Proof of Humanness Over Bots: Designing Personhood Credentials for Usability, Security, and Trust

Ayae Ide, Tanusree Sharma

Unlike traditional authentication which is typically tied to account ownership (does not prevent creating multiple account) and used for login and authorization, Personhood Credentials (PHCs) have emerged as safeguards to verify human uniqueness and provide protection against AI-driven threats such as bots, deepfakes, and social media manipulation without disclosing personal information. The fundamental differences between PHC and existing technology may lead end-users to misunderstand PHCs as merely an alternative login method instead of a unique system. For instance, in PHC systems, biometrics are only used to generate a uniqueness proof and are not stored. However, users may not understand this privacy guarantee, leading to friction in adoption and a mismatch of expectations in design and development. To address this, we conducted semi-structured user interviews with 27 participants from the US and EU to provide concrete design recommendations. Our study shows how people reason about the uncertain guarantees of PHCs and how preferences depend on trusted issuers such as governments, ground truth data such as biometrics or IDs, and issuance models (e.g., centralized or decentralized systems). In think-aloud sessions, participants suggested designs including periodic biometrics verification; time-bound credentials; visually interactive human-check; and government oversight. We contextualized our user-study findings within the broader identity management policy landscape to lay out potential governance pathways for future digital personhood credential systems.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; *Authentication*; • **Human-centered computing →** *User studies.*

Additional Key Words and Phrases: Personhood Credentials, Digital Identity, Usable Privacy and Security

ACM Reference Format:

Ayae Ide, Tanusree Sharma. 2026. Proof of Humanness Over Bots: Designing Personhood Credentials for Usability, Security, and Trust. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation email (Conference acronym 'XX).* ACM, New York, NY, USA, 30 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

Identity management has long been a cornerstone of user-facing systems such as social media, gaming, and collaborative tools, and has increasingly become integral to Human-AI systems [53, 71]. The recent proliferation of artificial intelligence (AI) has rendered traditional methods of multi-factor [41], and CAPTCHA [124] verification unreliable, as AI can now generate highly convincing fake human interactions [39, 51, 70]. Amid growing concerns over how major technology companies handle user data [10], there has been a noticeable technological and ideological shift towards decentralized identity systems, commonly known as self-sovereign identity [92]. One widely recognized approach involves decentralized identifiers (DIDs). Emerging proposed systems, such as DECO [132], Town-Crier [131], exemplify this model, where users authorize the release of personal credentials from user devices to websites for proving certain characteristics about themselves. Although initiatives like the W3C Decentralized Identifier Working Group seek to

Manuscript submitted to ACM

establish standards for decentralized identity [11, 13], many proposed frameworks struggle to meet both technical and usability requirements. Recent efforts, such as CanDID, have made progress in areas like usable key recovery [93].

Building on concepts, such as decentralized identifiers (DIDs) and proof-of-personhood [67], Personhood Credentials (PHCs) have been proposed as safeguards to verify human uniqueness and provide protection against AI-driven threats such as bots, deepfakes, and social media manipulation[37]. PHC is defined as **digital credentials that empower users to demonstrate that they are legitimate (e.g., human, not bot), unique (e.g., distinct), and human with a certain property (i.e., us residency, certain age, etc) to online services and platforms, without disclosing any personal information."** PHCs are designed not merely to verify digital attributes, but to allow individuals to demonstrate their unique human [37] where the credentials are stored digitally on devices and verified through zero-knowledge proof systems [67]. A prominent example is World ID, launched in the U.S. in May 2025 [78], which promotes itself as a **privacy-preserving proof of personhood**. Using biometric iris scans via Orb devices, it links a World ID to a single individual [60]. Once issued, a World ID is stored in the user's digital wallet, enabling them to prove their uniqueness to online services. More recently, World ID has expanded into mainstream applications through partnerships in the gaming (e.g., World Card, and Razer), finance (e.g., Visa), and dating (e.g., Tinder, Hinge) areas, which have long been targets for bot-driven abuse and malicious actors exploiting false or misleading identities to perpetrate fraud[16, 26, 33].

Recent advances of AI have further amplified these risks, giving rise to the long-standing deceptive schemes, and infiltrating elements of society where users' signals are crucial [3, 37]. Despite the growing importance of personhood credentials and similar tools, there is a lack of understanding about how PHCs could be designed from a user-centered perspective, and in particular, what factors might influence users' preferences with regard to onboarding and managing PHCs. New technologies might introduce some friction due to users' misunderstandings and mismatched expectations [80]. Furthermore, a fundamental limitation of current approaches to PHC is their failure to address PHC issuance, which echoes challenges faced in the development of DIDs [68]. Even after years of industry effort toward decentralized credentials, state-issued digital IDs remain scarce, currently implemented at scale only in California [7]. Similarly, PHCs present unknowns and design challenges, including who should issue them, through what mechanisms, and what forms of verification should be required, and more importantly, how these systems should be designed to meet end-users' privacy and security expectations. To address these gaps and complement existing system-centric perspectives, our paper explores a user-centered approach. Towards this goal, we conducted interviews with 27 US and EU/UK participants to explore user preferences and the factors (RQ1) influencing their choices of personhood credentials (RQ2). Finally, we conceptualized participants' desired approaches in managing personhood credentials (RQ3). Our study provides insights into the following research questions:

RQ1: What are the users' perceptions of personhood credentials to verify themselves as legitimate and unique individuals in online interactions?

Our study uncovered a wide range of users' perceptions regarding PHCs. Participants exhibited skepticism towards PHCs, partly because of *"unknown risk"* vectors as a new technology compared to traditional verification. Despite these concerns, we find diverse levels of adoption preferences influenced by the *"type of data required"* for PHC credential issuance and verification, as well as personal *"security standards"* for different services (e.g, finance, health, government-related). Our findings also indicate benefits, including aspects that promote fairness by ensuring opportunities for legitimate users in platforms such as gaming and survey platforms.

RQ2: What factors influence user preferences on how people would like to verify themselves as legitimate and unique individuals in online interactions?

We surfaced nuanced preferences of how participants would like to onboard and manage PHC credentials. Their preferences depended on the type of ground truth data required for issuance, along with the familiarity, usability, and sensitivity of those data sources. They often considered facial recognition a more resilient verification process than fingerprints. Other factors influencing preferences included the issuing ecosystem (centralized vs. decentralized), the issuer (government vs. private company), and the onboarding method (physical vs. remote).

RQ3: How can personhood credentials be designed to ensure usability and security, enabling users to verify themselves as legitimate and unique individuals in online interactions? We identified practical design suggestions to accommodate participants' needs, including periodic biometric checks and time-bound credential verification to ensure only the intended user accesses the credential; visually interactive human checks to prevent social engineering during onboarding, and collaboration between industry and government to establish decentralized standards for broader adoption. We then triangulated these findings with policy analysis to derive requirements that are uniquely tailored to PHCs as anonymous, Sybil-resistant, renewable, and multi-issuer credentials, which rely on public trust and users' accurate understanding of PHC privacy and security guarantees.

Contributions We contributed to several key areas that inform the future design of user-centered PHC systems:

(1) Our work identified a gap between the privacy protections PHCs provide and how users understand them, which can guide future work of the broader adoption of PHCs. Our findings offer nuanced insights into users' perceptions and the factors shaping their preferences around personhood verification.
(2) We integrate user-centered design insights from interactive sketch sessions with the policy context of personhood verification to develop a conceptual framework. This provides technical, governance, and design requirements for various stakeholders.

2 Related Work

Our study of the personhood credential is positioned from two angles: identifying limitations of current identity verification to motivate the need for personhood credentials, and adding new knowledge of user-centric perspectives to design personhood credentials.

2.1 Landscape of Verification Tools & Practices

Identity verification has evolved rapidly with a range of technical modalities to support diverse applications from regulatory compliance (e.g., KYC/AML) to fraud prevention and digital onboarding. These tools span from document-based verification, biometric authentication, behavioral biometrics, knowledge-based techniques, and device signals. A common tool we encounter in everyday life is **CAPTCHA** [124], designed with an automated public Turing test to distinguish humans from bot interaction. While this method is widely used and provides some extent of security for now, studies indicated challenges where CAPTCHAs are vulnerable to automated solvers or bots and often outperform humans in both speed and accuracy [72, 86, 111, 125]. Another popular method for its' usability and convenience is **physiological biometrics** (e.g., Face ID, CLEAR) involving fingerprint, voice, and face unlock [44, 59, 94, 134] are increasingly challenged by deepfakes, voice cloning, and high-quality presentation attacks [101] and privacy concerns about biometric data in the authentication process [126, 134]. Selfies and video calls have become popular as **liveliness tests** to reduce bot interaction, as seen in platforms like Instagram [23], ID.me offering self-service selfie or video call with trusted referee verification for government use cases, such as obtaining an identity protection PIN to prevent tax-related identity theft [25]. **Behavioral biometrics** (e.g., Android Smart Lock/Extend Unlock) [84, 96] has also

emerged as an alternative identification method, leveraging users' interaction characteristics, such as body movements and gait patterns. Even such dynamic biometrics are recognized as more resilient against deepfake threats. An expert interview study on biometric authentication noted that advanced generative models can convincingly mimic micro-expressions and subtle eye movements [75]. Another form of verification is **digital identifiers, device fingerprinting, or provenance**, which assigns persistent identities or metadata based on browser, device, and network traits [87, 130]. However, these checks may verify hardware, not people, thus users with shared or changing devices are misidentified or fragmented into multiple digital personas [43, 102]. Recent studies also demonstrated that the challenges of tamper-proof and resilient **watermarking** for verifying the source of the data are more critical in many disinformation cases [133]. To address some challenges, newer methods like DECO, CANDID, or attestation via trusted hardware (e.g., TPMs) encode provenance to validate that actions originate from verified or bound environments [93, 132]. Another significant portion of contemporary identity verification practices centers around **public identifiers** (e.g., email addresses, phone numbers) often embedded within broader frameworks such as multi-factor authentication (MFA) or risk-based authentication (RBA) [41, 112]. To improve user convenience and reduce the need for repeated identity creation, federated login systems such as OpenID and OAuth 2.0 emerged [73, 90, 103]. However, these methods are still prone to privacy issues and have limited pseudonymity when most federated systems are tied to real-world identifiers (e.g., Gmail accounts or Apple IDs). It lacks Sybil resistance since emails and phone numbers are easy to acquire or automate, thus bot farms can generate massive numbers of accounts, undermining trust and fairness in open digital environments.

To address these limitations, particularly to provide user control over identity management, research began introducing user-centric and decentralized identity systems. Notably, self-sovereign identity (SSI) architectures leverage decentralized identifiers (DIDs) and verifiable credentials (VCs) [48, 97, 120] to enable individuals to generate and receive cryptographically signed credentials from trusted issuers, present those credentials selectively and privately as per service needs. The recent launch of World App by Tools for Humanity marked a significant inflection point in the deployment of verifiable credential systems within public and decentralized environments, which combine usability components by incorporating biometrics to prove claims, such as humanness and uniqueness as a human, as well as users' agency of data disclosure [74].

2.2 Nuances of Personhood Credentials

Proof of Personhood (PoP) Verifying online identities has been particularly crucial for blockchain systems to mitigate the risks of impersonation and fraudulent activities. Proof of Personhood (PoP) has emerged to counter Sybil attacks, which manipulate peer-to-peer networks by operating multiple pseudonymous identities. It verifies an individual's humanness and uniqueness digitally on blockchain [46] while preserving anonymity by linking virtual and physical identities. For instance, the Idena: proof of person blockchain runs a Turing test to prove the humanness and uniqueness of its participants [21]. Similarly, Humanode [81, 82], which ensures one Human one Node, safeguarded by cryptographically bio-authorized nodes using 3D users' faces. BrightID and Proof of Humanity leverage a social mechanism, such as a social graph and social vouching, to achieve PoP [113] and guarantees that the users exist and are not duplicates of another entity. Recent identity verification platforms reflected such social needs for PoP; Gitcoin Passport, and Civic Pass serve as a self-sovereign data collection protocol with a PoP algorithm [113]

Personhood Credentials (PHCs) The fundamental architecture of PHCs includes three entities: *User; Issuer; Service providers*. First, the user gets PHC from the issuer by providing evidence to verify their identity. Then, the user can use PHC across different service providers without providing identity evidence again. It enables users to demonstrate humanness to online service providers without disclosing any personal information. An example of PHC implemented

in the application is Worldcoin, which is based on PoP and Zero-Knowledge Proofs (ZKPs) [20, 34, 60]. It maintains privacy and anonymity via ZKPs while employing the human iris pattern as a conclusive biometric marker for PoP.

2.3 Why End-User Perspectives Matter for PHC: Challenges & Emerging Design Space

PHC represents a new class of identity technologies distinct from conventional authentication methods. Instead of tying identity to account ownership or preventing multiple accounts, it verifies that a user is a unique human without revealing personal information [37, 54]. This shift introduces a design space that diverges from traditional authentication workflows and creates uncertainty about how end-users will interpret, trust, and ultimately adopt PHCs. Prior research on authentication and identity systems has underscored that the success of solutions is not only in technical soundness but in careful human-centered design. For instance, small variations in message framing [104], step-by-step authentication flows [63], or perceived cognitive effort can significantly shape user trust and comprehension.

In the PHC design space, especially in how they preserve privacy, system builders can not assume users will interpret them in line with cryptographic intentions. Furthermore, the contexts in which PHCs may operate are rapidly expanding and becoming more complex than the traditional use cases (e.g., KYC), due to generative AI and synthetic identity proliferation. Recent incidents where now AI-generated IDs are bypassing financial KYC checks [4, 35], social platforms, and public services face escalating attacks from synthetic accounts [1, 14, 31]. Biometric systems in sectors such as healthcare continue to encounter spoofing and robustness challenges [64, 79], and LLM ecosystems face emerging threats like prompt poisoning [55, 128]. These developments expand verification challenges that exceed traditional identity workflows, underscoring the need for anonymous yet reliable proof-of-humanness solutions [127]. Despite this demand, PHC systems are early-stage, with limited real-world deployments and an active user base. In this work, thus, we approach from a human-centered approach to determine factors that influence people's mental models around PHC and may conflict with real-world adoption boundaries.

The expanding verification landscape also highlights the limits of relying on existing authentication research only. While prior work shows that biometric authentication (e.g., fingerprint, facial recognition) is widely used and valued for convenience [44, 56, 59, 94, 134], studies also highlight user concerns around privacy, susceptibility to physical changes, and environmental robustness [44, 94]. However, conventional authentication does not directly translate to PHCs, whereas biometric authentication verifies identity (or device ownership), whereas PHCs verify humanness without linking to identity. Moreover, authentication typically occurs in controlled, single-device contexts (e.g., unlocking a phone), whereas PHCs must operate across diverse platforms with varying risk profiles [37, 60]. This fundamental difference introduces a new design space where users may prioritize different expectations, such as balancing between minimal disclosure and credible proof of humanness. In digital environments increasingly populated by artificial entities and bots, we will have more situations where we hope to prove our humanness without sharing personal information. In this work, we fill the gap by identifying the design requirements of PHC from the user and policy landscape.

2.4 Policy & Standards of Identity Management Systems

We conducted **policies and standards analysis** [1]**,** to account for legal and regulatory constraints of identity management systems. We choose documents based on their relevance to identity verification or digital identity infrastructure, contextual diversity (e.g., geographic, technical focus, audience), and regulatory impact (e.g., international, national,

[1]https://anonymous.4open.science/r/PHC-user-study-14BB/policy_review.pdf

Table 1. Policy Overview of Digital Identity System Requirements

Policy	Data Requirements	Data Storage Requirements	Issuer Requirements	Transparency	Risk Adaptability	Interoperability	Privacy Control
eIDAS [15]	Not clearly defined yet, EU Digital Identity Wallets are still in the testing phase.	Data is stored on the user's device wallet (decentralized) and kept separate from other data. Member states should integrate privacy-preserving technologies. (e.g., zero-knowledge proof)	Trusted organisations that have been authorized by a national competent authority.	●	●	●	●
U.S. BSA [17]	Financial institutions must collect customer information (name, DOB, address, SSN/TIN) for KYC.	The bank must retain the information for five years under CIP rule.	Each bank must implement a Customer Identification Program.	×	●	×	×
California State Law, California Digital ID Framework [9]	One or more of the following: 1) Something you know – e.g., password, 2) Something you have – e.g., a code sent to your device, 3) Something you are – e.g., face or fingerprint recognition	Centralized, California Identity Gateway minimizes ID and eligibility data and shares it with third parties.	Identity Gateway (OpenID Connect) to federate identity providers and agencies.	●	×	×	●
Wyoming State Law [2]	Not specified.	Decentralized; Defined "personal digital identity" as a self-sovereign intangible digital representation.	Not specified.	×	×	○	×
Utah State Law [18, 29]	Not specified.	Not specified; but identity use must be free from surveillance, visibility, tracking, or monitoring.	The state is the only governmental entity that may endorse an individual's digital identity.	×	×	×	●
NIST SP 800-63 Digital Identity Guidelines [24]	Data requirements of identity proofing (e.g., ID documents, biometrics) based on Assurance Level (e.g., IAL2, IAL3).	Data protection requirements based on Assurance Level (e.g., Approved cryptographic techniques are required at IAL2.)	Credential service providers and identity providers must meet NIST requirements.	×	●	×	×
W3C Recommendation [12, 32]	A verifiable credential can contain any data attested to by an issuer, allowing for selective disclosure. Emphasizes user control over data.	Prove that the information is not tampered with a cryptographic proof (e.g., digital signatures and zero-knowledge proofs)	Any entity can be an issuer of Verifiable Credentials if it can cryptographically sign the data.	○	×	●	●

Transparency: The identity system clearly outlines the data to be collected, stored, and shared. / Risk-based Adaptability: The identity system is flexible and adjusts according to risk. / Interoperability: The identity system is portable across different services. / Privacy Control: Users have control over their data in the identity system.

●= Explicitly address the themes, showing alignment with it; ○= Not explicitly, but directionally relevant; × = Not addressed.

state). We summarized data requirements, storage requirements, and issuer requirements (Table 1) as well as mapped policies' alignment with user-centric themes, such as Transparency, Risk-based Adaptability, Interoperability, and Privacy Control. For instance, California's ID Framework uses a centralized identity gateway to minimize and manage ID and eligibility data, requiring either knowledge, possession, or biometrics, and facilitating issuance through third parties via federated identity providers using OpenID Connect. We found that issuer-related specifications are often underdefined. In the case of decentralized standards, an entity can be an issuer if it is a verifiable credential. In contrast, government regulations often require approval from an official authority to perform as an issuer. These insights guided our interview study design to investigate design possibilities for future PHC systems.

Legal regulations define how identity systems should manage data and verify users. Recent policies also highlight government and institutional expectations for future identity systems, specifically which values matter most, such as privacy, security, and user control. Our review examined policies and standards affecting the governance of identity verification systems. We categorized the reviewed policies into five groups- Legislation; State-level Laws; Standards and Requirements; Strategic Frameworks; Guidance and Recommendations. This categorization reflects on legal constraints, technical requirements, national strategies, and sector-specific best practices that shape how identity systems are designed and governed. Specifically, **Legislation** informed the legal constraints on how identity data is collected and used. **State-level laws** captured early policy innovations around blockchain-based identity. **Standards and requirements** clarified the technical and regulatory conditions for deploying identity systems. **Strategic frameworks** revealed

long-term national goals for secure and privacy-respecting identity infrastructure. **Guidance and recommendations** implied best practices for interoperability and sensitive sectors like finance.

Across our review of policies and standards, we observed a consistent direction toward users' rights for data control. The EU is advancing a universal digital identity wallet, keeping users in control through selective disclosure, while the United States is moving through state-level pilots of DID and verifiable credentials, and technical standards emphasize privacy protection and interoperability. These directions are deeply interwoven with the emerging role of personhood credentials, which also aim to verify individuals while minimizing the amount of personal information disclosed. By enabling proof of humanness without broad identity exposure, personhood credentials align closely with this broader shift toward user-centric, privacy-preserving identity ecosystems. The full analysis table is available through the footnote link, which details the relevance and implications for identity system users and covers 13 policies and standards in total.

3 Method

In this section, we outline the method to investigate users' perceptions and preferences of personhood credentials. We conducted semi-structured interviews with 27 participants from the US and the EU/UK from October 2024 to January 2025. The study was approved by the Institutional Review Board (IRB).

3.1 Participant Recruitment & Participants

We recruited participants through (1) social media posts, (2) online crowdsourcing platforms, including CloudResearch and Prolific. We invited respondents to our study if they met the selection criteria: a) 18 years or older and b) living in the US or the EU/UK. We focused on these regions because the US and EU have led regulatory and technical deployments of digital identity and have played a central role in shaping the foundational regulatory framework in the early stages [77, 91, 100]. Each participant received a $30 Amazon e-gift card upon completing an hour-and-a-half interview. We interviewed a total of 27 participants: 13 from the US, 13 from the EU/UK, and 1 from other regions (Table 2). The majority of the participants (59%) were in the age range of 25-34, followed by 19% who were 35-44 years old, with the remaining age groups (18–24, 45–54, and 55–64) each representing 7% of the total. The participants were from the United States and various countries, namely Spain, Sweden, Germany, Hungary, and the United Kingdom. Participants had different backgrounds of education levels, with 85% of participants holding a Bachelor's degree and 67% holding a graduate degree. 63% of participants had a technology background, while 48% of them had a CS background. Our sample is concentrated in a limited region due to our design choice. Prior usable security research shows that security behaviors and expectations vary widely across cultural and regional contexts, and that context-aware, user-centered design is more effective than universal, one-size-fits-all approaches [63, 76]. We prioritize context-rich insights, which might not generalize to all regions. In addition, the recent Kantar's survey of consumers shows that awareness and usage of digital identity solutions were notably higher among the 25-34 age group [122]. Therefore, the demographic composition of our sample reflects the population most likely to interact with such systems in real-world settings.

Although most participants were familiar only with traditional authentication methods, a small subset reported experience beyond these practices. Some participants (P4, P13, P18, P20, P23) described using personhood-like features, for example, self-custody crypto wallets, human-liveness checks through ID.me for tax filing, video-liveness verification in German online banking, or cross-platform KYC apps. Our sample had limited experience with these systems, as personhood credential technologies are still emerging and only beginning to form partnerships with mainstream social, gaming, and finance applications in 2025 [16, 26, 33].

3.2 Semi-Structured Interview Procedure

We designed the interview script based on our research questions outlined in the introduction Section 1. The study protocol was structured according to the following sections: (1) ask about current practices of identity verification; (2) present an educational video to provide an overview of PHCs; (3) investigate factors that influence users' preferences for PHCs as identity verification through scenario-based sessions; (4) facilitate a design session to conceptualize users' expectations.

In the first section, we first asked a set of questions to understand participants' current practices of online platforms and the types of identity verification methods they had experience with. This aims to understand their familiarity with various types of verification, including biometrics and physical IDs.

In the second section, we then asked about participants' current understanding and perception of personhood credentials, either from prior knowledge or from intuition, by just hearing the term. The majority found this an unfamiliar terminology; however, it referred to a form of personal identification, often associated with biometric verification. PHCs remain an emerging technology with a limited user base. To ensure our participants had a baseline understanding of PHCs before proceeding, we created and showed them an introduction video [2] that explains the core concepts of PHCs using accessible visuals and audio. This video encompasses an overview of PHCs based on literature[37], using World App as a real-world example (Appendix A.1). We asked the same set of multiple-choice knowledge questions both before and after the video. We observed an improvement in response rate, such as *"What is the primary goal of PHC?"* from 85% to 100% after watching the video.

In the third section, we explored specific application scenarios of PHC to understand factors that influence participants' preferences towards PHCs as well as identify their perceived risks and benefits. We examined the following six scenarios: (1) Financial service, (2) Healthcare service, (3) Social media, (4) LLM applications, (5) Government portal, and (6) Employment background check. We grounded our scenario design based on literature and existing PHC systems to capture broader design preferences and tensions around emerging challenges of identity verification (Section 2.3) as well as to reflect real-world contexts where identity verification is commonly required or is likely to be incorporated in the near future. We have also incorporated various types of data or credentials requirements (e.g., physical ID, biometrics, etc.) across scenarios to maintain diversity in our discussion with participants based on former literature and existing systems. For each of the six scenarios, we explored participants' perceptions of using PHC in hypothetical situations that align with the research focus, as well as to help participants relate PHC concepts to real-world applications. This is particularly useful for this study, where user perceptions and expectations under specific conditions are crucial to devise solutions [52]. We asked about their feelings, perceived benefits, and risks. We also nudge them to think about any privacy and security perception around using PHC and types of data (e.g., iris, face, government id, etc.) involved in issuing PHC.

In the fourth section, we began by refreshing participants' memories of the various risks and concerns discussed in the earlier section. Following this, we guided participants to brainstorm potential design solutions by sketching their ideas. To facilitate the sketching process, we developed sketch notes in Zoom to help participants generate ideas, particularly when starting from scratch is challenging. This exercise aimed to understand participants' thought processes and visualize the measures they would suggest for PHC design. We encourage participants to explain their reasoning in a think-aloud manner.

[2] https://anonymous.4open.science/r/PHC-user-study-14BB/

Theoretical Saturation. In our early interviews, each session yielded some additional codes regarding the benefits, perceptions, and expectations of PHC, such as *less uploading documents, easier than the usual verification, trusted 3rd party involvement.* As we conducted, the new code gradually slowed over time, and increasingly reinforced existing themes. In line with studies of a similar nature [85, 107], we interviewed participants until we observed thematic saturation [69, 98, 110]. We assessed saturation at the point where new interviews no longer produced novel codes. At 25 participants, interviews primarily repeated established themes where our codebook reached 97 codes, increased to 98 at participant 26, and remained at 98 for participant 27. We concluded recruitment upon achieving saturation.

Post-Survey. We conducted a post-survey to obtain participants' PHC preference quantitatively. It included questions on participants' preferences regarding credential type, issuer, and issuance system for the scenarios (e.g., financial, medical, etc.) considered in our interview.

3.3 Data Analysis

Once we got permission from the participants, we obtained interview data through the audio recording and transcription on Zoom. We utilized a thematic analysis method for evaluating our qualitative data, as described by Braun and Clarke [47]. Firstly, first coder independently coded 40% of the data, then compared and developed new codes until we got a consistent codebook. After that, they split the remaining data and coded separately with the codebook. We grouped the codes into sub-themes and then into main themes that aligned with the research questions. These themes were organized into broader categories. We have made our codebook publicly available in the project repository linked in the footnote [3].

4 RQ1: Users' Current Impression of PHC

Current Verification Practices. Participants most commonly mentioned financial services, including online banking and investment platforms, as well as health services, government-related, and cross-border regional verifications in digital and physical forms of credentials for identity verification. Several participants mentioned the requirement to upload government IDs (e.g., social security number, driver's license) when onboarding, as P7 said– *"For Robinhood, it asked for uploading my government-issued IDs like driver's license and passport."* Similarly, P2 explained her verification experience in government services requiring multiple information *"Last year I was requesting my tax filing documents in IRS. I had to verify my identity with my face, as well as information from government-issued IDs to confirm my identity. [id.me [22]]."* Beyond financial and government services, identity verification has also become essential in marketplace apps, P1 illustrated this trend with Airbnb, explaining that they are reluctant to provide IDs *"If you book as a renter, you would need to verify your government ID for eligibility to book your first stay."*

Trade-offs between known and unknown privacy guarantee. Participants often made trade-offs between familiar security guarantees associated with traditional verification methods and the less clear assurances of emerging PHC. As P18 mentioned, she heard about World ID as a personhood credential and remarked *" They scan your iris, create a unique code, and re-verify me again later time. I guess that means they still keep some sort of data from the iris scan. I would still stay with email or traditional verification as I know what they are keeping. Even though World App guarantees privacy with hi-tech, I don't exactly know how much privacy I have in human tests. I'm not saying it's a bad idea, it's just i am unsure."* P23 with age ranges from 45-52 noted– *"it's just easier to do with email or my physical photo ID in an old system Newer technology is supposed to be faster and more user-friendly, but to me, iris scan or selfie scan, I can't*

[3] https://anonymous.4open.science/r/PHC-user-study-14BB/

even know if I am doing it correctly. I'm getting to the point where I can say I'm old-fashioned." This underscores the generational divide in preferences with emerging technologies compared to established methods.

Perceived Benefits of PHC: Fairness in Representation. Participants discussed fairness and the potential benefits of PHCs. P19 shared her experience with online study platforms which is one of the primary means of earning, *"often time I got "time out or returned" in this platform and earlier I thought I am slow responding to survey request I received on my account. Lately, it happens too often, feels like there are bots or a group of people are more proactive in participating in surveys. honestly, it reduces the chances for me being selected for research studies "* She emphasized that personhood verification could help filter out bots and increase her chances as a genuine participant. P21, who is a dedicated gamer, finds it disheartening to encounter players, likely bots, who level up so quickly. To emphasize the benefit of PHC, he mentioned *"I play online games with other people around the world, like shooting games. We regularly encounter bots in these games, which basically dilutes our experience. As an experienced player, I can usually tell when someone isn't a real person based on how they play. Personhood verification could be a good feature."* P27 sees the potential of personhood with privacy in sensitive areas involving children. *"Kindergarten registration, you have to give all sorts of proof. Instead I would like to verify certain things with personhood credentials given based on all those proof."*

Perceived Concerns of PHC: Power, Control, Security Participants expressed concerns about potential risks, including the centralized power of the issuer, uncertain regulations of emerging technology, the authenticity of PHC, and misuse of anonymity. For instance, P6 pointed out that centralization of credential information with PHC issuers could lead to power being misused, saying, *"you're gonna give all your information to a small group or institutions to issue PHC. So they have the power that can be abused later."* P10 also highlighted the risks in high-stakes situations, such as employment background verification, where an inauthentic PHC could have serious consequences. He noted *"I don't know if it's possible to fake government-issued ID. I feel like I'm probably concerned about an inauthentic PHC."* P4 expressed similar concerns about data exposure to an employer if they only share PHC *"For instance, I had a job offer that required details about my criminal record from five years ago. It would probably reveal more even if I only share PHC."*

PHC Preference Dilemma: Physical and Digital Verification Many participants often relate their offline experiences when describing their preference for credentials and issuance systems. For instance, some of them described the inconvenience of carrying physical IDs , saying *"When you need to buy some alcohol drinks, take a flight, you need to show your driver's license or passport. But it's not a very convenient, because I have to carry the physical ID all the time."* Another participant pointed out the potential risk of IDs being stolen, citing, *"I think this information may be lost, or maybe stolen. So it's a risk."* While participants highlighted the inconvenience and physical vulnerabilities of traditional IDs, they simultaneously shared the limitations of digital identifiers, such as verification through phone number [OTP] during international travel.

Regulatory Uncertainty in Emerging Technologies Participants emphasized that the trust in PHC depends not only on their technical implementation but also on the certainty and interoperability of accompanying policy regulations. Although they recognized PHC's potential to reduce fraud, some raised negative impressions related to the absence of solid policy regulations with other emerging technologies, often linked to experiences with cryptocurrency or blockchain systems. P13 expressed concern that PHC could face sudden restrictions with the fragility of such systems: *"The only problem actually was with cryptocurrency and things like that. There are no regulations, so when the UK brought out some new legislation, they just decided that UK users couldn't use their service anymore. My only concern with that would be kind of. It might get a bit complicated, especially if the websites you are signing up to are in different countries to you."* Such uncertainty reinforced perceptions of PHC as vulnerable and difficult to rely on.

Limited Understanding of Cryptographic Protections Participants' reflections revealed misconceptions about how data in PHC would be protected. P8 assumed that any credential data could eventually be stolen once adversaries found a way to misuse it: *"Everything is able to be stolen. It might work in the short term until people who do bad things figure out how to steal it and use it. We came up with paper versions of authentication, like a driver's license, because we needed something to identify people. But now we realize that it is not as secure as it can be. So when you start a new job, you have to bring more than one form of identification to prove. So I think using biometrics would feel secure until a way is found to misuse it, just like a paper identification."* This perspective suggests that participants might believe that attackers, similar to physical IDs, could directly access digital data. What was missing in their mental model was an understanding of PHC's underlying cryptographic protections, such as zero-knowledge proofs, which ensure that sensitive information is never directly revealed while still allowing verification of personhood.

5 RQ2: Factors Influence on How People Would like to Verify Themselves

In this section, we discuss various factors that influence people's preferences, including application types, credential types, stakeholders as issuers, and architecture types.

5.1 Data Requirements to Issue Credential

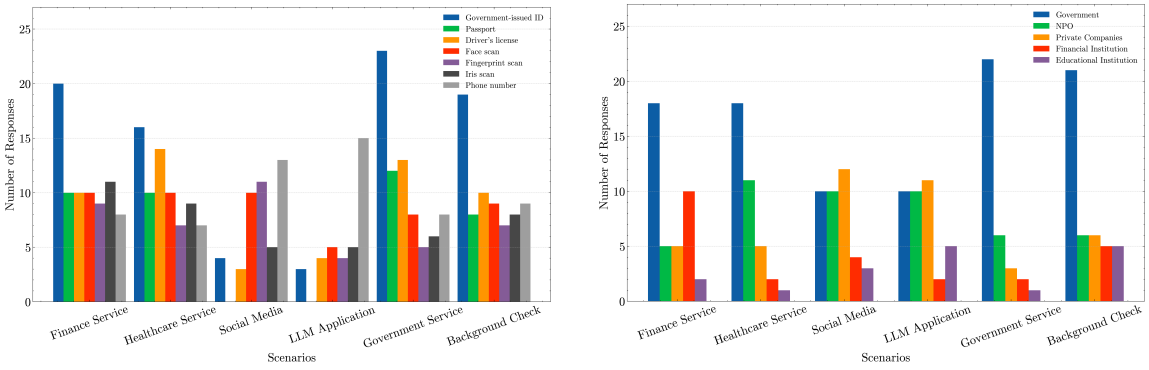
Participants generally categorized data requirements into three main types: ❶ Government-issued IDs, such as social security numbers, passports, and driver's licenses; ❷ Biometrics, including face, fingerprints, and iris; and ❸ Digital identifiers, such as phone numbers and email addresses. In figure 1a, government-issued ID is the most preferred data to issue PHC across applications, except social media and LLM applications. Phone number is most preferred for LLM applications, followed by iris scan.

Sensitivity, Security, & Efficiency Across Different Biometrics Several participants highlighted their preference for their PHC associating with government-issued IDs, as they were most familiar with this approach and perceived it as reliable. We found that individuals have varying preferences across biometric types, such as fingerprints, facial recognition, selfies, and iris scanning. Firstly, participants considered fingerprints as less invasive and less sensitive. In contrast, facial recognition was discussed as a more sensitive method, as P5 said, *"I would say fingerprint is fine, but face is too much. you can be identified in public settings in streets. If they have camera [surveillance], anyone can just trace your whereabouts."* Most participants expressed their views about the iris method without having direct experience with this method. Notably, P8 said- *"iris verification is probably the more secure of all, fingerprints and facial recognition can be regenerated. But eye is a very complex organ in the body. I would choose iris, because I think it's the most secure."* On the same note, P23 highlighted challenges with his father's fingerprint, noting that it had become difficult to identify due to the construction work making his prints blur over time.

Combination of Multiple Credentials Participants emphasized the importance of using multiple types of credentials to enhance security. P13 indicated this preference, *combination of facial scan and fingerprint combination. If you're wanting to prove this is the person. Then it would make sense to have more than one biometric. I don't know if it's possible to fake somebody's. If there are completely two different biometrics, it would be more difficult to fake."* In cases like financial services, many participants preferred PHC issuance based on both physical ID (e.g., gov ID) and biometrics (e.g., iris).

5.2 Stakeholder Types

Preferences of PHC Issuers: Control and Practicality Participants expressed varied levels of acceptance regarding the preferred issuers of PHC. Across all application scenarios (Figure 1b), government entities emerged as the most



(a) Results of Credential Preference: Which type of credentials would you prefer to use as personhood verification for each scenario? (Multiple selections were allowed.)

(b) Results of Issuer Preference: Which type of issuers would you prefer to issue and manage your PHC for each scenario (Multiple selections were allowed.)

Fig. 1. Survey Responses of PHCs (a) Credential Preference (b) Issuer Preference: Participants' preferences are context-dependent, particularly showing contrasts between financial, healthcare, and government services versus social media and LLM applications.

trusted issuers for the majority of participants, followed by nonprofit organizations (NPOs). P5 noted– *"Government is my preferred. If there are certain organizations are leveraging 3rd party organizations, they should be regulated and under government supervision. The least favored one is private companies without supervision."* P24 suggested that local-level governance could serve as a practical intermediary, reflecting his experience in the Netherlands, where municipalities serve as the central point for identity verification. However, practical considerations influenced participants' views in certain domains, particularly social media and LLM applications, where private companies were rated as acceptable issuers. As P19 said *"I don't see it happening - social media involve govt vetted PHC. its just not practical. i don't want gov issued phc for social media, i am not fool to allow govt to another layer of surveillance."* In contrast, a group of participants favored nonprofit organizations for domains like healthcare and social media, valuing their balance of trust and regulation, P10 stating *"So NPOs with government backing, they could be another trustworthy source, but not as intense as the govt. to balance it out."* This contrast underscores the complex trade-offs individuals consider when evaluating trust, regulatory oversight, and practicality in selecting entities to issue PHCs.

Trustworthiness of Stakeholders: Legal Authority vs. Brand Value Due to the nature of PHC issuers being responsible for handling identity information, participants expected them to be secure enough to leave sensitive information. We observed that participants' perceptions of trustworthiness were closely tied to the presence of legal and regulatory oversight. P5 explained his trust in banks comes from regulatory systems: *"They are being monitored by federal agencies. Their activities are monitored. They are under a lot of regulations. So there is a monitoring system that is tracking banks."* P26 similarly noted that healthcare systems are safe and confident because of legal protections such as HIPAA. Several participants emphasized the role of brand value and familiarity in shaping their confidence in issuers. P1 noted, *"I generally try to stay away from platforms that I haven't heard before, where they ask for very sensitive material, like my passport or my driver's license for verification. "* This perspective illustrates how users relied on brand familiarity as a proxy for trust, even without knowing the actual security practices. While governments, financial and healthcare service providers derived trust from legal and regulatory oversight, well-known technology companies earned trust through their reputation and visibility in everyday services.

5.3 Architecture Types

Decentralized vs. Centralized Participants highlighted the risks of centralized storage, preferring decentralization for its enhanced security. P8 stated *" You've created a wall between any problems with data theft, with a centralized data storage. They only have to breach the walls of one castle with decentralized. They have to breach the walls of two different castles, which makes it a lot more complex and most people won't. "* In contrast, participants who expressed a preference for a centralized approach highlighted its simplicity and ease of use. P21 stated *"I feel like central authority can respond to any threat aftermath more effectively for centralized issuance and I guess central, like if gov is issuer then it will have global legitimacy, i can use it for customs."*

In Between Centralization and Decentralization Some participants expressed preferences for issuers with a balanced approach of centralized and decentralized systems. P1 highlighted a mixed preference, favoring decentralization while emphasizing the government's oversight, *"I think it's sort of in the middle. I think decentralized would be the right way to go, because. as expecting the Government to have enough resources to keep verifying PHCs would be hard...But the verification, like the issuing authority, is still a government, and the Government still has oversight on how these verification systems work."*

6 RQ3: Design Suggestions for PHC

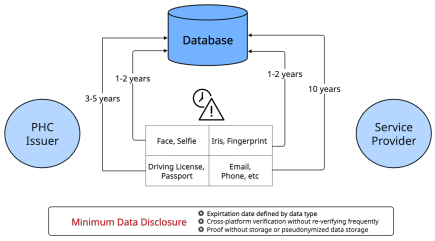
6.1 Design Themes from Participants' Sketch

Participants expressed specific needs for PHC systems, primarily focusing on enhancing security and trust while accommodating diverse needs. From the design sessions, we identified the following themes.

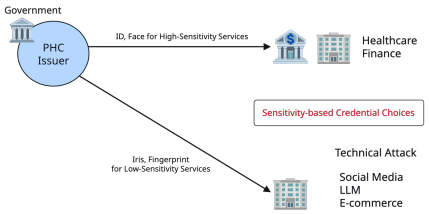
Design Theme 1: Time-bounded Credential for Minimum Data Disclosure Some participants expect credentials to verify personhood with the least amount of personal data, avoiding detailed personal or biometric data collection for a long period. Another expectation was the portability of preferred credentials to be used across platforms without re-verifying frequently. To address these, some suggested features or design concepts that were limited to a validity period, proof without storage, or pseudonymization of the data when storing it. P21 mentioned - *"I want a credential that works like a trusted pass—valid only for a set time (e.g., 30 days, 6 months, or 1 year), with reminders before it expires. It should prove I am a real person without storing my sensitive details or tying them to my real-world identity, like some level of anonymity. Just give me the freedom to be verified without being exposed."* , which is depicted in Figure 2a.

Design Theme 2: Sensitivity-based Usable Credential Choice for PHC Many participants expressed sensitivity-dependent credentials as presented in Figure 2b. They suggested a design that allows choices for end users based on their perceived level of security needs across services in healthcare, finance, social media, etc. To illustrate the concept, P3 provides a design where she made a choice of government-issued ID or face to obtain a PHC for services in healthcare and finance. In her words- *"I think it very much depends on the scenario. Creating a bank account or an account on a government website, or with a healthcare provider. In terms of financial security, or on the government side, my preferred would be a face scan or a video call to verify my face and uploading a doc like my government-issued residence permit, or my passport. Whereas in cases that don't have that much of a security concern, like an account on ChatGPT, or a social media account, I would be okay with a fingerprint scan or an iris scan."* She considers fingerprint and iris are less sensitive since face scan can potentially reveal one's identity, stating *" I think the iris, fingerprint scanning less of a risk, because bad actor needs to have a advanced or physical technology to do so unlike face."*

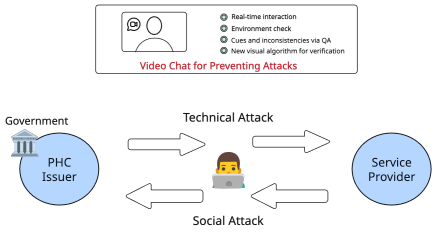
Design Theme 3: Visually Interactive Human Check. Another design theme comes up where participants explain how *"video chat"* offers several advantages in preventing social attacks during personhood credential issuance by



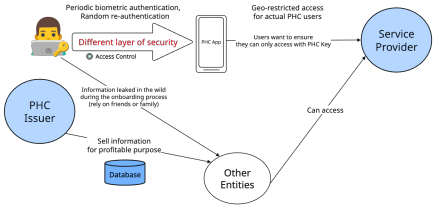
(a) Illustration to depict time-bounded credential with mechanisms that minimize data exposure



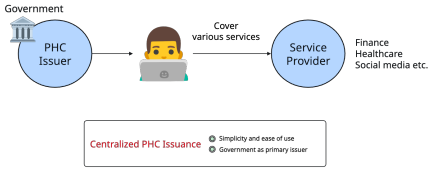
(b) Illustration of choice for users to choose various data requirements for PHC issuance for different applications



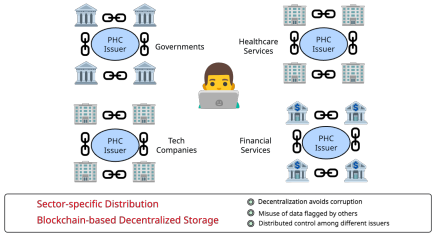
(c) Illustration to depict a comprehensive, visually interactive human check with video chat for humanness, environment check



(d) Illustration to depict periodic biometrics, dynamic authentication, geo-restricted access



(e) Illustration to depict single issuer system with the government



(f) Illustration to depict decentralization for PHC governance

Fig. 2. Design suggestions for PHC: each represents the following design themes (a) Time-bounded credential for minimum data disclosure; (b) Sensitivity-based usable credential choice for PHC; (c) Comprehensive, visually interactive human check; (d) Mitigate PHC misuse; (e)(f) Distribute power across issuer: decentralized vs centralized.

triangulating real-time interaction, visual verification, and environment check. As P2 said *"video chat could be a way to avoid social attacks. This way service provider would ask you a lot of questions to make sure you are not controlled by someone else, and they would ask to move my camera, take videos of my whole room to make sure there's no one else beside me. And of course, it's it would. It would not be a 100% thing, things [only face, ids] are still the old stuff. This could be a new step to developing PHC algorithm."* P2 further emphasized how **human interaction** is still a key when stepping into new technological innovation where in the issuance process, trained staff can assess subtle cues and inconsistencies that automated systems might miss, potentially **detecting social engineering attempts** or ask personalized questions based on the user's responses and behavior, making it difficult for attackers to prepare scripted answers (Figure 2c).

Design Theme 4: Mitigate PHC Misuse: Periodic Biometrics, Dynamic Authentication, and Geo-Restricted Access. Participants suggested enhanced key management for the PHC system to address potential misuse, such as identity selling, credential sharing, and unauthorized account setup (Figure 2d). Suggestions included periodic biometric

verification (e.g., facial recognition or fingerprint scans during login) or random re-authentication to ensure that only the credential holder can access the system (P6, P8, P13, P18, P23). P13 highlighted the risk of credential sharing during onboarding, where users may rely on friends or family for setup assistance, potentially leading to unauthorized access. To mitigate this, P13 proposed combining biometrics with dynamic authentication methods, such as time-sensitive push notifications. Additionally, P13 suggested implementing geo-fencing to restrict access from unfamiliar locations or devices, reducing the risk of misuse if credentials are leaked. These suggestions aim to ensure that PHCs are used securely and by the intended user across different services.

Design 5: Distribute Power Across Issuer: Decentralized vs Centralized Participants (P5, P9, P10) frequently highlighted the importance of a single issuer for PHC, prioritizing a unified point of trust. For example, P10 suggested the government as the primary issuer for various services, arguing that involving third parties, such as insurers in health contexts, complicates credential management (Figure 2e). Conversely, others (P1, P7, P11) supported a multi-issuer approach, leveraging blockchain-based systems to enable decentralized storage and sector-specific distribution of power, addressing trust and governance concerns in PHC. The main design concept focuses on ensuring that any misuse of data by one entity would be immediately flagged by others and distributed control among different issuers when included as decentralized issuance systems. P7 illustrated the concept by stating *"The important part is, they will have the same information all at once and they are synced together. So someone is uploading their document or info, all these companies are going to have it in sync together, so that if there is any misuse of information is going on here, the other companies would get to know it."* (Figure 2f)

6.2 User and Policy Informed Conceptual PHC Design Framework

In this section (Figure 6.2), we present a conceptual framework that synthesizes our findings from user study and policy analysis into concrete design requirements. We outline how each stakeholder plays a key role in technical implementation, regulatory governance, and user experience design. From our work, we present requirements that are uniquely tailored to PHCs as **anonymous, Sybil-resistant, renewable, and multi-issuer credentials** which depend on public trust and correct interpretation of privacy and security guarantees of this emerging technology.

Technical Safeguard For System Builders: Our user study and policy analysis highlight the engineering scope for PHC if adopted in mainstream applications. We found five themes on system requirements. Many of which exceed the requirements of conventional authentication systems.

(1) Time-bound & Renewable Credentials. Prior work in decentralized identity and verifiable credentials [95] sheds light on limiting long-term correlation and storage of sensitive attributes, as specified in the W3C Verifiable Credentials Data Model and GDPR Art. 5 [6, 32]. Participants echoed this concern in our interviews. A possible system requirement is to issue renewable credentials with cryptographic ephemeral periods for limited credential lifetimes (e.g., 30 days, 6 months, 1 year) [46, 129]. To further facilitate anonymity, system builders may provide non-linkable renewal tokens, similar to unlinkable credential refresh in anonymous credential systems [50]. Finally, for the privacy of biometrics and sensitive data used in credential issuance, developers could enforce automatic deletion of raw biometrics immediately after one-way transformation.

(2) Sensitivity-aligned Issuance Paths: Regulatory frameworks such as NIST 800-63 define assurance levels based on context and risk. Users in our study similarly desired tiered issuance models [24, 99]. PHCs can thus support parallel issuance tiers such as High sensitivity: government ID and biometric, Medium: biometric only, Low: phone number

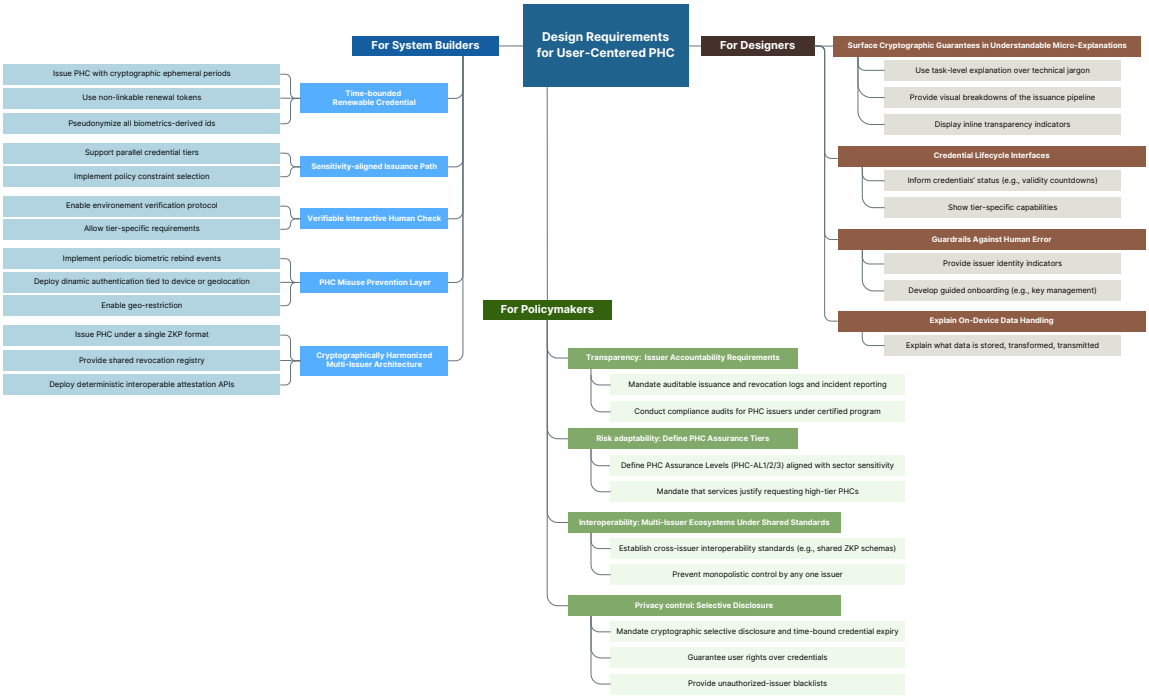


Fig. 3. Overview of user-centered PHC design requirements for different stakeholders: system builders, policymakers, and designers.

and liveness. On top of that, they could add policy constraints based on state and federal-level policy, where certain high-risk sectors (e.g., healthcare, finance) cannot accept low-tier PHCs.

(3) Verifiable Interactive Human Checks: Emerging PHC literature [37] emphasizes that bot resistance must incorporate human-in-the-loop verification. In our study, participants also strongly preferred interactive verification steps in high-risk contexts, such as camera pan, dynamic prompts, and voice liveness. Service providers may produce non-identifying proofs, consistent with privacy-preserving verification mechanisms.

(4) PHC Misuse-Prevention Layer: From our policy analysis, we found identity standards such as the FTC Red Flags Rule and NIST emphasize detection of unusual credential activity [24, 28]. Thus, PHC requires an adapted form of misuse detection, such as biometric re-verifications that generate binary proofs (yes/no) without revealing identity through a liveness test at login or random intervals.

(5) Multi-Issuer Architecture: Our policy analysis shows a critical gap where issuer requirements are underspecified across most digital ID policies. Some frameworks allow "any entity that can sign credentials" (W3C), while others require strict governmental authorization (eIDAS, BSA) [15, 17, 32]. Thus, PHCs should adopt multi-issuer credential architectures that enable PHC issuers, such as governments, nonprofits, and regulated private organizations, to issue PHCs under a single zero-knowledge proof format with a shared revocation registry through certain deterministic attestation APIs.

Governance Requirements For Policymakers: Drawing from the four dimensions highlighted in our policy review, policymakers play a central role in shaping the governance infrastructure for PHC.

(1) Transparency: In OECD identity governance recommendations [27] and GDPR transparency obligations [5], one of the main requirements is issuer accountability in the governance process to maintain auditable issuance, revocation, and regular compliance audits under certified programs and report incidents similar to financial KYC breaches [28].
(2) Risk Adaptability: Mirroring NIST 800-63 [24] security requirements, policymakers should define PHC Assurance Label (e.g., PHC AL1/2/3) aligned with sector sensitivity, where services are obliged to justify their requests for a certain tier of PHC.
(3) Interoperability: Consistent with eIDAS 2.0, EBSI, and W3C standards [12, 15, 19], interoperability expects multi-issuer ecosystems under shared standards. This ensures establishing cross-issuer interoperability standards (e.g., shared zero-knowledge proof schemas) to prevent monopolistic control by any single governmental or corporate issuer.
(4) Privacy Control: Building on selective disclosure frameworks (eIDAS wallet, W3C VC Data Model) [15, 32] polices should enhance users' privacy control via selective disclosure. A potential way is mandating cryptographic selective disclosure as a baseline feature and users' right to deletion, renewal, and reissuance.

Communication & Interaction Requirement For Designers: Our findings reveal four design directions from human factor perspectives.

(1) Understandable Micro-Explanations: Users struggled to interpret humanness proofs, a challenge echoed in prior work on privacy-preserving cryptographic UX [61, 62, 65, 117]. Designer needs to mitigate the gap by surfacing privacy guarantees in understandable micro-explanations. For instance, designers need to translate privacy guarantees into task-level messages ("We confirmed you are a human without learning who you are") rather than stating abstract terminology like "zero-knowledge".
(2) Credential Lifecycle Interfaces: Users frequently shared concerns on how long PHC data will be stored or whether it will be stored. To address these concerns, designers can break down the issuance pipeline, depicting the path of user data, which information the system records, how that data is processed, and deleted into a visual depiction (e.g., "biometric > encrypted hash > deleted immediately").
(3) Guardrails Against Human Error: Research shows that trust depends on issuer recognizability and operational clarity [118]. Thus, for emerging technology, like PHC, design can provide clear issuer identity indicators (e.g., *"Issued by: State X"*). This will help users verify they are interacting with legitimate issuers. Another way is to educate users throughout the onboarding process on key areas, such as privacy notices, key management, and confidence checks, to ensure they understand their workflow within the services for receiving credentials.
(4) Explain On-Device Data Handling: For most participants, the main uncertainty was where biometric or liveness data lives. Thus, interfaces must explicitly explain on-device data handling at every stage on *what stays on device, what transforms into ZK proofs, what is never transmitted, how deletion occurs post issuance.* These explanations align with the "privacy dashboards" required in eIDAS 2.0 and California privacy frameworks (CCPA/CPRA) [8, 15, 30].

7 Discussion

Our findings shed light on a wide range of human factors in designing personhood credentials. In this section, we discuss how the findings can contribute to the current state of knowledge in designing user-centered and secure PHC design.

7.1 Main Findings

Our findings add new knowledge to the literature with the underlying reasoning of why users have certain preferences for PHCs, while existing literature has been limited to identifying preferences alone [83]. A novel discussion is the role of issuers in PHCs. Although prior PHC and Proof-of-Personhood literature emphasizes cryptographic design and systemic architectures (e.g., decentralized issuers, Sybil resistance, ZKPs)[46, 60, 67], limited research has examined how end-users evaluate issuer legitimacy. More recently, a cross-industry collaboration [37] resurfaced the conversation of personhood credentials, highlighting the need for a robust ecosystem of PHC issuers. Participants viewed issuers as a critical determinant of trust where preferences differ by context, with governments most trusted in sensitive domains and private issuers accepted in everyday-life applications, which reflects the need for multiple issuers to avoid centralization risks and prevent monopoly by any single stakeholder [46, 67]. The launch of World App in the U.S. [74] further signals a move toward scalable implementation. A fundamental challenge remains the "chicken-and-egg" dilemma: the absence of a broad ecosystem of PHC issuers hinders the adoption of systems that rely on PHCs, and conversely, the lack of such systems makes it difficult to incentivize the establishment of PHC issuers. Our findings highlight an interdependence and the importance of carefully considering both the issuing ecosystem (e.g., centralized versus decentralized models) and the type of issuer. Finally, participants' uncertainty about PHC mechanisms highlights comprehensibility as a primary barrier, as a new technology [36]. Previous work shows that users misinterpret cryptographic protections when they are not surfaced in accessible ways [38, 88]. Our findings also show that participants' analogies to familiar authentication cues such as behavioral biometrics (e.g., touch dynamics, keystroke dynamics) [84, 96]. This might reduce some friction and improve usability; however, it may introduce threats of linkability and anonymity. Future design may consider strictly on-device processing to broaden the discussion on usability and security trade-off in PHC re-verification. Drawing on findings from the user study and policy analysis, we synthesize a set of technical, governance, and interaction-design requirements for developers, policymakers, and designers.

7.2 Risk–Benefit Analysis and the HCI Trajectory of PHC, as a Privacy-Preserving Technologies

Our result shows a tension between awareness of bot in online environments (e.g., survey platforms, games, and social media) and reluctance to "unknown risk" vectors as a new technology compared to traditional verification. Given this tension, their adoption decision towards PHC is likely to be influenced by risk-benefit analysis shaped by Protection Motivation Theory (PMT) [40, 45, 105, 121], in which individuals act to protect themselves from threats based on perceived severity and costs of adaptive behavior.

Often, participants overlook a central property of PHC systems, the cryptographic or privacy guarantee that ensures personal information used for obtaining PHCs is not disclosed to service providers and is never stored in a directly identifiable form. Nevertheless, our results show that PHC preferences differ across scenarios, clearly revealing a significant gap between the data safety offered by PHC and the end-user's understanding. This hinges upon an emerging issue in human-centered security *"how to communicate cryptographic privacy protections to non-experts."*. Although zero-knowledge proofs have been extensively studied in security research as a key technology underlying modern blockchain systems, they remain largely unexplored within the HCI domain. This gap is significant when mainstream applications can widely benefit from this emerging tool, PHC to defend human signal and interaction in digital communication from bot, non-human and generative communication [37, 60]. This mirrors historical patterns in usable privacy, where innovations such as differential privacy remained technical concepts until widespread deployment forced researchers to develop user-facing explanations[49, 108, 114].

PHCs now occupy a similar moment. The underlying technologies, such as ZKPs of PHC are particularly crucial to enable individuals to prove specific features of their identity while preserving anonymity, making them a foundational mechanism for future identity systems [63, 89, 109]. Yet their benefits remain inaccessible unless PHC systems directly articulate what privacy protections and how these protections map onto users' existing concerns about privacy, misuse, and accountability. As established work on the Technology Acceptance Model (TAM) [57, 58, 123] framed *perceived usefulness* and *perceived ease-of-use* as correlated factors of actual use. Thus, advancing perceptual risk-benefit analysis to actual PHC use requires careful attention to these practical dimensions of system design. For instance, to improve perceived ease-of-use, PHC workflows must make clear that verification occurs only once with the issuer and subsequent interactions rely solely on non-identifying cryptographic proofs [106].

7.3 Standardization of Personhood Credential

As PHCs gain more attention in the AI-mediated world, there is a need for standardized frameworks for secure and reliable system implementation. However, there are still gaps between end-user expectations and existing regulations. The findings of our user study revealed clear expectations for the implementation of PHCs. For example, they expected data expiration that would prevent misuse and leakage. However, current regulations do not clearly define how long personal data (e.g., credential information) will be stored. To enhance transparency within PHC systems, a potential approach from policy analysis is eIDAS, which allows implementing a user-facing dashboard that displays what data is shared and the purpose of data sharing [15]. Making the retention period of the credential information visible would help users better understand and control how their credentials are used. The participants supported a sensitivity-based approach, favoring verification methods that reflect the sensitive nature of each service. Although eIDAS defines different levels of authentication based on risk, most regulations do not provide standardized guidance on how to implement flexible verifications that align with users' contextual needs. To meet these expectations, regulatory frameworks should support multiple credential options and allow users to choose verification methods appropriate to the sensitivity of each service context.

Participants expressed contrasting preferences regarding PHC issuers. While some supported a centralized model led by trusted public institutions, others favored a distributed approach involving multiple issuers across sectors. Current regulations rarely address how credential issuance authority should be structured, leaving open questions around accountability and governance. To address these concerns, future regulatory frameworks should accommodate both centralized and decentralized issuance models. In decentralized contexts, policies must define mechanisms for cross-issuer data consistency and mutual auditability. Similarly, in centralized issuance models, regulatory frameworks must include safeguards to prevent power concentration and misuse, such as independent oversight and clearly defined accountability mechanisms [116].

7.4 Design Implications

Drawing upon users' needs and preferences, we suggest actionable design implications for personhood credentials.

Interface Design to Facilitate Verification Choice. Our findings indicate diverse levels of adoption/onboarding preferences towards PHC issuance, such as the type of data requirement to verify themselves, which largely depends on their own *"security standard"* developed for different types of services. As presented in the center mock-up of Figure 4, sensitivity-based credential choice via tiered assurance levels allows users to choose ground truth data (e.g., gov ID, face, video, fingerprint, social graph, etc) based on their security standards. The interface could explicitly add a design of tiered verification options, each corresponding to a different level of security: Level 1 (Low Sensitivity): email or phone

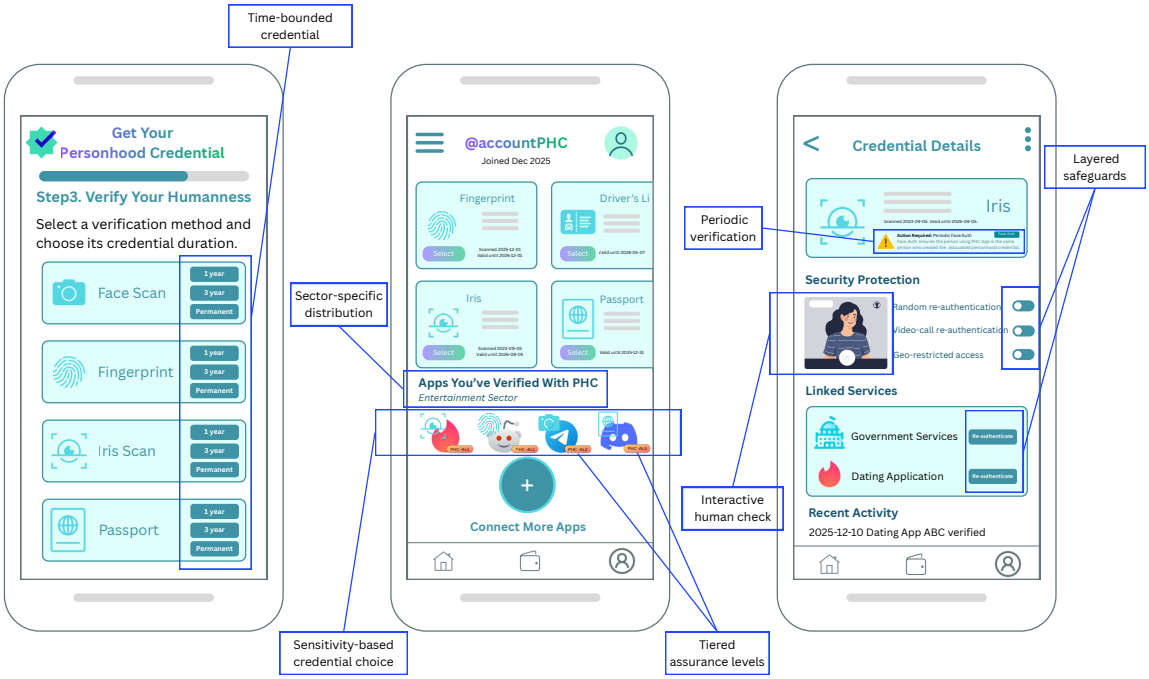


Fig. 4. Integrated PHC interface mock-ups spanning design themes - (Left) Onboarding: Users choose a credential's validity period. (Center) Account Home: Users select which credential to use based on sensitivity contexts. (Right) Credential Management: Users add complementary safeguards, such as interactive human checks.

verification; Level 2 (Medium Sensitivity): physical id; Level 3 (High Sensitivity): Biometric fusion (e.g., facial recognition + voice print); Level 4 (Very High Sensitivity): Multi-factor PHC (e.g., biometrics + social graph verification+physical id), etc.

Portability of Personhood Credential. Our result reveals varied preferences across different services, ranging from financial, health, government, to social media. A possible way is to design interoperable cryptographically verifiable credentials. A verifiable credential contains a claim about the credential holder, issued by a trusted entity, and can be verified without contacting the issuer to prove themselves across various platforms. This approach leverages emerging solutions, such as zero-knowledge proofs [119], in conjunction with design principles and standards, including the W3C verifiable credentials data model and the DIF universal resolver [95]. Figure 4 shows that a single PHC application can support interoperable PHC, where users can prove their personhood across services without verifying multiple times.

Dynamic & Multi-factor Personhood Verification One of the repeated concerns in our study was whether PHC can be inadvertently shared/used by friends/family, hacked, or stolen. To address this concern, a potential design implication is to design a dynamic Multi-Factor Personhood Credential (PHC). First, when users verify themselves for the first time, the prompt can combine interactive biometrics, such as a video call, with interaction knowledge questions and sharing a physical ID to compare several ground truth data to issue a robust PHC. Second, to maintain security, a periodic biometrics verification with a time-based trigger system can be designed to prompt for biometrics verification at random intervals or during high-risk activities. These layered safeguards are illustrated in Figure 4 as interactive human checks and periodic verification.

Decentralized Standards for Industry-Government Issuance System. Our work indicates issuance system and issuers (e.g., govt, private company; decentralized vs centralized) are one of the main factors leading to security and trust perception, thus the broader adoption. To ensure global accessibility in supporting multiple stakeholders as issuers, the system would incorporate cross-chain interoperability protocols like Polkadot or Cosmos and utilize a permissioned blockchain network (e.g., Hyperledger Fabric) to create a distributed ledger for credential issuance and verification. A smart contract would govern the issuance process, ensuring compliance with predefined standards set by both industry and government entities.

Communicate Underlying Cryptographic Mechanisms Our findings show that privacy and security safeguards underlying PHCs remained largely invisible to participants. This communication gap between technical protections and users' perceptions created uncertainty about how their data would be exchanged and safeguarded. Prior work reports that end-users often struggle to make sense of cryptographic operations [38, 42, 61, 62, 66, 115]. However, small design choices such as the rock icon for browser security status can improve user perception of safety [66]. In this context, human-centered security research would develop metaphors and interface designs to clearly convey whether credential information is being handled securely through emerging cryptographic mechanisms such as zero-knowledge proofs.

8 Limitations and Future Work

This study has some limitations. Participants formed their opinions based on a conceptual explanation in an informational video presented during the study. While we focused solely on the basic overview of PHCs, it may have constrained participants' engagement with more abstract concepts such as privacy and security. Their responses might differ from those based on direct interaction with functional PHC applications. For future work, we aim to develop an interactive prototype that incorporates concrete user interfaces and task flows to understand participants' interaction and challenges of PHC use and allow for the evaluation and refinement of interface design tailored to real-world application scenarios. Another consideration is that our sample size may limit the diversity of user preferences; however, our findings provide valuable qualitative insights that lay the groundwork for broader PHC research. Building on the design implications that emerged from users' reflections, future work can involve experts such as identity architects, policymakers, and eventually individuals who gain real-world exposure to PHC systems by examining how they translate into system requirements and interface design needs. By connecting user perspectives with expert development practices, future research can support the creation of PHC systems that remain socially acceptable as the technology matures and moves toward deployment.

9 Conclusion

Our study uncovered diverse user perceptions, including trade-offs between traditional verification methods and emerging approaches such as PHCs, as well as dilemmas between physical and digital verification. Furthermore, we highlighted nuanced preferences for each system design dimension: credentials, issuers, and architectures. Additionally, practical PHC functions such as limited credential validity, sensitivity-based selection, interactive human checks, and distributed issuance architectures were identified through design suggestions. To our knowledge, this is the first user study to focus on PHCs. Our findings extend beyond PHCs, shedding light on key insights for identity verification.

References

[1] [n. d.]. 106 defendants indicted in Social Security disability fraud costing federal taxpayers hundreds of millions — ice.gov. https://www.ice.gov/news/releases/106-defendants-indicted-social-security-disability-fraud-costing-\federal-taxpayers. [Accessed 30-05-2025].

[2] [n. d.]. 2024 Wyoming Statutes :: Title 40 - Trade and Commerce :: Chapter 30 - Digital Identity Act :: Section 40-30-101 - Definitions. — law.justia.com. https://law.justia.com/codes/wyoming/title-40/chapter-30/section-40-30-101/. [Accessed 02-06-2025].

[3] [n. d.]. 3 Questions: How to prove humanity online — news.mit.edu. https://news.mit.edu/2024/3-questions-proving-humanity-online-0816. [Accessed 06-06-2025].

[4] [n. d.]. AI-Generated Fake IDs Bypass Crypto Exchange KYC Checks, OKX Says Industry-Wide Issue. https://www.nasdaq.com/articles/ai-generated-fake-ids-bypass-crypto-exchange-kyc-checks-okx-says-\industry-wide-issue. [Accessed 30-05-2025].

[5] [n. d.]. Art. 12 GDPR – Transparent information, communication and modalities for the exercise of the rights of the data subject - General Data Protection Regulation (GDPR) — gdpr-info.eu. https://gdpr-info.eu/art-12-gdpr/. [Accessed 05-12-2025].

[6] [n. d.]. Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR) — gdpr-info.eu. https://gdpr-info.eu/art-5-gdpr/. [Accessed 05-12-2025].

[7] [n. d.]. CA DMV Wallet & mDL Pilot - California DMV — dmv.ca.gov. https://www.dmv.ca.gov/portal/ca-dmv-wallet/. [Accessed 23-01-2025].

[8] [n. d.]. California Consumer Privacy Act (CCPA) — oag.ca.gov. https://oag.ca.gov/privacy/ccpa. [Accessed 02-06-2025].

[9] [n. d.]. California State Digital ID Strategy — digitalidstrategy.cdt.ca.gov. https://digitalidstrategy.cdt.ca.gov/index.html. [Accessed 05-06-2025].

[10] [n. d.]. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far (Published 2018) — nytimes.com. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. [Accessed 23-01-2025].

[11] [n. d.]. Decentralized Identifiers (DIDs) v0.13 — w3c-ccg.github.io. https://w3c-ccg.github.io/did-spec/. [Accessed 23-01-2025].

[12] [n. d.]. Decentralized Identifiers (DIDs) v1.0 — w3.org. https://www.w3.org/TR/did-1.0/. [Accessed 05-06-2025].

[13] [n. d.]. DIF - Decentralized Identity Foundation — identity.foundation. https://identity.foundation/. [Accessed 23-01-2025].

[14] [n. d.]. Disability benefits cheat secretly filmed completing 5k runs — bbc.com. https://www.bbc.com/news/articles/c88z8jn8gj0o. [Accessed 30-05-2025].

[15] [n. d.]. eIDAS 2.0 | Updates, Compliance, Training — european-digital-identity-regulation.com. https://www.european-digital-identity-regulation.com/. [Accessed 02-06-2025].

[16] [n. d.]. Experience Real Connections with World ID and Match Group — world.org. https://world.org/blog/announcements/experience-real-connections-with-world-id-and-match-group. [Accessed 12-09-2025].

[17] [n. d.]. FinCEN.gov — fincen.gov. https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act. [Accessed 02-06-2025].

[18] [n. d.]. HB470 GOVERNMENT DIGITAL VERIFIABLE 2 RECORD AMENDMENTS. https://le.utah.gov/~2023/bills/hbillenr/HB0470.pdf. [Accessed 02-06-2025].

[19] [n. d.]. Home - EBSI - — ec.europa.eu. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI. [Accessed 05-06-2025].

[20] [n. d.]. Humanness in the Age of AI — world.org. https://world.org/blog/engineering/humanness-in-the-age-of-ai. [Accessed 30-10-2024].

[21] [n. d.]. Idena Whitepaper. https://docs.idena.io/docs/wp/summary/. [Accessed 26-05-2025].

[22] [n. d.]. New identity verification process to access certain IRS online tools and services | Internal Revenue Service — irs.gov. https://www.irs.gov/newsroom/new-identity-verification-process/-to-access-certain-irs-online-tools-and-services. [Accessed 20-01-2025].

[23] [n. d.]. New Ways to Verify Your Age on Instagram — about.instagram.com. https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram. [Accessed 30-10-2024].

[24] [n. d.]. NIST SP 800-63 Digital Identity Guidelines — pages.nist.gov. https://pages.nist.gov/800-63-4/. [Accessed 02-06-2025].

[25] [n. d.]. Promoting Access, Equity, and Inclusion With AI and Digital Identity. https://network.id.me/wp-content/uploads/IDme-Anti-Bias-Whitepaper.pdf. [Accessed 26-05-2025].

[26] [n. d.]. Razer ID - Be Verified As Human | Razer United States — razer.com. https://www.razer.com/software/proof-of-human. [Accessed 12-09-2025].

[27] [n. d.]. RECOMMENDATION OF THE COUNCIL ON THE GOVERNANCE OF DIGITAL IDENTITY. https://one.oecd.org/document/C/MIN(2023)8/FINAL/en/pdf. [Accessed 05-06-2025].

[28] [n. d.]. Red Flags Rule — ftc.gov. https://www.ftc.gov/business-guidance/privacy-security/red-flags-rule. [Accessed 05-12-2025].

[29] [n. d.]. SB0260 — le.utah.gov. https://le.utah.gov/~2025/bills/static/SB0260.html. [Accessed 02-06-2025].

[30] [n. d.]. The CPRA — thecpra.org. https://thecpra.org/. [Accessed 02-06-2025].

[31] [n. d.]. U.S. says Russian bot farm used AI to impersonate Americans. https://www.npr.org/2024/07/09/g-s1-9010/russia-bot-farm-ai-disinformation. [Accessed 30-05-2025].

[32] [n. d.]. Verifiable Credentials Data Model v2.0 — w3.org. https://www.w3.org/TR/vc-data-model-2.0/. [Accessed 05-06-2025].

[33] [n. d.]. World Card: Your Digital Assets, Accepted Anywhere Visa Is — world.org. https://world.org/blog/announcements/world-card-your-digital-assets-accepted-anywhere. [Accessed 12-09-2025].

[34] [n. d.]. World Whitepaper — whitepaper.world.org. https://whitepaper.world.org/. [Accessed 26-05-2025].

[35] [n. d.]. You can now generate fake passports with GPT-4o. It took me 5 minutes to… | Borys Musielak | 439 comments — linkedin.com. https://www.linkedin.com/posts/musielak_you-can-now-generate-fake-passports-with-activity-\7312844061973917698-v_sF/. [Accessed 30-05-2025].

[36] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[37] Steven Adler, Zoë Hitzig, Shrey Jain, Catherine Brewer, Wayne Chang, Renée DiResta, Eddy Lazzarin, Sean McGregor, Wendy Seltzer, Divya Siddarth, et al. 2024. Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online. *arXiv preprint arXiv:2408.07892* (2024).

[38] Omer Akgul, Wei Bai, Shruti Das, and Michelle L Mazurek. 2021. Evaluating {In-Workflow} messages for improving mental models of {End-to-End} encryption. In *30th USENIX Security Symposium (USENIX Security 21)*. 447–464.

[39] Mohammad Majid Akhtar, Rahat Masood, Muhammad Ikram, and Salil S Kanhere. 2024. SoK: False Information, Bots and Malicious Campaigns: Demystifying Elements of Social Media Manipulations. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*. 1784–1800.

[40] Elham Al Qahtani, Peter Story, and Mohamed Shehab. 2024. The impact of risk appeal approaches on users' sharing confidential information. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–21.

[41] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj. 2009. Two factor authentication using mobile phones. In *2009 IEEE/ACS international conference on computer systems and applications*. IEEE, 641–644.

[42] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. 2015. Leading Johnny to water: Designing for usability and trust. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 69–88.

[43] Sarah Barrington, Romit Barua, Gautham Koorma, and Hany Farid. 2023. Single and multi-speaker cloned voice detection: from perceptual to learned features. In *2023 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 1–6.

[44] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iPhone and android: Usability, perceptions, and influences on adoption. In *Proceedings 2015 Workshop on Usable Security*. Internet Society, Reston, VA, 1.

[45] Hendrik Boer and Erwin R Seydel. 1996. Protection motivation theory. In *Predicting health behaviour: Research and practice with social cognition models. eds. Mark Conner, Paul Norman*. Open University Press, 95–120.

[46] Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. 2017. Proof-of-personhood: Redemocratizing permissionless cryptocurrencies. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 23–26.

[47] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[48] Clemens Brunner, Ulrich Gallersdörfer, Fabian Knirsch, Dominik Engel, and Florian Matthes. 2020. Did and vc: Untangling decentralized identifiers and verifiable credentials for the web of trust. In *Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications*. 61–66.

[49] Brooke Bullek, Stephanie Garboski, Darakhshan J Mir, and Evan M Peck. 2017. Towards Understanding Differential Privacy: When Do People Trust Randomized Response Technique?. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3833–3837.

[50] Jan Camenisch and Els Van Herreweghen. 2002. Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*. 21–30.

[51] Nicholas Carlini, Matthew Jagielski, Christopher A Choquette-Choo, Daniel Paleka, Will Pearce, Hyrum Anderson, Andreas Terzis, Kurt Thomas, and Florian Tramèr. 2024. Poisoning web-scale training datasets is practical. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 407–425.

[52] John M Carroll. 2003. *Making use: scenario-based design of human-computer interactions*. MIT press.

[53] Orhan Cetinkaya and Deniz Cetinkaya. 2007. Verification and validation issues in electronic voting. *Electronic journal of e-government* 5, 2 (2007), pp117–126.

[54] Hervé Chabanne and Alberto Ibarrondo. 2025. Turnstile cookies: A new root of trust for personhood credentials. In *2025 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 186–188.

[55] Bocheng Chen, Hanqing Guo, Guangjing Wang, Yuanda Wang, and Qiben Yan. 2024. The dark side of human feedback: Poisoning large language models via user inputs. *arXiv preprint arXiv:2409.00787* (2024).

[56] Geumhwan Cho, Jun Ho Huh, Soolin Kim, Junsung Cho, Heesung Park, Yenah Lee, Konstantin Beznosov, and Hyoungshick Kim. 2020. On the security and usability implications of providing multiple authentication choices on smartphones: The more, the better? *ACM Transactions on Privacy and Security (TOPS)* 23, 4 (2020), 1–32.

[57] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA.

[58] Fred D Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q* 13, 3 (Sept. 1989), 319–340.

[59] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I feel like I'm taking selfies all day!: Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA.

[60] Dario Elias Félix de Oliveira Rodrigues. 2024. Personhood Global Whispers: Ethical Echoes of Decentralization? *Procedia Computer Science* 237 (2024), 767–774.

[61] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 401–415.

[62] Albese Demjaha, Jonathan M Spring, Ingolf Becker, Simon Parkin, and M Angela Sasse. 2018. Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In *Proc. USEC*, Vol. 2018. Internet Society.

[63] Matthias Fassl, Lea Theresa Gröber, and Katharina Krombholz. 2021. Exploring user-centered security design for usable authentication ceremonies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15.

[64] Kalsoom Fatima, Sumbal Nawaz, and Sobia Mehrban. 2019. Biometric authentication in health care sector: A survey. In *2019 International Conference on Innovative Computing (ICIC)*. IEEE, 1–10.

[65] A Felt, R Reeder, A Ainslie, Helen Harris, Max Walker, Christopher Thompson, M Acer, E Morant, and Sunny Consolvo. 2016. Rethinking connection security indicators. *Symp Usable Priv Secur* (2016), 1–14.

[66] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 1–14.

[67] Bryan Ford. 2020. Identity and personhood in digital democracy: Evaluating inclusion, equality, security, and privacy in pseudonym parties and other proofs of personhood. *arXiv preprint arXiv:2011.02412* (2020).

[68] Decentralized Identity Foundation. [n. d.]. Decentralized Identity Foundation Grows To 56 Members In Our First Year — medium.com. https://medium.com/decentralized-identity/decentralized-identity-foundation-grows-to-56-members-in-our-first\-year-3ec117e811d8. [Accessed 06-06-2025].

[69] Patricia I Fusch Ph D and Lawrence R Ness. 2015. Are we there yet? Data saturation in qualitative research. (2015).

[70] Brittney Goodrich, Marieke Fenton, Jerrod Penn, John Bovay, and Travis Mountain. 2023. Battling bots: Experiences and strategies to mitigate fraudulent responses in online surveys. *Applied Economic Perspectives and Policy* 45, 2 (2023), 762–784.

[71] Robert Gorwa and Douglas Guilbeault. 2020. Unpacking the social media bot: A typology to guide research and policy. *Policy & Internet* 12, 2 (2020), 225–248.

[72] Meriem Guerar, Luca Verderame, Mauro Migliardi, Francesco Palmieri, and Alessio Merlo. 2021. Gotta captcha'em all: A survey of 20 years of the human-or-computer dilemma. *ACM Computing Surveys (CSUR)* 54, 9 (2021), 1–33.

[73] Dick Hardt. 2012. The OAuth 2.0 Authorization Framework. *Internet Engineering Task Force (IETF) RFC* 6749 (2012).

[74] Robert Hart. [n. d.]. Worldcoin Surges On OpenAI's Sora Announcement — forbes.com. https://www.forbes.com/sites/roberthart/2024/02/19/sam-altmans-worldcoin-soars-after-launch-of-openais-sora-video-tool/. [Accessed 05-06-2025].

[75] Shijing He, Yaxiong Lei, Zihan Zhang, Yuzhou Sun, Shujun Li, Chi Zhang, and Juan Ye. 2025. Identity Deepfake Threats to Biometric Authentication Systems: Public and Expert Perspectives. *arXiv preprint arXiv:2506.06825* (2025).

[76] Franziska Herbert, Collins W Munyendo, Jonas Hielscher, Steffen Becker, and Yixin Zou. 2025. Digital Security Perceptions and Practices Around the World: A {WEIRD} versus {Non-WEIRD} Comparison. In *34th USENIX Security Symposium (USENIX Security 25)*. 1455–1474.

[77] Jennifer Holt and Steven Malčić. 2015. The privacy ecosystem: regulating digital identity in the United States and European Union. *Journal of Information Policy* 5 (2015), 155–178.

[78] https://www.nytimes.com/by/jason henry. [n. d.]. Could Eye-Scanning Crypto Orbs Save Us From a Bot Apocalypse? — nytimes.com. https://www.nytimes.com/2025/05/03/technology/world-eye-scanning-crypto-orbs-launch-in-us.html. [Accessed 01-06-2025].

[79] Sharmin Jahan, Mozammel Chowdhury, and Rafiqul Islam. 2017. Robust fingerprint verification for enhancing security in healthcare system. In *2017 International Conference on Image and Vision Computing New Zealand (IVCNZ)*. IEEE, 1–5.

[80] Laurie A Jones, Annie I Antón, and Julia B Earp. 2007. Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. 91–98.

[81] Dato Kavazi, Victor Smirnov, Sasha Shilina, MingDong Li, Rafael Contreras, Hardik Gajera, Dmitry Lavrenov, et al. 2021. Humanode whitepaper: You are [not] a bot. *arXiv preprint arXiv:2111.13189* (2021).

[82] Dato Kavazi, Victor Smirnov, Sasha Shilina, Jonathan Shomroni, Rafael Contreras, Hardik Gajera, and Dmitry Lavrenov. 2023. Humanode: The First Crypto-Biometric Network. In *Proceedings of the 2023 4th Asia Service Sciences and Software Engineering Conference*. 216–227.

[83] Sandra Kostic. 2024. Who is the better operator of an identity wallet prioritised by the user?-A quantitative survey between state and company. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 1–7.

[84] Masoud Mehrabi Koushki, Borke Obada-Obieh, Jun Ho Huh, and Konstantin Beznosov. 2021. On smartphone users' difficulty with understanding implicit authentication. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[85] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel Von Zezschwitz. 2019. " If HTTPS Were Secure, I Wouldn't Need 2FA"-End User and Administrator Mental Models of HTTPS. In *2019 IEEE Symposium on security and privacy (SP)*. IEEE, 246–263.

[86] Mohinder Kumar, M K Jindal, and Munish Kumar. 2022. A systematic survey on CAPTCHA recognition: Types, creation and breaking techniques. *Arch. Comput. Methods Eng.* 29, 2 (March 2022), 1107–1136.

[87] Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, and Gildas Avoine. 2020. Browser fingerprinting: A survey. *ACM Transactions on the Web (TWEB)* 14, 2 (2020), 1–33.

[88] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. " It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About {FIDO2} Biometric {WebAuthn}. In *30th USENIX Security Symposium (USENIX Security 21)*. 91–108.

[89] Ryan Lavin, Xuekai Liu, Hardhik Mohanty, Logan Norman, Giovanni Zaarour, and Bhaskar Krishnamachari. 2024. A survey on the applications of zero-knowledge proofs. *arXiv preprint arXiv:2408.00243* (2024).

[90] Wanpeng Li and Chris J Mitchell. 2020. User access privacy in OAuth 2.0 and OpenID connect. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 664–6732.

[91] Silvia Lips, Natalia Vinogradova, Robert Krimmer, and Dirk Draheim. 2022. Re-Shaping the EU digital identity framework. In *Proceedings of the 23rd Annual International Conference on Digital Government Research*. 13–21.

[92] Stanislav Mahula, Evrim Tan, and Joep Crompvoets. 2021. With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case. In *DG. O2021: The 22nd Annual International Conference on Digital Government Research*. 495–504.

[93] Deepak Maram, Harjasleen Malvai, Fan Zhang, Nerla Jean-Louis, Alexander Frolov, Tyler Kell, Tyrone Lobban, Christine Moy, Ari Juels, and Andrew Miller. 2021. Candid: Can-do decentralized identity with legacy compatibility, sybil-resistance, and accountability. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1348–1366.

[94] Shrirang Mare, Mary Baker, and Jeremy Gummeson. 2016. A study of authentication in daily life. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 189–206.

[95] Carlo Mazzocca, Abbas Acar, Selcuk Uluagac, Rebecca Montanari, Paolo Bellavista, and Mauro Conti. 2025. A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials* (2025).

[96] Masoud Mehrabi Koushki, Borke Obada-Obieh, Jun Ho Huh, and Konstantin Beznosov. 2020. Is implicit authentication on smartphones really popular? On android users' perception of "smart lock for android". In *22nd International Conference on Human-Computer Interaction with Mobile Devices and Services*. 1–17.

[97] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review* 30 (2018), 80–86.

[98] Luciana de Cassia Nunes Nascimento, Tania Vignuda de Souza, Isabel Cristina dos Santos Oliveira, Juliana Rezende Montenegro Medeiros de Moraes, Rosane Cordeiro Burla de Aguiar, and Liliane Faria da Silva. 2018. Theoretical saturation in qualitative research: an experience report in interview with schoolchildren. *Revista brasileira de enfermagem* 71 (2018), 228–233.

[99] Aleksandra Nenadic, Ning Zhang, Li Yao, and Terry Morrow. 2007. Levels of authentication assurance: An investigation. In *Third International Symposium on Information Assurance and Security*. IEEE, 155–160.

[100] Brooke Norton. 2024. Navigating the Legal Framework: Implementing a Government-Backed Digital Identity in the United States. *Jurimetrics: The Journal of Law, Science & Technology* 64, 2 (2024).

[101] Anil Kumar Pakina, Deepak Kejriwal, Anshul Goel, and Tejaskumar Dattatray Pujari. 2023. AI-Generated Synthetic Identities in Fin Tech: Detecting Deep fakes KYC Fraud Using Behavioral Biometrics. *IOSR Journal of Computer Engineering* 25, 3 (2023), 26–37.

[102] Amna Qureshi, David Megías, and Minoru Kuribayashi. 2021. Detecting deepfake videos using digital watermarking. In *2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 1786–1793.

[103] David Recordon and Drummond Reed. 2006. OpenID 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*. 11–16.

[104] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages.. In *SOUPS*, Vol. 57. 93.

[105] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.

[106] Michael Rosenberg, Jacob White, Christina Garman, and Ian Miers. 2023. zk-creds: Flexible anonymous credentials from zksnarks and existing identity infrastructure. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 790–808.

[107] Malak Sadek, Marios Constantinides, Daniele Quercia, and Celine Mougenot. 2024. Guidelines for integrating value sensitive design in responsible AI toolkits. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–20.

[108] Jayshree Sarathy, Sophia Song, Audrey Haque, Tania Schlatter, and Salil Vadhan. 2023. Don't look at the data! How differential privacy reconfigures the practices of data science. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA.

[109] Hirokazu Sasamoto, Nicolas Christin, and Eiji Hayashi. 2008. Undercover: authentication usable in front of prying eyes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 183–192.

[110] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity* 52 (2018), 1893–1907.

[111] Andrew Searles, Yoshimichi Nakatsuka, Ercan Ozturk, Andrew Paverd, Gene Tsudik, and Ai Enkoji. 2023. An Empirical Study & Evaluation of Modern {CAPTCHAs}. In *32nd usenix security symposium (usenix security 23)*. 3081–3097.

[112] Tanusree Sharma, Vivek C Nair, Henry Wang, Yang Wang, and Dawn Song. 2024. "I Can't Believe It's Not Custodial!": Usable Trustless Decentralized Key Management. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–16.

[113] Sasha Shilina. 2023. Revolutionizing identity verification: An introduction to Proof of Personhood (PoP) protocols. (2023).

[114] Mary Anne Smart, Dhruv Sood, and Kristen Vaccaro. 2022. Understanding Risks of Privacy Theater with Differential Privacy. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2 (Nov. 2022), 1–24.

[115] Christian Stransky, Dominik Wermke, Johanna Schrader, Nicolas Huaman, Yasemin Acar, Anna Lena Fehlhaber, Miranda Wei, Blase Ur, and Sascha Fahl. 2021. On the Limited Impact of Visualizing Encryption: Perceptions of {E2E} Messaging Security. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 437–454.

[116] Matthias Stürmer, Jasmin Nussbaumer, and Pascal Stöckli. 2021. Security implications of digitalization: The dangers of data colonialism and the way towards sustainable and sovereign management of environmental data. *arXiv preprint arXiv:2107.01662* (2021).
[117] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and L Cranor. 2009. Crying wolf: An empirical study of SSL warning effectiveness. *USENIX Secur Symp* (Aug. 2009), 399–416.
[118] Moritz Teuschel, Daniela Pöhn, Michael Grabatin, Felix Dietz, Wolfgang Hommel, and Florian Alt. 2023. 'don't annoy me with privacy decisions!' — designing privacy-preserving user interfaces for SSI wallets on smartphones. *IEEE Access* 11 (2023), 131814–131835.
[119] Andrew Tobin and Drummond Reed. 2016. The inevitable rise of self-sovereign identity. *The Sovrin Foundation* 29, 2016 (2016), 18.
[120] Kalman C Toth and Alan Anderson-Priddy. 2019. Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security & Privacy* 17, 3 (2019), 17–27.
[121] Ehsan Ul Haque, Mohammad Maifi Hasan Khan, and Md Abdullah Al Fahim. 2023. The nuanced nature of trust and privacy control adoption in the context of Google. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–23.
[122] Emily Vella. [n. d.]. Digital Identity awareness grows, but benefits can still be misunderstood - ConnectID — connectid.com.au. https://connectid.com.au/digital-identity-awareness-grows-but-benefits-can-still-be-misunderstood/. [Accessed 18-11-2025].
[123] Viswanath Venkatesh and Hillol Bala. 2008. Technology acceptance model 3 and a research agenda on interventions. *Decis. Sci.* 39, 2 (May 2008), 273–315.
[124] Luis von Ahn, Manuel Blum, Nicholas J Hopper, and John Langford. 2003. CAPTCHA: Using hard AI problems for security. In *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, Berlin, Heidelberg, 294–311.
[125] Ping Wang, Haichang Gao, Xiaoyan Guo, Chenxuan Xiao, Fuqi Qi, and Zheng Yan. 2023. An experimental investigation of text-based CAPTCHA attacks and their robustness. *Comput. Surveys* 55, 9 (2023), 1–38.
[126] Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2019. "Pretty Close to a Must-Have": Balancing Usability Desire and Security Concern in Biometric Adoption. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–12.
[127] Yanfeng Xu, Sarah Pace, Jaeseung Kim, Aidyn Iachini, L Bailey King, Theresa Harrison, Dana DeHart, Sue E Levkoff, Teri A Browne, Ashlee A Lewis, et al. 2022. Threats to online surveys: Recognizing, detecting, and preventing survey bots. *Social Work Research* 46, 4 (2022), 343–350.
[128] Hongwei Yao, Jian Lou, and Zhan Qin. 2024. Poisonprompt: Backdoor attack on prompt-based large language models. In *ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 7745–7749.
[129] Pavol Zajac. 2021. Ephemeral keys authenticated with merkle trees and their use in iot applications. *Sensors* 21, 6 (2021), 2036.
[130] Desheng Zhang, Jianhui Zhang, Youjun Bu, Bo Chen, Chongxin Sun, and Tianyu Wang. 2022. A survey of browser fingerprint research and application. *Wireless Communications and Mobile Computing* 2022, 1 (2022), 3363335.
[131] Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. 2016. Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 aCM sIGSAC conference on computer and communications security*. 270–282.
[132] Fan Zhang, Deepak Maram, Harjasleen Malvai, Steven Goldfeder, and Ari Juels. 2020. Deco: Liberating web data using decentralized oracles for tls. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. 1919–1938.
[133] Hanlin Zhang, Benjamin L Edelman, Danilo Francati, Daniele Venturi, Giuseppe Ateniese, and Boaz Barak. 2023. Watermarks in the sand: Impossibility of strong watermarking for generative models. *arXiv preprint arXiv:2311.04378* (2023).
[134] Verena Zimmermann and Nina Gerber. 2017. "If It Wasn't Secure, They Would Not Use It in the Movies" – Security Perceptions and User Acceptance of Authentication Technologies: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings. In *Human Aspects of Information Security, Privacy and Trust*, Theo Tryfonas (Ed.). Lecture Notes in Computer Science, Vol. 10292. Springer International Publishing, Cham, 265–283.

A Appendix: Tables & Figures

A.1 PHC Introduction Video

Transcripts: *A personhood credential is a concept used to verify that an individual is a real, unique human being A widespread verification method is CAPTCHA that asks users to complete tasks that are easy for humans but difficult for bots. However, with advances in AI, these tasks are now easily solved by bots. An emerging PHC is World app which uses device to scan users' iris, creating a unique digital identity. With this verified identity, users can access various online services. A well-designed PHC protects the privacy of users instead of sharing identifiable information. The credential simply confirms the user is a unique individual. Let's take a look at how the PHC architecture works. There are three main roles, the PHC issuer, the user and the service provider. First, the user requests a PHC from a trusted issuer which can be government or a private organization, etc. You can request a credential with verification evidence. Once verified, the issuer provides you with a PHC. You can then use this credential to authorize services, ensuring your identity is validated without exposing*

Table 2. Participant demographics and background.

ID	*Gender*	*Age*	*Country*	*Education*	*Tech*
P1	Male	25-34	US	Master's degree	Yes
P2	Female	25-34	US	Master's degree	Yes
P3	Female	25-34	UK	Master's degree	Yes
P4	Female	35-44	UK	Some college, but no degree	Yes
P5	Male	25-34	US	Doctoral degree	Yes
P6	Male	35-44	US	Less than a high school diploma	No
P7	Male	25-34	US	Doctoral degree	Yes
P8	Male	45-54	US	Bachelor's degree	Yes
P9	Female	25-34	New Zealand	Master's degree	No
P10	Male	25-34	US	Master's degree	No
P11	Female	25-34	UK	Bachelor's degree	No
P12	Male	18-24	UK	Master's degree	Yes
P13	Male	35-44	UK	Bachelor's degree	Yes
P14	Male	25-34	Sweden	High school graduate	No
P15	Female	25-34	Spain	Master's degree	Yes
P16	Female	25-34	Germany	Master's degree	Yes
P17	Female	25-34	Spain	Doctoral degree	No
P18	Female	35-44	US	Bachelor's degree	No
P19	Female	25-34	Germany	Master's degree	Yes
P20	Male	25-34	Hungary	Master's degree	Yes
P21	Male	35-44	US	Bachelor's degree	Yes
P22	Female	18-24	France	Master's degree	Yes
P23	Male	45-54	US	Master's degree	No
P24	Male	25-34	Netherlands	Master's degree	Yes
P25	Male	55-64	US	Master's degree	No
P26	Male	25-34	US	High school graduate	Yes
P27	Female	55-64	US	Master's degree	No

Tech: Technology background.

your personal information. The service provider verifies your PHC, confirming you are a human. This is an overview of personhood credentials. You can prove your personhood without sharing personal details through various online services. This credential ensures digital services, requiring human interaction can distinguish genuine users from automated or fake accounts. For instance, only humans participate in online polls, resulting in less bot activity and fewer fake accounts on social media.

B Appendix: Study Protocol

B.1 Knowledge Questions

(1) What could happen if online identities are poorly verified?
- ○ Digital platforms could become more secure.
- ○ **Fake accounts, bots, and fraud could increase significantly.**
- ○ Users could feel more confident and trusting in online environments.
- ○ Privacy could be better protected across online services.

(2) What are Personhood Credentials (PHCs)?
- ○ **Digital credentials that confirm a person's identity**
- ○ A method for storing personal data online for easy access
- ○ Credentials issued by social media platforms to verify account authenticity
- ○ A tool used by online services to track user activity and preferences

(3) What is the primary goal of PHC?
   - To reduce the number of online accounts.
   - To track a user's online activity across platforms.
   - **To verify a person's identity without exposing personal information.**
   - To simplify the process of logging into multiple services.

(4) To whom do you provide minimal personal information during the PHC process?
   - Online service providers (e.g., social media)
   - Entities handling data storage for online accounts
   - Third-party platforms
   - **PHC issuers (e.g., governments or trusted organizations)**

(5) Which of the following options are considered as credentials of PHCs? Select all that apply.
   - **Government credentials (e.g., passport, driver's license)**
   - **Biometric indicators (e.g., face, fingerprint, iris)**
   - Email address
   - Phone number

B.2 Post-Survey

(1) **Credential Preference**: Which types of credential would you prefer to use as personhood verification for each scenario? Select all that apply. *(This question is displayed in a multiple choice grid, prompting responses for each scenario: Finance Service, Healthcare Service, Social Media, LLM Application, Government Service, and Employment Background Check.)*
   - Government issued ID (e.g., SSN))
   - Passport
   - Driver's license
   - Face scan
   - Fingerprint scan
   - Iris scan
   - Phone number

(2) **Issuer Preference**: Which type of issuer would you prefer to issue and manage your PHC for each scenario? Select all that apply. *(This question is displayed in a multiple choice grid, prompting responses for each scenario: Finance Service, Healthcare Service, Social Media, LLM Application, Government Service, and Employment Background Check.)*
   - Government
   - NPO (nonprofit organization)
   - Private Companies
   - Financial Institution (e.g., banks)
   - Educational Institution (e.g., universities)

(3) Do you have any other issuer in mind that you would prefer to issue PHC? *(This question is open-ended.)*

(4) **Architecture Preference**: Which type of system would you prefer to issue and manage your PHC for each service provider? *(This question is displayed in a multiple choice grid, prompting responses for each scenario: Finance Service, Healthcare Service, Social Media, LLM Application, Government Service, and Employment Background Check.)*
   - Centralized
   - Decentralized

C Appendix: Interview Protocol

C.1 Section 1: Current practices regarding digital identity verification

(1) Can you tell me about any online platforms or services you have used before or currently using that ask you to verify your identity, like uploading your ID or confirming your identity in other ways?

(2) You mentioned using online platform X. Can you tell me what method you used to verify your identity for platform X? [repeat question 2 for other services mentioned Y, Z, ...]

(3) Can you share your experience with that verification method? Was it easy to use, or did you run into any issues?

(4) Did you encounter any challenges when using this method?

(5) Have you ever used services where you had to verify yourself through face, fingerprints, or iris scans, or other biometrics?

(6) Can you tell me more about your experience with those methods? What worked well? Were there any concerns you had?

C.2 Section 2: Users' perception of PHC (RQ1)

C.2.1 Pre-Understanding of Personhood Credentials.

(1) Do you know the term 'Personhood Credentials'? If not, can you explain what you think it means by just hearing the term?
(2) Have you used any 'Personhood Credentials' before? If you say yes, then ask, What are those?
(3) Do you know how 'Personhood Credentials' work within the services you use?
(4) Do you know how the service providers handle the credentials you provide as 'Personhood Credentials' so you can access the service?

(Participants are asked to fill the online survey to assess their pre-understanding of personhood credentials.)

C.2.2 Educational Session. (Participants are shown a 2-minute educational video about the concept of personhood credentials. The video can be accessed in the following link: https://anonymous.4open.science/r/PHC-user-study-14BB/)

C.2.3 Post-Understanding of Personhood Credentials.

(1) After reviewing the educational materials, how would you explain your understanding of personhood credentials?
(2) Can you think of any benefit of a personhood credential based on your understanding? Why?
(3) Can you think of any risk of a personhood credential based on your understanding? Why?

(Participants are asked to fill the online survey to assess their post-understanding of personhood credentials.)

C.3 Section 3: Scenario Session (RQ1)

Now, we will go over some specific application scenarios of personhood credentials to understand your perception and how we can better design the personhood credential for different services.

Scenario 1: Financial Service Imagine you are opening a new bank account with a bank that offers a fully digital onboarding experience. The bank requires you to verify your identity using personhood credentials, such as facial recognition for a liveliness test, and then uploading a government-issued ID (like your passport or driver's license). Once verified, you can open a bank account access your bank account, and manage your funds.

(1) How did you feel about using personhood credentials to verify your identity when opening your bank account?
(2) **Benefits**: What potential benefits do you see in using PHC in this online banking context?
(3) **Security**: Do you think using personhood credentials improves the security of your bank account?
(4) **Privacy**: Did this method of identity verification make you feel more confident about your privacy?
(5) **About Data**: Were you comfortable providing your government-issued ID and using facial recognition?
(6) **Concerns**: What concerns do you have in providing your government-issued ID and using facial recognition, is being stored and used by the online bank?

Scenario 2: Healthcare Services Imagine you are using an online healthcare platform to schedule appointments and receive virtual consultations with doctors. To provide access to the platform, the healthcare service requires you to verify your identity using personhood credentials, such as a biometric verification using a fingerprint for a liveliness test, and then upload a government-issued ID (like your health insurance card or passport). Once your identity is verified, you can access your medical records, schedule appointments, and have virtual consultations with healthcare providers.

(1) How did you feel about using personhood credentials to verify your identity when using an online healthcare platform?
(2) **Benefits**: What potential benefits do you see in using PHC in this healthcare context?
(3) **Security**: Do you think using personhood credentials improves the security of the healthcare platform?
(4) **Privacy**: Did this method of identity verification make you feel more confident about your privacy?
(5) **About Data**: Were you comfortable providing your government-issued ID and using fingerprint?
(6) **Concerns**: What concerns do you have in providing your ID and fingerprint information, is being stored and used by the healthcare platform?

Scenario 3: Social Media Imagine you are creating a new premium social media account. You are required to verify your identity with personhood credentials, such as a video call or selfie for a liveliness test (or proof you are a real, unique user), and then upload your government-issued ID (SSN, national ID card). Once your identity is verified, you can access social media.

(1) How did you feel about using personhood credentials to verify your identity when creating a new premium social media account?
(2) **Benefits**: What potential benefits do you see in using PHC in this social media context?
(3) **Security**: Do you think using personhood credentials improves the security of the social media platform?
(4) **Privacy**: Did this method of identity verification make you feel more confident about your privacy?
(5) **About Data**: Were you comfortable providing your government-issued ID and a video selfie?
(6) **Concerns**: What concerns do you have in providing your ID and using a video selfie, is being stored and used by the social media platform?

Scenario 4: LLM Application Imagine you are signing up for an AI language model application like ChatGPT to assist you with tasks and information. Identity verification is also crucial in LLM-based applications because the interaction between multiple users and its model can significantly impact the reliability and safety of the platform. For example, malicious users could submit harmful prompts or requests that might lead to biased or damaging outputs from the model. With identity verification, the platform can confirm that each user is legitimate, thereby reducing these risks. Thus, imagine to sign up for the application, the LLM service requires you to verify your identity using personhood credentials, such as a biometric verification using an iris recognition scan for a liveliness test.

(1) How did you feel about using personhood credentials to verify your identity when signing up for the AI language model application?
(2) **Benefits**: What potential benefits do you see in using PHC in this AI application context?

(3) **Security**: Do you think using personhood credentials improves the security of the AI language model application?
(4) **Privacy**: Did this method of identity verification make you feel more confident about your privacy?
(5) **About Data**: Were you comfortable providing your iris scan?
(6) **Concerns**: What concerns do you have in using iris scan, is being stored and used by the LLM application providers?

Scenario 5: Government Service Imagine You are applying for government assistance or social benefits (e.g., healthcare, unemployment benefits) to government portal (e.g., USAGov, Your Europe). To ensure that only eligible citizens access these services, the platform asks you to verify your identity using personhood credentials by using an iris scan for a liveliness test and then uploading your government-issued ID to confirm your identity for government benefit.

(1) How did you feel about using personhood credentials to verify your identity when using a government portal?
(2) **Benefits**: What potential benefits do you see in using PHC in this government portal context?
(3) **Security**: Do you think using personhood credentials improves the security of the government portal?
(4) **Privacy**: Did this method of identity verification make you feel more confident about your privacy?
(5) **About Data**: Were you comfortable providing your government-issued ID and iris information?
(6) **Concerns**: What concerns do you have in providing your ID and using iris scan, is being stored and used by the government portal?

Scenario 6: Employment Background Check Imagine you have received a job offer from a company, and as part of the final hiring process, they require an employment background check. To confirm your eligibility and verify your work history, the background check service asks you to submit personhood credentials using fingerprint verification and uploading your government-issued ID to verify your identity.

(1) How did you feel about using personhood credentials to verify your identity for an employment background check?
(2) **Benefits**: What potential benefits do you see in using PHC in this background check context?
(3) **Security**: Do you think using personhood credentials improves the security of the employment background check?
(4) **Privacy**: Did this method of identity verification make you feel more confident about your privacy?
(5) **About Data**: Were you comfortable providing your government-issued ID and fingerprint information?
(6) **Privacy Concerns**: What concerns do you have in providing your ID and using fingerptint, is being stored and used by the background check service?

C.4 Section 4: Users' preference of PHC (RQ2)

We talked about several scenarios where different types of potential credentials to issue you PHC that could verify yourself as a unique human. In this section, we would like to discuss on different types of credentials you might prefer in issuing personhood credentials for you and how you might want to manage those based on your privacy and security need.

If you were to use PHC for identity verification,

(1) What types of credentials would you prefer to use as personhood verification?
(2) Which organizations or stakeholders would you prefer to issue and manage your PHC?

C.5 Section 5: Design Session(RQ3)

In the former session, we discussed the concerns/potential risks in PHC. I wrote down these potential problems in the top of whiteboard. We would like to brainstorm the idea how we can solve these problems by sketching your ideas. For sketching, you can use this digital whiteboard, or use pen and paper in your desk if you prefer. *(We send the link to the zoom whiteboard where pre-arranged components like the PHC issuer and database are placed on the left, while potential concerns or risks suggested by participants during interviews are noted as topics in the top right.)*

(1) In your opinion, how can we improve the design for PHC to address issues/concerns we discussed? Could you sketch a solution?
(2) Could you explain your drawing?