01 ACKNOWLEDGEMENTS

ACKNOWLEDGEMENTS

This thesis is the culmination of a reflection that would not have been possible without the support and guidance of many folks.

My deepest gratitude goes to my supervisor, Joëlle Bitton, for her invaluable insights, patience, and encouragement throughout this process. I could not have been assigned a better tutor.

I am profoundly thankful to all the participants and colleagues who generously shared their time and experiences for the field observations, surveys, discussions and interviews.Your stories and insights form the empirical heart of this research.

To my friends, especially Sander and Emma: thank you for your sincere support, for your incredible insights, and for giving me constructive criticism.

And finally, to my mother, Mulki ALI: thank you for supporting me throughout this entire process, and continuing to believe in me more than I believe in myself.

02 ABSTRACT

ABSTRACT

This thesis examines the act of logging in as a cultural and design practice that defines how people gain access, are recognized, and take part in digital systems. It approaches authentication as a site of negotiation between user and machine, drawing from interface theory, anthropology, and design history to trace its evolution. This trajectory reveals how login processes inherit older logics of verification and control while masking them under convenience. As authentication becomes externalized to devices and identity providers, users lose awareness of the systems that validate them. Through historical analysis, user studies and speculative prototypes, the research explores how "the login experience" could instead support user experience by making context, friction, and user participation central to the experience of recognition online.

TABLE OF CONTENTS

TABLE OF CONTENTS

04 GLOSSARY

GLOSSARY

Because this research moves between computing, design, and philosophy, several terms require clarification. These definitions explain their words as I understand and use them throughout this thesis. They are not meant as universal truths, rather as working interpretations that situate the vocabulary of this research within the cultural and technical history of login.

Authentication is the process through which a system verifies a user's claim to identity, typically by testing a credential. It includes all processes through which an identity or ownership of an account are verified.

Identification is the first act of naming oneself before a system. It signals presence ("this is me") but not yet recognition. Identification precedes authentication, but together they form the process of entry.

Login, interpreted as "Connexion" in french, is the moment of passage into a digital environment, a process by which a user enters an authentication sequence to be recognised by a platform, device, or service. For me, "login" implies relation: a first exchange between human and system, a gesture closer to connexion than to verification. It is different from the act of authentication, due to the fact that this term only includes human-computer interactions. In that sense, this memoir is HCI research.

The externalisation of login describes the process through which authentication leaves its native platform and becomes distributed across other infrastructures. Through authenticator apps, passkeys, Single Sign-On systems, or biometric devices, recognition migrates toward third parties who guarantee trust on the platform's behalf. In this displacement, the act of entry becomes dependent on external institutions and technologies.

Liminality refers to the state of being in-between, neither fully inside nor outside. Borrowed from anthropological theory, it marks the moment when users are suspended between access and denial, or self and system. Login inhabits this liminal zone, where recognition has not yet been granted but the gesture has already begun.

Alienation, or aliénation, describes the user's estrangement from the means and meanings of recognition. It appears when the ability to authenticate, and thus to appear before a system, belongs more to infrastructures that mediate on users' behalf, than to the people being identified themselves. Alienation manifests as frustration, opacity, and doubt about ownership; the unsettling question of whether one's account, data, or identity still belong to oneself. It is a source of frustration.

Trust, or "confiance" as I understand it in french, defines the dynamic relation of belief between user and platform. Both technical and affective, it can be engineered through interface design, reinforced through repetition, or betrayed through breach. Trust is what allows users to hand over their credentials despite knowing little of where or how they will be processed. It is, in short, the faith that the system will keep its promise.

Opacity names the opposite of transparency. It describes a system whose inner workings, decisions, and data flows remain hidden from the user. Opacity in login demands belief in the system's decisions rather than understanding, shaping interactions through secrecy. In the context of login, it is both a condition of security and a source of alienation or estrangement.

05 INTRODUCTION

INTRODUCTION

Observe a familiar scene: a person stands before a door. They hold a key and attempt to enter: insert, twist, step through. Yet in our digital present, entry is neither simple nor singular. The key has multiplied. One key unlocks another; a code is sent elsewhere to an inbox or a phone; a fingerprint or face must confirm it; a secondary device must approve. What was once a straightforward threshold now unfolds as a distributed action, enacted across screens, devices, and platforms. This condition, which I call the externalisation of login, forms the first focus of this thesis.

Externalisation describes how authentication has migrated away from the immediate relationship between user and platform. To access one service, users must pass through another (Google Authenticator, Microsoft, Apple, SMS verification, recovery emails, or biometric prompts). Each intermediary extends the act of recognition outward, fragmenting it across corporate infrastructures that claim to simplify while quietly centralising control. The interface no longer belongs entirely to its designer or its user; its language and gestures are dictated by standards imposed from elsewhere.

This memoir begins with a simple question: what would the login experience look like if we designed it differently?

To ask this is to challenge a fundamental pillar of digital life. We are taught that frustration is the necessary price of safety, and that opacity is a feature of security. Worse yet, users remain frustrated, and are faced with countless more steps to make them "feel more secure", and yet few of the technologies employed inform users or succeed in enhancing users' experiences. This relegates additional login steps to another daily chore that erodes patience and, ultimately, care for security itself. Users often make a rational rejection of security advice, when the costs outweigh the perceived benefits (Lazar et al., 2009). Making users care for their security is a step that matters as much as making them secure.

What remains of this act we perform daily, if we reconsider its defined protection? The answer, I propose, is that login reveals something deeper about how we are taught to appear before

machines, in how we are trained to submit proof, how we internalise authority, and how we come to believe that friction equals safety.

Building on Alexander Galloway's notion of the interface as an agent of control and Arnold van Gennep's understanding of liminality, this thesis approaches login as a designed threshold that produces both subject and system. It does not simply connect the user to the system, more so that it produces the user, the system, and the world that both inhabit. The login, from this perspective, is a miniature apparatus of governance, defining who may enter, under what terms, and through which gestures of recognition. Following Wendy Hui Kyong Chun, I treat such interfaces as ideological performances that render invisible infrastructures of power into visible acts of participation. The login is therefore a checkpoint and a daily affirmation of faith in unseen systems that promise protection.

This thesis proceeds from three hypothesis:

> The login experience is a repetitive practice that, prior to entry, dictates part of users' feelings relating to the platforms they interact with.
>
> The externalisation of login marks a political and aesthetic shift; trust is displaced from individual platforms toward corporate infrastructures, leading to a loss of design independence, as those external infrastructures impose a new design theme platforms struggle to clash with or implement.
>
> Reimagining login requires an approach that questions its inheritances and imagines other modes of authentication, perhaps some that are more interactive or playful. The current login models can be improved upon.

From these claims emerge the guiding questions: What does the login process login teach us about being a user in networked systems? Can it be redesigned as a moment of relation-building between user and platform? Can it have an additional layer of play added to its design?

To address these questions, this research combines theoretical inquiry with design practice. First, it offers a history of authentication, tracing its origins from ancient seals and watchwords to modern biometric and federated systems. Second, it performs critical interface analysis, drawing on semiotics, media theory, user surveys, field research and human–computer interaction to expose how login scripts behaviour and emotion. Third, it develops speculative prototypes, paper or virtual experiments that enact alternative logics of recognition, and tests to see how those first solutions interact with users.

To redesign login is to rethink how we enter the virtual world, a world increasingly organised by credentials, permissions, and proofs of identity. Any reimagining must begin by reclaiming login's lost spaces of relation. The goal is to highlight how secure interactions can feel legible and engaging without endangering safety: to design thresholds that express comprehension and play as part of protection.

My motivation for this research begins with how I, like many users, first experienced them.

06 MOTIVATION

Fig. 1. “Verify You Are Human” reCAPTCHA interface

MOTIVATION

My motivation for this research began with something deceptively simple: noticing how often I felt friction in my everyday digital life. In many places online, platforms were adding new steps, new warnings or new demands, always in the name of "security." Yet the people and friends I spoke to did not feel safer. They felt frustrated, surveilled, and strangely powerless. Interfaces changed constantly, rules shifted without explanation, and once-familiar spaces now asked for more data in exchange for the same access.

At the same time, a contradictory pattern kept appearing. Whenever a service became "too annoying," a sleeker alternative would appear. It would promise fewer hurdles but hide new, obscure forms of data extraction. In the corners of comment sections, users were venting about having to "log in for everything," from restaurant Wi-Fi to small websites that once required nothing at all.

That was the moment the real question formed: Why has authentication evolved into such a universal, compulsory ritual?

Security can explain some of it, but not the whole thing. Especially when two-factor authentication, verification apps, and CAPTCHAs moved the tone away from invitation, straight into obligation. Then came the phrase that crystallized the issue for me:

> "PROVE YOU ARE HUMAN."

The absurdity of the demand (its theatricality, almost) made me wonder about the hidden logic behind these systems. Why must "my humanity" be proven through pattern recognition? What do we lose when access becomes a test? Which bodies and devices are excluded by default? Can I really only be identified through that?

Trivial in isolation, these questions revealed an emerging pattern. Many people I've met seem to have experienced a fear of losing their accounts during recovery, the stress of Multi-Factor Authentication, and the struggles that come with changing and remembering passwords.

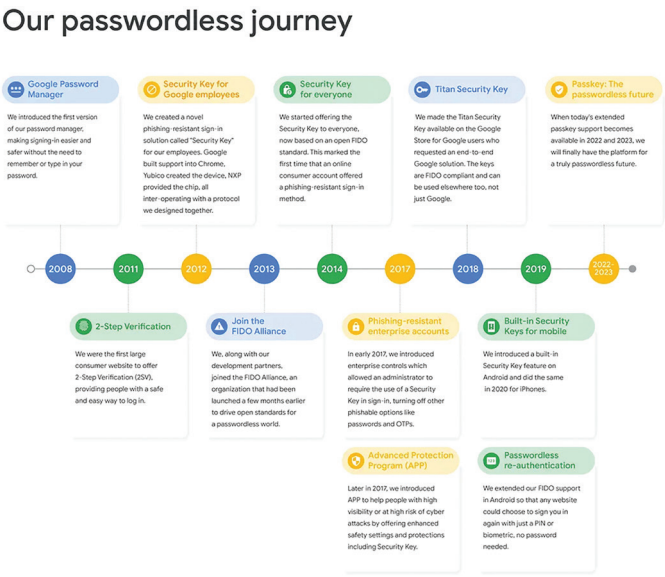


Fig. 2. Google's passwordless journey (timeline 2008–2023)

For security's sake, login needed to be complicated, and for security's sake, human comfort was set aside. Some companies, like Google, publicly aim for a 'passwordless future,' pairing devices to a private key for a simpler and more secure sign-in (Google Safety & Security, 2023). But is getting rid of the password the sole solution? Bringing the login outside of its platform and making it dependent on devices creates more dependencies in other infrastructures.

Furthermore, this pursuit of frictionless, universal security often contradicts established guidelines, such as those from the National Institute of Standards and Technology (2024), which emphasize that digital identity solutions must balance assurance levels with usability. The historical logic of using bodily metrics for identification, rooted in discriminatory practices like anthropometry, finds its echo in modern biometrics. These systems are not neutral; well-documented evidence shows they often fail on darker skin, meaning the very act of login can become a site of exclusion for some users. Adding to that material exclusion from people who lack the means to acquire a device with network access... The command to "prove you are human" then takes on a different, more charged meaning.

The issue is also that the language and looks of security have been universalized: one corporate "design grammar" applied to every context, from banking to gaming. I argue that we can, and must, design authentication systems that prioritize both security and usability without externalizing control or sacrificing autonomy. This thesis explores alternatives that restore proportionality and meaningful reciprocity between users and platforms. The goal is not to sentimentalize login, but to reclaim it as a designed space of encounter—one that can be legible, contextual, and humane.

Ultimately, this work demonstrates how everyday interactions reproduce systems of recognition and exclusion, while providing designers the tools to rethink authentication as a deliberate, situated, and reciprocal act.

"The login experience" is a space of encounter between humans and machines, and can be improved upon.

07 BEGINNINGS OF LOGINS

BEGINNINGS OF LOGINS

The first question this research must ask is: in what context does our current system of authentication exist? Early on, within this questioning, a good amount of reflections came in. The trends of externalising logins did not originate from nothing. This hypothesis rests on the idea that login systems are not isolated inventions but cultural continuities constructed by the ideologies of their time. Which philosophies generated those developments in login experience design?

The act of login, far from being a purely technical necessity, is a routine of recognition with its own historical and cultural roots. It is a social practice, so to speak, in the repetitive and sacralised sense. To "log in" is to cross a threshold; to present oneself in a way that a system acknowledges as valid, and is often repeated multiple times.

But what constitutes "valid" to a system is entirely subjective, despite the objectivity seen within the practice of authentication. This practice has taken many forms across history: from tokens and seals in ancient societies, to anthropometric measurement and fingerprints in the 19th century, to passwords, multi-factor authentication, and biometrics in the digital era. Each stage represents a technical solution certainly, one that is defined by a cultural and political mindset that dictates how identity is defined and constructed, and who controls access. The act of identification begins there, in authentication, and its origins.

FIRST IDEAS OF AUTHENTICATION

Long before the invention of digital systems, human communities devised rituals and instruments for controlling access within their spaces and communities. To authenticate was to demonstrate belonging, and to do so, they exchanged words and writings that only they would know. In this sense, authentication is one expression of what the anthropologist Victor Turner described as a rite of passage: a process of separation, liminality, and reintegration that marks movement from outsider to member. "In this, ritual participants are removed from ordinary society (separation) and enter a space where there is an absence of structure, where they are neither inside nor outside society (liminality), before returning to their previous positions at the end of the ritual process (re-aggregation)." (Haggar, 2025)Authentication is a "rite of entry", a cultural moment where identity was recognized by others and validated through symbolic means.

TOKENS AND SEALS...?

One of the earliest material forms of authentication appeared in Mesopotamia. Archaeological sources describe the use of cylinder seals, which were small carved stones rolled onto clay tablets or containers.

These were used to mark ownership and prevent tampering. According to the Metropolitan Museum of Art, " when seals were impressed on sealings – lumps of clay that were used to secure doors and the lids of storage jars– the seal impressions served to identify their owner and protect against unauthorized opening." (The Metropolitan Museum of Art, n.d.)

Medieval wax seals continued this tradition. Legal historians note that "Seals were the only form of personal authentication in the Middle Ages. Deeds were not usually signed until the sixteenth century."(University of Nottingham, n.d.) Seals could be forged, broken, or stolen, certainly, but their power lay in the shared recognition of their authority. That very act of material recognition through detailed craftsmanship defined authentication.

Fig. 3. Mesopotamian cylinder seal and its impression

WATCHWORDS AND SPEECH...!

Alongside objects, language itself became a credential. The Roman tessera militaris, a watchword distributed nightly to soldiers, accompanied with their tokens ensured that entry into a camp was restricted to those who knew the word. In Epitoma Rei Militaris which is a roman military handbook, Vegetius (a Roman writer from the Late Roman Empire circa late 4th century AD) emphasized the role of this verbal ritual in maintaining cohesion, noting that soldiers who spoke the watchword correctly were admitted as comrades, while those who failed were treated as outsiders."Vegetius, in his Epitoma Rei Militaris, emphasized the role of this verbal ritual in maintaining cohesion: soldiers who spoke the word correctly were admitted as comrades, while those who failed were treated as outsiders. Here, recognition resided in the correct performance of speech." (Vegetius, as cited in Thayer, n.d.)

Some linguists and sources highlight that authentication has always been performative, and performative utterances are powerful because they do not merely describe reality but enact it. To utter the correct watchword was to enact membership."...To utter the sentence (in, of course, the appropriate circumstances) is not to describe my doing of what I should be said in so uttering to be doing or to state that I am doing it: it is to do it." (Austin, 1955)

Fig. 4-6 . Medieval wax seals and document authentication

AUTHENTICATION IS SOCIAL...

Not unlike current IT security concerns, these early systems were never purely secure. Seals could be counterfeited, secret words discovered, and documents forged. Similar to today, in which passwords leak, identities are stolen, and phishing exploits the fallibility of our identifiers. But their value was never in their infallibility. Authentication has always been a negotiation of trust, situated within material culture and collective belief. This negotiation persists, even as authentication migrates from shared symbols to algorithmic proofs. A seal or watchword only "worked" because those within a community agreed to treat it as binding. In this sense, authentication is less about the object itself than about the shared confidence that sustains it.

Seen in this light, contemporary logins (whether password entries or biometric scans) are not fundamentally new. They extend a long lineage of recognition practices in which access is not guaranteed by technology alone or by its supposed objectivity, but by the social consensus and institutional authority that define it. Each design decision in authentication arises from a cultural logic that legitimises certain kinds of proof over others. Yet the persistence of breaches and forgeries kept exposing the limits of trust as a human arrangement. To overcome that uncertainty, thinkers sought a proof that could not be faked, forgotten, or negotiated... They searched for a form of verification that would seem absolute. The answer, they believed, was the body itself.

Fig. 7. Collection of Roman tesserae

BERTILLONAGE AND FINGERPRINTING

The nineteenth century marked a decisive turn in the history of authentication. A token, seal, or pass... Those were now less trustworthy than desired. If earlier systems relied on social recognition, the new ambition was to locate certainty in the body itself. The ideal of an infallible credential gave rise to techniques that transformed the body into data. Under the banner of science, identity became a matter of measurement and classification.This drive to quantify the human body was not born in a vacuum. It was deeply entangled with the colonial and racist ideologies of the era, which sought to create hierarchical classifications of race and "deviance." As historian Simon Cole (2001) documents, the same tools of anthropometry used to identify criminals in Paris were deployed in colonial contexts to classify and subjugate indigenous populations, lending a veneer of scientific objectivity to white supremacist projects.

In 1883, Alphonse Bertillon's anthropométrie judiciaire embodied this shift. Combining photographs with precise bodily measurements (That is: head length, arm span, ear size), Bertillon sought to identify recidivists through a repeatable system of metrics. His method, quickly institutionalised by the Paris police, promised to replace human judgment with standardised evidence. Historian Simon Cole notes that this bureaucratic logic "replaced the marking of the criminal body with the marking of the criminal record" (Cole, 2001, p. 67).

What had once been a social negotiation of trust became an administrative production of identity, through the body as the ultimate identifier.

This period was also one of profound scientific confidence. The dominant discourse of the late nineteenth century was structured around classification, control, and the rational mastery of nature. Figures such as Paul Broca, founder of the Société d'Anthropologie de Paris, extended anatomical measurement into social theory, linking bodily features to hierarchies of race and character (Broca, 1875). Within this context, Bertillonage did more than distinguish criminals: it enacted a belief that human difference could be rendered legible, and thus governable, through quantification.

Fig. 8. Anthropometric classification of head profiles.(Bertillon system)

Yet Bertillon's system proved fragile. It demanded trained staff, careful conditions, and produced errors as it scaled. Fingerprinting, refined by Francis Galton in the 1890s, appeared to offer what anthropometry could not: permanence. "Finger prints," Galton wrote, "are self-signatures, free from all possibility of faults in observation or clerical error; they apply throughout life" (Finger Prints, 1892, p. 168). With this claim, the body ceased merely to be measured and became its own proof. The ridge of the fingertip stood as a natural password. To this day, we see them as immutable, individual, and allegedly incorruptible.

This transition from social to biological proof marked the birth of biometric reasoning: the conviction that truth resides in the body, independent of context or community. In making the body measurable and comparable, modernity redefined authentication as an act of possession by institutions over individuals. It is a perceived logic that continues.

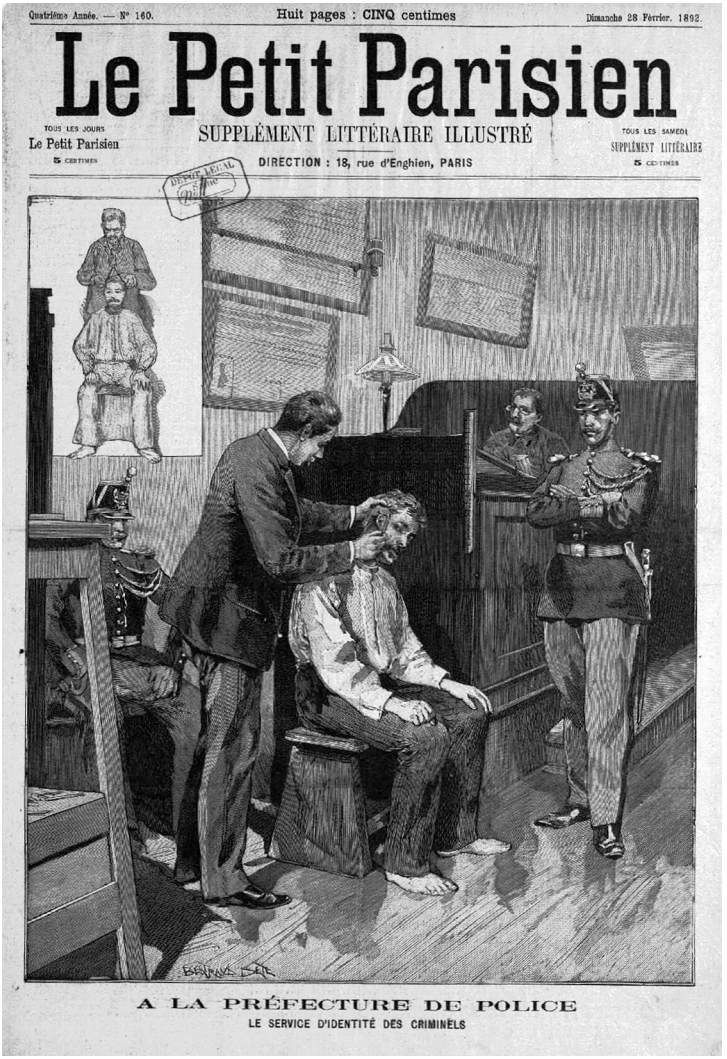


Fig. 9. Criminal identification service at the Prefecture of Police, Paris

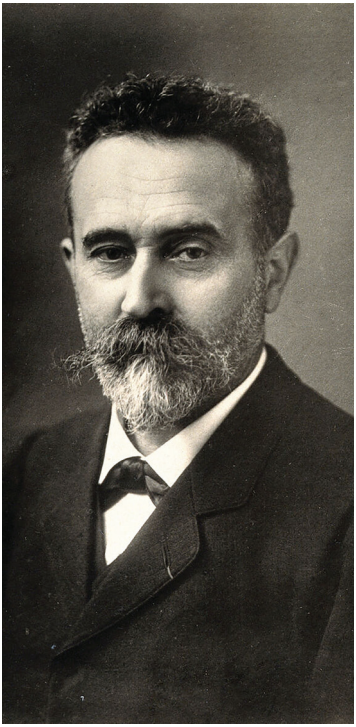


Fig. 10. Portrait of Paul Broca
Fig. 11. Portrait of Alphonse Bertillon

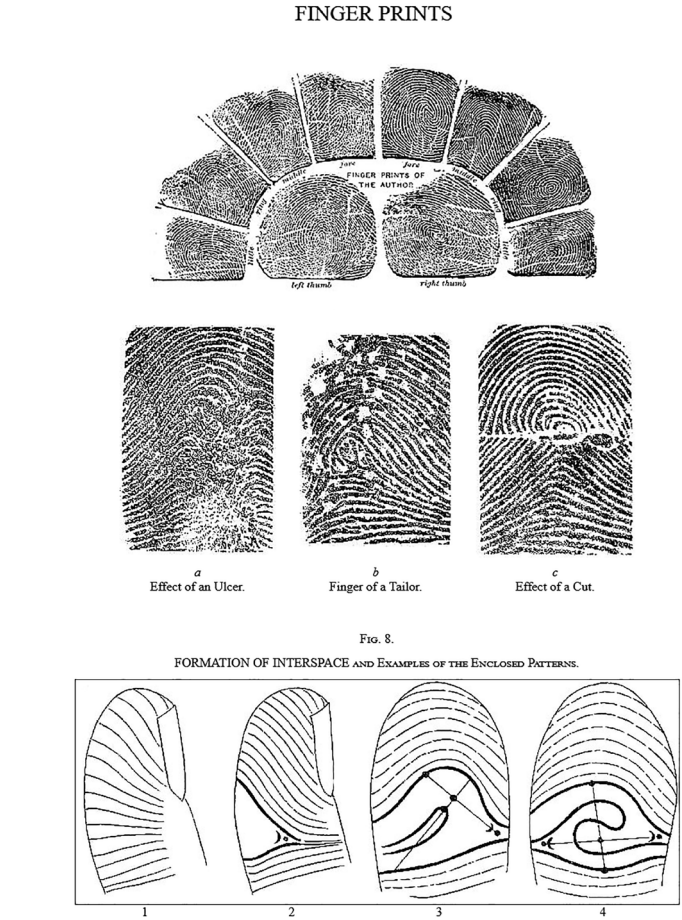


Fig. 12-13. Title page of Finger Prints (1892) & Examples of fingerprint variations and ridge formations

CORBATÓ AND THE INVENTION OF PASSWORDS

The first password was not a grand security innovation but a pragmatic design patch. In 1961, Fernando J. Corbató's team at MIT created the Compatible Time-Sharing System (CTSS) to allow multiple users to share the same computer. Each user needed private storage, and the simplest solution was to separate accounts by a short secret string. As Corbató recalled, "Putting a password on for each individual user as a lock seemed like a very straightforward solution."(McMillan, 2012) What began as a routine partition of computational access introduced the cultural figure of the password, a digital echo of the Roman watchword.

The illusion of control collapsed quickly. In 1966, a minor programming error caused CTSS to display its entire password file as the system's "message of the day." This event produced the first recorded password breach and prompted the introduction of hashed storage[1], later formalised in Multics and Unix.

But the lesson was deeper than mathematics. Even the most rational systems inherit the vulnerabilities of the people who use and design them.[2]

1 Hashed storage refers to a cryptographic process where a password is run through a one-way mathematical function (a hash algorithm). This converts the password into a unique, fixed-length string of characters (a "hash"). The system stores only this hash. When a user logs in, the system hashes the entered password and compares it to the stored hash. If they match, access is granted. This means the system never stores the actual password, so even if the password file is stolen, the original passwords are not immediately exposed.

2 The Multics (Multiplexed Information and Computing Service) and Unix operating systems were highly influential successors to CTSS. They institutionalized the practice of storing hashed passwords in a separate, more secure file (e.g., /etc/passwd in Unix), establishing this as a fundamental security standard for decades of computing.

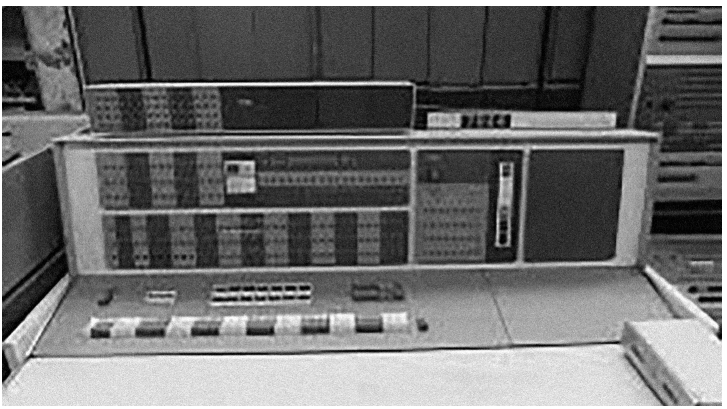


Fig. 14-15. Fernando Corbató with the IBM 7094 computer at MIT & The Compatible Time-Sharing System (CTSS) console

SOCIO-TECHNICAL FRAGILITIES

By 1979, Robert Morris and Ken Thompson had already identified the problem of digital authentication: people are the weakest algorithm. "Human beings being what they are," they wrote, "there is a strong tendency for people to choose short and simple passwords they can remember" (Morris & Thompson, 1979, p. 594)

This was empirically confirmed by Yan et al. (2000), whose research on password memorability and security found that users' choices are inevitably molded by the tension between creating secure strings and the limitations of human memory.

The statement clarified the importance of understanding people within security, as it was a socio-technical problem. Passwords were never purely cryptographic, since users reproduced behaviour within their passwords and security hygiene. These were behavioural interfaces entangled with memory, feeling and habit. A colleague named Peter Ha, whom I informally discussed with, echoed this sentiment beautifully: "A password is a part of you, and it changes with you."

FROM PASSWORDS TO PLATFORMS

As networked life expanded, the single password could not keep pace. Users faced "password fatigue," while large-scale breaches (such as the LinkedIn breach in 2012, the Yahoo breach in 2016, and the Equifax breach in 2017) showed that storing secrets centrally merely multiplied exposure.[3]

The 2012 LinkedIn breach serves as a stark case study: analysis of the leaked (hashed) passwords revealed a heavy reliance on simplistic, easily guessable sequences like 12345, 1234567, and 11111 (Paganini, 2016).

3 These breaches are consistently documented in industry reports. See, for example, Verizon (2017). 2017 Data Breach Investigations Report (10th ed.). https://www.verizon.com/business/resources/reports/2017_dbir.pdf

SWITZERLAND

RANK	PASSWORD	COUNT
1	dominaria	18,556
2	admin	10,064
3	purzi123	7,979
4	Divinorum88	7,672
5	123456	5,708

WORLDWIDE

RANK	PASSWORD	COUNT
1	123456	21,627,656
2	admin	21,030,012
3	12345678	8,274,408
4	123456789	5,673,712
5	12345	3,950,777

Table 1: A comparison of common passwords in Switzerland and globally (2024-2025)

Adapted from: NORDPASS. Most Common Passwords List [online]. 2023 [visited 2023-10-26]. Available from: https://nordpass.com/

Industry responded with layers in an attempt to sidestep the user as the primary vulnerability: combining passwords with tokens, devices, and biometrics. Multi-Factor Authentication increased theoretical security but also fragmented the gesture of access. Users and systems, who had a direct interaction for logging in, are now dispersed across devices, emails, and apps. All of these factors introduced logistical friction while concealing the logic of verification. Recovery processes became the real test of trust: users learned that security could lock them out as easily as it protected them, a sentiment echoed in interviews where participants described the panic of losing access to an authenticator app.[4]

To reduce this cognitive burden, the 2000s introduced Single Sign-On and federated identity systems such as OAuth.[5] By the late 2000s, standards like OAuth formalized delegated access. As was written in 2007 on the release of OAuth 1.0:

"OAuth aims to unify the experience and implementation of delegated web service authentication into a single, community-driven protocol. [...] An open standard, supported by large and small providers alike, promotes a consistent and trusted experience for both application developers and the users of those applications. " (OAUTH CORE WORKGROUP, 2007).

"Login with Google" and "Login with Apple" promised convenience but effectively externalised trust: the act of verification left the platform and entered a corporate infrastructure. Users no longer authenticated to a service, and instead went through an intermediary that authenticated on their behalf. In exchange for simplicity, authentication became infrastructural. The login experience was thus opaque, distant, and dependent.

4 This observation is supported by user interviews conducted for this research. Angela, for instance, stated, "I panicked because the system no longer recognised me," after losing their phone (Personal communication, October 2025).

5 Single Sign-On (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. Think of how logging into Google also logs you into Youtube, Google Drive, etc...

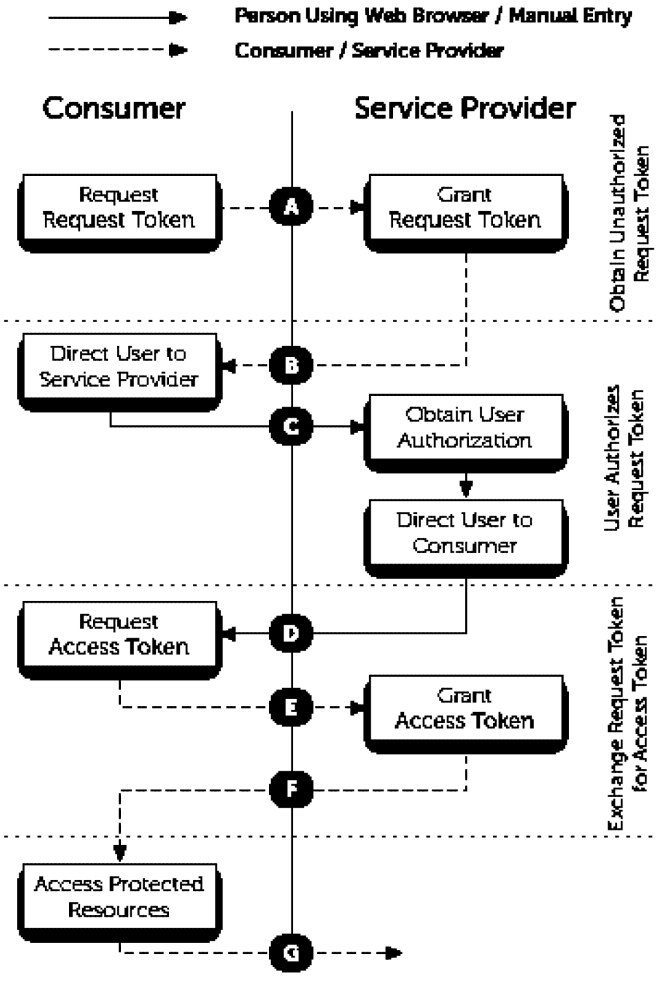


Fig. 17. OAuth 1.0a authentication flow

THE BIOMETRIC TURN

The 2010s extended this logic into the body once again. With Apple's Touch ID (2013) and Face ID (2017), authentication became instantaneous and intimate. "Your fingerprint is one of the best passwords in the world," declared Dan Riccio, Apple's senior vice president of Hardware Engineering. "It's always with you, and no two are exactly alike." (Hughes, 2013).

The rhetoric echoed Francis Galton's 1892 claim that fingerprints were "self-signatures… free from all possibility of clerical error." Biometric devices promise security without effort, yet they also collapse the distinction between person and credential: the user's body is the key.

The same principle underlies the Fast IDentity Online Alliance's "passkeys," which replace passwords with cryptographic credentials bound to devices and unlocked through biometrics. FIDO (Fast IDentity Online) is an open standard developed to eliminate password dependence by using public-key cryptography[6]: one key remains on the user's device, while a paired public key validates access on the server.

Its extensions, WebAuthn[7] and Client-to-Authenticator Protocol (CTAP) as defined by the FIDO Alliance (2023), coordinate communication between the browser, the authenticating device, and the online service. Together, these standards offer robust protection

6 Public-key cryptography uses a pair of keys: a private key (kept secret on the user's device) and a public key (shared with the online service). A passkey login works by the service sending a challenge that only the holder of the private key can answer, proving identity without ever transmitting the secret itself. This is more secure than a password, which is transmitted and stored.

7 WebAuthn (Web Authentication) is a core component of the FIDO standard that allows websites to update their login pages to use passkeys instead of passwords. CTAP (Client to Authenticator Protocol) allows external devices (like a security key or your phone) to work as the authenticator for your computer. Together, they create the infrastructure for a passwordless web.

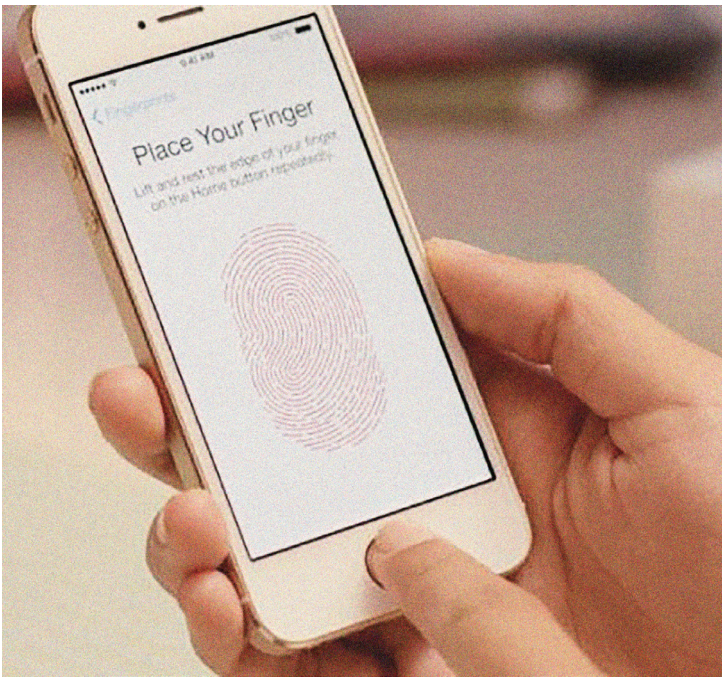


Fig. 18. Apple Touch ID registering screen

against phishing and repeat attacks while minimising visible interaction. Yet they also deepen dependence on proprietary hardware and invisible infrastructures.

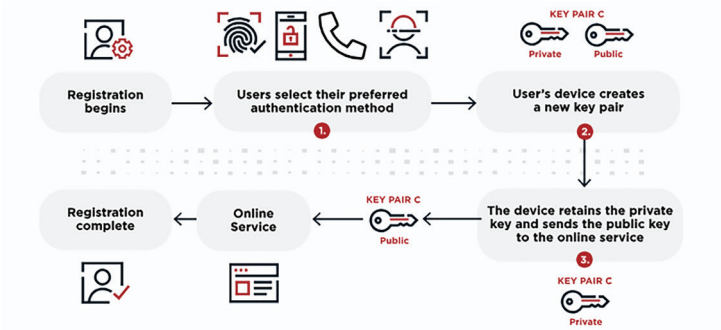
Each advance improves cryptography yet diminishes legibility. The process feels simpler but grows more opaque: the act of login dissolves into the background, beyond the user's comprehension or control.

A REFLECTION ON THE DESIGN OF SECURITY

Contemporary authentication thus inherits a long pattern. From Bertillon's anthropometry to Google's passkeys, every attempt to guarantee identity displaces trust away from the user. First integrated into the body, then into the machine, now into the network itself. The pursuit of frictionless entry creates new forms of distance. This goes beyond a loss of effort taken to login. Indeed, users gain protection but risk losing tech literacy.

The problem, then, is unintelligible friction; wherein effort disperses across devices and interfaces without meaning or relation. Rather than erasing it, design could redirect it: make verification contextual, perceptible, and proportionate. The challenge for authentication design is not to remove the user from the loop, but to re-engage them within it.

Reconsidering login as a design space opens a different possibility. Security could involve users rather than abstract them, through context, memory, and interaction that make the process legible.



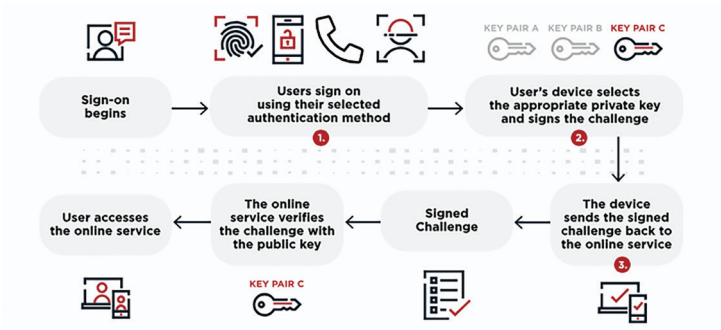


Fig. 19. FIDO authentication sequence: registration process
Fig. 20. FIDO authentication sequence: sign-on process

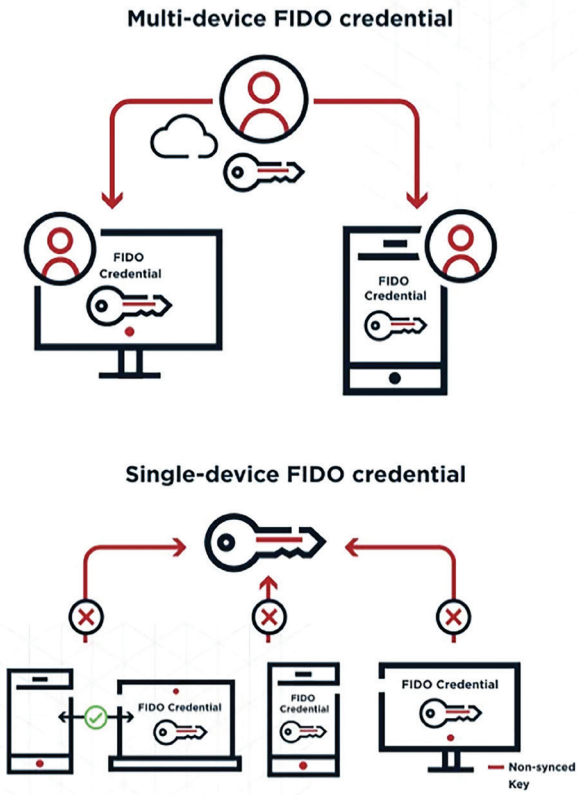


Fig. 21. Single-device vs. multi-device FIDO credentials

08 PROBLEMATIC

CONTEMPORARY CONDITION OF LOGIN

PROBLEMATIC: THE CONTEMPORARY CONDITION OF LOGIN

Contemporary authentication systems promise frictionless access and uncompromising security. Passwords, biometrics, and device-based passkeys operate invisibly, distributed across platforms and infrastructures. This invisibility is not neutral. When authentication is delegated to corporate infrastructures or embedded in proprietary devices, users lose interpretive agency. The process that should confirm identity instead reinforces dependence. As observed in the fieldwork, people describe authentication as confusing, unpredictable, or alienating. Security succeeds technically but fails relationally, since the experience is governed by systems they cannot see or influence.

The problem, therefore, is not that login requires too much effort, but that its friction is perceived by users as meaningless. Verification is dispersed across devices, emails, and biometrics, yet none of these actions invite understanding or provide context. This situation leaves users both over-protected and disempowered, a state that aligns with what the National Institute of Standards and Technology (2016) has identified as 'security fatigue,' which can cause computer users to feel hopeless and act recklessly.

INTERFACES AND SITES OF PRODUCTION

As Alexander R. Galloway (2012) reminds us, the interface is not a neutral passageway between user and system but an active site of production that shapes both. To log in is not simply to gain access; it is to perform the gestures that sustain a structure of recognition and control. Each act of authentication reaffirms the authority of the system, transforming users into compliant participants in its choreography of trust.

In The Interface Effect, he writes, "One must transgress the threshold, as it were, of the threshold theory of the interface. A window testifies that it imposes no mode of representation on that which passes through it. A doorway says something similar, only it complicates the formula slightly by admitting that it may be closed from time to time, impeding or even blocking the passengers within" (p. 40).

Wendy Hui Kyong Chun (2011) extends this argument by showing that interfaces do more than mask power; they make ideology feel like interaction. The login's minimalism, its repetitive neutrality, and its polite reassurance teach users to conflate safety with submission. The seemingly seamless design leads, in fact, to the codification of obedience as usability (p. 59).

As she argues, "Both conceptually and thematically, these interfaces offer their users a way to map and engage an increasingly complex world allegedly driven by invisible laws of late capitalism. Most strongly, they induce the user to map constantly so that the user in turn can be mapped" (p. 59).

From this perspective, authentication produces a behavioural relation. Each prompt ("Verify," "Allow," "Continue") rehearses a micro-performance of obedience. The repetition of these actions transforms security into a daily practice of compliance, and may enhance feelings of reactance in users.

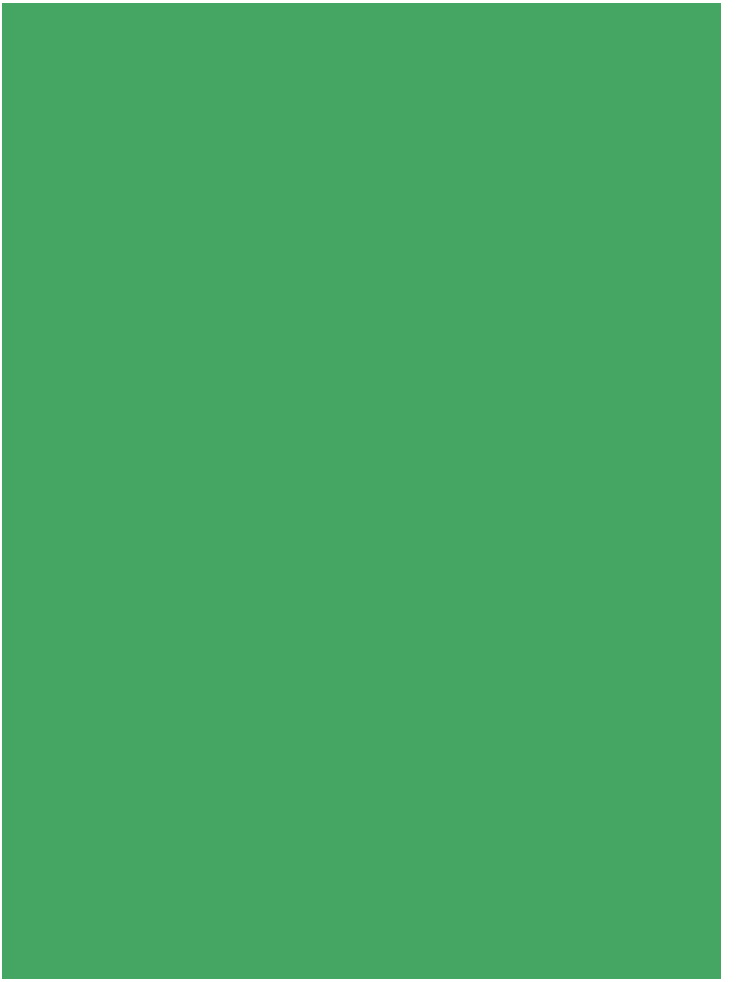


Fig. 22. The Externalisation of Login

THE EXTERNALISATION OF LOGIN

Each new method of authentication (Login with Google, Sign in with Apple, Face ID, passkeys, or two-factor verification) transfers a piece of the user's identity to another entity, both technically and symbolically.

Recognition no longer happens between the user and the platform they wish to access; it now occurs through external infrastructures that authenticate on the platform's behalf. In exchange for convenience, users and designers surrender control over the very process of entry.

This dependency brings a quiet but profound loss of agency. A user may "log in" to an independent service, but the gatekeeping is performed elsewhere. The act of recognition is displaced, abstracted, and standardised. As platforms integrate single sign-on or passkey systems, they relinquish their thresholds to corporate design languages and infrastructural protocols. The login, once a symbolic interface between user and platform, becomes a borrowed window governed by external authority.

The convenience of a universal button hides the political fact that authentication now resides within a few private ecosystems. Designers lose access to the symbolic real estate of the threshold, as the look, feel, and logic of entry are dictated elsewhere.

The problematic nature of contemporary authentication is also reflected and critiqued by a growing body of artistic work. R. Sikoryak's Terms and Conditions masterfully embodies the core issue of opacity: he republishes Apple's entire labyrinthine legal agreement as a graphic novel. The work makes visible the sheer scale of what we are expected to blindly accept, transforming an indigestible wall of text into a readable, breathable narrative. Similarly, projects like Heather Dewey-Hagborg's Stranger Visions warn against the potential for bodily data, the supposed "ultimate password," to be used against us. This work does so by reconstructing faces from discarded genetic material found in trash. Together, such works help demonstrate that the problematic is, as of yet, increasingly relevant, and requires a different and more user-centric approach.

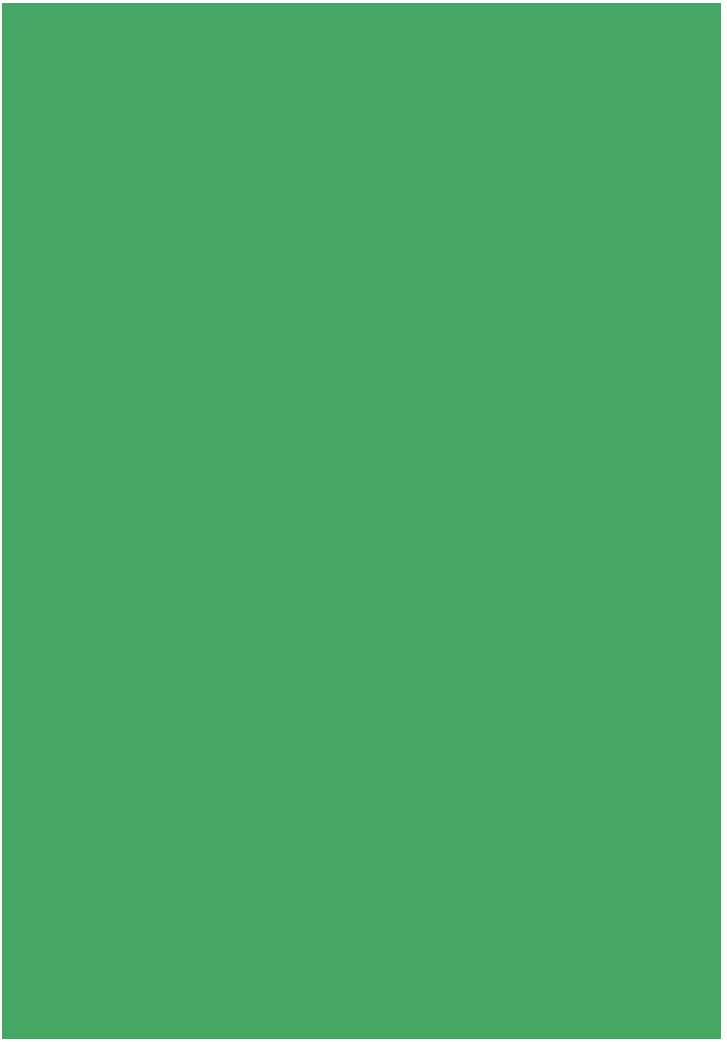


Fig. 23. Contemporary Authentication Journey

TOWARD A SITUATED DESIGN OF SECURITY

The problem of contemporary login design is therefore structural. It achieves universality and predictability, by removing context and visibility from the user. It builds trust through consistency of design, looks and methods, but erodes understanding in the process. The user's role is reduced to one of procedural confirmation rather than informed participation

There is a palpable tension between the demand for seamless, universal access and a growing public resistance to the datafication of identity. The Swiss public's skepticism towards the e-ID law, rooted in fears of data theft and surveillance, alongside the vehement backlash against intrusive age-verification measures on social platforms, reveals a critical juncture. Users are increasingly aware that the price of entry is often their biometrics, their anonymity, or their personal data, leading to a climate of distrust where the command to "prove who you are" feels less like a security measure and more like an extraction of private data.

Design can intervene in this imbalance. Rather than removing friction, it can redefine it, making authentication contextual, perceptible, and situated in experience. The challenge is to imagine login as a moment of engagement rather than surrender, where security and comprehension reinforce one another. But how does one do that?

This problematic situates the core of this research: to explore how authentication might be redesigned as a proportional, contextual, and participatory act, one that strengthens digital security by giving users a meaningful role within it. The following research aims to figure out, first and foremost, how users feel and interact within the context of the "login experience."

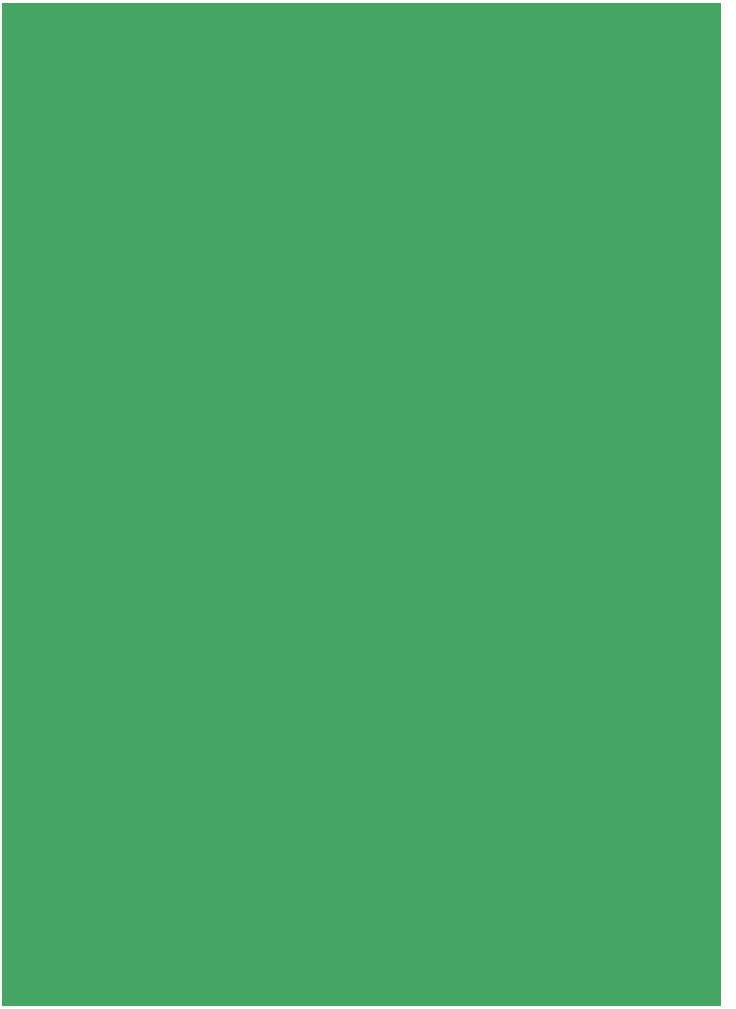


Fig. 24. Consequences of Login Externalisation

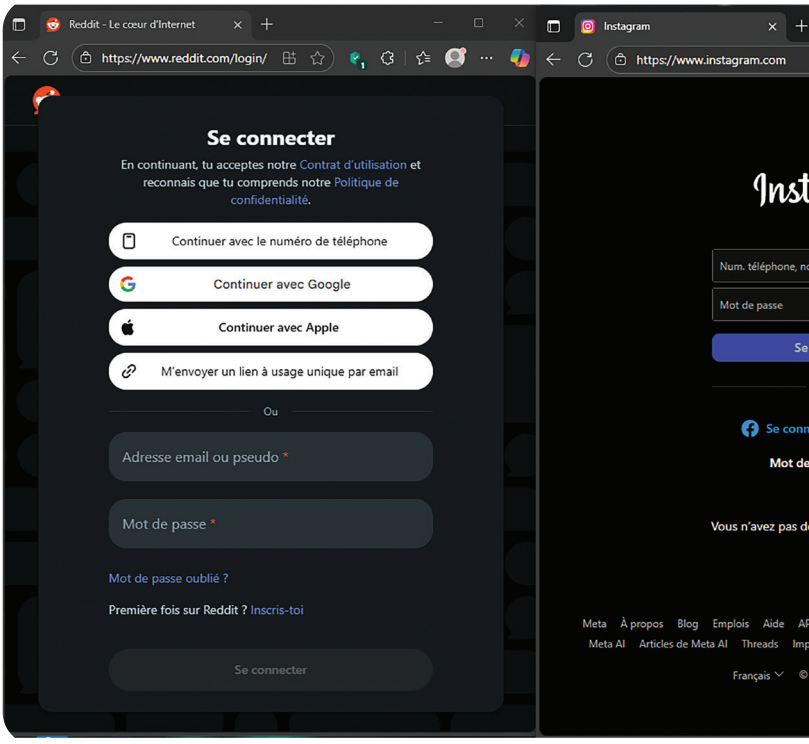
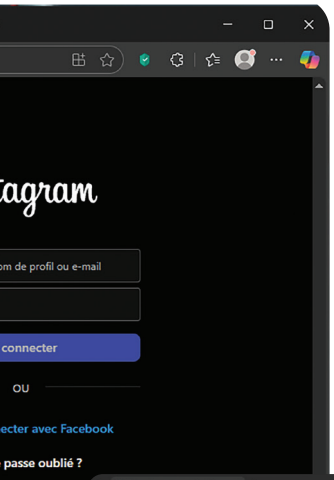
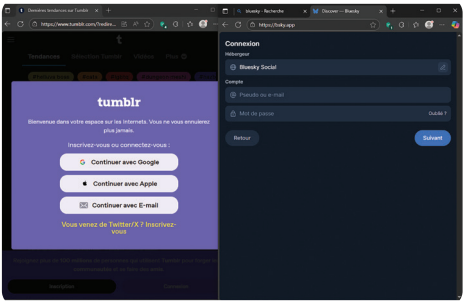
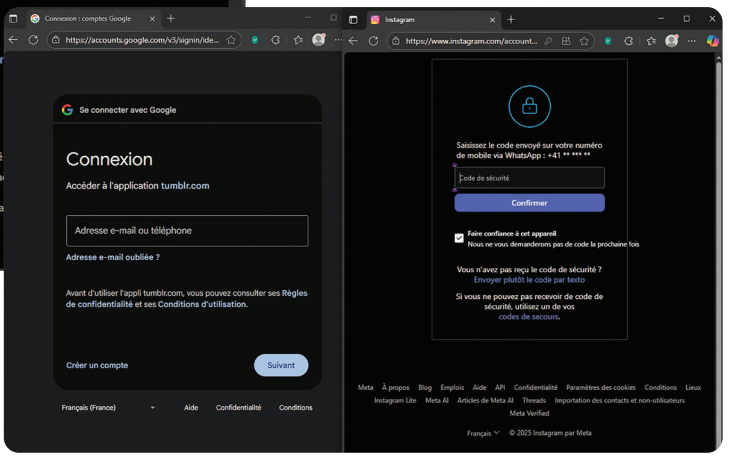


Fig. 25. Reddit login interface and Google sign-in prompt
Fig. 26. Bluesky login interface
Fig. 27. Tumblr login interface
Fig. 28. Google account setup: address promp
Fig. 29. Two-factor authentication screen (Instagram)


agram
m de profil ou e-mail
connecter
OU
ecter avec Facebook
passe oublié ?
e compte ? Inscr
Confidentialité
ortation des conta
2025 Instagram pa


tumblr
Bienvenue dans votre espace sur les Internets. Vous ne vous ennuierez plus jamais.
Inscrivez-vous ou connectez-vous :
Continuer avec Google
Continuer avec Apple
Continuer avec E-mail
Vous venez de Twitter/X ? Inscrivez-vous
Connexion
Hébergeur
Bluesky Social
Compte
Pseudo ou e-mail
Mot de passe
Oublié ?
Retour
Suivant


Connexion | comptes Google
https://accounts.google.com/v3/signin/ide...
Se connecter avec Google
Connexion
Accéder à l'application tumblr.com
Adresse e-mail ou téléphone
Adresse e-mail oubliée ?
Avant d'utiliser l'appli tumblr.com, vous pouvez consulter ses Règles de confidentialité et ses Conditions d'utilisation.
Créer un compte
Suivant
Français (France)
Aide
Confidentialité
Conditions
Instagram
https://www.instagram.com/account...
Saisissez le code envoyé sur votre numéro de mobile via WhatsApp : +41 ** *** **
Code de sécurité
Confirmer
Faire confiance à cet appareil
Nous ne vous demanderons pas de code la prochaine fois
Vous n'avez pas reçu le code de sécurité ?
Envoyer plutôt le code par texto
Si vous ne pouvez pas recevoir de code de sécurité, utilisez un de vos codes de secours.
Meta À propos Blog Emplois Aide API Confidentialité Paramètres des cookies Conditions Lieux
Instagram Lite Meta AI Articles de Meta AI Threads Importation des contacts et non-utilisateurs
Meta Verified
Français © 2025 Instagram par Meta

09 RESEARCH

FIELD, SURVEYS, INTERVIEWS

METHODOLOGY AND RESEARCH DESIGN

This research combines observation, user inquiry, and speculative experimentation to understand users' relationships with modern authentication methods. Rather than pursuing quantitative generalisation, the study seeks to find situated insight, in how authentication systems shape, and are shaped by, everyday work and perception. Because authentication is embedded in everyday gestures, its analysis requires methods capable of addressing lived, situated interactions. Research-through-design supports this by allowing iterative reflection between design artefacts, contexts and theories of recognition.

SCOPE AND PHASES

The research developed in three interrelated phases:

Field Observation — ethnographic observation within a clinical-administrative healthcare environment (approximately three weeks of 40h of observation, over multiple shifts, Between June 23rd 2025 and July 11th 2025).

User Inquiry — an online survey (n = 20 valid responses) and seven semi-structured interviews exploring users' perceptions of login, security, and trust. (In September 2025)

Prototype research — design experiments that re-interpret authentication as a situated or playful interaction. (From September 2025 to October 2025)

DATA COLLECTION AND PARTICIPANTS

Field Observation — Conducted in a public-sector healthcare institution. Notes documented the frequency of authentication, points of friction, informal workarounds, and the spatial organisation of access points.

Survey — Distributed via professional and personal networks; respondents represented healthcare, education, IT, and administrative domains. Questions combined multiple-choice and open-ended items to capture attitudes

toward passwords, two-factor authentication, and recovery procedures.

Interviews — Seven participants (One healthcare worker, two IT engineers, two finance employees, one general user) were interviewed for 30–60 minutes each. Conversations focused on authentication routines, perceptions of ownership, and emotional responses to friction and dependency.

ANALYTICAL FRAMEWORK

Transcripts, notes, and survey responses were recorded qualitatively. Recurring ideas (friction, externalisation, ownership, and literacy) emerged through iterative comparison and were used as thematic axes in the analysis that follows. Rather than measuring frequency, the analysis identifies qualitative patterns that reveal how users experience their login experiences, and relationships with platforms they use.

ETHICAL CONSIDERATIONS

All participants were informed of the study's aims and of their right to anonymity and withdrawal. No personal identifiers or patient data were collected.

OUTCOME AND RELEVANCE

This methodological design connects empirical observation with speculative design. The field and user studies reveal how contemporary authentication practices distribute effort, dependence, and literacy. The subsequent speculative and experimental phases test how these relations might be redesigned to produce security that is robust as well as comprehensible and proportionate to context. But first, to ground this theory in the material reality of daily work, field research was conducted in a setting where the stakes of authentication are immediately tangible: a military healthcare-administrative setting. Here, the abstract consequences of externalisation and opaque design become vividly clear, impacting data as well as patient care itself.

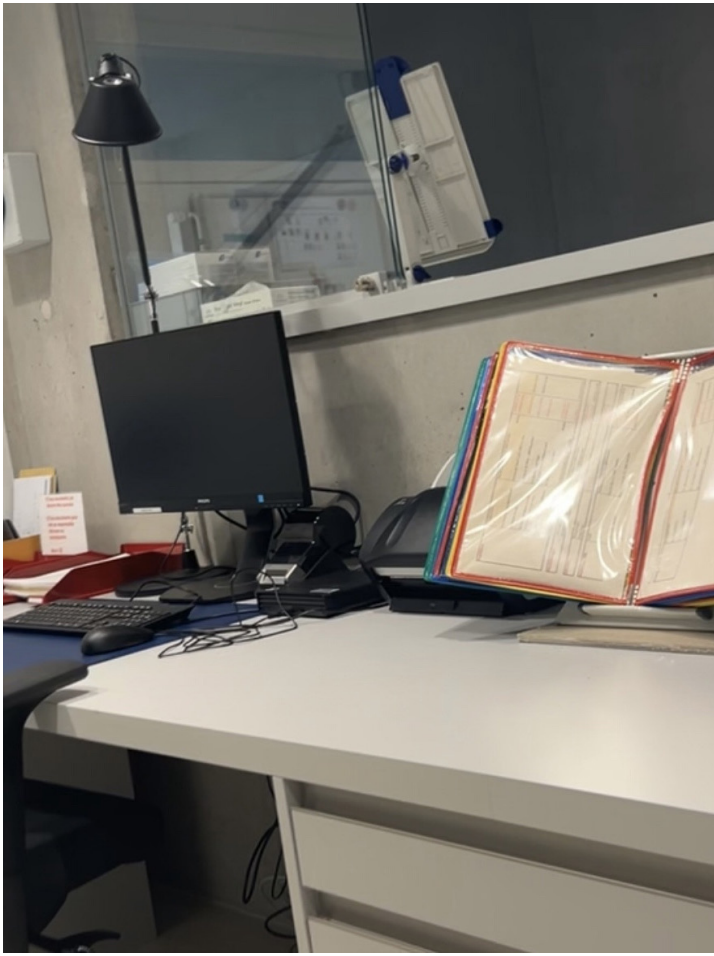
FIELD RESEARCH — ADMINISTRATIVE HEALTHCARE CONTEXT

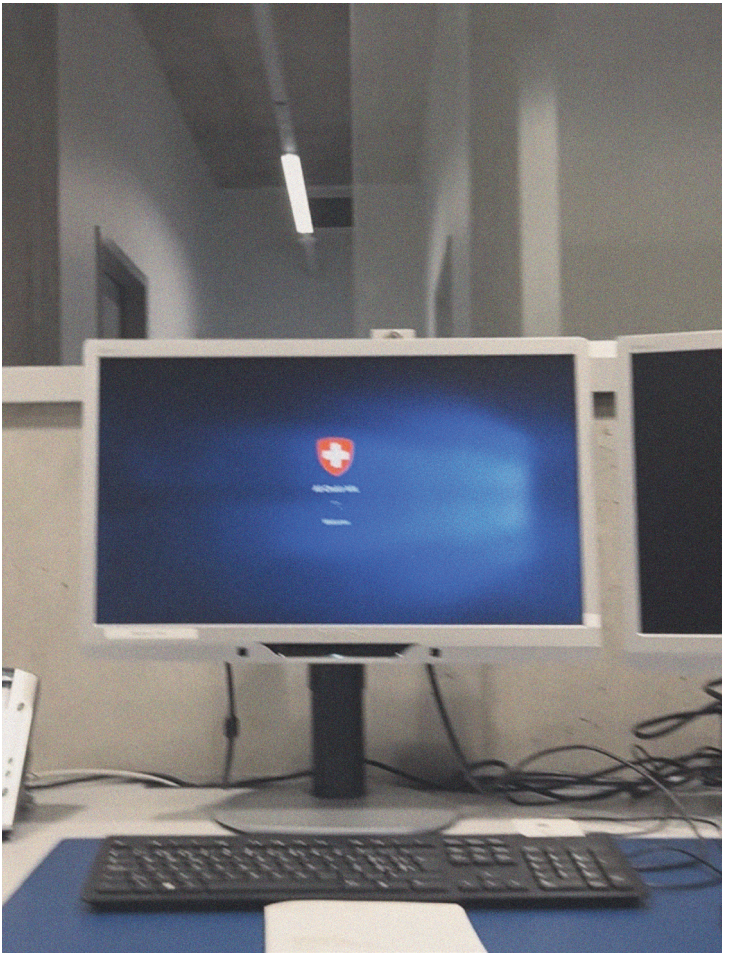
In a military healthcare-administrative setting, authentication processes illustrate the broader policy shift toward total digitalisation. Access to facilities and digital infrastructures was mediated by a single smartcard issued through a central authority. Activation required identity confirmation via distant IT services located in Bern (Switzerland), including verification of personal details and coordination with on-site technicians who could later revoke access remotely. This procedure often delayed healthcare work for several hours or days, leaving staff dependent on both human and bureaucratic intermediaries to perform basic tasks, and sometimes impeding on crucial health procedures.

The card simultaneously served as both a physical and digital key. Staff were required to insert it into terminals to access medical data systems, yet the same card was also necessary for entering or exiting the building. The result was an operational conflict: to remain authenticated digitally, the user had to stay physically anchored to the workstation. Leaving the card in a terminal was a risk for security; removing it meant immediate disconnection. However, since it was impossible to remain at the workstation at all times due to growing patients' needs, the card was left unattended for quite a good amount of time.

Some staff resorted to informal workarounds (borrowing cards, leaving terminals open, or sharing credentials) to sustain workflow continuity. These practices, while technically insecure, represented pragmatic responses to inflexible design. Staff also reported being locked out of the infirmary numerous times, as a result of leaving the card on-site for convenience's sake.

This situation exposes the tension between centralised security and a need for local autonomy. Authentication, intended to protect sensitive information, became a mechanism of constraint.This echoes the problematic's argument that security, when excessively externalised, immobilises the very agents it is meant to empower. The feeling of agency was displaced from those responsible for patient care to distant infrastructures capable of granting or revoking access at will. Security here functioned more as a mode of control that immobilised the actors it sought to safeguard.

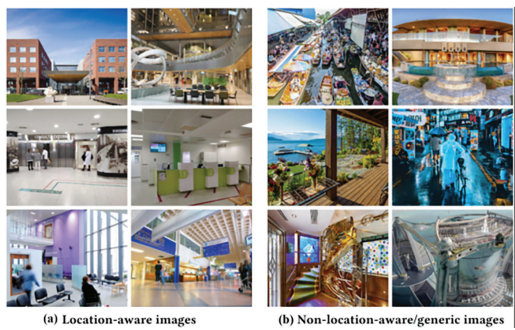




COMPARISON WITH DUOPASS

The failure of this hardware-based system highlights the need for a different approach, perhaps one that is both secure and aligned with human workflows. This need is addressed by research into cognitive authentication models, such as the DuoPass study (Liu, Yadav, Ganti, and Kasiviswanathan, 2022). Developed specifically for healthcare environments, DuoPass employed a dual-password mechanism that paired user-chosen images with textual cues. By anchoring the login in associative memory and personal context, the system improved memorability, reduced lockouts, and increased perceived security. Unlike the rigid smartcard, DuoPass transformed the login from a procedural hurdle into a meaningful, user-driven gesture, demonstrating that robust authentication need not depend on external hardware or create workflow bottlenecks.

The contrast is stark. Where the smartcard system of the previous field research produced friction and workarounds, a system like DuoPass aims to generate ease-of-use and comprehension. This case demonstrates that security can be strengthened by integrating contextual and cognitive design principles, rather than by multiplying external layers of verification that ultimately displace user agency.



(a) Location-aware images (b) Non-location-aware/generic images

USER SURVEYS AND EVERYDAY PATTERNS

A qualitative online survey was conducted in September 2025 to explore how users perceive authentication in their daily digital lives. Twenty participants between the ages of 21 and 36 responded. Most were based in the United States, with others in Switzerland, the Netherlands, Germany, Sweden, Canada, Hungary, and France. Respondents described themselves through a wide range of gender identities, with a notable proportion identifying as nonbinary or agender. Many reported long familiarity with computers, several having “been online for most of [their lives]” or “introduced to computers through public schooling in the 90s.” The sample, while small, represents a digitally fluent and socially diverse group

Most participants used both phone and computer daily, often across work and leisure contexts. Tumblr, Discord, YouTube, and Gmail were the most common platforms, indicating hybrid personal–social–institutional use.The survey thus captures authentication as it occurs across overlapping ecologies of use, rather than within a single service.

TEXTURES OF FRICTION

Younger respondents (21-26) express visceral frustration with additional security steps ("if a login takes more than typing a bit and clicking enter i explode" and "Two-factor is so annoying sometimes") while simultaneously showing deep emotional attachment to their digital spaces ("My dragons :)" for Flight Rising accounts). This conflict illuminates how externalized authentication disrupts the intimate relationship between user and platform, transforming what should feel like "coming home" to one's digital belongings into a bureaucratic checkpoint. Participants also consistently described login as a minor but persistent friction. It is seen as an act that interrupts flow, produces mild irritation, and occasionally escalates into crisis. Notably, a few specific design patterns concentrated frustration.

TWO-FACTOR AUTHENTICATION'S BURDEN

Phone-based verification was the dominant source of frustration.

> What is the most frustrating moment, question or action you face when logging into a website?
>
> "Anything that asks me to confirm who I am - a text to my mobile, a requirement of my face, or something. Any "extra" "safety" step. I do detest 2-factor authentification - something that was implemented in my workplace not long after I started working there, and it makes it even more impossible to log in to my work email and other services."
>
> "Two-factor is so annoying sometimes. I do understand it's for heightened security, but sometimes bouncing between my phone to search for a code or an email or opening a separate app becomes clunky and inconvenient."
>
> "Any time a website refuses to accept a password to login (e.g. 'check your e-mail for a code'), or requires 2FA (not everyone has a phone nor should)."

Across these statements, authentication's externalisation becomes literal: a process that migrates from one device to another, demanding the user's attention and physical effort.

The frustration was more so linked to disproportion. The asymmetry between the perceived sensitivity of the task and the level of verification demanded generated user frustration.

The accessibility dimension emerges as a crucial but underexamined aspect of the externalisation critique. Multiple respondents highlight systemic exclusion: "not everyone has a phone nor should" and the cascading lockouts when "phone broke, locked out of everything that needs verification codes."

CAPTCHA AND UNCLEAR LIMITS

CAPTCHAs, re-entry limits, and similar "proofs of humanity" were another recurrent theme.

> What is the most frustrating moment, question or action you face when logging into a website?
>
> "Telephone number. I hate when the stupid thing asks to text me. D2L and other college related sites especially want my phone number way too often. Also I Hate Captchas. "
>
> "If it requires me to do the photo captcha."
>
> "When the website won't tell me how many chances I have left to type in my password."

Such mechanisms, meant to confirm humanness, often reversed trust by making participants feel scrutinized or distrusted. Rather than reassurance, they generated doubt about system transparency.

> CROSS-DEVICE DEPENDENCE

Some frustrations pointed toward infrastructural dependence—authentication spread across multiple connected devices.

> What is the most frustrating moment, question or action you face when logging into a website?
>
> "Having to use my phone all the time. Sometimes i'm out of battery, or my phone is charging in another room. Having to wait or physically interrupt what i'm doing to get up and check an SMS or something is annoying. I use to have a 2fa app on my PC that discontinued the app and now is exclusively on mobile. WHY??? Or more generally, the 'suspicious actions' login you out or google suddenly deciding they're not sure you're you and needing extra email confirmation or other steps to let you in."

Here, the very architecture of convenience introduces fragility. A broken phone or a missing secondary device may lock the user out entirely, revealing how identity has been outsourced to hardware. At the same time, this tendency does bring in the notion of material dependency. For those that lack phones and other devices, it creates material exclusion.

LOCKOUT

Lockouts, though relatively rare, were among the most emotionally charged experiences.

> When was the last time you were locked out of an account?
>
> "Genuinely a few days ago. My phone broke, until it's fixed I am locked out of any website that wants to send a verification code to my phone number or wants to contact my phone to allow me to login."
>
> "Two years ago I was locked out of discord for joining too many servers. I could luckily recover it, but I needed to give a phone number."
>
> "Just last week actually! I was trying to log into my banking app and I must have typed my password in wrong so I was rejected, then assumed I had remembered the password wrong and started trying different passwords until I got locked out. It wasn't too bad to get back in, but the whole process did feel a bit clunky at times."

Lockout marks the moment when authentication ceases to be an invisible background operation and becomes a breakdown of trust. Measures intended to protect the user can generate anxiety, exposing a contradiction at the heart of the system: the very mechanisms designed to ensure safety can make users more vulnerable when they fail.

WHAT COUNTS AS 'GOOD' LOGIN

Positive experiences were defined less by pleasure than by absence of disturbance.

AUTOMATION AND BIOMETRICS

What's a login experience you actually liked or found satisfying?

"The iPhone's face recognition has made so many of my logins on my phone smoother. It's a double-edged sword. A lot of people don't trust the facial recognition... but for me personally, I've found it useful."

"Apple's Touch ID Fingerprint login was satisfying."

Biometrics were accepted when seamlessly integrated into personal devices—where login merged with gesture. Even so, participants remained aware of the trade-off between convenience and data exposure. Users who've adopted biometrics (Face/Touch ID) report more satisfaction, while those relying on SMS/email 2FA express consistent frustratio

PREDICTABILITY AND MEMORY

What's a login experience you actually liked or found satisfying?

"Using my password manager to fill in the login details on a website. It saves time and gives the satisfaction of feeling secure."

"When my details are properly remembered and no dual factor authentication is needed."

Trust was cemented in consistency from the ground up. A good login works as expected, and behaves the same way every time.

CONTEXT AND PROPORTIONALITY

Several responses articulated a pragmatic scale of tolerance: greater security for high-stakes platforms, minimal friction for low-stakes ones.

> What other ways do you think online platforms could use to identify you?
>
> "Im genuinely not sure. Facial recognition isn't always feasible for everything, and some websites like banking managers or government websites (to name a couple) could benefit from added security. At this point, it's about convenience, which is a constantly moving target and could be hard to pin down."
>
> "I'm honestly not sure. I can understand calling and texting (as from a bank) being important, but I do hate it. Just lemme in. But yeah no I don't know. Echolocation would be bonkers, though."

This confirms a proportional approach to friction. The presence of barriers does not irritate, however their misplacement does. Participants accepted friction as meaningful only when its intensity matched perceived risk.

Device ecosystems reinforced this logic:

> Within a day, how many times do you think you login, or engage in an act that requires you to confirm your identity online or with a device?
>
> "Outside of work there is the login into my Desktop. Most of my frequently used applications are already logged in when I start them up, so I don't often have to login once im in my computer. When I need to make use of services im not automatically logged into, I use a password manager to login, thus requiring me to login to the manager first before login into the service I intend to use. My phone on the other hand requires a login attempt every time I try to use it, which intermittently throughout the day adds up."

Predictable devices produced calm; inconsistent ones produced alertness.

CONTROL, PORTABILITY, CONSENT. OWNERSHIP.

Almost every participant agreed in principle that accounts "should belong" to them, but meanings diverged.

> Should your online accounts belong to you? What does online ownership mean to you?
>
> "Yes. I do feel like I have a too-simplistic view of online ownership, but my account is my account, which means it's mine and for me. My things :) and also my responsibility."
>
> "Yes and no? I think you should have the right to keep everything on an account you make, but if this is an account on the internet that means somewhere there has to be a server holding that data. [...] The same goes for an account, I think it's right for it to be in your ownership, but the thing is, you're not the person who has your data. Someone else has that data, so you don't have control over it. "
>
> "Yes. It's hard to articulate. But at the very least, even if my account is technically 'borrowed' or more of an admission ticket, the things i upload are mine. This is important to me as someone who does art. Even if the owner of the site disagrees, preserving the illusion that I own my account by not messing with it is prefereable."
>
> "Preserving the illusion that I own my account by not messing with it is preferable"

Ownership, in these accounts, is relational rather than legal: it concerns the right to access, export, and consent. Users equated ownership with autonomy: the ability to enter and exit on their own terms, to recover what they contributed, and to refuse unwanted extraction. Participants tied ownership to reversibility and to informed consent:

> Online ownership to me means getting to control who knows what about me. Why is it so difficult for me to find an old tumblr post or a tweet that I know the exact wording of, but if someone knows my phone number they can find my address and the contact information of everyone I've ever known? Why do so many people (at least where I live) seem so eager to take away our right to privacy online and who stands to benefit from that? If I can't own my online accounts, then so be it. But these people are insane if they think I'm going to upload my drivers license for the chance to look at some posts, you know?"

For several, ownership was also an ethical stance against data extraction:

> "Yes. I think it should be illegal for data brokers to sell your information online. (getting spam mail and stuff for example eventho you never used you gave out your e-mail for that.) also all the AI stuff used to scan your pictures/ art and text to train an engine shouldn't be allowed since you never gave consent to it. Only because you choose to share something on a social media platform shouldnt mean you forfeit ownership of it."

RELUCTANCE AND LIMITS

Most participants expressed resistance to intensified identification procedures.

> What other ways do you think online platforms could use to identify you?
>
> "They should leave me alone forever!"
>
> "Ha, nothing else than an account made with name and password is neccessary is it? I loathe even giving away my email if i'm being quite honest. "

Alternative methods such as passkeys or facial recognition were mentioned but rarely endorsed with enthusiasm. Even those who valued convenience showed awareness of its potential for

overreach. Identification, for this group, was acceptable only within clear, voluntary limits

> What other ways do you think online platforms could use to identify you?
>
> "They could do all kinds of evil stuff, like requiring government ID or assigning a token to the hardware. Anonymity is a very important part of the internet."

Participants understood identification as a trade-off between privacy and predictability, and few wanted new forms of "trust."

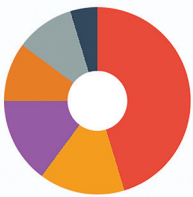
INTERPRETATION

The survey situates plausible user relationships. Reactance towards extra-steps and the externalisation of login underlines the problem posited at the start of this research. Users felt dejected when login became opaque, delegated, or imposed. Security was experienced emotionally, as it was something felt rather than only reasoned. Predictability and proportionality anchored trust more effectively than transparency or novelty. In design terms, the findings emphasize situated friction: effort that communicates intentions behind the steps taken towards security, rather than suspicion, systems that respect reversible boundaries, and ownership conceived as the right to exit, archive, and choose.

The survey thus provides the empirical base to the claim that authentication should evolve into an interactive act of co-recognition, in which both user and platform acknowledge one another's boundaries and capacities.

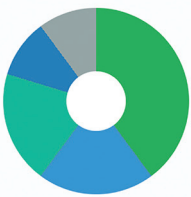
Login design should respond to its context, not only in terms of security level but also of aesthetic and experiential coherence. When authentication inherits the tone and texture of its environment, it ceases to interrupt and instead becomes part of the experience.

"What is the most frustrating moment, question or action you face when lo



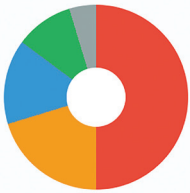
2FA/Phone Verification Hatred	45% (9 responses)
Phone Unavailable/Battery Issues	15% (3 responses)
CAPTCHA/Verification Loops	15% (3 responses)
Account Lockouts	10% (2 responses)
Password Problems	10% (2 responses)
Other Issues	5% (1 response)

"What's a login experience you actually liked or found satisfying?"



Biometrics (Face/Touch ID)	40% (8 responses)
Password Managers	20% (4 responses)
Simple Password Entry	20% (4 responses)
SSO (Google/Apple)	10% (2 responses)
No Good Experiences	10% (2 responses)

"Should your online accounts belong to you? What does online ownership



Strong Yes - "Obviously mine"	50% (10 responses)
Conditional - "If I pay/create"	20% (4 responses)
Pragmatic - "Data portability"	15% (3 responses)
Technical - "Decentralized solutions"	10% (2 responses)
Uncertain/Fatalistic	5% (1 response)

"Within a day, how many times do you think you login, or engage in an act identity?"

High Frequency (20-50+ times)	35% (7 responses)
Medium (5-15 times)	20% (4 responses)
Low (1-5 times)	20% (4 responses)
Variable/Context-dependent	15% (3 responses)
Rarely/Almost Never	10% (2 responses)

INTERVIEWS; THE LIVED EXPERIENCE OF LOGIN

To complement the historical and theoretical framing of authentication, a series of semi-structured interviews was conducted between June and October 2025. Participants were drawn from different professional contexts: healthcare (Angela), government IT (Finn and Emeric), finance (Rami and Serena), and everyday consumer use (Idris). The goal was not to produce generalizable data but to understand how people describe and manage the act of logging in in their daily work and personal routines.

Participants spoke of login as a repetitive negotiation between convenience and control. They were aware of the security measures protecting their data, but often described them as excessive or inconsistent. Some had learned to adapt (saving passwords, synchronising apps, or using Face ID) while others had developed workarounds or avoidance habits. What emerged most clearly was a sense that login design has stagnated: that its gestures are now predictable, mechanical, and frustrating, particularly when recovery processes fail. For some, the problem was not the need to verify identity but the absence of design sensitivity, as systems felt indifferent to context or use.

FRICTION

For many participants, friction is both nuisance and reassurance.

Serena, who works in auditing, described a login chain that included a password, a CAPTCHA, and a text message confirmation. "It's annoying," she said, "but at least I know nobody will hack my account, because there are so many steps." The irritation became part of her sense of protection: the delay made her feel safer. The presence of friction, regardless of if it was a source of true online protection or not, provided a sense of security and trust towards the system's judgment.

Angela, a psychology student working in healthcare, voiced the opposite side of that conflict. Multi-factor authentication at work and school initially felt excessive, and when her phone broke and she lost access to the authenticator app, the same friction turned to panic. "If you don't have much affinity with technology,

it's really hard to use that stuff once it doesn't work the way it should," she said. The process that once comforted her became a barrier that only a technically literate user could overcome.

Emeric, an IT project manager working for the Canton of Neuchâtel, situated himself between those two extremes. From his professional standpoint, security is complex albeit poorly communicated: "It's very uniform and not necessarily the easiest for users," he explained, noting that even government platforms that prioritize safety often disregard user experience. "How do we manage when we have several passwords to remember or for different platforms? And then we see all kinds of practices and derives with post-its on the screen…".

These contradictory feelings point to a common pattern: security communicates itself through resistance. Yet friction without communication breeds anxiety. This is the critical distinction between mere obstruction and meaningful effort. The DuoPass study demonstrates that when friction is translated into comprehension (when the effort of login itself becomes a legible, even meaningful, interaction) it preserves a sense of security without the accompanying punishment. This transformation from an obstructive checkpoint to a coherent gesture is what current systems so rarely achieve.

EXTERNALISATION

Externalised authentication was accepted by some participants, rejected by others. Finn, who works in government IT, described a pragmatic trust in official systems: "I don't mind the tax office tracing me; that's the point. But Facebook or Uber Eats don't need that justification." For him, externalisation is legitimate only when socially mandated; otherwise, it becomes surveillance without a contract. He further crystallized the ideal of user-centric authentication by defining a "good login" as one where "you can confirm you are the owner of an account, but where the account… cannot be used to confirm that you are the owner." This distinction captures the critical difference between proving control and disclosing identity that most contemporary systems blur.

Emeric elaborated on this institutional trust from an insider's view. He described how many systems he manages depend on

authentication chains that users "don't necessarily understand," which produces dependence rather than literacy. Yet even he relies on a password manager to handle the complexity of his multiple roles and accounts—an arrangement he finds convenient but precarious. "I like when it automates everything," he admitted, "but I also know that every password manager can fail. There's always a breach somewhere.",then explained a breach in his previous password manager caused him to switch to a new one. The security that comforts him is simultaneously the source of vulnerability, illustrating how externalisation distributes risk away from the user only to return it through systemic fragility.

Angela's experience exposed the emotional cost of this dependence. When her authenticator stopped working, she realised her identity was tethered to her phone, and the subsequent loss of it caused much more damage. "I panicked," she said, "because the system no longer recognised me."

Together these accounts suggest that externalisation is not inherently problematic; it becomes so when it is applied uniformly across contexts that do not demand it. In practice, dependency on opaque infrastructures shifts the burden of trust outward, while leaving the user responsible for failures they cannot fix.

OWNERSHIP

Ownership was the most fragile and emotionally charged theme. Idris, a restaurant worker, felt that his accounts "never really belonged" to him: "They can delete everything tomorrow." He described a sense of temporary tenancy within platforms, a feeling echoed by Angela, who said she only felt ownership when she could decide whether her account was deleted. "I guess really owning it would mean having your name on it and having a say on where it goes," she reflected.

Finn articulated a key distinction that resonates with current design debates: "A good login should confirm ownership, but not identify who I am and what constitutes me." His remark captures what many authentication systems overlook: the difference between control and disclosure. Users do not necessarily want to be known; they want to remain in charge, and have access to user-centric methods. These methods, Finn explains, include what

he calls "discardable identifiers provided by the user." (such as passwords, public/private key pairs, or keycards.) These can be changed or revoked without altering one's core identity. This contrasts with non-discardable identifiers, like biometrics or state-issued IDs, which are intrinsically tied to the person and often provided to and by an external, authoritative party.

LITERACY

The interviews also revealed how design choices shape everyday discipline. Rami, a finance worker who also worked in healthcare settings, celebrated the seamlessness of modern logins: "Everything's easier now," he said, "I don't understand why you'd want to change anything. I have 2FA on my devices, a password manager, and all is fine. Do you know how many hacking attempts there are during a single day?" equating his multiple security methods with safety. Yet in his professional environment, he routinely left secured terminals unlocked, and his behaviour was reported to be lax regarding safety issues. Assuming the system would handle risk automatically, he took more local security threats as less of a risk. His belief in seamlessness produced complacency, and in turn, risked being costly for his supervisors.

Angela represented the opposite response: constant verification left her anxious and over-attentive, afraid of losing access. Both cases stem from the same design impulse, which was to hide complexity from the user. When security becomes invisible, awareness atrophies; when it becomes over-visible, anxiety replaces understanding. This mirrors Chun's (2011) critique of transparency as control: systems oscillate between opacity and hyper-visibility without fostering understanding.

In truth, it is possible to improve these through design, by instead cultivating literacy as calm awareness: users should know what each step achieves without being overburdened by it. This balance recalls the principle demonstrated by DuoPass, that anchored cognitive security in meaningful cues increases both retention and confidence. By working with, rather than against, users' memory and perception, login can become a site of comprehension instead of compliance.

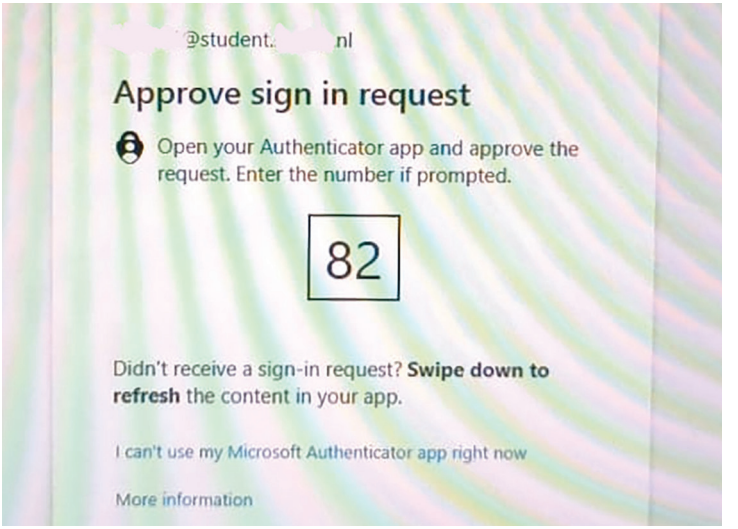
SYNTHESIS

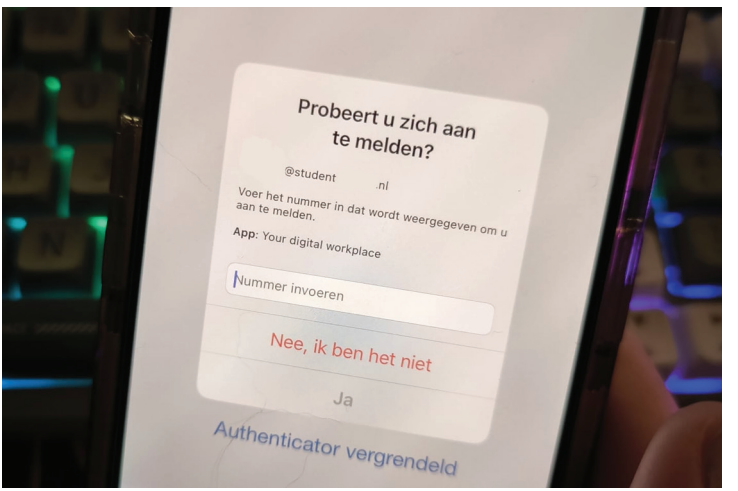
The testimony of users coalesces around a central tension: security is accepted as necessary, but rejected when its implementation feels arbitrary or opaque. Friction is tolerated, even welcomed, when it is perceived as proportional to the context, and explicitly disclosed. However, when authentication becomes a standardized experience of externalized checks (disconnected from the user's understanding and control) it generates frustration and a sense of alienation.

These findings give empirical weight to the central problematic of this thesis. The login, far from being a neutral gateway, emerges as a practice that can alienate users from the very systems meant to serve them. The anxiety of lockout, the resentment towards opaque multi-factor steps, and the nuanced desire for ownership without over-identification...Each of these experiences point to a relational failure in contemporary authentication design.

This diagnosis suggests a constructive path. The solution is not necessarily more security, but a different kind of security: one that engages the user's own faculties of memory, context, and comprehension. The positive response to systems like DuoPass indicates a promising direction. By anchoring the authentication process in meaningful, user-defined cues, security can become more memorable and less punitive, in an attempt to enhance user participation.

Guided by these principles, the following chapter transitions to research-through-design. The experimental prototypes presented function as speculative instruments, not final proposals. Their primary importance to this research is twofold: first, to translate abstract principles like 'participation' and 'legibility' into concrete interactions that can be experienced and evaluated; and second, to provoke new ways of thinking about what login could be. This hands-on, propositional phase is essential for exploring how to redesign authentication as a contextual, legible, and participatory interaction. The aim was to unearth and address in real-time the core tensions uncovered by the users in this study.


@student. nl
Approve sign in request
Open your Authenticator app and approve the request. Enter the number if prompted.
82
Didn't receive a sign-in request? Swipe down to refresh the content in your app.
I can't use my Microsoft Authenticator app right now
More information


Probeert u zich aan te melden?
@student .nl
Voer het nummer in dat wordt weergegeven om u aan te melden.
App: Your digital workplace
Nummer invoeren
Nee, ik ben het niet
Ja
Authenticator vergrendeld

10 EXPERIMENTS

EXPERIMENT 1 — LOGIN CARD GAME

PARTICIPANTS AND SETTING

Three sessions were held with groups of design students aged roughly twenty to forty.The sessions took place in a classroom, lasting under thirty minutes each. Group sizes were three, four, and six participants. All participants already knew one another, which helped maintain an informal atmosphere.

PURPOSE

This experiment explored how people respond when the act of login is turned into a shared, physical performance. The guiding question was: what happens when authentication depends on other people rather than on a machine? The goal was to make participants feel the dependency, hesitation, and suspicion that often accompany digital security routines.

MATERIALS

A deck of Login Cards printed with short sentences describing actions.

Blank Cards so players could invent new actions.

A sealed envelope acting as the “reward.”

One Game Master (the researcher) to read the rules, validate actions, and observe play.

The printed rules described a simple sequence: each player received one hidden Login Card, visible only to the Game Master. A round ended when a secret action was completed or when only one player remained.

OBSERVATIONS

The first session became playful and competitive. Players quickly tried to trick others with impossible or confusing actions to win faster.

In later sessions, as the groups grew larger hesitation blundered the experience. Many stopped acting altogether, afraid of being "found out." One participant remarked, "I can't perform this or I'll be found out immediately." That sentence captured the central mood: a mix of self-consciousness and surveillance. While two groups managed to complete the game, most participants spent their time watching and second-guessing one another.

RESEARCHER'S NOTES

Explaining and remembering all the rules proved unexpectedly hard. As Game Master, I often felt lost, which weakened the structure of play. In retrospect, that confusion in users and myself mirrored the opacity of real-world login procedures: users follow instructions they did not design and may not fully understand. The disorientation almost became a part of the result, showing how certain rules can foster more hesitation rather than comprehension.

SYNTHESIS

Transforming login into a group practice revealed how fragile trust becomes once verification moves beyond individual control. The mechanics of guessing and observation reproduced the unease of multi-factor systems where authentication is distributed across external checks. The main insight is that excessive layers can stall participation entirely. The challenge for later prototypes is therefore to preserve meaningful friction: enough resistance to signal care and recognition, but not so much that it prevents action altogether.


LOGIN CARD
LOGIN CARD
LOGIN CARD
BLANK CARD


LOGIN CARD
Get another player to
pinky promise to you

EXPERIMENT 2 — THE SHARED ACCESS GAME

OBJECTIVE AND PREMISE

This exercise examined what happens when entry depends on another person rather than on a system. The aim was to test the limits of collective authentication. Could access function through mutual agreement instead of automated verification?

SETUP

The experiment took place in a classroom with small groups of participants (usually in pairs or trios). Each person could only enter the room after leaving if someone already inside agreed to let them back in. When a participant wanted to return, they messaged the researcher (me), who in turn asked the person in the room whether to approve or refuse entry. The setting was intentionally simple and physical, as no interface and no screens were used. It was only mediated communication through the researcher, myself. Each session lasted around an hour.

OBSERVATIONS

At first, the interactions were playful. Participants teased each other, delayed responses, or jokingly refused permission. The situation felt like a game of minor power. Some laughed and tried to "test the system" by keeping the door closed for long stretches. As time passed, amusement quickly turned into fatigue. Those waiting outside described the experience as "annoying," "pointless," or "a waste of time." Inside, participants admitted to feeling "guilty" or "bored" by the responsibility of deciding who could enter.

A few drew parallels to shared or co-owned accounts in real life, where one person's access depends on another's device or phone number. One participant mentioned an old shared login where "you had to call the other person just to get a code"... She described the process as "impossible to manage" once schedules between the two of them diverged.

RESEARCHER'S NOTES

Managing the flow of messages and responses was slow and inconsistent. The lag between request and approval created tension, but not the productive kind found in earlier experiments. The social negotiation overshadowed the simple goal of entry. The more "human" the process became, the less usable it felt.

SYNTHESIS

The shared-access model revealed that mutual consent often collapses under the weight of coordination and social discomfort. Participants valued clear rules and impersonal judgment in digital systems precisely because they prevent such awkward dependencies.

Where Experiment 1 exposed confusion through over-structured rules, this test exposed exhaustion through social mediation. Human-based verification made access feel arbitrary and personal rather than procedural. Trust, when made too visible, became an irritating game of negotiation.

The outcome suggests that the absence of human judgment in everyday login design is practical and protective. People prefer systems that remove interpersonal gatekeeping, even at the cost of abstraction.

EXPERIMENT 3 - THE CUSTOMISED STEP LOGIN

OBJECTIVE AND PREMISE

This prototype examined whether giving users control over their own verification logic could procure a more tangible sense of ownership. Instead of following fixed procedures, participants defined what would count as proof of identity, which they would perform within a 30-second window after signing in.

SETUP

Participants accessed a minimal test webpage containing a registration field where they created an additional confirmation step to perform immediately after login.

Examples included:

Creating a new folder in their workspace;

Writing a short message in a text box (writing a new post);

Waiting without interaction for 30 seconds,or uploading a small image.

Failure to complete the declared action within the time limit automatically logged the participant out. The prototype was tested with five participants on their own laptops in a brief 15-minute session.

OBSERVATIONS

Reactions divided between those who found the experience empowering and those who found it stressful. Some enjoyed the idea of designing a step that reflected their habits, while others struggled to remember what they had set.

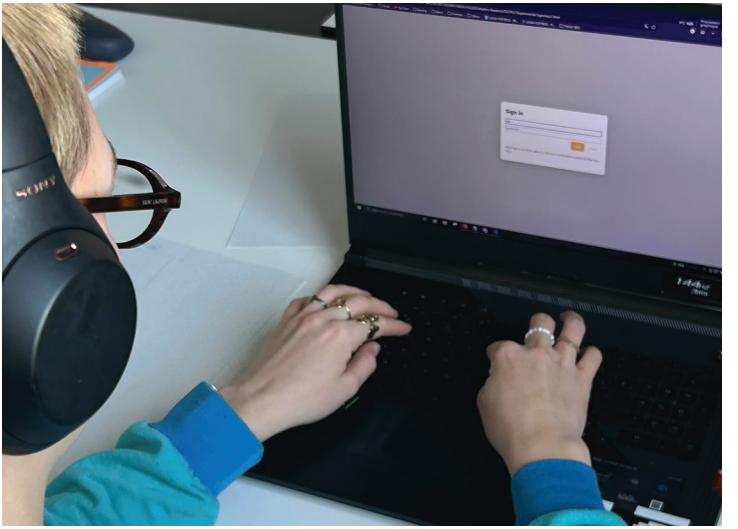
When participants misremembered their own step, the resulting lockout produced laughter, confusion, annoyance, or embarrassment. The short 30-second window introduced temporal pressure, turning the act into a small stressful test of self-consistency.

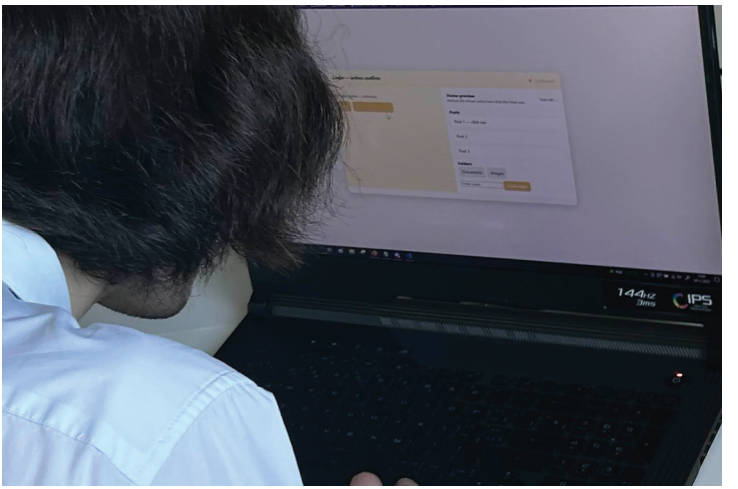
A recurring theme was their intentionality. Logging in felt more interactive and entrancing by adding one small, user-defined verification step that forced interaction with the website in some way.

SYNTHESIS

Letting users define their own confirmation logic inverted the usual relationship between user and system. Since the user authored their verification method, the platform no longer dictated sources of proof. Yet this autonomy introduced a form of fragility. Several noted they "wouldn't want this on an important site," fearing they might forget their chosen action, which makes sense regarding proportionality.

Practically, this experiment underscores the limits of self-determination: while people appreciate flexibility, they also rely on stable systems of identification to sustain continuity across sessions.


Sign in
144Hz
3ms


144Hz
3ms
IPS

KEY INSIGHTS FOR DESIGN

Across field studies, interviews, and experiments, several principles emerged for what makes authentication genuinely effective. A good login balances friction with comprehension: it asks for effort that feels necessary. It is predictable without being rigid, and demands that it remains secure while not being too punitive or asking for private personal data. Users trust systems that communicate intent clearly. Recovery needs to also be device-centric. Material exclusion or dependency should be avoided, which is problematic for Passkeys and other Authentication methods. Recovery needs to perhaps ask for other possibilities, instead of private home data or giving a set of permanent codes to not lose.

In practice, this means designing authentication that fits its context (visually and systemically) integrating with familiar gestures, and making verification an understandable part of interaction rather than an interruption. Play could be injected into the login process, as well. It could be enriching to add quizzes, or other practices and forms of entertainment into authentication, allowing it to be less alienating, depending on the context.

From these findings emerges a framework for human-centred authentication design:

> Effort to login must align with the importance of the platform. When friction is interpretable and situated, it enhances trust rather than disrupts it. (Proportional)
>
> Login should correspond to the sensitivity and purpose of the platform; not all systems require identical proofs or procedures. (Contextual)
>
> Users who feel cared for are more vigilant ; Clear feedback, guidance, and empathetic tone reduce circumvention (Transparency)
>
> Confirming legitimate control need not demand personal disclosure. Separating ownership from real physical identity preserves privacy while maintaining accountability. (User-owned relation instead of Identifying-platform)
>
> Login interactions that require a minimal amount of cognitive effort and a play-like aspect to login can help inform users how authentication works. (Play and interaction can enhance tech literacy)

These principles provide the foundation for a series of speculative designs that reimagine the login experience.

11 SPECULATIVE LOGINS

SPECULATIVE LOGINS

DESIGN PROPOSALS

Guided by the aforementioned framework, this chapter translates theory into tangible form. It presents three concrete design proposals that target specific pain points in the contemporary login experience. They are not final products. These are speculative instruments, each one a material argument for how we can build a more contextual, proportional, and participatory authentication future.

CONTEXT

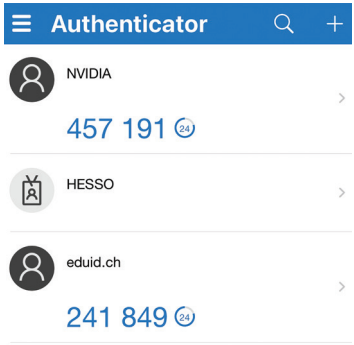
First, to begin, it is important to understand which levels of friction correspond to the right context. As such, a graph has been made based on user commentaries.

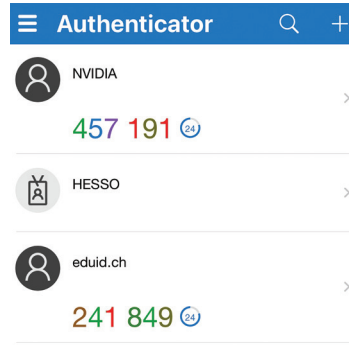
This graph outlines how users perceive login friction across different contexts. High-friction methods such as authentication apps, 2FA codes, and physical tokens are accepted for banking, healthcare, and other high-risk platforms.

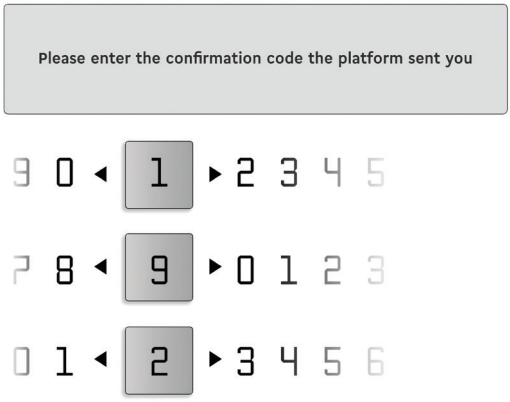
Medium friction, like magic links or SMS codes, fits semi-private spaces such as social media or personal storage. Standard passwords or QR scans suit casual or creative platforms, while low-friction logins (like "Sign in with Google" or simple security questions) are preferred for low-stakes, anonymous, or community spaces. The data shows that users link the level of friction to the perceived sensitivity of the context, and not to convenience alone.

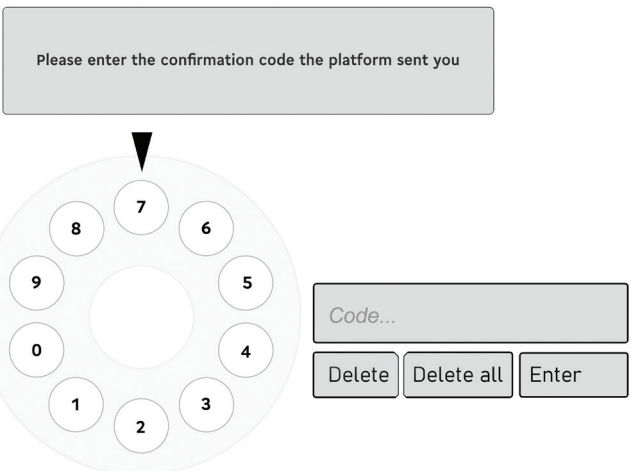
ACCESSIBLE AUTHENTICATOR

A redesign of the standard authenticator app to reduce affective friction and improve accessibility. It employs a dual approach: color-by-Position coding for one-time passwords to aid users with dyslexia or visual stress, and an optional Skeuomorphic Rotary Dial for number entry, providing a tactile, sequential input method that may reduce errors and enhance the perceived security through more deliberate interaction.






Please enter the confirmation code the platform sent you
9 0 1 2 3 4 5
7 8 9 0 1 2 3
0 1 2 3 4 5 6


Please enter the confirmation code the platform sent you
7
8
6
9
5
0
4
1
3
2
Code...
Delete
Delete all
Enter

PASSWORD SECURITY QUEST

To combat the overwhelming tasks of security maintenance, this proposal redesigns the password manager interface for breached credentials. It breaks down the monolithic task of updating "100+ compromised passwords" into a series of managed, daily "quests" (e.g., "Update your 3 most critical accounts"). This playful and proportional approach reduces cognitive pressure, and attempts to generate a sense of ownership and accomplishment. The system would provide guided, one-click access to password change pages, storing new credentials only upon user action

POST-LOGIN VIGILANCE CONFIRMATION

This is an extension of one of the previous experiments.This proposal introduces a native, post-password confirmation method, to replace or supplement externalised two-factor methods. Upon correct password entry, the user must perform a simple, contextual action within the platform (e.g., clicking a specific UI element, trace a pattern, click on parts of the page) within a 1 minute window. This creates a proportional and contextual method that aims to confirm user presence against automated attacks and phishing, all while keeping the verification process internal to the platform. Success is measured through completion rates, time-on-task, and perceived clarity.

PROPORTIONAL DESIGN

This proposal confronts the aesthetic alienation of standardized login pop-ups (e.g., "Sign in with Google") by advocating for login interfaces that are thematically integrated with their host platform. A children's educational site should not have the same design language as and login methods as a bank, for example. This contextual design refuses a generic checkpoint in benefit of a login page that reinforces the platform's identity. Extending this, platforms could offer user-customizable themes or community-generated "skins," in an attempt to preserve a sense of ownership and belonging even before authentication is complete.

INTEGRATION

These features are conceived as configurable options, with fallbacks to standard flows to ensure universal access. More importantly, the process of designing them was fundamental to this research. Creating these prototypes forced a translation of abstract principles (contextuality, participation, legibility) into tangible design dilemmas and decisions. They served as vital tools for thought, making the possibilities and trade-offs of a more humane authentication future concretely visible. It is this practice of critical making that can inspire other designers to move beyond critiquing the existing experience of login and to begin constructing, testing, and arguing for alternatives through their own material proposals.

12 CONCLUSION

CONCLUSION

This thesis has examined login as a defining gesture of digital life, an interface where access, trust, and identity are continuously negotiated. Through historical, theoretical, and experimental inquiry, it has shown that authentication is not a neutral checkpoint but a cultural practice shaped by long genealogies of measurement, control, and recognition. From Bertillon's anthropometry to biometric scans and single sign-on infrastructures, the same ambition persists: to secure entry by rendering identity verifiable. Through authentication, an attempt is made at making identity quantifiable.

By situating login within this lineage, the study revealed how the externalisation of authentication (the delegation of trust to corporate identity providers and automated systems) has distanced users from the very infrastructures meant to protect them. The design of security has become abstract, invisible, and emotionally detached. Yet this condition is not irreversible: principles of play, contextuality, and literacy-oriented design can strengthen, rather than weaken, security.

Through speculative and game-based prototypes, the research tested what happens when authentication becomes participatory. These experiments reframed login as a form of interaction in which users act as co-agents rather than passive subjects. In several cases (most notably those inspired by DuoPass) participants performed better when verification drew on familiar, user-defined, meaningful cues. When friction was contextualised and emotionally legible, it improved both recall and engagement. The presence of play and relational feedback fostered attentiveness rather than complacency, producing a form of applied security grounded in understanding and transparency.

This framework remodels authentication as a more dynamic threshold where the basis of design can be rebuilt, through systems in which protection and participation coexist. Carefully designing with play and contextual literacy does not indeed trivialise security; it deepens it by aligning technological rigour with human comprehension.

Ultimately, the future of authentication lies in reconciling security with user experience. By combining contextual awareness, proportional effort, and relational design, authentication can become both safer and more humane.

The challenge for future designers is not to remove friction, but to make it meaningful: to build systems that protect through understanding and secure through participation.

13 BIBLIOGRAPHY

REFERENCES AND BIBLIOGRAPHY

BOOKS

AUSTIN, John L., 1955. How to Do Things with Words. The William James Lectures delivered at Harvard University in 1955. [online]. Note: Published posthumously in 1962. Originalcopy. Available at : https://www.ocopy.net/2016/10/19/john-l-austin-how-to-do-things-with-words-1955/ (Accessed 9 october 2025).

BROCA, Paul, 1875. Instructions craniologiques et craniométriques. Paris : C. Reinwald

CHUN, Wendy Hui Kyong, 2011. Programmed Visions: Software and Memory. Cambridge, Mass : MIT Press. (Software studies). ISBN 978-0-262-01542-4.

COLE, Simon A., 2001. Suspect Identities: A History of Fingerprinting and Criminal Identification. Cambridge, MA : Harvard University Press.

GALTON, Francis, 2011. Finger Prints [online]. Édition originale 1892. Project Gutenberg. Available at : https://www.gutenberg.org/files/36979/36979-h/36979-h.htm (Accessed 10 october 2025).

GALLOWAY, Alexander R., 2012. The Interface Effect. Cambridge, UK ; Malden, MA : Polity, p. 40. ISBN 978-0-7456-6252-7.

WARE, Colin, 2013. Information Visualization: Perception for Design. 3rd ed. Burlington, MA: Morgan Kaufmann.

ACADEMIC JOURNAL ARTICLES

HAGGAR, Sarah, 2025. Communitas revisited: Victor Turner and the transformation of a concept. Anthropological Theory, vol. 25, no 3, p. 313-337. DOI: 10.1177/14634996241282143.

KALUSZYNSKI, Martine, 2014. Alphonse Bertillon et l'anthropométrie judiciaire. L'identification au cœur de l'ordre républicain. Criminocorpus, revue hypermédia [online]. DOI : 10.4000/criminocorpus.2716.

MORRIS, Robert & THOMPSON, Ken, 1979. Password Security: A Case History. Communications of the ACM [online], vol. 22, no. 11, p. 594-597. Available at : https://dl.acm.org/doi/pdf/10.1145/359168.359172 (Accessed 10 october 2025).

STAR, Susan Leigh, 1999. The Ethnography of Infrastructure. American Behavioral Scientist, vol. 43, no. 3, pp. 377-391. DOI 10.1177/00027649921955326. [online]. Available at : https://www.ics.uci.edu/~wscacchi/GameLab/Recommended%20Readings/ethnography-infrastructure-Star-1999.pdf

CONFERENCE PROCEEDINGS & TECHNICAL REPORTS

BONNEAU, Joseph, HERLEY, Cormac, VAN OORSCHOT, Paul C. & STAJANO, Frank, 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: 2012 IEEE Symposium on Security and Privacy. San Francisco, CA, USA: IEEE, p. 553-567.

BUSSE, Kristina, et al., 2019. "What did I do?" versus "What did I get?": The Role of Contextual Integrity in Online Behavioral Advertising [online]. In: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS). Available at : https://www.usenix.org/system/files/soups2019-busse.pdf (Accessed 10 october 2025).

CORBATÓ, Fernando J., MERWIN-DAGGETT, Marjorie & DALEY, Robert C., 1962. An Experimental Time-Sharing System. In: *Proceedings of the May 1-3, 1962, spring joint computer conference*. San Francisco, California: ACM Press, p. 335-344. DOI: 10.1145/1460833.1460871.

LIU, Y., YADAV, A.D., GANTI, K.S.R.K.K. et KASIVISWANATHAN, S.P., 2022. Practical Differential Privacy for Location Data. In: Proceedings of the ACM on Measurement and Analysis of Computing Systems [online]. 1 December 2022. Vol. 6, no. 3, 57. (Accessed 10 october 2025. Available at: https://doi.org/10.1145/3564610

GAW, Shiri & FELTEN, Edward W., 2006. Password Management Strategies. In: *Proceedings of the 2006 Workshop on Human-Computer Interaction and Security*. Pittsburgh, Pennsylvania: USENIX Association.

WHITTEN, Alma & TYGAR, J. D., 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium [online]. Available at : https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf (Accessed 10 october 2025).

YAN, Jianxin, et al., 2000. The Memorability and Security of Passwords: Some Empirical Results. University of Cambridge Computer Laboratory Technical Report [online], no. 500. Available at : https://dl.acm.org/doi/pdf/10.1145/322796.322806(Accessed 10 october 2025).

STANDARDS, SPECIFICATIONS & GOVERNMENTAL REPORTS

FIDO ALLIANCE, 2019. Client to Authenticator Protocol (CTAP). Proposed Standard, 30 janvier 2019 [online]. Available at : https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html (Accessed 10 october 2025).

FIDO ALLIANCE. Client to Authenticator Protocol (CTAP) [online]. Proposed Standard, Version 2.2, 21 March 2023. Available at : https://fidoalliance.org/specs/fido-v2.2-rd-20230321/fido-client-to-authenticator-protocol-v2.2-rd-20230321.html (Accessed 10 october 2025).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), 2024. Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B) [online]. Available at : https://pages.nist.gov/800-63-4/sp800-63b.html (Accessed 10 october 2025).

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Security Fatigue Can Cause Computer Users to Feel Hopeless and Act Recklessly [online]. 4 October 2016. Available at : https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly (Accessed 10 october 2025).

OAUTH CORE WORKGROUP, 2007. OAuth Core 1.0 [online]. Available at : https://oauth.net/core/1.0/ (Accessed 10 october 2025).

SALTZER, Jerome H. & KAASHOEK, M. Frans, 2009. Principles of Computer System Design: An Introduction [online]. Burlington, MA : Morgan Kaufmann Publishers. Chapter 11, "Information Security". Available at : https://booksite.elsevier.com/9780123749574/casestudies/05~11~chapter_11.pdf (Accessed 10 october 2025).

ONLINE ARTICLES, NEWS & BLOG POSTS

BRECKENRIDGE, Keith, 2005. Towards the theory of the biometric state. Seminar paper [online]. Available at : https://phambo.wiser.org.za/files/seminars/Breckenridge2005.pdf (Accessed 10 october 2025).

GOOGLE SAFETY & SECURITY. One step closer to a passwordless future [online]. 4 May 2023. Available at : https://blog.google/technology/safety-security/one-step-closer-to-a-passwordless-future/ (Accessed 10 october 2025).

HUGHES, Neil, 2013. Inside Apple's iPhone 5s: « s » is for « sensors ». AppleInsider [online]. 14 september 2013. Available at : https://appleinsider.com/articles/13/09/14/inside-apples-iphone-5s-s-is-for-sensors (Accessed 10 october 2025).

LAZAR, David, et al., 2009. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users [online]. Microsoft Research. Available at : https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SoLongAndNoThanks.pdf (Accessed 10 october 2025).

MCMILLAN, Robert, 2012. The World's First Computer Password? It Was Useless Too. Wired [online]. 27 January 2012. Available at : https://www.wired.com/2012/01/computer-password/ (Accessed 9 october 2025).

PAGANINI, Pierluigi. LinkedIn Breach from 2012 Still Haunting the Security Community [online]. Security Affairs, 25 May 2016. Available at : https://securityaffairs.com/47691/data-breach/linkedin-breach-2012.html (Accessed 11 november 2025).

ONLINE MUSEUM, LIBRARY & ARCHIVAL RESOURCES

NATIONAL LIBRARY OF MEDICINE, n.d. Alphonse Bertillon (1853–1914). Visible Proofs: Forensic Views of the Body [online]. Available at : https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/biographies/bertillon.html (Accessed 10 october 2025).

SMITH, William, 1875. Tessera. In: THAYER, Bill (éd.). A Dictionary of Greek and Roman Antiquities [online]. LacusCurtius. Available at : https://penelope.uchicago.edu/Thayer/E/Roman/Texts/secondary/SMIGRA*/Tessera.html (Accessed 9 october 2025).

THE METROPOLITAN MUSEUM OF ART, n.d. Cylinder seal and modern impression: hunting scene [online]. Available at : https://www.metmuseum.org/art/collection/search/329090 (Accessed 9 october 2025).

UNIVERSITY OF NOTTINGHAM, n.d. Authentication of legal and administrative documents [online]. Available at: https://www.nottingham.ac.uk/manuscriptsandspecialcollections/researchguidance/medievaldocuments/authentication.aspx (Accessed 9 october 2025).

CUMMINS, Harold & MIDLO, Charles, 1943. Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics [online]. Philadelphia : The Blakiston Company. Available at : https://www.ojp.gov/pdffiles1/nij/225321.pdf (Accessed 10 october 2025).

ARTISTIC WORKS

DEWEY-HAGBORG, Heather, 2012-2013. Stranger Visions [online]. Available at: https://deweyhagborg.com/projects/stranger-visions (accessed 20 August 2025).

SIKORYAK, R., 2017. Terms and Conditions [online]. Montréal: Drawn & Quarterly. Available at: https://itunestandc.tumblr.com/tagged/itunes%20terms%20and%20conditions/chrono (accessed 20 August 2025).