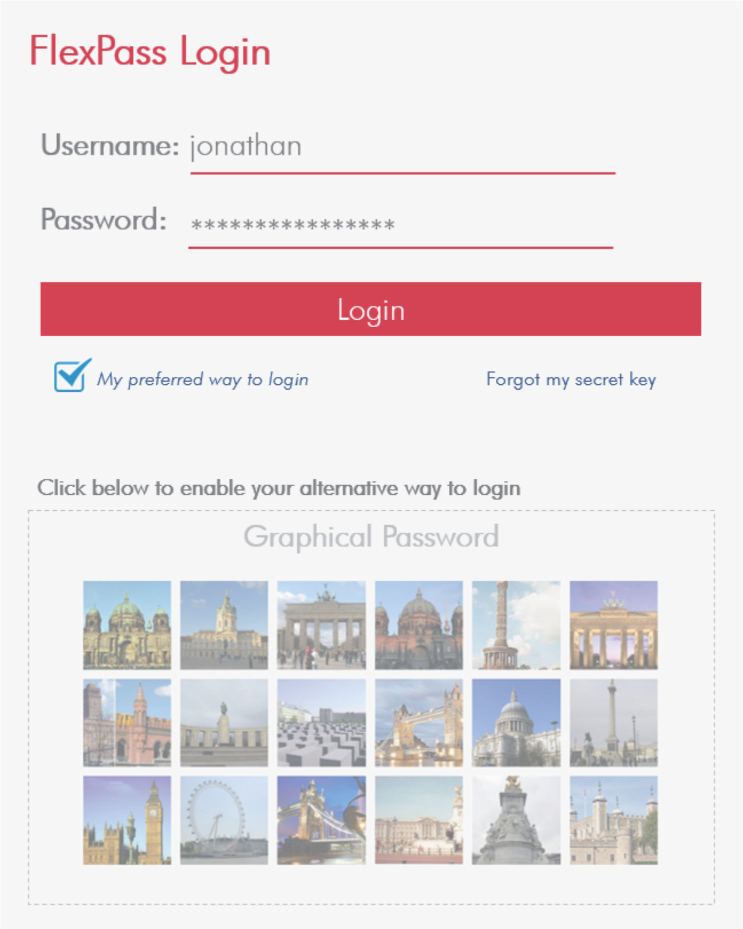
Search for images to create your graphical secret

monuments in berlin, london, athens, rome

Graphical Key Selection

Figure 7. User enrolment/registration of the FlexPass prototype [157]. In this scenario, the user performs a query in which images are asynchronously retrieved for example from Google Images using the Google Custom Search API.

User-Adaptable Authentication. During user authentication, users can choose their preferred way to authenticate; either by entering the textual key or the graphical key. Figure 8 illustrates a login scenario in which the user has selected a textual password as her preferred way to login. In each login session, the alternative option (*e.g.*, graphical password) is available to switch based on the user's preference. Entering the textual key follows the same process as traditional passwords. For entering the graphical key, a grid containing the user-selected and system-generated decoy images are presented. The image positions in the selection grid are randomly positioned in each login session. Thereafter, users have to select their images in the specific sequence, as entered in the enrolment phase to login.



FlexPass Login

Username: jonathan

Password: ****************

Login
☑ My preferred way to login
Forgot my secret key
Click below to enable your alternative way to login
Graphical Password

Figure 8. User-adaptable authentication in which the user can choose between the textual and graphical mechanism [157].

6.3 Initial Personas

Persona is a User-Centered Design method that provides a practical approach to understanding better the requirements and simultaneously keeping user perspectives in mind when designing interactive systems [172]. Personas represent patterns of users' behavior, goals and motives, compiled in a fictional description of a single individual [172]. It also contains made-up personal details, in order to make the persona more tangible, alive and memorable for the development team [173].

Within a User-Centered Design approach, personas are refined throughout the projects lifetime by taking into consideration results of conducted user studies. Accordingly, we have used the information from the semi-structured interviews to develop four preliminary personas based on typical user profiles of the Serums system. The personas will be used as a basis for the baseline evaluation studies and will be further refined and validated in *D5.3 - Software on the Refined Verified User Authentication Scheme*. The images used for the personas were derived from [174-177].

Rolf Mueller – Doctor

Demographics
- 52 years old male
- Cardiologist
- Languages: German and English (secondary)

Education
- MD Cardiology in the USA

Goals
- Access E-Health portal as fast and hassle-free as possible

Rolf is a medical doctor with specialization in cardiology. Rolf is working for over 20 years at a large healthcare organization in Germany. Rolf needs to authenticate several times per week to the E-Health portal of his organization. Rolf is travelling very frequently attending medical conferences, hence he uses interchangeable interaction device types to access the portal depending on the context of use. The framework maintains for Rolf a static and dynamic (change over time) user profile, from which no variations relating to human factors can be derived (*e.g.*, text and image processing has no differences for this individual). In this case the technology factor is considered as predominant. Rolf has already a text-based password, however he would like to be able to authenticate depending on the interaction device used through a recognition-based method as he prefers this rather than typing letters in the small virtual keyboard of his mobile phone. The healthcare organization has a user-friendly password policy and allows a user, through the FlexPass framework, to create semantically similar text- or picture-based passwords with the aim to deliver according to the user preferences best-fit solutions.

Linda Parker – Caregiver

Demographics
- 29 years old female
- Languages: Spanish and English (secondary)

Education
- Diploma in Caregiving in Spain

Goals
- Access patient records as fast as possible

Linda is a caregiver and has just started working at a large healthcare organization in Spain. Linda provides assistance to the elderly by visiting their homes. For planning her visits, she uses a smart calendar application. Linda is using interchangeable, depending on circumstances, various interaction device types (desktop, mobile or tablet) to access her patient profiles. FlexPass maintains an expanded user and modelling profile of Linda and compares this static profile with other registered users with similar static (age, gender, region, etc.) and dynamic (number of attempts to authenticate, error rates, etc.) characteristics. Through its embedded adaptive collaborative mechanisms that exploit the preference and recommendations of other people (sharing similar profiles) the framework decides to recommend to Linda a recognition- or pattern-based user authentication mechanism than the usual text-based user authentication mechanism.

Emma Bielka – Patient

Emma is in her retirement and one of her hobbies is to travel around the world. Emma also uses a smart E-Health application which provides recommendations for a healthier lifestyle, *e.g.*, recommendations for being more active, socialize with friends, etc. The application also allows access to the daily medicine that was prescribed by her doctor. Since Emma is a frequent traveler, she uses interchangeable various interaction device types (desktop, mobile or tablet) to access her E-Health application. The framework takes into consideration that the cognitive and visual strengths of human declines over time, and hence it weighs the user cognitive factor as predominant. The framework decides to recommend to Emma a recognition-based authentication mechanism than the usual text-based password mechanism which requires from a user to recall information (that is a heavier cognitive process). Emma is excited that this provider offers alternative user authentication solutions as she had difficult times to remember and type her password through her medium-sized mobile interaction device.

Demographics
- 68 years old female
- In her retirement
- Occupation prior to retirement: Real estate agent
- Languages: Dutch and German (secondary)

Education
- Property and Construction Management at the University of Salford, Manchester, UK

Hobbies
- Travelling

Goals
- Access her E-Health application efficiently

John Hart – IT Expert with specialization in Cybersecurity

John is a 34-year-old passionate IT expert at a large healthcare organization in Europe. The organization’s mission is to provide technology-driven services to its patients aiming to provide high quality and patient-centric care. John works at the Cybersecurity department with specialization on penetration testing. Also, John is responsible for accessing and maintaining the user records in which he first needs to authenticate several times per day. Since he is familiar with textual passwords and very efficient in typing text, he prefers to login through a traditional textual password mechanism. For increased security, John also needs to verify his identity by approving an OTP push notification before proceeding to the login screen.

Demographics
- 34 years old male
- Native languages: English

Education
- M.Sc. in Cyber Security, University of Bristol, UK
- B.Sc. Computer Science, University College London, UK

Computer Proficiency
- Experienced in cryptography
- Experienced penetration tester

Goals
- Provide secure services to various stakeholders in his organization

6.4 Initial Security Measurements and Metrics

In this section, we describe the initial security and usability measurements and metrics that will be used for the design and development of the initial user authentication system (*D5.2 - Software on the Initial Verified User Authentication System*). These metrics will also be used in the initial evaluation studies of the project (*D7.3 - Initial Report on Use Cases and Evaluation*) for evaluating the baseline user authentication schemes at the end-user organizations and the initial user authentication system. According to the outcome of the evaluation studies, the reported metrics and policies will be refined and reported in *D5.3 - Software on the Refined Verified User Authentication Scheme*.

Key space

Description: Key space (k_p) is defined as the set of all different permutations of a key [138]. It is usually designed to be large enough to prevent adversaries from using brute-force attacks. The key space range is determined by the adopted password policy which declares number of unique codes and password length.

Relevant Success Indicator: SI 1
Relevant Key Performance Indicator: KPI 1.1 – Guessability

Theoretical entropy

Description: Entropy is a measure on how difficult it is to guess a password [138]. In particular, entropy is measured as the expected value (in bits) of the information contained in a string [137], and can be related to authentication key strength by providing a lower bound on the expected number of guesses to find a text. The primary difference between key space and entropy is that key space is an absolute measure of maximum combinations, whereas entropy is related to how users select from the key space. The password key space (k_p) can be related directly to the maximum entropy as follows [139]:

$$H_{max} = log_2 k_p \; [\text{bits}]$$

Relevant Success Indicator: SI 1
Relevant Key Performance Indicator: KPI 1.1 – Guessability

Practical entropy

Description: A true measure of Shannon's theoretical entropy cannot be computed in cases of user-chosen authentication keys since users tend to choose more memorable than random keys. For measuring practical entropy, we will use modern tools and services that entail methods to estimate the entropy of passwords. For example, we intent to use methods from KeePass [179] which is a free and open-source password manager that implements an algorithm to measure entropy. In addition, we will consider the work described in [83, 84] utilizing a variation of Shannon's entropy calculation. In particular, since Shannon's formula allows to calculate in an additive manner, the adjusted calculation formula measures the practical entropy based on the various facets of the generated authentication keys by considering the placement of each character class (lower-case, upper-case, numbers, symbols) and image, and the content of each character and image. The final entropy is the summation of the entropy calculation of each facet.

Relevant Success Indicator: SI 1
Relevant Key Performance Indicator: KPI 1.1 – Guessability

Guess number

Description: Guess number refers to how many guesses a particular password-cracking algorithm with particular training data would take to guess a password. For textual passwords, we will assess the strength of user-generated password keys using Carnegie Mellon University's Password Guessability Service (PGS) [135]. To perform the password guessability calculations, PGS uses four high-level approaches to password cracking: *i)* using the software tool oclHashcat; *ii)* using the software tool John the Ripper; *iii)* using probabilistic Markov models; and *iv)* using a probabilistic context-free grammar implementation (PCFG).

For graphical passwords, we will assess the strength of user-generated graphical password keys by measuring their resistance to an offline brute-force attack. We will implement a brute-force attack that will check all possible permutations of graphical keys, starting from the upper left corner of the image and traversing it row-by-row. We selected this for implementing the exhaustive password search based on research findings which revealed that when users are browsing a page of images they tend to scan the image grid in a horizontal pattern line by line [168, 169]. We will measure guessability by calculating the average "guesses" performed per user until each corresponding graphical password is guessed correctly.

Relevant Success Indicator: SI 1
Relevant Key Performance Indicator: KPI 1.1 – Guessability

Graphical password complexity

Description: An additional measure for graphical passwords is graphical password complexity. This will be calculated, using the equation developed by Sun et al. [170] as follows:

$$PS_P = S_p \, x \, log_2 \, (L_p + I_p + O_p)$$

In the above equation, S_p is the size of the password (*i.e.*, total number of images); L_p is the physical length of the password (*i.e.*, the sum of the Euclidean distances between the selected images of the password); I_p is the total number of intersections (*i.e.*, when two non-consecutive line segments have a common point); and O_p is the number of overlaps of the password pattern (*i.e.*, when a line segment of the password pattern is covered by another segment). The higher the score, the more complex the password is.

Relevant Success Indicator: SI 1
Relevant Key Performance Indicator: KPI 1.1 – Guessability

Shoulder surfing rate

Description: Following state-of-the-art approaches for measuring shoulder surfing attacks (*e.g.*, [77]), shoulder surfing will be measured with participants that will act as shoulder surfers which will perform a hypothetical shoulder surfing attack. Shoulder surfing attacks will be based on a one-time view of the input followed by three guesses. For each password-entry, we will compute the binary success (true/false) and the relative success rate (overlap of correct digits) based on the best of the three guesses.

Relevant Success Indicator: SI 1
Relevant Key Performance Indicator: KPI 1.2 – Password leaks (through social engineering)

Password cracking resistance

Description: The password cracking rate will be measured in a leaked database storing hardened credentials through an offline brute-force attack.

Relevant Success Indicator: SI 2
Relevant Key Performance Indicator: KPI 2.1 – Password cracking resistance

6.5 Initial Usability Measurements and Metrics

Time to register

Description: Time to register will be measured from page load (after training) until the user successfully creates the password, for attempts that will be completed at first trial.

Relevant Success Indicator: N/A
Relevant Key Performance Indicator: N/A

Time to login

Description: Time to login will be measured from user's engagement with the password entry until a successful login occurs.

Relevant Success Indicator: N/A
Relevant Key Performance Indicator: N/A

Memory time

Description: Following existing approaches for measuring the memorability of a password [156], memory time will be measured over time by considering the login attempts of the end-users. In particular, memory time refers to the greatest length of time between a password creation and a successful password login using the same password. As an additional measure of memorability, the number of password resets per participant will be used. The longer the memory time, the higher the memorability, while the less the number of password resets per participant, the higher the memorability.

Relevant Success Indicator: SI 1
Relevant Key Performance Indicator: KPI 1.2 – Password leaks (through social engineering)

Perceived usability

Description: Usability and User Experience questionnaires will be designed for the assessment of perceived usability. Accredited questionnaires such as SUS, AttrakDiff, etc. will also be used for measuring perceived usability. Furthermore, interviews will be conducted, which will enable the interviewer to collect detailed information from the interviewees regarding the perceived usability. Thematic content analysis will be used in order to find common patterns across the data set on the perceived usability. Last, focus groups will be conducted to elicit end-users' perceptions about the perceived usability. The qualitative analysis of Focus Groups results will be a five-step process that includes Data Grouping, Information Labels, Knowledge (Findings), Theory, and Implications.

Relevant Success Indicator: SI 3
Relevant Key Performance Indicator: KPI 3.1 – Perceived Usability

Perceived memorability

Description: Specific questionnaires will be designed for the assessment of perceived memorability. Specific rules will be used for producing scores based on the answers of respondents. Furthermore, interviews will be conducted, which will enable the interviewer to collect detailed information from the interviewees regarding the perceived memorability. Thematic content analysis will be used in order to find common patterns across the data set on the perceived memorability. Last, focus groups will be conducted to elicit end-users' perceptions about the perceived memorability. The qualitative analysis of Focus Groups results will be a five-step process that includes Data Grouping, Information Labels, Knowledge (Findings), Theory, and Implications.

Relevant Success Indicator: SI 3
Relevant Key Performance Indicator: KPI 3.2 – Perceived memorability

Perceived security

Description: Specific questionnaires will be designed for the assessment of perceived security. Specific rules will be used for producing scores based on the answers of respondents. Furthermore, interviews will be conducted, which will enable the interviewer to collect detailed information from the interviewees regarding the perceived security. Thematic content analysis will be used in order to find common patterns across the data set on the perceived security. Last, focus groups will be conducted to elicit end-users' perceptions about the perceived security. The qualitative analysis of Focus Groups results will be a five-step process that includes Data Grouping, Information Labels, Knowledge (Findings), Theory, and Implications.

Relevant Success Indicator: SI 3 ***Relevant Key Performance Indicator:*** KPI 3.2 – Perceived security

Perceived trust
Description: Technology Acceptance Model questionnaires will be designed for the assessment of perceived trust. Specific rules will be used for producing scores based on the answers of respondents. ***Relevant Success Indicator:*** SI 3 ***Relevant Key Performance Indicator:*** KPI 3.4 – Trust in the proposed PUA scheme

6.6 Initial Evaluation Measurements and Metrics for Push Notifications

Accuracy of push notifications
Description: Accuracy of the suggested push notification method will be assessed through False Acceptance Rate (FAR), False Reject Rate (FRR), Failure To Enroll (FTE), Failure to Acquire (FTA) [152]. ***Relevant Success Indicator:*** SI 1 ***Relevant Key Performance Indicator:*** KPI 1.1 – Guessability

Integration of push notifications
Description: Integration capabilities of the suggested push notification method will be assessed based on hardware compatibility, software compatibility, systems interoperability, vendor independency, and access to source code [152]. ***Relevant Success Indicator:*** N/A ***Relevant Key Performance Indicator:*** N/A

6.7 Serums: Adaptive and Adaptable User Authentication Policy

For designing the initial user authentication policy of the Serums authentication system, we have considered the constraints of the three end-user organizations as well as followed state-of-the-art security metrics and authentication policies [71, 83, 138]. In Table 4 we summarize the main characteristics of the proposed user authentication policy.

The proposed user authentication paradigm relies on a single, user-selected secret that can be reflected as a textual key and a graphical key. Hence, we will apply various policies for each knowledge-based authentication type. The textual password keys will rely on a basic 16-character password policy, allowing the creation of dictionary words with no composition requirements. Studies have shown that the proposed policy is more usable and as secure as traditional complex 8-character policies [83] (NIST predicts that both policies generate 30 bits of security entropy [38]). The recognition-based graphical keys will rely on a 5-image policy out of a 14x9 image grid which generates 34.41 bits of security entropy [167]. We chose this policy as a guideline by following well-cited works that consider this entropy as sufficient for everyday computing [86, 126]. The recall-based graphical keys are created as gestures on a background image that acts as a cue. Following the implementation of Microsoft Windows^{TM} Picture Gesture Authentication [171], a minimum of three types of gestures are allowed: taps, lines and circles. Free line gestures are not permitted, hence, they are automatically converted into one of the three permitted gestures. According to [178], a 3-gesture picture password generates 1,155,509,083 different combinations, a 5-gesture picture password generates 612,157,353,732 combinations, and 5-gesture picture password 398,046,621,309,172 combinations.

Table 4. Summary of baseline security aspects of the user authentication mechanisms at the three end-user organizations.

	Policy 1	**Policy 2**	**Policy 3**
Main user authentication type	Textual password	Recognition-based graphical password	Recall-based graphical password
Minimum length	16 alphanumeric characters	5 images	3 gestures on 1 image
Dictionary check	Dictionary words are allowed	No check	No check
Policy within the network	Textual password, At least 16 characters with no restrictions applied Two-factor authentication (Password + Push notification)	Grid of images, length>=5 images out of 120 images during registration During login, a set of 25 images will be displayed including the 5 user images and 20 decoy images Two-factor authentication (Graphical password + Push notification)	Gestures on an image background length>= 3 gestures any combination of a single tap, line, and circle Two-factor authentication (Graphical password + Push notification)
Policy outside the network	VPN connection, Same policy as within		
Alternative Authentication	Selection between textual passwords and graphical passwords depending on users' preference and/or usage statistics		
Waiting time between failed login attempts	No waiting time		
Maximum login attempts	5 attempts		
Authentication process logging	Yes		
Action taken after exceeding the maximum allowed login attempts	*(Depending on organization's internal policy)* lock account and require users to follow the password reset method, or automatically unlock account at the end of the day		
Password life	90 days		
Password reset method	*(Depending on organization's internal policy)* Contact organization's helpdesk and answer security questions, or reset through dedicated mobile application		

In order to increase the security of the knowledge-based authentication schemes, service providers have the option to apply a second layer of authentication using push notifications in which users will be required to approve a notification (SMS or mobile application) in order to proceed entering their preferred user authentication type.

During login, no waiting time will be applied between unsuccessful logins, however, the account will be locked after five unsuccessful login attempts. In order to unlock the account, three methods will be followed depending on the organization's internal policy: *i)* users will contact the organization's helpdesk and answer specific security questions to unlock their account; *ii)* users will reset their authentication key through a dedicated mobile application that will send a one-time password reset code that will be approved by the user in order to start the creation process of the new authentication key; and *iii)* the account will be automatically unlocked at the end of the day that the password was locked. Passwords will be forced to be reset after 90 days. Finally, given the User-Centered Design nature of the user authentication system, usage statistics (*e.g.*, time to login, number of failed attempts, number of password resets, etc.) will be applied aiming to evaluate the usability of the user authentication scheme for each user and identify possible usability issues.

In this realm, it is important to note that the suggested policy will be adjustable based on the organization's internal policy as well as the unique characteristics of each user. The idea is to move from "one-size-fits-all" user authentication policies, towards adaptive and adaptable policies which will be personalized to each user's characteristics and service provider's requirements and constraints. Figure 9 illustrates a personalization paradigm in which the "best-fit" user authentication design (*e.g.*, textual *vs.* graphical), framed by a given security policy, is provided to the users considering human factors (*e.g.*, cognitive abilities, preference) and technology factors (*e.g.*, device type). Such a personalization approach would support multiple security policies, aligned to multiple individual context models' groups. It would also allow service providers to fully customize usability aspects of user authentication towards the benefit of end-users.

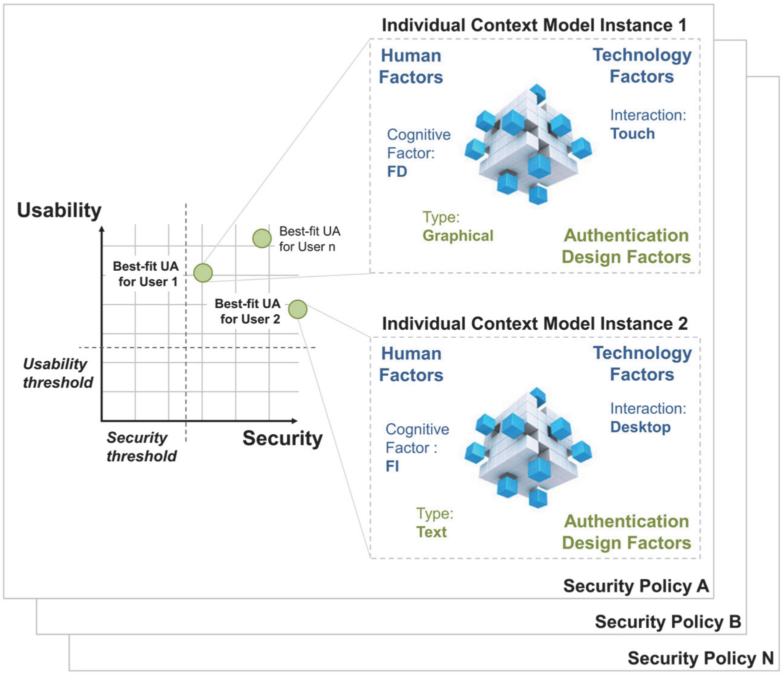


Figure 9. "Best-fit" authentication type, framed by a security policy [115].

7 Conclusions

The aim of this deliverable *"D5.1 - Initial Report on Security Metrics and Authentication Policies"* is to propose the main user authentication types and approach, identify initial personas and use-cases, as well as identify initial evaluation metrics and policies of the Serums user authentication system. For doing so, we have conducted a thorough analysis of state-of-the-art research and practices in user authentication along three pillars (knowledge-based authentication, token-based authentication, biometric-based authentication) as well as an analysis of state-of-the-art security and usability metrics. We further conducted a literature review on user authentication practices in healthcare environments, and a series of semi-structured interviews with nine stakeholders with various backgrounds and roles (Chief Information Security Officers, Enterprise Architects, Department Managers, etc.) from three different countries. Main aim of these interviews was to elicit current user authentication policies, practices and procedures at large healthcare organizations in Europe, as well as to form a baseline of the suggested user authentication metrics and policies that will be applied at the three end-user organizations during the evaluation studies.

These tasks are an essential first step towards an iterative software development cycle of the user authentication scheme. It is important to stress that within a User-Centered Design approach, the current document is a living document which is continuously revised and enhanced throughout the project's lifetime according to research and technology developments, stakeholders' and end-users' feedback and partner's refined vision of Serums. Evidently, the research dimension of Serums will be a predominant factor in the evolution of this document.

References

[1] Vasco DIGIPASS GO range, last visited May 2019, https://www.vasco.com/products/two-factor-authenticators/hardware/one-button/digipass-go-6.html

[2] RSA SecurID, last visited May 2019, http://www.rsa.com/node.aspx?id=1156

[3] Feitian OTP tokens, last visited June 2011, http://www.ftsafe.com/products/otp.html

[4] SafeNet SafeWord GOLD, last visited May 2019, https://safenet.gemalto.com/uploadedFiles/Support_and_Downloads/SafeWord/SafeWord_Authenticators_Administration_Guide__all_versions.pdf

[5] Van Rijswijk, R. M., & Van Dijk, J. (2011, December). tiqr: a novel take on two-factor authentication. In Proceedings of LISA'11: 25th Large Installation System Administration Conference (p. 81).

[6] A. Litan, "SMS/OTP under attack – Man in the Mobile", Gartner, last visited May 2019, https://blogs.gartner.com/avivah-litan/2010/09/28/smsotp-under-attack-man-in-the-mobile/

[7] Kaavi, Janne. "Strong authentication with mobile phones." Helsinki University of Technology, Fall (2010).

[8] Mare, Shrirang, Mary Baker, and Jeremy Gummeson. "A study of authentication in daily life." In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016), pp. 189-206. 2016.

[9] Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. "Multi-factor authentication: A survey." Cryptography 2, no. 1 (2018): 1.

[10] Schneier, B. Two-factor authentication: Too little, too late. Commun. ACM 2005, 48, 136

[11] Petsas, T.; Tsirantonakis, G.; Athanasopoulos, E.; Ioannidis, S. Two-factor authentication: Is the world ready?: Quantifying 2FA adoption. In Proceedings of the 8th European Workshop on System Security, Bordeaux, France, 21 April 2015; ACM: New York, NY, USA, 2015; p. 4.

[12] Wang, D.; He, D.; Wang, P.; Chu, C.H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Trans. Dependable Secur. Comput. 2015, 12, 428–442.

[13] Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput. Secur. 2011, 30, 208–220.

[14] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." IEEE Transactions on circuits and systems for video technology 14, no. 1 (2004).

[15] Jain, Anil K., and Ajay Kumar. "Biometric recognition: an overview." In Second generation biometrics: The ethical, legal and social context, pp. 49-79. Springer, Dordrecht, 2012.

[16] Unar, J. A., Woo Chaw Seng, and Almas Abbasi. "A review of biometric technology along with trends and prospects." Pattern recognition 47, no. 8 (2014): 2673-2688.

[17] Lee, J.D.; Caven, B.; Haake, S.; Brown, T.L. Speech-based interaction with in-vehicle computers: The effect of speech-based e-mail on drivers' attention to the roadway. Hum. Factors 2001, 43, 631–640.

[18] Thullier, F.; Bouchard, B.; Menelas, B.A.J. A Text-Independent Speaker Authentication System for Mobile Devices. Cryptography 2017, 1, 16.

[19] Hautamäki, R.G.; Kinnunen, T.; Hautamäki, V.; Laukkanen, A.M. Automatic versus human speaker verification: The case of voice mimicry. Speech Commun. 2015, 72, 13–31.

[20] Hautamäki, R.G.; Kinnunen, T.; Hautamäki, V.; Leino, T.; Laukkanen, A.M. I-vectors meet imitators: On vulnerability of speaker verification systems against voice mimicry. In Proceedings of the Interspeech, Lyon, France, 25–29 August 2013; pp. 930–934.

[21] Ahonen, T.; Hadid, A.; Pietikainen, M. Face description with local binary patterns: Application to face recognition. IEEE Trans. Pattern Anal. Mach. Intell. 2006, 28, 2037–2041

[22] Zhao, W.; Chellappa, R.; Phillips, P.J.; Rosenfeld, A. Face recognition: A literature survey. ACM Comput. Surv. (CSUR) 2003, 35, 399–458.

[23] Smeets, D.; Claes, P.; Vandermeulen, D.; Clement, J.G. Objective 3D face recognition: Evolution, approaches and challenges. Forensic Sci. Int. 2010, 201, 125–132.

[24] Kakadiaris, I.A.; Passalis, G.; Toderici, G.; Murtuza, M.N.; Lu, Y.; Karampatziakis, N.; Theoharis, T. Three-dimensional face recognition in the presence of facial expressions: An annotated deformable model approach. IEEE Trans. Pattern Anal. Mach. Intell. 2007, 29, 640–649

[25] Wójtowicz, W.; Ogiela, M.R. Biometric watermarks based on face recognition methods for authentication of digital images. Secur. Commun. Netw. 2015, 8, 1672–1687.

[26] Tan, T.; He, Z.; Sun, Z. Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition. Image Vis. Comput. 2010, 28, 223–230.

[27] Bhattacharyya, D.; Ranjan, R.; Alisherov, F.; Choi, M. Biometric authentication: A review. Int. J. u- e-Serv. Sci. Technol. 2009, 2, 13–28.

[28] Bowyer, K.W.; Burge, M.J. Handbook of Iris Recognition; Springer: Berlin, Germany, 2016.

[29] Wong, Alexandra LN, and Pengcheng Shi. "Peg-Free Hand Geometry Recognition Using Hierarchical Geomrtry and Shape Matching." In MVA, pp. 281-284. 2002.

[30] Zheng, Gang, Chia-Jiu Wang, and Terrance E. Boult. "Application of projective invariants in hand geometry biometrics." IEEE transactions on Information Forensics and Security 2, no. 4 (2007): 758-768.

[31] Guo, Jing-Ming, Yun-Fu Liu, Mei-Hui Chu, Chia-Chu Wu, and Thanh-Nam Le. "Contact-free hand geometry identification system." In 2011 18th IEEE International Conference on Image Processing, pp. 3185-3188. IEEE, 2011.

[32] Kumar, A.; Hanmandlu, M.; Madasu, V.K.; Lovell, B.C. Biometric authentication based on infrared thermal hand vein patterns. In Proceedings of the Digital Image Computing: Techniques and Applications (DICTA'09), Melbourne, Australia, 1–3 December 2009; pp. 331–338.

[33] Kang, W.; Wu, Q. Contactless palm vein recognition using a mutual foreground-based local binary pattern. IEEE Trans. Inf. Forensics Secur. 2014, 9, 1974–1985.

[34] Piekarczyk, M.; Ogiela, M.R. Touch-Less Personal Verification Using Palm and Fingers Movements Tracking. In New Trends in Analysis and Interdisciplinary Applications; Springer: Berlin, Germany, 2017; pp. 603–609.

[35] Tome, P.; Vanoni, M.; Marcel, S. On the vulnerability of finger vein recognition to spoofing. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10–12 September 2014; pp. 1–10.

[36] Tome, P.; Marcel, S. On the vulnerability of palm vein recognition to spoofing attacks. In Proceedings of the International Conference on Biometrics (ICB), Phuket, Thailand, 9–22 May 2015; pp. 319–325.

[37] Yang, Wencheng, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. "Security and accuracy of fingerprint-based biometrics: A review." Symmetry 11, no. 2 (2019): 141.

[38] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." IEEE Transactions on circuits and systems for video technology 14, no. 1 (2004).

[39] Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain. "Biometric recognition: Security and privacy concerns." IEEE security & privacy 2 (2003): 33-42.

[40] Jain, Anil K., Ruud Bolle, and Sharath Pankanti, eds. Biometrics: personal identification in networked society. Vol. 479. Springer Science & Business Media, 2006.

[41] Maltoni, Davide, Dario Maio, Anil K. Jain, and Salil Prabhakar. Handbook of fingerprint recognition. Springer Science & Business Media, 2009.

[42] De Luca, Alexander, and Janne Lindqvist. "Is secure and usable smartphone authentication asking too much?." Computer 48, no. 5 (2015): 64-68.

[43] Krišto, Mate, and Marina Ivasic-Kos. "An overview of thermal face recognition methods." In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1098-1103. IEEE, 2018.

[44] Kong, Seong G., Jingu Heo, Faysal Boughorbel, Yue Zheng, Besma R. Abidi, Andreas Koschan, Mingzhong Yi, and Mongi A. Abidi. "Multiscale fusion of visible and thermal IR images for illumination-invariant face recognition." International Journal of Computer Vision 71, no. 2 (2007): 215-233.

[45] Guzman, Ana M., Mohammed Goryawala, Jin Wang, Armando Barreto, Jean Andrian, Naphtali Rishe, and Malek Adjouadi. "Thermal imaging as a biometrics approach to facial signature authentication." IEEE journal of biomedical and health informatics 17, no. 1 (2012): 214-222.

[46] Bhowmik, M. K., Saha, K., Majumder, S., Majumder, G., Saha, A., Sarma, A. N., ... & Nasipuri, M. (2011). Thermal infrared face recognition–a biometric identification technique for robust security system. In Reviews, refinements and new ideas in face recognition. IntechOpen.

[47] Hu, Shuowen, Jonghyun Choi, Alex L. Chan, and William Robson Schwartz. "Thermal-to-visible face recognition using partial least squares." JOSA A 32, no. 3 (2015): 431-442.

[48] Denning, Dorothy E., and Peter F. MacDoran. "Location-based authentication: Grounding cyberspace for better security." Computer Fraud & Security 1996, no. 2 (1996): 12-16.

[49] Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2016). Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. IEEE Systems Journal, 11(2), 513-521.

[50] Mahbub, U., & Chellappa, R. (2016, October). PATH: person authentication using trace histories. In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 1-8). IEEE.

[51] Javaid, Ahmad Y., Farha Jahan, and Weiqing Sun. "Analysis of Global Positioning System-based attacks and a novel Global Positioning System spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation." Simulation93, no. 5 (2017): 427-441.

[52] Hammad, A., & Faith, P. (2017). U.S. Patent No. 9,721,250. Washington, DC: U.S. Patent and Trademark Office.

[53] Nighswander, Tyler, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley. "GPS software attacks." In Proceedings of the 2012 ACM conference on Computer and communications security, pp. 450-461. ACM, 2012.

[54] M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition," In Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing, Apr. 2007. USA, pp. 121 - 126.

[55] Sharif, Mahmood, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1528-1540. ACM, 2016.

[56] Kurakin, Alexey, Ian Goodfellow, and Samy Bengio. "Adversarial examples in the physical world." arXiv preprint arXiv:1607.02533 (2016).

[57] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca, “GEORBAC: A Spatially Aware RBAC,” ACM Transactions on Information and System Security, vol. 10, Feb. 2007, doi:10.1145/1210263.1210265.

[58] D. Kulkarni and A. Tripathi, “Context-Aware Role-based Access Control in Pervasive Computing Systems,” Proceedings of the 14th Symposium on Access Control Models and Technologies (SACMAT), 2008.

[59] R. J. Hulsebosch, A. H. Salden, M. S. Bargh, P. W. G. Ebben and J. Reitsma, “Context Sensitive Access Control,” Proceedings of the 11th Symposium on Access Control Models and Technologies (SACMAT), 2005, pp. 111-119.

[60] Bertino, Elisa, and Michael Kirkpatrick. "Location-Aware Authentication and Access Control Concepts and Issues." In 2009 International Conference on Advanced Information Networking and Applications, pp. 10-15. IEEE, 2009.

[61] Shrestha, B.; Mohamed, M.; Tamrakar, S.; Saxena, N. Theft-resilient mobile wallets: Transparently authenticating NFC users with tapping gesture biometrics. In Proceedings of the 32nd Annual Conference on Computer Security Applications, Los Angeles, CA, USA, 5–9 December 2016; ACM: New York, NY, USA, 2016; pp. 265–276.

[62] Gascon, H.; Uellenbeck, S.; Wolf, C.; Rieck, K. Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior. In Proceedings of the Conference “Sicherheit”, Sicherheit, Schutz und Verlässlichkeit, 19–21 March 2014; pp. 1–12.

[63] Buschek, D.; De Luca, A.; Alt, F. Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; ACM: New York, NY, USA, 2015; pp. 1393–1402.

[64] Meng, W.; Wong, D.S.; Furnell, S.; Zhou, J. Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surv. Tutor. 2015, 17, 1268–1293.

[65] Buriro, A.; Crispo, B.; Del Frari, F.; Wrona, K. Touchstroke: Smartphone user authentication based on touch-typing biometrics. In Proceedings of the International Conference on Image Analysis and Processing, Niagara Falls, ON, Canada, 22–24 July 2015; Springer: Berlin, Germany, 2015; pp. 27–34.

[66] Van Goethem, T.; Scheepers, W.; Preuveneers, D.; Joosen, W. Accelerometer-based device fingerprinting for multi-factor mobile authentication. In Proceedings of the International Symposium on Engineering Secure Software and Systems, London, UK, 6–8 April 2016; Springer: Berlin, Germany, 2016; pp. 106–121.

[67] Figueira, C.; Matias, R.; Gamboa, H. Body Location Independent Activity Monitoring. In Proceedings of the International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSIGNALS), Rome, Italy, 21–23 February 2016; pp. 190–197.

[68] Grankin, M.; Khavkina, E.; Ometov, A. Research of MEMS accelerometers features in mobile phone. In Proceedings of the 12th Conference of Open Innovations Association FRUCT, Oulu, Finland, 5–9 November 2012; pp. 31–36.

[69] Arra, Adriano, Alessio Bianchini, Joana Chavez, Pietro Ciravolo, Fatjon Nebiu, Martina Olivelli, Gabriele Scoma, Simone Tavoletta, Matteo Zagaglia, and Alessio Vecchio. "Personalized Gait-based Authentication Using UWB Wearable Devices." In Proceedings of the 27th ACM Conference on User Modeling, Adaptation and Personalization, pp. 206-210. ACM, 2019.

[70] Koved, L., & Stobert, E. (2016). Who are you?! Adventures in authentication (WAY). Workshop at the Symposium on Usable Privacy and Security (SOUPS 2016), USENIX Association.

[71] Biddle, R., Chiasson, S., & van Oorschot, P. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4), 41 pages.

[72] Mare, S., Baker, M., & Gummeson, J. (2016). A study of authentication in daily life. In Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS 2016), USENIX Association, 189-206.

[73] Renaud, K. (2005). Evaluating authentication mechanisms. In: Cranor, L., Garfinkel, S. (eds.), Security and usability: Designing secure systems that people can use, chapter 6, 103-128. O'Reilly Media.

[74] Wang, J., & Katabi, D. (2013). Dude, where's my card?: RFID positioning that works with multipath and non-line of sight. In Proceedings of the ACM SIGCOMM 2013 Conference, ACM Press, 51-62.

[75] Cao, K., & Jain, A. (2016). Hacking mobile phones using 2D printed fingerprints. MSU Technical Report MSU-CSE-16-2.

[76] Herley, C., & van Oorschot, P. (2012). A research agenda acknowledging the persistence of passwords. Security and Privacy, 10(1), 28-36.

[77] von Zezschwitz, E., De Luca, A., Brunkow, B., Hussmann, H. (2015). SwiPIN: Fast and Secure PIN-Entry on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 1403-1406

[78] Passfaces Corporation (2009). The Science Behind Passfaces. White paper, http://www.passfaces.com/enterprise/resources/white_papers.htm

[79] Dhamija, R., & Perrig, A. (2000). DejaVu: A user study using images for authentication. In Proceedings of the USENIX Security Symposium, USENIX Association.

[80] Herley, C., van Oorschot, P., & Patrick, A. (2009). Passwords: If we're so smart, why are we still using them? In Financial Cryptography and Data Security, Dingledine, R., & Golle, P. (eds.), LNCS, Vol. 5628, Sprin-ger-Verlag

[81] Bonneau, J., Herley, C., van Oorschot, P., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Proceedings of the Symposium on Security and Privacy (SP 2012), IEEE Computer Society, 553-567

[82] Shay, R., Kelley, P., Komanduri, S., Mazurek, M., Ur, B., Vidas, T., Bauer, L., Christin, N., & Cranor, L. (2012). Correct horse battery staple: Exploring the usability of system-assigned passphrases. In Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2012), ACM Press, Article 7, 20 pages

[83] Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. In Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2011), ACM Press, 2595-2604

[84] Shay, R., Komanduri, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviors. In Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2010), ACM Press, Article 2, 20 pages.

[85] Inglesant, P., & Sasse A. (2010). The true cost of unusable password policies: Password use in the wild. In Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2010), ACM Press, 383-392

[86] Florencio, D., & Herley, C.A. (2007). Large-scale study of web password habits. In Proceedings of the ACM Conference on World Wide Web (WWW 2007), ACM Press, 657-666

[87] Adams, A., & Sasse, A. (1999). Users are not the Enemy: Why users compromise security mechanisms and how to take remedial measures. Communications of the ACM, 42(12), 40-46

[88] Forget, A., & Biddle, R. (2008). Memorability of persuasive passwords. In Extended Abstracts of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2008), ACM Press, 3759-3764

[89] Forget, A., Chiasson, S., van Oorschot, P., & Biddle, R. (2008). Improving text passwords through persuasion. In Proceedings of the ACM Symposium on Usable Security and Privacy (SOUPS 2008), ACM Press, 1-12

[90] Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. IEEE Security & Privacy Magazine, 2(5), 25-31

[91] Wright, N., Patrick, A., & Biddle, R. (2012). Do you see your password?: Applying recognition to textual passwords. In Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2012), ACM Press, Article 8

[92] Vu, K., Proctor, R., Bhargav-Spantzel, A., Tai, B., Cook, J., & Schultz, E. (2007). Improving password securi-ty and memorability to protect personal and organizational information. International Journal of Hu-man-Computer Studies, 65(8), 744-757

[93] Kuo, C., Romanosky, S., & Cranor, L. (2006). Human selection of mnemonic phrase-based passwords. In Proceedings of the ACM International Symposium on Usable Privacy and Security (SOUPS 2006), ACM Press, 67-78

[94] Leonhard, M.D., & Venkatakrishnan, V.N. (2007). A comparative study of three random password generators. In Proceedings of the IEEE International Conference on Electro/Information Technology (EIT 2007), IEEE Computer Society, 227-232

[95] Shay, R., Bauer, L., Christin, N., Cranor, L., Forget, A., Komanduri, S., Mazurek, M., Melicher, W., Segreti, S., & Ur, B. (2015). A spoonful of sugar? The impact of guidance and feedback on password-creation be-havior. In Proceedings of ACM Conference on Human Factors in Computing Systems (CHI 2015), ACM Press, 2903-2912

[96] Nelson, D., & Vu, K. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. Computers in Human Behavior, 26(4), 705-715

[97] Halderman, J.A., Waters, B., & Felten, E. (2005). Convenient method for securely managing passwords. In Proceedings of the ACM International Conference on World Wide Web (WWW 2005), ACM Press, 471-479

[98] Chiasson, S., van Oorschot, P., & Biddle, R. (2006). Usability study and critique of two password managers. In Proceedings of the USENIX Security Symposium, USENIX Association, 1-16

[99] Findlater, L., Wobbrock, J., & Wigdor, D. (2011). Typing on flat glass: Examining ten-finger expert typing patterns on touch surfaces. In Proceedings of the ACM SIGCHI Conference on Human Factors in Com-puting Systems (CHI 2011), ACM Press, 2453-2462

[100] Angeli, A.D., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. Human-Computer Studies, 63(1-2), 128-152

[101] Everitt, K., Bragin, T., Fogarty, J., & Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In ACM International Conference on Human Factors in Computing Systems (CHI 2009), ACM Press, 889-898

[102] Tullis, T.S., Tedesco, D.P., & McCaffrey, K.E. (2011). Can users remember their pictorial passwords six years later? In Proceedings of the ACM SIGCHI International Conference on Human Factors in Computing Systems (CHI 2011), ACM Press, 1789-1794

[103] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The design and analysis of graphical passwords. In Proceedings of the USENIX Security Symposium (Security 1999), USENIX Association, 1-1

[104] Dunphy, P., & Yan, J. (2007). Do background images improve "draw a secret" graphical passwords? In Pro-ceedings of the ACM International Conference on Computer and Communications Security (CCS 2007), ACM Press, 36-47

[105] Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. (2008). YAGP: Yet another graphical password strategy. In Proceedings of the IEEE Conference on Computer Security Applications, IEEE Computer Society, 121-129

[106] Varenhorst, C. (2004). Passdoodles: A lightweight authentication method. MIT Research Science Institute

[107] Tao, H., & Adams, C. (2008). Pass-Go: A proposal to improve the usability of graphical passwords. Network Security, 7(2), 273-292

[108] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2005), ACM Press, 1-12

[109] Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. (2008). Influencing users towards better passwords: Persuasive cued click-points. In Proceedings of the BCS Conference on People and Computers, British Computer Society, 121-130

[110] Bulling, A., Alt, F., & Schmidt, A. (2012). Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In Proceedings of the ACM International Conference on Human Factors in Computing Systems (CHI 2012), ACM Press, 3011-3020

[111] Davis, D., Monrose, F., & Reiter, M. (2004). On user choice in graphical password schemes. In Proceedings of the USENIX Security Symposium, USENIX Association

[112] Mihajlov, M., & Jerman-Blazic, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. Interacting with Computers, 23(6), 582-593

[113] Nicholson, J., Dunphy, P., Coventry, L., Briggs, P., & Olivier, P.A. (2012) Security assessment of tiles: A new portfolio-based graphical authentication system. In Extended Abstracts of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2012), ACM Press, 1967-1972

[114] Nicholson, J., Coventry, L., & Briggs, P. (2013). Age-related performance issues for PIN and face-based authentication systems. In Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2013), ACM Press, 323-332

[115] Belk M., Fidas C., Germanakos P., Samaras G. (2017) The interplay between humans, technology and user authentication: a cognitive processing perspective, Computers in Human Behavior (CHB), 184-200, Elsevier

[116] Belk, M., Germanakos, P., Fidas, C., Samaras, G. (2014). A personalisation method based on human factors for improving usability of user authentication tasks. User Modeling, Adaptation, and Personalization (UMAP 2014), 13-24

[117] Katsini, C., Fidas, C., Raptis, G., Belk, M., Samaras, G., Avouris, N. (2018). Influences of human cognition and visual behavior on password security during picture password composition. ACM SIGCHI Human Factors in Computing Systems (CHI 2018), ACM Press, paper 87

[118] Ma, Y., Feng, J., Kumin, L., & Lazar, J. (2013). Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users. ACM Transactions on Accessible Computing, 4(4), Article 15, 27 pages

[119] Forget, A., Chiasson, S., & Biddle, R. (2014). Towards supporting a diverse ecosystem of authentication schemes. In Proceedings of the Who are you?! Adventures in Authentication Workshop (WAY 2014) at the Symposium on Usable Privacy and Security (SOUPS 2014), USENIX Association

[120] von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014). Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. In Proceedings of the Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (NordiCHI 2014), ACM Press, 461-470

[121] Schlöglhofer, R., & Sametinger, J. (2012). Secure and usable authentication on mobile devices. In Proceedings of the ACM Conference on Advances in Mobile Computing & Multimedia (MoMM 2012), ACM Press, 257-262

[122] Schaub, F., Deyhle, R., & Weber, M. (2012). Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In Proceedings of the Conference on Mobile and Ubiquitous Multime-dia (MUM 2012), ACM Press, 1-10

[123] Brostoff, S., & Sasse, M. A. 2000. Are Passfaces more usable than passwords? A field trial investigation. In People and Computers XIV—Usability or Else!, Springer, 405-424.

[124] Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. (2013). Are graphical authentication mechanisms as strong as passwords?. In Proceedings of the Federated Conference on Computer Science and Infor-mation Systems (FedCSIS 2013), IEEE Computer Society, 837-844

[125] De Luca, A., von Zezschwitz, E., Pichler, L., & Hussmann, H. (2013). Using fake cursors to secure on-screen password entry. In Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2013), ACM Press, 2399-2402

[126] Winkler, C., Gugenheimer, J., De Luca, A., Haas, G., Speidel, P., Dobbelstein, D., & Rukzio, E. (2015). Glass unlock: Enhancing security of smartphone unlocking through leveraging a private near-eye display. In Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2015). ACM Press, 1407-1410

[127] Katsini, C., Belk, M., Fidas, C., Avouris, N., Samaras, G. (2016). Security and Usability in Knowledge-based User Authentication: A Review. PCI 2016: 63

[128] Oechslin, P. 2003. Making a faster cryptanalytic time memory trade-off. In Annual International Cryptology Conference Springer Berlin Heidelberg, 617-630.

[129] Van Oorschot, P. C., & Wan, T. 2009. TwoStep: An authentication method combining text and graphical passwords. In International Conference on E-Technologies Springer Berlin Heidelberg, 233-239

[130] Weir, M., Aggarwal, S., Collins, M., and Stern, H. 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). ACM, New York, NY, USA, 162-175.

[131] De Carné de Carnavalet, X., and Mannan, M. 2014. From very weak to very strong: Analyzing password-strength meters. In Network and Distributed System Security Symposium (NDSS 2014).

[132] Dürmuth, M., Angelstorf, F., Castelluccia, C., Perito, D., & Chaabane, A. 2015. OMEN: Faster password guessing using an ordered markov enumerator. In International Symposium on Engineering Secure Software and Systems (Mar 2015) Springer International Publishing, 19-132.

[133] Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., and Lopez, J. 2012. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In 2012 IEEE Symposium on Security and Privacy (May, 2012) 523-537.

[134] Ma, J., Yang, W., Luo, M., & Li, N. 2014. A study of probabilistic password models. In 2014 IEEE Symposium on Security and Privacy (May 2014) 689-704.

[135] Ur, B., Segreti, S. M., Bauer, L., Christin, N., Cranor, L. F., Komanduri, S., & Shay, R. 2015. Measuring real-world accuracies and biases in modeling password guessability. In USENIX Security Symposium (Security 15). 463-481.

[136] Castelluccia, C., Dürmuth, M., & Perito, D. 2012. Adaptive Password-Strength Meters from Markov Models. In Network and Distributed System Security Symposium (NDSS 2014).

[137] Shannon, C. E. 2001. A mathematical theory of communication. SIGMOBILE Mob. Comput. Commun. Rev. 5, 1 (Jan 2001), 3-55.

[138] Burr, W. E., Dodson, D. F., & Polk, W. T. 2004. Electronic authentication guideline, 800-63. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

[139] O'Gorman, L. 2003. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.

[140] Rass, S., Schuller, D., & Kollmitzer, C. 2010. Entropy of graphical passwords: towards an information-theoretic analysis of face-recognition based authentication. In IFIP International Conference on Communications and Multimedia Security Springer Berlin Heidelberg, 166-177.

[141] Shepard, R. N. 1967. Recognition memory for words, sentences, and pictures. Journal of verbal Learning and verbal Behavior, 6(1), 156-163.

[142] Kayem, A. V. 2016. Graphical Passwords-A Discussion. 30th International Conference on Advanced Information Networking and Applications Workshops. IEEE, 596 – 600.

[143] Srivastava, Shilpa, Millie Pant, Ajith Abraham, and Namrata Agrawal. "The technological growth in eHealth services." Computational and mathematical methods in medicine 2015 (2015).

[144] Kogetsu, Atsushi, Soichi Ogishima, and Kazuto Kato. "Authentication of Patients and Participants in Health Information Exchange and Consent for Medical Research: A Key Step for Privacy Protection, Respect for Autonomy, and Trustworthiness." Frontiers in genetics 9 (2018).

[145] Okoh, Ebenezer, and Ali Ismail Awad. "Biometrics applications in e-health security: A preliminary survey." In International Conference on Health Information Science, pp. 92-103. Springer, Cham, 2015.

[146] Li, Yanyan, Mengjun Xie, and Jiang Bian. "USign—A security enhanced electronic consent model." In 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 4487-4490. IEEE, 2014.

[147] Marohn, Dana. "Biometrics in healthcare." Biometric Technology Today 14, no. 9 (2006): 9-11.

[148] Krawczyk, S., Jain, A.K.: Securing electronic medical records using biometric authentication. In: 5th international conference on Audio- and Video-Based Biometric Person Authentication, AVBPA'05. pp. 1110–1119. Springer-Verlag, Berlin, Heidelberg (2005).

[149] Silva, H., Loureno, A., Fred, A., Filipe, J.: Clinical data privacy and customization via biometrics based on ECG signals. In: Holzinger, A., Simonic, K.M. (eds.) Information Quality in e-Health, Lecture Notes in Computer Science, Vol. 7058, pp. 121–132. Springer Berlin Heidelberg (2011).

[150] Modi, S.K.: Biometrics in identity management: Concepts to applications. Artech House (2011).

[151] Rui, Zhang, and Zheng Yan. "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification." IEEE Access 7 (2018): 5994-6009.

[152] Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. "Multi-factor authentication: A survey." Cryptography 2, no. 1 (2018): 1.

[153] Hassenzahl M, and Tractinsky N (2006) User experience - a research agenda. Behaviour and Information Technology, 25(2):91-97

[154] ISO 9241-11 (1998) Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability. International Organization for Standardization (ISO), Switzerland

[155] ISO 9241-210 (2009) Ergonomics of human system interaction - Part 210: Human-centered design for interactive systems (formerly known as 13407). International Organization for Standardization (ISO), Switzerland

[156] Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. In Proc. of the ACM Symposium on Usable Privacy and Security (SOUPS 2013), ACM Press, article 15, 14 pages.

[157] Belk, M., Fidas, C., Pitsillides, A. (2019). FlexPass: Symbiosis of seamless user authentication schemes in IoT. ACM SIGCHI Human Factors in Computing Systems (CHI 2019), ACM Press

[158] Hadjidemetriou, G., Belk, M., Fidas, C., Pitsillides, A. (2019). Picture passwords in mixed reality: Implementation and evaluation (2019). ACM SIGCHI Human Factors in Computing Systems (CHI 2019), ACM Press

[159] Fidas, C., Belk, M., Hadjidemetriou, G., Pitsillides, A. (2019). Influences of mixed reality and human cognition on picture passwords: An eye tracking study. IFIP TC13 Human-Computer Interaction (INTERACT 2019), Springer-Verlag

[160] Constantinides, A., Belk, M., Fidas, C., Pitsillides, A. (2019). On the accuracy of eye gaze-driven classifiers for predicting image content familiarity in graphical passwords. ACM User Modeling, Adaptation and Personalization (UMAP 2019), ACM Press, 201-205

[161] Win, K.T., Susilo, W., Mu, Y. (2006). Personal Health Record Systems and Their Security Protection, Journal of Medical Systems, 30 (4), 309-315.

[162] Santangelo, J., Christly, J., Sehgal, S., Venkat, C., Wyrick, B. (2016). Two-Factor Authentication and Digital Identity Management in Healthcare. Research Report by Healthcare Informatics & Institute for Health Technology Transformation.

[163] Personalised Centralized Authentication System - PCAS. 7th Framework Programme for Research and Technological Development, Grant Agreement #610713. Available online: https://cordis.europa.eu/project/rcn/110720/factsheet/en

[164] Secure Cloud Identity Wallet – CREDENTIAL. Horizon 2020, Grant Agreement #653454. Available online: https://cordis.europa.eu/project/rcn/194869/factsheet/en

[165] (ultra)Sound Interfaces and Low Energy iNtegrated SEnsors – SILENSE. Horizon 2020, Grant Agreement #737487. Available online: https://cordis.europa.eu/project/rcn/210803/factsheet/en

[166] ACTivating InnoVative IoT smart living environments for AGEing well – ACTIVAGE. Horizon 2020, Grant Agreement #732679. Available online: https://cordis.europa.eu/project/rcn/206513/factsheet/en

[167] Katsini, C., Fidas, C., Belk, M., Samaras, G., Avouris, N. (2019). A human-cognitive perspective of users' password choices in recognition-based graphical authentication. International Journal of Human-Computer Interaction, Taylor and Francis

[168] Djamasbi, S., Siegel, M., and Tullis, T. (2011). Visual hierarchy and viewing behavior: An eye tracking study. In International Conference on Human-Computer Interaction, pages 331-340. Springer.

[169] Shrestha, S. and Lenz, K. (2007). Eye gaze patterns while searching vs. browsing a website. Usability News, 9(1):1-9.

[170] Sun, C., Wang, Y., and Zheng, J. (2014). Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. Journal of Information Security and Applications, 19(4-5):308{320.

[171] Johnson, J.J., Seixeiro, S., Pace, Z., van der Bogert, G., Gilmour, S., Siebens, L., & Tubbs, K. (2014). Picture gesture authentication. Retrieved from https://www.google.com/patents/US8910253

[172] Cooper, Alan. (1999). The Inmates are running the Asylum, Macmillan.

[173] James E. Nieters, Subbarao Ivaturi, Iftikhar Ahmed. (2007). Making Personas Memorable, Conference on Human Factors in Computing Systems, San Jose, CA, US, pp.1817-1824.

[174] Creativeart. Freepik. Retrieved online from: https://www.freepik.com/free-photo/smiling-touching-arms-crossed-room-hospital_1073859.htm

[175] Vgstockstudio. Freepik. Retrieved online from: https://www.freepik.com/premium-photo/female-doctor-is-posing-hospital-reception_4884219.htm

[176] Pressfoto. Freepik. Retrieved online from: https://www.freepik.com/free-photo/healthy-woman-doctor-s-office_862482.htm

[177] Katemangostar. Freepik. Retrieved online from: https://www.freepik.com/free-photo/smiling-young-man-using-tablet-computer_4167190.htm

[178] Sinofsky, S. (2011). Signing in with a picture password. MSDN Blog. Available online: https://blogs.msdn.microsoft.com/b8/2011/12/16/signing-in-with-a-picture-password

[179] KeePass Password Safe. Available online: https://keepass.info/download.html

ABBREVIATIONS

2FA	Two-factor authentication
DAS	Draw-a-Secret
DNA	Deoxyribonucleic acid
ECG	Electrocardiographic
EEG	Electroencephalographic
FAR	False Acceptance Rate
FRR	False Rejection Rate
GPS	Global Positioning System
HCI	Human-Computer Interaction
IoT	Internet of Things
IR	Infrared
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NFC	Near Field Communication
NTLM	New Technology LAN Manager
OTP	One-Time Password
PGS	Password Guessability Service
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SI	Success Indicator
SMS	Short Message Service
UCD	User Centered Design
UX	User Experience

ANNEXES

Interview Schedules

Participants. Stakeholders that relate to the user authentication schemes of the end-user organizations (*e.g.*, Chief Information Security Officer, Policy Maker, Decision Maker, Security Expert, IT Department Manager, etc.)

(Part A) Introduction *(approx. 5 min)*

Give a brief description of Serums and clearly state to the interviewee the purpose of the interview which is to gather information related to the user authentication scheme of the interviewee's organization.

(Part B) Discussion Topics *(approx. 45 min)*

Initial Profiling *(approx. 5 min)*	
Question	Hints for the interviewer
1. Could you please tell us about your **position in your company**? 2. Could you please tell us **about your background**? 3. With regards to the topics listed in the questionnaire, in which stakeholder category would you identify yourself, policy maker, decision maker, security expert? 4. Can you please identify any problems/issues with the current user authentication policy/scheme/procedure at your organization?	The purpose is to understand the background of the interviewee. This will help us to understand the context of his /her answers.

Topic 1: User Authentication Policy *(approx. 20 min)* *Relevant stakeholders: Information Security Officer, Policy Maker, IT Department Manager, etc.*	
Question	Hints for the interviewer
1. How was the current **user authentication policy derived**? 2. Have you based your user authentication policy on existing **best practices, research studies**, etc.? 3. How was the current **user authentication policy applied**? 4. Since **when** is the policy **valid**? 5. **What type of user authentication** (*e.g.*, textual, graphical, etc.) is your organization currently using? 6. How often does the authentication policy **change**? If yes, based on which **data**? 7. Is any **user research applied** for creating the authentication policy? 8. Does your current policy consider **user accessibility aspects**?	The purpose is to understand the current policy and precured applied with regards to user authentication as well as the reasoning behind the design of the policy.

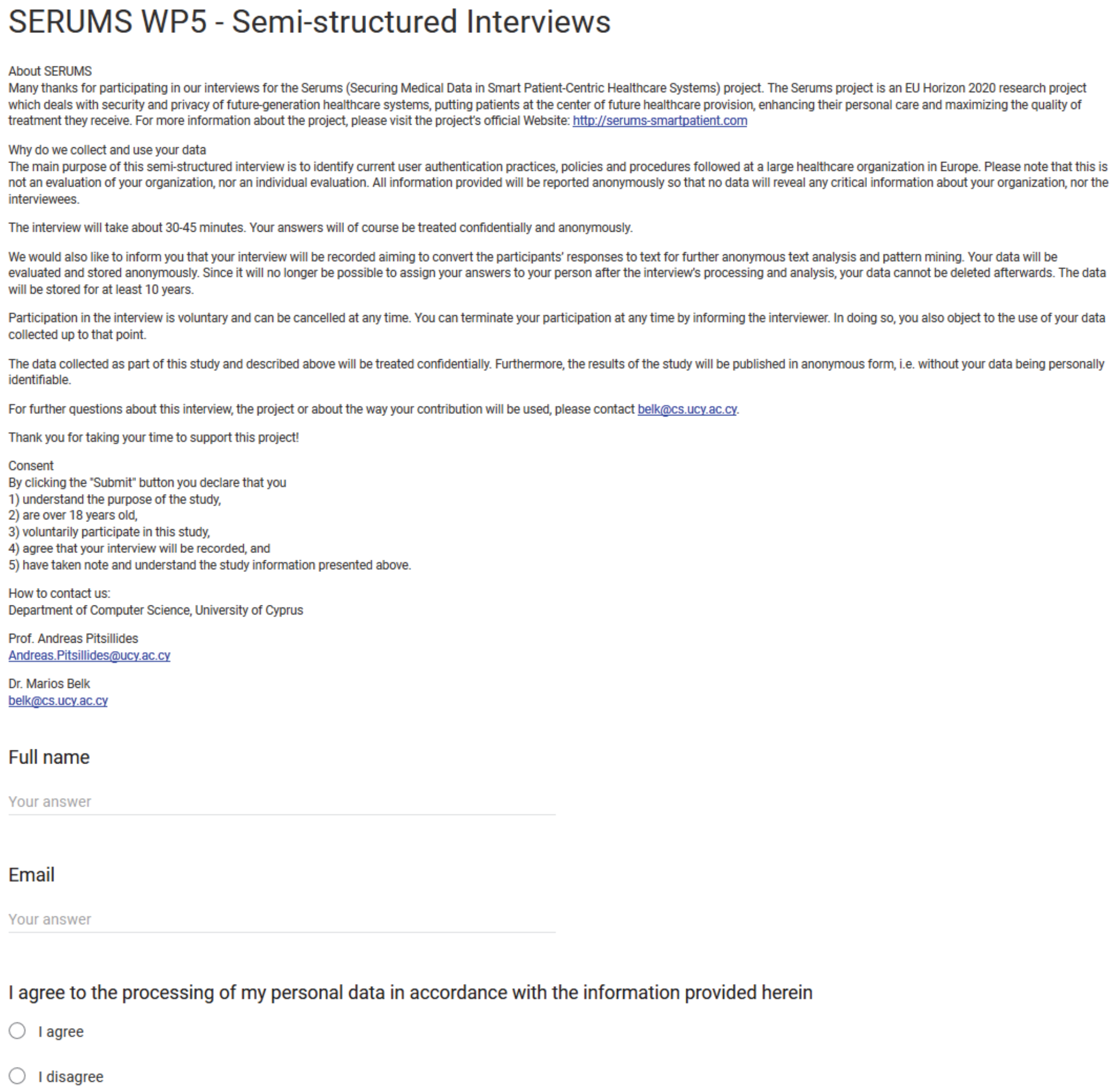
9. Does your current policy consider **usability aspects** in its design? If not, why was not usability considered? 10. Do you consider including a **user-centered design approach** in your user authentication scheme? If not, what are the difficulties to streamline this at your organization? 11. Do you receive **complaints** about your authentication policy? 12. Does your organization deploy different types and policies for user authentication depending on the user's **context of use**? (*e.g.*, use complex passwords for remote access *vs.* medium complex passwords within the network) 13. Could you please describe a **typical profile** of an end-user? 14. Did you experience any **security threats** related to user authentication?	

<table>
<tr><th colspan="2"><b><i>Topic 2: Technical Details and Workflows related to User Authentication Policy</i></b> <i>(approx. 20 min)</i>
<i>Relevant stakeholders: Information Security Officer, IT Department Manager, etc.</i></th></tr>
<tr><td>Question</td><td>Hints for the interviewer</td></tr>
<tr><td>1. What is the <b>minimum allowed password length</b> of your user authentication policy (<i>e.g.</i>, 8 characters)?
2. Does your authentication policy allow to include <b>dictionary words</b> (<i>e.g.</i>, names, objects, etc.)?
3. What is the current <b>password complexity</b> of your applied authentication policy (<i>e.g.</i>, password must have at least 8 characters including an uppercase and lowercase letter, a symbol, and a digit. It may not contain a dictionary word)?
4. Which is the maximum number of days a <b>password may be used</b> (<i>e.g.</i>, between 30 and 90 days)?
5. What is the maximum number of <b>login retries</b> in case of bad password (<i>e.g.</i>, 5)?
6. What is the maximum time (sec) between <b>unsuccessful logins</b> (<i>e.g.</i>, 60 sec)?
7. What is the maximum time (sec) of <b>login timeout</b> when max login retries have been reached (<i>e.g.</i>, 15 minutes)?
8. Does your organization deploy <b>multi-factor authentication</b> to increase security?
9. Which <b>device types are being mostly used</b> for user authentication (<i>e.g.</i>, desktop, smartphones, tablets, etc.)?
10. Which <b>hashing algorithms</b> do you apply at the database layer to hash the secret passwords?
11. Do you use any <b>benchmarks</b> of user authentication usability and security metrics?</td><td>The purpose is to understand rather technical details of the user authentication scheme and its policy.</td></tr>
</table>

12. Do you keep any **usage data** related to user authentication tasks (*e.g.*, time to login, number of failed attempts, etc.)? 13. Have you **quantified the security strength** of the current authentication policy (*e.g.*, theoretical entropies, practical entropies, etc.)? 14. Have you applied any **brute-force attacks** to measure the strength of the current authentication policy? 15. Do you **consider any user categories/profiles** during the user authentication task? 16. Do you apply **access control/authorization**?	

Topic 3: End-users Opinions and Behaviors with regards to their Organization's User Authentication Scheme *(approx. 20 min)* *Relevant stakeholders: End-users*	
Draft Questions	Hints for the interviewer
1. How **many user accounts** do you use at your organization? 2. Please list the **primary interaction device types** (*e.g.*, desktop, smartphone, tablet, etc.) you use when you login to your account. 3. How **many times per day** do you login to your account? 4. Do you **remember effectively** your password? 5. Do you believe your password is **secure**? 6. Do you use the same password **across accounts**? 7. Do you **save** your password in your **browser**? 8. Do you **write down** your password? 9. Which **memorability practices** do you employ for building your password? In other words, what practices do you follow to memorize more effectively your password (*e.g.*, includes names, birth dates, etc.)? 10. What is your **wish list for better passwords**? 11. Could you please give some **more feedback** related to your overall user experience when interacting with the password scheme at your organization? 12. Would you be willing to use an **alternative user authentication** type to login to your work profile? *E.g.*, picture passwords that require users to memorize images or draw secret patterns as their secret key. Please explain the reasoning behind your answer.	The purpose is to understand the users' behavior and their opinion about the currently deployed user authentication scheme and its policy.

Participants’ Consent Form



SERUMS WP5 - Semi-structured Interviews

About SERUMS
Many thanks for participating in our interviews for the Serums (Securing Medical Data in Smart Patient-Centric Healthcare Systems) project. The Serums project is an EU Horizon 2020 research project which deals with security and privacy of future-generation healthcare systems, putting patients at the center of future healthcare provision, enhancing their personal care and maximizing the quality of treatment they receive. For more information about the project, please visit the project's official Website: http://serums-smartpatient.com

Why do we collect and use your data
The main purpose of this semi-structured interview is to identify current user authentication practices, policies and procedures followed at a large healthcare organization in Europe. Please note that this is not an evaluation of your organization, nor an individual evaluation. All information provided will be reported anonymously so that no data will reveal any critical information about your organization, nor the interviewees.

The interview will take about 30-45 minutes. Your answers will of course be treated confidentially and anonymously.

We would also like to inform you that your interview will be recorded aiming to convert the participants' responses to text for further anonymous text analysis and pattern mining. Your data will be evaluated and stored anonymously. Since it will no longer be possible to assign your answers to your person after the interview's processing and analysis, your data cannot be deleted afterwards. The data will be stored for at least 10 years.

Participation in the interview is voluntary and can be cancelled at any time. You can terminate your participation at any time by informing the interviewer. In doing so, you also object to the use of your data collected up to that point.

The data collected as part of this study and described above will be treated confidentially. Furthermore, the results of the study will be published in anonymous form, i.e. without your data being personally identifiable.

For further questions about this interview, the project or about the way your contribution will be used, please contact belk@cs.ucy.ac.cy.

Thank you for taking your time to support this project!

Consent
By clicking the "Submit" button you declare that you
1) understand the purpose of the study,
2) are over 18 years old,
3) voluntarily participate in this study,
4) agree that your interview will be recorded, and
5) have taken note and understand the study information presented above.

How to contact us:
Department of Computer Science, University of Cyprus

Prof. Andreas Pitsillides
Andreas.Pitsillides@ucy.ac.cy

Dr. Marios Belk
belk@cs.ucy.ac.cy

Full name

Your answer

Email

Your answer

I agree to the processing of my personal data in accordance with the information provided herein

○ I agree

○ I disagree