Proposal for a Wallet/Credential Manager Framework for Age Assurance Solutions

A Multistakeholder Dialogue on Assurance

November 2025

Centre for Information Policy Leadership (CIPL) & WeProtect Global Alliance

A Multistakeholder Dialogue on Age Assurance

Proposal for a Wallet/ Credential Manager Framework
for Age Assurance Solutions

Introduction

The digital world, while offering unparalleled opportunities for education, connection, and creativity, also presents challenges in safeguarding children and young people from age-inappropriate experiences. The current landscape of online age assurance remains fragmented, characterised by inconsistent technical implementations and a lack of unified standards. This not only burdens app developers and other service providers but, crucially, leads to a disjointed and often frustrating experience for users themselves - including for parents.

Recognising this critical need, we commend the European Commission's proactive steps in addressing online safety for minors, particularly through initiatives under the Digital Services Act (DSA) and the ongoing development of an EU-wide age verification framework. In this context, we are pleased to note that the recently released Commission guidelines under Article 28 of the DSA align well with the vision of a robust and privacy-preserving age assurance framework CIPL is working to develop. The Commission's commitment to fostering a safer internet for kids (BIK+ Strategy) and exploring privacy-preserving solutions, such as the age verification app leveraging zero knowledge proof (ZKP) technologies and the upcoming European Digital Identity (EUDI) Wallet, is a vital step forward. Similarly, in the UK Ofcom has issued extensive guidance on effective age assurance for different service levels in scope of the UK Online Safety Act and lists a variety of age assurance methods that can be considered highly effective. It also highlights the importance of interoperability between the possible age assurance methods, to ensure a more streamlined experience for the user and ultimately limit the collection of personal data.

We agree that further potential for protecting minors and streamlining compliance lies in enabling further choice for developers to leverage some of the recent advancements made by technology platforms. The introduction of credential management APIs - which empower users to share identity signals from their preferred stored credential with relying parties - by companies like Google[1] and Apple[2] represents a pivotal moment. These APIs offer the promise of standardised, privacy-preserving mechanisms for age

[1] Google. 2024. Credential Manager API. Android Developers. https://android-developers.googleblog.com/2024/12/build-high-quality-enagaing-age-appropriate-apps.html
[2] Apple. 2024. Declared Age Range API. Apple Developer Documentation. https://developer.apple.com/support/downloads/Helping-Protect-Kids-Online-2025.pdf

assurance that could be used by app developers and website providers to offer flexible age-appropriate experiences to their users.

However, the efficacy of these promising developments hinges on the development of a broader, interoperable framework. By defining shared principles, technical standards, and levels of assurance, these powerful APIs can operate seamlessly across diverse platforms, providers, and jurisdictions. This would deliver significant benefits for all stakeholders:

- for all users, a consistent, less intrusive, and highly secure experience when verifying their age online;
- for minors, a more age-appropriate experience across the mobile ecosystem;
- for developers, drastically reduced complexity and uncertainty by providing clear guidelines and alleviating the burden of navigating disparate regulatory requirements.

For this to occur, industry needs key regulators in both the privacy and content spheres to encourage these developments by aligning on practical, flexible guidance that:

- holds companies who know their services' risks best ultimately responsible for implementing age assurance that is proportionate to those risks;
- recognises that companies' good faith efforts to address appropriate age assurance on their services should be supported if they offer adequate protection without forcing companies to adopt new approaches;
- balances the need to protect user privacy with the need to provide robust age signals to support age appropriate experiences;
- incentivises cross-industry standards through recognition of developing and other standards that promote consistency; and
- spurs adoption and integration of official digital credentials and related apps by supporting integration with developing industry approaches to expand usage and promote interoperable methods that support the entire ecosystem.

This discussion document provides a draft framework to support an interoperable approach to age assurance. It outlines principles and elements for consideration as a part of an infrastructure approach, while acknowledging that developers may choose alternative and/or complementary approaches to meet their age assurance objectives or regulatory obligations. Digital credentials infrastructure could be a powerful option for interoperability and user convenience but should not be considered a mandatory single point of entry.

1. Framework Objectives

The proposed Interoperability Framework for Age Assurance Solutions seeks to:

- Leverage a **common taxonomy** and classification of age assurance methods: This aims to create a shared understanding and common language for all stakeholders. It involves defining and classifying different methods based on their confidence levels (Levels of Assurance - LoA) and the associated privacy impacts (e.g., anonymous, pseudonymised, identifiable). An example is the latest ISO standard draft.

- Promote the need for **technical standardisation** for signal generation, exchange, and verification: There is a need to develop and promote robust, privacy-preserving technical standards for how age signals are generated, exchanged and verified. This includes emphasising data minimisation principles and exploring advanced Privacy-Enhancing Technologies (PETs), like ZKP technologies[3], ensuring seamless and secure data flow while protecting user privacy. For example, through the ongoing efforts to finalise an ISO framework on age assurance.
- Support **trust and accountability** among ecosystem actors (governments, regulators, providers, platforms, users): Beyond technical specifications, building confidence in the system is paramount. We believe a crucial consideration is comprehensive user education. As this introduces a fundamentally new digital experience for users interacting with apps and websites, a robust educational component will be essential to successfully introduce and embed this new approach for both child and adult users. Thus, this objective focuses on establishing mechanisms for transparency, ensuring users understand how their age is verified and what data is used and stored through, among other things, where common user interfaces could be used to help develop user comfort with verification. Supporting relying parties like developers in understanding the source and reliability of relevant signals is also paramount and part of this effort.
- Create pathways for **cross-jurisdictional recognition** and mutual compatibility: This includes exploring mechanisms for mutual compatibility and recognition, leveraging existing EU initiatives like the European Digital Identity (EUDI) Wallet for recognised age credentials. Such pathways are crucial for reducing duplication of effort and ensuring a consistent user experience across the single market and beyond.

2. Foundational Principles

2.1. Risk-Based Proportionality

[3] Zero-knowledge proof is a technique that enables one party (the prover) to prove a claim to another party (the verifier) without revealing anything more than the truth of the claim. Through the use of complex mathematical algorithms, the proof is generated in such a way that it is computationally infeasible for someone who does not know the claim to generate a similar or related proof.
A zero-knowledge proof has three main properties:

- Completeness: If the claim being proved is true, then an honest verifier will be convinced of this fact with high probability.
- Soundness: If the prover does not know the claim, then he cannot deceive the verifier with high probability.
- Zero-knowledge: The verifier does not learn anything other than the validity of the claim. There are two main types of zero-knowledge proofs: interactive and non-interactive.

Centre for Information Policy Leadership (2023) *Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age*.
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf

A key principle underpinning an effective and proportionate age assurance framework is the adoption of a risk-based approach. This means that the stringency and invasiveness of the age assurance method applied should be commensurate with the potential harm that age-inappropriate content or experiences could pose to a minor. Instead of a "one-size-fits-all" solution, a risk-based approach allows for flexibility, ensuring that less intrusive methods are used for lower-risk scenarios, while more robust verification is reserved for higher-risk contexts.

While first-party mechanisms, such as machine learning-based age estimation models, can be suitable for certain contexts, access to some high-risk 18+ goods and services may require a higher degree of confidence in age verification (e.g., adult content, gambling).

Risk levels should be aligned with service-specific risk assessments, where available, drawing on approaches such as **Ofcom's risk-based model** under the UK Online Safety Act or the Commission's similar approach with regard to minor risks in the proposed Guidelines for Article 28 of the DSA. More broadly, companies should understand the risks posed by their services where those are likely to be accessed by children and be expected to apply the level of assurance best suited to address those risks.

2.2. Privacy by Design

In line with the foundational principles of data protection and privacy, particularly those enshrined in the GDPR, any age assurance framework must be designed and implemented with a paramount focus on safeguarding personal data. This commitment necessitates a proactive and integrated approach that prioritises several key areas:

Age assurance must be implemented in accordance with data protection and privacy principles, prioritising:

- **Data minimisation**: The system must be engineered to collect and process only the minimum amount of personal data necessary to confirm age. The aim is to achieve the desired level of assurance with the least possible data footprint and providing the minimum needed signal. Ideally, data protection authorities will align on support of a range of appropriate signals.
- **Anonymisation or pseudonymisation**: Rather than linking age directly to a user's real-world identity, interoperable age assurance mechanisms should strive to operate with data that has been obfuscated in a manner that mitigates risks of reidentification. This reduces the risk associated with data breaches and enhances user privacy by default.

PETs can support robust age assurance while maintaining privacy. For example:

- Zero-knowledge proofs: ZKP technology allows users to prove they meet a certain age requirement without revealing unnecessary personal details.
- Selective disclosure credentials: Building upon verifiable credentials, this would allow users to selectively disclose only the specific attributes required for age verification (e.g., "over 18") from a broader digital identity credential, rather than revealing their full identity document.
- Cryptographic age attestations: These involve trusted third parties issuing signed attestations of a user's age, which can then be presented to service providers without the need for the service provider to directly interact with the identity provider or store sensitive age data.

2.3. Transparency and User Autonomy

User empowerment and transparency are cornerstones of a trustworthy age assurance framework. All users, regardless of their technical proficiency, should receive clear, accessible, and concise information about:

- The nature of an age check: This includes explaining *why* an age check is required for a particular service or experience.
- Available redress mechanisms: Users should be able to obtain their age information and be provided the ability to request an update if they believe it is incorrect.
- Users should be empowered with a level of control over their age information and should be asked to consent to the sharing of their information.
- Where necessary, parents or guardians should have that same level of control over the sharing of the age information of the supervised child.

3. Interoperability Standards for Digital Credential Holders

3.1. Platform Neutrality

Digital credential holders, including for example digital wallet providers (private or government backed digital wallets) or digital age verification apps, can allow users to store assurances for their age (e.g., verified credentials from a trusted issuer) in their digital wallets or similar credential holder. Digital credential holders can leverage trusted credentials from first or third parties, or tools available through the digital wallet, including verification by government or other official IDs.

Digital credential holders should allow users to share assured age signals from trusted credentials in their digital wallets. For example, users should be able to share assured age signals with:

- app stores to download age gated app;
- app developers when registering for an account on an age gated service;
- app developers to access age gated features;
- web browser apps when seeking to access an age gated website.

Digital credential holders should work with industry to consider whether and how to support the integration of other forms of age assurance into the digital wallet model, including estimation (such as facial recognition) and inference technologies (such as models analysing user behavior).

Where credential APIs are provided by an operating system or elsewhere in the software stack, these should support sharing age-related information between users and developers through digital wallets or other digital credential holders.

3.2. Standards

The framework needs to be flexible enough to accommodate diverse regulatory landscape, including technical specifications from multiple regulators operating in different regulatory contexts, for example:

- Security standards are a key consideration, particularly when thinking beyond government-issued IDs and credentialed solutions. This could be handled through the developing ISO standard or a similarly respected body.

4. Roles and Responsibilities

4.1. Age Assurance Providers

In an infrastructure built on trust and verifiable credentials, allocation of responsibility is paramount. Therefore, a fundamental principle of this framework is that the original issuer of the credential bears responsibility for the accuracy and validity of the age signal it provides related to that credential, as appropriate based on the facts and circumstances.

This means that the entity which initially verifies a user's age (e.g., a government body issuing a digital ID, a bank performing KYC, or an accredited third-party age verification service) and subsequently issues a verifiable age credential or attestation, is accountable for the correctness of that information at the point of issuance, taking into account the agreed-upon level of assurance of the credential and having exercised reasonable care.

4.2. Credential Holders

While the issuer holds responsibility for the accuracy of the age credential itself, it is equally crucial to define the scope of accountability for other actors within the age assurance ecosystem, particularly digital wallet providers or other parties providing the infrastructure to facilitate the sharing of age information.

4.3. API Providers

Credential APIs are foundational infrastructure. Providers of this technology are primarily responsible for ensuring the technical integrity and functionality of the mechanisms that enable the user to present their age credential to a relying party and are neither processors nor controllers. Ensuring these providers are appropriately positioned with liability protections, for example regarding the accuracy of the age signal they convey, will help spur continued innovation.

4.4. App Developers and Website Providers

The framework must empower app developers and website providers with the flexibility to specify their precise needs regarding age assurance, aligned with their service's risk profile and regulatory obligations, where they chose to rely on a third-party signal via this framework. This means:

- App developers and website providers should be able to specify the *level of assured age signal* they require from a digital credential holder, based on available signal and the assessment of their compliance needs. This could range from a simple confirmation of being above a certain age threshold (e.g., "over 18") to a precise date of birth, depending on their specific requirements. Users should have the choice whether to share after receiving sufficient notice.

- The app developer and website provider are solely responsible and liable for decisions when and how to use that assured age signal, including whether it needs that age signal, depending on the risks associated with their service, user choice, and regulatory guidance.