NWI-IMC029

Master Thesis

Restricting Authentication Token Sharing: Holder-Binding

An Investigation into Established Mechanisms and Proposed Approaches

Radboud University & Accenture Netherlands
Lemonia-Effimia Papanikolaou (s1102108)

Under the supervision of:

Dr. J.H. Hoepman (Jaap-Henk) (RU, academic)
Fabian Emmen (Accenture)

August 27, 2024

Contents

Chapter 1

Introduction

“Treat your password like your toothbrush.
Don’t let anybody else use it,
and get a new one every six months.”
– Clifford Stoll

Personal identities hold considerable importance in society. Individuals value their sense of identity because, psychologically, it encompasses memories, experiences, relationships, and personal values. These elements collectively create a stable self-perception image over time, continually evolving as new facts and experiences are incorporated [1].

In legal and social contexts a person’s identity is defined by specific attributes and characteristics. These include personal details such as name, date of birth, physical features, and other identifiers, which collectively distinguish one individual from another and are crucial for defining identity. In the digital landscape, a person’s digital identity refers to the electronic representation of this set of attributes and characteristics, enabling individuals to interact with digital systems and services.

This notion of identity extends into *Identity and Access Management* (IAM) systems, which are frameworks that manage and control digital identities and their access to resources within a system [2]. Within IAM frameworks, there is often confusion regarding the interchangeable use of the terms *“identification”* and *“authentication”*.

The process of identification entails claiming a particular digital identity within a digital system or its applications, usually using publicly available information like a username or email. Such information uniquely distinguishes a user but does not grant access on its own, as these identifiers can be known or observed by anyone. Therefore, identification establishes the claimed identity of a user, but it must be followed by a verification process to confirm and authorize access, known as authentication.

The core function of authentication is to verify that a user genuinely is who they claim to be, ensuring the validity of an identity claim. This is typically done through private information, such as passwords, which proves the legitimacy of the account holder. Traditionally, authentication focused on verifying the complete identity of an individual, often requiring personal and physical identifiers. In contemporary contexts, however, authentication processes are designed to also establish and verify claims about a user's role or qualifications, such as confirming if someone is a certified professional, or holds a specific permission, such as a digital badge or license.

Digital credentials are crucial for digital identity, connecting attributes to individuals and representing their qualifications and characteristics. These credentials link physical individuals to the digital world. Different types of credentials serve distinct purposes; for instance, anonymous credentials associate attributes with a holder without revealing their identity, while identity credentials directly link attributes to a specific natural person. Both types involve attributes issued by an authority to an individual.

In contrast, authenticators such as usernames, passwords, and cryptographic keys primarily enable individuals to authenticate themselves in digital environments, facilitating the process of verifying one's identity to securely access accounts or systems. Authenticators, or *authentication tokens*, can be used to link a natural person to a credential, connecting individuals with their accounts and enabling access to credentials. In this paper, we will refer to authentication tokens as *tokens*, for brevity.

1.1 The challenge of token-sharing

A fundamental challenge in the digital landscape is securely linking a natural person to their digital identity, crucial for proving qualifications and credentials online. Achieving this binding involves establishing a secure authentication token that links a natural person to their digital identity and interactions.

In the physical world, achieving this binding is relatively straightforward, and is normally executed by presenting an ID card with a biometric photo, which a verifier checks to ensure it matches the individual's appearance. However, issues arise when attempting to connect a natural person from the physical domain to their digital identity using tokens. Remote presentations lack the certainty of the physical world, making it difficult for service providers to authenticate individuals conclusively.

Therefore, since it is hard to bind individuals to their digital credentials, users often have the *"power"* to share their authentication tokens, lending them to another individual voluntarily. In certain applications, a very strong guarantee of tokens not being shared is essential, such as in governmental matters or financial services. This could be dangerous for the borrower of the tokens as well, potentially leading to involvement in illegal activities. For instance, proof-of-drinking-age credential access could be distributed to a minor [3].

1.1.1 Motives behind token-sharing

Despite the widely acknowledged risks, token-sharing remains widespread. Approximately 70% of individuals confess to sharing tokens with their spouse or partner, and many are comfortable sharing them with family members, coworkers, or others [4]. Moreover, recent surveys show that half of adolescents have shared passwords or PINs with their best friends, a significant increase compared to previous studies which reported rates between 16-30% [5]. This indicates that the problem is worsening among younger generations.

Understanding why individuals share tokens despite warnings is crucial for shaping security measures. While people are typically cautious with personal belongings, they often share tokens, heightening their vulnerability to digital crime. This behavior is driven by factors such as unrealistic optimism, minimized perceived risk, social influence, lack of awareness, or prioritizing convenience over security [6].

Our analysis of studies on token-sharing motivations in social contexts reveals several common reasons [5],[6],[7],[8].

- **Trust and Friendship:** Individuals often perceive sharing their tokens as a gesture of trust and service towards friends or spouses, and often reciprocating after having their tokens shared, as reported in [5].
- **Convenience and Practicality:** Individuals often share their tokens to help their social circle complete tasks more quickly, such as internet searches or making calls. Additionally, people share temporary access to their tokens when traveling.
- **Emergency reasons:** People share their tokens as a backup solution in case of emergencies or if they get locked out due to forgetting their tokens.
- **Unintentional access:** Sometimes, token-sharing occurs unintentionally; the borrower might have observed or guessed the token. In such cases, the legal owner may choose not to complain or simply not change the tokens.
- **For App maintenance:** To maintain streaks in apps like Snapchat [1], which require daily interaction, some individuals share their tokens with trusted contacts.
- **For mutual communication:** Users share tokens in order to read and respond to messages in messaging apps.
- **As requested:** Sometimes, individuals share their tokens simply in response to requests, willingly granting access and permission for their use.
- **Relaxed attitude for privacy:** Many individuals adopt a nonchalant attitude towards token-sharing, often dismissing concerns about the importance of the information contained in their accounts.
- **Community-Based token-sharing:** In regions with limited digital access, including Indigenous communities, sharing tokens helps with essential tasks like community business and shopping. Likewise, in medical centers, doctors often share login tokens to quickly access medical records, a practice that could extend to other sectors for efficient data access among large groups.
- **Cost-Sharing for Paid Services:** Sharing tokens is common for dividing expenses related to accessing paid websites or subscription services.
- **For Parental Monitoring:** Many teenagers are required to share their tokens with their parents for monitoring purposes.

[1] The Snapchat Streak is a unique gamified function within the app that motivates users to participate in daily interaction, by exchanging content [9].

- **For Accessibility Needs:** People with disabilities often rely on sharing authentication tokens to enable caregivers or support networks to effectively assist them in using electronic devices to access goods and services.

- **Other motivations:** People share tokens for various reasons; for example, young individuals may do so to avoid regrettable actions while under the influence of alcohol by handing their device to a friend.

1.1.2 Methods of token-sharing

How tokens are shared can vary significantly depending on where and how they are stored. For example, users who store tokens in a password manager might share a specific set of tokens or provide access to the master token. Alternatively, users with tokens stored on a smart card can simply lend the physical card. For devices containing saved tokens, users might share the entire device, thereby allowing access to all its features. In more complex scenarios, such as a full IAM system, sharing might involve providing access to a master account or creating a new guest account.

These examples highlight the diverse approaches users take, demonstrating that sharing methods are not exhaustive but are instead shaped by the authentication system and its context. The flexibility in different authentication methods and credential systems provides users with numerous ways to share tokens. This complexity should be considered in efforts to restrict token-sharing.

1.1.3 Negative effects of token-sharing

Effective security systems ultimately depend on end-user behaviors [10]. In a survey by Fagade and Tryfonas [11], IT professionals assessed security practices among colleagues. The most alarming finding was widespread token-sharing, a major risk to the cybersecurity stance of businesses [12].

1. **Exposure to Security Risks and Compliance issues:** Sharing tokens among employees exposes the company to cyber threats, as they can be intercepted by malicious actors through unsafe channels like emails or messaging apps. Compromised tokens enable attackers to access sensitive company data and networks, threatening data security and potentially leading to legal and financial repercussions for non-compliance with regulations such as the GDPR *(General Data Protection Regulation)* [13].

2. **Lack of Accountability:** Token-sharing allows multiple individuals to access the same account tokens, complicating the traceability of malicious activities to a specific user. This complicates the company's ability to analyze security incidents and enforce protocols effectively. Moreover, employees using another's tokens may perform actions under that account, potentially blaming the legitimate owner and creating internal issues. Proving innocence in such cases becomes exceedingly challenging for the affected user.

3. **Internal Threats:** Token-sharing increases the risk of insider threats, as individuals might misuse their privileges for malicious purposes, harming the business through data leaks, sabotage, or fraud.

Apart from within the corporate settings, it is also ill-advised for users to share their tokens, even within more personal or social circles. Negative consequences of such actions may include:

1. **Token exposure:** When tokens are shared with another individual, the legitimate owner increases the risk of those tokens falling into the wrong hands.

2. **Token-sharing chain:** Once a user has shared their tokens, there is no guarantee that they will not be further distributed. This chain reaction increases the risk of unauthorized access, as shared tokens may fall into the hands of cybercriminals, or individuals with malicious intent.

3. **Expanded access:** Sharing tokens may lead to access grants to additional personal resources or assets beyond the sharer's intended scope. For instance, this can occur through linked tokens or exposure of other data stored within a single account.

4. **Abuse of privileges:** Sharing tokens, especially those associated with financial matters or other similar privileges, can lead to misuse and potential legal repercussions. This could also endanger the borrower.

5. **False accusations of abuse:** Token-sharing undermines the principle of non-repudiation, as users may struggle to prove commitments made under their tokens. With multiple users accessing the same tokens, attributing actions to specific individuals becomes challenging, leading to confusion and potential loss of account ownership. Moreover, the legitimate owner is often held accountable for actions performed by others to whom they lent their tokens, which can lead to serious legal issues, especially in cases involving illegal activities.

1.2 The principle of Non-Transferability

Taking the previous sections into consideration, it is clear that the issue of token-sharing requires attention. There must be proactive measures in place to address, deter or eliminate the practice altogether.

We can introduce the concept of *Non-Transferability* (NT), a security notion which ensures that tokens are only used by their intended owners [14], and cannot be transferred between individuals. A token ensures this principle when it cannot be moved from one individual to another.

One way to achieve NT is through binding, which aims to establish a direct link between the tokens and the holder's physical identity. Binding essentially ties the token to the individual they were issued to, making it impossible to transfer them to another person. By creating this personal identity connection, the principle of NT is ensured.

1.3 Research Aim

This thesis aims to investigate methods to restrict individuals from voluntarily sharing their authentication tokens by exploring the concept of holder-binding. Throughout this paper, the primary emphasis will be on addressing the following question:

Can the sharing of digital authentication tokens be prevented or disincentivized by binding them to a specific natural person?

We will focus on the following sub-questions:

- **Can we formally define the concept of *'binding'*?**
- **What existing mechanisms and emerging concepts are designed to prevent users from willingly sharing their tokens?**
- **How can we determine whether a system is binding to the user, and is it possible to quantify the extent to which it satisfies specific binding criteria?**
- **What potential ethical implications could arise from the concept of *'binding'*?**

In Chapter 1, we introduced the contextual background and outlined the research objectives. The remainder of the paper is structured into a total of six chapters. Chapter 2 will define the core ideas essential for analyzing the concept of binding. Chapter 3 will examine the authentication framework, focusing on established binding mechanisms. Chapter 4 will explore the theoretical binding framework. Chapter 5 will evaluate the final binding landscape. Chapter 6 will discuss the potential ethical implications of binding. Finally, Chapter 7 will provide a conclusion summarizing our key findings.

Chapter 2

Core Concepts

In this chapter, our goal is to provide a formal definition of the central concept of this paper: *holder-binding*. However, before that, it is important to address the foundational principles of *Identity and Access Management*. Clarifying the definitions, entities, and processes of IAM is essential for understanding the principle of binding. For this analysis, we follow the denotations outlined in the latest version of the digital identity guidelines and the glossary provided by the *National Institute of Standards and Technology* (NIST) [15],[16].

2.1 The NIST Digital Identity Model

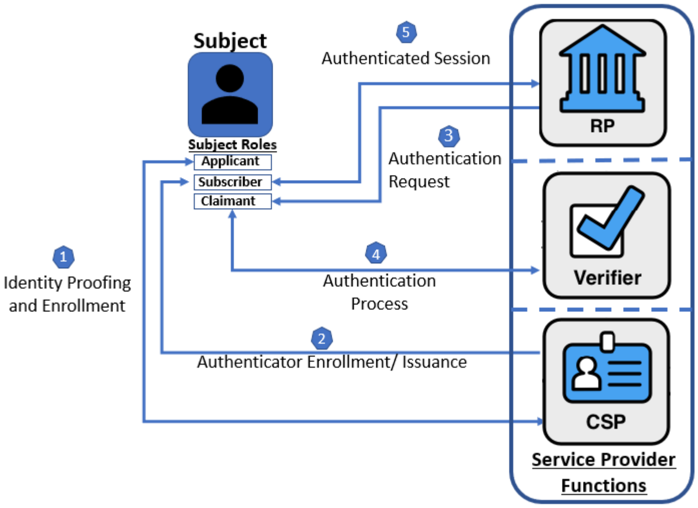


Figure 2.1: *Common sequence of interactions in the NIST Digital Identity Model [15]*

Identity, in its broad sense, refers to a distinct attribute or combination of attributes that uniquely defines a subject within a specific context.

On the other hand, *Digital Identity* is a form of identity that applies to the digital landscape, encompassing the unique representation of a person or entity engaged in online interactions. Digital identities are defined by digitized attributes and characteristics, which may include personal data, online behaviors, and interactions in digital environments. An *Attribute* is a quality or characteristic assigned to an individual, whereas *Digital Attributes* are digitized versions of such characteristics.

To confirm an individual's digital identity, *Authenticators* such as cryptographic modules or passwords are employed. These were formerly referred to as authentication tokens in earlier NIST Digital Identity Guidelines. In digital authentication, users control authenticators tied to their account, containing secrets to prove identity online. Authentication occurs by demonstrating control of these authenticators over a network. Some in-person authentication methods, like using a physical driver's license for in-person verification do not apply to digital services. Authentication systems typically rely on three authenticator factors: something the user knows (e.g., password), something the user has (e.g., cryptographic key), and something the user is (e.g., biometric data).

In typical IAM systems, several key entities and roles are integral to managing identities and ensuring access. NIST distinguishes the following entities and roles (see Figure 2.1). The *Subject* plays various roles: as an *Applicant*, initiating identity proofing, as a *Subscriber*, successfully completing identity proofing or authentication, and as a *Claimant*, seeking authentication when accessing services. The *Credential Service Provider* (CSP) is a trusted entity responsible for verifying identities, registering authenticators for subscriber accounts, and maintaining associated data. The *Verifier* authenticates the claimant by verifying their authenticators and ensuring they are correctly bound to their account. Lastly, the *Relying Party* (RP) utilizes authenticated information provided by the CSP through an authentication protocol to authorize transactions or grant system access.

The aim of all stages in a digital identity ecosystem is to enable *Access*, allowing the subjects to interact with various discrete functions of an online digital service. Central to this system, is the role of *Digital Credentials*, also referred to as electronic credentials. They play a crucial role in authentication processes by securely linking an attribute or more to a subscriber's authenticator. They consist of objects or data managed by the subscriber to establish the connection between identity and authenticator. An emerging category of digital credentials, namely *Anonymous credentials*, enable users to prove their authorization without disclosing personal information. Moreover, distinct uses of the same anonymous credential cannot be correlated or linked to each other.

It is important to understand the notion of binding. NIST defines *Binding* as an association between a subscriber entity and an authenticator. This term will be explored more in later sections. A *Subscriber Account* binds one or more authenticators to the subscriber individual, via an identifier established in the registration process, while *Authenticator Binding* is the process of linking a specific authenticator to a subscriber account, allowing it to be used, either alone or with other authenticators, for authentication purposes within that account.

2.1.1 The NIST Identity Management Processes

NIST has formally defined and standardized the sequence of the different digital identity processes between the aforementioned entities of the Subject, the CSP, the RP, and the

Verifier (see Figure 2.1) [15].

2.1.1.1 Identity Proofing and Enrollment

The typical sequence of interactions for Identity Proofing and Enrollment activities is as follows:

1. Initially, an applicant undergoes an enrollment process with a CSP. The CSP performs identity proofing to verify the applicant's identity.

   During the process of *Identity Proofing*, the CSP collects and verifies information about an individual to issue unique credentials for identification. This process follows three main objectives: *Identity Resolution*, which ensures the claimed identity is unique among all users by combining core identity attributes into a single validated profile, *Identity Validation*, which ensures the authenticity, integrity, and accuracy of the presented identity evidence through tools like document validation and authoritative resource verification, and *Identity Verification*, which confirms that the claimed identity matches the real person presenting the evidence by linking the evidence to the individual's live presence, using methods such as biometric matching and liveness detection, as categorized by NIST.

2. Upon successful identity proofing, the applicant transitions to becoming a subscriber within the identity service. This involves creating a subscriber account, registering authenticators between the CSP and the subscriber, completing the enrollment process. The CSP is responsible for maintaining the subscriber account, including its status and enrollment data, while the subscriber manages their authenticators.

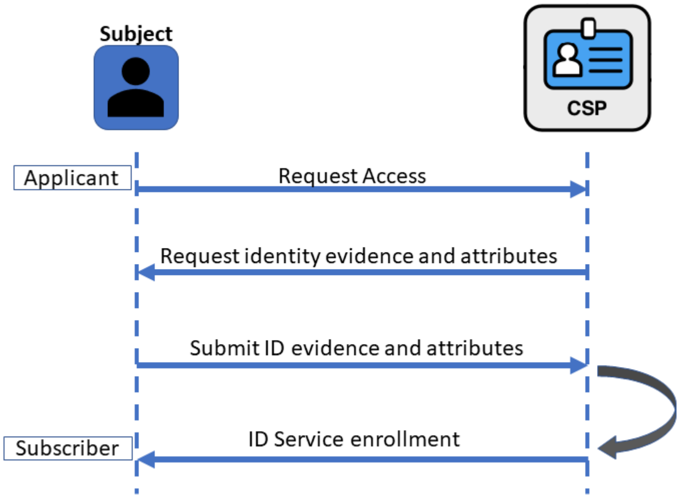

Subject
CSP
Applicant
Request Access
Request identity evidence and attributes
Submit ID evidence and attributes
Subscriber
ID Service enrollment

Figure 2.2: *Identity Proofing and Enrollment Sequence [15]*

2.1.1.2 Authentication

The sequence of interactions involved in digital authentication proceeds as follows:

1. An RP initiates a request for authentication from the claimant. It utilizes the results of an authentication protocol to confirm the identity or attributes of a subscriber, enabling secure online transactions.

2. The claimant demonstrates possession and control of their authenticators to a verifier during the authentication process. The verifier then interacts with the CSP to confirm the binding of the claimant's identity to their authenticators within the subscriber account [1]. Optionally, the verifier may also retrieve additional attributes of the subscriber from the CSP.

3. Based on the authenticated identity and attributes obtained, the RP establishes an authenticated session with the subscriber. This session enables the RP to make informed authorization decisions as needed, based on the roles associated with the account.

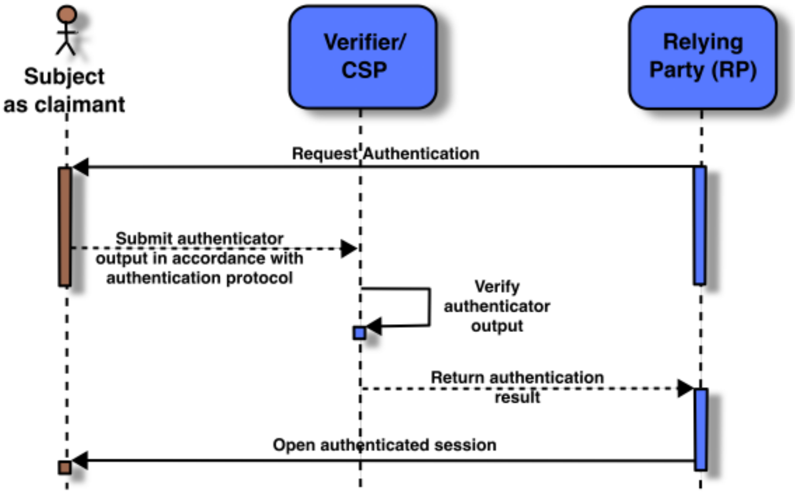


Figure 2.3: *Sample Authentication Process [15]*

2.2 Defining Binding

One of the research questions of this thesis involves formally defining the fundamental concept of ***binding***.

Binding is the establishment of a secure, exclusive connection between an individual and their authentication tokens, preventing replication or forgery. Despite appearing

[1] Typically, in anonymous credentials, instead of verifying the claimant's identity and retrieving additional attributes from the CSP, the process involves proving possession of credentials through cryptographic techniques such as zero-knowledge proofs and selective disclosure of attributes. However, these methods are not yet incorporated in the NIST guidelines.

simple at first glance, formal definitions for binding are rare. Bastian et al. note that the challenge lies not just in the lack of a clear definition, but in its often vague interpretation, relying on context or examples for understanding [17]. Accurately binding a person to their tokens is widely acknowledged as difficult and quite ambiguous across various proposals, complicating its application and causing confusion. Clarifying this concept is crucial for designing effective authentication frameworks.

In various contexts, binding refers to the process of associating identifiers with entities, which can either be a party (any person or organization) or a component (actor) acting on behalf of such a party, thereby enabling their identification and authentication [17]. Binding spans various applications: from associating data with applicants in document management [18], legally connecting legal or natural persons [2] to their states in physical ID documents like passports or certificates [20], to linking user accounts to software programs for authentication [21]. NIST defines binding as a *"trusted association"* that validates relationships between related items of information [22]. In PKI systems, binding verifies the connection between a digital certificate and the respective identities of entities (such as people and organizations) by proving possession of the corresponding private key [23]. Standards and specifications define binding in diverse ways, such as confirming the rightful holder of a verifiable credential (any person or organization), ensuring privacy in credential linking, and enabling authentication through cryptographic keys [24, 25, 26].

Various terms are used to describe the individual directly linked to tokens [3]. These include *"holder,"* who controls and presents verifiable credentials, *"subscriber,"* common in identity proofing and authentication standards, *"claimant,"* proving identity in authentication protocols, *"subject,"* verified in privacy and security standards, and *"user,"* bound to tokens across web services. In essence, all these terms refer to the same concept: *there exists a natural person to whom the binding to a specific token applies.*

2.2.1 Our definition

Upon analysis, it is evident that there are no standardized definitions for binding, nor standardized terms (e.g., holder-binding, subject binding, identifier binding, user binding), which complicates the concept. The appropriate terminology varies depending on the context, leading to ambiguity and differing assumptions. In our thesis, we concentrate on authenticator tokens linking *only* natural persons to credentials, excluding legal entities like corporations and credentials related to systems or entities beyond individual persons. Therefore, we aim not to adhere strictly to the previously mentioned definitions.

> Instead, we define binding as the process of linking tokens and/or credentials to natural persons, ensuring they can only be used by the individual to whom they were issued and cannot be transferred to others.

For clarity, we adopt the term *"holder-binding"* [4] to denote this concept, aligning with its common usage in authentication frameworks.

[2] In law, a human person is called a natural person (sometimes also a physical person), and a non-human person is called a juridical or legal person. Juridical persons are entities such as corporations, firms, and many government agencies [19].

[3] In other contexts, the entity is not mentioned to avoid misfocus, emphasizing instead the concept of identifier binding [17].

[4] We may also refer to the entity as the *"user"* in contexts relevant to commercial tools focusing specifically on user accounts.

Chapter 3

Established Mechanisms

In this chapter, established methods of holder-binding will be discussed. Our goal is to examine the current landscape of commercial offerings that enhance authentication security, in order to determine how holder-binding can be achieved. The first section analyzes *biometric* binding, covering *physiological* and *behavioral* biometrics, as well as a novel biometric-based method called *Visual Presence Identification.* Following this, we explore *Device-based*, *Knowledge-base*, and *Context-based* binding mechanisms. Each method's functionality is presented alongside a case study of a selected commercial tool, illustrating its practical operation.

3.1 Biometric Binding

One of the most commonly used forms of authentication that does not require the use of a password, is biometric authentication. Biometric authentication, or simply biometrics, means automatic person recognition based on an individual's physical or behavioral traits [27]. This method uses distinct biological characteristics, such as fingerprints and voice patterns, to verify a person's identity. There are over 20 biometric modalities that can be used for authentication, categorized as either *behavioural* (dynamic) or *physiological* (static).

In a biometric system, when a person's biometric data is initially captured, it is converted into a digital template, which is stored for future authentication. During an authentication request, a new biometric sample will be extracted from the individual.

Biometrics can be employed for *identification*, often referred to as a *"one-to-many"* matching approach, where the new sample is compared against all templates in a database. For example, this is utilized in law enforcement for non-consensual identification. Alternatively, it can be used for *verification*, known as a *"one-to-one"* matching approach, where the new sample is compared with a single individual's template. This is commonly used in smartphone authentication, with data typically stored on the device, or in passport control at airports.[28]

To evaluate a biometric system's performance, several key metrics can be used, to measure its accuracy and efficiency. The process is typically based on two types of errors [28]. The first category detects matching errors and includes metrics like *False Acceptance*

Rate (FAR) [1] and *False Rejection Rate* (FRR) [2]. FAR measures the likelihood of the system incorrectly matching biometric data from different individuals, while FRR measures the probability of the system failing to match biometric data from the same individual. A high FAR implies that the system is overly lenient, whereas a high FRR suggests the system may overly deny access to legitimate users. The second type detects acquisition errors, involving metrics such as *Failure to Acquire Rate* (FTA) and *Failure to Enroll Rate* (FTE). FTA measures the probability that a biometric system fails to capture data from a biometric input despite proper presentation to the sensor, while FTE evaluates the system's ability to create reference templates out of the biometric samples.

3.1.1 Physiological Biometrics

Throughout history, the use of physiological cues for identification has been significant, with the earliest trace dating back 31,000 years, where handprints found in caves, served as personal unique signatures [29].

Physiological Biometrics refer to the analysis of an individual's physical characteristics for identity verification, such as facial features or palmprints. They can be divided into two main categories: *biological*, and *morphological* traits [30]. Biological traits include dynamic, vital elements, typically physiological responses of a person's body, like an individual's DNA or body odor. On the other hand, morphological traits include static, structural features, such as fingerprint patterns.

3.1.1.1 Functionality and Categories

For Physiological Biometrics, the process of data capture generally involves a biometric scan, which captures the individual's unique patterns. This scan then produces detailed maps of the measured traits to create a digital template [31].

Physiological Biometrics are commonly employed for authentication purposes, such as unlocking smartphones using fingerprint recognition. This process is known as a physiological biometric login, where biometric information is utilized to authenticate a user's identity and give access to digital systems [31].

Modern physiological biometric solutions typically include the analysis of various biometric traits [32], including:

- **Facial Recognition:** Facial recognition is a non-intrusive method that analyzes the facial features of an individual, which are among the most commonly used biometric attributes for human identification. It is commonly implemented in modern smartphone devices.

- **Voice Recognition:** AI-powered voice recognition is used to distinguish voices based on different pitch and voice characteristics, serving purposes such as securing voice-operated systems.

- **Fingerprint scans:** Fingerprint scanning is a widely adopted biometric authentication method that identifies individuals based on the unique patterns on their fingerprints. These patterns develop during the first seven months of fetal development, making each person's fingerprints distinct. Even identical twins have different

[1] This is also referred to as *False Match Rate* (FMR) in other contexts.

[2] This is also referred to as *False Non-Match Rate* (FNMR) in other contexts.

fingerprints, and each finger on the same person possesses its own unique prints [33]. Fingerprint scanning is considered one of the most reliable methods due to its cost-effectiveness and efficiency.

- **Hand Geometry:** Hand geometry, among the earliest forms of biometrics, identifies individuals by analyzing the shape and distinctive features of their hands. These systems implement parameters such as length, width, depth, and surface area of the hand.

- **Iris or Retina Scanning:** Both these biometric techniques involve scanning different parts of the eyes to authenticate individuals. Iris scanning analyzes the distinctive patterns of the iris, the circular part at the front of the eye. On the other hand, retina scanning captures an image of the retina and its unique network of blood vessels, located at the back of the eye.

- **Vein Patterns:** Vascular pattern recognition, also known as vein matching, utilizes differences in vein patterns for identification purposes. This biometric method employs infrared light to illuminate veins beneath the skin and is commonly applied to fingers, hands, or arms. Vein patterns, as a biometric modality, represent a relatively recent advancement.

- **DNA Matching:** This process involves examining a DNA sample to identify its human origin and is frequently employed in healthcare and forensic contexts. DNA can be extracted from biological materials such as hair, saliva, skin, or blood, and may be compared against existing DNA samples in a database for authentication purposes.

3.1.1.2 Case Study

In this section, we explored various commercially accessible identification tools that implement Physiological Biometrics, including VeriDas [34], LumenVox [35], PingOne Verify [36], IDR&D[37], AWARE [38], accurascan [39], Oz Forensics [40], FusionAuth [41], LoginID [42], Biometric Vision [43], facial-login-web [44], facephi [45], CloudABIS by M2SYS [46], BioID[47], Cognitec [48], Rohos [49], Imageware [50], NEC [51], Iris ID [52], FaceTec [53], Windows Hello [54], PalmID [55], and irisguard [56].

As a case study, we will examine the Voice Biometric Authentication solution developed by *VeriDas* [34], which employs the physiological characteristics of the voice to identify users within a system.

The voice-based speaker recognition solution is capable of verifying user identities with just 3 seconds of voice samples, in passive authentication mode. This means that users can engage in normal monologue, without the need to repeat specific phrases or prompts. Additionally, the system is text and language-independent, which eliminates the need for users to memorize or read the same prompts every time. VeriDas performs liveness checks by integrating voice activity detection, noise detection, and voice authenticity verification to protect against various types of spoofing, such as deepfakes or synthetic voices.
This type of technology is normally incorporated for authentication services in call centers, where users have to register using their phone number, which will then also be used for their authentication, by performing a call.

General Workflow

During the enrollment stage, a user's voice characteristics are captured and transformed into an irreversible biometric voice vector. This process only takes three seconds, during which the user simply speaks into the application. By using voice activity detection, the system analyzes the user's voice stream without processing the content being spoken, only the speaking style. When the three seconds have passed, the registration process is automatically finished.

In the authentication process, users initiate a call using the same registered account. When the call starts, the authentication process begins immediately. After collecting the first three seconds of the user's speech, the system matches the voice vector to the registered sample. Within approximately 0.14 seconds, the system provides an immediate result that indicates whether the user's identity has been successfully authenticated or not.

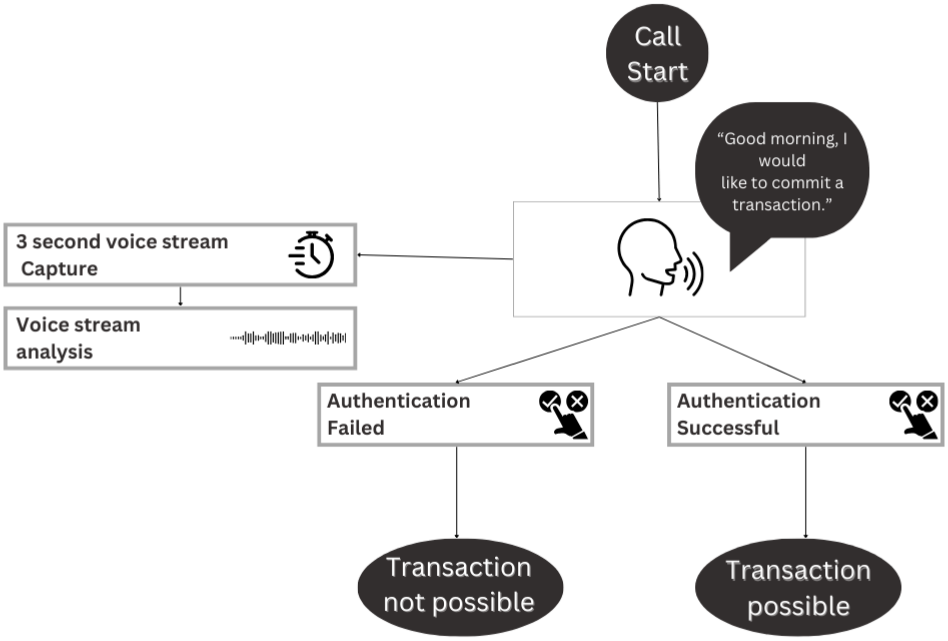

Call Start
"Good morning, I would like to commit a transaction."
3 second voice stream Capture
Voice stream analysis
Authentication Failed
Authentication Successful
Transaction not possible
Transaction possible

Figure 3.1: *VeriDas voice authentication example*

System Performance

VeriDas' voice biometric authentication solution achieves an accuracy rate of over 99% [34]. This is supported by a certification from NIST, recommending it as the second-best engine globally for voice evaluation. Additionally, when coupled with VeriDas facial evaluation, VeriDas' voice biometric authentication system has the top spot as the leading commercial biometric solution worldwide for this type of joint authentication [57].

3.1.2 Behavioral Biometrics

Humans have attempted to identify individuals based on their behavioral characteristics since long before, tracing back to the Second World War, when allies developed methods to recognize each other through unique typing patterns in sensitive messages in Morse code [58]. Behavioral Biometrics, a development from this idea, involves measuring and analyzing human behavioral traits, often through interactions with computer peripherals such as mice, keyboards and phones. The primary aim is to distinguish between a legitimate user and unauthorized individuals accessing an account. For example, a legitimate user typically enters information manually by memory, whereas someone else using the account would typically copy/paste information [59].

Behavioral Biometrics can be used for dynamic authentication, continuously monitoring and verifying the user's identity throughout a session by analyzing data in the background. This enables systems to detect changes in user behavior and create dynamic profiles based on unique movements. They are considered passive since they typically require little to no additional action from the user [60] [3].

3.1.2.1 Functionality and Categories

Behavioral Biometrics authentication verifies users by analyzing their behavior patterns. This process involves assessing behavioral characteristics and then cross-referencing them with existing data on user records. Behavioral biometric systems assess a wide range of human behavior characteristics for identification and measure different human abilities, such as motor skills, style, preference, knowledge, or strategy. Depending on the skills and attributes used to capture human behavior, these systems can be categorized as [61],[62]:

- **Skill-based:** This focuses on analyzing the unique muscle actions associated with learned skills or activities, typically practiced over time. For instance driving habits, typing dynamics, programming techniques, and gaming patterns.
- **Motor-skill-based:** This examines a broader range of muscle-control actions, often those that are more involuntary or instinctual. For instance, GAIT style, blinking pattern, handgrip, voice/speech style, and lip movement.
- **Knowledge-based:** The user's knowledge is captured through their typical behavior [4]. Examples include what is called a biometric sketch, proposed by Bromme et al. [63], where users are prompted to create unique simple sketches (for example

[3] In our analysis of tools utilizing Behavioral Biometrics, we found that they are commonly employed as components for log-in authentication. Consequently, in Chapter 5 of our evaluation, we categorize behavioral biometrics as a means to prevent token sharing. While they can indeed be used to detect such activities, our focus here is on their role in authentication, leaving the user's continuous interaction with the device to be addressed by context-based authentication mechanisms, which will be explored further.

[4] Later in the paper, another knowledge-based authentication technique is discussed, differing in operation from the one in this section. Knowledge-based Behavioral Biometrics authenticate users by analyzing their typical behavior or actions through reaction challenges to determine their uniqueness. In contrast, Dynamic Knowledge-based Authentication, described in section 3, relies on users recalling specific information stored in their memory, such as answers to security questions. Thus, users are evaluated based on their recall ability rather than their unique behavioral responses.

a few circles) during authentication. The system analyzes their different reactions, taking into account knowledge of the content provided during registration, leveraging the variability in how users interpret and draw simple shapes.

- **Style-based:** This is based on distinct user styles that can be utilized for authentication. For instance, De Vel et al. [64] have applied authorship identification techniques, including email-specific features like greetings, farewells, signatures, attachments, and total number of HTML tags, to determine the likelihood of an email's true author.
- **Preference-based:** Derived from the analysis of a user's choices and preferences when executing specific tasks. For instance, Fawcett and Provost [65] proposed calling behavior as a behavioral biometric trait, based on the idea that each individual has a unique pattern of choices when making phone calls, examining factors such as frequency, duration, and pattern of contacts.
- **Strategy-based:** Each user develops different strategies for different scenarios, for example in gaming. An example of this includes a scheme proposed by Yampolskiy et al. [66], for verifying online poker players by analyzing their behavioral profiles, which include frequency measures of card ranges and aggression levels.

3.1.2.2 Case Study

In our study, we examined several commercially available identification tools that utilize Behavioral Biometrics, namely: Prove [67], typingdna [68], BioCatch [69], simprints [70], Plurilock [71], ThreatMark [72], Biometric Signature ID [73], ZIGHRA [74], VoiSentry by aculab [75], cynet [76], sardine [77], BehavioSec by LexisNexis [59], SECUREAUTH [78], arvato [79], UnifyID [80], and NuData [81].

In this section, we will highlight *typingdna* [68], a Behavioral Biometrics company that distinguishes users based on their typing patterns, with a specific focus on their Authentication API product.

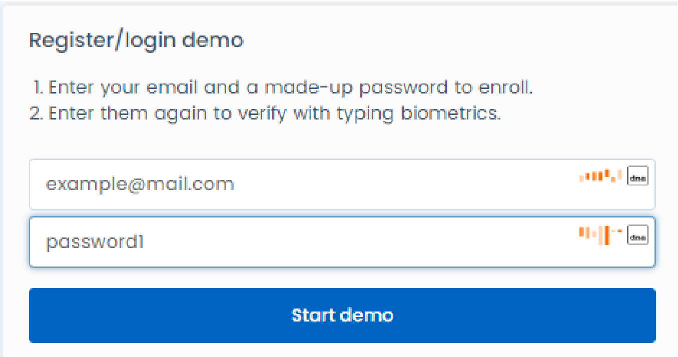
Typingdna is compatible with any device and keyboard, operating in passive mode in the background of the system. It can identify non-legitimate users with just one typing sample. The technology analyzes users' typing patterns, by examining micro-patterns in their keystrokes. During registration, samples of their typing, such as key press latencies, are analyzed—examining the time taken to release or press keys and move between them, aiming to create a typing profile of the user, a *"typing DNA"*. The data collected are used for future authentication and login attempts. This product can be implemented into any consumer app.

Authentication API

The API can be implemented in log-in interactions, such as log-in webpages, to authenticate users. Instead of traditional methods, such as *One-Time Password* (OTP) codes, users can authenticate themselves by just typing their credentials. This method reduces the reliance on other devices for *Two-Factor Authentication* (2FA), such as phones. Users are now authenticated in the background through typing biometrics. The whole process can be integrated into another typingdna product, called *the ActiveLock product*, which continuously monitors already authenticated users by analyzing their typing behavior, to prevent account sharing. If an unauthorized typing pattern is detected, the system automatically locks the device to prevent unauthorized access and credential sharing.

General Workflow

When a user creates their profile for the first time, typingdna gathers information about their typing style, so as to create a unique typing profile. During the registration process, the user has to input their email and password, while typingdna monitors their typing style in the background (with the user's consent, since they have to agree by clicking on a text bubble). They are required to type their credentials three times in total, which allows typingdna to create three different typing profiles, which collectively form the main typing profile of the user. This main profile is then used for comparison every time the user requests authentication, with a typing sample that is provided in real-time.



Register/login demo

1. Enter your email and a made-up password to enroll.
2. Enter them again to verify with typing biometrics.

example@mail.com

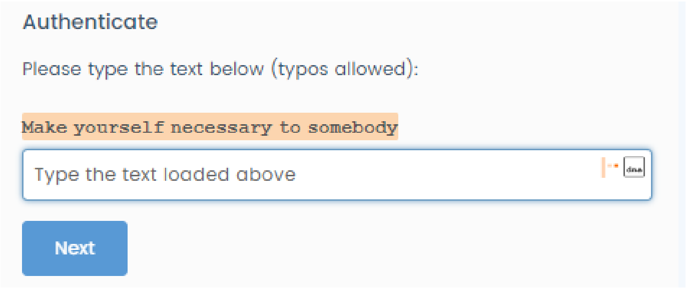
password1

Figure 3.2: *typingdna authentication request*

Main Components

The Authentication API can include various add-ons besides the login authentication layer, that offer extra layers of security according to the preferences of the system manager. When a user attempts authentication, if their typing pattern matches the expected profile, they are successfully authenticated. Otherwise, they receive a message indicating authentication failure, and they are unable to access their account.

- **Short phrase add-on:** Users have to type specific pre-defined phrases, that are the same for each attempt.



Authenticate

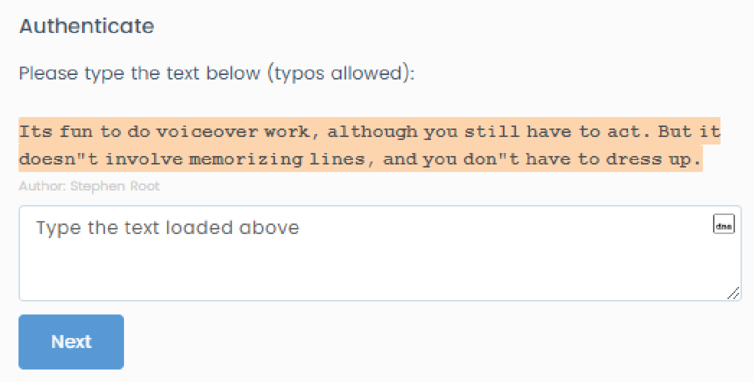
Please type the text below (typos allowed):

Make yourself necessary to somebody

Type the text loaded above

Figure 3.3: *typingdna short phrase authentication*

- **Different texts add-on:** Users have to type pre-defined phrases, that do not need to be the same each time, but can change for each attempt. The texts are a bit longer than the short phrases add-on.



Authenticate

Please type the text below (typos allowed):

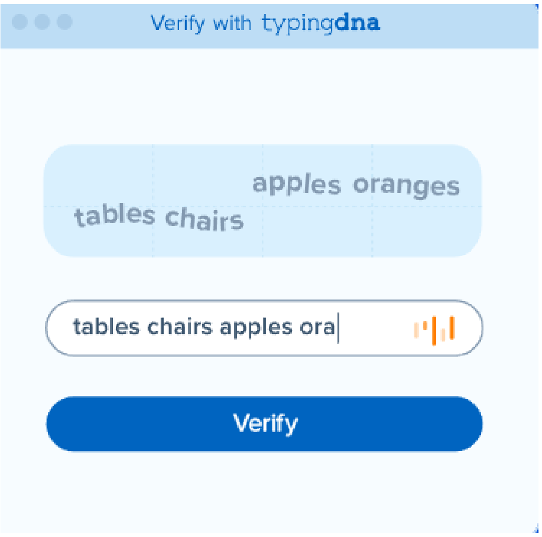
Its fun to do voiceover work, although you still have to act. But it doesn"t involve memorizing lines, and you don"t have to dress up.

Author: Stephen Root

Type the text loaded above

Figure 3.4: *typingdna different text authentication*

- **Verify 2FA:** There exists an additional 2FA option available within the Authentication API. Unlike traditional methods, this option relies solely on the user's primary device, eliminating the need for another device such as a phone, and a message, or a one-time code retrieval. Instead, users simply type four specific words, which are then compared against their unique typing profile for authentication.



tables chairs apples ora

Figure 3.5: *typingdna Verify 2FA*

3.1.3 Visual Presence Identification

Since biometrics are closely linked to an individual's genetic makeup, they provide a unique factor valuable in the authentication scheme. However, they are certainly not immune to attacks. In particular, attacks on the biometric sensor of a system are frequently attempted, with one of the most prevalent being a presentation attack. In this type of attack, adversaries utilize *Presentation Attack Instruments* (PAIs), like photographs, masks, or video replays, to deceive biometric sensors, attempting to pass as another individual and trick the sensor [82]. A key mitigation strategy against presentation attacks, as well as other attempts to bypass sensors, is liveness detection.

Liveness detection is defined as a system's ability to authenticate the legitimacy of biometric attributes by ensuring that the characteristics presented during a verification process comes from a real person and not a fabricated representation. Liveness detection can be active [83], involving motion analysis, involuntary action recognition (identifying random and unpredictable user actions, like winks), and blink pattern analysis to verify if they match a real person. It can also be passive [83], without user collaboration, through methods such as texture analysis (extracting textural features from facial images), depth detection to verify if the sample is three-dimensional, background motion analysis to detect abnormal motion signals, or micro-video capture by capturing a series of images from a micro video.

However, merely ensuring that a person is alive is not enough for authentication. It is important to verify not only that the entity is a natural person and alive but also that the identity matches the expected credentials at that time. This is where Visual Presence Identification could be beneficial, aiming to confirm both the physical presence and the expected identity during the authentication process.

3.1.3.1 Functionality

Visual Presence Identification allows real-time identity verification by analyzing videos and images [5]. Through Visual Presence Identification, the main objectives, are to confirm that the user requesting authentication [84]:

- **Is the correct entity:** Ensuring that the individual seeking authentication is the rightful owner with authorization to access the online account or service that is being handled.
- **Is a genuine person:** Confirming the entity is a real person, removing the possibility of a representation through a photo, mask, or any other PAI.
- **Is presently attempting authentication:** This process involves verifying the freshness quality [6] of the authentication attempt, by confirming its time-validity. It ensures that the individual is actively present and requesting authentication themselves, rather than employing a prerecorded video, deepfake, or attempting a replay attack.

3.1.3.2 Case Study

Currently, various services utilize this solution as a part of their identity verification process. In our analysis, we examined several commercially available Visual Presence Identification tools to understand their functionalities and operations, namely: **Amazon**'s Rekognition [86], **iDcentral**'s 360 Degree Identity Verification [87], **iProov**'s Genuine Presence Assurance [84], **Veriff**'s Identity Verification Product [88], **Facia**'s Online Identity Verification Package [89], **Onfido**'s Real Identity Platform: Verification Suite [90], **FACEKI**'s Document Identity Verification [91], **PXL**'s Vision Identity Verification [92], **Authme**'s Identity Verification product [93], **Jumio**'s Holistic Risk View Product [94], **AU10tix**'s Identity Verification Suite [95], **Passbase** [96], **Unico**'s Check [97], and **Persona** [98].

In this section, we will present the technology of *Amazon Rekognition* [86], focusing on its Visual Presence Identification capabilities.

Amazon Rekognition functions as a cloud-based image and video analysis service. It includes pre-trained features for facial recognition and analysis, allowing for applications like identity verification via its face-based user identity verification system. Typically, the user authentication process is completed in seconds, while the tool confirms user identities by comparing faces in newly submitted images to reference face images.

General Workflow

For user enrollment, users must complete all steps that will be mentioned in the workflow. However, for user authentication, only part two of the workflow is required (steps c-f).

[5] It is important to mention that this technology lacks a standardized name since each company or tool defines it with different terms. Common names for this technology include Presence verification through Video-Images, Genuine Presence Assurance, Liveness detection along with Identity Recognition, and Biometric Selfie Verification.

[6] This is one of the quality metrics typically used to assess data. It is also referred to as timeliness in other contexts [85].

1. The user enters the system and is instructed to submit a picture of their ID card, or another identification document. Amazon Rekognition executes the following actions:

    (a) **Classify the ID document:** Object detection is employed to determine the type of user identity document that has been submitted, such as a driver's license or a passport.

    (b) **Extract user ID data:** Text detection extracts key pieces of text from the identification card, like name, age, and identification number. The data, along with the document, is stored within the account information.

2. The user is instructed to record a selfie video that captures a selfie picture. Amazon Rekognition executes the following actions:

    (c) **Validate the quality of the image submitted:** The Face Detection technology determines whether the user's selfie is captured accurately, based on predefined attributes such as facial landmarks, like eye position, and other characteristics such as the presence of glasses.

    (d) **Verify the liveness of the user:** The Face Liveness technology ensures that only genuine users, rather than intruders using spoofs, attempt authentication. It analyzes a brief video in real-time, during which the user is instructed to take a selfie. The process requires near passive user action, by instructing the user to move their face into an oval rendered on the user's device screens. This process verifies the presence of the user in the video feed, ensuring live interaction.

    Moreover, the technology uses *machine learning* [7] and *computer vision* technologies [8] to detect fake elements within the user's camera feed. By analyzing facial dynamics such as expressions and blinking patterns, the system can separate between genuine and artificial interactions. Normally, live interactions have natural facial dynamics, while fake attempts would have unnatural or static facial features. Additionally, analyzing movement patterns, such as head turns, nods, and tilts, enables the system to differentiate between live users, static images, and video playback. Environmental cues, like lighting conditions, also help in the differentiation process. The technology can identify various forms of fraud, such as digital photos, videos, or 3D masks presented to the camera. Additionally, the system can detect sophisticated spoofing techniques like pre-recorded or deepfake videos that aim to deceive real-time authentication.

    (e) **Compare the selfie picture with the ID card picture:** The Face Comparison technology of Amazon Rekognition aims to measure the similarity of two faces, to determine if they belong to the same person. It generates a similarity score prediction for the user's captured selfie picture against their submitted identity document in real-time.

[7] A type of artificial intelligence that enables systems to learn and improve from experience without being explicitly programmed [99].

[8] Software algorithms designed to extract meaningful information from visual data [100].

(f) **Search the selfie picture against the system's collection of users' faces:** When a user is enrolling on the system, their captured selfie is stored in the system, and transformed into what is known as a *"face vector"* which essentially represents the unique characteristics of the user's face. These face vectors are stored in a database along with those of all other users, called a *"face vector collection"*. If someone tries to sign up again, their new face vector is compared to those already in the database. If there is a match, it means they already have an account, and they will not be allowed to create another one. This process helps prevent duplicate account creation.

When a user requests authentication, the system retrieves their stored face vector from the database and compares it to the new selfie they have submitted. If the two match, the user is authenticated and allowed access. This ensures that only authorized users can access their accounts.

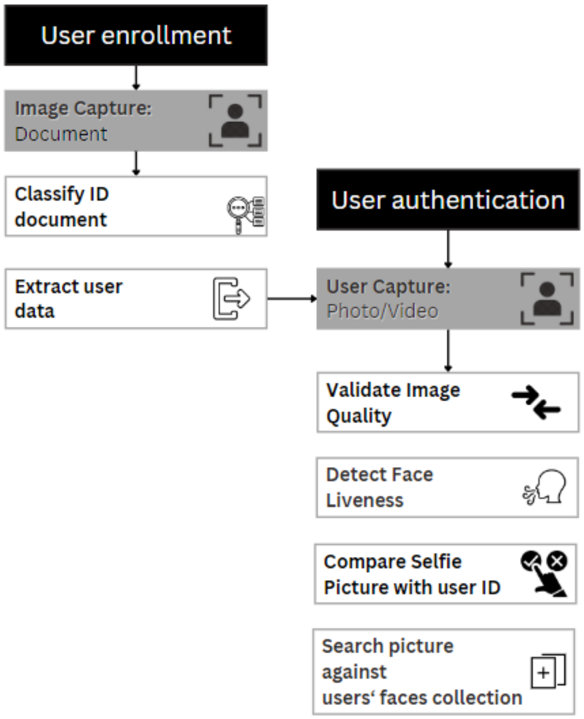


Figure 3.6: *Amazon Rekognition for Identity Verification*

3.2 Device-based Binding

Device fingerprinting, also known as machine fingerprinting, is a technique used by systems to gather information about a user's device. It collects details about hardware, software, and other parameters to create a unique identifier, known as the device hash, using a fingerprinting algorithm [101]. This algorithm considers the combination, frequency, and correlation of various attributes, using advanced mathematical models and statistical analysis [102]. The generated device IDs are stored on a server-side database, enabling verification of user access from the same device. In terms of security, detecting changes in the user's device choices, such as using different browsers or displaying distinct preferences, can indicate potential credential compromise. Inspecting changes in the device fingerprint can help determine if the user's credentials have been shared with others. If suspicious activity, such as accessing multiple devices at the same time or using a new device, is detected, the application can take measures like blocking or further reviewing the account.

An application could incorporate device fingerprinting to collect data about a user's device, even after they log out. This collected data could then be used to identify the user upon subsequent interactions, allowing the system to provide personalized recommendations. While a device fingerprint alone may not be the strongest authentication method, its value increases when combined with other data, serving as a persistent identifier.

The term *device fingerprinting* is often used interchangeably with *browser fingerprinting* [103], although they typically rely on different sources for identification. Browser fingerprinting is a method of identifying web browsers by analyzing the information they provide, including screen dimensions, installed plugins, system languages, and other characteristics. Device fingerprinting uses comparable techniques to identify the specific device in use. This approach remains effective even when different software is utilized to access a service, such as switching web browsers [104]. Therefore, we could consider browser fingerprinting as using a subset of the sources employed for device fingerprinting.

Many services utilize device fingerprinting as a part of their identity verification process. In our analysis, we examined several commercially available device identifying tools to understand their functionalities and operations, namely: **TrustDecision** [102], **Incognia** [105], **SEON** [106], **Callsign** [107], **Appsealing** [108], **Radware** [109], **STYTCH** [110], **PingOne** [36], **JumpCloud** [111], **ForgeRock** [112], **Beyond Identity** [113], **InstaSafe** [114], **Castle** [115], **IPQS** [116], *"What every Browser knows about you"* by **Webkay**[117], *"Cover Your Tracks"* by **EFF**[118], **Am I Unique?** [119], **CreepJS** [120], **Fingerprint** [121], **BroprintJS** [122], **Supercookie** [123], and **detectIncognito** [124].

3.2.1 Data Sources

Sources for data for typical device fingerprinting tools could include [102]:

- **Hardware attributes:** This includes details such as the device's processor type, memory, screen resolution, and device model. These hardware characteristics provide a foundation for creating a device fingerprint.

- **Software configurations:** Device fingerprinting takes into account software-related attributes like the browser version, installed plugins and extensions, time zone settings, language preferences, and installed fonts. These software configurations further define the device fingerprint.

- **User behavior patterns:** Device fingerprinting can also consider user behavior patterns, such as typing speed, mouse movements, touchscreen gestures, and browsing habits.

- **Network properties:** Information such as the IP address, *Internet Service Provider* (ISP), and geolocation can be used to supplement the device fingerprint. Network properties provide additional context to identify devices accurately. These characteristics may not be solely tied to one device, since various devices might exhibit different network properties at times. Nonetheless, they can serve as an additional verification factor.

Table 7.1 Includes all the distinct data sources we found in our analysis.

General Device	Mobile	Web
802.11 traffic	Accessories Information	AdBlock Status
Antivirus Name	Advertising Identifier (ADID)	Audio And Video Settings
API version	Android ID	Audio fingerprint
App version	App version	Audiocontext Fingerprint Status
Application package name	Apple Pay status	Battery Level
Available memory size	Audio information	Browser features: flash, java etc.
Baseband version	Available memory size	Browser Hash
Battery information	Battery information	Browser name-brand
Battery level	Battery Level	Browser system language
Brand	Boot information	Browser Version
Carrier	Build Information	Canvas device fingerprint
Charge state	Bundle id	Color analysis (e.g. inverted colors, monochrome status)
Clock Skew	Carrier information	Color Depth
Color depth	Charge state	Color GAMUT
Country code	Color Depth	Connection type (e.g. corporate)
CPU hardware information	Country code	Cookie Hash
CPU type	CPU information	CPU glass
Current time	Current time	CSS styles (computed + system)
Device Name	Device model	Current time
Device sensors (e.g. accelerometer)	Device name	Device Memory
Device software version number	Device orientation	Device Sensors
DNS address	DNS address	DeviceType
Flash data	Emulator detection	Display settings (e.g.menu bar)
GPS location	GPS location	DNS: Geo ISP
Hardware reset status	iCloud Ubiquity token	DNT header enabled status
Host	iOS version data	DomRect
Information about wireless card chipsets, drivers, firmware	IP address	Download Speed
Installed application package name	IPV6	Emojis (DomRect)
IP Address	Jailbreak status	FP_version
IP location (e.g. continent, country)	Kernel information	GPU information (e.g. params, model)
IPV6 identifier	Language	Hardware concurrency
Language	Latitude	HTTP accept headers
Latitude	Local IP address	HTTP request headers
Local IP address	Longitude	Installed Browser Fonts
Longtitude	Mobile country code	Installed extensions
Microsoft silverlight data	Mobile network code	Installed plugins
Country Code	Mobile Operators	IP address
Mobile network code	Network configuration	is unique? (IP address check)
Model	Network type	is_crawler?
Network Type	Passive SSL/TLS handshake analysis	JS Engine (Console Errors)
Operating System (e.g. version, major)	Pasteboard data	JS runtime (Math)
Processor type	Proximity sensor data	Language
Product Code	Proxy information	Limited Supercookie test
Proxy information /VPN	Root status	List of browser mime-types
Running application package name	Screen brightness	MimeTypes
Screen brightness	Screen resolution	Mouse and Keyboard Interactions
Screen resolution	SDK version	Operating System
SDK version	Startup time	Operating system language
MD5 signature	System version	Other HTTP header attributes (e.g. content encoding)
Sim card operator	TCP/IP fingerprint	Other JS attributes (e.g.list of fonts)
Startup time	Time zone (+offset)	PDF viewer enabled
System version (e.g. domain name, serial number)	Total memory size	Previous Page
Time Zone (+offset)	Total storage size	Private click measurement
Total memory size	Unique device identifier (UDID)	Proxy, VPN, TOR detection
Total storage size	UP time	Recent_abuse status
Unique device hash/identifier	VPN	ID address Referrer
Uptime	Wifi SSid	Resistance (Known Patterns)
VPN IP address	Wireless IP address	Screen checks (e.g.width, height)
Wireless IP address	Wireless mac address	Screen resolution
Wireless MAC address	Wireless network name	SDP capabilities
Wireless network name	—	Size of browser windows
Antivirus Enabled	—	SSL fingerprint
—	—	STUN connection
—	—	SVG
—	—	Text Metrics
—	—	Time analysis (e.g. click_date, first_seen)
—		Time_Zone
—	—	Timestamps
—	—	Timezone Offset
—	—	Touch support
—	—	URL
—	—	User_Agent (String)
—	—	WebGL fingerprint test (e.g.rendered, data)
—	—	webRTC IPs

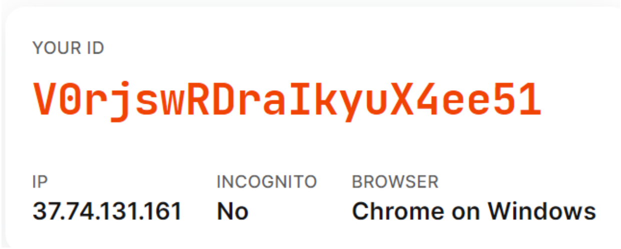
Table 3.1: Device fingerprinting data sources

3.2.2 Case Study

In this section, we will introduce *Fingerprint* [125], a leading tool for device identification, with a specific focus on its product *Fingerprint Identification*.

The software operates on a client-server model, utilizing both a client-side *Software Development Kit* (SDK) and back-end infrastructure to generate unique fingerprints, aiming to help companies prevent unwanted instances such as account sharing and duplicate account creation, by identifying unique visitors. It has the ability to differentiate between identical physical devices, such as two identical iPhone 15s.

Unlike older versions and other similar products reliant on browser fingerprinting, this system utilizes data matching techniques, including statistical ID generation [9] and machine learning algorithms, with an end goal of user identification, not only device identification. This is why the identifiers produced by Fingerprint Identification are known as *"VisitorIDs"* rather than *"fingerprints"*. These VisitorIDs are represented as strings of characters, such as xPFysGV25VxZcGQUxVIt. They remain consistent over extended periods, unaffected by changes in device attributes or software updates. Additionally, the visitorID generated remains constant even after the credentials are used in incognito mode or through a *Virtual Private Network* (VPN).



YOUR ID

V0rjswRDraIkyuX4ee51

IP	INCOGNITO	BROWSER
37.74.131.161	No	Chrome on Windows

Figure 3.7: *Fingerprint Identification VisitorID example*

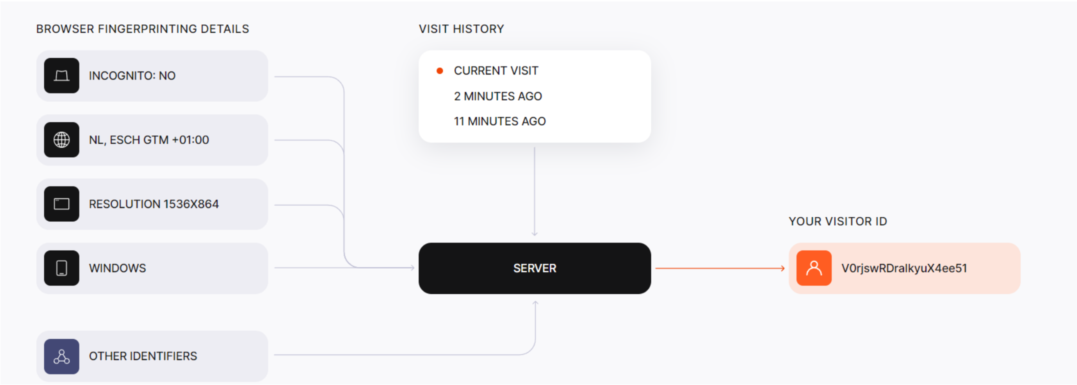


Figure 3.8: *Fingerprint Identification algorithm outcome example*

[9] A method of creating unique identifiers based on statistical analysis of data patterns [126].

Identification Use Cases

- **Comparing fingerprints:** Before an important action, a fingerprint is generated for the user and subsequently compared with the previously tracked fingerprint associated with that user. If the two fingerprints match, the user is verified. If the fingerprints do not match, a different device is used. There exist different restrictions for accounts. For instance, a user can not log in using their credentials from a device not linked to their fingerprint.

- **Counting fingerprints associated with data:** This method is an advanced iteration of the previous *"comparing fingerprints"* approach. Each significant action in an application triggers the generation of a fingerprint, such as user logins. These fingerprints are then added to the user's known collection. If the number of distinct fingerprints exceeds a threshold, such as three, it suggests multiple devices attempting actions for the same user, posing potential security risks.

- **Counting data associated with a fingerprint:** This involves counting the number of internal identifiers linked to a single fingerprint.

3.3 Knowledge-based Binding

Knowledge-Based Authentication (KBA) involves generating a series of questions, designed to assess the user's knowledge and verify their identity [10]. The purpose is to prevent unauthorized access by ensuring that only the legitimate owner of an account, who has the required knowledge, can answer the questions correctly. KBA functions under the premise that only the true owner would have, or be able to find, the necessary information to answer these questions accurately [127].

Typically, strong KBA questions should operate under these guidelines [128]:

- The answer should be relatively easily remembered.

- The question should not have more than one correct answer.

- The answer must not be easy to guess, or discover through research.

- The question should be suitable for a broad section of the population.

There are two distinct main categories of KBA authentication, static and dynamic. The classification is determined by the basis of the questions, for example from basic personal information to more complex information requested from the user.

Static KBA, also referred to as *"shared secret"* authentication, involves predetermined questions and answers, that are both known before an authentication attempt, by both the system and the user [127]. Users select questions and provide answers beforehand,

[10] While this technique, similar to knowledge-based Behavioral Biometrics discussed in section 3.1.2, also employs knowledge for authentication, its operation differs significantly. Knowledge-based Behavioral Biometrics authenticate users by analyzing their typical behavior or actions, using reaction challenges to calculate their uniqueness relative to other individuals. In contrast, dynamic knowledge-based authentication, as presented in this section, relies on information stored in the user's memory, using data and security questions. Consequently, users are assessed mainly on their ability to recall specific information, rather than being evaluated based on their unique responses to information, as in Behavioral Biometrics.

and the system stores these pairs for future identity verification. Typically, passwords and *"secret questions"* are examples of static KBA. Static KBA often employs basic personal questions such as: "What is your mother's maiden name?", that can be factual, such as "Where did you spend your honeymoon"?, or preference-based, such as "Who was your favorite teacher"? [128]. A significant drawback of static KBA questions, is the likelihood of answers being publicly available, especially since the amount of personal information on social media is huge. This vulnerability exposes static KBA to security breaches. If malicious actors manage to find the answers, there is an enhanced risk, especially when they are consistently provided in the same way at every login. For instance, in a 2008 incident, the email account of the Alaska governor was compromised. During that time, an attacker was able to change her Yahoo! password, since the answers to static security questions, were available on the internet.

Dynamic KBA refers to an authentication method where the system presents questions that are not pre-known to the authenticating user. This approach is considered safer than static KBA [129], as it improves security by introducing unpredictability into the authentication process.

3.3.1 Functionality and Data Sources

Dynamic KBA is a modern approach to identity verification. Unlike static KBA, it does not rely on easily guessable information, but generates questions in real-time, based on a comprehensive pool of data, gathered from various sources. It operates by presenting users with questions based on their personal history, selecting from a wide range of information such as past addresses, vehicle ownership, or employment history. The user has no idea what questions will be asked. This approach, often referred to as *"out-of-wallet questions"*, searches deep into an individual's personal history. By dynamically generating questions, this method adds an extra layer of security, therefore making it harder for other users to impersonate the legitimate owner.

One of the key advantages of dynamic KBA is its ability to adapt and respond to real-time or historical data, ensuring that questions remain relevant and difficult to guess. If the user attempting authentication fails to respond within a specified timeframe, the question is discarded [128], preventing account takeover attempts.

Examples of dynamic KBA include questions such as *"Which address matches a residence you lived in during 2005"*?, or *"What were the two last digits of your social security number?"* [127]. A user could have to also choose one of multiple answers [130], to test how quickly he would find the correct one compared to a malicious actor.

There also exists a more protected version of dynamic KBA, known as advanced dynamic KBA, which uses security questions derived from data stored behind firewalls [131].

Dynamic KBA uses various data sources to obtain data for the question generation, such as:

- The user's recent activities or transactions
- Credit reports
- Device information (e.g., IP address, device fingerprint)
- Location information

- Social media activity
- Account history and previous interactions
- Public records (employment, education, healthcare)

3.3.2 Security Concerns

While a common concern about the security of KBA is the public accessibility of data used in its questions, the time frame for answering plays a crucial role. Most systems, give a very short time period for the user to answer them. Attackers would need significantly more time to respond correctly to complex questions. Additionally, much of the data used is system and account-specific, limiting access to legitimate users. Requiring responses within a short timeframe, as well as mandating answers to multiple questions, helps prevent unauthorized access attempts. Thus, while the data sources may be public, dynamic KBA could be secure due to these factors. Nevertheless, the system could still be vulnerable to guessing attacks, where the adversary would just try different outcomes until they get access.

3.3.3 Privacy Concerns

Dynamic question generation often involves accessing personal data, which can raise privacy concerns and potentially violate data protection regulations. Individuals may feel uneasy knowing that the authentication system relies on accessing and analyzing public records, which contain a vast amount of personal information, including addresses, phone numbers, and financial history.

Using sensitive data for authentication without explicit consent raises significant concerns. Moreover, inaccuracies in public records and outdated information could lead to access problems. Additionally, how the data is handled, stored, and transmitted is crucial.

In summary, a dynamic KBA system should incorporate privacy safeguards, transparent practices, and provide clear information to users.

3.3.4 Case Study

In this section, we will present the dynamic KBA service implemented in the *ZohoSign* electronic signature services [132]. The offering is powered by IDology [133], a global identity verification and document authentication platform.

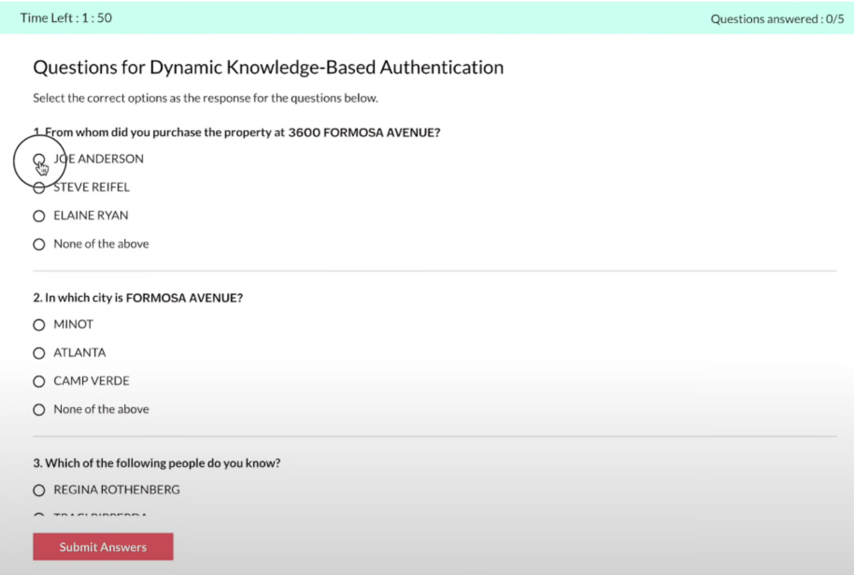
Introduction: ZohoSign currently offers Dynamic KBA exclusively for US residents. This feature allows verification through out-of-wallet questions, which are generated based on credit charges and demographic data obtained from public records. Typically, the service aims to authenticate the signer's identity before opening or signing a document, ensuring they are the rightful owner and not an impersonator.

The authentication process: The authentication process involves collecting specific information from the signer, which is not stored after the authentication process, including their first name, last name, year of birth, the last four digits of their social security number, and their address. This data is then transmitted to the IDology data center, where questions are generated based on matching information derived from public records, such as past addresses, phone numbers, and financial history.

Typically, the authentication process consists of five questions that must be answered within a two-minute timeframe. The system manager has the flexibility to adjust this timeframe and other parameters related to the authentication process based on specific requirements or preferences. In case the user fails to complete the questions within the allocated time, the selected options are automatically submitted for verification.

The validation process: If the answers provided by the signer match the expected responses, the user is successfully validated, and access is granted. However, if there are differences between the answers provided and the expected information, access is denied.

Question generation: The questions presented to the signer are varied and dynamic, drawing from multiple sources and changing with each authentication attempt. This makes it significantly more challenging for unauthorized individuals to successfully impersonate the signer. The questions may involve countries of residence or properties owned during a specific time period.



Time Left : 1 : 50

Questions answered : 0/5

Questions for Dynamic Knowledge-Based Authentication

Select the correct options as the response for the questions below.

1. From whom did you purchase the property at 3600 FORMOSA AVENUE?

○ JOE ANDERSON

○ STEVE REIFEL

○ ELAINE RYAN

○ None of the above

2. In which city is FORMOSA AVENUE?

○ MINOT

○ ATLANTA

○ CAMP VERDE

○ None of the above

3. Which of the following people do you know?

○ REGINA ROTHENBERG

Figure 3.9: *ZohoSign dynamic KBA questions example*

3.4 Context-based Binding

Context-based authentication [11] relies on multiple factors and contexts, such as user account location, device information, and behavioral patterns, to create a distinctive user profile. Although it is not usually implemented as a standalone authentication solution

[11] Aside from Context-based authentication, this method is also referred to as Risk-based authentication, Contextual authentication, and Adaptive authentication.

due to its reliance on dynamic data, it can enhance security as part of a multi-factor authentication strategy, complementing passwords or other authentication methods [134].

This method involves gathering various pieces of information about a user, including geographical location, time of access, network information, preferred device, and behavioral patterns. This data is then analyzed to create a unique behavioral profile [12] for the user. Each time they request authentication, this main profile will be compared with the current user information, which is analyzed in the background, to generate a risk score[135].

If there are significant deviations, the system may prompt the user for additional verification, or deny access altogether if the risk score is high. That is why users must consistently exhibit their typical behavior to reserve access. This helps reduce the risk of account takeover and credential sharing.

Context-based authentication can be used to improve authentication security, by combining multiple factors to verify the user's identity. This ensures that users are who they claim to be, even if someone else attempts to use their credentials.

3.4.1 Functionality

Main Processes

Context-based authentication typically involves two main processes: creating a baseline, and responding to anomalies [136].

In the first process, the system evaluates what user behaviors, actions and scenarios, will be considered suspicious, by collecting data about the user. This creates a baseline for each user account, to define what constitutes normal activity.

Once the baseline is created, the context-based authentication system compares each login attempt against this norm. It continuously scans for anomalies in the background, such as login attempts from unusual locations or suspicious VPNs. If increased risk levels are detected, the system triggers more authentication factors and verification steps.

Main Components

A context-based authentication system typically involves a risk engine and context sources. The risk engine continuously collects and analyzes data from the context sources to determine the risk level with each user access request, through machine learning algorithms, and data mining. The more varied the risk signals and information sources, the more effective the risk engine [136].

Data sources for the risk engine include all the contextual signals of information that can be extracted, such as network signals.

In addition to the risk engine and context sources, a typical context-based authentication system also involves real-time action orchestration to enforce specific access policies. These actions may include denying access or requesting additional steps for identity verification.

[12] While both context-based authentication and Behavioral Biometrics utilize the behavior of the user as a factor, they serve different purposes. Context-based authentication assesses whether the current login attempt aligns with the user's typical behavior patterns, while Behavioral Biometrics (as seen in section 3.1.2) focuses on the unique ways a user behaves, distinct from other individuals, to try to differentiate them and authenticate their identity.

3.4.2 Context Sources:

During a context-based authentication process, factors like location, time, behavior, risk, network and device contexts are typically considered [137].

- **Location-based context:**

  This factor of the risk score involves examining the location from which access is attempted. For instance, if the user requesting authentication is accessing the system from their usual office location, it might be considered lower risk compared to accessing from a remote or unexpected location. Typically, this type of context helps to verify if the access request aligns with the user's normal location patterns.

- **Time-based context:**

  This factor of the risk score analyzes the timing of the access request, a factor important in understanding user patterns. For example, if a user accesses sensitive information during typical working hours, that could be less suspicious than requesting it late at night. In general, time-based context can help to identify deviations from expected behavioral patterns, and raise alerts.

- **Behavioral-based context:**

  By examining various aspects of user behavior, and preferences, and analyzing personal information such as age and gender the system can build a profile of the user's typical behavior and detect any suspicious activities that do not match the normal behavior. This typically involves tracking cookies to understand a user's online behavior, examining call and messaging history for communication patterns, and considering the language and typing preferences.

- **Risk-based context:**

  This process involves evaluating the risk associated with the user account or the information requested. This involves determining whether the user has accessed similar content before, analyzing transaction history for fraud patterns, and examining user activity for irregularities.

- **Network-based context:**

  Factors such as the user's IP address and network characteristics are analyzed, along with network-related data, to identify potential threats, such as suspicious IP addresses or unusual network behavior.

- **Device-based context**

  Examining the device used for access is important to determine the risk of the authentication attempt. This context includes analyzing whether the device has been used previously for similar activities, checking its reputation and status for signs of compromise, and analyzing its usage patterns for anomalies [13].

[13] It is important to note that this approach differs from device fingerprinting, which was mentioned in section 2 of this chapter. While device context analysis focuses on specific aspects of the device's history and behavior, device fingerprinting involves identifying devices based on their unique characteristics.

3.4.3 Case Study:

In this section, we explored various identification tools that implement context-based authentication, namely: BioCatch [69], Sardine [77], TrustBuilder [138], Entersekt [139], Zighra [74], Appgate [140], Cynet UBA [76], SecureAuth [78], ThreatMark [72], Beyond Identity [113], Okta [141], OneSpan [142], Cisco Duo [143], and context-based authentication solutions by Thales [144].
As a case study, we will introduce *SecureAuth* [78], a leading tool in identity and access management solutions, with a specific focus on its SecureAuth *adaptive authentication* capability, part of the Identity platform.

SecureAuth's adaptive authentication technology aims to create a detailed digital profile for the user, collecting hundreds of variables, such as human patterns and geolocation. This technology functions as a *Multi-Factor Authentication* method (MFA), allowing systems to dynamically adjust authentication requirements based on contextual factors when a user requests authentication on a login page. The technology aims to verify the user's identity by considering factors such as location, device status, user behavior, risk profile, and user role. Each factor requires different background tests, for example, device analysis involves examining the endpoint device or server characteristics, while for location information, the system assesses a user's physical location, against known access locations.

By examining all the different factors, the system achieves multi-layer security, making it difficult for an impostor to copy or imitate another account.

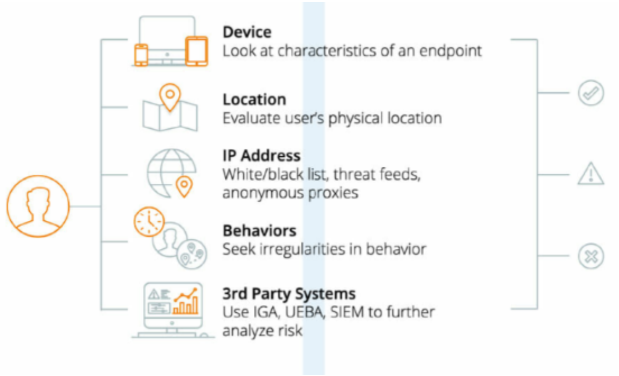
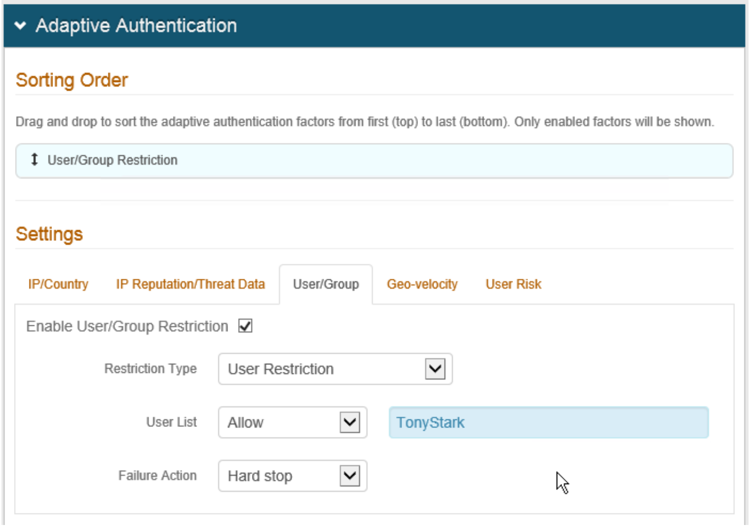

Device
Look at characteristics of an endpoint
Location
Evaluate user's physical location
IP Address
White/black list, threat feeds, anonymous proxies
Behaviors
Seek irregularities in behavior
3rd Party Systems
Use IGA, UEBA, SIEM to further analyze risk

Figure 3.10: *SecureAuth user profile context factors for adaptive authentication*

General Workflow:

Each time a user requests authentication, the authentication request undergoes evaluation, and the system assigns a risk score. Based on this score, the user could be prompted to provide additional information and credentials, or be allowed to log in immediately. This is known as *step-up authentication* since the user could be required to be subject to further authorization if the requested page contains sensitive data and their risk score is high. Other authentication steps could include denying access, allowing access without MFA, requiring an MFA step, forcing a password reset, or redirecting to a secure zone.


Adaptive Authentication

Sorting Order

Drag and drop to sort the adaptive authentication factors from first (top) to last (bottom). Only enabled factors will be shown.

User/Group Restriction

Settings

Enable User/Group Restriction ☑

Restriction Type: User Restriction

User List: Allow TonyStark

Failure Action: Hard stop

Figure 3.11: *SecureAuth access policy set for adaptive authentication*

Chapter 4

Conceptual Framework

In this chapter, we build on the insights from Chapter 3 regarding commercially available holder-binding tools. Our focus now shifts to the underlying principles and fundamental methods of holder-binding. This chapter delves into theoretical cryptographic approaches to address the issue of token-sharing, extending beyond practical applications.

In *Section 4.1*, we classify non-transferability strategies into three categories: disincentivizing, preventing, and detecting token-sharing. This classification helps organize our concepts accordingly.

In *section 4.2*, we discuss disincentivizing token-sharing. This includes Embedding Valuable Secrets in token systems *(Section 4.2.1)*, methods adhering to All-or-nothing Disclosure principles *(Section 4.2.2)*, and controlling and limiting Token Usage by users *(Section 4.2.3)*. *Section 4.3* focuses on preventive mechanisms. Our findings delve into theoretical strategies for Embedding Tokens in Physical Cards *(Section 4.3.1)*, frameworks that use biometric data for secure binding in cryptographic applications *(Section 4.3.2)*, along with the innovative concept of Cognitive Biometrics *(Section 4.3.3)*.

We also define detecting methods, although our research did not uncover proposed theoretical proposals in this area.

4.1 Non-Transferability Strategies

The strategies aimed at achieving the NT principle of tokens and satisfying holder-binding can be classified into three main approaches for managing token-sharing: disincentivizing, preventing, and detecting.

Disincentivization strategies discourage token-sharing through penalties such as legal consequences, loss of privileges, or restricted access. They also increase the complexity or risk in the authentication process, for example, by requiring individuals to disclose more personal information or share physical media with borrowers.

Token-sharing *prevention* strategies involve implementing measures to stop token-sharing from happening in the first place. Key methods include employing strong authentication methods that ensure only legitimate users can authenticate successfully. Additionally, access controls should be applied, allowing access based on contextual factors like the user's device, thereby reducing the risk of unauthorized token use.

Token-sharing *detection* strategies aim to identify instances of token-sharing during, or after, the occurrence of the event. This involves using activity monitoring tools to analyze user behavior for irregularities, suspicious activities, or deviations from normal usage patterns. Despite the availability of various activity monitoring commercial tools, we have not identified any proposed research in this area, which is an intriguing consideration for future exploration.

4.2 Disincentivization Strategies

Individuals often lend their belongings to others for their convenience, or to help out someone close to them. For instance, you might easily lend your bike to a friend so they can buy groceries for you or use it if they do not have access to their own. This type of sharing generally involves little effort, and individuals tend to comply with it quite easily.

However, imagine if lending your bike also meant giving your friend a key to your brand-new car and your house. The bike key could unlock your other valuable belongings too, leaving you without any assurance that your friend would not access them. They would have all the means to use your other personal belongings simply because they borrowed your bike.

Consider another scenario: lending your bike also requires you to share your credit card account information, giving your friend access to your bank account and other credentials.

In both cases, you would probably hesitate or decline to lend your bike because the risks involved, such as giving away personal items or sensitive information, outweigh the benefits of helping your friend or their convenience.

These principles relate to two key concepts in cryptography designed to implement the NT principle of tokens and to discourage their sharing [145], [146]:

- **PKI-assured NT**, where users are prevented from sharing their tokens because doing so would entail exposing a valuable secret outside the system, usually associated with the specific token that was shared. However, it is important to note that such valuable keys are not always present.

- **All-or-nothing NT**, where sharing just one pseudonym or token implies sharing all of the user's other tokens and pseudonyms in the system, i.e., sharing all of the user's secret keys inside the system.

These concepts aim to deter users from attempting to transfer or share their tokens and belong to the category of token-sharing disincentivization strategies. These principles, along with additional deterrent methods identified in our analysis, will be discussed below.

4.2.1 Embedded Valuable Secrets

We can extend the concept of PKI-assured NT by implementing a disincentivization method for token-sharing, using Embedded Valuable Secrets.

Embedding valuable secrets within tokens involves adding sensitive information that users wish to keep private. In this paradigm, tokens not only provide access to services or platforms but also act as containers for additional layers of sensitive information, such as credit card details. This approach discourages sharing by linking access to tokens with access to the user's secret information, aiming to prevent unauthorized disclosure.

However, this strategy faces challenges in effectively identifying valuable secrets that prevent the sharing of tokens, particularly among close family members. Despite these difficulties, the risks associated with such systems can be significant. For example, if a parent were to share their login tokens for a streaming service with their child to facilitate access, they might have reservations upon realizing that their account also contains adult content watch history or similar material. This would inadvertently grant the child access to sensitive and inappropriate content.

There are multiple approaches to implementing Embedded Valuable Secrets in a system, and we present a simplified version inspired by the system of *Digital Signets* proposed by Dwork et al. [147]. The system operates using secret keys, which are utilized to generate digital signets for individual users. These signets serve as authentication tokens associated with specific users, authorizing access to designated content or services. Upon authentication, the system generates a signet precursor using a trapdoor function [1] from the signet, ensuring that users cannot access the content without the necessary authorization. However, if someone were to distribute content along with their secret key, it could potentially compromise the system's security by allowing unauthorized access to the signet precursor, thereby revealing sensitive private information associated with it.

The aforementioned system was designed to prevent the illegal redistribution of digital content via CD-ROMs and other devices, so it faces challenges when adapted to a context without physical devices. Additionally, our primary concern is not the sharing of content but rather the sharing of the tokens themselves. However, we can still draw inspiration from the original idea of binding secrets to credentials that users would not want exposed. We can integrate the signets into a system where they function as separate authentication tokens, identifying users. This approach ensures that if a user shares their tokens, they can assume that the borrower can decrypt the signet and access sensitive information.

4.2.1.1 Simplified System Overview

User Registration: When a user registers for an online service, they provide their authentication tokens (username/email/password) along with sensitive information. The sensitive information is transmitted to the Authorization Center for processing and storage.

Sensitive Information: The sensitive information in this system varies depending on specific scenarios, such as credit card details that could lead to financial loss, or personal identification information that could result in identity theft. Additionally, critical account credentials like those for Google are of significant concern due to their central role in the digital landscape. While the exact nature of sensitive information may vary across social contexts, the underlying principle remains consistent: sharing tokens entails the risk of exposing valuable personal data, serving as a strong deterrent against credential sharing.

Signet Generation: After registration, the authorization center generates a unique cryptographic signet for each user. This signet is derived from their sensitive information and serves as a digital identity key for the service. The signets are stored and associated

[1] A trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the *"trapdoor"* [148].

with each user that has registered. The signet is then transferred to the specific service the user requests registration for and stored in their records for future authentication.

Signet Precursor: When a user attempts to access a specific service, the authentication center sends them a signet precursor for that specific service, that they can unlock with their tokens and obtain the signer. This precursor is a transformed version of the actual signet and requires additional processing to obtain the full signet.

Trapdoor Function: The transformation from the signet precursor to the full signet involves a trapdoor function, a cryptographic algorithm based on the user's tokens. If a user shares their tokens, unauthorized individuals could access the signet precursor, allowing them to derive the full signet and gain unauthorized access to features and sensitive information.

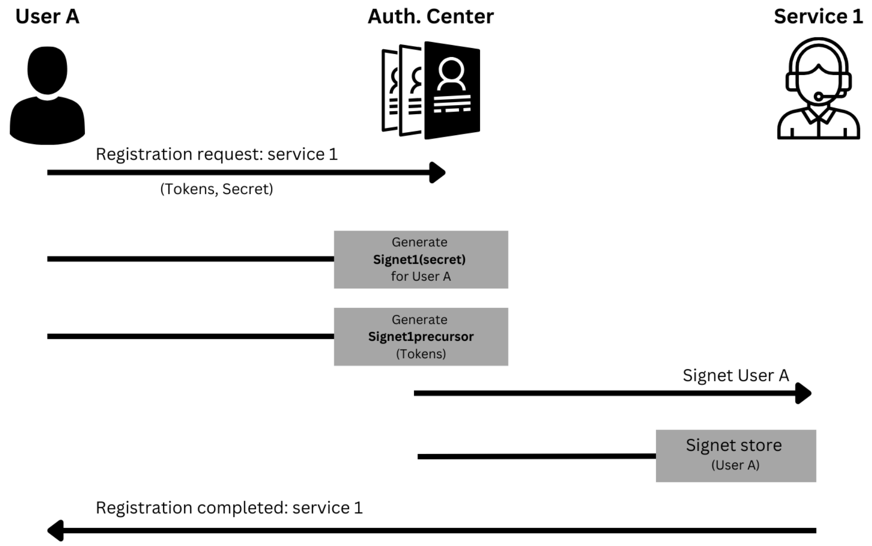


Figure 4.1: *Embedded Valuable Secrets through Signets - Service registration*

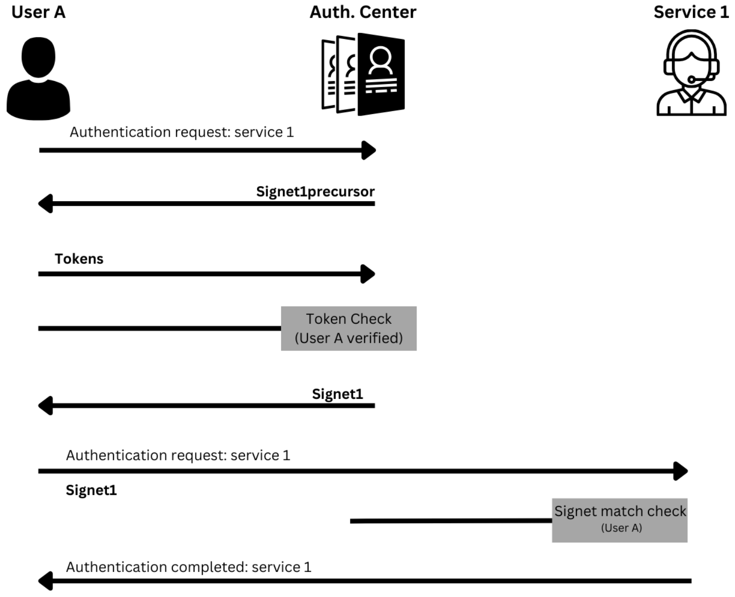


Figure 4.2: *Embedded Valuable Secrets through Signets - Service authentication*

4.2.2 All-or-nothing Disclosure

We can envision an implementation of the All-or-nothing NT principle by linking tokens together through a centralized authentication service. Essentially, users would only need to use one *"powerful"* master token to access any service within the system. For instance, a user's Google account could serve as this master account, linking all the user's services together. This approach could deter users from giving away access to one service since that could be proven dangerous and risky, giving out the master tokens. This means the recipient would gain access to all services the user is registered for, not just the intended ones.

A potential implementation protocol is the *Central Authentication Service* (CAS) [149], which functions similarly to a *Single Sign-On* (SSO) system [2]. The purpose of CAS is to allow a user to access multiple applications while providing their tokens (such as user ID and password) only once. One of the most powerful features of the CAS protocol is its ability to act as a proxy for services, transmitting the user's identity. When an application requires authorization, it will redirect the user to a centralized, trusted CAS server.

4.2.3 Limited Use Control

Another approach would be to limit the usage frequency of tokens, aiming to discourage users from sharing them with others. This measure could be valuable in scenarios offering

[2] SSO refers to an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems [150].

resources with limited access, such as article libraries. By imposing restrictions on the number of times a token can be used within a specific timeframe, e.g., only once a day, users are less inclined to share them and waste their resources on someone else. This introduces inconvenience to the authentication process, thus acting as a deterrent to token-sharing. This concept, similar to API throttling (a practice commonly employed to manage system services effectively and prevent threats like brute force attacks [3] and DDoS attacks [4]) now aims to prevent token-sharing. Some strategies for implementing this process could be:

- **Time-based access controls:** Systems can be configured to grant access only during specific time slots predetermined by the user. For example, access might be restricted to business hours, reducing the likelihood of token-sharing during non-essential periods.
- **Usage quotas and session management:** Systems can establish predetermined quotas for token usage within specific time intervals.
- **Access monitoring:** System administrators can monitor token usage and trigger alerts for unusual activity, such as frequent usage or simultaneous access from multiple devices.
- **Personalized service rates:** Different service categories can have varying usage restrictions. For instance, financial services may impose stricter limitations on token usage to enhance security.
- **Rate limiting:** Systems can enforce predefined restrictions on the number of login attempts within a specified timeframe from a single user or IP address. Another solution is to restrict access to a specific IP address for each account or token. Both solutions make it challenging for multiple users to share the same tokens effectively, as they would encounter login limitations.

4.2.3.1 For Anonymous Credentials

This concept could be applied similarly to conditional anonymity, a commonly proposed strategy that applies to anonymous credentials. Initially, users are granted a default privilege, such as anonymity, which may be revoked if they commit an unauthorized activity that is detected by the system. This concept allows for the identification of misbehaving anonymous users under well-defined conditions [153], while ensuring user actions remain anonymous until certain criteria are breached.

Damgård, Dupont, and Pedersen introduced the first scheme aimed at addressing this challenge by examining the frequency of transactions within a given time period [154]. Users could anonymously submit data at a limited rate, enabling the system to flag participants who exceed this threshold. Before this, many schemes focused on detecting double spending in e-cash transactions. In such schemes, a user's privacy was guaranteed

[3] A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly [151].

[4] Denial-of-service attacks (DoS attacks) and distributed-denial-of-service attacks (DDoS attacks) are attempts to make a computer, computer network or service unavailable or more difficult to reach for the intended customers [152].

if they used coins only once; however, if a coin was reused, the bank could trace it back to the user's account and identify the double transaction [155], [156].

Double transactions, in the case of money or other tokens, might be an easily definable case of *"user misbehavior"*. However, in most scenarios, it is difficult to objectively and clearly define misbehaviors by rule, as there are often subjective acts of such (e.g., posting a false article on Wikipedia).

The *Blacklistable Anonymous Credential system* (BLAC) [157], defined by Tsang et al., is a cryptographic construction of anonymous credentials that supports anonymous blacklisting based on subjective judgments of misbehaviors, without revoking anonymity, which might be too strong a punishment for users. In this system, simply blocking misbehaving users from making future access attempts, while still maintaining anonymity, is sufficient. Users anonymously authenticate to *Service Providers* (SPs) using credentials issued by a *Group Manager* (GM). The GM enrols legitimate users and issues credentials that remain private to the user. The GM's role is limited to user enrollment and credential issuance without compromising user privacy. SPs serve anonymous users as long as they are enrolled by the GMs and have not misbehaved, maintaining their own blacklists of misbehaving users without knowing their identities.

Another solution, proposed by Camenisch et al. [158], introduces a *glitch protection scheme*, which defines a token that the user can reuse up to a predefined threshold number of times. In this context, a glitch refers to the occasional reuse of a token. This reuse may not necessarily indicate malicious actions but could be a simple mistake. However, if the number of glitches detected exceeds the predefined threshold, all of the user's transactions are revealed. This framework can be applied beyond the scope of anonymous credentials. For instance, in scenarios not limited to anonymous credentials, detecting the double use of credentials within a specific time frame could lead to account suspension, termination, or other penalties. The underlying concept remains consistent: a user is granted a privilege by default, which is revoked if they break certain rules, such as sharing their credentials.

4.3 Prevention Strategies

Unlike disincentivizing methods, preventive strategies ensure that users are unable to access the system using tokens that have not been specifically issued to them. This is achieved through robust access controls. Most of the commercial tools discussed in Chapter 3 fall into this classification, offering a strong security guarantee. Below, we will present the theoretical frameworks identified within this category.

4.3.1 Embedded Tokens in Physical Cards

We now propose the use of tamper-resistant [5] physical cards. This concept can be classified as both a disincentivizing and a preventive mechanism against token sharing. Incorporating a physical item in the authentication process adds an extra layer of security and acts as a deterrent against sharing. Users are less likely to share tokens if it means losing

[5] Tamper-resistance refers to the ability of a device to defend against a threat that has the objective to compromise the device and or the data processed by the device [159]. The stored information must remain protected, even when the attacker can work on several samples of the module undisturbed for weeks in a well-equipped laboratory [160].

access until the card is retrieved. The physical card represents tangible ownership, increasing accountability and awareness of the risks associated with sharing. Furthermore, the inconvenience of replacing a lost card serves as an additional deterrent. However, throughout this concept, we explore incorporating biometrics or other advanced security measures into physical cards, making them a preventive mechanism. By adding the risk associated with sharing the physical object, this approach becomes stronger against token sharing.

The concept involves delegating tokens to a physical medium, enhancing their security, given the information on the card cannot be directly read. By embedding tokens in a physical object, unauthorized use decreases significantly, as tokens become harder to transfer. Various recommendations exist for the content and functionalities of such cards.

A proposed approach involves storing the tokens within the owner's identity card [161]. In this concept, having access to a token also implies having access to the identity card of the legitimate user to whom it was issued. In that way, lending the card to give away the token, poses a significant risk of impersonation for the legitimate owner. This scenario mirrors embedding valuable secrets in the token, where exposure reveals the user's identity. This could deter users from lending their tokens, as it would mean sharing their identity card. Furthermore, the biometric image on the card significantly reduces the likelihood of users being impersonated by someone attempting to bypass authentication.

Another approach is to store tokens on smart cards, offering a privacy-friendly solution independent of identity cards. A proposed implementation of this involves *dual-interface smart cards* [161]. One interface could be dedicated to identifying and authenticating the holder, while the other side could be used for presenting the tokens. This setup would ensure that the holder can verify their identity and showcase the tokens separately. This distinction is particularly important for anonymous credentials, where users must prove their identity or remain anonymous in different scenarios. The smart card should have mechanisms implemented to ensure that one interface, for example, a contact-enabled one, is exclusively used for identity verification, while the contactless interface would be used for displaying tokens [6]. So, for instance, when the card would be inserted into a reader, the user's identity would be revealed, whereas holding the card close to a scanner would only display the tokens anonymously. This setup would discourage users from giving away their authentication rights and token use rights simultaneously, as that would expose them to the risk of impersonation attacks. This system could be applied in scenarios where users would initiate authentication by inserting their card into a trusted central authority system. Subsequently, they would scan the token side of the card on a specific service's system. If the tokens stored on the card matched those of the legitimate user in the ecosystem's server, access would be granted.

Another method for embedding tokens on smart cards, proposed by Hesse et al. [162], involves binding anonymous credentials to a user using a smart card that displays the user's picture. The scheme is designed solely for in-person verification, requiring credentials to be issued and possession to be proven face-to-face. Issuers and verifiers must confirm the cardholder's identity by matching them to the photo on the card. While this reliance on in-person verification is a possible shortcoming, it remains important to look into how the scheme functions. The authentication process consists of three phases:

[6] The tokens could also be stored in a tamper-proof module within a smartphone or a computer. The outcome would be the same.

1. **Smart Card Registration:** In the first phase, the holder authenticates in person to the card issuer and obtains a smart card displaying their picture, along with necessary authenticity marking. The card contains a secret *Unique Identifier* (UID) and other confidential values important for the digital authentication protocol. It is important to note that the UID is not disclosed to the holder of the card.

2. **Credential registration:** The legitimate owner further authenticates in person to a credential issuer, presenting the genuine card for visual confirmation. Upon successful authentication, the holder then receives a digital credential from the issuer, certifying a set of attributes, including the card's UID. This necessitates involvement from the smart card: during the authentication process, the credential issuer scans the card to obtain the blind signature request component for the UID. Subsequently, the credential issuer proceeds to sign this component, along with other attributes in the credential.

3. **Credential presentation:** During an authentication request, the holder selectively discloses certain attributes while proving knowledge of them, to the verifier. Since the UID is unknown, it cannot be proven by the holder. Therefore, the card must be present during the authentication process to fulfil two roles: visually authenticating the holder, and contributing to the cryptographic authentication protocol by proving knowledge of the undisclosed UID attribute.

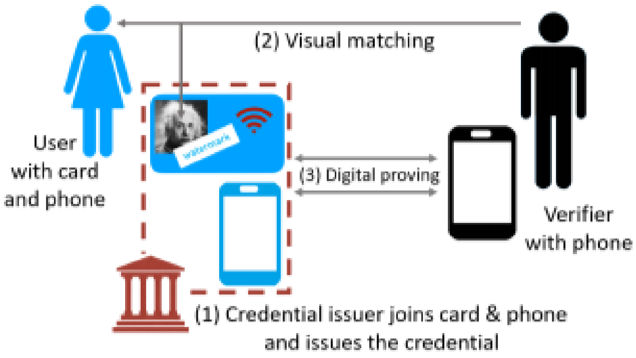


Figure 4.3: *Overview of the anonymous credential system that binds digital proving (3) to visual authentication of the phone holder (2), with the help of picture-showing smart cards that are bound to phones by credential issuing authorities(1)[162].*

A potential enhancement for the existing physical smart card schemes would be integrating *Biometric Cryptographic Systems* (BCSs), which will be discussed later in this chapter (*section 4.3.2*). For dual-interface smart cards, this involves equipping the cards with local biometric scanners (e.g., fingerprint or facial recognition) and secure processing units for cryptographic operations. The card firmware must support secure storage and matching of biometric templates, ensuring data protection and quick interaction between the components. This change improves security by binding the card to its legitimate owner through biometrics, reducing the risk of unauthorized use even if the card is lost or stolen.

In the case of the proposal by Hesse et al., the integration of BCSs would facilitate online authentication, thereby extending the smart card's functionality to online platforms. This would address the previously discussed limitation of relying exclusively on physical verification. This enhancement would necessitate secure online communication protocols to ensure safe data transmission. When a user initiates an authentication request remotely, the smart card could perform a kind of biometric verification locally. The data would be processed within the card's secure environment, and once verified, the status would be communicated to the remote system using encrypted protocols. This enhancement would enable remote authentication by verifying the user's identity through biometrics.

4.3.2 Biometric Cryptosystems

Biometrics, encompassing physiological and behavioral forms, provide viable alternatives to traditional password-based authentication systems. These systems use classifiers to differentiate legitimate users from imposters [163]. However, there is another way to utilize biometric systems. Biometrics can be used in bio-cryptography to create *Biometric Cryptosystems* (BCSs), where a digital key is securely bound to or generated from a biometric. Such keys serve as personal user keys to encrypt and decrypt information and are already employed in symmetric and asymmetric cryptosystems [164], [165]. Through bio-cryptography, access control can be enhanced for mobile devices, ATMs, financial services, and other facilities requiring secure access [166].

4.3.2.1 BCS Schemes

Biometric encryption combines cryptography with biometrics by storing cryptographic keys in a trusted container. It involves taking biometric data from an individual, extracting the biometric characteristic sets, comparing them to the data in the registration database, and returning the result. The key is released only after successful biometric verification, and then enters a cryptosystem. This process creates a double-layered security scheme, where biometric data is used as a key to access the cryptographic key in the first layer, and then the cryptographic key unlocks the second layer [166].

BCSs are typically split into three categories.

1. **Key binding**
   In key binding schemes, helper data are created by linking a selected key to the biometric template. This creates a combination of the secret key and biometric data stored as helper data. During authentication, keys can be extracted from this helper data using a chosen algorithm. Cryptographic keys are separate from biometric features, allowing for the revocation of keys. However, updating the key usually involves reenrolling to generate new helper data [167]. A potential drawback is that this process assumes attackers cannot access resources revealing the key, such as selection tables or user-specific models, which might not hold true if the key generation device is vulnerable to capture or examination [163].

2. **Key generation**
   Key generation systems produce cryptographic keys from biometric data [168].

However, extracting keys from such data is challenging and presents several issues [163]. For instance, noise is introduced during the capturing and analysis of a sample, making it difficult to derive a consistent cryptographic key from noisy data. Moreover, key extraction typically applies to data following specific distributions, whereas biometric data are sparse and do not follow normal distributions. Therefore, quantizers, which are algorithms that map biometric templates to a discrete domain, are needed to convert them into a finite set of points.

Many BCSs correct the noise in the data by using public information derived from the original biometric template. This requires storing biometric-dependent public information, known as helper data, which is used to retrieve or generate keys. Helper data must not reveal information about the original biometric template. Error and entropy control are essential in this process, and it is desirable that little information about the biometric templates is revealed even in the worst case (i.e., the entropy loss should be low).

There have been many BCSs designed, with each system deriving different information. For reference, here are the main proposals:

- **Fuzzy Commitment Scheme [169]:** One of the first proposed techniques, based on binary-error correcting codes, considers binary strings. The fuzzy extractor algorithm converts biometric data into secret, uniformly random, reproducible strings.
- **Fuzzy Vault Scheme [170]:** Uses polynomial interpolation to correct errors by taking a set of elements in a finite field with set difference as the distance function.
- **Secure Sketches Scheme [163]:** Generates a public sketch from quantized biometric data, enabling efficient reconstruction of the original data for cryptographic key extraction while revealing minimal information about the biometric template itself. The key is extracted from the reconstructed data, ensuring that no data about the original template is revealed.

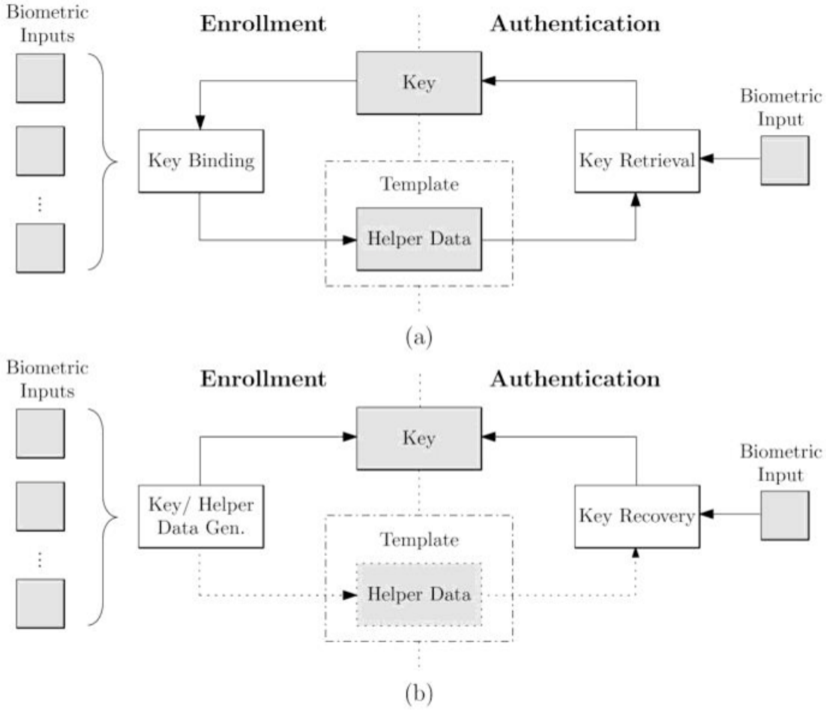


Figure 4.4: *Key binding (a), Key generation (b) schemas [167]*

3. **Hybrid schemes**

   There are many schemes that mix methods. These are combinations of different schemas, to enhance the features and protection against different attacks.

4.3.2.2 Related Work

There also exist less cryptographic methods for key generation from different biometric modalities. For instance, Venčkauskas et al. [175] propose a method for generating complex cryptographic keys from finger vein minutiae points by using several instances of finger vein patterns and combining them with a password. Similarly, Sheng et al. [176] propose a method that employs modifications to individual features and groups of features to identify numerous reliable and distinctive elements for generating keys from handwritten signatures. This approach can enhance security when combined with biosalting (passwords) and additional data such as PINs, usernames, and emails, making decryption more challenging. However, these methods do not offer a sufficiently rigorous treatment of security compared to well-established cryptographic techniques [163].

Type	Method	Operation mode	+Strength/-Weakness
Key binding	Bio-encryption [171]	Template matching	+ Encrypted template - Vulnerable to certain attacks
	Fuzzy commitment [169]	Key binding and release; Helper data	+ High protection of bio-data, Error Correction, - Reconstruction of bio-data from template if secret key is disclosed
	Fuzzy vault [170]	Secret key; Minutiae	+ Error Correction, polynomial encoding, - Vulnerable to certain attacks
	Shielding function [167]	Helper data; Random key	+ Hash function, - Vulnerable to certain attacks
Key generation	Fuzzy extractor [171]	Helper data; Random Keys	+ Eliminates template; secure bio-data, - No revocable keys
	Secure sketch [163]	Helper data; Quantization of features	+ Does not store template, - Vulnerable to certain attacks
Hybrid	Fuzzy vault and password hardening [172]	Secret key	+ Improved vault security, - Higher entropy
	Cancellable and Secure Sketch [173]	Template transform	+ Error Correction
	Fuzzy vault and cancellable [174]	Regional transform; Feature Vector	+ Error Correction, -Higher entropy

Table 4.1: Comparison of existing bio-cryptosystems [166]

4.3.3 Cognitive Biometrics

Cognitive Biometrics introduce a new scheme that utilizes the cognitive, emotional, and conative state of an individual as the basis of user authentication and/or identification [177]. This method complements the traditional biometric modalities of physiological characteristics (what we possess), such as fingerprints or iris patterns, and behavioral characteristics (how we behave), such as gait or typing dynamics, by incorporating *"the way we think, feel, and respond"* [178]. Cognitive Biometrics refer to methods and techniques for authenticating people based on the measurement of signals generated directly or indirectly from their thought processes, which reflect their mental and emotional states [179]. This approach could be likened to a challenge-response paradigm, where the system presents a challenge (such as a task) to the user, who then responds in a characteristic way. For instance, consider a cognitive security system employing user identification through the recall of a sequence of images. Each user is presented with a sequence of pictures and is requested to recall them in a predefined order. The system then not only verifies the correctness of the sequence but also monitors additional metrics including time taken, hesitations between selections, and specific errors made. These data are utilized to generate cognitive patterns for individual identification, such as memory recall speed and error recognition. Essentially, this new version of biometrics aims to capture individuals' cognitive and emotional patterns for authentication purposes.

Cognitive Biometrics are extracted through the recording of biosignals by various methods, including *Electroencephalography* (EEG [7]), *Electrocardiography* (ECG [8]), *Blood Volume Pulse* (BVP [9]), *Electromyography* (EMG [10]), *eye trackers* (Pupilometry[11]), and related technologies [177]. These signals directly or indirectly measure the human thought processes, emotions, perception and understanding. Typically, Cognitive Biometrics analyze responses of nervous tissue to the presented stimuli, following a stimulus-response paradigm. Stimuli could include familiar photographs, memorable events, songs, or even Rorschach ink blots [12], presented in video and/or audio formats [186], [177]. Stimuli are selected to collect characteristic changes in acquired biosignals, representing unique responses from individuals. Machine learning algorithms process these changes to create a unique signature for individual identification or authentication. Cognitive Biometrics can operate in static or continuous modes, either alone or in combination with other modalities [177].

One of the notable security benefits is that Cognitive Biometrics inherently support liveness detection and continuous authentication, thereby reducing susceptibility to spoofing attacks. Additionally, Cognitive Biometrics are difficult to mimic, steal, or coerce because individuals' cognitive reactions are unique and not easily replicable.

Moreover, a common security concern with other types of biometrics, such as Physiological Biometrics, is their invariability over a person's lifetime, making them '*uncancellable*' in the manner of a password [187]. Once leaked, such biometric information cannot be reused for authentication, posing a long-term security risk. In contrast, the cancellable nature of Cognitive Biometrics allows compromised identifiers to be replaced with new ones, thereby enhancing security.

Certain sources discussing Cognitive Biometrics, such as [178], argue that Cognitive Biometrics offer enhanced privacy because biosignals are internal traits and are not exposed to the public, unlike fingerprints, for example. However, it is important to note that while there are security benefits as mentioned above, Cognitive Biometric systems also raise significant privacy concerns due to the handling of sensitive data and their invasive nature. These concerns call for attention and will be examined further in the next section.

4.3.3.1 Discussion

Despite the promising potential of Cognitive Biometrics, several concerns regarding privacy, ethics, and usability have been raised.

- **Cost and Equipment Accessibility:** Cognitive Biometrics are hindered by the need for costly specialized equipment, such as EEG technology, which can be im-

[7] A method of recording an electrogram of the spontaneous electrical activity of the brain [180].

[8] The process of producing a recording of the heart's electrical activity through repeated cardiac cycles [181].

[9] A method of detecting heart-beats by measuring the volume of blood passing the sensor in either red or infrared light [182].

[10] A technique for evaluating and recording the electrical activity produced by skeletal muscles [183].

[11] The measurement of pupil size and reactivity [184].

[12] The Rorschach test is a projective psychological test in which subjects' perceptions of inkblots are recorded and then analyzed using psychological interpretation, complex algorithms, or both [185].

practical and off-putting to users. This requirement acts as a barrier to widespread adoption, limiting accessibility and implementation.

- **Security Vulnerabilities:** Security concerns arise with Cognitive Biometrics, particularly regarding the potential for identity theft and simulation. Just as models can be trained to recognize individuals based on their signals, malicious actors could capture these signals and train models to simulate a person's identity, posing significant risks to security and privacy.

- **Limited Availability and Commercial Offerings:** Despite promising potential for the field of biometric authentication, Cognitive Biometrics are constrained by limited public availability and commercial viability. This lack of accessibility and availability restraints widespread adoption and integration into existing systems.

- **Reproducibility and Uniqueness Concerns:** Questions regarding the reproducibility and uniqueness of stimulus-response mapping in Cognitive Biometrics have been raised. While there is inherent variability in biosignals, research suggests that with further investigation into how emotions affect these signals, they can be accurately reproduced and used for authentication purposes. Additionally, biosignals may contain genetically transmittable features that contribute to individual uniqueness, offering potential solutions to reproducibility concerns.

Cognitive Biometrics are not available to the public or have commercial offerings yet, however show promising offerings in the biometric scheme in the future, binding people to the way they think and feel, and considered to be much easier for the user to remember, and more difficult for an attacker to imitate [186].

Chapter 5

Evaluation

In Chapters 3 and 4, our objective was to investigate techniques for binding authentication tokens to individuals, aiming to provide an overview of the current landscape. In Chapter 3, we examined established mechanisms in the commercial environment. We have identified six primary commercial mechanisms, grouped into four categories. In Chapter 4, our goal was to move beyond existing commercial binding methods. We focused on exploring theoretical concepts through proposed papers and frameworks that could shape the future of identity management, binding individuals to their tokens without yet having practical offerings. In the end, we identified six more theoretical concepts. Altogether, the Binding Ecosystem consists of twelve methods for binding tokens to their holders.

In this Chapter, we aim to form a classification system for the collected holder-binding strategies. Our objective is to try to create an evaluation of these methods to assist in deciding the optimal solution for different credential system scenarios based on various criteria.

5.1 Mapping the Binding Landscape

In this section, we will revisit the gathered binding landscape, aiming to provide an overview and group our findings further. As previously outlined in *Section 4.1*, we categorized NT strategies into three primary categories based on their objectives for token-sharing: sharing *disincentivization*, sharing *prevention*, and sharing *detection*. We have already applied this classification to the proposed concepts discovered. Now, we aim to classify our collective findings on holder-binding techniques within each of these categories.

Type	**Theoretical Concepts**	**Commercial Mechanisms**
Disincentivize	Embedded Valuable Secrets All-or-nothing Disclosure Limited Use Control	
Prevent	Biometric Cryptosystems Cognitive Biometrics Embedded Tokens in Physical Cards	Physiological Biometrics Behavioral Biometrics Visual Presence Identification Knowledge-based Binding
Detect		Context-based Binding Device-based Binding

Table 5.1: The three types of Binding Strategies

The first category of strategies focuses on disincentivizing token-sharing. This is accomplished by increasing the risks or costs associated with the authentication process for individuals who choose to share their tokens. We were unable to identify any commercial tools that operate under this principle. This is understandable, as it provides a theoretically weaker security foundation. Relying solely on the idea that users might be less motivated to share their tokens does not offer a strong basis for professional systems. However, we identified three distinct theoretical concepts in this category.

The first method involves *Embedding Valuable Secrets* into tokens, by integrating sensitive information like credit card details, discouraging token-sharing by making it risky of exposing such data. Users register with tokens and a unique cryptographic identity key, discouraging the sharing by linking personal data directly to the authentication process. The second approach is *All-or-nothing Disclosure*, which involves linking pieces of secret information or tokens. Users authenticate with their master account token across all services, and therefore sharing this token grants access to all associated services. In the last concept, we explored *Limited Use Control* methods to deter token sharing. Techniques such as time-based access controls, session management and rate limiting are implemented to restrict how often tokens can be used.

The next category of strategies focuses on preventing users from sharing their tokens, ensuring that only tokens issued to a specific user can be used for authentication. This is achieved through robust access control measures and by examining various characteristics of each individual, effectively preventing unauthorized token-sharing.

We identified three theoretical concepts for this category. First, we discussed *Biometric Cryptosystems*, systems in bio-cryptography that securely bind or generate digital keys from biometrics, enhancing access control for various secure applications by integrating these keys into symmetric and asymmetric cryptosystems. We also explored a novel form of biometrics known as *Cognitive Biometrics*, which detects individuals' cognitive, emotional, and conative states, similar to a challenge-response paradigm. Users are presented with tasks that monitor their responses, providing insights into their thoughts, emotions, and behaviors. Lastly, we identified *Embedded Tokens in Physical Cards*, a concept centered around binding users to tamper-resistant physical credential cards, utilizing a physical medium as an obstacle against token-sharing.

Alongside the theoretical concepts, we identified a few commercial mechanisms designed to prevent token-sharing. The first category of these mechanisms involves biometric binding. Biometric binding ties a holder to their biometric traits, proving ownership of a token through specific biometric characteristics. We have identified three biometric binding approaches, all categorized as preventive strategies due to their reliance on strong access control measures.

The first approach, *Physiological Biometrics*, analyzes physiological characteristics like fingerprints and facial features. We reviewed 23 tools and presented *VeriDas*, a voice biometric system verifying identities within 3 seconds of voice samples. The second approach, *Behavioral Biometrics*, verifies holders by analyzing their behavioral patterns and unique characteristics. We identified 16 such tools and discussed *TypingDNA* as a case study, distinguishing users based on typing patterns and profiles. The third method, *Visual Presence Identification*, verifies the individual as the legitimate owner of a token and ensures they are a genuine person attempting authentication. We reviewed 14 such tools and presented the case of *Amazon Rekognition*, which authenticates users by recording a selfie video to verify liveness, comparing it with the user's ID picture, and checking for uniqueness within the system's database.

As another preventive commercial mechanism, we studied *Knowledge-based Binding*, where individuals are linked to their tokens through dynamic and static knowledge verification methods. We focused on dynamic KBA, which uses real-time knowledge questions (out-of-wallet questions) based on factors like credit reports, device and location data, and social media activity. Our case study looked at how *ZohoSign* integrates *IDology*'s dynamic KBA to authenticate US residents with out-of-wallet questions based on public records, ensuring identity verification before document signing within a specific timeframe.

The third and final category involves detecting the sharing of tokens after it has occurred. This approach focuses on identifying token sharing by employing adaptive authentication, where access controls adjust based on the detected individual. We did not identify any proposed research for the category of token-sharing detection, despite the focus of many commercial tools in this area and its popularity in the commercial sector.

Regarding commercial mechanisms, we first explored *Device-based Binding* through device fingerprinting. This technique gathers hardware, software, and network details to create a unique identifier called a device hash, which uniquely identifies individuals. We reviewed 22 commercial tools employing device fingerprinting for authentication and presented a case study on *Fingerprint Identification*, a product by *Fingerprint*. This tool uses advanced algorithms to generate unique *VisitorIDs*, distinguishing between identical physical devices and their respective owners.

Lastly, we discussed *Context-based Binding*, which ties a holder to multiple factors like location, device information, and behavioral patterns to form a detailed user profile. While not a standalone authentication solution, it plays a crucial role in multi-factor authentication. We reviewed 14 tools implementing context-based authentication and examined *SecureAuth* as a case study. SecureAuth's adaptive authentication feature dynamically adjusts authentication requirements based on contextual factors such as location, device status, behavior, and risk profile, utilizing hundreds of variables.

Concluding our findings, most strategies were identified in the category of token-sharing prevention strategies, with 4 commercial mechanisms and 3 theoretical concepts. These strategies are based on strong access controls to ensure individuals cannot access a system with tokens that were not issued to them, which would make sense, as it is typically the most common requirement for secure systems. For detection strategies, we only discovered commercial mechanisms. In contrast, for disincentivization, we found only theoretical concepts.

5.2 Evaluating the Binding Landscape

This section outlines the metrics and criteria for evaluating the collected strategies. We will first assess how effectively the methods adhere to the principle of holder-binding, using various factors to determine their security in this aspect. Following this, we will conduct a broader analysis based on general criteria relevant to different stakeholders. By combining these two evaluations, we can present a more complete picture of the strategies, making it easier to identify what best suits the needs of different systems.

5.2.1 Methodology

To establish the metrics for both types of evaluations, we reviewed a range of standards, proposals, and system guidelines. These include the information security management framework *ISO/IEC 27001* [188], the *NIST SP 800-63-3* digital identity management guidelines [25], the *OWASP Authentication Cheat Sheet* with recommendations for secure authentication practices [189], the *FIDO* standards [190], which define protocols for secure and user-friendly authentication, the *ISO/IEC 25010* framework for software quality evaluation [191], and the authentication evaluation criteria proposed by Way et al. [192].

However, we faced challenges in classifying our collected systems according to the required metrics. These standards require precise numerical data, such as error rates which are currently not available to most of the strategies, as well as comprehensive practical details, such as detailed performance evaluations. This gap is due to either undisclosed information from commercial tools or the current premature development stages of the concepts. For instance, although NIST guidelines provide a range of confidence levels for assessing controls related to user accounts, which would be useful for evaluating our strategies, implementing these guidelines is challenging due to the limitations of our current data and the potential inconsistencies in how the strategies are practically applied.

To address this, we reviewed the existing standards and included a number of metrics in a modified version. This new version captures the intended meaning rather than the exact requirements and incorporates additional metrics specific to our adopted definition of holder-binding. Although this approach does not provide precise numerical evaluation, it enables us to estimate the effectiveness of the systems against token-sharing and offers a measure of the grade of assurance regarding the strategies' performance and practicality.

5.2.2 Strength of Binding

This section examines the security of strategies in relation to holder-binding. Under this principle, systems should ensure that only individuals with valid tokens can access resources, and tokens must not be misused or shared. Tokens can be voluntarily shared when the holder intentionally lends them to a trusted party, for various reasons (*see section 1.1.1*). This process requires mutual consent. On the other hand, in insecure systems, tokens can be stolen through attacks or exploited vulnerabilities. Malicious actors may exploit these weaknesses, or individuals might be coerced or deceived into revealing their tokens. These are instances of involuntary token-sharing. While this thesis mainly addresses voluntary token-sharing, we will also examine resistance to involuntary sharing to identify differences and assess their impact on our evaluation results.

5.2.2.1 Protection against Voluntary Sharing

To satisfy this side of holder-binding, a system must restrict individuals from willingly lending their tokens or resources and ensure borrowers cannot authenticate as the original holders. This process must protect against both the potential sharing of tokens by holders, and the risk of borrowers bypassing authentication with the assistance of lenders, thereby gaining access to the account. Achieving this requires addressing various factors and implementing specific measures that differ from those used for protecting against involuntary sharing. We use *four* criteria to assess a system's effectiveness in protecting against voluntary sharing. A system that meets most of these requirements and demonstrates these abilities is considered better protected.

1. **Device Presence**: Adding a device to the authentication process creates a challenge for individuals who wish to share their tokens. Consequently, any system that requires device-based authentication is typically more secure. Compared to text-based credentials, hardware tokens are less convenient for sharing because they can only be used by the person who currently has possession of the device. Additionally, there is a risk that the device could be lost or damaged while in the borrower's possession, which the lender might prefer to avoid. Moreover, individuals who choose to share their tokens may face challenges due to distance, as the borrower could be far away, and they would have to transfer the tokens.

2. **Physical User Presence:** Sharing tokens becomes more challenging and inconvenient when it requires the individual's physical presence to perform an action or complete a task during the authentication process. The likelihood of attempted sharing decreases, especially with long distances involved between the individuals. Attributes related to physiology and individual behavior provide inherently stronger security than other types of tokens, such as text-based ones, which are more susceptible to imitation. For instance, cognitive or Behavioral Biometrics are uniquely secure because they cannot be shared or easily replicated. Additionally, if the user is actively monitored during the authentication process, such as through video surveillance, it becomes more challenging to bypass the security measures, since they are visibly identified and monitored.

3. **Continuous Authentication:** There is a risk that a user might use their tokens and then pass their device or account to someone else while still being logged in. Ideally, we want to prevent users from authenticating themselves and then lending their device or session, by implementing *post-authentication* monitoring. This is more manageable in physical settings. For example, an inspector can ensure that the authenticated individual remains in the room during a university examination and that no one else takes their place. Achieving this level of assurance is more challenging in digital environments. Continuous authentication enhances security by ensuring the user remains authenticated and cannot easily transfer access to another person. Moreover, if holders know that this is the case, they might be less likely to attempt token-sharing.

4. **Risk Increase:** To discourage users from sharing their tokens, systems could implement several measures. This may involve enforcing penalties for those who share their tokens, monitoring and limiting token usage to detect and prevent sharing, and

emphasizing the risk of exposing personal information if tokens are shared. Additionally, sharing tokens could disrupt normal account functionality and continuous access.

	Device Presence	**Physical User Presence**	**Continuous Authentication**	**Risk Increase**	**Total Score**	**Protection Level**
Physiological Biometrics		✓		✓	2	Medium
Behavioral Biometrics		✓			1	Low
Visual Presence Identification		✓			1	Low
Knowledge-based Binding					0	Very Low
Biometric Cryptosystems		✓		✓	2	Medium
Cognitive Biometrics		✓			1	Low
Context-based Binding	✓	✓	✓	✓	4	High
Device-based Binding	✓	✓	✓	✓	4	High
Embedded Valuable Secrets				✓	1	Low
All-or-nothing Disclosure				✓	1	Low
Embedded Tokens in Physical Cards	✓	✓		✓	3	High
Limited Use Control			✓	✓	2	Medium

Table 5.2: Strength of Binding: Voluntary Sharing

Table 5.2 shows which criteria each strategy meets, with an "✓" indicating a criterion is satisfied. Strategies meeting two criteria offer medium protection, those meeting more than two provide high protection, fewer than two provide low protection, and zero offer very low protection.

The method of *Physiological Biometrics* does not fulfil the device presence criterion, as it lacks a hardware token essential for authentication. While a sensor can capture biometric data, it does not involve a physical object that serves as the basis for authentication. Users also do not need to lend their devices to share the authenticator. However, this method does meet the second criterion, requiring the user's active participation and the direct placement of their physiological traits into the sensor. Physical proximity is crucial because physiological tokens cannot be transferred to someone else remotely to bypass the authentication process. However, these tokens can be spoofed in various ways. Therefore, in voluntary scenarios, we must consider the possibility that a borrower might bypass the scan by impersonating the lender. It does not satisfy criteria three, as continuous authentication is not applied. Moreover, the risk of sharing or transferring authentication is considerable, because biometric tokens typically cannot be reused by others once the lender has passed authentication on behalf of the borrower. However, if a borrower successfully spoofs and replicates the lender's biometric data to bypass authentication, they could potentially reuse that biometric information to access other accounts where it is used. Overall, Physiological Biometrics provide only moderate protection against voluntary sharing.

Behavioral Biometrics are evaluated similarly to the previous method. They necessitate explicit user action, as individuals must actively exhibit their unique behavioral traits, which are challenging for others to replicate. Consequently, credentials can only be shared voluntarily if the user is present during the sharing process. However, other criteria are not met, so this method also offers low protection.

Visual Presence Identification also falls short of meeting the first criterion, as it relies on software rather than hardware. It does, however, satisfy the second criterion because it necessitates the user's physical presence and active demonstration of liveness, often with visual monitoring by a live agent. Consequently, if a user were to lend their authentication credentials, they would need to be present during the sharing process. This method does not require continuous authentication and poses minimal risk if credentials are shared. Overall, Visual Presence Identification provides limited protection in terms of voluntary security.

Knowledge-based Binding fails to meet any of the criteria. It relies solely on software, the holder does not need to be physically present, and someone with the knowledge needed can easily authenticate on their behalf. Furthermore, it lacks continuous authentication and does not impose any risk on the lender if they choose to share their credentials. Although the answers and required information change with each instance, preventing reuse to bypass authentication, the overall protection provided is minimal. Consequently, it scores very low in terms of protection.

BCSs also fall short of the first criterion, as they are not hardware-based tokens. They do, however, require active user engagement since they depend on biometric data [1]. The lender must be present to assist the borrower in gaining access. However, BCSs do not offer continuous authentication, but do present some considerable risk to the lender, similar to physiological biometric methods. As a result, BCSs score medium in terms of protection against voluntary sharing.

The next strategy, Cognitive Biometrics, is rated similarly to other biometric methods. It meets only the second criterion by analyzing the user's thoughts and cognitive processes, which are difficult for others to replicate. Since it relies on devices like EEG machines for capturing the data, the lender must be present during the process. Overall, this strategy also provides limited protection.

Context-based Binding does not technically require an additional hardware token for authentication. However, the device used must be registered to the user's account to complete authentication checks, thereby satisfying the first criterion. It also demands active user involvement by monitoring various factors such as device usage, location, and behavior. Additionally, it functions as a token-sharing detection method that supports continuous authentication. There is a risk for the lender who allows someone else to use their account, as they must also provide their registered device. While the lender can use another device concurrently, there is still a risk of the borrower damaging or losing the registered one. By meeting all four criteria, Context-based Binding offers a very high level of protection.

Device-based Binding also adheres to the device presence criterion, which is the primary criterion for evaluation. The lender must share their device for the borrower to complete the authentication process, thus satisfying the first criterion. In many cases, the system monitors device usage, accounting for changes in monitored data sources that

[1] For this evaluation, we assume that BCSs implement physiological characteristics, as most proposals suggest.

may affect access control. While this approach does not exactly represent continuous authentication, like in Context-based Binding, which depends on user-specific behavior, it still tracks post-authentication changes related to the device, network, and other relevant factors. The method also meets the fourth criterion, as sharing tokens requires the registered device. Although the lender can use a different device concurrently, similar to Context-based Binding, all four criteria are met, indicating a high level of protection.

Moving on to the next strategy, Embedding Secrets in Tokens provides a low level of protection. Firstly, it is software-based, so there is no device presence. The user does not need to be present for authentication, as they can simply share their token with someone else, and it does not involve continuous monitoring. However, this approach increases the risk for the lender, as they must disclose a personal secret when sharing their tokens, and the tokens, being text-based, can be easily reused beyond their intended purpose.

Similarly, All-or-nothing Disclosure offers low protection against voluntary sharing. It does not meet the first three criteria for the same reasons previously noted, but it does satisfy the last criterion. Sharing a master account with a borrower provides them with access beyond the intended scope, exposing all associated accounts and personal information. Consequently, the last criterion is notably strong in this context as any information connected to the user's master account could be revealed.

Embedding Tokens in Physical Cards offers protection that depends on the implementation, as this concept can be applied in various ways. However, most implementations involve the use of biometrics, so we evaluate this approach. This method involves a hardware token, meaning the holder must give up their sole token for use, which satisfies the criterion for increased risk with sharing. If the borrower loses or damages the token, the holder will be unable to use it. Additionally, having only one device means the holder cannot use it while the borrower has it, and there is a risk of identity exposure if identity smart cards are involved. Active user engagement is required due to the biometric component. The only downside is the lack of continuous authentication. Overall, this method provides high protection.

Lastly, Limited Use Control of tokens is software-based and does not satisfy the device presence criterion for token-sharing. The user does not need to be present for authentication and can simply share their tokens with the borrower. However, the method does monitor token usage over time, addressing the third criterion. While not precisely continuous authentication, token usage is monitored to ensure that users remain within their intended scope of action. The risk increases when tokens are shared, as the user may exhaust their allowed uses and lose access. Furthermore, the lender has limited control over whether the borrower reuses the tokens, aside from changing or deleting them. As a result, this method offers medium protection against voluntary sharing.

5.2.2.2 Protection Against Involuntary Sharing

To prevent involuntary sharing, a system must guard against coercion, deception, and hacking by addressing common authentication threats and securing user devices. To assess a strategy in this regard, we need to consider the threats to different types of authentication tokens [193]. For *knowledge-based tokens*, threats include disclosing secrets, guessing passcodes, accessing shared tokens, capturing secrets via malware, or conducting offline database attacks. For *possession-based tokens*, threats involve theft, damage, cloning, or interception of the token. For *biometric tokens*, the main threat is replicating biometric data.

We have compiled the following collection of threats, based on the *NIST* Table of Authenticator Threats [193], along with some additions specific to involuntary token-sharing and other types of common attacks [2].

Authentication Threat	**Description**
Assertion Manufacture or Modification	Attacker generates or modifies an assertion [3].
Theft	Attacker steals a physical token.
Duplication	Attacker copies a token with or without the subscriber's knowledge.
Eavesdropping	Attacker sees the secret during authentication or intercepts an out-of-band secret by compromising the communication channel.
Offline Cracking	Attacker uses analytical methods outside the authentication mechanism to expose the token.
Side Channel Attack	Attacker exposes the secret using the physical characteristics of the token.
Phishing or Pharming	Attacker captures the output by fooling the subscriber.
Social Engineering	Attacker convinces the subscriber to reveal their secret or output.
Online Guessing	Attacker connects to the verifier and attempts to guess the output.
Endpoint Compromise	The attacker can use malicious code on the endpoint to proxy remote access to a token without the subscriber's consent, redirect authentication to an unintended verifier, or compromise a multifactor software token.
Unauthorized Binding	Attacker causes a token to be bound to a subscriber's account.
Coercive Authentication	Attacker makes the holder reveal their tokens through coercion or intimidation.
Deceptive Authentication	Attacker exploits the holder to pass authentication without their knowledge or while they are unconscious, using deceptive means to gain unauthorized access.
Other Attacks	An attacker can perform other types of common attacks (Credential stuffing, Replay, MitM, Brute Force, DoS, Session Hijacking, XSS, APTs, SQL injection etc.)

Table 5.3: Threat Landscape

We evaluate the effectiveness of our strategies for preventing involuntary token-sharing using *six* different metrics, in accordance with the authentication threat landscape and the respective *NIST* mitigation strategies. Systems meeting more criteria and exhibiting

[2] These attacks are already part of the threat landscape but are not explicitly listed. For clarity, we have included them as a separate category.

[3] An *Assertion* is defined as a verifiable statement from an *Identity Provider* (IdP) to an RP that contains information about an end user [194]. Assertions may also contain information about the end user's authentication status at the IdP.

relevant capabilities are estimated to offer stronger protection. Note that some significant security measures have been excluded, due to limited or undisclosed information about the strategies. For example, while the implementation of *system and network security controls* is crucial for an authentication system, we lack sufficient information to accurately evaluate these aspects.

1. **Localized Data Management:** Is the strategy dependent on centralized management and secure communications, or is it solely based on the user's individual device? When authentication relies only on the user's device, storage remains localized, reducing the risk of exposure over potentially insecure channels. Physical devices enhance security by being less susceptible to tampering compared to software-only systems, which can be accessed and attacked remotely. Software systems are more vulnerable to hacking, as attackers can manipulate credentials and execute various cyber-attacks. To meet this criterion, a strategy must depend on localized data management for the primary authenticator secret.

2. **Multiple Factors:** When authentication relies on multiple steps and factors it becomes significantly harder to bypass. For example, using both a physical medium *(like a security card)* and inherent factors *(like biometric data)* enhances security by requiring multiple forms of verification. Besides the different types of factors considered, we also account for the number of factors involved. For example, if the strategy examines a wide range of values, it is generally considered more effective. To achieve this, a strategy must employ multiple types of authenticators or assess a wide array of parameters for user profiling.

3. **Continuous Authentication:** Continuously updated authentication checks and context-aware procedures such as behavioral analysis, are crucial for ensuring that authentication steps are not bypassed. Monitoring user behavior for anomalies can help detect compromised tokens or suspicious activities. When a method meets this criterion, it includes some form of user monitoring for the token.

4. **Non-Reliance on Human Factors:** Does the strategy depend on human factors to complete the authentication process? Involving humans can increase the risk of errors. For example, face verification tools can be vulnerable to deception if minor details are not accurately processed. Additionally, using authentication methods that are vulnerable to social engineering risks can expose users to attacks, for instance, those involving customer service agents. A strategy is considered to meet this requirement when it relies on automation rather than the human factor, which could introduce errors or unauthorized access.

5. **Coercion Protection Level:** How easy is it for an individual to coerce someone into completing authentication on their behalf or to share their tokens? This factor is evaluated based on the secret token and how easily it can be forced out. Authentication strategies that rely on biometric factors are generally more resistant to coercion, especially when the biometric factor is not easily cloned. For example, cognitive or behavioral tasks, which often involve multiple tasks, are less susceptible to coercion. These methods are harder to force or steal compared to knowledge-based authentication methods.

6. **Deception Protection Level:** How easy is it to bypass authentication when the user is unconscious or unaware? Methods requiring active consent, such as Behavioral Biometrics, are more resistant to deception because they rely on active engagement from the user. Similarly, authentication methods based on focus or memory, like knowledge-based techniques, tend to be more secure under these conditions. In contrast, Physiological Biometrics, such as fingerprint scanners, can be exploited if the user is unconscious, as these methods do not require the user's active participation. Authentication factors that are easily observable or memorable are generally more vulnerable. This vulnerability is evident in scenarios involving replay attacks, phishing attacks, and other similar threats where the authentication factor can be accessed without the user's direct involvement.

	Localized Data Management	**Multiple Factors**	**Continuous Authentication**	**Non-Reliance on Human Factors**	**Coercion Protection Level**	**Deception Protection Level**	**Total Score**	**Total Protection Level**
Physiological Biometrics				✓	Medium	Low	**0**	**Low**
Behavioral Biometrics				✓	High	High	**3**	**Medium**
Visual Presence Identification		✓			High	High	**3**	**Medium**
Knowledge-based Binding				✓	Low	High	**1**	**Low**
Biometric Cryptosystems	✓			✓	Medium	Low	**1**	**Low**
Cognitive Biometrics				✓	High	High	**3**	**Medium**
Context-based Binding		✓	✓	✓	High	High	**5**	**High**
Device-based Binding			✓	✓	High	High	**4**	**Medium**
Embedded Valuable Secrets				✓	Low	Medium	**0**	**Low**
All-or-nothing Disclosure				✓	Low	Medium	**0**	**Low**
Embedded Tokens in Physical Cards	✓	✓		✓	High	High	**5**	**High**
Limited Use Control			✓	✓	Low	Medium	**1**	**Low**

Table 5.4: Strength of Binding: Involuntary Sharing

Table 5.4 presents our evaluation results. The evaluation process differs slightly from the previous assessment due to variations in information and understanding related to the different strategies. For the first four criteria, any strategy meeting an additional protection requirement (denoted by a ”✓” in the table) receives an extra point in the final protection score. Coercion protection and deception protection levels are rated as low, medium, or high, corresponding to -1, 0, or +1 points, respectively. Strategies with total scores ranging from 0 to 1 are considered to provide low protection against involuntary sharing, while scores below 0, down to -2, indicate very low protection. Scores from 2 to 4 indicate medium protection, while scores between 5 and 6 denote high protection.

The binding strategy of Physiological Biometrics relies on centralized communication, where biometric samples are compared with a database template. This method lacks multiple authentication factors, relying solely on inherent traits, and does not support continuous authentication. Coercion and deception protection are somewhat complex to evaluate: physical proximity is required for biometric capture, which provides some defence. However, coercing someone into a quick biometric verification is relatively easy compared to other methods. Deception protection is weak unless additional measures like liveness detection are used. Without these, users may be tricked into authenticating unintentionally, as seen in cases where individuals unlock devices while the owner is asleep [195], [196]. This method is typically independent of human factors.

Behavioral Biometrics offer stronger coercion protection, as pressuring someone to provide their behavioral data is challenging due to its reliance on psychological and stress factors. Deception protection is also robust, as the individual must be fully aware and conscious to bypass authentication, making it difficult to trick them. This method does not rely on human factors.

Visual Presence Identification yields a medium total score, with dual-factor authentication, combining inherent traits with possession of an identification document for enrollment. It excels in coercion protection because, although someone could be forced to complete the process, it requires physical presence at the time of authentication and relies on environmental monitoring, stress indicators, and recognition algorithms or human verifiers to ensure authenticity. It also performs well in deception protection, as the process is difficult to manipulate and includes liveness detection and video surveillance. The method is challenging to replicate and, with robust liveness detection, is generally resilient against deepfake attacks. However, it generally still relies on human factors for verification.

Knowledge-based Binding offers a low level of security. Once questions are answered, they cannot be reused or exploited, and the system is automated, minimizing reliance on human factors. However, it scores poorly in coercion protection as the required knowledge can be forcibly extracted, and physical proximity is not a factor, making it vulnerable to threats via email or other system attacks. On the other hand, it excels in deception protection, as it is not vulnerable to replay or phishing attacks, based on the very limited timeframe and unique nature of the questions, even though it is technically based on text-based authenticators.

BCSs benefit from strong local device data management, as sensitive biometric data remains on the device and relies on local communication. In terms of coercion protection, BCSs receive a medium score, similar to Physiological Biometrics, and they are denoted with a low score in deception protection, as the biometric data could potentially be vulnerable to manipulation.

Cognitive Biometrics are highly secure and non-observable, making them more resistant to capture and replay attacks, which are more difficult than with other types of biometrics, or text-based methods. They are independent of human factors and score exceptionally well in coercion protection because forcing someone to provide their Cognitive Biometrics is nearly impossible, since it relies on thoughts and stress, requiring device-based capture like EEGs. This means the user must be present with the device, protecting against a few types of attacks. Additionally, Cognitive Biometrics offer excellent deception protection since the user must be highly conscious and aware to pass authentication.

Context-based Binding scores highly due to its use of multiple factors to assess a user profile, surpassing device-based methods in the number of variables considered and providing continuous authentication. As it involves testing various factors rather than relying on static data, it is resistant to eavesdropping and independent of human factors.

In terms of coercion and deception protection, it also performs well. Forcing someone to pass authentication through behavioral means is extremely challenging, and the system is difficult to trick. Device-based Binding receives similar evaluation results. It does not score as high due to its reliance on fewer authentication factors, but it benefits from continuous monitoring and strong resistance to coercion and deception.

The strategy of Embedded Valuable Secrets is rated similarly to All-or-nothing Disclosure. Its key advantage is the complete absence of human factors. It scores very low in coercion protection since it involves sharing text-based content, which is easier to trick someone into sharing through attacks, and also vulnerable to replication and reuse. However, the risk of deception is considered medium because it is more difficult to trick someone who is unconscious or unaware into sharing their text-based authenticators, compared to other types, such as physiological characteristics.

Evaluating Embedded Tokens in Physical Cards can be complex due to the variety of implementation approaches. These systems often use Physiological Biometrics, such as image verification or fingerprint scanners, or integrate biometrics into identity smart cards. Consequently, they involve local device management for authentication and utilize at least two factors: inherent biometrics and hardware, with possible additional text-based authenticators. The secret shared in this method is non-observable due to the use of biometrics and does not rely on human factors. If a smart card is involved, physical verification might be required, although some systems are designed to avoid this. In terms of coercion and deception protection, this approach scores highly. It is challenging to force someone to provide both their card and biometric data, and the vulnerability to deception seen in Physiological Biometrics is mitigated by incorporating a physical medium with locked tokens.

Concerning the Limited Use control strategy, it involves continuous monitoring of the token and the user's behavior throughout the day. It is also independent of human factors. However, since it is essentially based on a text-based token, it is highly vulnerable to coercion and moderately susceptible to deception, such as through phishing attacks.

5.2.2.3 Total Protection Against token-sharing

Finally, we will present the total security findings, combining the results from both voluntary and involuntary token-sharing evaluations. Table 5.5 portrays the outcome.

	Voluntary Sharing	**Involuntary Sharing**	**Total Strength of Binding**
Physiological Biometrics	Score: 2 Protection Level: Medium	Score: 0 Protection Level: Low	Score: **2** Protection Level: **Medium**
Behavioral Biometrics	Score: 1 Protection Level: Low	Score: 3 Protection Level: Medium	Score: **4** Protection Level: **Medium**
Visual Presence Identification	Score: 1 Protection Level: Low	Score: 3 Protection Level: Medium	Score: **4** Protection Level: **Medium**
Knowledge-based Binding	Score: 0 Protection Level: Very Low	Score: 1 Protection Level: Low	Score: **1** Protection Level: **Low**
Biometric Cryptosystems	Score: 2 Protection Level: Medium	Score: 1 Protection Level: Low	Score: **3** Protection Level: **Medium**
Cognitive Biometrics	Score: 1 Protection Level: Low	Score: 3 Protection Level: Medium	Score: **4** Protection Level: **Medium**
Context-based Binding	Score: 4 Protection Level: High	Score: 5 Protection Level: High	Score: **9** Protection Level: **High**
Device-based Binding	Score: 4 Protection Level: High	Score: 4 Protection Level: Medium	Score: **8** Protection Level: **Medium**
Embedded Valuable Secrets	Score: 1 Protection Level: Low	Score: 0 Protection Level: Low	Score: **1** Protection Level: **Low**
All-or-nothing Disclosure	Score: 1 Protection Level: Low	Score: 0 Protection Level: Low	Score: **1** Protection Level: **Low**
Embedded Tokens in Physical Cards	Score: 3 Protection Level: High	Score: 5 Protection Level: High	Score: **8** Protection Level: **High**
Limited Use Control	Score: 2 Protection Level: Medium	Score: 1 Protection Level: Low	Score: **3** Protection Level: **Medium**

Table 5.5: Total Strength of Binding

Ultimately, we combine both scores to determine an overall protection level, which indicates the total effectiveness of the binding mechanism. The protection level is categorized as low, medium, or high. To achieve a high rating, both evaluations must score high; if both scores are low, the protection level is rated as low. In other cases, the protection level is assigned a medium rating.

The only strategies that achieved a high level of protection were Context-based Binding and Embedded Tokens in Physical Cards. Although Device-based Binding also received a high overall score, it was rated as providing medium protection. This indicates that detection methods are highly effective at restricting token-sharing, likely due to their association with continuous authentication, which provides strong security against threats. In contrast, biometric methods received low to medium scores and text-based authentication methods, such as Dynamic KBA, along with All-or-nothing Disclosure, generally offered lower levels of protection.

It is noteworthy that the difference in scores between involuntary and voluntary sharing is relatively minor, with only a one- to two-point variation. This suggests that, despite some differences in metrics, the protection levels between these two types of sharing are not significantly different. Additionally, the evaluation process revealed an interesting notion, showing that certain metrics perform differently depending on the type of sharing. For example, text-based authenticators were found to be a disadvantage in protecting against voluntary sharing, as they could simplify the process, but they provided an advantage in countering deception.

5.2.3 General Assessment

We now move on to the second main type of evaluation. In this section, we will establish several general metrics to assess strategies from a broader perspective beyond just security and binding. This evaluation focuses on overall performance and responsiveness to various criteria, offering a clearer picture of their effectiveness across different implementations. We will first evaluate the system's usability and user experience, focusing on its impact on user authentication. Additionally, we will assess the maturity of the technology being implemented, the projected cost-efficiency of the system, and the privacy measures in place for handling user data during authentication and overall data management.

In this type of evaluation, instead of assigning numerical scores, we categorize each strategy into high, medium, or low levels. This approach helps reduce the risk of errors caused by insufficient data. The overall rating is then determined by the most frequently occurring level among the individual ratings.

5.2.3.1 Usability

This metric assesses the system's impact on user experience during authentication and overall engagement. It considers the following factors:

1. **User Experience:** This metric assesses how the user experience is expected to be influenced by the new binding systems, by examining how easily users can register and authenticate within the new strategies. It evaluates the system's intuitiveness and simplicity, focusing on how much knowledge and information users need to retain. Additionally, providing clear instructions, support, and error protection to help prevent user mistakes contributes positively to the user experience. This metric also considers the level of acceptability we expect from users regarding these systems.

2. **Authentication Speed:** Tracks the time required for registration/authentication and measures whether the response time and throughput meet requirements.

3. **Accessibility:** Evaluates the system's inclusivity for all individuals, including those with physical limitations. It examines how accessible the system is to users from diverse backgrounds, including various ages, cultures, ethnicities, abilities, genders, economic situations, and languages.

	User Experience	**Authentication Speed**	**Accessibility**	**Usability Level**
Physiological Biometrics	Medium	Medium	Low	Medium
Behavioral Biometrics	Medium	Low	Medium	Medium
Visual Presence Identification	Medium	Low	Medium	Medium
Knowledge-based Binding	Low	Low	Low	Low
Biometric Cryptosystems	Medium	Medium	Low	Medium
Cognitive Biometrics	Low	Low	Low	Low
Context-based Binding	Low	High	High	High
Device-based Binding	Medium	High	High	High
Embedded Valuable Secrets	Low	High	High	High
All-or-nothing Disclosure	Medium	High	High	High
Embedded Tokens in Physical Cards	Medium	Medium	Medium	Medium
Limited Use Control	Low	High	High	High

Table 5.6: Usability Assessment

Table 5.6 summarizes our evaluation of strategies based on their usability. Physiological Biometrics and BCSs received a medium score for user experience. This is because both can be intrusive, requiring a physiological test that users often resist, making them uncomfortable. In general, Physiological Biometrics have encountered considerable public resistance, largely attributable to cultural or religious reasons [197]. There have been many instances of protests or campaigns against biometric surveillance systems [198], [199]. However, as these systems continue to evolve and become more widely used, it is anticipated that users will gradually become more familiar with them. Additionally, the environmental sensitivity of sensors may pose challenges in usability. On the plus side, users do not need to recall passwords or credentials, and the system requires minimal user input, as measurements are taken passively and without the need for specific instructions. In terms of authentication speed, while sensor issues might cause delays, enrollment and authentication times are generally acceptable compared to other biometrics, though still slower than some other authentication methods. Consequently, they also received a medium speed score. Accessibility is a concern, as Physiological Biometrics can be problematic for people with disabilities, impairments, or older age groups due to its intrusive nature. Overall, these systems received a medium usability score.

Behavioral Biometrics are software-based and generally easy to use, as they do not require the user to be examined on physiology[4] or interact with physical devices, which often encounter resistance. However, they can be complex and demanding at times, requiring specific instructions that might become annoying. Despite this, they offer convenience since users typically do not need to remember specific tokens, earning a medium score for user experience. In terms of authentication speed, Behavioral Biometrics are slower compared to other biometric methods. Users may need to repeat actions and go

[4] We refer to the most common types of software-based Behavioral Biometrics. More complex types, such as gait analysis, require separate consideration due to their complexity and are not grouped with the simpler methods.

through the process multiple times to ensure system recognition. The system often analyzes multiple interactions, such as typing patterns and mouse movements, which can further slow down the process. Enrollment is also lengthy, so we assign a low score for authentication speed. In terms of accessibility, Behavioral Biometrics receive a medium score. While some users, such as those with hand impairments, might still face challenges with typing style authentication, these methods are generally more accessible compared to other biometric options.

Visual Presence Identification scored moderately in user experience. It offers good error correction, with continuous instructions and error messages, but is intrusive due to video surveillance, and relies on environmental and user conditions. The lengthy setup and verification process is annoying, but users benefit from not needing to remember tokens or perform complex actions. For authentication speed, it received a negative score because it requires the longest enrollment time among biometrics due to personal data verification, potentially taking days to approve. The process can be slow, especially with human verification and adjusting lighting or environmental conditions. In terms of accessibility, Behavioral Biometrics might pose challenges for individuals with visual impairments, but they remain more accessible than other biometric methods.

Dynamic KBA received negative scores in all usability metrics. The system is complex and time-consuming, which can be frustrating, especially if more specific and complex questions are added. Users may find it troublesome to recall and verify personal information, leading to potential errors and lockouts. The 1-2 minute authentication timeframe can feel too long, and add stress, particularly for users with memory recall issues. Additionally, its accessibility across different languages and countries is uncertain, which may complicate the processing of attaining the records of all individuals.

Cognitive Biometrics also face several challenges and negative aspects. First, they are difficult to use due to their complexity, requiring specific instructions and user training that many people might find irritating. Additionally, they often require devices like EEGs, which can be uncomfortable for users, and the idea of sharing thoughts and mental processes may feel intrusive. The main advantage of Cognitive Biometrics, like other biometric systems, is that users do not need to remember passwords. However, the authentication process can be slow and time-consuming. Users might need to perform numerous tasks, and the accuracy of authentication depends heavily on the devices used to capture the data, resulting in long enrollment times. Furthermore, Cognitive Biometrics are not accessible to individuals with cognitive impairments, such as those with dementia or Alzheimer's disease.

Context-based authentication has some drawbacks regarding user experience. It considers more factors than device-based authentication, which can feel intrusive to users. Additionally, it may seem limiting when users want to change devices or locations, as this can lead to access issues. On the positive side, context-based authentication operates in the background, so users do not need to take any active steps. It is generally fast and not slowed down by the background processes. This method is also accessible to all individuals.

Device-based authentication is user-friendly and operates seamlessly in the background, relying on fewer contextual factors than context-based authentication. However, it restricts users to their registered devices, which can be frustrating. Despite this limitation, it is a fast and accessible authentication method for everyone.

Embedded secrets is not considered very user-friendly, as holders are generally reluctant to share their secrets and may not value the added security of not sharing tokens. This approach feels intrusive and burdens users with the responsibility of remembering text-based tokens. However, it does offer fast authentication and remains accessible to everyone, as the authentication process remains consistent.

All-or-nothing Disclosure can feel intrusive because users have the added responsibility of protecting master accounts. However, it is rated as medium in user experience because users no longer need to remember separate account tokens or passwords, reducing time and complexity. This method offers fast authentication, is accessible to all, and has a generally high usability level.

Using Embedded Tokens in Physical Cards has a medium rating across all protection aspects, since certain aspects could vary based on the implementation. Users must safeguard the physical token, which can be burdensome, and it is typically restricted to use by one person at a time. Additionally, concerns about the intrusiveness of biometrics still apply. Authentication speed also receives a medium rating, as it depends on factors such as the sensor quality and the verification method. Accessibility varies with the type of biometric technology used.

Limiting the use of tokens negatively impacts user experience, as it adds the burden of managing biometrics and can feel like constant monitoring. Users might worry about running out of tokens. The change in the authentication process also does not remove the need to remember text-based tokens and increases the risk of losing access. Despite these concerns, it is a fast and accessible strategy, contributing to a high overall usability level.

5.2.3.2 Maturity

This metric is inspired by the Technology Readiness (TRL) scale, which ranges from 1 to 9 and measures the progress or maturity level of a technology. This scale was originally developed by NASA [200] and has since been adapted and used by various organizations, including the European Union [201]. We have adapted the EU-modified scale to create our own metric, as it is more applicable to general technology systems. However, instead of using the full 1-9 scale, we have opted for a simplified low-medium-high classification. This approach allows for easier comparison with other metrics in our general assessment and provides a general idea of maturity rather than a highly specific measurement. In the future, as error rates and performance projections become available for all systems, we will be able to assess technology readiness with greater accuracy for binding strategies.

Our scores for the maturity assessment of the binding strategies are as follows

1. **Low:** In such a system, the basic principles of authentication are being observed and formulated. The research and experimentation are still in the early stages, and the development is at a very preliminary level.

2. **Medium:** For such binding systems, there are more research efforts and proposals than the previous score. The technology has been proposed with detailed implementation plans for demonstrating its effectiveness under real-life conditions.

3. **High:** Fully developed and proven binding system. It should be complete, qualified, and operational in its intended environment (including competitive manufacturing).

	Maturity Level
Physiological Biometrics	High
Behavioral Biometrics	High
Visual Presence Identification	High
Knowledge-based Binding	High
Biometric Cryptosystems	Medium
Cognitive Biometrics	Low
Context-based Binding	High
Device-based Binding	High
Embedded Valuable Secrets	Low
All-or-nothing Disclosure	Low
Embedded Tokens in Physical Cards	Medium
Limited Use Control	Low

Table 5.7: Maturity Assessment

Table 5.7 presents our results. We assigned a high rating to Physiological Biometrics due to its extensive research and development. This field benefits from a diverse array of metrics and error rates, with many systems demonstrating impressive performance. The technology is fully developed, well-established, and operational. Similarly, we awarded a high score to Behavioral Biometrics, despite their less widespread adoption compared to Physiological Biometrics. The impressive results demonstrated by various systems validate this high rating. Visual Presence Identification also received a high score due to its extensive exploration during the COVID-19 pandemic. Increased research and advancements in algorithms, along with improved efficiency, have contributed to this positive evaluation and the method's growing effectiveness. Similarly, Context-based, Device-based, and Knowledge-based Bindings are employed in competitive manufacturing environments and have been thoroughly tested, though they are primarily used as secondary authentication factors.

On the other hand, Biometric Cryptosystems and Embedded Tokens in Physical Cards can be assigned a Medium Maturity Score. While there is substantial research and numerous proposals on their potential applications for widespread authentication in real-life conditions, practical implementations and testing are still lacking.

Lastly, we assigned a low maturity level score to Cognitive Biometrics, Embedded Valuable Secrets, All-or-nothing Disclosure, and Limited Use Control. Although there is some research on these concepts, detailed information about actual systems is sparse. Most of what we have are theoretical frameworks and ideas with few practical implementations or offerings.

5.2.3.3 Cost Efficiency

This metric assesses the financial and operational impact of transitioning to the new authentication systems. Due to the lack of specific information about the systems and their associated financial and operational impact, we can only provide a general estimate of the complexity and financial burden. Consequently, we do not break this metric down into more specific factors but instead focus on key questions that may arise. What is the financial impact of the new system? This includes expenses related to new devices and hardware, as well as modifications to existing infrastructure. Are there significant operational costs, such as the need for human oversight in verification processes and ongoing support, that might hinder deployment and scalability to a bigger degree? Are updates and repairs to the hardware required?

	Cost Efficiency Level
Physiological Biometrics	Medium
Behavioral Biometrics	High
Visual Presence Identification	Low
Knowledge-based Binding	High
Biometric Cryptosystems	Medium
Cognitive Biometrics	Low
Context-based Binding	High
Device-based Binding	High
Embedded Valuable Secrets	High
All-or-nothing Disclosure	High
Embedded Tokens in Physical Cards	Low
Limited Use Control	High

Table 5.8: Cost Efficiency Assessment

Regarding the cost and potential for widespread deployment of each strategy, we assessed the methods in Table 5.8 as follows.

Physiological Biometrics received a medium rating. Although these systems depend on external sensors and devices, which have become relatively affordable, they still require maintenance and initial setup. Many users already have the necessary devices, such as cameras, which helps reduce costs as the system scales. However, the need for device upkeep and initial setup contributes to the medium cost rating. Behavioral Biometrics, on the other hand, are software-based and do not need additional hardware beyond what is commonly available among users, making them cost-effective. Since no extra devices or human operators are required, they are rated with a high score. Visual Presence Identification benefits from the existing cameras in devices, so there is no additional hardware cost. However, scaling this approach can be challenging due to its reliance on human operators for authentication verification or enrollment, complicating large-scale implementation. This may improve as automation technology advances. BCSs have device requirements similar to those of the Physiological Biometrics they measure and do not need human operators. As a result, they are expected to have a moderate cost. Cognitive Biometrics demand specialized and expensive tracking equipment, making them costly and difficult to scale globally. The high cost is also due to the intensive maintenance required for these devices. Embedding tokens in physical cards involves additional hardware tokens and the associated development costs, making this strategy relatively expensive. For the remaining strategies, which do not require specific devices or operators, the cost is very low.

5.2.3.4 Privacy

This metric is intended to evaluate the systems based on their data handling practices. Our research focuses on holder-binding methods that create precise user profiles for accurate recognition. These methods are generally more invasive than traditional text-based systems like passwords. However, we can still define requirements and criteria to evaluate the data handling processes and potential risks associated with these mechanisms. Key factors to consider include:

1. **User Control:** Does the user have control over their personal data and authentication tokens, or are these managed solely by the system?

2. **Data Scope and Impact:** This criterion assesses the quantity and variety of data collected for user profiling, including the range of personal aspects covered and the nature of the data (e.g., physiological characteristics, which might make users uncomfortable). It also evaluates the potential intrusiveness users might feel regarding their privacy and how their data is handled. For instance, it considers whether verification is conducted by humans or Artificial intelligence (AI). Unlike human verifiers, who may forget details after verification, AI systems can retain and record user interactions indefinitely, potentially impacting privacy. Additionally, the assessment considers whether the method might intrude on the user's personal space, such as through video monitoring.

3. **Localized Data Management:** As in section 5.2.2.2 (*Protection Against Involuntary Sharing*), we take into account whether the data leaves the device for central processing or if it remains stored locally, which can offer enhanced privacy protection. Although we reuse the scores from this section, the focus shifts from defending against attacks to safeguarding users by protecting the exposure of their personal authentication data.

	User Control	Data Scope and Impact	Localized Data Management	Privacy Level
Physiological Biometrics	Low	Low	Low	Low
Behavioral Biometrics	Low	Medium	Low	Low
Visual Presence Identification	Low	Low	Low	Low
Knowledge-based Binding	Low	Medium	Low	Low
Biometric Cryptosystems	Low	Medium	High	Medium
Cognitive Biometrics	Medium	Low	Low	Low
Context-based Binding	Low	Low	Low	Low
Device-based Binding	Low	Low	Low	Low
Embedded Valuable Secrets	Medium	Medium	Low	Medium
All-or-nothing Disclosure	High	Medium	Low	Medium
Embedded Tokens in Physical Cards	Medium	Low	High	Medium
Limited Use Control	Medium	Medium	Low	Medium

Table 5.9: Privacy Assessment

Table 5.9 outlines our privacy assessment findings. A high privacy score is granted when users have significant control over their data, including modification and deletion options. Systems with minimal user/token monitoring, management of a smaller volume of personal data, and on-device processing also score higher, as these factors enhance privacy protection.

Physiological Biometrics score poorly on user control because individuals cannot modify, delete, or manage their biometric data, which is a common issue across many biometric types. While verifying physiological characteristics is less intrusive than other methods, the data handled are very sensitive due to its personal and permanent nature, which raises significant privacy concerns. Additionally, because this data leaves the device and is stored in a database, it receives a low score for data management.

Behavioral Biometrics share the same rating as Physiological Biometrics in terms of user control and data management. However, they are generally considered less intrusive because they primarily involve pattern matching rather than direct physiological analysis, and the data involved is typically regarded as less privacy-sensitive than physiological data. Nonetheless, behavioral analysis is less explored ethically and could present potential risks. Overall, this approach receives a low privacy score.

Visual Presence Identification receives a poor privacy protection score. Users have minimal control over their data, as it involves both Physiological Biometrics and additional identification methods. the intervention is highly intrusive, with AI algorithms analyzing and recognizing individuals' presence and liveness, which can be unsettling. Furthermore, the data involved is highly sensitive, unique, and permanent.

Knowledge-based Binding receives a low privacy score. Users lack control over how their personal data from records is used and cannot opt out if it is a required authentication factor. However, it scores medium on data scope and impact because, although it does not involve real-time monitoring or personal space surveillance, it may still cause discomfort among users when asked to provide access to their personal records and information.

BCSs receive a medium privacy score. Users have very limited control over their data, which involves handling highly sensitive biometric information. However, it is important to highlight that communication is local and device-based, meaning the data does not leave the device. This localized processing results in less monitoring and may feel less intrusive to users.

Cognitive Biometrics receive a low privacy score. Like other biometric data, Cognitive Biometrics cannot be modified, but they are cancellable, which addresses some concerns associated with other types of biometrics. Consequently, they receive a medium score for user control. This method might also feel invasive to the holder, as it involves pattern matching based on past thoughts and actions. Additionally, the data handled are of very sensitive nature. The exploration of cognitive data delves into personal thoughts for user profiling, a new and potentially more invasive approach than physiological data sharing.

Context-based Binding receives a very low privacy rating, as all its metrics score poorly. Users have no control over the data being shared about them or the timing of the monitoring. The intervention is automated, but it still involves extensive user profiling, which raises concerns. While the data may seem less sensitive because it is not inherent to the user, the large volume of data collected is significantly greater compared to other methods, such as Device-based Binding. Device-based Binding also receives a negative privacy rating. Although the data is considered less sensitive compared to Context-based Binding due to fewer factors being involved, this does not fully mitigate privacy concerns. The reduced scope of data collection does make it somewhat less intrusive for the user, but it still falls short in terms of overall privacy protection.

Embedded secrets in tokens receive mixed privacy scores. User control is rated as medium because, while the holder cannot choose the secret being shared (which can feel intrusive), they do retain possession of and the ability to modify the original authentication token. Considering the scope of the data and its impact, it scores medium. On one hand, there is no ongoing monitoring of the token, nor is it personalized or tracked. On the other hand, the nature of the data handled might still be unsettling to the user. Although involving a personal secret, it is less sensitive than physiological or inherent data. Despite this, it remains very personal and users might be reluctant to share it.

All-or-nothing Disclosure receives one positive privacy score. User control is rated highly because users have complete control over their master account, and no additional exposure is introduced. However, considering the second criterion, even though the process is not fully monitored, the exposure of data could still have a potentially harmful impact on the user. If information is compromised, it could potentially expose a vast amount of user data across multiple accounts, making it significantly more risky than similar tactics.

Embedded Tokens in Physical Cards yields varying privacy scores depending on the implementation. If biometrics are involved, user control is minimal. Considering the data scope and impact, it remains concerning, similar to Physiological Biometrics. Data sensitivity is very high due to the integration of biometrics with personal identification tokens, resulting in a low score in the second criterion. Data processing is centralized, which positively impacts the score. Overall, this leads to a medium privacy level rating.

The last proposed strategy, Limited Use Control, receives a medium privacy score. Users retain significant control over the data they share, and no additional tokens are introduced. However, there is full monitoring of the use, which users may not control or be informed about. The process involves automated management and monitoring of tokens, which could potentially lead to user profiling but is less intrusive than other methods. The data involved is not personal or highly sensitive, contributing to the medium privacy rating.

5.2.3.5 Outcome

Finally, we present the general evaluation findings by combining the results from the four main metrics: *usability, maturity, cost efficiency, and privacy.*

	Usability	**Maturity**	**Cost Efficiency**	**Privacy**
Physiological Biometrics	Medium	High	Medium	Low
Behavioral Biometrics	Medium	High	High	Low
Visual Presence Identification	Medium	High	Low	Low
Knowledge-based Binding	Low	High	High	Low
Biometric Cryptosystems	Medium	Medium	Medium	Medium
Cognitive Biometrics	Low	Low	Low	Low
Context-based Binding	High	High	High	Low
Device-based Binding	High	High	High	Low
Embedded Valuable Secrets	High	Low	High	Medium
All-or-nothing Disclosure	High	Low	High	Medium
Embedded Tokens in Physical Cards	Medium	Medium	Low	Medium
Limited Use Control	High	Low	High	Medium

Table 5.10: General Assessment

The findings suggest that most strategies performed well in terms of usability and user experience. However, the maturity scores varied across different metrics. Similarly, cost efficiency ratings showed a range of outcomes. Privacy evaluations were generally in the low to medium range, with no strategy achieving a high rating. This was expected, as holder-binding authentication is inherently more intrusive than traditional methods.

For this section, we do not provide a total score, as the importance of various factors and metrics can vary depending on stakeholder priorities. Since different parties may prioritize aspects like cost or performance differently, it is not possible to assign a definitive score that would be meaningful to everyone.

Chapter 6

Ethical Implications

In the previous chapters, we examined various types of binding strategies, aiming to build a collection of methods to restrict token-sharing. Our exploration included an examination of established mechanisms designed to bind tokens to natural persons, as well as proposed research on the broader conceptual framework. We then evaluated these strategies to determine which framework offers the most effective holder-binding across different scenarios.

Given the existing strong strategies against token-sharing, it is reasonable to assume that these measures will likely become even more advanced. As digital identity processes evolve rapidly and the adoption of digital identity wallets becomes more prevalent, it is reasonable to expect that future developments will emphasize the principle of strong binding. In such a scenario, we might envision a digital ecosystem where authentication systems are predominantly bound to the user. This evolution would entail that every text-based token, password, cryptographic key, and digital asset would be uniquely and specifically tailored to each individual, making the act of sharing tokens virtually impossible without significant consequences, even in more personal contexts, such as between family members. If these advancements come into practice, they would lead the way for a more secure identity landscape, eliminating the risks associated with token-sharing for both business and personal use, as discussed in *section 1.1.3* of this thesis.

However, as with many advancements in the digital age, particularly those involving sensitive data, it is essential to acknowledge that this increased level of personalized security may come at a certain ethical cost. It is crucial to explore these concerns and understand the broader impact on individuals. In this chapter, we will explore the potential ethical issues associated with strong holder-binding methods, by examining the various concerns and questions that arise throughout their development.

6.1 The Principle of Trust

Could personal connections be undermined, if individuals are prohibited from sharing their tokens?

The principle of trust is fundamental to human development. While there is no universally accepted scholarly definition of trust, it could be described as *"a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another"* [202]. This definition highlights that trust is crucial to human interactions, playing an important role in individual well-being and interpersonal dynamics. Trustworthy individuals are characterized by their consistency, honesty, and ability to foster security and emotional support in their relationships [203]. Trust is fundamentally rooted in human relationships, as it is not merely an individual trait but is shaped by the mutual feelings and interactions between people.

As we fully transition into the digital landscape, it is only natural that the concept of trust has also shifted into this space. In such discussions, digital trust is frequently explored through the lens of both user reliance on secure systems and the expectations SPs should have for trustworthy environments in interactions and communications. However, the value of interpersonal digital identities is less commonly addressed. Current token policies tend to emphasize a lack of trust by discouraging individuals from sharing their passwords, highlighting the negative consequences of such actions, even among family members and partners. Businesses frequently implement campaigns to prevent employees from sharing their credentials. The methods we have studied are designed to eliminate trust altogether, focusing not just on encouraging distrust, but on making it a mandatory practice.

This shift raises significant concerns about its potential impact on relationships. Individuals are now instructed to adopt a stance of mistrust even towards those they rely on the most, which could affect trust in both personal and professional contexts. This situation prompts questions about whether such practices might contribute to a broader trend of increasing distrust in digital interactions. As more aspects of life become digital, *will the fundamental principle of trust be undermined in online relationships?*

Security measures and enforced policies can have unintended consequences on personal relationships. When an individual is unwilling to share passwords, it may be perceived as a lack of trust or transparency. This perception can lead to misunderstandings, feelings of alienation, and conflict. Poor communication resulting from digital restrictions might undermine trust in others and create barriers in personal relationships. These are critical issues to explore, as they touch upon the balance between security and trust in the digital world.

Does binding holders to their tokens undermine their trust in the system?

In traditional authentication landscapes, individuals generally have digital autonomy through their account tokens, which they use to conduct transactions, verify ownership, and access services. They are expected to register and manage their tokens independently, whether by using a password manager, writing them down on notes, or even sharing them verbally with someone else so they remember them. The system imposes no restrictions on token handling, placing full responsibility for protection and maintenance on the holder.

Of course, this approach has proven to be flawed. Human errors can lead to unintended consequences, compromising system integrity and endangering other system users' identities. Many examples in this paper illustrate this point, the sharing of tokens or the failure to protect them can endanger the system, the company or service, and the individual.

However, as holders become legally bound to their tokens, a shift is underway. There might be a loss of trust in the system, and holders might feel that the once-granted digital freedom is now constrained. Initially offering holders control over their tokens, selective attribute disclosure, and anonymity, the system now feels restrictive: specifying how tokens are to be used, prohibiting sharing, and limiting user autonomy due to centralized management and monitoring, especially through disincentivizing binding methods.

This shift towards binding holders introduces a new dynamic in the relationship between users and the system. No longer are individuals solely responsible for safeguarding their tokens, but they are now subject to the dictates of the system, which imposes restrictions on their usage. This change can feel less empowering, as individuals may feel that their autonomy is being threatened. Additionally, holder-binding raises other trust issues. *Do holders even trust the system to safeguard their tokens and manage them responsibly?* Conversely, *does the system trust holders to adhere to usage guidelines?* This delicate balance of trust is crucial, and mishandling it can undermine the effectiveness of strong holder-binding methods.

6.2 Privacy and Anonymity

Could holder-binding be misused for major surveillance?

It is almost certain that, without standardized rules and proper guidelines, the principle of holder-binding could lead to significant issues, particularly concerning user surveillance. If tokens are bound to the extent that they can accurately identify individuals and prevent sharing, several concerns arise.

One major issue is constant monitoring. The identification mechanisms for user binding, intended to prevent misuse, are often based on monitoring user movements and detecting patterns. This continuous surveillance can be perceived as an invasion of privacy, making users uncomfortable with the knowledge that their every action is being tracked. Every move they make is analyzed and recorded, which can be both unsafe and uncomfortable for users. They are not only identified but also have their behaviors, activities, and preferences documented in detail. This information can be used for non-consensual targeted marketing and other forms of digital exploitation.

Additionally, this is one of the first times we will be able to know individuals and have their complete identity in digital form. When text-based methods are used for authentication, a few details could be revealed about an individual, such as their account activity, but not a deeper level of user profiling, such as distinguishing between users who use identical devices or recording their thoughts. In extreme cases, this could lead to a surveillance state where individuals are monitored and controlled by governments or corporations. We have already seen scenarios where such practices have proven dangerous for users [204], or read such scenarios in Orwellian literature [205]. Governments might use this information for surveillance purposes, monitoring political activities and potentially violating user privacy. Corporations could exploit the data for profit, manipulating user

choices and pushing products and services in ways that maximize profit at the expense of user autonomy.
Another aspect briefly mentioned in the previous chapter (*section 5.2.3.4)* is the invasion of personal space. New binding methods often require some form of verification of user recorded footage. For instance, there may be monitoring of the person during the verification process, tracking of their actions, or even monitoring of their surroundings, such as their location. This level of surveillance can definitely feel like an invasion of personal space to users, especially given the heavy implementation of AI technologies in these processes. In physical scenarios, even when authentication involved similar actions, such as verifying a passport picture at an airport, there was an understanding that the human agent performing the check was unlikely to remember and later recall the person's face. It is nearly impossible for the human brain to recognize a person, remember their identity, and consistently match it to their face with great accuracy, especially given the volume of performed checks a typical agent has to perform. With AI, however, there is potential for ongoing recognition and data retention, which raises additional privacy concerns. This technology has the capacity to accomplish this, as well as to analyze a user's personal space, surroundings, location, and more. The extent of its capabilities and potential for misuse in surveillance may be beyond our current comprehension.

Does incorporating identity factors such as behavioral patterns, user engagement, and psychological traits in binding strategies compromise user privacy?

The strategies related to holder-binding suggest that for the first time in authentication schemes, individuals' behavior is being monitored on such a large scale. This monitoring includes their interactions with devices, behaviors, and even thoughts, which raises several privacy considerations. One major concern is the handling of sensitive data. Profiling holder behavior can reveal highly personal information, such as health conditions, habits, and emotional states, which individuals may prefer to keep private. As these authentication systems become more widespread, users might find it difficult to opt out, even if they feel that sharing such data intrudes on their personal identity. Additionally, the complexity of the information collected requires users to fully understand what data is being gathered, how it will be used, and the potential risks involved, adding layers of complexity to the user experience. This constant monitoring can also induce stress and anxiety, as individuals may fear judgment or evaluation based on their monitored behavior, affecting both their mental health and the effectiveness of the authentication process. Furthermore, this detailed monitoring might lead users to alter their behavior, self-censoring or modifying actions to meet perceived expectations, which could compromise both the authenticity of their behavior and their personal freedom in digital environments.

Does binding go against the idea of digital anonymity?

We could argue that linking tokens to the behavior or usage patterns of their holders can make these tokens identifiable, even if they were initially anonymous. Binding tokens to holders in a non-transferable manner may indeed undermine the concept of anonymous credentials, which are intended to allow users to prove certain attributes or rights without revealing their identity. When tokens are tied to specific users and their actions are monitored, a traceable log of their activities or behaviors can be created. Although principles like conditional anonymity can be employed to manage digital anonymous credentials, our focus lies on the notion that the system will gain a much deeper understanding of its users compared to previous methods. Even if the data is anonymized at first, it can often be re-identified by correlating it with other data sources. For example, if a system closely monitors how a user interacts with its platform, it can likely identify an anonymous account by matching it to the behavior of a known user. This is further reinforced by the creation of holder profiles that can accurately identify and track users, such as through Behavioral Biometrics and continuous authentication, potentially contradicting the principle of digital anonymity.

6.3 User Experience and System Control

Is it ethical for system providers to make the authentication process more challenging or risky to deter users from sharing tokens, and do they have the right to significantly influence the user experience in such way?

The strategies collected in this thesis that aim to disincentivize token-sharing by complicating or increasing the risk of the authentication process, such as All-or-nothing Disclosure, raise ethical concerns. *Is it justified to increase the cost or risk for users to deter token-sharing, even if it ultimately benefits and protects them?*

On the one hand, preventing token-sharing enhances security and safeguards system integrity and data. It also ensures fair access to services and resources, as sharing tokens can lead to unauthorized access and misuse. On the other hand, increasing the complexity or risk of the authentication process raises concerns about user autonomy and fairness. Users may feel pressured into compliance due to the heightened difficulty or risk, which could lower trust in the system and reduce their willingness to participate. Moreover, this could be the first instance where systems are negatively impacted specifically based on the way tokens are used, and this might change the dynamics of the user experience.

Can there be legitimate reasons for individuals to share tokens, and could binding strategies have negative effects in these scenarios?

When examining the reasons behind token-sharing *(Section 1.1.1)*, it becomes evident that some motivations are significant and cannot be easily dismissed. It can be argued that individuals may share tokens out of necessity or due to the negative consequences of not doing so. While motivations such as peer pressure, cost-saving on streaming services, or personal relationships may seem minor, other reasons can have a crucial impact on people's lives. For instance, users may share tokens to prevent being locked out or losing access in emergency situations, or for community support reasons. Imagine a scenario where a doctor needs urgent access to a hospital but is unable to enter because their colleague, who has the necessary tokens, is occupied. Consider an elderly person unable to provide access to their son to coordinate an emergency call, potentially resulting in an accident. Parents often share access to educational platforms or location-tracking apps with teachers or caregivers to ensure their child's safety, which can be crucial if the child goes missing. Additionally, individuals with disabilities often rely on others to assist them with electronic devices and access codes to navigate essential services. Restricting token-sharing could severely impact their ability to receive necessary support and care.

It is clear that not all aspects of token-sharing are negative, and some scenarios are critical for ensuring safety and well-being. Developing systems that accommodate these needs without excluding or disadvantaging specific user groups is essential. Failing to do so could lead to severe consequences that extend beyond what is initially expected.

Chapter 7

Conclusion

Through this thesis, we addressed the challenge of verifying that a natural person using a token is indeed the individual to whom it was originally issued. Digital authentication systems often lack the certainty of identity verification provided by their physical counterparts, primarily due to the widespread issue of token-sharing in the digital environment. This practice, driven by various motivations, undermines both the lenders and borrowers, as well as the overall functionality of the system.

To counter this, we introduced the principle of *Non-Transferability* for authentication tokens, aiming to ensure that these tokens remain exclusively with their intended recipients. We proposed holder-binding as a method to achieve this, linking tokens and/or credentials to natural persons, ensuring that they can only be used by the individual to whom they were issued and cannot be transferred to others. We investigated the efficacy of holder-binding in preventing the sharing of authentication tokens.

Our analysis covered six commercial mechanisms and six research concepts that support holder-binding, which we categorized based on their objectives: *disincentivizing, preventing*, or *detecting* token sharing. These systems enhance the effectiveness of digital authentication by ensuring more secure token handling and greater resistance to misuse.

7.1 Key Findings

In chapter 5, we evaluated the binding strategies presented throughout this thesis. We initially focused on holder-binding factors, particularly regarding the security of systems against both voluntary and involuntary token sharing. Additionally, we conducted a broader evaluation concerning the practical implementation of the strategies. Table 7.1 presents our collective findings.

	Usability	**Maturity**	**Cost Efficiency**	**Privacy**	**Voluntary Sharing Protection**	**Involuntary Sharing Protection**
Physiological Biometrics	Medium	High	Medium	Low	Medium	Low
Behavioral Biometrics	Medium	High	High	Low	Low	Medium
Visual Presence Identification	Medium	High	Low	Low	Low	Medium
Knowledge-based Binding	Low	High	High	Low	Very Low	Low
Biometric Cryptosystems	Medium	Medium	Medium	Medium	Medium	Low
Cognitive Biometrics	Low	Low	Low	Low	Low	Medium
Context-based Binding	High	High	High	Low	High	High
Device-based Binding	High	High	High	Low	High	Medium
Embedded Valuable Secrets	High	Low	High	Medium	Low	Low
All-or-nothing Disclosure	High	Low	High	Medium	Low	Low
Embedded Tokens in Physical Cards	Medium	Medium	Low	Medium	High	High
Limited Use Control	High	Low	High	Medium	Medium	Low

Table 7.1: Combined Ratings

As mentioned in *Section 5.2.3.5*, which presents the results of the general assessment, we believe that providing a baseline score is not appropriate for this type of analysis. This is because we cannot be completely certain of the evaluation, given the data limitations due to undisclosed information or the current development stage of the different strategies. Additionally, the priorities and the weights assigned to each metric in determining the final score for selecting a system for authentication would vary depending on the stakeholder (e.g., user, system provider, service provider). However, we believe the results can still be valuable in this process. Depending on the specific priorities and requirements of each stakeholder, they can contribute to the selection of a secure, practical system that is more advanced in restricting token-sharing.

However, it would be valuable to explore whether there is a trade-off between security and the overall practicality of the binding strategies, a frequent challenge in more secure systems.

	General	**Binding**
Physiological Biometrics	Medium	Medium
Behavioral Biometrics	Medium	Medium
Visual Presence Identification	Medium	Medium
Knowledge-based Binding	Medium	Low
Biometric Cryptosystems	Medium	Medium
Cognitive Biometrics	Low	Medium
Context-based Binding	High	High
Device-based Binding	High	Medium
Embedded Valuable Secrets	Medium	Low
All-or-nothing Disclosure	Medium	Low
Embedded Tokens in Physical Cards	Medium	High
Limited Use Control	Medium	Medium

Table 7.2: Practicality-Security Tradeoff

Table 7.2 showcases the comparison of general assessment ratings relative to the strength of binding for the binding strategies. The findings reveal that, to varying extents, there is a trade-off between token-sharing protection and practicality. While only Context-based Binding excels in both areas simultaneously, all methods vary by at most one score grade, such as from low to medium or medium to high. Notably, during the evaluation, we realized that different metrics can have both positive and negative tradeoffs for the two types. For example, while device requirements enhance protection against voluntary sharing, they negatively impact cost efficiency. Physiological and Behavioral Biometrics, as well as BCSs offer moderate practicality and security. Visual Presence Identification also gets a medium rating in both categories. Knowledge-based Binding is moderately user-friendly but less secure. Cognitive Biometrics are complex and less practical, with moderate security. Device-based Binding offers medium security with high practicality. Embedded Valuable Secrets and All-or-nothing Disclosure are practical but less secure. Embedded Tokens in Physical Cards have high security but moderate practicality. Limited Use Control shows medium security and practicality. Overall, methods that are highly secure tend to be harder to implement, while those that are more broadly applicable may offer less robust security.

7.2 Final Reflections

Taking everything into consideration, we are inclined to believe that it is indeed possible, and perhaps more so than previously anticipated, to quantify the extent to which a binding mechanism represents an individual's identity throughout the various stages of authentication. The evaluation provided a clearer understanding of how effectively these mechanisms link authentication tokens to their rightful holders.

In the final chapter of the thesis, we explored the ethical implications of a future where individuals are closely tied to their authentication tokens. We observed that, with the advent of progressive authentication methods that are more personal and tied to the individual, potentially recognizing people through their behavior and digital activities even in anonymous scenarios, there are significant concerns. These methods could facilitate massive surveillance similar to dystopian scenarios, enable manipulation of user behavior for profit, or lead to the violation of user privacy. We discussed how such advancements might result in scenarios where users are compelled to reveal sensitive personal data, such as physiological information, which could affect their behavior, lead to self-censorship, and threaten digital freedom. While these technologies might offer some benefits, it is uncertain whether the necessity for token sharing truly serves the individual's best interests. Furthermore, this could mark the first instance where authentication systems, rather than users, control personal data, potentially compromising user experience and autonomy.

In concluding this thesis, we aim to spark an important discussion on the future of authentication, with a particular focus on holder-binding. As evident in our research, holder-binding is increasingly recognized in current systems, though often without formal definition. The failure to configure and implement it in a standardized manner could have detrimental effects. It is crucial to question whether it is within our responsibilities to determine whether users should share their tokens, even if it appears to be in their best interest. Without explicit standards and thorough research, implementing holder-binding could potentially lead to significant privacy violations and impact the evolving digital landscape. The future of authentication, and its implications for user privacy, remains a critical area for continued exploration and careful consideration.

Abbreviations

- **2FA**: Two-factor authentication
- **AI**: Artificial intelligence
- **BCS**: Biometric Cryptographic System
- **BLAC**: Blacklistable Anonymous Credential system
- **BVP**: Blood Volume Pulse
- **CAS**: Central Authentication Service
- **CSP**: Credential Service Provider
- **EEG**: Electroencephalography
- **ECG**: Electrocardiography
- **EMG**: Electromyography
- **FAR**: False Acceptance Rate
- **FRR**: False Rejection Rate
- **FTA**: Failure to Acquire Rate
- **FTE**: Failure to Enroll Rate
- **GDPR**: General Data Protection Regulation
- **GP**: Group Manager
- **IAM**: Identity and Access Management
- **IdP**: Identity Provider
- **ISP**: Internet Service Provider
- **KBA**: Knowledge-Based Authentication
- **MFA**: Multi-Factor Authentication
- **NIST**: National Institute of Standards and Technology

- **NT**: Non-Transferability
- **PAI**: Presentation Attack Instrument
- **OTP**: One-Time Password
- **RP**: Relying Party
- **SDK**: Software Development Kit
- **SP**: Service Provider
- **SSO**: Single Sign-On
- **TLR**: Technology Readiness Level
- **UID**: Unique Identifier
- **VPN**: Virtual Private Network

Bibliography

[1] Psychology Today. *Identity: Self-Image, Self-Concept.* [Online; accessed 19-April-2024]. URL: https://www.psychologytoday.com/gb/basics/identity.

[2] Sandra Gittlen and Linda Rosencrance. *What is identity and access management? Guide to IAM.* [Online; accessed 19-April-2024]. URL: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system%5C#:%5C~:text=Identity%5C%20and%5C%20access%5C%20management%5C%20(IAM,critical%5C%20information%5C%20within%5C%20their%5C%20organizations.

[3] Jaap-Henk Hoepman. *On using identity cards to store anonymous credentials.* Blog post. Nov. 2011. URL: http://blog.xot.nl/2011/11/16/on-using-identity-cards-to-store-anonymous-credentials/.

[4] Beyond Identity Blog. *Password Faux Pas.* May 2021. URL: https://www.beyondidentity.com/resource/password-faux-pas.

[5] Joris Van Ouytsel. "The prevalence and motivations for password sharing practices and intrusive behaviors among early adolescents' best friendships - A mixed-methods study". In: *Telematics and Informatics* 63 (2021), p. 101668. ISSN: 0736-5853. DOI: https://doi.org/10.1016/j.tele.2021.101668. URL: https://www.sciencedirect.com/science/article/pii/S0736585321001076.

[6] Monica Whitty et al. "Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords". In: *Cyberpsychology, Behavior, and Social Networking* 18.1 (2015). PMID: 25517697, pp. 3–7. DOI: 10.1089/cyber.2014.0179. eprint: https://doi.org/10.1089/cyber.2014.0179. URL: https://doi.org/10.1089/cyber.2014.0179.

[7] Supriya Singh et al. "Password sharing: implications for security design based on social practice". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* CHI '07. Association for Computing Machinery, 2007, pp. 895–904. ISBN: 9781595935939. DOI: 10.1145/1240624.1240759. URL: https://doi.org/10.1145/1240624.1240759.

[8] Joseph 'Jofish' Kaye. "Self-reported password sharing strategies". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* CHI '11. Association for Computing Machinery, 2011, pp. 2619–2622. ISBN: 9781450302289. DOI: 10.1145/1978942.1979324. URL: https://doi.org/10.1145/1978942.1979324.

[9] Christina M. van Essen and Joris Van Ouytsel. "Snapchat streaks—How are these forms of gamified interactions associated with problematic smartphone use and fear of missing out among early adolescents?" In: *Telematics and Informatics Reports* 11 (2023), p. 100087. ISSN: 2772-5030. DOI: https://doi.org/10.1016/j.teler.2023.100087. URL: https://www.sciencedirect.com/science/article/pii/S2772503023000476.

[10] Jeffrey Stanton et al. "Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices." In: *Proceedings of the 10th Americas Conference on Information Systems* (Jan. 2004), p. 175.

[11] Y.M. Hausawi. "Current trend of end-users' behaviors towards security mechanisms". In: *HAS 2016*. Ed. by T. Tryfonas. Vol. 9750. LNCS. Springer, 2016, pp. 140–151. DOI: 10.1007/978-3-319-39381-0_13.

[12] Anne-Marie Blazdell. "5 dangers of password sharing in the workplace". In: *Syn-Star* (Apr. 2024). Checked by: Verity Armstrong. URL: https://www.syn-star.co.uk/5-dangers-of-password-sharing-in-the-workplace/#:~:text=Password%20sharing%20among%20employees%20increases,leaks%2C%20sabotage%2C%20or%20fraud..

[13] *General Data Protection Regulation (GDPR)*. 2018. URL: https://gdpr-info.eu/.

[14] F. Betül Durak et al. *Non-Transferable Anonymous Tokens by Secret Binding*. 2024. URL: https://eprint.iacr.org/2024/711.

[15] National Institute of Standards and Technology (NIST). *Digital Identity Model*. NIST Special Publication 800-63-4. 2021. URL: https://pages.nist.gov/800-63-4/sp800-63/model/.

[16] Paul A. Grassi et al. *NIST Special Publication 800-63A: Digital Identity Guidelines - Enrollment and Identity Proofing*. Tech. rep. National Institute of Standards and Technology, 2017. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf.

[17] Paul Bastan et al. *Identifier Binding: Defining the Core of Holder Binding*. White Paper 1. RWOT XI: The Hague, Feb. 2023.

[18] ENISA. *Remote ID Proofing - Good Practices*. Mar. 2024. URL: https://www.enisa.europa.eu/publications/remote-id-proofing-good-practices.

[19] Wikipedia contributors. *Legal person*. [Online; accessed 10-July-2024]. URL: https://en.wikipedia.org/wiki/Legal_person.

[20] Bridget Chalk. *Modernism and mobility: The passport and cosmopolitan experience*. Jan. 2014, pp. 1–240. ISBN: 978-1-349-49435-4. DOI: 10.1057/9781137439833.

[21] J.S. Park and R. Sandhu. "Binding identities and attributes using digitally signed certificates". In: *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00)*. 2000, pp. 120–127. DOI: 10.1109/ACSAC.2000.898865.

[22] NIST Glossary. *Binding*. [Online; accessed 10-July-2024]. URL: https://csrc.nist.gov/glossary/term/binding.

[23] Wikipedia contributors. *Public Key Infrastructure.* [Online; accessed 10-July-2024]. URL: https://en.wikipedia.org/wiki/Public_key_infrastructure#:~:text=In%20cryptography%2C%20a%20PKI%20is,a%20certificate%20authority%20(CA).

[24] OAuth. *OAuth 2.0.* [Online; accessed 12-June-2024]. URL: https://oauth.net/2/.

[25] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-63B: Digital Identity Guidelines.* Tech. rep. [Online; accessed 12-June-2024]. NIST. URL: https://pages.nist.gov/800-63-3/sp800-63b.html.

[26] National Institute of Standards and Technology (NIST). *Identity Binding.* [Online; accessed 12-June-2024]. URL: https://csrc.nist.rip/glossary/term/Identity_Binding.

[27] Anil K. Jain et al. *Introduction to Biometrics.* [Online; accessed 24-May-2024]. URL: https://link.springer.com/book/10.1007/978-0-387-77326-1.

[28] Krishna Dharavath, F. A. Talukdar, and R. H. Laskar. "Study on biometric authentication systems, challenges and future trends: A review". In: *IEEE International Conference on Computational Intelligence and Computing Research.* 2013, pp. 1–7. DOI: 10.1109/ICCIC.2013.6724278.

[29] Stephen Mayhew for Biometric Update. *History of Biometrics.* [Online; accessed 24-May-2024]. URL: https://www.biometricupdate.com/201802/history-of-biometrics-2.

[30] Thales. *Biometrics: definition, use cases, latest news.* [Online; accessed 24-May-2024]. URL: https://www.thalesgroup.com.

[31] Fraud. *Employing biometric information for identity verification.* [Online; accessed 24-May-2024]. URL: https://www.fraud.com/post/biometric-information.

[32] builtin. *What Is Biometrics?* [Online; accessed 24-May-2024]. URL: https://builtin.com/hardware/what-is-biometrics.

[33] Anil K. Jain, Patrick Flynn, and Arun A. Ross. *Handbook of Biometrics.* 1st. Springer Publishing Company, Incorporated, 2010. ISBN: 1441943757.

[34] *VeriDas.* [Online; accessed 24-May-2024]. URL: https://veridas.com/en/voice-biometric-authentication/.

[35] *LumenVox.* [Online; accessed 24-May-2024]. URL: https://www.lumenvox.com/.

[36] *PingOne Verify.* [Online; accessed 24-May-2024]. URL: https://www.pingidentity.com/en.html.

[37] *IDR&D.* [Online; accessed 24-May-2024]. URL: https://www.idrnd.ai/.

[38] *AWARE.* [Online; accessed 24-May-2024]. URL: https://www.aware.com/.

[39] *accurascan.* [Online; accessed 24-May-2024]. URL: https://accurascan.com/.

[40] *Oz Forensics.* [Online; accessed 24-May-2024]. URL: https://ozforensics.com/.

[41] *FusionAuth.* [Online; accessed 24-May-2024]. URL: https://fusionauth.io/.

[42] *LoginID.* [Online; accessed 24-May-2024]. URL: https://loginid.io/.

[43] *Biometric Vision.* [Online; accessed 24-May-2024]. URL: https://biometricvision.com/.

[44] *facial-login-web*. [Online; accessed 24-May-2024]. URL: https://susantabiswas.github.io/facial-login-web/.

[45] *facephi*. [Online; accessed 24-May-2024]. URL: https://en.facephi.com/.

[46] *M2SYS*. [Online; accessed 24-May-2024]. URL: https://www.m2sys.com/cloud-based-abis-automated-biometric-identification-system-api/.

[47] *BioID*. [Online; accessed 24-May-2024]. URL: https://www.bioid.com/.

[48] *Cognitec*. [Online; accessed 24-May-2024]. URL: https://www.cognitec.com/.

[49] *Rohos*. [Online; accessed 24-May-2024]. URL: https://rohos.com/products/rohos-face-logon/.

[50] *Imageware*. [Online; accessed 24-May-2024]. URL: https://imageware.io/.

[51] *NEC*. [Online; accessed 24-May-2024]. URL: https://www.nec.com/.

[52] *Iris ID*. [Online; accessed 24-May-2024]. URL: https://www.irisid.com/.

[53] *FaceTec*. [Online; accessed 24-May-2024]. URL: https://www.facetec.com/.

[54] *Windows Hello*. [Online; accessed 24-May-2024]. URL: https://www.microsoft.com/.

[55] *PalmId*. [Online; accessed 24-May-2024]. URL: https://www.redrockbiometrics.com/palmid-pay/.

[56] *irisguard*. [Online; accessed 24-May-2024]. URL: https://www.irisguard.com/.

[57] *NIST ranks Veridas as the world's second best facial biometric engine. VeriDas*. [Online; accessed 24-May-2024]. URL: https://veridas.com/en/nist-ranks-veridas-world-top-facial-biometric-engines/.

[58] Megan Rees. *The Future Of User Authentication: A Guide To Behavioral Biometrics*. [Online; accessed 24-May-2024]. URL: https://expertinsights.com/insights/a-guide-to-behavioral-biometrics/.

[59] LexisNexis. *What Is Behavioral Biometrics?* [Online; accessed 24-May-2024]. URL: https://risk.lexisnexis.com/.

[60] OneSpan. *Behavioral Biometrics*. [Online; accessed 24-May-2024]. URL: https://www.onespan.com/topics/behavioral-biometrics.

[61] Roman V. Yampolskiy and Venu Govindaraju. "Taxonomy of Behavioural Biometrics". In: *Behavioral Biometrics for Human Identification: Intelligent Applications*. Ed. by Liang Wang and Xue Geng. IGI Global, 2010, pp. 1–43. DOI: 10.4018/978-1-60566-725-6.ch001. URL: https://doi.org/10.4018/978-1-60566-725-6.ch001.

[62] Mridula Sharma and Haytham Elmiligi. "Behavioral Biometrics: Past, Present and Future". In: *Recent Advances in Biometrics*. Ed. by Muhammad Sarfraz. Rijeka: IntechOpen, 2022. Chap. 4. DOI: 10.5772/intechopen.102841. URL: https://doi.org/10.5772/intechopen.102841.

[63] Stephan Al-Zubi, Arslan Brömme, and Klaus Tönnies. "Using an Active Shape Structural Model for Biometric Sketch Recognition". In: *Pattern Recognition*. Ed. by Bernd Michaelis and Gerald Krell. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 187–195.

[64] Michael R. Schmid, Farkhund Iqbal, and Benjamin C.M. Fung. "E-mail authorship attribution using customized associative classification". In: *Digital Investigation* 14 (2015). The Proceedings of the Fifteenth Annual DFRWS Conference, S116–S126. ISSN: 1742-2876. DOI: https://doi.org/10.1016/j.diin.2015.05.012. URL: https://www.sciencedirect.com/science/article/pii/S1742287615000572.

[65] Tom Fawcett and Foster Provost. "Adaptive Fraud Detection". In: *Data Mining and Knowledge Discovery* 1 (1997), pp. 291–316. DOI: 10.1023/A:1009700419189. URL: https://doi.org/10.1023/A:1009700419189.

[66] Roman Yampolskiy and Venu Govindaraju. "Strategy-based behavioural biometrics: A novel approach to automated identification". In: *IJCAT* 35 (Apr. 2009), pp. 29–41. DOI: 10.1504/IJCAT.2009.024593.

[67] *Prove*. [Online; accessed 24-May-2024]. URL: https://www.prove.com/solutions/identity/.

[68] *Typingdna*. [Online; accessed 24-May-2024]. URL: https://www.typingdna.com/.

[69] *BioCatch*. [Online; accessed 24-May-2024]. URL: https://www.biocatch.com/.

[70] *Simprints*. [Online; accessed 24-May-2024]. URL: https://www.simprints.com/.

[71] *Plurilock*. [Online; accessed 24-May-2024]. URL: https://plurilock.com/.

[72] *ThreatMark*. [Online; accessed 25-April-2024]. URL: https://www.threatmark.com/transaction-risk-analysis/strong-invisible-authentication/.

[73] *Biometric Signature ID*. [Online; accessed 24-May-2024]. URL: https://www.biosig-id.com/.

[74] *ZIGHRA*. [Online; accessed 24-May-2024]. URL: https://zighra.com/.

[75] *Aculab*. [Online; accessed 24-May-2024]. URL: https://www.aculab.com/biometric-technologies/voisentry/.

[76] *Cynet*. [Online; accessed 25-April-2024]. URL: https://www.cynet.com/platform/user-behaviour-analytics/?_gl=1*xgr2un*_up*MQ..*_ga*NzQyNTk3OTkwLjE3MTMyNTg1NjE.*_ga_6ZET9Y5B2X*MTcxMzI1ODU2MC4xLjAuMTcxMzI1ODU2MC4wLjAuMA...

[77] *Sardine*. [Online; accessed 25-April-2024]. URL: https://www.sardine.ai/identity-fraud.

[78] *SECUREAUTH*. [Online; accessed 25-April-2024]. URL: https://www.secureauth.com/.

[79] *Arvato*. [Online; accessed 24-May-2024]. URL: https://arvato.com/.

[80] *UnifyID*. [Online; accessed 24-May-2024]. URL: https://www.crunchbase.com/organization/unifyid.

[81] *NuData*. [Online; accessed 24-May-2024]. URL: https://www.crunchbase.com/organization/nudata-security.

[82] AntiSpoofing. *Presentation Attacks: Types, Instruments, and Detection*. [Online; accessed 25-April-2024]. URL: https://antispoofing.org/presentation-attacks-types-instruments-and-detection//.

[83] Elvira Carrero. *What is liveness detection?* [Online; accessed 25-April-2024]. URL: https://www.mobbeel.com/en/blog/what-is-liveness-detection/.

[84] iProov. *Genuine Presence Assurance.* [Online; accessed 25-April-2024]. URL: https://www.iproov.com/iproov-system/technology/genuine-presence-assurance.

[85] Leo Pipino, Yang Lee, and Richard Wang. "Data Quality Assessment". In: *Communications of the ACM* 45 (July 2003). DOI: 10.1145/505248.506010.

[86] Amazon. *Guidance for Identity Verification on AWS.* [Online; accessed 25-May-2024]. URL: https://aws.amazon.com/solutions/guidance/identity-verification-on-ws/.

[87] iDCentral. *Identity Verification Platform.* [Online; accessed 25-May-2024]. URL: https://www.idcentral.io/.

[88] Veriff. *THE IDENTITY VERIFICATION PLATFORM.* [Online; accessed 25-April-2024]. URL: https://www.veriff.com/.

[89] Facia. *Online Identity Verification Package.* [Online; accessed 25-April-2024]. URL: https://facia.ai/.

[90] Onfido. *Real Identity Platform: Verification Suite.* [Online; accessed 25-April-2024]. URL: https://onfido.com/tour/.

[91] FACEKI. *FACEKI Identity Verification KYC.* [Online; accessed 25-April-2024]. URL: https://kycdocv2.faceki.com/.

[92] PXL. *Automated ID Verification in less than 30 seconds.* [Online; accessed 25-April-2024]. URL: https://www.pxl-vision.com/.

[93] Authme. *Keep Your Identity Safe.* [Online; accessed 25-April-2024]. URL: https://authme.com/zh_tw/.

[94] Jumio. *IDENTITY VERIFICATION SOLUTIONS.* [Online; accessed 25-April-2024]. URL: https://www.jumio.com/.

[95] AU10tix. *Advanced Identity Verification in Seconds.* [Online; accessed 25-April-2024]. URL: https://www.au10tix.com/.

[96] Passbase. *Passbase.* [Online; accessed 25-April-2024]. URL: https://parallelmarkets.com/?utm_source=passbase.com/.

[97] Unico. *Unico Check.* [Online; accessed 25-May-2024]. URL: https://developers.unico.io/en/docs/.

[98] Persona. *Identity Verification Solution.* [Online; accessed 25-May-2024]. URL: https://withpersona.com/.

[99] ISO. *Machine learning: Everything you need to know.* [Online; accessed 24-May-2024]. URL: https://www.iso.org/artificial-intelligence/machine-learning#:~:text=future%20of%20AI%3F-,What%20is%20machine%20learning%3F,data%20without%20being%20explicitly%20programmed..

[100] IBM. *IBM Trusteer Solutions.* [Online; accessed 25-4-2024]. URL: https://www.ibm.com/trusteer.

[101] Wikipedia. *Device fingerprint.* [Online; accessed 24-May-2024]. URL: https://en.wikipedia.org/wiki/Device_fingerprint.

[102] Trust Decision. *Device fingerprint.* [Online; accessed 24-May-2024]. URL: https://trustdecision.com/resources/blog/what-is-device-fingerprint-how-does-it-work.

[103] Pierre Laperdrix et al. *Browser Fingerprinting: A survey.* 2019. arXiv: 1905.01051 [cs.CR].

[104] Mark Nottingham. “Not Similar to Cookies: Device and Browser Fingerprinting as Sensitive Personal Data”. In: *SSRN* (Dec. 2020). DOI: 10.2139/ssrn.3890545. URL: https://ssrn.com/abstract=3890545.

[105] Incognia. *Incognia.* [Online; accessed 24-May-2024]. URL: https://www.incognia.com/.

[106] SEON. *What Is Device Fingerprinting and How Exactly Does It Work?* [Online; accessed 24-May-2024]. URL: https://seon.io/resources/device-fingerprinting/.

[107] Callsign. *Detecting fraud with device fingerprinting.* [Online; accessed 24-May-2024]. URL: https://www.callsign.com/knowledge-insights/preventing-fraud-with-device-fingerprinting.

[108] Appsealing. *How Device Fingerprinting works.* [Online; accessed 24-May-2024]. URL: https://www.appsealing.com/device-fingerprinting/.

[109] Radware. *Radware Documentation.* [Online; accessed 24-May-2024]. URL: https://portals.radware.com/Not-Logged-In/SSOLogin/?ReturnURL=/ProductDocumentation/Alteon_Command_Reference_33_0_0_0/Alteon_Command_Reference/Preface_struct.02.2.htm.

[110] STYTCH. *Fraud API reference.* [Online; accessed 24-May-2024]. URL: https://stytch.com/docs/fraud/api.

[111] JumpCloud. *Bind Users to Devices.* [Online; accessed 24-May-2024]. URL: https://jumpcloud.com/support/bind-users-to-devices.

[112] Forge Rock. *Device Binding Node.* [Online; accessed 24-May-2024]. URL: https://backstage.forgerock.com/docs/auth-node-ref/latest/auth-node-device-binding.html.

[113] *BEYONDIDENTITY.* [Online; accessed 25-April-2024]. URL: https://www.beyondidentity.com/products/secure-workforce.

[114] InstaSafe. *Device Binding.* [Online; accessed 24-May-2024]. URL: https://instasafe.com/zero-trust-features/device-binding/.

[115] Castle. *Prevent account and platform abuse at scale.* [Online; accessed 24-May-2024]. URL: https://castle.io/?ref=blog.castle.io.

[116] IPQUALITYSCORE. *Device fingerprinting.* [Online; accessed 24-May-2024]. URL: https://www.ipqualityscore.com/device-fingerprinting.

[117] WebKay. *What every Browser knows about you.* [Online; accessed 24-May-2024]. URL: https://webkay.robinlinus.com/.

[118] EFF. *Cover your Tracks.* [Online; accessed 24-May-2024]. URL: https://coveryourtracks.eff.org/.

[119] AMIUnique. *AmIUnique.* [Online; accessed 24-May-2024]. URL: https://amiunique.org/fingerprint.

[120] CreepJS. *Creep JS.* [Online; accessed 24-May-2024]. URL: https://abrahamjuliot.github.io/creepjs/.

[121] Fingerprint. *Fingerprint JS*. [Online; accessed 24-May-2024]. URL: https://fingerprint.com.

[122] BroPrint. *Browser FingerPrint*. [Online; accessed 24-May-2024]. URL: https://broprintjs.netlify.app/.

[123] Supercookie. *Supercookie*. [Online; accessed 24-May-2024]. URL: https://supercookie.me/.

[124] DetectIncognito. *detectIncognito*. [Online; accessed 24-May-2024]. URL: https://detectincognito.com/.

[125] Fingerprint. *The device Intelligence Platform*. [Online; accessed 24-May-2024]. URL: https://fingerprint.com/.

[126] Institute of Data. *Uncovering Data Patterns and Trends with Data Science*. [Online; accessed 24-May-2024]. URL: https://www.institutedata.com/blog/uncover-data-patterns-with-data-science/#:~:text=Techniques%20for%20identifying%20patterns%20in%20data&text=These%20techniques%20include%20statistical%20analysis,data%20by%20analysing%20data%20patterns..

[127] Incognia. *Knowledge-based authentication (KBA) [explanation and examples]*. [Online; accessed 25-April-2024]. URL: https://www.incognia.com/the-authentication-reference/knowledge-based-authentication-kba-meaning-and-examples.

[128] Tech Target. *What is knowledge-based authentication?* [Online; accessed 25-April-2024]. URL: https://www.techtarget.com/searchsecurity/definition/knowledge-based-authentication.

[129] K2 enterprises. *Comparing Static And Dynamic Knowledge-Based Authentication*. [Online; accessed 25-April-2024]. URL: https://www.k2e.com/articles/knowledge-based-authentication/.

[130] PingIdentity. *What is Knowledge-based Authentication (KBA)?* [Online; accessed 25-April-2024]. URL: https://www.pingidentity.com/en/resources/blog/post/what-is-knowledge-based-authentication-kba.html.

[131] diro. *Knowledge-Based Authentication (KBA) Guide*. [Online; accessed 25-April-2024]. URL: https://diro.io/knowledge-based-authentication-kba-guide/.

[132] *ZohoSign*. [Online; accessed 25-April-2024]. URL: https://www.zoho.com/sign/features-and-benefits/knowledge-based-authentication.html.

[133] *GBG IDology*. [Online; accessed 25-April-2024]. URL: https://www.idology.com/solutions/dynamic-kba-knowledge-based-authentication/.

[134] Stephan Wiefling, Luigi Lo Iacono, and Markus Dürmuth. "Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild". In: *ICT Systems Security and Privacy Protection*. Ed. by Gurpreet Dhillon et al. Cham: Springer International Publishing, 2019, pp. 134–148.

[135] Lauren Ballejos. *What Is Context-Based Authentication?* [Online; accessed 25-4-2024]. URL: https://www.ninjaone.com/it-hub/remote-access/what-is-context-based-authentication/.

[136] Shelley Leveson for HYPR. *How to Use Context-Based Authentication to Improve Security.* [Online; accessed 25-April-2024]. URL: https://blog.hypr.com/context-based-authentication-to-improve-security.

[137] miniOrange. *5 Reasons to Deploy Context-Based Authentication.* [Online; accessed 25-April-2024]. URL: https://www.miniorange.com/blog/5-reasons-to-deploy-context-based-authentication-for-your-organization/.

[138] *TrustBuilder.* [Online; accessed 25-April-2024]. URL: https://www.trustbuilder.com/use-cases/contextual-authentication.

[139] *Entersekt.* [Online; accessed 25-April-2024]. URL: https://www.entersekt.com/products/context-aware-authentication.

[140] *Appgate.* [Online; accessed 25-April-2024]. URL: https://www.appgate.com/risk-based-authentication/.

[141] *Okta.* [Online; accessed 25-April-2024]. URL: https://www.okta.com/products/adaptive-multi-factor-authentication/.

[142] *OneSpan.* [Online; accessed 25-April-2024]. URL: https://www.onespan.com/products/identity-verification.

[143] *Cisco DUO.* [Online; accessed 25-April-2024]. URL: https://duo.com/solutions/risk-based-authentication.

[144] *THALES.* [Online; accessed 25-April-2024]. URL: https://cpl.thalesgroup.com/en-gb/access-management/context-based-authentication.

[145] Sebastian Pape. "A Survey on Non-transferable Anonymous Credentials". In: *The Future of Identity in the Information Society.* Ed. by Vashek Matyáš et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 107–118.

[146] Jan Camenisch and Anna Lysyanskaya. "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation". In: *Advances in Cryptology — EUROCRYPT 2001.* Ed. by Birgit Pfitzmann. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 93–118. ISBN: 978-3-540-44987-4.

[147] Cynthia Dwork, Jeffrey Lotspiech, and Moni Naor. "Digital Signets: Self-Enforcing Protection of Digital Information (Preliminary Version)." In: Jan. 1996, pp. 489–498. DOI: 10.1145/237814.237997.

[148] Wikipedia contributors. *Trapdoor Function.* [Online; accessed 24-May-2024]. URL: https://en.wikipedia.org/wiki/Trapdoor_function.

[149] Wikipedia contributors. *Central Authentication Service.* [Online; accessed 24-May-2024]. URL: https://en.wikipedia.org/wiki/Central_Authentication_Service.

[150] Wikipedia contributors. *Single sign-on.* [Online; accessed 7-June-2024]. URL: https://en.wikipedia.org/wiki/Single_sign-on.

[151] Wikipedia. *Brute-force attack.* [Online; accessed 12-June-2024]. URL: https://en.wikipedia.org/wiki/Brute-force_attack.

[152] Pascal Vyncke. *Attacks on websites explained.* Accessed on June 7, 2012. Archived on June 19, 2022.

[153] Anna Lysyanskaya. *Anonymous credentials.* Presented at Special Topics on Privacy and Public Auditability (STPPA), Event #4, by video-conference. Nov. 2022. URL: https://csrc.nist.gov/Presentations/2022/stppa4-anonym-cred.

[154] Ivan Damgård, Kasper Dupont, and Michael Østergaard Pedersen. *Unclonable Group Identification.* https://eprint.iacr.org/2005/170. 2005. URL: https://eprint.iacr.org/2005/170.

[155] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. "Compact E-Cash". In: *Advances in Cryptology – EUROCRYPT 2005.* Ed. by Ronald Cramer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 302–321. ISBN: 978-3-540-32055-5.

[156] David Chaum, Amos Fiat, and Moni Naor. "Untraceable Electronic Cash". In: *Advances in Cryptology — CRYPTO' 88.* Ed. by Shafi Goldwasser. New York, NY: Springer New York, 1990, pp. 319–327. ISBN: 978-0-387-34799-8.

[157] Patrick P. Tsang et al. "Blacklistable anonymous credentials: blocking misbehaving users without ttps". In: *Proceedings of the 14th ACM Conference on Computer and Communications Security.* CCS '07. Alexandria, Virginia, USA: Association for Computing Machinery, 2007, pp. 72–81. ISBN: 9781595937032. DOI: 10.1145/1315245.1315256. URL: https://doi.org/10.1145/1315245.1315256.

[158] Jan Camenisch et al. *How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication.* 2006. URL: https://eprint.iacr.org/2006/454.

[159] Tom Caddy. "Tamper Resistance". In: *Encyclopedia of Cryptography and Security.* Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 1278–1278. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_230. URL: https://doi.org/10.1007/978-1-4419-5906-5_230.

[160] Markus Kuhn. "Smartcard Tamper Resistance". In: *Encyclopedia of Cryptography and Security.* Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 1225–1227. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_228. URL: https://doi.org/10.1007/978-1-4419-5906-5_228.

[161] Jaap-Henk Hoepman. *On using identity cards to store anonymous credentials.* 2011. URL: https://blog.xot.nl/2011/11/16/on-using-identity-cards-to-store-anonymous-credentials/index.html.

[162] Julia Hesse, Nitin Singh, and Alessandro Sorniotti. *How to Bind Anonymous Credentials to Humans.* https://eprint.iacr.org/2023/853. 2023. URL: https://eprint.iacr.org/2023/853.

[163] Qiming Li, Yagiz Sutcu, and Nasir Memon. "Secure Sketch for Biometric Templates". In: vol. 4284. Dec. 2006, pp. 99–113. ISBN: 978-3-540-49475-1. DOI: 10.1007/11935230_7.

[164] D. B. Ojha and A. Sharma. "A fuzzy commitment scheme with McEliece's cipher". In: *Survey in Mathematics and Its Application* 5 (2010), pp. 73–83.

[165] C.-J. Chae et al. "Enhanced biometric encryption algorithm for private key protection in BioPKI system". In: *Journal of Central South University* 21.11 (Nov. 2014), pp. 4286–4290.

[166] Tomas Trainys. *Encryption Keys Generation Based on Bio-Cryptography Finger Vein Method*. 2018. URL: `https://api.semanticscholar.org/CorpusID:53513123`.

[167] C. Rathgeb and A. Uhl. “A survey on biometric cryptosystems and cancelable biometrics”. In: *EURASIP Journal on Information Security* 2011.3 (2011), pp. 1–25. DOI: `10.1186/1687-417X-2011-3`. URL: `https://doi.org/10.1186/1687-417X-2011-3`.

[168] Yevgeniy Dodis et al. “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”. In: *CoRR* abs/cs/0602007 (2006). arXiv: `cs/0602007`. URL: `http://arxiv.org/abs/cs/0602007`.

[169] Ari Juels and Martin Wattenberg. “A fuzzy commitment scheme”. In: *Proceedings of the 6th ACM Conference on Computer and Communications Security*. New York, NY, USA: ACM, 1999, pp. 28–36.

[170] Ari Juels and Madhu Sudan. “A fuzzy vault scheme”. In: *Proceedings of the 2002 IEEE International Symposium on Information Theory*. IEEE, 2002, p. 408.

[171] N. I. Udzir, A. Abdullah, and R. Mahmod. “State of the Art in Biometric Key Binding and Key Generation Schemes”. In: *International Journal of Communication Networks and Information Security (IJCNIS)* 9.3 (2017).

[172] F. Benhammadi and K. Beghdad Bey. “Password hardened fuzzy vault for fingerprint authentication system”. In: *Image and Vision Computing* 32.8 (Aug. 2014), pp. 487–496.

[173] Julien Bringer, Hervé Chabanne, and Boumediene Kindarji. “The best of both worlds: Applying secure sketches to cancelable biometrics”. In: *Science of Computer Programming* 74.1–2 (Dec. 2008), pp. 43–51.

[174] C. Li and J. Hu. “A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures”. In: *IEEE Transactions on Information Forensics and Security* 11.3 (2016), pp. 543–555.

[175] Dr. Algimantas Venckauskas and Povilas Nanevicius. *IJESRT INTERNATIONAL JOURNAL Cryptographic Key Generation from Finger Vein*. 2013. URL: `https://api.semanticscholar.org/CorpusID:18115910`.

[176] W. Sheng et al. “A Biometric Key Generation Method Based on Semi-supervised Data Clustering”. In: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 45.9 (Sept. 2015), pp. 1205–1217.

[177] Kenneth Revett. “Cognitive biometrics: A novel approach to continuous person authentication”. In: *Int. J. of Cognitive Biometrics* 1 (Jan. 2012), pp. 1–9. DOI: `10.1504/IJCB.2012.046516`.

[178] M. Wang et al. “Representation Learning and Pattern Recognition in Cognitive Biometrics: A Survey”. In: *Sensors (Basel)* 22.14 (July 2022), p. 5111. DOI: `10.3390/s22145111`.

[179] Ashwini S Chatra. “Cognitive biometrics based on EEG signal”. In: *2014 International Conference on Contemporary Computing and Informatics (IC3I)*. 2014, pp. 374–376. DOI: `10.1109/IC3I.2014.7019605`.

[180] Wikipedia contributors. *Electroencephalography.* [Online; accessed 24-May-2024]. Wikipedia. URL: https://en.wikipedia.org/wiki/Electroencephalography.

[181] Nicholas H. Bunce, Robin Ray, and Hitesh Patel. "Cardiology". In: *Kumar and Clark's Clinical Medicine*. Ed. by Adam Feather, David Randall, and Mona Waterhouse. 10th. Elsevier, 2020, pp. 1033–1038. ISBN: 978-0-7020-7870-5.

[182] Bitbrain. *Versatile Bio Sensor Guide: Blood Volume Pulse (BVP).* [Online; accessed 24-May-2024]. Bitbrain. URL: https://help.bitbrain.com/versatile-bio-bvp-sensor.

[183] D. G. E. Robertson et al. *Electromyographic Kinesiology, Research Methods in Biomechanics.* Champaign, IL: Human Kinetics, 2014. ISBN: 978-0-7360-9340-8.

[184] R. Kerr. "Underestimation of pupil size by critical care and neurosurgical nurses". In: *American Journal of Critical Care* 25.3 (2016), pp. 213–219. DOI: 10.4037/ajcc2016554.

[185] *Rorschach Test.* [Online; accessed 13-May-2024]. URL: https://en.wikipedia.org/wiki/Rorschach_test.

[186] Noel Richards. *Slides from Security+ Guide to Network Security Fundamentals, Fifth Edition.* 2018.

[187] HITACHI. *Cancellable Biometrics.* [Online; accessed 2-June-2024]. URL: https://www.hitachi.com/rd/glossary/c/cancellable_biometrics.html.

[188] *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements.* © ISO 2024. 2022. URL: https://www.iso.org/standard/27001.

[189] OWASP Foundation. *Authentication Cheat Sheet.* [Online; accessed 27-July-2024]. 2024. URL: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html.

[190] FIDO Alliance. *FIDO Alliance.* [Online; accessed 27-July-2024]. URL: https://fidoalliance.org/.

[191] ISO 25010. *System and Software Quality Models.* 2024. URL: https://iso25000.com/index.php/en/iso-25000-standards/iso-25010.

[192] Steven Way and Yufei Yuan. "Criteria for Evaluating Authentication Systems." In: vol. 4. Jan. 2009, p. 338.

[193] National Institute of Standards and Technology (NIST). *Threats and Security Considerations.* Tech. rep. SP-800-63-4. NIST, 2024. URL: https://pages.nist.gov/800-63-4/sp800-63b/security/.

[194] National Institute of Standards and Technology (NIST). *Assertion.* [Online; accessed 27-July-2024]. URL: https://csrc.nist.gov/glossary/term/Assertion#:~:text=Definitions%5C%3A,authentication%5C%20event%5C%20at%5C%20the%5C%20IdP..

[195] Gabriella Paiella. "Child Genius Uses Sleeping Mom's Thumb to Unlock Phone and Order Presents". In: *The Cut* (Dec. 2016). URL: https://www.thecut.com/2016/12/child-uses-sleeping-moms-thumb-to-unlock-phone-order-gifts.html.

[196] Josh Constine. “Your Nosy Boy/Girlfriend Can Unlock Your iPhone 5s With Your Thumb While You Sleep”. In: *TechCrunch* (Sept. 2013). URL: https://techcrunch.com/2013/09/20/fingerprint-unlock-while-sleeping/.

[197] National Research Council (US) Whither Biometrics Committee. *Cultural, Social, and Legal Considerations*. Ed. by J. N. Pato and L. I. Millett. Washington, DC: National Academies Press, 2010. Chap. 4. URL: https://www.ncbi.nlm.nih.gov/books/NBK219893/.

[198] Agence France-Presse. “Greeks rally against biometric ID card plan”. In: *NEOS KOSMOS* (Sept. 11, 2023). URL: https://neoskosmos.com/en/2023/09/11/news/greeks-rally-against-biometric-id-card-plan/.

[199] Big Brother Watch. *Stop Facial Recognition*. [Online; accessed 27-July-2024]. 2024. URL: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/.

[200] NASA. *Technology Readiness Level Definitions*. PDF. Public Domain. 2017. URL: https://www.nasa.gov/wp-content/uploads/2017/12/458490main_trl_definitions.pdf?emrc=da53fb.

[201] European Commission. *Technology Readiness Levels (TRL); Extract from Part 19 - Commission Decision C(2014)4995*. Material is available under a Creative Commons Attribution 4.0 International License. 2014. URL: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf.

[202] Jan Camenisch, Ronald Leenes, and Dieter Sommer. *Digital Privacy: PRIME - Privacy and Identity Management for Europe*. © 2011. Springer, 2011.

[203] Psychology Today. *Trust*. [Online; accessed 15-June-2024]. URL: https://www.psychologytoday.com/us/basics/trust.

[204] Kalev Leetaru. “As Orwell’s 1984 Turns 70 It Predicted Much Of Today’s Surveillance Society”. In: *Forbes* (May 2019). URL: https://www.forbes.com/sites/kalevleetaru/2019/05/06/as-orwells-1984-turns-70-it-predicted-much-of-todays-surveillance-society/.

[205] Wikipedia contributors. *1984 (book)*. Wikipedia, The Free Encyclopedia. [Online; accessed 27-July-2024]. URL: https://nl.wikipedia.org/wiki/1984_(boek).