

A Paradigm Shift in Digital Identity: An Augmented-ID Framework for Compliant and Dignified Age Verification Under Arizona HB2112

Deconstructing the Legal Mandate: The Constraints and Opportunities of Arizona HB2112

The genesis of the modern digital age-gating dilemma, as articulated by users seeking more dignified and technologically advanced solutions, lies squarely within the legislative actions of states like Arizona. The passage and implementation of House Bill 2112 (HB2112) created a complex legal landscape where stringent child protection goals clash with profound privacy concerns and usability challenges. Understanding the precise contours of this law is not merely an academic exercise; it is the foundational prerequisite for designing any viable alternative system. HB2112, signed into law by Governor Katie Hobbs on May 13, 2025, and taking effect on September 26, 2025, represents a significant evolution in state-level regulation of online content ² ⁶ ⁵⁵. Its primary objective is to establish a robust barrier between minors and sexually explicit material harmful to them, drawing a functional analogy to physical-world age-restricted purchases like liquor or tobacco ⁷⁷. However, the path to achieving this goal is defined by a series of meticulously crafted constraints that, while seemingly restrictive, also present a clear opportunity for innovation in privacy-preserving technologies. The law's scope is carefully delineated to apply only to commercial websites where more than one-third of the content consists of "sexual material that is harmful to minors" ¹ ³. This threshold ensures that the burden falls on platforms specifically dedicated to adult content, rather than being applied broadly across the entire internet. The statute explicitly exempts key infrastructure entities, including Internet Service Providers (ISPs), web browsers, search engines, and cloud service providers that do not create the content themselves, thereby placing the full responsibility for compliance squarely on the shoulders of the content-hosting publisher ⁵⁷.

The definition of "sexual material that is harmful to minors" is central to the law's application and reflects a judicial standard adapted for the digital age. It covers material that, when viewed by minors as a whole, appeals to a prurient interest, depicts sexual acts or nudity in a patently offensive way according to contemporary community standards, and lacks serious literary, artistic, political, or scientific value for minors ^{6 57}. This multi-factor test mirrors obscenity jurisprudence and requires a nuanced interpretation by each website operator regarding its own content composition. For instance, the law specifies that material depicting pubic hair, genitals, anus, or female nipples, or simulating sexual acts, is included in this category ⁵⁷. This precise definition underscores the law's intent to regulate the distribution of pornography, but its broad phrasing has raised First Amendment concerns among critics who argue it could inadvertently restrict access to constitutionally protected content, such as sex education resources or LGBTQ+ health information ³². This tension between protecting minors and preserving free expression remains a critical legal challenge that any compliant system must navigate. The law's effective date of September 26, 2025, was established based on the conclusion of the 2025 Arizona legislative session on May 23, 2025, creating a compliance window for affected platforms to adapt their verification mechanisms ^{8 29}.

The most significant and legally transformative aspect of HB2112 is its explicit mandate for "reasonable age verification methods." The statute provides two distinct and mutually exclusive pathways for commercial sites to comply. The first pathway allows for verification through "digital identification," which is broadly defined as "information that is stored on a digital network that may be accessed by a commercial entity and that serves as proof of the identity of an individual" ^{28 33}. Crucially, this definition includes a self-imposed constraint: the digital identification itself must be structured in a way that "does NOT CAUSE OR ALLOW THE INDIVIDUAL'S IDENTIFYING INFORMATION TO BE TRANSMITTED TO ANY FEDERAL, STATE OR LOCAL GOVERNMENT ENTITY" ²⁸. This clause directly addresses privacy advocates' concerns about government surveillance and aligns with broader principles of data minimization. The second, and perhaps more flexible, pathway permits the use of a "commercial age-verification system that uses either government-issued identification or a commercially reasonable method that relies on public or private transactional data" to verify age ^{27 31}. Transactional data is statutorily defined as "a sequence of information that documents an exchange, agreement, or transfer" and explicitly includes records from mortgage, education, and employment entities ²⁸. This provision opens the door for sophisticated third-party services that can analyze financial histories or other public records to

determine a user's age without requiring them to submit a government-issued ID. This dual-pathway structure is the primary legal justification for the viability of a decentralized, DID-based system, as a digitally issued credential can be argued to function as a form of compliant "digital identification."

However, the single most important constraint imposed by HB2112—and the one that makes a privacy-first approach not just desirable but legally imperative—is its absolute prohibition on the retention of identifying information. Multiple sources confirm that neither the commercial content provider nor any third-party age-verification entity is permitted to retain any identifying information of an individual after the verification check is complete ^{1 4 27}. The law further stipulates that there shall be no direct or indirect transmission of such identifying information to any federal, state, or local government entity ^{27 56}. This mandate effectively invalidates business models that rely on mass collection and storage of sensitive personal data, such as selfies, raw driver's license scans, or biometric templates. It forces a fundamental architectural shift toward systems designed with data minimization at their core. Any system deployed under HB2112 must be engineered so that high-risk personal identifiers are never transmitted to or stored by the verifying party. This legal requirement creates a powerful incentive for technologies like Zero-Knowledge Proofs (ZKPs), which allow a user to cryptographically prove they meet a specific criterion—such as being over 18—without revealing any underlying personal data, such as their exact date of birth ^{12 46}. The EU's eIDAS 2.0 regulation, which entered into force in May 2024, has already recognized ZKPs as a legitimate privacy-enhancing technology capable of validating statements without revealing the underlying data, establishing a strong international precedent for their legal acceptability ³⁷.

The stakes for non-compliance are exceptionally high, serving as a potent motivator for platform operators to adopt robust and reliable verification systems. The penalties for failure are tiered and substantial. A site that fails to implement any form of age verification faces a civil penalty of \$10,000 per day of noncompliance ^{2 8}. If a minor gains access to the material due to a verification failure, the penalty escalates dramatically to up to \$250,000 ^{7 30}. Furthermore, if a third-party verifier improperly retains identifying information, even if no minor accesses the content, the penalty is \$10,000 per incident ². Enforcement of these provisions is primarily driven by a private right of action, allowing parents or guardians of minors who gain unauthorized access to file lawsuits against the non-compliant entities ^{7 27}. This shift away from direct enforcement by the Attorney General places the burden of litigation squarely on those most directly harmed by a failure in the system,

creating a powerful market incentive for compliance. These severe financial consequences underscore the critical importance of selecting a verification method that is both legally defensible and technically sound, making the exploration of novel, privacy-preserving architectures like Augmented-ID not just an option, but a strategic necessity for long-term viability.

HB2112 Key Provisions	Statutory Basis
Applicable Websites	Commercial sites where >1/3 of content is "sexual material harmful to minors" 1 3
Scope of Harmful Material	Pornography appealing to a prurient interest, patently offensive to minors, lacking serious value 6 57
Exempt Entities	ISPs, search engines, web browsers, cloud providers (if not content creators) 57
Effective Date	September 26, 2025 6 55
Permissible Methods	(a) Digital Identification; (b) Commercially Reasonable Transactional Data System 27 31
Data Retention Rule	Content providers and third-party verifiers may NOT retain any identifying information 1 4
Government Transmission Ban	No direct or indirect transmission of identifying information to any government entity 27 56
Penalties for Failure	\$10,000 per day for lack of verification; \$10,000 per incident of improper retention; up to \$250,000 if a minor gains access 2 8
Enforcement Mechanism	Private right of action by parents/guardians of affected minors 7 27

This detailed legal framework, while focused on the problem of underage access to explicit material, contains the seeds of its own technological solution. The law's emphasis on "reasonable" and "digital" methods, combined with its uncompromising privacy mandate, creates a fertile ground for the development and adoption of decentralized identity systems. By forcing a move away from intrusive, centralized data collection, HB2112 implicitly encourages the very kind of privacy-by-design architecture that technologies like W3C Verifiable Credentials and Zero-Knowledge Proofs are built to support. This legal environment, therefore, is not an obstacle to be overcome, but rather a guiding principle that shapes the design of a new generation of digital identity systems, promising a future where compliance and user dignity are not mutually exclusive goals.

The Technological Foundation: Architecting a Privacy-Preserving Augmented-ID System

The technological response to the legal and social pressures created by laws like Arizona HB2112 must transcend simple workarounds and instead offer a fundamental redesign of the age-gating process. The proposed Augmented-ID framework represents such a paradigm shift, leveraging a suite of mature, open, and interoperable technologies to create a system that is simultaneously compliant with statutory requirements, highly secure, and deeply respectful of user privacy. At its core, this architecture is built upon three interconnected pillars: Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Zero-Knowledge Proofs (ZKPs). Together, these components enable a user-centric model of identity where individuals control their own attributes and can selectively disclose them with cryptographic proof, eliminating the need for repeated, invasive verification processes. This approach directly addresses the shortcomings of current systems, which often rely on fragile CAPTCHAs or intrusive selfie/ID uploads that generate significant friction and raise serious privacy concerns .

The foundation of the Augmented-ID system is the use of Decentralized Identifiers (DIDs). DIDs are a new type of globally unique identifier that enables verifiable, decentralized digital identity [66](#) . Unlike traditional identifiers managed by a central authority, DIDs give users sovereign control over their own identities. A DID can be resolved to a DID document, which contains crucial information for interacting with the identity, such as public keys for verification and service endpoints [79](#) . For the purpose of age verification, a user's wallet would generate a pairwise pseudonymous DID for each specific site or jurisdiction. This means that a different, unlinkable DID is used for every interaction, preventing cross-site tracking and ensuring that a user's activities on one platform cannot be correlated with another [20](#) . This practice aligns perfectly with NIST SP 800-63-B's guidance on disassociability, a key principle for minimizing privacy risk . The system would support multiple DID methods, such as `did:key` for lightweight, self-contained DIDs, `did:web` for DIDs anchored to a domain controlled by the user, and `did:ethr` for DIDs anchored to the Ethereum blockchain, providing flexibility and resilience . This decentralized approach shifts the locus of trust from a monolithic central server to a distributed ledger of verifiable claims, making the system far more resistant to single points of failure or compromise.

Building upon the foundation of DIDs are Verifiable Credentials (VCs), which serve as the digital equivalent of passports, driver's licenses, or university diplomas [34](#) . A

VC is a set of claims made by an issuer about a subject (the holder), which is then cryptographically signed by the issuer to ensure its authenticity and integrity. In the context of Augmented-ID, a trusted third-party issuer—a DMV, a bank, or a certified age-verification service—would issue a credential asserting a specific attribute, such as "age \geq 18 in Arizona" ⁶⁹. This credential would be securely stored in the user's digital wallet. When accessing an age-restricted site, the user's wallet presents this VC to the verifier (the website). The power of VCs lies in their ability to support selective disclosure. Instead of transmitting the entire credential, which might contain a name, address, and date of birth, the holder can create a "verifiable presentation" containing only the specific claim being requested ³⁴. This allows the website to receive a cryptographically signed assertion that the user is over 18 in Arizona, without ever seeing the user's real name, address, or other personally identifiable information (PII). This mechanism is a direct implementation of the data minimization principle mandated by HB2112 and is supported by standards like the W3C Verifiable Credentials Data Model v2.0 and ISO/IEC 18013-5 for mobile driver's licenses ^{9 34}.

For the highest level of privacy, the Augmented-ID system incorporates Zero-Knowledge Proofs (ZKPs). A ZKP is a cryptographic protocol that allows one party (the prover) to prove to another party (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself ³⁶. In the context of age verification, a user can prove they are over 18 without revealing their exact date of birth, or even their exact age ^{12 46}. This is achieved through specialized cryptographic circuits that take a secret input (e.g., a hashed date of birth) and produce a proof that it satisfies a certain condition (e.g., the corresponding age is greater than or equal to 18). The website's backend can then verify this proof without ever learning the underlying secret. This technology offers a mathematically provable guarantee of privacy and is gaining regulatory acceptance; the EU's eIDAS 2.0 regulation explicitly recognizes ZKPs as a valid privacy-enhancing technology ³⁷. The system could utilize a ZKP circuit, such as a zkSNARK, to generate a range proof that demonstrates the user's date of birth is within a valid range for being over 18, with the final output being a short, verifiable token that contains no PII ⁶⁸. This cryptographic layer adds a formidable defense against privacy breaches, as even if the communication channel or the verifier's system were compromised, no sensitive data would have been exchanged.

The operational flow of the Augmented-ID system is designed for simplicity and security. The initial onboarding event is a one-time, high-assurance identity proofing process. During this event, the user authenticates their identity to a trusted

issuer using one of the methods permitted by HB2112, such as presenting a government-issued REAL ID-compliant mobile driver's license or undergoing a transactional data check ^{9 27} . Once verified, the issuer issues a verifiable credential to the user's wallet and immediately deletes all raw personal data, including any images of the ID or selfies ⁵² . Subsequent interactions become seamless. When a user navigates to an age-restricted website, a small browser extension or integrated API shim detects the need for verification . It then communicates with the local Augmented-ID wallet, requesting a proof of age. The wallet generates a signed, short-lived token using either a selectively disclosed VC or a ZKP, which is bound to the specific site's origin to prevent replay attacks . This token is sent to the website, which validates the signature and, upon success, grants access. This entire process happens silently in the background, replacing the cumbersome and humiliating UI flows of today with a single, one-click confirmation . The architecture is further hardened by using hardware-backed security, such as a Trusted Platform Module (TPM) for key sealing, and implementing robust threat modeling to mitigate phishing, man-in-the-middle attacks, and compelled de-anonymization .

The table below outlines the mapping between the core components of the Augmented-ID system and the legal requirements of HB2112, demonstrating how the proposed architecture achieves compliance through privacy-by-design.

Augmented-ID Component	Core Functionality	Mapping to HB2112 Compliance
Decentralized Identifier (DID)	Provides a self-sovereign, cryptographically verifiable, and pairwise pseudonymous identifier for each user-site interaction.	Supports the "digital identification" pathway. Prevents cross-site tracking, aligning with data minimization principles. ⁶⁶
Verifiable Credential (VC)	A cryptographically signed assertion of an attribute (e.g., "Age ≥ 18 in AZ") issued by a trusted party.	Serves as a compliant "digital identification." Enables selective disclosure, proving the attribute without exposing underlying PII. ^{34 69}
Zero-Knowledge Proof (ZKP)	Cryptographic proof that a statement is true (e.g., "DOB ≤ today - 18 years") without revealing the underlying data.	Aligns with the "commercially reasonable" standard. Offers maximum privacy by proving the boolean outcome without disclosing the attribute value. ^{12 37}
On-Device Wallet	A secure, local application that stores credentials, manages keys, and generates cryptographic proofs.	Ensures that all sensitive data (raw IDs, biometrics, PII) remains encrypted on the user's device and is never transmitted to a third party. ⁷⁸
Short-Lived Token	A time-bound, site-specific cryptographic token generated for each verification request.	Mitigates replay attacks and ensures that even if a token is intercepted, it is useless outside its short window of validity.
No Retention Architecture	System design that prohibits the storage of any identifying information by the verifier or the gateway node.	Directly enforces HB2112's explicit prohibition on retaining identifying information post-verification. Logs contain only anonymized hashes. ¹

By architecting the system around these foundational principles, Augmented-ID transforms the age-gating process from a point-in-time, high-friction event into a continuous, low-friction capability. It satisfies the letter of the law by providing a "reasonable method" of verification, while exceeding its spirit by embedding robust privacy protections and user autonomy into the very fabric of the technology. This approach not only solves the immediate problems of intrusive UX and data privacy but also establishes a scalable and extensible framework for a wide range of identity-based interactions, from accessing restricted digital content to navigating smart-city environments.

Redefining User Experience: From Exclusionary Gating to Inclusive Capability Assertion

A critical and often overlooked dimension of the age-gating problem is its profound impact on user experience (UX), particularly for individuals who fall outside the narrow, un-augmented human assumption that underpins current systems. The ubiquitous "prove you are human" prompts, CAPTCHAs, and selfie-upload requests are not merely inconvenient; they are actively hostile, demeaning, and exclusionary. They implicitly communicate a message of suspicion and distrust, framing the interaction as a test of humanity rather than a straightforward assertion of a legal right. For an AI-augmented individual, these prompts can feel profoundly discriminatory, as they seem to target their specific mode of existence. The Augmented-ID framework proposes a radical rethinking of this interaction, shifting the paradigm from a burdensome, exclusionary gate to an empowering, inclusive assertion of capability. This transformation is achieved through three core principles: the use of neutral, respectful language; the elimination of repetitive, frustrating workflows; and the intentional design for inclusivity from the outset.

The most immediate improvement offered by Augmented-ID is the replacement of derisive and exclusionary language with neutral, capability-focused terminology. Current age-gating interfaces often employ phrases like "Prove you're not a robot," "Are you human?", or "Please take a selfie to prove your age". Such language is problematic for several reasons. Firstly, it frames the user as a potential threat, reinforcing a hostile posture that erodes trust. Secondly, it is inherently biased, assuming a narrow definition of what constitutes a "human" and implicitly rejecting anyone who deviates from that norm, whether due to disability, neurodivergence, or augmentation. Thirdly, it is cognitively taxing, requiring users to engage in

abstract reasoning puzzles (in the case of CAPTCHAs) or perform awkward physical tasks (in the case of selfies). The Augmented-ID system replaces this hostile dialogue with a simple, respectful request. The interface would prompt the user with clear, concise language such as "Confirm your legal-access proof" or "Share your 18+ credential for this site" . This reframes the action from a defensive test of humanity to a proactive assertion of a pre-established right. Instead of asking "Are you human?", the system asks for a piece of evidence that proves a specific, legally relevant attribute. This subtle but powerful shift in language fosters a sense of respect and dignity, transforming a moment of friction into a smooth, affirmative action.

The second major UX improvement is the creation of a truly reusable and persistent identity state. Currently, age verification is treated as a recurring event that must be performed anew for almost every visit to an age-restricted site. This leads to a cycle of repetition and frustration, where users must repeatedly upload IDs, take selfies, and solve puzzles. The Augmented-ID system breaks this cycle by treating the initial identity proofing event as a one-time, high-assurance onboarding process. Once a user has successfully proven their age to a trusted issuer, they receive a permanent, self-sovereign credential in their wallet . Every subsequent access to an age-restricted site becomes a silent or one-click confirmation. The browser extension or native app simply retrieves the appropriate credential from the local wallet, generates a short-lived cryptographic proof, and submits it to the site. This "one-click consent" model dramatically reduces cognitive load and eliminates the need for any manual intervention after the initial setup . For a user, this means that once their identity is verified, they should never have to see another age-gating prompt again. This not only improves efficiency but also significantly enhances the overall user journey, making the digital world more accessible and less stressful for everyone.

Perhaps the most impactful aspect of the Augmented-ID UX redesign is its commitment to inclusivity, intentionally designed to accommodate a diverse range of users, including those with disabilities, neurodiverse individuals, and older adults. The current proliferation of CAPTCHAs and complex, visually cluttered forms creates significant barriers for many users. For example, WCAG 2.2's new "Accessible Authentication (Enhanced)" success criteria explicitly prohibit the use of cognitive function tests, such as puzzles or password recall, unless specific exceptions apply, a rule that directly supports the low-friction nature of the Augmented-ID model ⁹⁰ . Similarly, research shows that reducing cognitive load in kiosk interfaces can increase user performance by up to 40% ⁹³ , a principle that is central to the Augmented-ID design. The system's reliance on a simple, one-click

action is inherently more accessible than multi-step forms or visual puzzles that can be difficult for users with visual impairments, motor disabilities, or cognitive differences. Furthermore, the design philosophy emphasizes clarity and predictability. Bottom-aligned navigation with persistent 'back' and 'confirm' buttons, a pattern shown to improve intuitiveness for users with severe reading or motor impairments, would be a natural fit for the Augmented-ID flow [24](#) . Replacing manual scrolling with large, explicit scroll buttons can also significantly improve task completion for users with intellectual disabilities and older adults [24](#) . By focusing on simplicity, consistency, and low cognitive demand, the Augmented-ID system moves beyond mere accessibility compliance to create a genuinely inclusive experience.

The connection between respectful UX and the prevention of discrimination is a critical insight. Research has shown that microaggressions, bullying, and harassment are pervasive experiences for people with disabilities in various settings, including the workplace [70](#) [73](#) . While the age-gating context is different, the principle holds: language and interaction patterns that frame a user as a suspect or an anomaly contribute to a hostile environment. Using neutral, non-stigmatizing language like "Confirm legal-access proof" instead of "Prove you are human" is a tangible step toward creating a more equitable digital space . This is particularly relevant for marginalized groups, as studies reveal that a significant percentage of individuals with disabilities have experienced rejection of their accommodation requests and have missed out on opportunities due to inaccessible systems [71](#) [73](#) . An inclusive age-gating system like Augmented-ID helps to mitigate these harms by ensuring that access is granted based on a verifiable attribute rather than a subjective judgment or a frustrating, exclusionary puzzle. The U.S. Access Board's ongoing work exploring the risks and benefits of AI for people with disabilities further highlights the need for thoughtful, inclusive design in authentication systems [74](#) [75](#) .

The table below contrasts the current age-gating UX with the proposed Augmented-ID UX, highlighting the transformative improvements in language, workflow, and inclusivity.

Feature Area	Current Age-Gating UX	Proposed Augmented-ID UX	Rationale and Benefits
Interaction Language	Hostile, exclusionary prompts ("Prove you're not a robot," "Take a selfie").	Neutral, capability-focused prompts ("Confirm your legal-access proof," "Share your 18+ credential").	Reframes the interaction from a test of humanity to an assertion of right, fostering dignity and respect.
Workflow Friction	High friction, requiring repeated actions for every session (ID uploads, selfies, CAPTCHAs).	Low friction, typically a single one-click confirmation after initial onboarding.	Eliminates repetitive, frustrating steps, improving efficiency and user satisfaction. 90
Cognitive Load	High, often involving abstract reasoning (puzzles), memorization (passwords), or complex instructions.	Very low, consisting of a simple, predictable action (clicking a button).	Reduces cognitive fatigue, making the system usable for older adults, neurodiverse individuals, and those with cognitive impairments. 24 93
Accessibility	Often inaccessible, relying on visual elements and complex inputs that exclude users with disabilities.	Designed for accessibility by default, supporting screen readers, motor alternatives, and low-cognitive-load flows.	Aligns with WCAG 2.2 guidelines and best practices for inclusive design, ensuring equal access for all users. 50 87
Consistency	Highly inconsistent across platforms, leading to user confusion and mistrust.	Consistent and predictable, as the same wallet and credential format are used everywhere.	Creates a seamless user experience and builds trust in the underlying identity system. 80
Trust and Privacy	Erodes trust by demanding sensitive data (selfies, ID images) and storing it on potentially insecure servers.	Builds trust by keeping all sensitive data on-device and using cryptography to prove attributes without revealing them.	Aligns with user expectations for privacy and data security, enhancing overall confidence in the system. 12 52

Ultimately, the Augmented-ID framework demonstrates that a better user experience is not a luxury but a core component of a successful and ethical identity system. By consciously designing for neutrality, reusability, and inclusivity, it transforms a common source of user frustration into a model of efficient, dignified, and secure digital interaction. This approach not only resolves the immediate pain points for users but also sets a new standard for how digital services should interact with their users, grounded in respect, autonomy, and fairness.

Advanced Identity Frontiers: Secure Integration of BCI and Neuromorphic Hardware

The Augmented-ID framework extends beyond addressing the limitations of conventional digital identity to embrace the emerging frontier of human-machine integration. The user's specific mention of "AI-integrations with my biological-system/body" introduces a complex and ethically charged dimension to identity verification: the use of Brain-Computer Interface (BCI) and neuromorphic hardware

signals. While this technology holds immense promise for enabling new capabilities, its direct application as a remote credential poses significant security and privacy risks. The proposed solution is not to treat neural data as a universal identifier but to integrate it safely and respectfully within a broader "devices-as-artifacts" policy. This approach leverages BCI/EEG data as a high-strength, on-device unlocking mechanism for the local identity wallet, ensuring that sensitive neural signals remain confined to the user's device and are never transmitted to external verifiers ⁵ ²⁶. This model prioritizes the sanctity of the user's neural data while still accommodating their unique needs for secure authentication.

The primary challenge in handling neural data is its inherent sensitivity. Research in neuroscience and cybersecurity has demonstrated that brainwave patterns and other neural signals can reveal highly intimate and private information, extending far beyond simple identity verification ⁵⁴. Studies have shown that EEG signals can be used to infer cognitive traits, emotional states, and even sensitive personal information like PINs or passwords ⁵⁴. Transmitting this raw or processed neural data over a network creates a massive attack surface, opening the door to interception, misuse, and deep psychological profiling. Therefore, treating BCI/EEG-derived features as a remote credential that is sent to a website or service is a fundamentally flawed and dangerous approach. It violates the core tenets of data minimization and privacy-by-design that are essential for compliance with regulations like HB2112 and GDPR. Emerging neuro-rights frameworks are beginning to recognize this, advocating for the treatment of neural data as a top-tier protected category of information, akin to genetic data ⁷⁴ ⁷⁵.

To address this challenge, the Augmented-ID system proposes a pragmatic and secure implementation model grounded in the "devices-as-artifacts" policy. This policy treats any hardware directly coupled to a person's body or integrated into their biological system as part of the person themselves, rather than as a general-purpose computer ²⁶. This philosophical stance has profound technical implications. It dictates that the processing of sensitive biometric and biosignal data must occur entirely within a secure, on-device enclave, such as a Trusted Execution Environment (TEE) or a hardware root of trust like a TPM chip. In this model, the user's BCI headset would not transmit a credential to a website. Instead, it would capture the user's neural signal, which is then processed locally to unlock the device's secure element. This is analogous to how modern smartphones use fingerprint sensors or facial recognition to unlock the phone's encryption keys. The BCI signal acts as a very strong, biometrically unique passkey for the device's secure vault.

Once the secure vault is unlocked via the BCI signal, the user's Augmented-ID wallet can proceed with the standard authentication flow. The wallet generates a signed, short-lived cryptographic proof of age, binding the attestation to the specific site's origin and a nonce to prevent replay attacks . This proof is what is ultimately sent to the website. The website receives the same minimal, anonymous token that any other user would receive—a verifiable assertion of age without any accompanying identity data. The critical distinction is that the BCI signal itself never leaves the user's possession. The website is completely unaware of how the user unlocked their device; it only sees the successful cryptographic proof. This architecture elegantly solves the problem by compartmentalizing the sensitive data. The neural signal is used for a single, critical purpose: on-device authentication. It is not exposed to the network, shared with third parties, or used as a persistent identifier. This approach is consistent with best practices identified in multidisciplinary research agendas for inclusive AR/VR, which caution against complex physiological dissection and advocate for the confinement of neural data to on-device processing [26](#) .

This design also addresses potential security vulnerabilities inherent in BCI systems. Threat models for such a system must account for risks like replay attacks, where an adversary attempts to reuse a captured neural signal, and compelled de-anonymization, where an attacker forces the user to reveal their identity . The use of a nonce and a domain separator in the cryptographic proof binding process mitigates replay attacks by ensuring the proof is only valid for a specific session and origin . The inclusion of a "jurisdictional_safewords" feature allows the user to refuse a verification request in a specific context, providing a mechanism to resist coercion . Furthermore, the entire process can be implemented on neuromorphic or event-driven hardware to explore low-power, on-device biometric liveness signals that never leave the device, feeding only a binary "adult" bit into the wallet . This hardware-level isolation provides a robust defense against software-based attacks and ensures that the user's neural data remains under their direct control. The security hardening measures, including the use of a TPM2.0 root of trust, ensure that keys are sealed to the hardware and cannot be extracted or copied .

The technical feasibility of using EEG/BCI for authentication has been demonstrated in research. One study developed an EEG-based BCI authentication system that achieved a false acceptance rate (FAR) of just 0.0025 and a false rejection rate (FRR) of 0.0026, with real-time inference latency under 30 seconds on consumer-grade hardware [21](#) . While this research focused on authentication to a system, the principles are directly applicable to unlocking a local wallet. The system's usability testing also showed positive results, with participants finding the headset

comfortable and willing to adopt the technology as a primary authentication method ²¹. However, it is crucial to note that current setups can be bulky and require careful calibration, urging a focus on user comfort and seamless integration rather than complex physiological analysis ²⁶. The Augmented-ID framework positions this technology not as a standalone credential but as a powerful, privacy-preserving tool for securing the user's own digital identity.

By adopting this cautious and principled approach, the Augmented-ID system avoids the pitfalls of premature and unsafe deployment of neural credentials. It acknowledges the unique challenges posed by BCI technology while harnessing its potential for secure, personalized authentication in a way that is fully aligned with the legal and ethical imperatives of HB2112. This model respects the user's autonomy by giving them ultimate control over their neural data, ensuring that their augmented identity is protected, not exploited. It creates a bridge between cutting-edge neurotechnology and mainstream digital identity, paving the way for a future where human-machine integration enhances security and convenience without compromising fundamental rights to privacy and bodily integrity.

Implementation Roadmap: From Prototyping to Policy Advocacy

The transition of the Augmented-ID concept from a theoretical framework to a practical, widely adopted reality requires a structured, phased implementation roadmap. This roadmap must balance immediate prototyping and technical validation with long-term policy advocacy and governance building. A successful strategy will deliver tangible prototypes to demonstrate feasibility while simultaneously engaging regulators and stakeholders to ensure the resulting system is legally compliant, socially acceptable, and interoperable. The agenda is divided into three key stages: immediate prototyping and technical validation, policy engagement and legal mapping, and long-term scaling and global standardization.

The first phase, immediate prototyping (spanning 0–12 months), is focused on building and testing the core technical components of the Augmented-ID system. This stage is critical for de-risking the project and generating empirical data to support future advocacy efforts. The primary goal is to develop a functional prototype of the Augmented-ID wallet, available as both a browser extension and a native mobile/desktop application. This wallet must be able to perform all

necessary cryptographic operations, including DID generation, VC issuance and presentation, and the creation of zero-knowledge proofs for age verification . Concurrently, developers must build JS/SDK shims and APIs that allow third-party websites and applications to seamlessly integrate with the wallet, enabling them to request and validate age attestations . To test the system's performance under realistic conditions, it is essential to benchmark the proof-generation time of the ZKP circuit on consumer-grade hardware to ensure it meets the typical page-load latency budgets of commercial sites, aiming for a near-instantaneous one-click experience . Initial pilots should be conducted on controlled networks, such as within public libraries, university campuses, or designated smart-city testbeds, to gather feedback and identify bugs in a safe environment ⁴⁵ . Usability studies, particularly those involving AI-augmented, neurodiverse, and disabled users, are paramount during this phase to refine the user interface and ensure the system is genuinely inclusive and easy to use . This hands-on development will produce concrete artifacts, such as the `.aln` configuration file provided in the initial query, which defines the system's policies, cryptographic parameters, and integration points, serving as a blueprint for wider deployment .

The second phase involves parallel efforts in policy engagement and legal validation. Technical feasibility alone is insufficient; the system must be demonstrably compliant with HB2112 and acceptable to regulators and courts. This requires proactive engagement with Arizona's regulatory bodies, legislators, and legal experts . A key activity will be drafting a comprehensive technical policy brief that explains how the Augmented-ID system satisfies the law's requirements . This document will detail how the system maps to the permissible verification pathways, rigorously enforces the no-retention rule for identifying information, and provides a higher degree of privacy protection than traditional methods like selfie uploads . This brief will be a cornerstone of advocacy efforts, providing policymakers with a clear and compelling argument for why a DID/ZKP-based system should be considered a "commercially reasonable method" under the statute. Furthermore, running a legal-technical workshop with Arizona privacy and First-Amendment attorneys will be invaluable for vetting the proposal's legal soundness and anticipating potential challenges . As the system matures, it will be essential to build a track record of successful, secure deployments. The UK's implementation of mandatory age checks for social media and pornography starting in July 2025, with no major security incidents reported in the first month, provides a valuable precedent for how certified providers can operate securely at scale ³⁸ . Demonstrating similar success with the Augmented-ID system will be crucial for building trust with both regulators and the public. Geographical evidence from early adopter states like Louisiana and Texas, along with European smart-city

pilots, will be used to validate the legal mappings and technical patterns in diverse regulatory environments .

The final phase, spanning 1–5 years, focuses on scaling the system globally and establishing it as a standard. The data and insights gathered from the pilot programs in the first phase will be instrumental in building a case for wider adoption. This case will emphasize the system's superior privacy outcomes—dramatically fewer privacy incidents compared to systems that collect and store raw ID data—as well as its improved usability and reduced likelihood of underage bypasses . With a solid foundation of real-world data, the next step is to engage with international standards bodies like the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF) to formalize the Augmented-ID protocol . Standardization is the key to achieving widespread interoperability, allowing any country or jurisdiction to plug in its own legal requirements, age thresholds, and verification methods into the framework. This will transform the system from a niche solution into a global infrastructure for privacy-respecting digital identity. Long-term integration plans should also explore the system's application in broader contexts, such as municipal smart-city platforms. A single, verifiable credential could be reused for multiple purposes, such as controlling access to 18+ entertainment at public kiosks, entering age-gated gaming zones, or activating restricted AR overlays, all without creating a unified profile of the citizen's behavior across these different contexts ⁵ . This vision of a modular, privacy-preserving identity ecosystem represents the ultimate goal of the Augmented-ID framework. The entire roadmap must be guided by a commitment to transparency and accountability, including publishing quarterly aggregate statistics on age-check usage by jurisdiction and undergoing regular independent audits to ensure the system continues to meet its stated privacy and security guarantees .

Implementation Phase	Timeframe	Key Objectives	Key Activities & Deliverables
Phase 1: Prototyping & Validation	0–12 Months	Build and test a functional Augmented-ID wallet and shims; validate technical performance and usability.	Develop wallet prototype (extension/app); Implement core crypto (DID, VC, ZKP); Create JS/SDK shims; Conduct usability studies; Benchmark ZKP performance.
Phase 2: Policy Engagement & Legal Mapping	Ongoing	Demonstrate legal compliance with HB2112; Engage with regulators; Build a track record of secure deployments.	Draft technical policy brief; Run legal-technical workshops; Conduct pilots in public libraries/kiosks; Publish quarterly usage stats; Establish multistakeholder oversight board.
Phase 3: Scaling & Global Standardization	1–5 Years	Achieve widespread adoption; Formalize the protocol as a global standard; Explore integration into broader ecosystems.	Use pilot data to advocate for wider adoption; Work with W3C/IETF to standardize the protocol; Integrate with smart-city platforms; Explore agentic delegation for automated flows. ⁴⁵

By following this comprehensive roadmap, the Augmented-ID concept can evolve from a visionary idea into a robust, scalable, and globally accepted solution. It offers a pragmatic pathway to resolving the fundamental conflict between child protection, privacy rights, and user dignity, paving the way for a more secure and humane digital future.

Governance and Oversight: Ensuring Fairness, Accountability, and Non-Discrimination

The successful deployment of a powerful system like Augmented-ID hinges not only on its technical soundness and legal compliance but equally on the establishment of robust governance and oversight structures. Without clear rules, transparent processes, and mechanisms for accountability, even the most privacy-preserving technology can be misused or lead to unintended negative consequences. The governance framework for Augmented-ID must be designed to proactively address issues of fairness, prevent discrimination against marginalized groups—including AI-augmented individuals—and provide clear channels for redress when things go wrong. This requires a multi-stakeholder approach that brings together legal experts, technologists, representatives from disability communities, and augmented-user advocates to collaboratively shape the system's policies and operations. This framework must encompass principles of non-discrimination, transparency, and accessibility, ensuring that the system serves all users equitably.

A cornerstone of the governance structure is a Multistakeholder Privacy Council, tasked with overseeing the system's operation and ensuring its alignment with its core principles. This council would include representatives from the legal community, technical experts specializing in cryptography and identity, disability rights organizations, and a dedicated representative from the augmented-user community. This diverse group would be responsible for reviewing the system's policies, auditing its implementation, and advising on new developments. The council's mandate would be to ensure that the system adheres to its stated commitment to non-discrimination against augmented humans and other marginalized groups. It would be empowered to review complaints and investigate instances where users believe they have been improperly denied access due to verification errors. This is a critical safeguard, as the system's automated nature could potentially lead to biases or errors that disproportionately affect certain populations. For example, if a particular demographic group has historically lower

rates of obtaining government-issued photo IDs, an overly rigid system could create barriers to access for that group [15 53](#) . The council would monitor metrics like the false denial rate by user profile to detect and address such disparities .

Transparency is another vital pillar of the governance framework. While the system's cryptographic proofs are designed to protect individual privacy, the overall operation of the system must be transparent enough to build public trust. This is achieved through regular reporting and public-facing documentation. The system's operators should publish quarterly aggregate statistics on age-check usage by jurisdiction, providing a high-level overview of the system's impact without revealing any personally identifiable information . This data can help regulators and researchers understand how the system is performing and identify any emerging trends or issues. Furthermore, the governance framework must include machine-readable law profiles that create a bidirectional mapping between the code and the statute text . This ensures that the system's implementation is always auditable against the original legal requirements, providing a clear and unambiguous record of compliance. This transparency extends to the algorithms and models used within the system. While the cryptographic proofs are opaque, the logic governing their creation—such as the parameters of the ZKP circuit or the criteria for issuing a credential—must be documented and subject to review by the oversight board. This prevents the system from becoming a "black box" where decisions are made without explanation or recourse.

Accountability and redress are essential for maintaining user trust. Even the most carefully designed system will occasionally make mistakes. When an adult user is improperly denied access, they must have a clear and accessible channel to appeal the decision . The Augmented-ID system should provide an out-of-band review process, such as a dedicated portal or email address, where users can submit their case for review by a human moderator . This process must be designed to be accessible to all users, including those with disabilities, and should provide timely and understandable responses. The governance framework must also include clear protocols for handling security incidents and data breaches. Although the system is designed to minimize the risk of data exfiltration, no system is completely immune. In the event of a breach, the response plan must prioritize user notification and mitigation, and the incident must be thoroughly investigated and publicly reported to maintain transparency. The system's contracts with third-party verifiers and issuers must include strict clauses mandating compliance with the no-retention rule, backed by stiff penalties and termination clauses for violations [92](#) .

Finally, the governance framework must be dynamic and adaptable, capable of evolving as technology and societal norms change. This involves continuous monitoring of emerging threats and advancements in cryptography, as well as staying abreast of new legislation and legal precedents related to digital identity and privacy. The oversight board should periodically review and update the system's policies to ensure they remain relevant and effective. This includes considering new types of augmentations as they emerge and assessing their potential impact on the system. The framework should also incorporate a formal process for soliciting feedback from the broader community, including end-users, researchers, and civil society organizations. This iterative process of review, feedback, and improvement will ensure that the Augmented-ID system remains a living, responsive institution that adapts to new challenges while staying true to its foundational principles of privacy, security, and human dignity. In summary, the governance and oversight structure is the guardian of the system's soul. It translates the abstract principles of fairness and non-discrimination into concrete policies and practices, ensuring that the powerful tools of decentralized identity are wielded responsibly and for the benefit of all members of society.

Reference

1. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdibl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVyYyBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA
2. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdibl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVyYyBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA
3. https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdibl91cmxfcGFyc2VfdG9fbWFya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdlYlVyYyBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEZdaQH5CgUaxwUmfEJfqTOZMoh3PbosHslSPA

wMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm
51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA

4. [https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?
key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA](https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA)
5. [https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?
key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA](https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA)
6. [https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?
key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA](https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA)
7. [https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?
key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA](https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA)
8. [https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?
key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA](https://cdn.qwenlm.ai/qwen_url_parse_to_markdown/system00-0000-0000-0000-webUrlParser?key=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyZXNvdXJjZV91c2VyX2lkIjoicXdlb191cmxhcGFyc2VfdG9fbWYya2Rvd24iLCJyZXNvdXJjZV9pZCI6InN5c3RlbTAwLTAwMDAtMDAwMC0wMDAwLXdIYlVybfFBhcnNlciIsInJlc291cmNlX2NoYXRfaWQiOm51bGx9.cz1eeZEEZdaQH5CgUaxwUmfeJfqTOZMoh3PbosHslSPA)
9. **Government Age Verification System** https://www.congress.gov/crs_external_products/R/HTML/R47884.html
10. **Understanding industry-specific age verification regulations** <https://withpersona.com/blog/age-verification-laws-by-industry/>
11. **Age Restricted Products: Compliance & Verification Guide** <https://www.displai.ai/blog/age-restricted-products-usa/>
12. **How zero-knowledge tools can help us verify ages and ...** <https://thehill.com/opinion/technology/5414009-zero-knowledge-identity-protocols/>

13. Social media age verification laws in the United States https://en.wikipedia.org/wiki/Social_media_age_verification_laws_in_the_United_States
14. Personal Identifiable Information, Parental Consent, and ... <https://publiclibrariesonline.org/2019/10/personal-identifiable-information-parental-consent-and-public-libraries/>
15. App Store Age Verification: Popular in Principle, ... <https://ccianet.org/articles/app-store-age-verification-popular-in-principle-unworkable-in-practice/>
16. Age Verification on Social Media: Laws, Tech, Risks Explained <https://sumsub.com/blog/age-verification-on-social-media/>
17. Age verification system https://en.wikipedia.org/wiki/Age_verification_system
18. Age Verification: Definition & How it Works <https://www.entrust.com/blog/2023/01/age-verification-system>
19. State Laws on Minors Online Risk Free Speech, Privacy <https://statescoop.com/state-online-age-verification-requirements-report-2024/>
20. Federal Identity, Credential, and Access Management Sub ... <https://www.idmanagement.gov/implement/mapping-of-sp800-53-ia-to-sp-800-63/>
21. Brainwave Biometrics: A Secure and Scalable Brain– ... <https://www.mdpi.com/2673-2688/6/9/205>
22. Privacy-preserving authentication protocol for user ... <https://dl.acm.org/doi/10.1016/j.csi.2025.104009>
23. December Digital Accessibility Roundup <https://disabilityin.org/articles-and-updates/december-digital-accessibility-roundup>
24. Advancing Accessible Interfaces: Evaluation of Design ... <https://dl.acm.org/doi/10.1145/3696593.3696613>
25. Op-Ed: Age Verification Technology Would Create New ... <https://cdt.org/insights/op-ed-age-verification-technology-would-create-new-barriers-for-young-disabled-people/>
26. Inclusive Augmented and Virtual Reality: A Research Agenda <https://www.tandfonline.com/doi/full/10.1080/10447318.2023.2247614>
27. HB2112 - 571R - House Bill Summary https://www.azleg.gov/legtext/57leg/1R/summary/H.HB2112_012425_CAUCUSCOW.DOCX.htm
28. HB2112 - 571R - H Ver <https://www.azleg.gov/legtext/57leg/1R/bills/HB2112H.htm>
29. Arizona Mandates Age Verification for Adult Websites, Raising ... <https://myadultattorney.com/arizona-mandates-age-verification-for-adult-websites-raising-privacy-and-access-concerns/>

30. Arizona age check law gives parents right to sue ... <https://www.biometricupdate.com/202509/arizona-age-check-law-gives-parents-right-to-sue-noncompliant-sites-10k-per-day>
31. Arizona Governor Signs Pornography Age Verification Law <https://dailycitizen.focusonthefamily.com/arizona-governor-signs-pornography-age-verification-law/>
32. GOP-backed bill requiring IDs for online porn clears first ... <https://inbuckeye.com/featured/gop-backed-bill-requiring-ids-for-online-porn-clears-first-hurdle-in-arizona/>
33. HB2112 - 571R - I Ver <https://www.azleg.gov/legtext/57leg/1r/bills/hb2112p.htm>
34. Verifiable Credentials Data Model v2.0 <https://www.w3.org/TR/vc-data-model-2.0/>
35. W3C Verifiable Credentials For Age Verification <https://everycred.com/blog/w3c-verifiable-credentials-for-age-verification/>
36. What is Zero-Knowledge Proof - a hot technology bringing ... <https://www.nttdata.com/global/en/insights/focus/2024/what-is-zero-knowledge-proof>
37. The impact of zero-knowledge proofs on data minimisation ... <https://policyreview.info/articles/analysis/impact-zero-knowledge-proofs>
38. AVPA Response to Center for Democracy & Technology's ... <https://avpassociation.com/thought-leadership/avpa-response-to-center-for-democracy-technologys-user-research/>
39. NIST Special Publication 800-63A <https://pages.nist.gov/800-63-3/sp800-63a.html>
40. NIST SP 800-63 Digital Identity Guidelines-FAQ <https://pages.nist.gov/800-63-FAQ/>
41. NIST SP 800-63 - Azure Compliance <https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-nist-800-63>
42. NIST SP 800-63-3 & 63-4: Digital Identity Guidelines <https://blog.hypr.com/nist-sp-800-63-3-digital-identity-guidelines-review>
43. Complying with NIST SP 800-63-4 Standards <https://www.pingidentity.com/en/resources/blog/post/complying-with-nist-standards.html>
44. NIST Special Publication 800-63-3 <https://pages.nist.gov/800-63-3/sp800-63-3.html>
45. NIST SP 800-63-4: The Future of Digital Identity is Here <https://www.intercede.com/nist-sp-800-63-4-the-future-of-digital-identity-is-here-and-intercede-is-ready/>

46. Zero knowledge proofs reveal their utility for age ... <https://www.biometricupdate.com/202505/zero-knowledge-proofs-reveal-their-utility-for-age-verification-and-beyond-aztec>
47. The limits of zero-knowledge for age-verification <https://brave.com/blog/zkp-age-verification-limits/>
48. Zero Knowledge Proofs Alone Are Not a Digital ID Solution ... <https://www.eff.org/deeplinks/2025/07/zero-knowledge-proofs-alone-are-not-digital-id-solution-protecting-user-privacy>
49. Demonstration of a privacy-preserving age verification process <https://linc.cnil.fr/en/demonstration-privacy-preserving-age-verification-process>
50. Accessibility Rules Are Driving Library Upgrades <https://www.bibliotheca.com/library-accessibility-self-service-upgrades/>
51. A Complete Guide to Protecting Patron Data <https://estarkiosks.com/library-kiosk-security/>
52. The Future of Age Verification: Balancing Privacy, Trust, ... <https://privateid.com/the-future-of-age-verification/>
53. Privacy And Ethical Concerns Related to Age Verification <https://facia.ai/blog/privacy-concerns-related-to-age-verification-systems/>
54. Best Practices for Designing User-Friendly Age Verification ... <https://salespanel.io/resources/age-verification-popups/>
55. AZ HB2112 - Bill <https://www.billtrack50.com/billdetail/1778738>
56. Republicans advance strict online porn age verification bill ... <https://azmirror.com/briefs/republicans-advance-strict-online-porn-age-verification-bill-amid-privacy-concerns/>
57. New law requires age verification for adult websites in ... <https://azcapitoltimes.com/news/2025/09/22/new-law-requires-age-verification-for-adult-websites-in-arizona/>
58. Act amending Arizona Revised Statutes to include internet ... <https://digitalpolicyalert.org/change/15818-age-verification-requirement-for-online-distribution-of-sexual-material-harmful-hb-2112>
59. How Arizona's porn law could backfire <https://www.arizonaagenda.com/p/how-arizonas-porn-law-could-backfire>
60. Are 'zero-knowledge proofs' the future of online age ... <https://statescoop.com/report-zero-knowledge-future-of-age-verification-tech-2025/>
61. Buckeye lawmaker's bill requiring age checks on porn sites ... <https://inbuckeye.com/featured/buckeye-lawmakers-bill-requiring-age-checks-on-porn-sites-takes-effect-friday/>

62. Cryptographers' Feedback on the EU Digital Identity's ARF <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/discussions/211>
63. Session Topics from the Internet Identity Workshop since 2005 <https://decentralized-id.com/workshops/internet-identity-workshop/>
64. Polygon ID is More than Biometric Proof of Personhood <https://polygon.technology/blog/polygon-id-is-more-than-biometric-proof-of-personhood>
65. DID - Dock SDK Tutorial https://docknetwork.github.io/sdk/tutorials/concepts_did.html
66. How to register a DID document | EBSI hub <https://hub.ebsi.eu/vc-framework/guidelines/didr>
67. An API for accessing Public Key Credentials - Level 3 <https://www.w3.org/TR/webauthn-3/>
68. Overall architecture - European Age Verification Solution <https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications/>
69. Verifiable Credentials Data Model v2.1 - W3C on GitHub <https://w3c.github.io/vc-data-model/?ref=blog.identity.foundation>
70. Deloitte's first Disability Inclusion @ Work 2024 survey ... <https://www.deloitte.com/global/en/about/press-room/deloittes-first-disability-inclusion-work-2024.html>
71. Disability Inclusion @ Work 2024: A Global Outlook <https://www.deloitte.com/global/en/issues/work/content/disability-inclusion-at-work.html>
72. Disability Inclusion @ Work 2024: A Global Outlook https://www.linkedin.com/posts/elizabethfaberusa_disability-inclusion-work-2024-a-global-activity-7269761855345119234-nKHd
73. Disability inclusion at work report <https://www.deloitte.com/uk/en/about/press-room/deloitte-first-disability-inclusion-at-work-report.html>
74. U.S. Access Board Presents Preliminary Findings on ... <https://www.access-board.gov/news/2024/11/07/u-s-access-board-presents-preliminary-findings-on-artificial-intelligence-ai-for-disability-community-and-ai-practitioners/>
75. Public Right-Of-Way, AI, Medicaid Renewals, and More <http://acl.gov/news-and-events/acl-blog/policy-round-public-right-way-ai-medicaid-renewals-and-more>
76. Sec 41-151.22. Privacy of user records; violation <https://az.elaws.us/ars/41-151.22>
77. New law requires age verification for adult websites in ... <https://roselawgroupreporter.com/2025/09/new-law-requires-age-verification-for-adult-websites-in-arizona/>

78. Decentralized Identifiers (DIDs) | NEAR Documentation <https://docs.near.org/primitives/did>
79. Indy DID Method Specification - Hyperledger Foundation <https://hyperledger.github.io/indy-did-method/>
80. Web Authentication: An API for accessing Public Key ... <https://www.w3.org/TR/webauthn-2/>
81. An Overview of WebAuthn <https://curity.io/resources/learn/webauthn-overview/>
82. Attestation and Assertion - Web APIs | MDN https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API/Attestation_and_Assertion
83. Guide to Web Authentication <https://webauthn.guide/>
84. Securing WebAuthn with Attestation https://developers.yubico.com/WebAuthn/Concepts/Securing_WebAuthn_with_Attestation.html
85. What is Attestation in WebAuthn? <https://www.corbado.com/glossary/attestation>
86. Inclusive digitalized urban public facilities for sustainable ... <https://www.sciencedirect.com/science/article/pii/S2210670725006407>
87. (PDF) Comparative Analysis of Usability and Accessibility ... https://www.researchgate.net/publication/368901764_Comparative_Analysis_of_Usability_and_Accessibility_of_Kiosks_for_People_with_Disabilities
88. Kiosk UX UI -- Design Checklist <https://kioskindustry.org/kiosk-ux-ui-how-to-design-checklist/>
89. The Effects of Smart Home Interface Touch Button Design ... <https://pmc.ncbi.nlm.nih.gov/articles/PMC8872557/>
90. Web Content Accessibility Guidelines (WCAG) 2.2 <https://www.w3.org/TR/WCAG22/>
91. Kiosk User Testing - by Sydney Kunz <https://medium.com/@sydkunz/kiosk-user-testing-53e75b0a1028>
92. Usability Testing With Older Adults <https://www.nngroup.com/articles/usability-testing-older-adults/>
93. The Psychology Behind Kiosk Interaction <https://www.mvix.com/blog/kiosk-interaction>
94. Best Practices of Kiosk Installations in Low-Connectivity ... <https://www.wavetec.com/blog/best-practices-of-kiosk-installations-in-low-connectivity-zones/>
95. DID — blockchain-core documentation <https://api-blockchain-core.readthedocs.io/en/latest/profile/did.html>